IJACSA
WHERE WISDOM SHARES
International Journal of Advanced Computer Science and Applications

Volume 6 Issue 9

September 2015

ISSN 2156-5570(Online)
ISSN 2158-107X(Print)

SAI

www.ijacsa.thesai.org

Editorial Preface

From the Desk of Managing Editor…

It may be difficult to imagine that almost half a century ago we used computers far less sophisticated than current home desktop computers to put a man on the moon. In that 50 year span, the field of computer science has exploded.

Computer science has opened new avenues for thought and experimentation. What began as a way to simplify the calculation process has given birth to technology once only imagined by the human mind. The ability to communicate and share ideas even though collaborators are half a world away and exploration of not just the stars above but the internal workings of the human genome are some of the ways that this field has moved at an exponential pace.

At the International Journal of Advanced Computer Science and Applications it is our mission to provide an outlet for quality research. We want to promote universal access and opportunities for the international scientific community to share and disseminate scientific and technical information.

We believe in spreading knowledge of computer science and its applications to all classes of audiences. That is why we deliver up-to-date, authoritative coverage and offer open access of all our articles. Our archives have served as a place to provoke philosophical, theoretical, and empirical ideas from some of the finest minds in the field.

We utilize the talents and experience of editor and reviewers working at Universities and Institutions from around the world. We would like to express our gratitude to all authors, whose research results have been published in our journal, as well as our referees for their in-depth evaluations. Our high standards are maintained through a double blind review process.

We hope that this edition of IJACSA inspires and entices you to submit your own contributions in upcoming issues. Thank you for sharing wisdom.

Thank you for Sharing Wisdom!

Managing Editor
IJACSA
Volume 6 Issue 9 September 2015
ISSN 2156-5570 (Online)
ISSN 2158-107X (Print)

Editorial Board

Reviewer Board Members

CONTENTS

Development of Social Media GIS to Support Information Utilization from Normal Times to Disaster Outbreak Times

Kayoko YAMAMOTO
Associate Professor,
Graduate School of Information Systems,
University of Electro-Communications
Tokyo, Japan

Shun FUJITA
Graduate School Student,
Graduate School of Information Systems,
University of Electro-Communications
Tokyo, Japan

***Abstract*—The present study aims to design, develop, operate and evaluate a social media GIS (Geographical Information Systems) specially tailored to mash-up the information that local residents and governments provide to support information utilization from normal times to disaster outbreak times in order to promote disaster reduction. The conclusions of the present study are summarized in the following three points. (1) Social media GIS, an information system which integrates a Web-GIS, an SNS and Twitter in addition to an information classification function, a button function and a ranking function into a single system, was developed. This made it propose an information utilization system based on the assumption of disaster outbreak times when information overload happens as well as normal times. (2) The social media GIS was operated for fifty local residents who are more than 18 years old for ten weeks in Mitaka City of Tokyo metropolis. Although about 32% of the users were in their forties, about 30% were aged fifties, and more than 10% of the users were in their twenties, thirties and sixties or more. (3) The access survey showed that 260 pieces of disaster information were distributed throughout the whole city of Mitaka. Among the disaster information, danger-related information occupied 20%, safety-related information occupied 68%, and other information occupied 12%.**

Keywords—Social Media GIS; Web-GIS; SNS; Twitter; Disaster Information; Disaster Reduction; Support for Information Utilization

I. Introduction

According to the White Paper on Disaster Management (2012) [1], measures for disaster prevention and reduction of the effects of natural disasters in Japan include “self-help”, “mutual help (cooperation)”, and “public help (rescue and assistance by public bodies)”. “Self-help” refers to local residents, businesses, and other entities protecting themselves from disaster; “mutual help (cooperation)” refers to local communities helping each other; and “public help” refers to measures by government bodies such as national and local governments. Further, the most fundamental form of help was said to be self-help, which involves measures taken by individuals. Nowadays, anybody, anywhere, anytime can use an information system to easily send, receive, and share information, and through the effective use of information systems, disaster information possessed by local residents can be accumulated and shared.

Additionally, the Science Council of Japan (2008) [2] divided “local knowledge” into “expert knowledge” based on scientific knowledge, and “experience-based knowledge” produced by the experiences of local residents, and indicated its importance. Concerning “local knowledge” that is the “experience-based knowledge” of local residents, and exists as “tacit knowledge” that is not visualized if it is not communicated to others, as a measure for disaster prevention and reduction, it is essential for the “experience-based knowledge” to be transformed into “explicit knowledge” which is of a form that can be accumulated, organized, utilized, and made publicly available through the use of information systems, and to have local related entities accumulate the knowledge together. Moreover, Committee for Policy Planning on Disaster Management – Final Report by the Central Disaster Management Council (2012) [3] particularly specified the importance of the roles of GIS (Geographic Information Systems) and social media in the collection and transmission of disaster information.

Regarding the examples of disaster management in other parts of the world, Greene (2002) [4] proposed five stages of disaster – identification and planning, mitigation, preparedness, response, and recovery –, and shows how GIS processes can be incorporated into each. Vivacqua et al. (2012) [5] considered the four phases of emergency management which are related in a cyclic fashion: mitigation, preparedness, response, and recovery. They discussed possibilities for the introduction of collective knowledge in emergency response systems. Mansourian et al. (2006) [6] addressed the role of Spatial Data Infrastructure (SDI) as a framework for the development of a web-based system to facilitate disaster management with emphasis on the response phase in Iran. Neuvel et al. (2012) [7] proposed the network-centric concept of spatial decision support for risk and emergency management in Netherland. In the present study, firstly, with reference to the White Paper on Disaster Management (2012) [8], Committee for Policy Planning on Disaster Management – Final Report (2012) [3], and Vivacqua et al. (2012) [5], disaster risk management is divided into three stages – normal times, disaster outbreak times, and times of recovery and reconstruction –.

In Japan, as a disaster countermeasure, local governments provide information to local residents in the form of disaster prevention maps and hazard maps which show local hazardous places, evacuation sites and so on. However, this information is mainly published as maps that are in paper form or in PDF format on the website. Therefore, it is difficult to update the information on disaster prevention maps and hazard maps in real time, and these forms of information are not very suited to being shared during a disaster outbreak. Further, so that information can be efficiently accumulated and shared during a disaster outbreak, it is desirable that information systems which people are accustomed to using in normal times can be used as is during disasters. However, when a disaster occurs, a situation where the amount of submitted information increases, and there is an excessive amount of information can be expected; therefore, it is necessary for systems to automatically classify submitted information.

Against the above-mentioned background, the present study aims to design and develop a social media GIS for reducing the effects of natural disasters in normal times through to disaster outbreak times. This is achieved by designing and developing a social media GIS that integrates a Web-GIS with an SNS and Twitter, and includes a function for classifying submitted information. The social media GIS enables disaster information provided by local residents and governments to be mashed up on a GIS base map, and for the information to be classified and provided to support the utilization of the information by local residents. Further, the present study also aims to operate the social media GIS and evaluate the operation. During normal times when there is no disaster, disaster information is collected via the SNS, and local disaster information is accumulated. Through this, the system aims to improve the disaster prevention awareness of local residents. Further, during disaster outbreaks when there is an excess of information, if a communications environment (electricity, internet, information terminals, etc.) can be secured, the system aims to support evacuation activities by automatically classifying disaster information, promptly displaying it on the digital map of the Web-GIS, and ensuring its noticeability. Through having people use the system routinely and get used to it in normal times in this manner, the possibility that the system can be effectively used with no problem as a means for reducing the effects of natural disasters even in tense situations during disaster outbreaks can be anticipated.

II. Related Work

The aim of the present study is to develop a social media GIS that supports the utilization of disaster information and acts as a measure for reducing the effects of natural disasters from normal times through to disaster outbreak times. Therefore, prior research in fields related to the present study [9]-[26] can be classified into the following three areas: (1) Research relating to system development which utilizes GIS; (2) Research relating to the development of social media GIS; and (3) Research relating to proposals for systems that classify submitted information.

As representative examples of research in recent years, in the research area of (1), as a measure to reduce the effects of natural disasters during normal times, Murakami et al. (2009) [9] developed a system that supports disaster prevention workshops by using a GIS. In the research area of (2), Okuma et al. (2013) [10] developed a social media GIS that integrated a Web-GIS, an SNS, and Twitter, and demonstrated improvement of local residents' disaster prevention awareness through the accumulation of disaster information, as a measure for reducing the effects of natural disasters during normal times. Further, Murakoshi et al. (2014) [11] integrated a function for classifying submitted information into the social media GIS of Okuma et al. (2013) [10], and developed a system effective as a measure for reducing the effects of natural disasters from normal times through to disaster outbreak times. Yamanaka et al. (2010) [12] proposed a support system for situation assessment which utilized text data with spatio-temporal information and was designed for use by managers of facilities. They conducted an experiment in a large-scale park which involved a hypothetical disaster outbreak, summarized submitted text data information, and displayed the congested local situation on a web map using icons as messages. Further, Moriya et al. (2009) [13] proposed a system in which text data relating to local information in blogs was used to display the local situation (such as image, impression, and atmosphere of a place) on a web map by using circular depictions.

In the above-mentioned prior research in fields related to the present study, measures for reducing the effects of natural disasters during normal times include development of a system which uses GIS to support disaster prevention workshops, and development of a social media GIS which accumulates disaster information. Government measures include the Japanese Ministry of Land, Infrastructure, Transport and Tourism's Hazard Map Portal Site (1), and disaster prevention maps and hazard maps provided by local governments. Further, there is research which proposed a system which utilizes text data to display the local situation on a web map using icons and circles which was demonstrated as being useful. However, except for in research by Murakoshi et al. (2014) [11], up to now, there has not been development of a system designed for use from normal times through to disaster outbreak times which, in order to reduce the effects of natural disasters on a sustained and continuous basis throughout such periods, supports utilization of disaster information possessed by local residents by automatically classifying disaster information provided by local residents and promptly displaying it, and providing it on a GIS base map together with disaster information provided by governments with which it is mashed up. Therefore, the present study is based on the research results of Murakoshi et al. (2014) [11] in particular, and is unique in that it uniquely designs and develops a social media GIS aimed at realizing the features outlined above. Further, the present study is unique in that it operates the social media GIS and conduct an evaluation of the operation.

III. Research Outline and Method

In the present study, research is conducted according to the following outline and method. Firstly, a social media GIS which specializes in the aim of the present study is uniquely designed (Section IV) and developed (Section V). Next, anticipating users are the general public who are more than 18 years, an operation test and operation of the social Media GIS (Section VI) are conducted. Further, the system is evaluated and measures for improving use of the system are identified

(Section VII). Anticipating that each user will use the system for about a month, an operation test and an evaluation of operation test are conducted, and then actual operation is conducted. In addition, access is analyzed using log data during the period of actual operation, and submitted information is analyzed. Based on the results of these steps, the system is evaluated, and measures for using the system in order to more effectively support people utilizing disaster information are identified. Mitaka City of Tokyo metropolis was selected as the region for operation. This is because Mitaka City is the advanced local government of regional computerization in Japan, and cooperated with the present study.

IV. Design of the System

A. System Features

In the present study, a social media GIS effective in supporting the utilization of disaster information has a design in which a function capable of classifying and displaying submitted information according to location information and content is included in a system which combines three web applications – a Web-GIS, an SNS and Twitter, as shown in Fig. 1. The system has a structure in which the Web-GIS and the submitted information classification function are installed in the SNS. Use of the SNS and twitter enables provision of information from local residents, and enables local information concerning disasters possessed by local residents as tacit knowledge to be converted to explicit knowledge, and accumulated and shared among users. During normal times, through the SNS and twitter, local residents who are the users of the social media GIS will submit information such as information concerning dangerous and safe places in disaster outbreak times which is not noted in detail on disaster prevention maps or hazard maps produced by the government. In disaster outbreak times, through the SNS and Twitter, the local residents will submit similar information, after ensuring their own safety. Further, disaster information provided by the government in normal times, such as that concerning overall degree of danger and facilities that provide support in disaster outbreak times, will be accumulated in advance, and disaster information provided by the government during disasters will also be collected and accumulated.

The above-mentioned disaster information submitted by local residents and disaster information provided by the government will be saved in a database, and the former information will be classified according to location information and content. Together with the disaster information from the government, the classified information will be integrated into the Web-GIS, mashed up on a digital map, and visualized. Therefore, on the Web-GIS digital map, even in situations where a disaster has occurred and there is an excess of information, high noticeability of all submitted information can be maintained, and on the digital map, users can efficiently accumulate and share disaster information which includes location information among themselves.

Based on the above, the usefulness of the present system lies in the fact that it can ease the restrictions mentioned in the following three points:

1) Bidirectionality of information transmission: In this system, information submission and viewing functions are installed in the SNS. This allows all users to submit and view information anytime from anywhere regardless of whether it is during normal times or disaster outbreak times.

2) Mitigation of burden of obtaining information: In this system, the system automatically classifies submitted information and displays it on the digital map of the Web-GIS. Therefore information can be processed in real time, and users can easily determine the riskiness and safety of places that is conveyed by the information. Further, the situation where a user does not know their own present location outside has been anticipated, and the system obtains location information and displays facilities that provide support during disasters in the neighborhood where the user is located, and also displays information submitted concerning the neighborhood where the user is located. Therefore the system can reduce the burden experienced when obtaining disaster information.

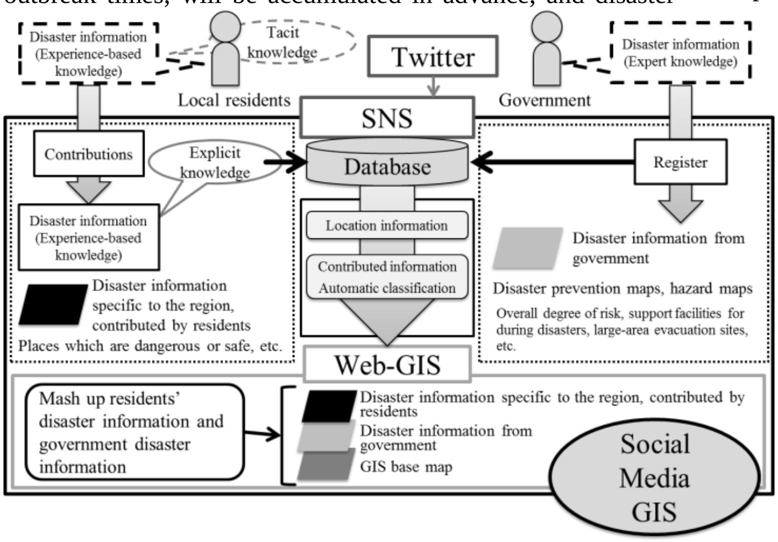


Fig. 1. System design of social Media GIS

3) Mitigation of spatial and temporal restrictions: The information terminals that this system is designed for use with are PCs and mobile information terminals. Concerning the latter, the system is designed for use with smartphones and tablet terminals, whose use has rapidly spread in recent years. Both these types of mobile information terminals have touch panels with large screens, making them easy to use when dealing with digital maps, and both types allow connection to the internet from anywhere via mobile phone data communication networks. Anticipating the situation of users using the system outdoors as well during both normal times and disaster outbreak times, a system compatible with both PCs and mobile information terminals has been designed and developed. Thanks to this, the system can be used anytime, regardless of whether the user is indoors or outdoors.

B. System Design

1) System configuration

The social media GIS of the present study is formed using three servers - a web server, a database server, and a GIS server. The web server mainly performs processing related to the SNS, and accesses the GIS server and the database server to integrate each of the functions. The SNS is operated using JavaScript and PHP, and the database server is managed using MySQL, and stores disaster information submitted by local residents which is collected through the SNS and Twitter, and disaster information from the government. For the web server and the database server, the rental server of the information infrastructure center of the organization to which the authors belong was used. For the GIS server, as the OS, Microsoft Corporation’s Windows Server 2008 was used, and as the GIS server software, Esri’s ArcGIS Server 10.0 was used.

2) Web-GIS

In the present study, for the Web-GIS, Esri’s ArcGIS Server 10.0 was used, and for the GIS base map of the Web-GIS, the SHAPE version (Rel.8) of Shobunsha Publications, Inc.’s MAPPLE10000, which is part of their MAPPLE digital map data and includes detailed road system data, was used. As the map that was superimposed with this digital map data, the user interface of Google Maps was used. Among the options provided by Esri that are ArcGIS Server 10.0 API targets, the Google Maps user interface is the one that has been used the most in earlier studies in fields related to the present study. Concerning the superimposition of MAPPLE10000 (SHAPE version) and Google Maps, Google Maps employs the new geodetic system coordinates, while MAPPLE10000 conforms to the former geodetic system coordinates; therefore, ArcTky2Jgd, which is provided by Esri as product support, was used to convert the MAPPLE10000 geodetic system coordinates to the new coordinates. Furthermore, editing was performed using ArcMap 10.0 such that disaster information provided by Mitaka City and the Metropolis of Tokyo, the regions for operation, and information peculiar to each place could be input.

Since the object of the present study is disaster information, users can use the Web-GIS to refer to a detailed road system that includes small streets that is output from MAPPLE10000, and by doing so they can accurately check locations related to submitted information, and in particular, precisely display disaster information related to the risk and safety of evacuation routes in disaster outbreak times. Further, the system has been set such that when the PC interface for users is used, the digital map can be viewed using full screen display. Thanks to this, users can get a general view of submitted information over a wide range, and enlarge the digital map to check information in detail.

3) SNS

In the present study, an SNS was firstly selected as the social media for integration with the Web-GIS. The SNS was uniquely designed and developed to suit the objectives of the present study. An SNS was chosen because if an SNS is used, the system can be uniquely designed and developed to suit the objectives of use, and detailed system configuration can be performed to suit regional characteristics of the regions in which the system is to be operated. In this system, community functions limiting topics and users were not included, and functions related to user personal data registration and profile publication, submission and viewing of information and image, and commenting were uniquely designed to suit to the objectives of the present study. Since the object of this system is disaster information, for which reliability is regarded as important, the system has been designed such that it requires users to register, and each individual user can be identified by either their real name or an assumed user name. Therefore, the system is designed such that an environment in which it is difficult to make inappropriate statements or behave inappropriately has been prepared in advance, and the reliability of submitted information and comments can be improved.

Further, a button function and ranking function have been included in the SNS. Concerning the button function, it is used when users view disaster information which has already been submitted, and allows users to easily express that they have the same information. Further, a ranking function was added to the button function, and on the disaster information ranking page of the user screen, the five information items for which the most amount of users have the same information are displayed in descending order.

4) Twitter

The present study employs a system design which allows realization of long-term operation by preventing reduction in the number of active users, and allows users to submit information anytime using mobile information terminals regardless of whether they are indoors or outdoors. Therefore, Twitter was secondly selected from among the various forms of social media, and was mashed up with the SNS which was uniquely developed, as mentioned in the previous section. Of the various forms of social media, Twitter has the easiest information submission method, and many tweets per day can be expected, so it is essential for realizing long-term operation of the system. The system is designed such that when users submit information from Twitter, they tag the information with the hashtag #mtkgis and with location information which employs a GPS.

5) Function for classifying submitted information

Anticipating situations where a lot of information is submitted when a disaster has occurred and there is an excess of information, a function which automatically classifies and organizes submitted information was set up and installed in the SNS. Similarly to what is described in Moriya et al. (2009) [13] in Section II, a method in which words related to local information are obtained from submitted information, and the local situation and that location are displayed on the digital map via a circular illustration is employed. In the present study, submitted information is classified into two categories according to whether it relates to either danger or safety. The system automatically classifies submitted information by searching submitted content using multiple character string searches which employ regular expressions. Specifically, when the words “danger” or “dangerous” are included in submitted information it is classified as information relating to danger, and when the word “safe” is included in submitted information it is classified as information relating to safety. Submitted information is classified right after being submitted and can be displayed on the Web-GIS digital map immediately.

Concerning this point, so that the system can accurately automatically classify and display submitted information as information related to either danger or safety, rules for making submissions which include specific illustrative examples are presented in advance on the initial page of the system and in the instructions for use of the system which are distributed to all users, so that users do not use vague expressions. Through this, due to having the users submit information according to the above-mentioned rules during normal times, even in disaster outbreak times it can be anticipated that users will continue to submit information in a similar manner; therefore, the probability that the system can appropriately classify submitted information can be increased.

As outlined above, when submitted information that has been classified is registered in the database, flags are added to it; therefore, the system is designed such that fields are created in advance in the database and flags can be stored in the database. When illustration is made using the Web-GIS, illustration is made using semitransparent circles that are color-coded based on the flags (red for danger, green for safety). Thanks to this, even in cases where many pieces of information are concentrated in certain areas, different types of submitted information can easily be distinguished. Further, taking into account the accuracy of acquisition of GPS location information of mobile information terminals, the radius of the circles was set at 50 m.

6) Function for checking facilities that provide support during disasters

In the present study, seven types of facilities included in the Tokyo Metropolitan disaster prevention maps (2) are designated as facilities that provide support during disasters. They are temporary stay facilities, shelters, evacuation areas, water supply points, medical institutions, stations for aiding return to home (shops, etc. that provide support when people for whom it is difficult to return home are returning home on foot), and gas stands. Further, a system has been designed which enables users to check facilities that provide support during disasters in an optional range based on present location or any location, and based on any facility category. The facility names, categories, and addresses of the facilities that provide support during disasters are published, but the distance between two points cannot be calculated based on addresses. Therefore geocoding is conducted, addresses are converted to latitude/longitude, and then that data is stored in the database in advance.

Therefore, the system has a design which allows the search range to be selected from the range of 50 to 500 m, and facility categories to be selected from the seven categories mentioned above. When a request for a check of facilities that provide support during disasters is sent from an information terminal, in order to measure the distance between the designated point and disaster support facilities in the area of that point, the difference between the latitude/longitude that is sent from the information terminal and the latitude/longitude of each disaster support facility is used to calculate the distance between the designated point and each disaster support facility. Thus, facilities that are within a range designated by the user are confirmed, and further, facilities in a designated category are displayed on the digital map of the Web-GIS.

V. System Development

A. System Front End

In the present study, as is described in detail below, unique functions for users are operated, and support for utilization of disaster information is conducted.

1) Disaster information submission and viewing functions

When a user submits disaster information, they go to the submission page using “Post disaster information”. On the submission page, they input “Title”, “Image”, “Main Text”, “Location”, and submit their information. Concerning input of location, when the PC interface is used, the user clicks the location on the map and location information is added; however, when the interface for mobile information terminals is used, it is possible to add location information using a GPS. Concerning display of the time, as described in detail in Section V-B, for this system, the development of an operation system run by multiple administrators that is operated starting from normal times of no disaster is anticipated. If users move from a dangerous place to a safe one and then submit information, concerning submitted information that describes circumstances at a time in the past, administrators change the time display to match that time. Further, as described in Section IV-B, in both normal times and disaster outbreak times, users can submit information about dangerous or safe places and so on, communicate by commenting about information submitted by other users, and update submitted information in real time by adding to or amending the contents of all submitted information using comments.

When users log into the system, they can check the latest five items of submitted information on the initial page, and check submitted content and images on the disaster information list page. Further, as outlined in Section IV-B, users can view all submitted information on the digital map of the Web-GIS, and when using the PC interface for users, users can also view submitted information in detail using full-screen display. Further, as described in Section IV-B, all submitted information is automatically classified by the system and illustrated on the digital map in semitransparent circles divided into red for danger and green for safety, so users can easily distinguish between different types of information.

2) Function for viewing disaster information provided by governments

The overall degrees of danger (the degrees of danger calculated by combining the risk of building collapse and the risk of fire) published on the disaster prevention maps provided by Mitaka City and the Metropolis of Tokyo (the regions for operation of the system), and the seven types of disaster support facility described in Section IV-B were input into the GIS base map using Esri's ArcMap, and a disaster prevention map unique to the system of the present study was created. Through this, disaster information submitted by users who are local residents and disaster information provided by governments is all mashed up on the GIS base map, and users can check all this information on the one screen using the Web-GIS.

3) Function for checking facilities which provide support in disaster outbreak times

Users can search for seven types of disaster support facility by setting their choice of range and facility category. Concerning search range, a radius of 50 to 500 m from a designated point can be selected from a pull-down menu. Facility category can be selected from among seven types, and disaster support facilities in the area of a present location or a location of the user's choice can be checked.

4) Disaster information ranking function

By viewing disaster information that has already been submitted and using the button function, users can easily indicate that they have the same information if that is the case. In addition, a ranking function has been added to the button function, so disaster information items for which the most amount of users have the same information are displayed in descending order on the disaster information ranking page of the user screen.

B. System Back End

1) System for classifying submitted information

When users submitted disaster information, the system classifies the submitted information. Before submitted information is stored in the database, matching using regular expressions with respect to character strings stored in PHP variables is performed. In the case when a character string which is a matching target matches when a preg_match function is used, a value returned by the function is obtained. In this case, 1 or 2 is assigned to the variable for a flag, and is stored in the database together with the submitted content. The character strings which are targets of matching are the words "danger" and "dangerous" for information relating to danger, and the word "safe" for information relating to safety. Concerning this point, misclassification due to fluctuation in expression is prevented by displaying submission examples on the initial page of the system in advance. Information classified as outlined above is updated when the web page is loaded, and is depicted on the digital map of the Web-GIS using color-coded semitransparent circles.

2) System for management of submitted information by administrators

Every user's submissions of information and image files are all stored as data in the database of the system. Administrators manage users and check submitted information using a list screen designed especially for the purpose. Administrators can take the measure of suspending accounts of users who have made inappropriate transmissions or behaved inappropriately, and if by any chance an inappropriate submission is made, administrators can delete the submission with just one click. Thanks to these features, there is no need for administrators to search to see whether or not inappropriate submissions of information have been made within the system; therefore, their burden can be lessened.

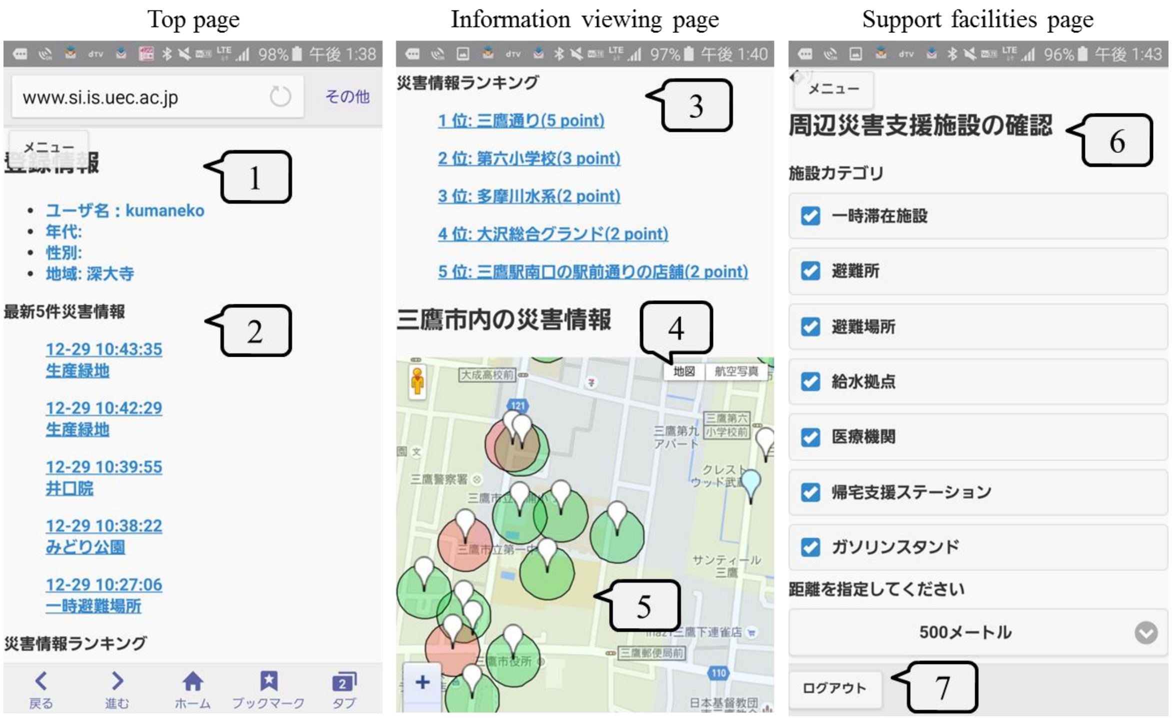
Further, for this system, it is desirable to develop a system of operation in which starting from normal times of no disaster, there are multiple administrators, consisting of government employees, people in firefighting and police organizations, and local residents. In addition, it is desirable that in the system of operation, information submitted by local residents is routinely checked on a high-frequency basis, and the reliability and consistency of information can always be guaranteed by taking the measure of deleting inappropriate submissions of information should any be discovered, and checking that submitted information is being appropriately classified by the system for classifying submitted information mentioned in the previous section. When a disaster has broken out, it is necessary to take not only the measures outlined above, but also to update published submitted information in real time and always guarantee the reliability and consistency of the information by taking the following measures. When multiple pieces of submitted information contradict each other, it is necessary to check the information by referring to information provided by other media and information systems, and then delete inappropriate information. Further, it is necessary to delete and amend information provided by local residents and governments in the case that it has become inappropriate in the circumstances of the disaster, which change by the minute.

C. System Interfaces

The system has three kinds of interface – a PC screen for users (Fig. 2), a mobile information terminal screen especially optimized for smartphones and tablet terminals (Fig.3), and a PC screen for administrators. Additionally, as examples of the PC pages for users, Fig. 4 shows the page for viewing submitted information, and Fig. 5 shows the page for checking facilities that provide support in disaster outbreak times. As mentioned earlier, they can communicate by commenting about information submitted by other users, and update submitted information in real time by adding to or amending the contents of all submitted information using comments on the former page. These pages are linked to the top page (Fig. 2), and this system has the similar pages to them optimized for mobile information terminals. Specifically for mobile information terminals, the pages for viewing submitted information and checking facilities that provide support during disasters are respectively shown on the middle and right parts in Fig. 3.

No.	Description
1	User profile publication
2	The five most recent items of submitted information
3	The five most important items of submitted information
4	The number of users
5	Go to my page
6	Go to the page where information can be submitted from computers
7	List of submitted information
8	Go to the page where support facilities in times of disaster can be checked
9	Go to the page where change and registration of personal data can be made
10	Logout
11	Explanation to use this system
12	Disaster information is displayed on Web-GIS digital map in the region of operation (Mitaka City)
13	General degree of risk
14	Explanation of disaster information submitted by users

Fig. 2. PC screen for users



No.	Description
1	User profile publication
2	The five most recent items of information submitted from computers and mobile information terminals
3	The five most important items of information submitted from computers and mobile information terminals
4	Submitted information is displayed on Web-GIS digital map using markers
5	General degree of risk
6	Support facilities in times of disaster
7	Logout

Fig. 3. Mobile information terminal screen screen for users

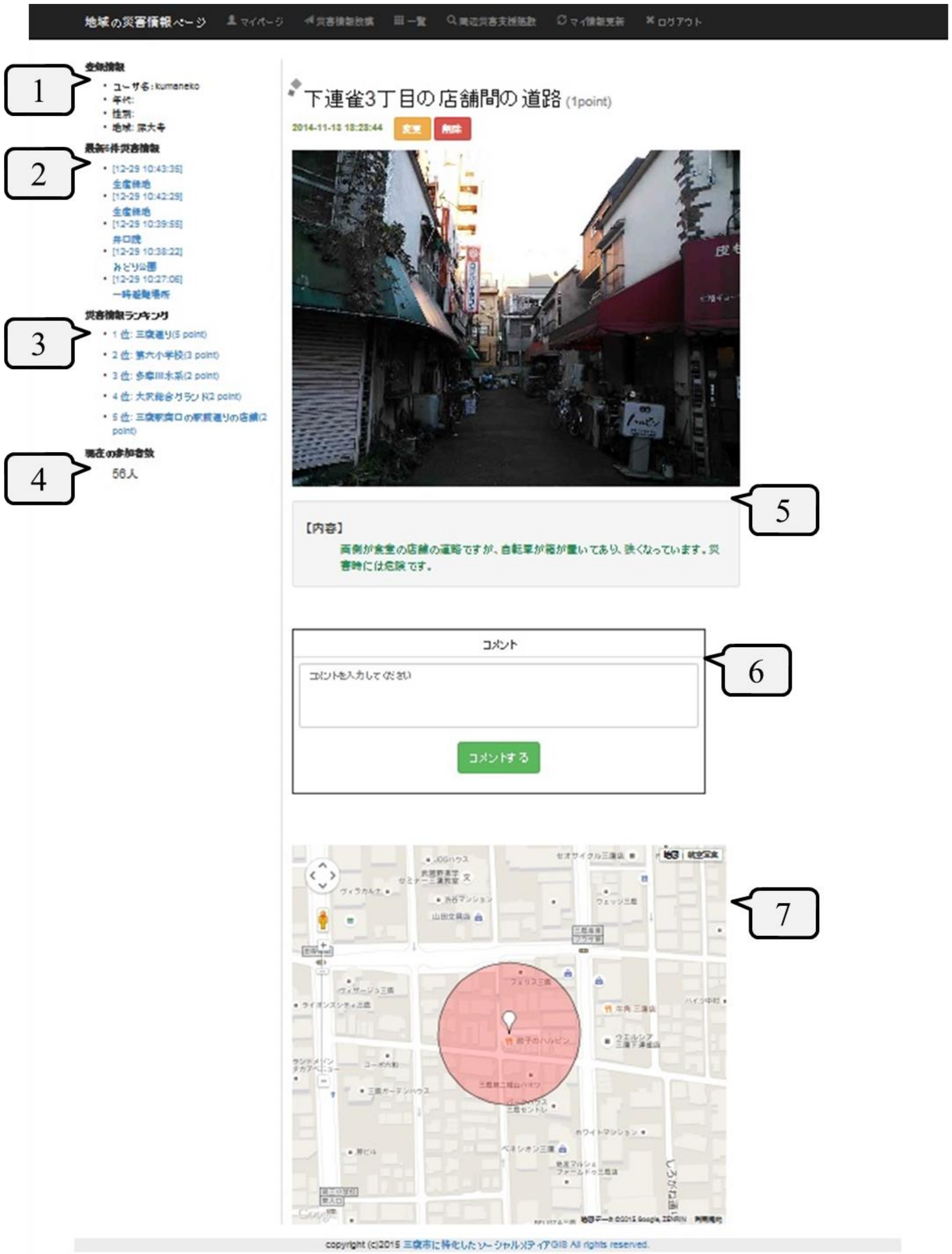
VI. Test Operation and Operation in the Regional Community

In accordance with the operation process in TABLE I, test operation of the social media GIS designed and developed in the present study and evaluation of the test operation were conducted, and then full-scale operation was conducted.

A. *Comparison with Existing Services in Region for Operation of System*

In Mitaka City, the region for operation of the system, a plan for supporting the evacuation of people requiring special help during disasters was formulated in 2011, and a disaster prevention map [(3)] has also been created and provided. TABLE II compares disaster prevention maps relating to Mitaka City with the features of the system of the present study. The Mitaka City disaster prevention map can be used to check locations of large-area evacuation sites designated by the city and the overall degree of danger of locations within the city (the degree of danger in Mitaka City is ranked using three levels only – 1 to 3). However, since it is published in PDF format, information cannot be viewed all at once. The Tokyo Metropolitan disaster prevention maps are published as digital maps, so it is easy for users to view information they need, and the maps include the facilities that provide support during disasters that were mentioned in Section IV-B and other information. However, the maps do not have detailed disaster information concerning each region. Further, these government disaster prevention maps do not include any disaster information that is experience-based information possessed by local residents at all.

Therefore, the system of the present study is useful in that it can effectively provide detailed disaster information specific to the region where it is operated, by gathering and accumulating disaster information submitted using an SNS and twitter by users who are local residents and displaying the disaster information on the digital map of a Web-GIS. Further, it is useful in that disaster information provided by users who are local residents and by governments can all be checked visually on the digital map, useful in that the system automatically classifies submitted information and immediately displays it on the digital map, and can also handle situations during disasters when there is an information glut, and useful in that users can use the system to check facilities that provide support during disasters. Even in disaster outbreak times, if an environment in which communication can be conducted can be secured, disaster information can be gathered, accumulated, and provided by the system, in the same way it is during normal times. Therefore, the system can also supplement efforts made by governments concerning disasters.



No.	Description
1	User profile publication
2	The five most recent items of submitted information
3	The five most important items of submitted information
4	The number of users
5	Submitted information and image
6	Comment column
7	Disaster information is displayed on Web-GIS digital map in the region of operation (Mitaka City)

Fig. 4. Page for viewing submitted information (PC screen)

No.	Description
1	User profile publication
2	The five most recent items of submitted information
3	The five most important items of submitted information
4	The number of users

Fig. 5. Page for checking facilities that provide support in disaster outbreak times (PC screen)

B. Operation Test and Evaluation of Operation Test

Before full-scale operation was conducted, three students in their twenties who were residing or attending school in Mitaka City were selected and a one-week operation test was conducted. After the operation test, the students who participated in the operation test were interviewed. In the interviews, the students expressed the opinion that a large-sized map was desirable when viewing disaster information on the digital map. Therefore, the system was redeveloped concerning this point only – the full-screen display for the PC interface for users, mentioned in Section IV-B.

C. Operation

When full-scale operation was conducted, local residents aged eighteen years or over residing in, commuting to, or attending school in Mitaka City were targeted as users. Pamphlets and operating instructions were placed in the city hall and bases of citizen activities in order to appeal for use of the system. When first using the system, users registered the personal information items of “User name”, “Password”, “Age group”, “Gender”, “Region”, and “Email address”. Concerning “Age group”, “Gender”, and “Region”, which were displayed on the screen, users could set whether or not to make these items public at their discretion. After registering, users could use the system when they logged in, and after logging in, users could reset the above-mentioned items of personal information that they had registered.

VII. Evaluation

In this section, according to the operation process shown in TABLE I, firstly based on results of access analysis utilizing log data, and analysis of submitted information from during full-scale operation, an evaluation of operation concerning the aim of the system – that is, the aim of supporting utilization of disaster information in order to reduce the effects of natural disasters from normal times through to disaster outbreak times – was conducted. Next, based on the results of these evaluations, measures of using the system even more effectively were identified.

A. Access count and means of access

1) Outline of access analysis

In order to analyze user trends, analysis was performed using access logs collected during the period of operation. In the present study, Google Analytics was used for collecting log data. Google Analytics is an access analysis service provided free of charge by Google, and is widely used. It can be used by setting up a tracking code in the source of a web page.

2) Results of access analysis

The total access count for the period of operation was 2,537. Although there were differences in the access counts for each week, the average weekly access count was approximately 24, and it can be said that users used the system on a continual basis. Concerning the access counts for each page, the access count for the submission page was the highest, being 34% of the total. Next was the access count for the page for checking facilities which provide support during disasters (10%), followed by the access count for the viewing page (9%). It can be seen that even if users did not submit information, many users checked disaster support facilities and viewed disaster information. Concerning means of accessing the pages, 95% of access was from PCs and 5% was from mobile information terminals; therefore, it can be presumed that use was mainly from PCs, and mobile information terminals were used as a supplementary means of access. However, the fact that mobile information terminals were also used shows that it is possible that the system can mitigate spatial and temporal restrictions during both normal times and disaster outbreak times.

B. Features of submitted information

Fig. 6 shows changes in the total number of users and the total number of submissions of information from week to week during the period of operation. Both the number of users and the number of submissions of information gradually increased, although there are differences in the rate of increase from week to week. The total number of submissions of information was 260 (the weekly average is approximately 26). Submissions from Twitter were all made using mobile information terminals, but there were only six submissions from Twitter. Of the total number of submissions, 81% included images, and 4% of submissions were commented on. The fact that the comment function was also used and users were able to communicate with each other indicates that it can be anticipated that this function will be used not only in normal times but also in disaster outbreak times. Information concerning danger made up 20% of the total, information concerning safety made up 68%, and other types of information made up 12%, and concerned disaster prevention storehouses, water supply points, and water wells for earthquake disasters.

TABLE I. OPERATION PROCESS OF THE SYSTEM

Process	Aim	Period	Specific details
1. Survey of present conditions	To understand efforts related to tourism in the region for operation (Mitaka City)	July 2014	- Survey of government measures and internet services - Interviews with government departments responsible, etc.
2. System configuration	Configure the system in detail to suit the region for operation	August 2014	- Define system requirements - System configuration - Create operation system
3. Operation test	Conduct the system operation test	September 2014	- Create and distribute pamphlets and operating instructions - System operation test
4. Evaluation of operation test	Reconfigure the system based on results of interviews with operation test participants	October 2014	- Evaluation using interviews - System reconfiguration - Amendment of pamphlets and operating instructions
5. Operation	Conduct actual operation of the system	October-December 2014	- Appeal for use of the system - Distribution of pamphlets and operating instructions - System operation management
6. Evaluation	Evaluate the system based on the results of access analysis which used log data during the period of actual operation, and the results of analysis of submitted information	January 2015	- Evaluation using access analysis which used log data, and analysis of submitted information - Identification of measures for using the system even more effectively

TABLE II. COMPARISON OF FEATURES WITH DISASTER PREVENTION MAP RELATED TO REGION FOR OPERATION

	Use of digital map	Viewing means	Submitted information from local residents	Automatic classification of submitted information
Tokyo Metropolitan disaster prevention maps	Yes	Digital map	No	No
Mitaka disaster prevention maps	No	PDF	No	No
The system of the present study	Yes	Digital map	Yes	Yes

Further, as shown by Fig. 7, submissions of information are dispersed over the whole area of Mitaka City, so it can be assumed that the locations of users' places of residence, commutation destinations, and schools were not concentrated in limited areas. However, there are regions where the amount of submissions of information is somewhat concentrated. In particular, there were many submissions of information concerning the area of the train station. This is considered to be due to the fact that many people come and go through this kind of area daily, and there are many places where narrow streets become even narrower due to bicycles, luggage, and the like.

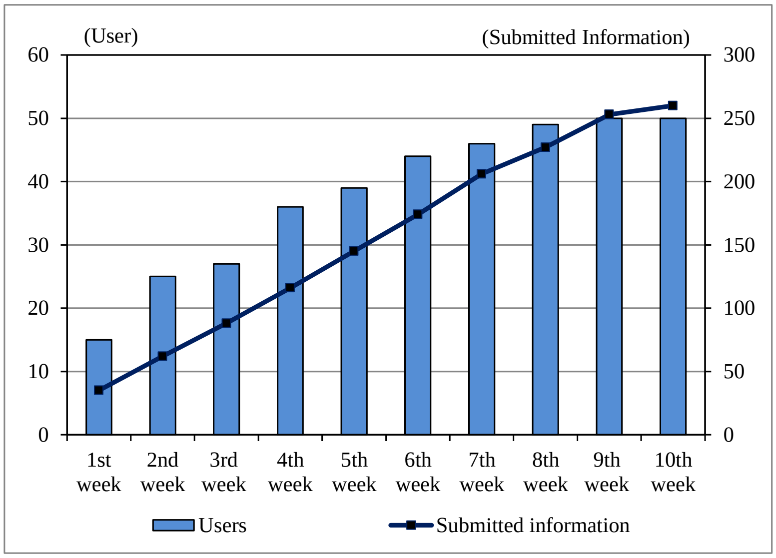


Fig. 6. Changes in the total number of users and the total number of submissions of information during the operation period

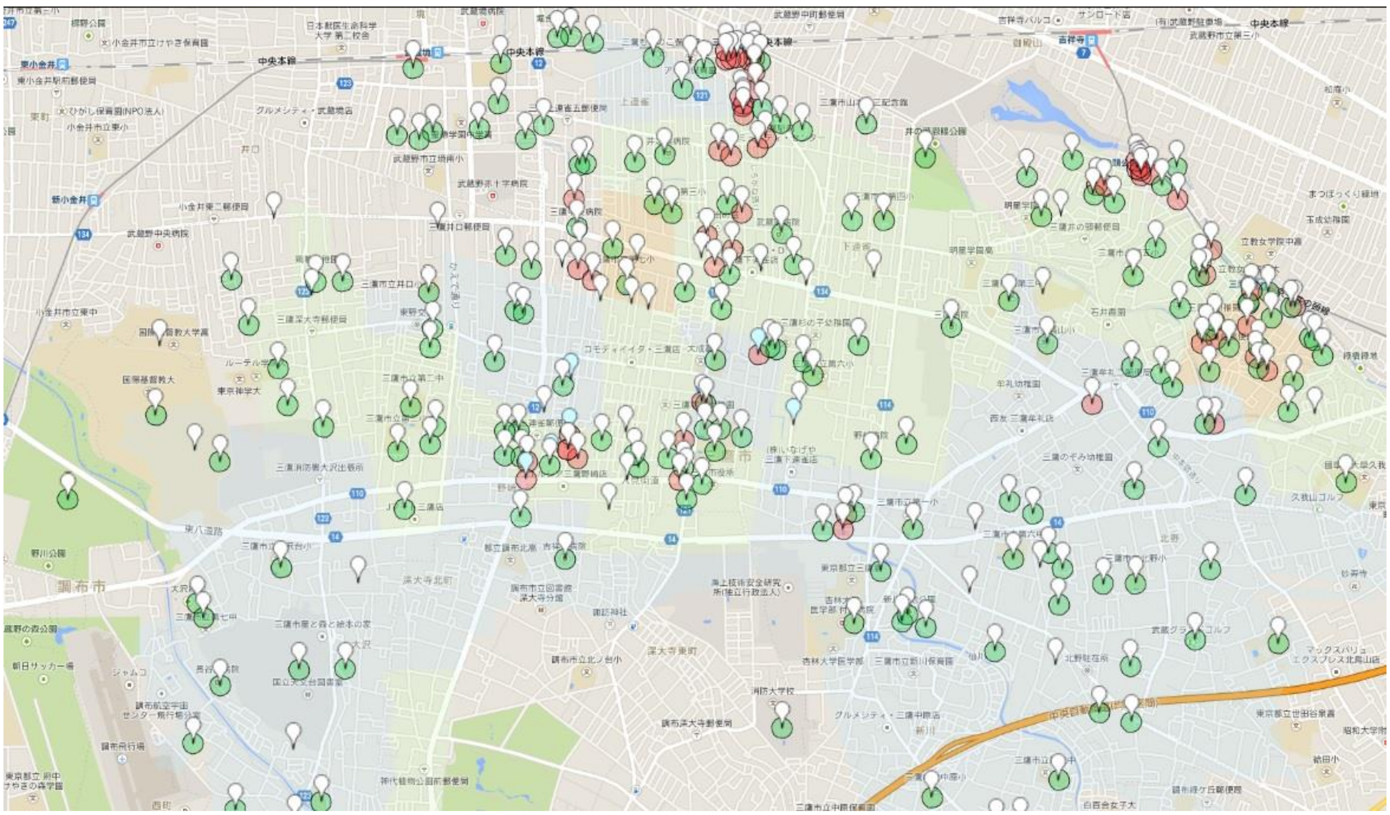


Fig. 7. Distribution of submitted information in the region for operation of the system (Mitaka City)

C. Identification of Measures for Using the System

Based on the results of the evaluation of the operation in this section, measures for using the system even more effectively were summarized into the two points below.

1) Notification of information to passive users

GPS information of users' information terminals is continually obtained at a set interval, and the system searches for disaster information in the vicinity of the user and push-notifies the user of information within a set range in the vicinity of the user. Through this, passive users are notified of information.

2) Operation of the system using cloud computing

In order to be sure the system operates even during disaster outbreaks, the system is distributed in earthquake-proof data centers. Doing this allows more reliable operation of the system than server operation by individuals. Further, combining ArcGIS Online (which is provided by Esri) with the system when it is used allows all servers to be operated using cloud computing.

VIII. Conclusion and Future Research Topics

The conclusion of the present study can be summarized into the following three points:

1) A social media GIS which integrated a Web-GIS, an SNS and Twitter and which included a function for classifying submitted information was designed and developed. A system which supports utilization of information in order to reduce the effects of natural disasters which anticipates use not only in normal times but also use during disasters when there is an information glut was proposed. The system supports utilization of information by depicting submitted information based on location information and content using color-coded semitransparent circles, and by displaying information based on information about present location. Mitaka City in the Metropolis of Tokyo was selected as the region for operation of the system. After a survey of existing conditions was conducted, the system was developed in detail.

2) Since full-scale operation was to be conducted for ten weeks, a one-week operation test was conducted in advance and an area for improvement of the system was identified. After that, the system was reconfigured. People targeted as users of the system were those residing in, commuting to, or attending school in Mitaka City aged eighteen years of age or over. The number of users was fifty in total. Users in their forties and fifties made up the greatest proportion of users, at 32% and 30%, respectively, while the proportion of users in their twenties, thirties, and sixties and above was 14%, 12%, and 10%, respectively, so the system was used by a wide range of age groups. During the period of operation, users accessed the system from PCs and mobile information terminals, and submitted and viewed information.

3) An evaluation of the operation was conducted based on access log analysis and submitted information. The former showed that the system was continually accessed throughout the period of operation, and the later showed that 260 pieces of disaster information were submitted, dispersed throughout Mitaka City. Based on the results of the evaluation of the operation, measures for using the system even more effectively were summarized into the following two points: (1) Notification of information to passive users, and (2) Operation of the system using cloud computing.

Future topics for research include expanding the stages of use of the system to times of post-disaster restoration and redevelopment, cooperating with firefighters and police, and operating the system with the participation of a wider user base, and increasing the track record of use of the system by operating it in other regions as well, and further increasing the significance of using the social media GIS developed in the present study.

Acknowledgements

In the operation of the social media GIS, enormous cooperation was received from those in Mitaka City of Tokyo metropolis and the neighboring area in Japan. We would like to take this opportunity to gratefully acknowledge them.

Notes

1) Japanese Ministry of Land, Infrastructure, Transport and Tourism's Hazard Map Portal Site: http://disapotal.gsi.go.jp/. (Accessed 2014, August 20). (Website)

2) Tokyo Metropolitan disaster prevention maps: http://map.bousai.metro.tokyo.jp/. (Accessed 2014, August 20). (Website)

3) Mitaka City disaster prevention map: http://www.city.mitaka.tokyo.jp/c_service/003/003310.html. (Accessed 2014, August 20). (Website)

References

[1] Cabinet Office, Government of Japan, "White paper on disaster management 2012", Tokyo, 2012.

[2] Regional Research Committee, Science Council of Japan, "Recommendations: towards the accumulation and utilization of Regional Knowledge", Tokyo, 2008.

[3] Central Disaster Management Council, "Committee for policy planning on disaster management – Final report: Toward reconstruction for a Japan that is unshakable", Tokyo, 2012.

[4] R. W. Greene, "Confronting catastrophe: A GIS handbook", ESRI Press, Redlands, 2002.

[5] A. S. Vivacqua and M. R. S. Borges,"Taking advantage of collective knowledge in emergency response systems", Journal of Network and Computer Applications, Vol.35, No.1, pp.189-198, 2012.

[6] A. Mansouriana, A. Rajabifardb, M. J. Valadan Zoej, and I. Williamson, "Using SDI and web-based system to facilitate disaster management", Computers and GeoSciences, Vol.32, No.3, pp.303-315, 2006.

[7] J. M. M. Neuvel, H. J. Scholten and A. van den Brink, "From spatial data to synchronized actions: The network-centric organization of spatial decision support for risk and emergency management", Applied Spatial Analysis and Policy, Vol.5, pp.51-72, 2012.

[8] Cabinet Office, Government of Japan, "White paper on disaster management 2012", Tokyo, 2012.

[9] M. Murakami, A. Shibayama, Y. Hisada, T. Ichii, S. Zama and M. Endo, "Development of an information gathering and sharing system that supports disaster prevention activities carried out by local residents and local governments", Journal of Japan Association for Earth Engineering, Vol.9, No.2, pp.200-220, 2009.

[10] T. Okuma and K.Yamamoto, "Study on Social Media GIS for accumulating urban disaster information: Accumulation of disaster information during normal times for purposes of disaster reduction measures", Socio-Informatics, Vol.2, No.2, pp.49-65, 2013.

[11] T. Murakoshi and K. Yamamoto, "Study on Social Media GIS for supporting utilization of disaster information: For disaster reduction measures in normal times through to times of disaster outbreak", Socio-Informatics, Vol.3, No.2, pp.17-31, 2014.

[12] T. Yamanaka, Y. Tanaka, Y. Hijikata and S. Nishida, "A supporting system for situation assessment using text data with spatio-temporal information", Japan Society for Fuzzy Theory and Intelligent Informatics, Vol.22, No.6, pp.691-706, 2010.

[13] K. Moriya, S. Sasaki and Y. Kiyoki, "A dynamic creation method of environmental situation maps using text data information", DEIM Forum 2009, pp.B1-6, 2009.

[14] S. Honjo and H. Yuhashi, "Information society for disaster reduction - Great East Earthquake and mobile communication-", NTT Publishing Co., Ltd., Tokyo, 2013.

[15] H. Ikemi, T. Esaki and Y. Mitani, "Sustainable data-sharing for disasters based on the Wiki and GIS technologies", Theory and Application of GIS, Vol.17, No.1, pp.93-99, 2009.

[16] S. Okano, S. Yasui, K. Okazawa, H. Ebara and H. Okada, "Hybrid disaster information distribution method for community networks", IEICE Technical Report, IN, Information Network, Vol.108(458), pp.499-504, 2009.

[17] T. Kato, M. Kobayashi, N. Sato and T. Yotsuyanagi, "Towards implementing a disaster management information mashup Ssystem in the community", Monthly Journal of the Institute of Industrial Science, University of Tokyo, Vol.62, No.4, pp.377-380, 2010.

[18] T. Takatani, T. Iwaki and Y. Kato, "Creation of a regional disaster prevention support system aimed at planning urban areas that are resistant to natural disasters", Bulletin of Mizuru National College of Technology, No.43, pp.34-50, 2008.

[19] M. Inoguchi, K. Tamura, T. Furuya, R. Kimura and H. Hayashi, "Proposal aimed at realization ofeffective on-site spatial information mashup for emergency map creation teams: A case study of the 2011 Great East Japan Earthquake", Journal of Social Safety Science, No.15, pp.219-229, 2011.

[20] A. Kawasaki and K. Meguro, "New trends in disaster response support using web mapping, observed in the 2010 Haiti Earthquake", Monthly Journal of the Institute of Industrial Science, University of Tokyo, Vol.62, No.4, pp.409-416, 2010.

[21] K. Yamamori, "Establishment of a bulletin board for times of disaster", Bulletin of Faculty of Education Mie University, No.61, pp.13-19, 2010.

[22] K. Korida, T. Kikuchi, N. Yoshiyama, Y. Shibata, M. Takahashi, M. Takenaka and E. Aoki, "Development of community disaster prevention SNS based on the trust and relationships between local inhabitant", The Special Interest Group Technical Reports of Information Processing Society of Japan, CSEC, "Computer Security", 2011-CSEC-52(16), pp.1-6, 2011.

[23] H. Wasaki, "Disaster and regional SNS: The connection effect for rescue/recovery that came to light through the Sayou Town Torrential Rain Disaster", Bulletin of the National Museum of Ethnology, No.106, pp.127-146, 2012.

[24] M. Yamamoto, H. Ogasawara, I. Suzuki and M. Furukawa, "Information dissemination network on Twitter during the Great East Japan Earthquake", Information Processing Society of Japan Magazine, Vol.53, No.11, pp.1184-1191, 2012.

[25] N. Yoshimura and T. Inoue, "Analysis of use of public institution accounts in the microblog service Twitter before, during, and after the Great East Japan Earthquake", The Special Interest Group Technical Reports of Information Processing Society of Japan, GN, "Groupware and Network Service", 2012-GN-83(5), pp.1-8, 2012.

[26] T. Yanagisawa and K. Yamamoto, "Study on information-sharing GIS for accumulating local knowledge in local communities", Theory and Applications of GIS, Vol.20, No.1, pp.61-70, 2012.

Building Safety Road Maps Based on Difference of Judgment of Road Users by their Smartphone

Viet Chau Dang
Department of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

Masao Kubo
Department of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

Hiroshi Sato
Department of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

Akira Namatame
Department of Computer Science
National Defense Academy of Japan
Yokosuka, Kanagawa, Japan

***Abstract*—Recently, there has been a growing demand and interest in developing methods for analyzing smartphone logs to extract traffic safety information. Because the log is high time resolution and closely related to user activities but fragmentary and myopic, it is difficult for currently available collision probability based quantitative risk assessment methods to create traffic safety maps automatically from the driving log which require all of concrete information about a collision for example, size of vehicle, speed of pedestrian. This paper proposes a computable risk measurement method for building traffic safety maps with the logs of different users' driving, which does not discuss collision probability. The proposal is designed to compute differences in the recognition of the road environment among road users mathematically. Drivers differ in their recognition, judgment, and handling of a given situation. Suppose that a difference in recognition among users in the same situation is a signal of danger. This signal is easy to calculate by Poisson process. Each user's recognition of road environment and the safety map integrated from the collection of the recognition are generated fully automated. A real-world experiment was carried out, and the results show that the assumption and the proposed method succeeded in generating an accurate and effective traffic safety map.**

Keywords—Traffic Safety Map; Risk Estimation; Occupancy Grid Map; Driving Model; Smartphone Sensing; Collective Intelligence

I. INTRODUCTION

This paper proposes a method for generating traffic safety maps based on differences in individual recognition of the road environment by using smartphone data from various users.

Currently, traffic safety maps are plotted annually using accident reports by police bureaus, and parts of these maps are made accessible to road users using a web-based geographic information system (GIS). Traffic safety maps show the locations of occurred accidents and other information, such as the type of collisions, the vehicles involved, and the time the collisions occurred [1],[2],[3].

Safety road map is absolute necessary for safety of road users, however it costs very high to create. That why current safety map is limited reluctantly. Moreover, it is lack of information because only accident records are used without any prediction of new risk locations. Recently, the development of new sensor technologies on smartphones-e.g., global positioning systems (GPS), accelerometers, and gyroscopes which can help to collect massive real-time traffic road data via smartphones, provides us many useful information of road conditions. Mohan et al. developed a road monitoring system named Nericell, which can automatically monitor braking, bumps in the road, honking and stop-and-go traffic via smartphone. It uses a smartphone's accelerometer, microphone, GSM communications and GPS for this purpose. Nericell aggregates sensed data from multiple participating smartphones on a centralized server [4].

Fathi et al. proposed a method for detecting road intersections from GPS traces [5]. Fazeen et al. developed an advanced driver-assistance system on a smartphone. Such a system advises a driver on dangerous situations that emerge from vehicle maneuvers and environmental factors. The aim of these systems is to recognize and classify driving behavior and to map road surface conditions [6]. Zhang et al. presented a method for integrating GPS traces and current road map towards a more accurate, up-to-data and detailed road map [7].

Safety map is a kind of risk analysis result of traffic environment. It is also a traffic road property and closely relates to the relationship among road users but has not been studied enough. There are some works related to risk analysis. For example, Google Live Traffic is a service that utilizes GPS data from Android smartphones to estimate traffic jams based on average GPS speed [8].

Honda initiated a project for traffic safety map in 2013 using data recorded by their Internavi in-vehicle unit, along with police reports and user contributions to their safety map website [9]. The locations where sudden brake occurs as risky spots are plotted automatically in the map.

However, there are gaps between the locations pointed out on these maps and actual hazard locations, for example, a sudden brake can occur for many reasons, and these often depend on the road type, road conditions, weather conditions, road equipment, and any driver distractions. A sudden breaking is a consequence of a decision-making; however all of the locations are not actual hazard spots.

It is easy to understand of traffic safety if actual hazard spots are plotted. For example, school zone marks are usually drawn on hand-written safety maps. Currently, there is not any automatic method to detect hazard spots from the logs. In previous works, we have proposed a method for detecting incident locations at which risk situation occurred frequently [10],[11]. The method can be used to detect hazard locations for road user by using smartphone logs.

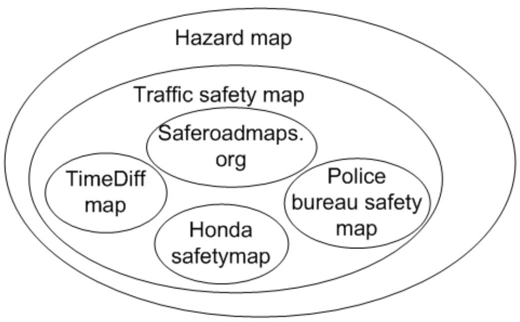


Fig. 1. Hazard map and traffic safety map

This paper proposes a method for integrating a collection of hazard locations based on differences in drivers' recognition of the road environment. The method is inspired by STEP technique [12] of risk analysis in traffic safety field. Suppose that if drivers have the same recognition of a crossroad, the level of danger will depend on one's driving skill. By contrast, where one driver recognizes a crossroad as passable and where other drivers recognize it as impassable, accidents are more likely to occur.

This paper is organized as follows. Section II reviews the related works and the requirements for traffic safety maps. The proposed method, related algorithms, and concept is described in Section III. The experiment and evaluation are discussed in Section IV. Section V provides the conclusion and future work.

II. Traffic Safety Maps and Related Research

In this section, the related research are reviewed. Objective of this research is to propose a method for calculating and providing safety information toward road users. Safety information of smartphone data from different users is extracted and provided to as much road users as possible. However, it is expected that smartphone does not directly senses "safety". Information collected by smartphone only contains the belonging vehicle information, and it cannot be used to measure the road condition and driver's behavior directly. Therefore, it is difficult to use current collision based risk analysis approaches to extract safety information from smartphone. This paper proposed a method based on difference on drivers' recognition of traffic road which inspired by STEP technique (the Sequentially Timed Event Plotting)[12]. STEP technique is a qualitative risk analysis technique.

First, the requirements for traffic safety maps generated with smartphone data are explained.

A. Requirements for Traffic Safety Maps

A traffic safety map is a type of hazard map that contains information regarding the road environment of which drivers should be aware(see Fig. 1). The requirements for traffic safety maps generated with smartphone data are as follows:

1) Accuracy: Accuracy depends on acknowledging frequent occurrences of unsafe events at particular locations. The locations and the frequency of accidents must be described accurately. This research considers the level of accuracy for alerting drivers of unsafe locations with location errors of 50 m.

2) Automatic generation: Generating traffic safety maps requires considerable time and effort. Thus, the map-generation process should proceed automatically. If possible, the process should be conducted on the smartphone, and the results should be forwarded to a GIS server over the Internet.

3) Privacy considerations: Private information should not be leaked from the smartphone.

4) Community participation: The more users that participate, the more coverage the traffic map has and the more accurate it becomes. Thus, motorcyclists, bicyclists, and pedestrians should also be able to join.

5) Reflecting individual differences: Differences in how users recognize the road environment should be reflected on the map.

6) Reflecting the number of participants: Busy roads with many commuters should be distinguished from quiet roads with few commuters, and this distinction should be reflected on the map.

7) Safety map for everyone: The safety map should be created for everyone uses not for vehicle's drivers only. The safety map can be generated by individual at first. The individual maps are then integrated to be global safety map for public use.

This paper discusses a global traffic safety map that meet above requirements.

B. Related Research

This section reviews related research for extracting safety information. Traffic safety map is a kind of hazard map which is a result of risk analysis, depicted in Fig. 1. Fig. 2 shows methods for risk analysis [12]. Risk analysis methods are categorized into three types: qualitative technique, quantitative technique, and a hybrid technique. In traffic safety research field, related research on traffic safety extraction are as follows.

1) Heat-map analysis and plot of past accidents distribution by Hilton et al.[1].

2) Analysis of near miss reports[13].

3) The Sequentially Timed Event Plotting (STEP) technique[12].

4) Hazard and Operability study (HAZOP) technique[12].

5) Estimation of collision probability between a vehicle and road users by Shimizu et al.[14].

6) Plot the occurrences of sudden brakes locations by Honda safetymap[9].

7) Traffic jams estimation by Google Live Traffic[8].

8) SNS based services where riders and pedestrians can contribute their experiences (Honda safetymap, and others)[9],[15].

Summation techniques use different safety elements such as hazard severity and probability is a common way to generate traffic safety map. Namely, $\sum_{\mathrm{hazard}_i} P_i w_i$,, where P_i, w_i is the occurrence probability and, w_i is the severity of hazard i, respectively.

From above techniques, following traffic safety maps and related works have been proposed.

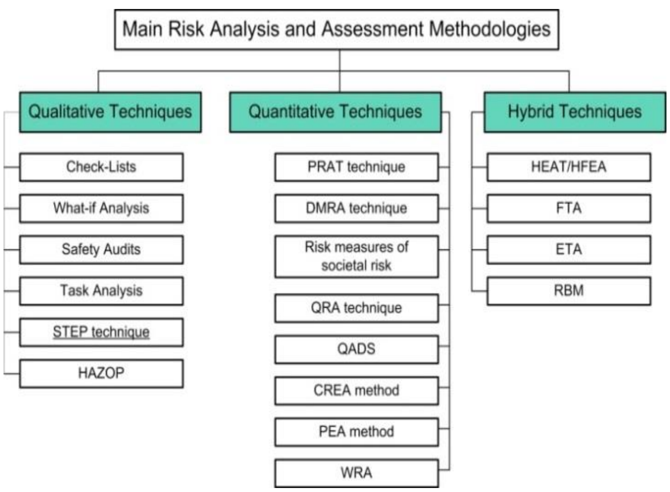


Fig. 2. Main risk analysis and assessment methodologies [12]

Firstly, there are methods to generate maps using accident reports directly. In Japan, each prefecture's police bureau publishes a safety map to improve traffic safety. These safety maps typically plot hot-spot locations with frequently occurring accidents, locations such as intersections with traffic signals. Other non-governmental organizations utilize Google My Map as a platform, relying on community submits hot-spot locations[15].

Next, a strategy to apply risk analysis methods into traffic safety is considered to generate maps of dangerous spots which not being listed in the police reports. Most of the current risk analysis methods usually assume that a hazard is a collision between cars, pedestrians, and others. In this case, a lot of precise information is needed to calculate collision risk probability of a given situation. For example, Shimizu et al.[14] presented a method for calculating collision probability between an ego-vehicle and road users. The model parameters include main road properties, pedestrian's road properties, pedestrian speed and next position probability. Therefore, it is difficult for this approach to predict risk probability of a given location because many collision patterns needed to be considered. It cannot apply this strategy for calculating probability of collision using smartphone data.

There are two approaches to avoid the above problem. The first approach utilizes topographical relations between accidents and set a dangerous value based on accidents distribution. For example, Hilton et al. presented a method to build safety maps using heat-map method, named as Saferoadmaps[1],[3]. This work utilizes data from the Fatality Analysis Reporting System (FARS). FARS's mission is to render vehicle-crash information accessible and useful for the sake of improving traffic safety. Fatality information derived from FARS includes motor-vehicle traffic collisions that resulted in the death of an occupant of a vehicle or of a non-motorist within 30 days of the collision. FARS contains data on all fatal traffic accidents in all 50 states, the District of Columbia, and Puerto Rico. Moreover, Saferoadmaps provides other useful tools, such as heat-map-based map analytics, crash analysis, a real-time safety tracker, and a commuter-stress index.

The second approach tries to estimate the factors caused accidents using vehicle's trace data. This approach considers the locations with high risk probability as unsafe locations, for example Google Live Traffic[8], Honda safetymap[9]. Honda initiated a project for traffic safety map in 2013 using data from their Internavi system, along with police reports and user contributions to their safetymap website. The core data for this safetymap system is sudden-brake data (>-0.25G, a deceleration of 25 km/h in 3 seconds) from vehicles made by Honda in Japan in 2012. The objective roads are more than 5.5m wide, and they are divided into 100m segments. Then, the system calculates the occurrence of sudden brake in each segment. Based on the occurrence rate, the sudden-brake level is classified into one of three groups: Level 1 is above 2,5%, Level 2 is above 5%, and Level 3 is above 10%. The locations where sudden brake occurs on Honda's safetymap are merely representative points; there is no guarantee that sudden brake occurred in that exact place[9].

These approaches need a technique to correct the errors when mapping the observations and the dangerous spots. There are two types of errors: 1) an observation location is not a dangerous spot, 2) an observation location is dangerous spot with a location error. In Honda safetymap, not all of sudden brake locations are near-miss locations. In addition, there are many accident locations provided by police do not include any sudden brakes provided by Honda Internavi system. This may be one reason that Honda adopts SNS service to allow community users to contribute their experience and upgrade safety road map accuracy.

The proposed method is classified into quantitative method's category and inspired by STEP technique[12] that uses to identify actions that contributed to the accidents: a) the time at which the event started; b) the duration of the event; c) the agent which caused the event; d) the description of the event; and e) the name of the source which offered the information. STEP technique provides a valuable overview of the timing and sequence of events/actions that contributed to the accident, or in other words, a reconstruction of the harm process by plotting the sequence of events that contributed to the accident. In this research, traffic road safety is quantified based on an inherited idea of STEP technique using difference in drivers' behaviors.

Table I shows the works related to integrating traffic maps. These methods use Web 2.0 technology with a server-based architecture. The input data for the mapping system can be classified into three types: smartphone-derived data, data derived from social networking services (SNSs), and data from public agencies. Owing to privacy concerns, data from public agencies is not open to the public. Smartphone- and SNS-based data usually contains individual differences (i.e., drivers tend to differ in how they recognize, judge, and handle a given situation). To predict traffic jams, mapping systems do not need to consider these individual differences. Google's Live Traffic service averages data in order to determine whether a traffic jam exists on a particular road[8].

TABLE I. RESEARCH RELATED TO TRAFFIC SAFETY MAPS

Related work	Smartphone	SNS	Public agency data (including road-side camera, probe car,…)	Human factor consideration
Google Live Traffic[8]	O			No
Honda safetymap[9]		O	O	No
Saferoadmaps.org[3]			O	No
Police bureau safety map[2]			O	No
Other SNS traffic safety map[15]		O		No

TABLE II. COMPARISON OF CROWD-SOURCED TRAFFIC SAFETY MAPS AND TRAFFIC SAFETY MAPS BASED ON POLICE REPORT. A: HIGH, B: MEDIUM, C: LOW, X: NO

Requirement	Google Live Traffic[8]	Honda Safetymap[9]	Saferoadmaps. org[3]	Police Bureau safety map[2]	Other SNS safety map[15]	Proposed Method
1) Accuracy	C	C	B-	A	C	B
2) Automatic generation	A	B	B	X	X	A
3) Privacy consideration	C	B	B	A	C	B
4) Community participation	A-	B	X	X	C	A
5) Reflecting individual differences	X	C	X	X	C	A
6) Reflecting the number of participants	A	A	X	X	C	A
7) Safety map for everyone	C	A	B	B	B	A

Table II compares the related works and the proposed method. The evaluation marks (A, B, C, X) are based on the requirements for safety road maps, the accuracy of the input data, and the privacy policy of the police bureau.

The police bureau safety map has an A rank for '*Accuracy*' because it's based on the report data. Meanwhile, Honda safetymap has a B- rank because their sudden-brake locations just appear at traffic signals only. Google Live Traffic got a C rank for displaying only traffic jams without safety information. Google Live Traffic and the proposal got an A rank for '*Automatic generation*' because of full automation of generation. Again, the police bureau safety map has an A rank for '*Privacy consideration*' because it's based on the report data.

The proposal got an A rank for '*Community participation*' for supporting both IOS and Android smartphone. Meanwhile, Google Live Traffic only supports Android smartphone. The proposal got an A rank for '*Reflecting individual difference*' because this is only method to support of reflection of human factors in the model. Honda safetymap, and the proposal got an A rank for '*Safety map for everyone*'. Meanwhile, the police bureau safety maps got a B rank because it needs to make accessible to more road safety information.

In this section, the related research has been reviewed. It is confirmed that there are two types of the input data for traffic safety maps. One utilizes accident reports provided by police bureau, and another utilizes probe car- or smartphone- based data. For purpose of generating traffic safety maps, it is necessary to detect hazard locations by some way. In addition, there are two methods of detecting hazards. The first method assumes accident locations reported to be hazard. The second method uses some sensible information, which sometimes leads accidents. The disadvantage of the first approach is that a near miss situation cannot be reflected on traffic safety maps because an accident has not happened. The disadvantage of the second is deviation from the true hazard locations and the sensed locations. The review's result pointed out that current difficulty of making safety maps automatically is the difficulty of computation of vehicle's collision probability. Based on the review's result, this paper proposes a method for detecting hazard locations based on different behaviors among road users in the next section.

III. PROPOSED METHOD

This section explains the proposed method.

A. *Generating the traffic safety map*

The process for generating the proposed traffic safety maps is depicted in Fig. 3. The proposed traffic safety map is referred as a TimeDiff map. The TimeDiff map is a kind of hazard map (Fig. 1). The map integrates a collection of traffic-incident maps that are generated from users' smartphone log data (proposed in [10], [11]). This section reviews the core components of this map-generating process-viz., the IMAC model[16] and the Simple Braking Model (SBM)[11]. Then, the method for constructing a user's traffic-incident map is explained (the left side of Fig. 3). Finally, the proposed summarization method for integrating these incident maps into a global hazard map is described (the right side of Fig. 3).

B. *Simple Braking Model(SBM)*

This section explains the method for generating a traffic incident map that can be used to interpret how a driver recognizes the road environment.

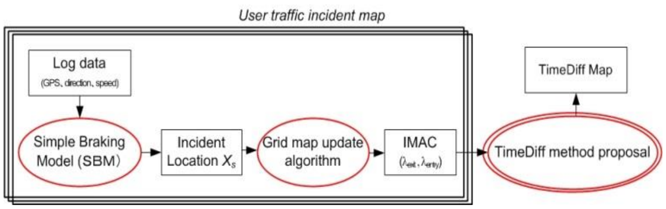


Fig. 3. Process for generating traffic safety map

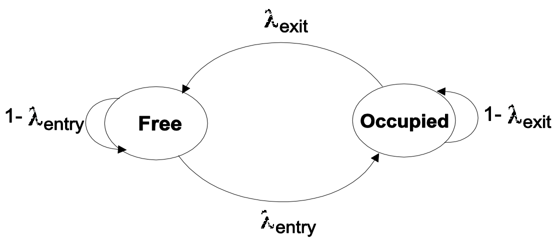


Fig. 4. Grid model – a two state Markov chain[16]

The Simple Braking Model (SBM) is firstly described. The SBM model will be used to measure vehicle deceleration behavior (i.e., upon approaching an incident). The SBM describes the relation between the vehicle's moving distance, the vehicle's speed, and the estimated incident location[11].

Assume that whenever a vehicle encounters an incident, it always decreases its speed to avoid accident. The relation between the current speed and the moving distance is described as follow braking equation:

$$\frac{dx}{dt} = v_0(1 - \frac{x}{X_s})^n \quad (1)$$

where X_s is the initial distance to the incident, x is current distance to the incident (x=0 when the vehicle begins to slow down), n>0, and v_0 is the initial speed.

C. Generating a traffic-incident map with IMAC

This section explains method for estimating the locations of incidents, and discusses individual driver characteristics, and the process for generating a user's traffic-incident map [10],[11]. Saarinen et al. proposed IMAC, a model for describing dynamic environments with an occupancy grid map[16], and this model is utilized to represent traffic incidents. With the IMAC model, the mapping environment is evenly divided into grids. Each grid is modelled as a two-state Markov chain with two states of being: *free* and *occupied* (see Fig. 4). The IMAC model is suitable for representing dynamic objects, such as traffic signals or traffic incidents, with a grid map. Furthermore, IMAC is used to estimate the transition-probability parameters ($\lambda_{exit}, \lambda_{entry}$) by observing the occurrence of the state occupied or free and the transitions between them.

Eq. (2) describes the behavior of a grid at each step of the observation.

$$P = \begin{bmatrix} 1 - \lambda_{entry} & \lambda_{entry} \\ \lambda_{exit} & 1 - \lambda_{exit} \end{bmatrix} \quad (2)$$

where λ_{exit} is the probability that the grid state changes from *occupied* to *free*, and λ_{entry} is the probability that the grid state changes from *free* to *occupied*. Suppose that these transitions to follow a Poisson process. A Poisson process describes the probability of observing a number of events within a certain amount of time. The stationary distribution of the grid state vector π is derived as follows:

$$\pi = \left(\pi_1 = \frac{\lambda_{exit}}{\lambda_{exit}+\lambda_{entry}}, \pi_2 = \frac{\lambda_{entry}}{\lambda_{exit}+\lambda_{entry}}\right) \quad (3)$$

The stationary distribution represents the probability of observing the grid in a particular state given an infinite number of steps. In Eq. (3), π_1 is the stationary probability of observing the grid in a free state, and π_2 is the stationary probability of observing the grid in an occupied state.

D. Map estimations with IMAC

To estimate the grid states from the observed events, Saarinen et al.[16] proposed a method for observing two processes in each grid in a dynamic environment with Eqs. (4) and (5):

$$\hat{\lambda}_{exit} = \frac{\alpha_{exit}}{\beta_{exit}} = \frac{\#events{:}occupied\ to\ free{+}1}{\#observations\ when\ occupied{+}1}, \quad (4)$$

$$\hat{\lambda}_{entry} = \frac{\alpha_{entry}}{\beta_{entry}} = \frac{\#events{:}\ free\ to\ occupied\ {+}1}{\#observations\ when\ free{+}1}, \quad (5)$$

where α_{exit} denotes the number of times a grid is observed switching from *occupied* to *free* (#OTF), β_{exit} is the number of observations made in the *occupied* state (#OCC), and α_{entry} and β_{entry} are the quantities for observing a grid switch from *free* to *occupied* (#FTO) and for observing the grid in the *free* state (#FREE). The additional +1 in Eqs.(4) and (5) follows from the initialization of all the parameters at one. The interpretation of $\hat{\lambda}_{exit}$ as a Poisson rate parameter is the expected number of state-change events per observation, given that the current state is *occupied*.

E. Estimations for untraveled roads and locations

Unknown locations are off-road locations upon which vehicles do not travel. In the IMAC model, λ_{exit} and λ_{entry} are probabilistic values (0< λ_{exit} <1, 0< λ_{entry} <1). This experiment stipulated λ_{exit}=λ_{entry}=1 for unknown locations.

F. TimeDiff method

This section proposes an integration method for generating a global map from a collection of IMAC users' grid maps for ($\lambda_{exit}, \lambda_{entry}$). This method is based on the average time that users hold a different recognition of the same road environment, it's called TimeDiff method. The global map (i.e., the TimeDiff map) shows the total time for road-recognition differences between users in a given area.

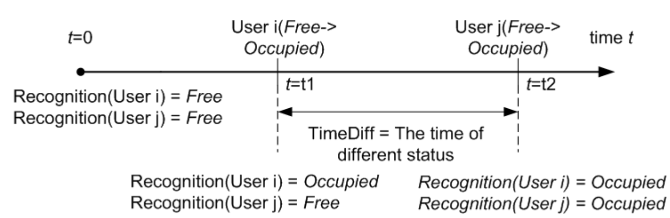


Fig. 5. Time differences in the judgment of a road environment

TimeDiff concept: Consider a scenario where two vehicles are driving along a road. At this time, the road upon which the vehicles are traveling is recognized as *Free* (see Fig. 5). As the two vehicles approach a red traffic signal, they encounter an incident, and the road at this location is recognized as *Occupied*. Consequently, both vehicles come to a stop. At this time, both vehicles must change their recognition of the road environment from *Free* to *Occupied*. TimeDiff method focuses on the time that each vehicle changes its status. It is clear that the occurrence of an accident depends on the recognition of both drivers. If two vehicles change their status at the same time, they both have the same recognition of road environment. Thus, an accident will not occur unless a driver makes a mistake in controlling the vehicle. By contrast, the more difference in time between when the recognition changes - that is, between when one vehicle recognizes the road as *Free* and other recognizes it as *Occupied* - the higher the likelihood of a collision. Thus, the global TimeDiff map is based on the road-recognition level of the users.

Let *D* be the set of users. Assume that all users generate their own traffic incident map (λ_{exit}, λ_{entry}) by using the update method in Eqs. (4) and (5).

The hazard level of each grid *g* in the global map is defined by Eq. (6). Suppose two users, *i* and *j* in *D*, initially report an *Occupied* status. Suppose further that user *i* changes this status to *Free* before user *j* does. Alternatively, suppose that *i* and *j* initially report a *Free* status, and that the status from user *i* switches to *Occupied* before that of user *j*. The total difference in time between such status changes (whether *Occupied* or *Free*) from all pairs of users *i* and *j* in *D* is calculated as follows:

$$TimeDiff_g = \sum_{i\in D}\sum_{j\neq i, j\in D} E\left(P^f_{dif}(i,j)\right) + E\left(P^o_{dif}(i,j)\right) \quad (6)$$

where $E\left(P^f_{dif}(i,j)\right)$ is the difference in time between switches when each pair of users initially reports a *Free* status, and $\left(P^o_{dif}(i,j)\right)$ is the difference in time between switches when each pair of users initially reports an *Occupied* status. Suppose that this follows a Poisson process.

$$E\left(P^f_{dif}(i,j)\right) = \int_0^{B_f} t\cdot Prob[X_i = occ \leq t]\, Prob[X_j = occ > t]dt \quad (7)$$

$$= \int_0^{B_f} t\ \cdot Prob[X_i = occ \leq t]\,(1 - Prob[X_i = occ \leq t])dt \quad (8)$$

$$= \frac{e^{-B_f(\lambda_{i,entry}+\lambda_{j,entry})}(1-e^{B_f(\lambda_{i,entry}+\lambda_{j,entry})}+B_f(\lambda_{i,entry}+\lambda_{j,entry}))}{(\lambda_{i,entry}+\lambda_{j,entry})^2} + \frac{1-e^{B_f\lambda_{j,entry}}(1+B_f\lambda_{j,entry})}{\lambda^2_{j,entry}} \quad (9)$$

when $t = 0$, then $X_i = X_j = free$. Moreover, B_f is a constant. Here, $\lambda_{i,entry}$ represents the λ_{entry} for user i, $\lambda_{j,entry}$ represents the λ_{entry} for user j.

$$E\left(P^o_{dif}(i,j)\right) = \int_0^{B_o} t\cdot\ Prob[X_i = free \leq t]\, Prob[X_j = free > t]dt \quad (10)$$

$$= \int_0^{B_o} t\cdot\ Prob[X_i = free \leq t]\,(1 - Prob[X_i = free \leq t])dt \quad (11)$$

$$= \frac{e^{-B_o(\lambda_{i,exit}+\lambda_{j,exit})}(1-e^{B_o(\lambda_{i,exit}+\lambda_{j,exit})}+B_o(\lambda_{i,exit}+\lambda_{j,exit}))}{(\lambda_{i,exit}+\lambda_{j,exit})^2} + \frac{1-e^{B_o\lambda_{j,exit}}(1+B_o\lambda_{j,exit})}{\lambda^2_{j,exit}} \quad (12)$$

when $t = 0$, then $X_i = X_j = Occupied$. Likewise, B_o is a constant. Here, $\lambda_{i,exit}$ represents the λ_{exit} for user i, $\lambda_{j,exit}$ represents the λ_{exit} for user j.

For example, when $\lambda_{i,exit} = 0{,}01$, $\lambda_{j,exit} = 0.1$, $B_o = 10$, then $E\left(P^o_{dif}(i,j)\right) = 1.5505$.

G. Summary

In summary, this section discussed the proposed map-integration method, TimeDiff, using smartphone data based on differences in the recognition of the road environment. In next section, two kinds of TimeDiff maps are discussed: the high-risk TimeDiff map and the low-risk TimeDiff map. The high-risk TimeDiff map presents locations at which the difference of the time recognition between two users is larger. On the contrary, the low-risk TimeDiff map presents locations at which the difference of the time recognition between two users is small.

IV. Experiment

This section evaluates the proposed method with a realistic scenario. The global hazard map (i.e., the proposed TimeDiff map) was quantitatively evaluated in terms of its effectiveness using the F-measure method. The datasets for the experiment comprised a month of data from two drivers with one bike (Honda CBR) and one car (Mazuda 6) on the test route. The smartphone is put on pocket door of vehicle or attached on drivers' arm. The latitude, longitude, speed, and azimuth extracted from GPS data are used for experiment.

Test course: The test course covers the Maborikaigan area in Kanagawa Prefecture, Japan, as shown in Fig. 6. The data includes 30 days of smartphone log data. Each day covers 8 km of road along the test course (the red road in Fig. 6). The road between Mabori Elementary School and the Otsu traffic signal is narrow, and traffic jams is common. The No. 16 National Road has four lanes, and it is rarely faced by traffic congestion.

Police accident data: The distribution of 260 locations of accident in Maborikaigan area(2010-2014) on this course provided by the Uraga police bureau is shown in Fig. 7. This distribution shows that accidents usually occur either on narrow roads with high-volume traffic and in areas with traffic signals. Fig. 8 shows the sudden-brake distribution of Honda's safetymap for the Maborikaigan area. The distribution of sudden-brake locations all occurred near traffic signals (known to be high-risk areas). However, from the accuracy point of view, these results are insufficient because the numbers of the spots in the Honda's map are 18 locations, too less than the number of the accidents provided by the Uraga police bureau.

A. Traffic safety map with TimeDiff method

The TimeDiff maps ($B_o = B_f = 10$) generated from Honda CBR's dataset and Mazuda 6's dataset are shown in

Figs. 9 and 10. The maps represent hazardous spots in terms of the time differences in the recognition of the road environment.

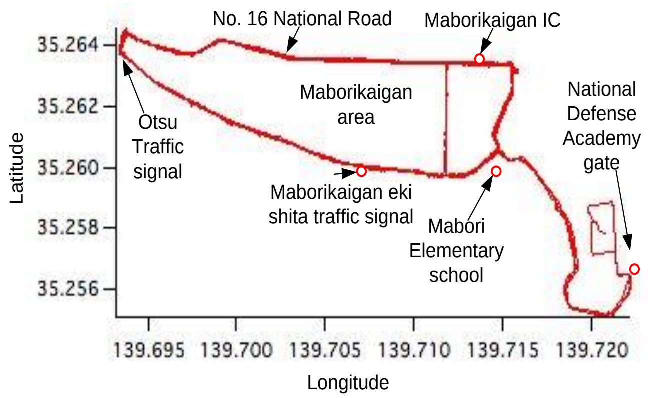


Fig. 6. Test course in Maborikaigan area

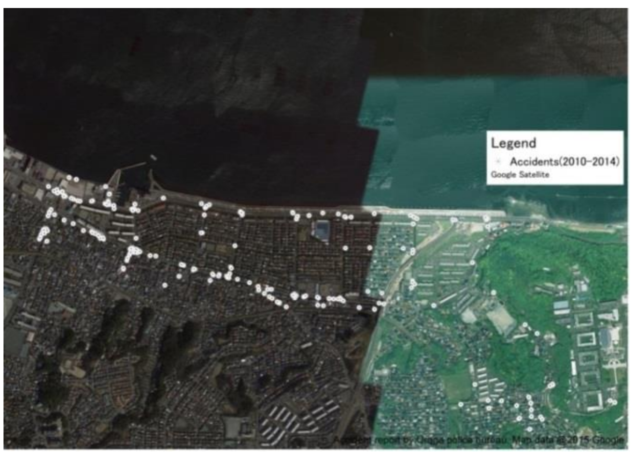


Fig. 7. Accident data in Maborikaigan area provided by the Uraga police bureau

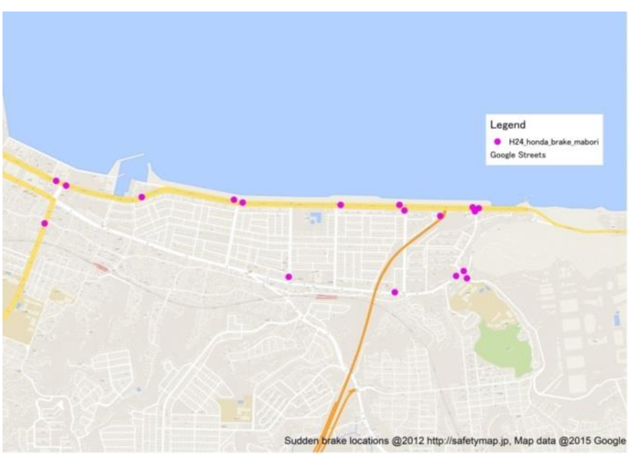


Fig. 8. Honda's sudden brake locations in Maborikaigan area[9]

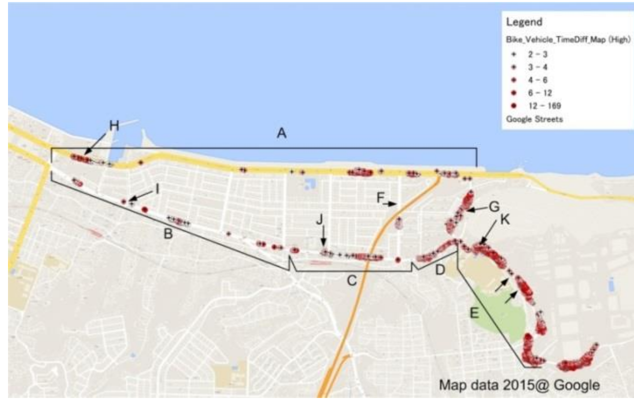


Fig. 9. Traffic safety map by TimeDiff method($B_o = B_f = 10$): high risk areas

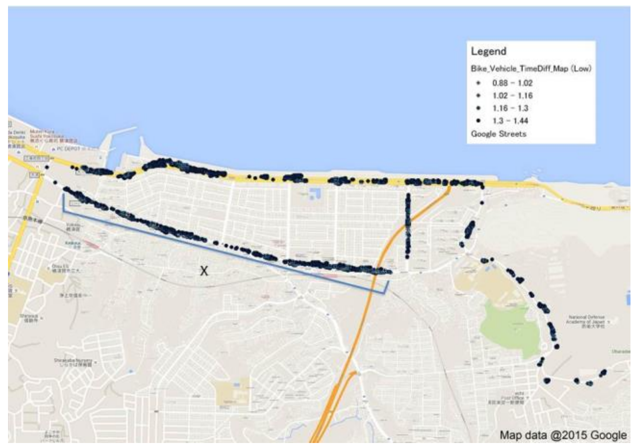


Fig. 10. Traffic safety map by TimeDiff method($B_o = B_f = 10$): low risk areas

There are two TimeDiff maps: the high-risk TimeDiff map (Fig. 9) and the low-risk TimeDiff map (Fig. 10).

The high-risk TimeDiff map is shown in Fig. 9. The white-red graduated circles with the plus sign denotes the level of time difference in recognition by two drivers. The TimeDiff value ranged from 2 to 169 based on the quantile, and this was divided into 5 levels. The high-risk map for the route between the Otsu traffic signal (interval B) to the Maborikaigan eki shita traffic signal through Mabori Elementary School (interval C, D) contains more hot-spots than does the route along the No. 16 National Road between Maborikaigan IC and the Otsu traffic signal (interval A). This result agrees with the accident data provided by the Uraga police bureau.

Moreover, most locations with a high distribution of accidents provided by the police bureau can also be verified with this map. Some representative accident locations which detected by the proposed method are depicted by the arrows with capital letters in Fig. 9. For examples, spots have many vehicles come in and out (the exit entry of packing area - spot H and the entrance to residence area - spot I); spots have many pedestrians (the Maborikaigan eki shita traffic signal - spot J, spot F, spot G).

Figs. 11 and 12 show scene photographs of spot I and K of Fig. 9. The features of spot I are narrow road with high volume traffic, lot of vehicles come in and out, four lanes road decreases to two lanes. The features of spot K are the road is poor visibility with a lot of jump out of the road. The proposed method successes in detecting such hazard locations.

Fig. 11. Accident location at the entrance to Otsu Sea Height Mansion (Spot I in Fig. 9)

Fig. 12. Accident location at the entrance to Mabori Elementary School (Spot K in Fig. 9)

Fig. 10 illustrates the low-risk TimeDiff map and the white-blue graduated circles with plus sign denotes the level of time difference in recognition by two drivers. The TimeDiff value ranges from 0.88 to 1.44 based on quantile, and this is divided into 5 levels. The low-risk map shows locations where there is little difference in recognition - that is, where two drivers' recognition of the road was almost same.

The proposed map suggests the traditional assumption that around a hazard spot is dangerous, is not always true and around a safe spot is not always safe. According to the low-risk map, the low-risk locations are distributed all over the test route. This means two drivers' recognition of this road is almost same. For example, two drivers have almost equal recognition of the road from Mabori Elementary School to the Otsu traffic signal (Fig. 10, interval X), meanwhile many hazard locations can be seen for the same area (see Fig. 9, interval B, C, D). That means unsafe locations exist among area looks safe.

From above result, most of hazard locations can be detected using the traffic safety maps based on the recognition difference of road environment. In the subsequent section, the proposed method is evaluated quantitatively by the F-measure method for further discussion.

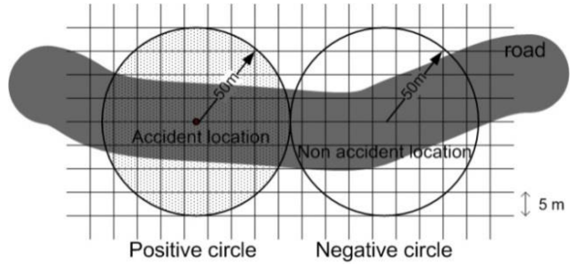


Fig. 13. Evaluation circles

TABLE III. DATASETS FOR EVALUATION

Data	Police data	Honda sudden-brakes data	Smartphone data
Data period	2010-2014	2012	2013,2015
Data region	Maborikaigan area	Maborikaigan area	Maborikaigan area
Data type	Accident report	Sudden-brakes data	Traffic safety map
Data for evaluation (in detail)	Accident distribution	Sudden-brakes distribution	TimeDiff value,

B. Evaluation result by F-measure method

The F-measure method was adopted to further evaluate the traffic safety maps that were generated. In statistical analysis of binary classification by an information retrieval system, the F-measure is a criteria of a test accuracy. This measure is harmonic mean of precision score and retrieval score. The precision score evaluates the number of the correct items in a search result. The retrieval score is the fraction of found correct items in the total correct items.

Suppose the accident distribution provided by the police bureau is the correct answer of the hazard locations for the F-measure method. The Honda's sudden brakes distribution is used for the baseline of evaluation. The detailed dataset for evaluation is shown in Table III.

"Evaluation circles" is used for calculating of F-measure (Fig. 13). Every road is divided into multiple circles with a radius of 50 m, including "positive circles" or "negative circles". Positive circles are created with the location of an accident at its center, and negative circles are continually created in other locations where accidents do not occur.

The F-measure method is defined as in Eqs. (15), (16), (17). AD_R is a set of the positive circles (the answer set). HL_R is a set of circles which detected as "hazards" by a given map method (the predict set).

$$F-measure = 2 \cdot \frac{Recall \cdot Precision}{Recall + Precision} \tag{15}$$

$$Precision = \frac{|AD_R \cap HL_R|}{|HL_R|} \tag{16}$$

$$Recall = \frac{|AD_R \cap HL_R|}{|AD_R|} \tag{17}$$

The result is closer to 1, the better performance they are.

Table IV shows the results from evaluating the proposed method. The proposed method's F-measure is the higher (=0.6542923), meaning that the TimeDiff map agrees with the police bureau's accident distribution by approximately 65.42%. Meanwhile, the Honda's sudden brakes distribution agrees with the police bureau's accident distribution of about 44.5%. From the value of precision and recall, the traffic safety maps by the proposed method better covers more hazard locations in the test route.

In summary, these results show that the traffic safety maps generated by the proposal provide better result than Honda's safetymap when compared to the police bureau's accident distribution. Moreover, the difference of recognition of road users can be used to estimate hazard locations.

TABLE IV. F-MEASURE EVALUATION RESULT

Method	**Precision**	**Recall**	**F-measure**
Honda sudden-brake	0.9746835	0.2883895	0.4450867
TimeDiff	0.8597561	0.5280899	0.6542923

V. CONCLUSION

This paper proposed a method that uses smartphone data to automatically generate traffic safety maps based on the differences in how individuals recognize the road environment. The generating traffic safety map is referred as a TimeDiff map. The TimeDiff maps achieved better results when compared to Honda's safetymap, which is based on the occurrence of sudden brakes. From the experiment result, the difference of recognition of road users can be used to estimate hazard locations.

The power consumption is a limitation of the proposed system. It must be minimized so that will not affect a user's smartphone usage. The power consumption could be decreased by developing computationally efficient algorithms and minimizing the GPS usage.

ACKNOWLEDGEMENT

We would like to thank the Uraga police bureau for providing the accident data of Maborikaigan area.

REFERENCES

[1] B. Hilton, T. Horan, R. Burkhard, and B. Schooley, SafeRoadMaps: Communication of location and density of traffic fatalities through spatial visualization and heat map analysis information visualization. Information Visualization 10.1(2011): 82-96.

[2] Traffic Safety Map & Near-miss Map. Kanagawa Pref. Police Department. 06 August 2015 Accessed.

[3] Saferoadmaps project. University of Minnesota. 2012 Published. 06 August 2015 Accessed.

[4] P. Mohan, N. Venkata, and R. Ramjee, Nericell rich monitoring of road and traffic conditions using mobile smartphones. In Proceedings of the 6th ACM conference on Embedded network sensor systems. pp. 323-336, 2008.

[5] A. Fathi and J. Krumm, Detecting road intersections from GPS traces, Geographic Information Science, Lecture Notes in Computer Science. Volume 6292, 2010, pp. 56-69.

[6] M. Fazeen, B. Gozick, R. Dantu, M. Bhukhiya, and M. C. Gonzalez, Safe driving using mobile phones, IEEE Transactions on Intelligent Transportation Systems, 13.3: 1462-1468, 2012.

[7] L. Zhang, F. Thiemann, and M. Sester, Integration of GPS traces with road map, Proceedings of IWCTS '10, Proceedings of the Second International Workshop on Computational Transportation Science, pp. 17-22, 2010.

[8] Google Live Traffic. Wikipedia. 01 June 2015 Last Modified. 06 August 2015 Accessed.

[9] Safety Map Project. Honda Company. 2013 Published. 06 August 2015 Accessed.

[10] V. C. Dang, M. Kubo, H. Sato, T. Shirakawa, and A. Namatame, Occupancy grid map of semi-static objects by mobile observer. Artificial Life and Robotics. 20.1: 7-12, 2014.

[11] V. C. Dang, M. Kubo, H. Sato, A. Yamaguchi, and A. Namatame, A simple braking model for detecting incidents locations by smartphones. In Computational Intelligence for Security and Defense Applications (CISDA), 2014 Seventh IEEE Symposium on, pp. 1-5, 2014.

[12] P. K. Marhavilas, D. Koulouriotis, and V. Gemeni. Risk analysis and assessment methodologies in the work sites: On a review, classification and comparative study of the scientific literature of the period 2000-2009. Journal of Loss Prevention in the Process Industries 24.5 (2011): 477-523.

[13] How to prevent accidents. Safety Transportation. Japan Ministry of Land, Infrastructure, and Transportation. 06 August 2015 Accessed.

[14] T. Shimizu, Y.Ohama, S. Nagata, J. Sakugawa, A computational framework for estimating collision risk against pedestrians. R&D Review of Toyota CRDL, Vol.43. No.1 (2012) 22-42.

[15] Traffic Accident Hotspots Map. General Insurance Association of Japan. 6 August 2015 Accessed.

[16] J. Saarinen, A. Henrik, and J. L. Achim, Independent markov chain occupancy grid maps for representation of dynamic environment. In Proceedings of IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), pp. 3489-3495, 2012.

The Impact of Learning Styles on Learner's Performance in E-Learning Environment

Manal Abdullah
Department of Computer Science
Faculty of Computing and Information Technology, FCIT
King Abdul-Aziz University, KAU
Jeddah, Saudi Arabia

Reem M. Bashmail
Department of Computer Science
Faculty of Computing and Information Technology, FCIT
King Abdul-Aziz University, KAU
Jeddah, Saudi Arabia

Wafaa H. Daffa
Department of Computer Science
Faculty of Computing and Information Technology, FCIT
King Abdul-Aziz University, KAU
Jeddah, Saudi Arabia

Mona Alzahrani
Department of Computer Science
Faculty of Computing and Information Technology, FCIT
King Abdul-Aziz University, KAU
Jeddah, Saudi Arabia

Malak Sadik
Department of Computer Science
Faculty of Computing and Information Technology, FCIT
King Abdul-Aziz University, KAU
Jeddah, Saudi Arabia

***Abstract*—due to growing popularity of E-Learning, personalization has emerged as important need. Differences of learners' abilities and their learning styles have affected the learning outcomes significantly. Meanwhile, with the development of E-Learning technologies, learners can be provided more effective learning environment to optimize their performance. The purpose of this study is to determine the impact of learning styles on learner's performance in e-learning environment, and use this learning style data to make recommendations for learners, instructors, and contents of online courses. Data analysis in this research represented by user performance gathered from an E-learning platform (Blackboard), where this user performance data is represented by actions performed by platform's users. A 10-fold cross validation was used to create and test the model, and the data was analyzed by the WEKA software. Classification accuracy, MAE, and the ROC area have been observed. The results show that the accuracy of classification by means of NBTree technique had the highest correct value at 69.697% and it could be applied to develop Felder Silverman's learning style while taking into consideration students' preference. Moreover, students' performance increased by more than 12%.**

Keywords—Learning style; Silverman; E-Learning; online learning; styling model

I. INTRODUCTION

The great population of the Internet and computer has affected the learning methodologies and education. Traditional education approaches have been changed using these new technologies. In fact the integration of new technologies in the field of education offers new challenges and opportunities in distance learning and e-learning in general. Online learning provides learners with more resources that cater to all needs in various fields of educations. Currently, various supporting technologies are available for teaching processes and learning practices in many universities and schools. This leads to an e-learning paradigm.

The transformation of the teaching-learning practices to the e-Learning environment has attracted researchers to understand, examine and evaluate the role of the information and communication technologies in the learning environment. It is evident that learning and education differ greatly between learners due to their different preferences, needs and approaches to learning. Psychologists call these individual differences learning styles. Therefore, it is very important to accommodate for the different styles of learners through learning environments that they prefer and find more efficient.

Learning style could be a good predicator of an individual's preferred learning behavior and a good indicator of successful distance learning. Majority of the research conducted are based on the learning styles as these are the most dynamics and give the best results if catered to properly. In other words, understanding the learners' needs and identifying their patterns of learning are crucial to design e-learning material according to learners' learning styles and to bridge the gap resulting from unfamiliarity of a triangular community members i.e. learners, instructors, and contents of online settings. It is necessary to determine what is most likely to grasp each learner's attention, and how to respond to his/her natural understanding style to produce long-term remembering. The main challenge is the detection of the learning styles. Identifying learners' learning style has been considered as vital element. Teaching methodology should be, in turn, adjusted with online instruction and delivery [1]. Researchers have described various learning styles models such as Kolb [2], Honey & Mumford [3], and Felder-Silverman [4].

Learning style affects how a student responds to stimuli and approaches new material. There are some ways that can use learning style data to enhance student's learning experience. Learning style data can be used to guide the student toward more effective study habits and that data can be used to help instructors in their selection of instructional strategies.

The system deals with information about learners and their learning activities to recommend the appropriate way to present the material for students based on their learning style and other data. This paper discusses the approach of intelligently detect student's learning style based on integrated Felder Silverman (IFS) learning style model, and then uses this data with Blackboard (BB) Learning Management system (LMS) to optimize student's learning outcomes.

The rest of this paper is organized as follows: In section2 Felder-Silverman learning style model (FSLSM) is introduced. Section 3 describes the combinations importance of electronic media and learning styles. Section 4 briefly presents some related work. Section 5, introduces proposed model. Section 6, section 7 and section 8 respectively, present experimental procedure, results and discussion then concluding the paper and future work.

II. Felder-Silverman Learning Style Model

Over seventy identifiable approaches are used to investigate and describe learning style preferences. Felder-Silverman learning style model (FSLSM) has been the most popular model because it seems to be the most appropriate for use in computer-based educational systems [5]. FSLSM has the advantage of the sliding scales supporting a classification of student's style which is more flexible than bipolar models. Most other models classify learners in few groups, whereas FSLSM identifies the learning style and distinguishes between preferences on four dimensions. Each dimension includes two variables [6] as shown in figure 1. Data collection tool, called Index of Learning Styles (ILS) assesses variations in individual learning style preferences across four dimensions or domains.

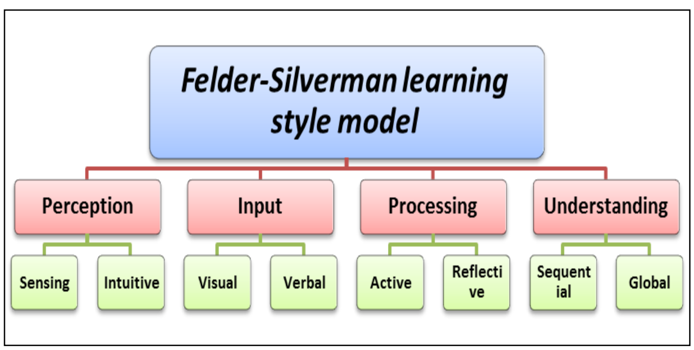


Fig. 1. Felder-Silverman Learning Style Model

A. *Index of Learning Styles (ILS) Felder Silverman*

The Index of Learning Styles (ILS), developed by Felder and Soloman, is 44 questions for identifying the learning styles according to FSLSM. As mentioned earlier, learner has a personal preference for each dimension. Each preference is expressed with a value between +11 to -11. This range is computed based on the 11 questions that are posed for each dimension. When learner answers a question with an active preference, +1 is added to the value of the active/reflective dimension. Whereas if he answers with a reflective preference, this decreases the value by 1. Therefore, each question changes total value for certain dimension with a value of +1 (answer a) or -1 (answer b). Answer a referes to the preference of the first pole for all dimensions (active, sensing, visual, or sequential), and answer b referes to the second pole of all dimensions (reflective, intuitive, verbal, or global).

B. *Grouping of Silverman Model*

Each learning style of FSLSM is described by different characteristics. Based on this description [4], the questions in ILS are manually grouped according to the similarity of semantics. Each dimension distinguishes between two oppisite characteristics. Active/reflective dimension represents the way of processing information. The second dimension covers sensing/intuitive learning. The third, visual/verbal dimension differentiates learners who remember best what they have seen. The fourth dimension characterizes learners' understanding. Sequential learners understand in small incremental steps, therefore have a linear learning progress. According to this model, learning styles determine different sets of learning sequences for learners with different learning styles. So, $\mathbf{2^4}$ = 16 different learning style are created by the combination of the four dimensions.

C. *Analyses of Semantic Groups*

To detect the most representative groups from the sixteen learning styles groups mensioed above, some analyses are performed based on data collected from the ILS questionnaire. Fisher discriminant analysis for linearly reducing dimensionality can be used to optimally separate the most representative semantic groups of each dimension. The research then compares the model given by Fisher discriminant analysis with some experimental results. Frequency and correlation analysis are performed in order to cross-validate the model used. It is also important to conduct some statistical analysis which transforms data to its absulute scale, that is frequecies. Let Q be the 25x44 matrix containing in rows instances of students and in columns the answer to each ILS question. For each question q_i, Q=44, two numerical variables are allowed, $a_1 = 1$ if $q_i = 1$ (otherwise 0) and $a_2 = 1$ if $q_i = -1$ (otherwise 0). Let A be the 40 x 88 matrix containing in rows individuals and in columns the a_i, i=1,…,88. The matrix A has ranked at most 44 by construction, since two columns are constrained to sum up to 1 in rows. Fisher linear discriminant analysis (LDA) is then performed on the whole matrix A of learners' answers to ILS.

III. Learning Style with Electronic Media

In the context of Information and Communication Technology ICT evolution and due to the wide spread of electronic media, making use of e-media with teaching and learning styles has facilitated the teaching process. Many researches studies the effectiveness of combining multimedia and hypermedia within educational systems [7] [8]. In these studies, authors associated specific e-media characteristics to different categories of learners and proposed tools and models for assessing learning style [9]. Most of these studies rely on Kolb's Learning Styles Inventory (LSI) [2] and Soloman-Felder Index of Learning Styles (ILS) [10]. However, e-media as a learning object may be used with different implementations to adapt different learning styles. The combinations of different electronic media are examined by few researchers to decide the appropriate combinations for certain learning style which yield effective learner's performance. For example [6], discussion forum object combined with some problem solving object may be used to assign a practical task to students in such a way that students discuss the assigned problem in a collaborative manner. Sensitive learning style can benefit this combination. Sequential style students may also make use of discussion forum by communicating with the teacher through sequential series of presentations associated with the corresponding discussion.

IV. Related Work

Many educational software has been developed to match students' learning style with the appropriate learning objects. These can be broadly classified into two categories: (A) Adaptive systems that adapt the course object to learners' learning styles, and (B) Tutoring systems that suggest appropriate learning activities through different recommendation techniques. These recommendations are based on learner's preferences, knowledge and the browsing history of other learners with similar characteristics.

A. *Adaptation Systems to Learner's Learning Styles*

A lot of research work had been proposed for determining learning style of individuals dynamically. The dynamic changes of the behaviour and the knowledge level of an individual determine the his/her learning style. The studies can be broadly classified into two approaches: data-driven approach (using Bayesian Networks and NBTree classifiers) and literature-based approach. The literature-based approach investigates learners' behaviors in their interactions with LMSs. Some of the noticeable works have been summarized here. Garcia et al. [11] proposed a Bayesian network based model that is used to infer the learning styles of the students according to their modelled behavior, in order to adapt styles in Web-based education system. O polar and Akbar [12], proposed an automated learner model based on FSLSM learning styles classifier using NBTree classification in conjunction with Binary Relevance Classifier. Montazeri and Ghorbani [13] proposed an Evolutionary Fuzzy Clustering (EFC) methodology with Genetic Algorithm (GA) for the recognition of learning styles of e-learners. The work of Graf et al. [14] proposed a literature-based approach that automatically detects the learning styles in LMSs. Dung and Florea [15] tracked data of learners' behaviors and used simple mapping rule to infer learning styles against Felder-Silverman Learning Style Model.

B. *Systems with Implemented Recommendation*

Data mining techniques can be used to recommend e–learning strategies by adapting learner's characteristics and preferences. Learner characteristics are such as learning styles, experince, knowledge etc. The "Adaptive Hypermedia Architecture", has been developed for providing online course recommendations [16]. Adaptation of presentation and navigation system based on specific prediction rules is used. Garcia et al. [11] extended their previous work by providing suggestions based on the learning styles of the students. An intelligent agent called eTeacher, was provided to help students at certain course through an eLearning system called SAVER. Example of recommendations advised to sequential learner are to read certain topic before reading another one. During the analysis, authors reported that 83% of the total feedback received was positive.

Beragasa-Suso et al. [17] designed a web browser-based system called iLessons. The system is embedded within Microsoft Internet Explorer enabling the teachers with various features such as reusing the materials available on the WWW by drag and drop, navigation options. The authors extended the iLessons system by assessing the students' learning styles based on FSLSM using the online available Index of Learning Styles (ILS) for recommending relevant web sites to the students. Finally, the active-reflective dimension, for examplr, was determined taking into account some parameters such as the ratio between the images and text of a page, the average time spent on a page, the scroll distance and direction changes and the mouse movements. These parameters were used to predict learner's learning style with an accurate rule.

Khiribi et al. [18] used learner navigational history and similarities among learners' preferences and educational contents to recommend the learning resources. The proposed framework is essentially based on two components: *the Modeling phase* and the *Recommendation phase.* Garth and Abdullah [19] introduced a novel architecture for an e-learning recommender system (ELRS) that is based on content-based filtering and good learners' ratings as learning materials recommendation method. Jyothi et al. in [20] stated that most of the existing studies used small datasets to build their models which cannot provide accurate results. They used the historical data to generate students' clusters. As a result, authors proposed a recommendation system to assist the instructor to identify clusters of learners who have similar learning styles identified by FSLSM rather than at the individual level. Milicevic et al. [21] proposed POTUS (Programming Tutoring System). This system used the interests and similar knowledge level of learners to recommend the learning contents for the student. Dwivedi and Bharadwaj [22] developed a weighted hybrid collaborative framework to recommend relevant learning contents to the learner by modeling learning style and the knowledge using collaborating filtering technique.

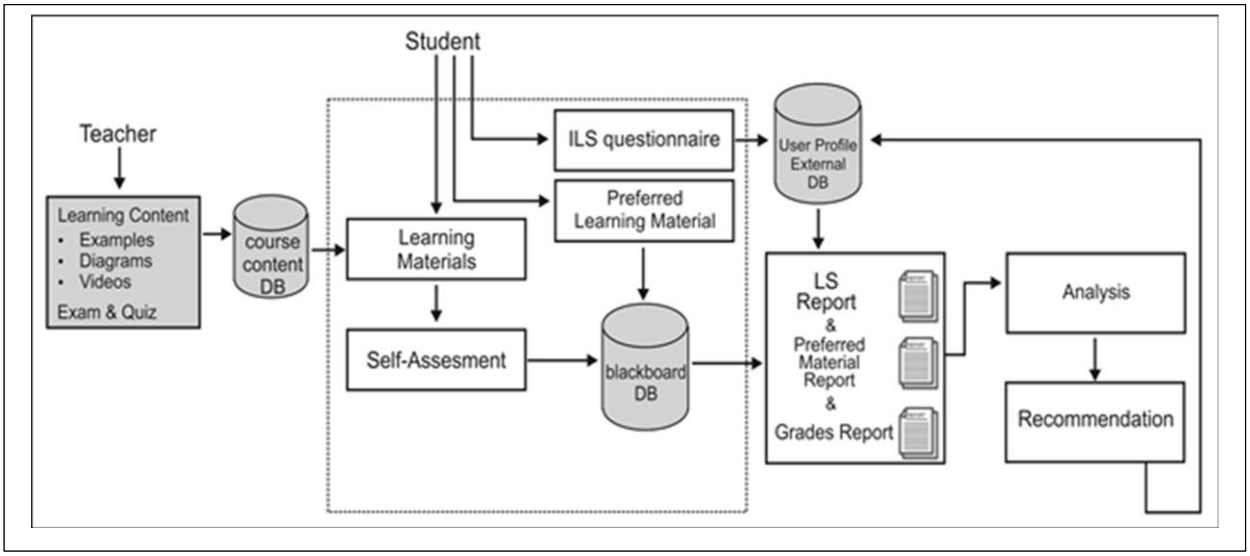


Fig. 2. Learning Style Blackboard Tracking System Model and Architecture

V. Proposed Model

The proposed model matches a student's particular learning style with the case method of teaching to influence course outcomes. This research aims to advise automatic recommendations to an active learner based on his/her learning style, grades and user preferred learning material.

Figure 2 shows the system architecture and design. The basic steps are; A) data collection and pre-processing, B) pattern discovery, and C) validation and interpretation. In the following, detailed explanation is presented.

A. Data Collection and Pre-Processing

The study was conducted on 33 learners, students of the Department of computer science at King Abdul-Aziz University. Three types of data is collected from learners: Learning style detection through questionnaire based on index of learning styles (ILS) developed by Felder and Soloman, quiz grade, and preferred learning style as the preferred learning method.

1) Learners need to complete the ILS questionnaire. This learning style questionnaire indicates a preference for some teaching case. Results are stored in the learner profile.

2) Learners have to log into the Blackboard system (BB), at the first-time, BB system is a leading Learning Management System LMS (or CMS) product used in North America and Europe. It is protected by a password environment and has administration tools that facilitate teaching online.

BB is Web-based server software. Some of its features include course management, customizable open architecture, and scalable design. Student information systems with authentication protocols are integrated to yield secured learning environment. Its main purposes are to develop online elements to courses traditionally delivered face-to-face, as well as providing users with a platform for communication and sharing contents.

3) After logging in, the BB system will display the "Course" screen as shown in figure 3. Students will be asked to complete a self-assessment test after completing the learning materials that have been assigned to them (Abstract, Overview, PowerPoint, Text, Videos & Images, and Examples) to assess their learning gain. The learners' grading can be interpreted according to the percentage of correct answers, as follows: (70 – 100%) is accepted, less than 70% is not accepted. The self-assessment grade is recorded in the Blackboard log and then stored in the learner profile.

4) The learner also needs to answer a short preferred learning style question that it used to determine his/her preferred learning material that most fulfill his requirements.

The profile table, shown as table 1, has eight columns in which first one is for user id. Next four columns are representing dimensions of the learning style model for ILS. Then next two columns are for self-assessment grade and learner's preferred learning materials. And last column is for recommended materials.

The data is then pre-processed and transformed into appropriate format (represented by numbers and stored in the form of CSV file.) in order to analyze and interpret the characteristics of the students based on Felder-Silverman learning dimensions.

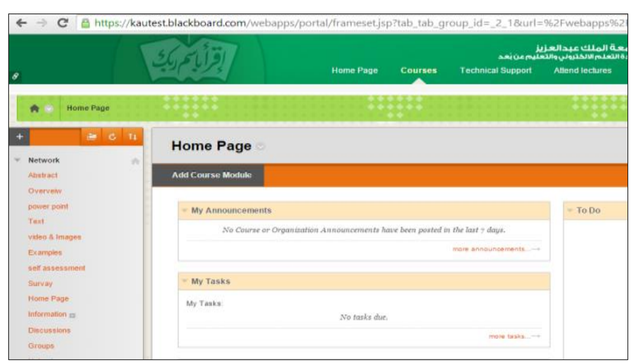


Fig. 3. Blackboard Learning Material Screenshot

B. Classification and Pattern Discovery

The aim of the classifying is to assign labels to each row of the learner profile table using dimensions of the FSLSM. Since each learning style can be associated with an appropriate learning object based on Felder and Soloman characteristics [6] [12], as shown in table 2.

After classifying all learner profile tables, the total score for each scale is calculated using class label counts. Among them, the two related learning style scores for each FSLSM dimension label are compared for that dimension to predict the style. As an example, if the total score for the processing dimension (as Active) is higher than the score for the opposite pole (as Reflective), the participant is reported to be Active. The label with the highest score is assigned to the respective record, as shown by example in Table 1.

Creation and test of the data classification model were conducted by WEKA data mining tool in order to infer the students' learning style. WEKA is developed by the University of Waikato in New Zealand [23] Using JAVA language. Various data mining algorithms are implemented by WEKA. These algorithms include data classification and regression. Also, clustering and association rules are exist. Bayes classifiers, Trees, Rules, Functions, Lazy classifiers and miscellaneous classifiers are examples of learning algorithms implemented in WEKA. WEKA normally uses ARFF file format.

TABLE I. SAMPLE LEARNER PROFILE

id	ILS				Self-assessment	Preferred Learning Material	material
	Active/ Reflective	Sensing / Intuitive	Visual/ Verbal	Sequential/ Global			
	percept	Input	process	understand			
3	% 27.27	% -9.09	% 100	% 45.45	80%	Video	Video

The data in this research has been running on Bayes network classifier (Naïve Bayes) and classification tree with pruning algorithms (J48, NBTree).

WEKA data mining tool has J48 algorithm as an open source Java implementation of C4.5 algorithm, while C4.5 is decision tree based algorithm that is a software extension and improvement to the basic ID3 algorithm. The improvements done by C4.5 over ID3 include accounts for unavailable values, continuous attribute value ranges, pruning of decision trees, rule derivation, and others. A hybrid algorithm called NBTree is a combination of Decision Tree and Naïve-Bayes. NBTree uses the classical recursive partitioning schemes except for pruning where the leaf nodes create Naïve-Bayes groups instead of node predicting a single class. Based on the probability theory, NaïveBayes algorithm is a simple classifier that calculates a set of probabilities using frequencies and combinations of values in a given data set. The algorithm uses Bayes theorem assuming all attributes are independent given the value of the class variable. This conditional independence assumption rarely holds true in real world applications. Although this characterization as Naïve still valid, the algorithm tends to perform well with various supervised classification applications [24], [25].

C. Model Validation

In this research, the used classifiers are evaluated using a 10-fold cross validation method. It divides a dataset into ten parts (folds), hold out each part in turn, and averages the results. Each data point is used once for testing, nine times for training. Finally, the results of the tests were compared in terms of students' performance.

VI. EXPERIMENTAL PROCEDURE

Based on the flexibility offered in Blackboard, various learning resources have been developed for an active "Data Communication and Networking" CS course. To test the effect of using various types of resources depending on students learning styles. Network course is chosen because it is foundation course for CS major. It provides basic networking concepts, including network architecture, design, network protocols, and protocol suit.

The foundation of this study was conducted on 33 learners, students of the Department of computer science at King Abdul-Aziz University. Learners of the training dataset learned based on the extracted learning style; then it is required to complete self-assessment test to evaluate their understanding. However, relying on questionnaires for classifying students' learning styles has main disadvantage that not all the students are motivated to fill out the questionnaire. Hence, misleading answers of the questionnaire which are not the real behavior of the student could be reported [24]. To overcome these problems, a supportive method (one-question) is used to collect the most preferred learning material directly from students. Table 2 shown the relevance keywords for groups of learning styles

Direct learning style (LS_D) and indirect learning style (LS_{IN}) detection methods have been used to extract student's LS. The resulting classification tree is illustrated in Figure 4.If direct and indirect LS doesn't match, their percentage will be compared after giving 60% weight to indirect (LS_{IN}) value as shown in Figure 5, where direct and indirect values indicate respectively, to the ILS questionnaire and the preferred learning style result.

TABLE II. RELEVANCE KEYWORDS FOR CLASSES OF LEARNING STYLES

Learning styles	*material*
active	Experimentally ,pair work , usually , ordinary , interactive
reflective	observation ,theory ,theorem ,challenges , alone work
sensing	Practically, in real world applications ,experimental data results
intuitive	Theoretically ,in principal
visual	Simulations ,Videos , graphs ,images ,charts ,figures
verbal	Forum ,discussion board ,text
Sequential	sequential ,outline ,first ,second ,flowchart, detail
global	Overall ,overview ,outlines , abstract, whole

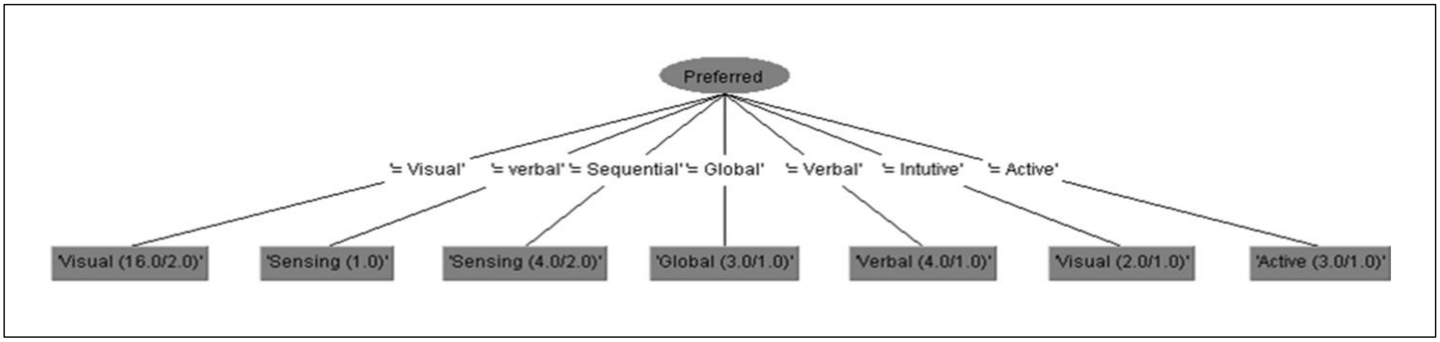


Fig. 4. Final Learning Style Classification Tree

During study session, learners from the training dataset were required to fill in the ILS questionnaire and the preferred learning style to explore self-study method in using e-learning system. They were also asked to take part in forum discussion and to acquire on-line quiz and on-line assessment. The material is introduced as power point presentations using powerful abstract and concrete learning materials. Animations, videos and simulations of some concepts can also be explored by the students. At the end of the tutorial, learners completed a self-assessment test, with the results being stored in the learner's profiles.

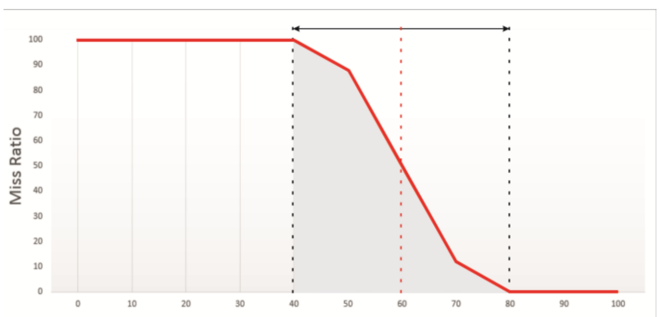


Fig. 5. Miss Ratio

VII. Results and Discussion

The ILS results, the number of correct answers as well as the learners' preferences in using the learning material have been analyzed. Table1 shows sample learner profile for these (FSLSM). Classifications were formed to determine learning styles for 90% learners from the training dataset. This way, the classifiers have been trained using 90% of the training data and evaluated their performance on the remaining 10%. Algorithms namely classification tree have been selected with pruning algorithms J48, NBtree, and Naïve Bayes Classifier. Finally 10-fold cross validation is used for every classifier. Since the amount of data available is limited, 10-folds validation reduces the variance of the estimated performance. Averaging over 10 different partitions makes the estimated performance is less sensitive to the partitioning of the data.

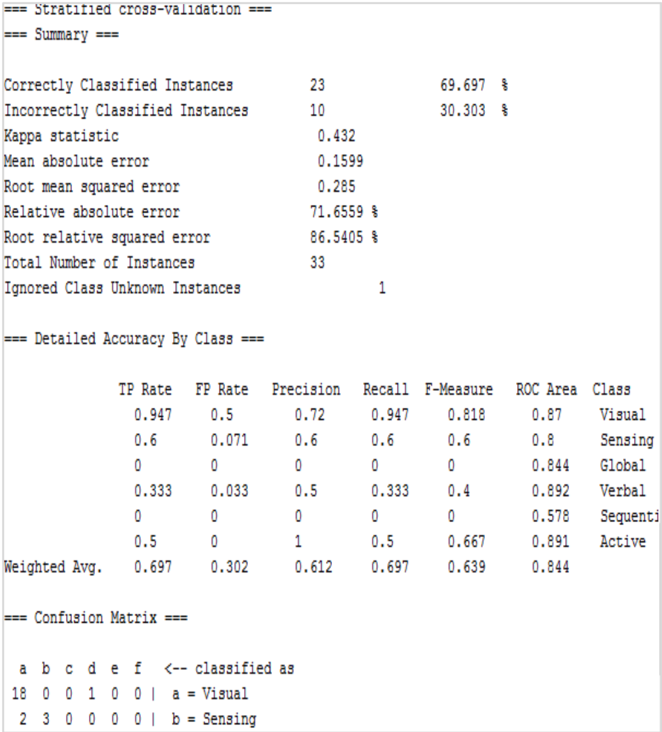
The experimental results are shown in table 3. It summarizes the results are recorded as correct and incorrect classified instances, Mean Absolut Error (MAE) and the weighted averages of True Positive rate (TP), False Positive rate (FP) and ROC area for each LS class. Mean Absolute Error (MAE) has been used to measure the accuracy of the final LS. MAE can be defined as the deviation between the predicted LS and the proposed LS which is derived from ILS (LS_{IN}) and preferred LS (LS_D). The smaller MAE value indicates that the LS prediction is closer to the proposed LS and has a high accuracy. Accuracy is also measured by the area under ROC curve. A Receiver Operating Characteristic (ROC), is a graphical plot showing the performance of a binary classifier with varying discrimination threshold. The curve plots the true positive rate against the false positive rate at various threshold settings. An area of 1 represents a perfect test; an area of 0.5 represents a worthless test. A snapshot of NBTree output is shown in figure 6.

TABLE III. Classification Accuracy and Training Errors

Algorithm	**Correctly Classified Instances (%)**	**Mean absolute error (%)**	**Weighted avg. TP**	**Weighted avg. FP**	**Weighted av. ROC**
J48	42.4242	0.2025	0.424	0.486	0.499
NBTree	69.697	0.1599	0.697	0.302	0.844
Naïve Bayes	69.697	0.1625	0.697	0.302	0.83

The final learning style classification can be seen by means of NBTree and NaiveBayes. It had an accuracy of 69.697%, with the value of MAE 0.1599 and 0.1625, respectively. Both classifiers had higher accuracy than J48. This percentage is expected to increase as the sample size increases. It is also discovered that the lowest error is found in NBTree, while the rest of the algorithms ranging around 0.1625 and 0.2025 error. The algorithm with lower error rate has more powerful classification capability, hence it is the preferred algorithm for use. Among these classifiers, NBTree has the highest weighted average ROC, 0.844. Figure 6 shows a snap shot of the NBTree classifier output and its area under ROC is shown in Figure 7.

Finally, evaluating the system, differences in self-assessment grades and material preference between learners' studies have been investigated with different learning style materials. Therefore, two plots illustrated for 12 students (match). The first represents the matching between Direct and Indirect learning styles for the self-assessment grades among the corresponding number of students (count) as shown in Figure 8. The second represents the matching between Direct and Final learning styles for each self- assessment grades along with the corresponding number of student (count) as shown in Figure 9.



```
=== Stratified cross-validation ===
=== Summary ===

Correctly Classified Instances          23               69.697 %
Incorrectly Classified Instances        10               30.303 %
Kappa statistic                          0.432
Mean absolute error                      0.1599
Root mean squared error                  0.285
Relative absolute error                 71.6559 %
Root relative squared error             86.5405 %
Total Number of Instances               33
Ignored Class Unknown Instances                  1

=== Detailed Accuracy By Class ===

               TP Rate   FP Rate   Precision   Recall  F-Measure   ROC Area  Class
                 0.947     0.5        0.72      0.947     0.818      0.87     Visual
                 0.6       0.071      0.6       0.6       0.6        0.8      Sensing
                 0         0          0         0         0          0.844    Global
                 0.333     0.033      0.5       0.333     0.4        0.892    Verbal
                 0         0          0         0         0          0.578    Sequenti
                 0.5       0          1         0.5       0.667      0.891    Active
Weighted Avg.    0.697     0.302      0.612     0.697     0.639      0.844

=== Confusion Matrix ===

  a  b  c  d  e  f   <-- classified as
 18  0  0  1  0  0 |  a = Visual
  2  3  0  0  0  0 |  b = Sensing
```

Fig. 6. NBtree Classifier Output

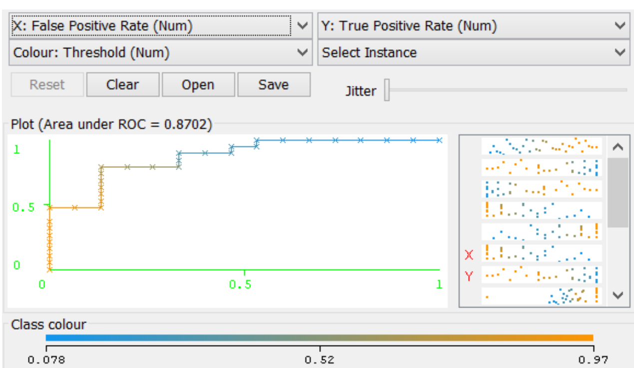


Fig. 7. Area under ROC

When the proposed LS is recommended to student then the direct LS would be more likely to match the final LS. Students' performance will be also improved as predicted by the classifiers (Figure 10). These have showed that incorporating learners' preference improves learner's performance.

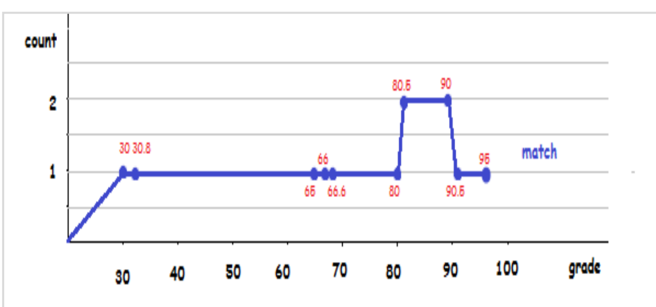


Fig. 8. Curve of Match Learning Styles between Direct and Indirect Styles

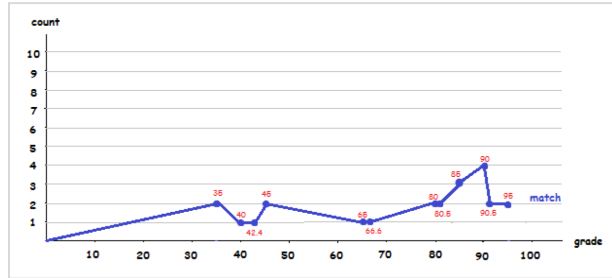


Fig. 9. Curve of Match Learning Styles between Direct and Final Styles

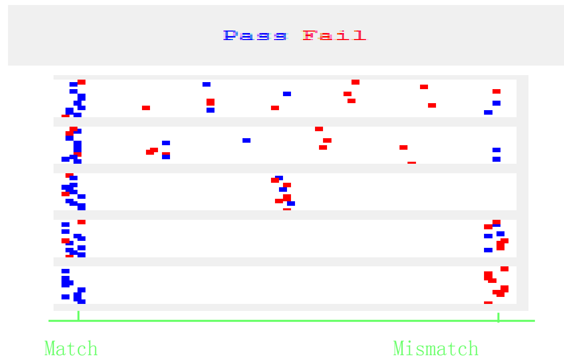


Fig. 10. Students Performance

VIII. Conclusion and Future Work

This paper introduced the effect of Learning Styles LS on learners in E-Learning environment based on proposed model created from FSLSM and the preferred learning style question to detect more accurate result than using only Felder-Silverman learning style model.

Experimental results showed that when taking into consideration the student's choice and including students' preferred learning style to the learning style detection method, students' performance could be increased by more than 12% as shown in Figure 10. The proposed approach had an accuracy of 69.697%, with the value of MAE 0.1599 and a weighted average ROC, 0.844. These results are expected to improve when increased the sample size.

Future work will extend this work by developing and providing adaptive modules for the online learning system. Modifying courses automatically, adding some learning objects, and/or some learning activities are some features which can be added in order to make system fits to students' learning styles. Furthermore, researchers would plan using advanced methods of student's pattern collection, such as students' navigation behavior in a learning system, patterns related to some other types of learning objects/activities, and so on. Also, apply the research model and architecture to other LMS is planned.

References

[1] C. Shih, J. Gamon, "Relationships Among Learning Strategies, Patterns, Styles and Achievement in Web-Based Courses," Journal of Agricultural Education, vol. 43, pp. 1-11, 2002.

[2] D. Kolb, Experiential learning: Experience as the source of learning and development: Prentice Hall, 1984.

[3] P. Honey , A. Mumford, The Manual of Learning Styles Maidenhead, 1986.

[4] R. M. Felder , L. Silverman, "Learning and Teaching Styles in Engineering Education," Engr. Education, 78(7), 674–681, 1988.

[5] C. Carver, R. Howard, W. Lane, "Addressing Different Learning Styles through Course Hypermedia," vol. 42, pp. 33–38, 1999.

[6] A. Franzoni, S. Assar, "Student Learning Styles Adaptation Method Based on Teaching Strategies and Electronic Media," Educational Technology & Society, vol. 12, 2009.

[7] L. NAJJAR, "Multimedia Information and Learning," Jl. of Educational Multimedia and Hypermedia, vol. 5, 1996.

[8] Y. Liao, "Effects of Hypermedia on Students' Achievement:A Meta-Analysis," JI. of Educational Multimedia and Hypermedia, vol. 8, 1999.

[9] R. Riding , S. Rayner, Cognitive styles and learning strategies: Understanding style differences in learning and behaviour: David Fulton Publishers, 1998.

[10] B. Soloman, R. Felder. (1993). Index of Learning Styles (ILS). Available: http://www4.ncsu.edu/unity/lockers/users/f/felder/public/ILSpage.html

[11] S. García, "An enhanced Bayesian model to detect students' learning styles inWeb-based courses," Journal of Computer Assisted Learning, vol. 14, pp. 305–315, 2008.

[12] G. Özpolat, "Automatic detection of learning styles for an e-learning system," Computers & Education, vol. 53, pp. 355–367, 2009.

[13] G. Ghorbani, "Learners Grouping in E-Learning Environment Using Evolutionary Fuzzy Clustering," International Journal of Information and Communication Technology, vol. 3, pp. 9-19, 2011.

[14] S. Graf, Kinshuk ; L. Tzu-Chien "Identifying Learning Styles in Learning Management Systems by Using Indications from Students' Behaviour," 2008.

[15] A. Dung, "An approach for detecting learning styles in learning management," presented at the International Conference on Education and Management Innovation, Singapore, 2012.

[16] De Bra, T. Santic, P. Brusilovsky ,"AHA! The adaptive hypermedia architecture," ACM, 2003.

[17] D. Sanders, J. Bergasa-Suso, "Inferring Learning Style from the Way Students Interact With a Computer User Interface," IEEE Transaction on Education, vol. 53, pp. 613-620, 2010.

[18] M. Khribi, M. Jemni, O. Nasraoui, "Automatic Recommendations for E-Learning Personalization Based on Web," 2009.

[19] K. Ghauth, N. Abdullah, "The Effect of Incorporating Good Learners' Ratings in e-Learning Contentbased Recommender System," Educational Technology & Society, vol. 14, pp. 248–257, 2011.

[20] N. Jyothi, K. Bhan , U. Mothukuri ,S. Jain, "A Recommender system assisting instructor in building learning path for," 2012.

[21] B. Vesin, M. Ivanović, Z. Budimac A. Klasnja-Milicevic, "E-Learning personalization based on hybrid recommendation strategy and learning style identification," Computers & Education, Elsevier Ltd, vol. 56, pp. 885-899, 2010.

[22] P. Dwivedi, , K. Bharadwaj, "Effective Trust-aware E-learning Recommender System based on Learning," Educational Technology & Society, vol. 16, pp. 201–216, 2013.

[23] "Weka 3: Data Mining Software in Java ", http://www.cs.waikato.ac.nz/ml/weka/

[24] T. Patil and S. Sherekar, "Performance analysis of naïve Bayes and J48 classification algorithm for data classification," International Journal of Computer Science and Applications, vol. 6, pp. 256-261, 2013.

[25] P. Pumpuang, A. Srivihok, P. Praneetpolgrang, "Comparisons of classifier algorithmss: Bayesian network, C4.5, decision forest and NBTree for course registration planning model of undergraduate students," IEEE International Conference on Systems, Man and Cubermetics (SMC), 2008.

Expansion of e-Commerce Coverage to Unreached Community by using Micro-Finance Infrastructure

Ashir Ahmed
Department of Advanced Information Technology
Kyushu University, Fukuoka, Japan

Takuzo Osugi
Institute for Academic Initiatives
Osaka University, Osaka, Japan

Kazi Mozaher Hossein
Department of Advanced Information Technology
Kyushu University, Fukuoka, Japan

Akira Fukuda
Department of Advanced Information Technology
Kyushu University, Fukuoka, Japan

Md. Asifur Rahman
Department of Advanced Information Technology
Kyushu University, Fukuoka, Japan

Hiroto Yasuura
Department of Advanced Information Technology
Kyushu University, Fukuoka, Japan

***Abstract*—Most people at the BOP (base of the economic pyramid, the largest but the poorest community in the world comprising 69% of world population) do not have access to e-commerce services. The way e-commerce is designed and practiced today does not enable their participation. The reasons are: their purchasing power is low, they do not have any means to make online payments, and there is no infrastructure to deliver the purchased items to their doors. To enable the participation of the people at BOP, we propose an e-commerce framework by engaging MFI resources and our recently developed ePassbook system. This paper shows how the BOP community can enjoy the benefits of the e-commerce service by using the proposed model. The advantages of making e-commerce available to the BOP are discussed, in addition to the challenges involved in implementing the model.**

Keywords—ICT; BoP; microfinance; E-commerce; social services; ePassbook

I. Introduction

E-commerce over the Internet has been in practice for more than a decade. E-commerce enables people to purchase products from a remote place at any time of the day and get the desired products delivered to their doors. It saves time, money and labor. A product seller can upload the product information on the web and can breach the boundaries of the local market to reach the customers on a global scale. A customer, on the other hand, can search for a desired product in a much more extensive selection space, and can find the suitable product. In this way, e-commerce brings benefits for both the buyers and sellers as indicated by the trend in e-sales. From 2006 to the second quarter of 2015, retail e-sales have increased at an average annual growth rate 35%, compared with 7.2% for the total retail sales in United States [1]. In order to purchase a product through a web-based e-commerce service, a customer needs access to the Internet and an online payment mechanism, typically a credit card. Presently 43% of world population has access to the Internet, however, 4 billion people from developing countries remain offline, representing 2/3 of the population [2]. Apparently, 16.42% people hold a credit card (this figure is assumed from the fact that 3.3 billion cards were issued globally and on an average each individual holds 3 credit cards). How about the remaining majority of the population? Do they not have any interest in participating and enjoying the benefits of e-commerce? These unreached are the 4 billion people at the BOP [3], comprising 69% of the world population shown in Fig.1. Despite their low income and limited purchase capacity, they make frequent purchases within their limited spending power [4]. According to [3], there is money at the BOP and their purchasing habits mean that they actually pay more for certain items than wealthier customers. This BoP penalty is the consequence of local monopolies, inadequate access, poor distribution and strong traditional intermediaries.

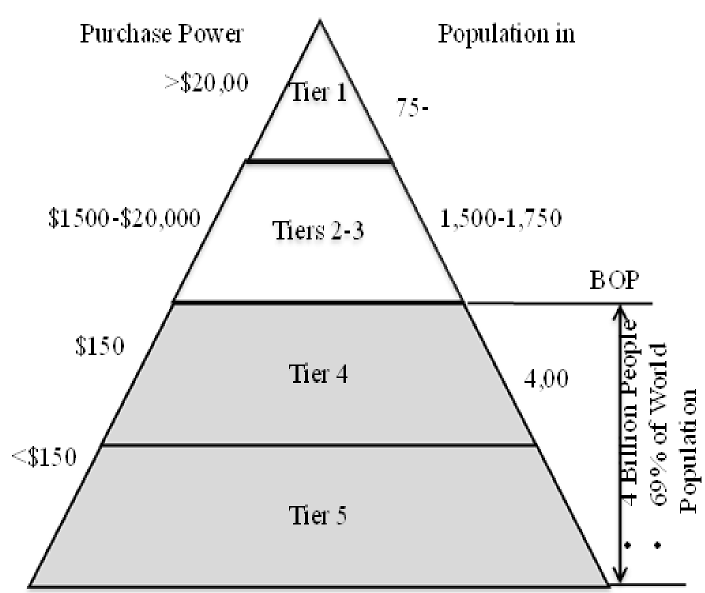


Fig. 1. Base of the Pyramid (BOP), the largest but the poorest community in the world

In this article, we introduce e-commerce system to this unreached community. Our model utilizes the MFI resources to act as an intermediary between the supplier and the consumer. In Bangladesh, around 20 million people representing BOP have access to micro-finance institutions (MFI) [7]. They carry out financial transactions in a regular basis with their associated MFIs. An MFI member not only borrows money from the MFI but also maintains a savings account. The accumulated savings of the 8.3 million Grameen Bank members is around 1.2 billion US dollars [8].

An MFI officer meets 300-500 members (clients of MFI) once a week. An MFI officer can compile a list of desired products from the members and a bulk purchase request can be handled on behalf of the members. It can be assumed that MFI officers have access to the Internet and know how to operate a computer. The members can withdraw their savings to purchase their daily needs such as soap, shampoo, rice, wheat, salt, and spices. They can receive the same product at a cheaper price through e-commerce. 8.3 million members in Grameen Bank alone have 30 million family members. If we consider soap as a product and one family consumes at least a piece of soap per month, 8 million pieces of soap per month will be the projected market size. An MFI like Grameen can make a business agreement with a soap producer ensuring 8 million soap purchases per month. The soap producer would find it viable to offer a different business plan for such a giant pre-paid customer. If we include other two MFIs in this service, 20 million soap bars can be sold in a month. In this way, MFI can offer an effective e-commerce service to its members.

Introducing e-commerce to the BOP, may affect the present non-e-commerce based businesses. The current business incentives also need to be considered. Selecting the products for the products for this system we need to carefully choose the products so that they do not affect the present business system but at the same time give a significant price advantage. At the consumer level a person at the BOP purchases the local produce like rice and lentils from the local market where a BoP penalty is rarely applicable. For consumers the list may contain edible oil, soap, sugar, salt etc. the items that is not produced locally and traditionally marketed from a central location. Our system would allow them to access the central supplier directly, eliminating the intermediary and increasing access to overcome the poor distribution problem. There are few other items that the consumers purchase seldom but the local retailers visits the wholesale market frequently. Keeping those items in the list would also allow the BoP people to purchase at a lower price at the time of necessity. The relevant items might be electrical items (bulbs, cables, sockets), traditional clothing (lungi, saree etc.). The list should also include seasonal items to address the demand when applicable. It is our intent to arrange the system in such a way that the gap between producer and consumer is reduced and an unnecessary intermediary disappear.

There are more advantages to including MFI in the BOP e-commerce model. In the present web-based e-commerce system, buyers do not feel comfortable sharing personal information and credit card information on the web. In MFI, the members have long credit relationship with the MFI officers. As the members meet their officer every week, they have some sort of trust relationship with the officer. The officer can collect the money from their savings and forward the money to the supplier of the product. If the seller is not a Grameen Bank member, the money can be sent to his bank account by using a third party bank.

The remainder of the paper is structured as follows: in section 2, we explain the present e-commerce system, the requirements and the limitations. We propose a model involving the MFI resources in Section 3. The advantages of the proposed model and the challenges are also discussed. Section 4 has the conclusion and the future works.

II. Present Web-Based e-Commerce System

A. Present E-Commerce

In a typical e-commerce scenario, a buyer visits a website. The website contains product information including the product stock status and the price. The buyer fills up a purchase order form which contains the list of items. Upon completing the purchase order form, the buyer is asked to make an online payment using some online payment system e.g. a credit card. The credit card details are communicated through a standard secured communication process. Once the payment process is complete, the list of ordered items is sent to the supplier along with the payment advice, the supplier delivers the purchased items accordingly. Fig.2 shows a typical e-commerce model. There are three major stakeholders in the present e-commerce system:

Buyer: is a person who buys a product. A buyer needs a means to find the product catalogue to select the product, a means to communicate with the seller to place the order and a method to make the payment. In a web-based e-commerce system, a buyer visits the product website, selects the product, makes the payment by credit card or other online transaction system. Upon confirming the payment, the supplier arranges for the product to be delivered to the address specified by the buyer.

In addition to online services, a buyer can also obtain product information through TV commercials or published catalogs and leaflets. The purchase order also can be processed by telephone, fax or postal order. The payment options are both prepaid and postpaid. Prepaid payment systems include credit cards and bank transfer. Some countries, such as Japan, have post-paid process where the money is collected when the product is delivered.

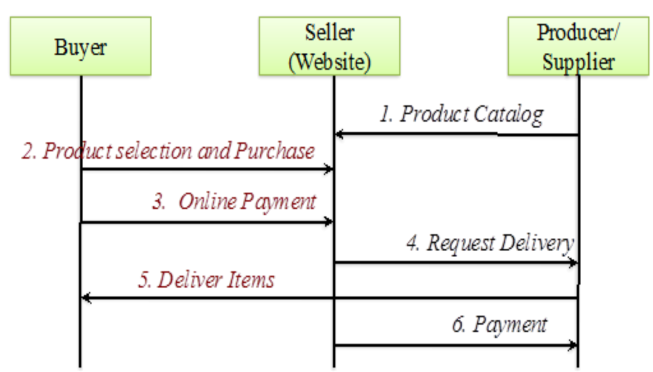


Fig. 2. Typical e-Commerce System Scenario

Seller: is a person who sells products. In a web-based system, a seller is a website that interfaces with buyers. Such a website offers a product catalog, an interactive interface to receive customers' preferences, a shopping cart system for the purchasing process and an online payment system. The website needs to ensure a secure system to handle customer information.

Supplier: receives purchase orders through the web and checks the payment process. A supplier needs store houses for the products. The storehouses can be either centralized or distributed. In order to minimize the delivery time, distributed suppliers can deliver the product from the closest distribution point. A supplier keeps the products in its possession and supplies them to the customers. A supplier can be a producer of the product, its representative, an agent or a distributor. A supplier also ensures the delivery of the product and post-sales services.

B. *Limitations of the Present E-Commerce System*

The present web-based e-commerce system brings enormous advantages to society. However, the participation of the BOP community is missing. A traditional business targets a consumer segment considering their purchasing power. The cost of maintaining the infrastructure and executing a delivery can be justified by a minimum transaction value. At the BOP, people's income is low and their purchasing power is limited. The purchase volume is not within the range to justify the overhead. Infrastructure support is also required for e-commerce. The following limitations kept the BOP community unreached and deprived them of the advantages of the e-commerce system.

1) Internet access: The BOP community usually does not have an affordable Internet access. As a result, online purchase orders cannot be made.

2) Electronic payment system: The BOP hardly has any means of electronic payment (credit card or PayPal account), nor do they have any communication infrastructure to support online payment facilities.

3) Lack of awareness of advance payment: The advantages of advance payment for products are not clear. BOP usually make face-to-face purchases and pay on the spot. Prepaid-based telephony services are popular because the charges are well defined and they consume product right away.

4) Home delivery: delivering a small supply to an individual address makes the delivery cost too high to justify.

5) Return handling: return of a small supply makes it difficult to plan an appropriate model. On the other hand, the BOP community would feel insecure bargaining with remote suppliers.

6) Post-sales customer service: providing post sale customer service to the BOP community is difficult because there is no communication infrastructure to support such a service.

III. E-COMMERCE USING MFI RESOURCES

In this section, first we describe how MFI structure and show how MFI resources can meet the requirements of e-commerce for the poor community. The advantages as well as the impact are also discussed.

A. *MFI Resources*

Microfinance institutions can be an excellent vehicle to provide e-commerce services to the BOP. MFIs have been successful in accessing the rural poor and introducing financial services to them. Fig.3 shows the operations and management system of Grameen Bank.

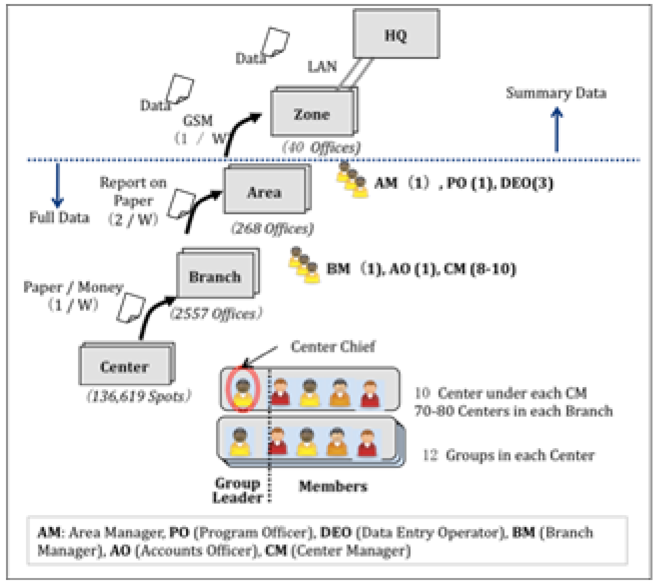


Fig. 3. Grameen Bank Operational Infrastructure

Like other Microfinance Institutions (MFIs), Grameen Bank provides financial services to poor people in the remotest parts of the country through a very efficient and closely monitored human network. In Grameen Bank, 8.3 million members throughout the country, are visited by 20,000 center managers once a week. A center manager has the socio-economic status of the affiliated members. These center managers deliver financial services (savings, loan, insurance, remittances etc.) to the members. The group solidarity and rapport of the MFI officer with the center members are the main driving forces behind successful operation of an MFI. A center manager belongs to a branch supervised by the branch manager. Branches are the main activity unit of any MFI which works on and maintains detailed data of the operations. Branches are closely monitored by mid-level managers at the area offices. These mid-level managers work on summary data aggregated from each branch. Top level managers in the headquarters and zonal offices manage the overall operation. This is how Grameen Bank's human network is connected.

MFI officers developed good relationships with the rural poor in terms of trust in financial transactions. In our previous work [5], we identified that MFIs have created a strong network among the BOP population.

Every 5 miles Bangladesh, there is an MFI office provided by at least one MFI: either by Grameen, BRAC or ASA. These three organizations serve more than 18 million members, through 75,000 field staff workers distributed among 8,000 branch offices in the country. An MFI officer visits 300-500 people per week. The network is an efficiently managed business with a yearly turnover of around 10 billion US dollars. The collective savings is also significant, at around 2 Billion US dollars. The relationship between the members and the MFI develops over decades. Most importantly, MFIs have detailed records of their members' credit worthiness. They also have moderate record of their transaction abilities over a period of time. Hence, it can be assumed that if we can use the harmony among the members of an MFI and access them through that MFI, a good business model can be generated. For example the daily consumption amount of edible oil is very low for one family. But collectively for 2000 members in a branch, the consumption amount is significant enough to make any supplier interested for business.

TABLE I. E-COMMERCE COMPONENTS AND MFI RESOURCES TO MEET THE REQUIREMENTS

Components	MFI resources
Access to Internet	The end user (MFI member) may not have access or skills to use the Internet. An MFI officer, on their behalf, accesses the product information for the client. A printed product catalog can be supplied to the members to mark the desired items. An MFI officer then can consolidate and submit the order through the web.
Electronic payment system	The eCash service provided by the ePassbook makes electronic payment possible. eCash is capable of handling payment from the cardholder's account to any other account within the same system.
Advance payment	Trust between the MFI and the members are leveraged to make this possible. The MFI would negotiate a good price discount for its members.
Home delivery	Individual delivery of small supply is expensive. MFI can use their meeting place for collecting purchased products where the MFI officer meets every week. The officer can also ensure safe product delivery.
Return handling	Return handling and warranty claims can be managed and negotiated by MFI officers. It gives the confidence to the MFI members of dealing with the suppliers.
Customer service	Customer services including return handling, complaints and other negotiation activities can be offered by the MFI.

In Section 2, we discussed the limitations of the present e-commerce systems. These limitations can be overcome if an MFI officer could be involved in e-commerce businesses. The advantages of involving an MFI officer in the system are:

a) Instead of a logical webpage, buyers can deal with a person to verify and get better understanding of product. Furthermore, they have the option to discuss with their peer group members. This also keeps a witness on the transaction. The trust level is significantly better than with a black box.

b) Buyers do not feel comfortable providing credit card information on the web. An MFI officer is trusted by the MFI members. Thus, members will feel more comfortable by being able to pre-pay for the e-commerce products. The peer witness also contributes to the creation of further trust.

c) Internet and credit cards used in today's e-commerce are not available to people in the BOP. Again, the concept of pay first and get the supply afterwards is not familiar to them. In our proposed model, the MFI officers are trusted since these officers oversee the members' monetary transactions every week. Thus, the MFI officer can work as a replacement for the website in traditional e-commerce. For secured order placement and payment, the MFI will use the ePassbook and related infrastructure.

B. ePassbook:

ePassbook is an electronic card developed by us for micro-finance members to maintain their financial records. The core component of this card is an IC chip which is common in other smart cards such as bankcards and employee cards. The developed ePassbook offers multiple services especially for the BOP, including microfinance, health, and e-cash. It keeps both MFI and health records. A user can view the records by using the display attached to the card. Traditional cards do not have this facility. ePassbook can transfer records by using the inbuilt RFID communication interface. An ePassbook reader is also developed for this purpose. An MFI officer with an "ePassbook reader" can communicate with the ePassbook device to update the bank transaction. A doctor in a hospital or clinic can access the health records. Now we want to use the same device for our proposed e-commerce framework.

C. E-Commerce with MFIs Involvement: The Proposed Model

Fig.5 explains the proposed system. The MFI members are the target consumers in this model. An MFI officer representing the consumers will play the role of intermediary. An established web platform for the villagers (gramweb.net) will contain the product information. The suppliers are selected based on their agreement with the MFIs.

1) The suppliers share their product catalog on a specified website. GramWeb [7] is a website containing village specific information. The local villagers own and maintain their village sites. Therefore, it will be effective for the suppliers to distribute village-specific catalogs considering their needs. As not all villagers have access to the Internet, these unreached people will not be able to view an online product catalog. The MFI officer can fill the gap.

2) An MFI officer will have an updated printed catalog to share with the MFI members. The catalog will be villager-friendly so that low-literate villagers can easily understand and use it for placing orders.

3) The consumers will select products from the catalog and put the order in a pre-printed form. An MFI officer meets 300-500 people per week. This is the customer segment that one MFI officer can cover per week.

4) An MFI member holds an ePassbook. The ePassbook will allow the MFI members to use their savings money to pay to a third party through the MFI headquarter. The MFI officer transfers the order value from the member's savings account to a special e-commerce account in the branch and records the transaction ID on the order form.

5) The MFI officer collects all the individual orders and enters them in the website on behalf of the members. The MFI officer needs to be properly authenticated by GramWeb.

6) GramWeb then proceeds with a delivery request to the supplier.

7) The supplier delivers the products to the place where MFI members meet the MFI officer. In Grameen, the place is called a center office.

8) The MFI officer then processes the final payment to the supplier.

Fig. 5. ePassbook for micro-finance borrowers

In this way, e-commerce services can be reached to the unreached, the largest socio-economic group in the world.

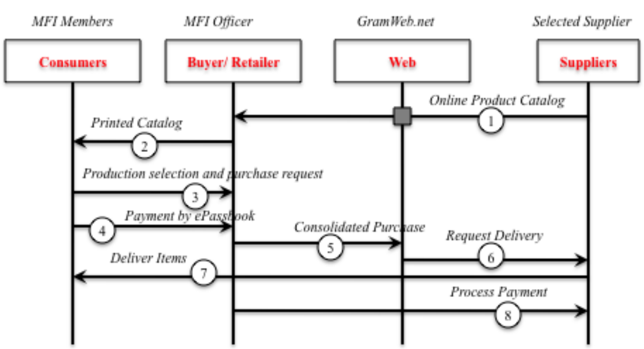


Fig. 4. eCommerce Model for BoP consumers using MFI Resources

D. Advantages

The proposed model brings the following benefits to its stakeholders-

A. Villagers: The villagers include the MFI members, local retailers and other villagers. By utilizing the proposed scheme, villagers can purchase reliable branded products at a cheaper price. Local retailers might seem to lose their business if MFI starts doing this business. However, they can also use this channel to purchase items directly from producers at a lower cost. Usually these retailers go to the wholesale shops individually which involves transportation costs and time. The proposed model offers a single trip for all necessary products. The transportation costs and time will be significantly minimized [Fig. 6].

B. The MFI: e-commerce will be a value added service for the MFI. Other benefits include: (a) Increased trust/loyalty from the members, (b) More savings from the members (c) Financial benefit from the advanced payment by the members (d) Wider transaction record (e) Additional line of revenue

C. Researchers: It is possible to archive the list of purchased items. The archive can be a good resource for analyzing and determining BOP purchase pattern, food behavior, and nutrition facts. Predictions about the future market can also be made.

D. Suppliers: Having a contract with giant a microfinance institution with millions of customers will provide an effective business opportunity. Analyzing the business trend, suppliers will be able to handle a larger market with reduced effort in an organized way.

E. Producers: The producer will receive first hand and regular consumer feedback. It will be possible to develop new products to meet the specific demands of the BOP. This will also help reduce copies, fakes and other undesirable items being peddled to the BOP market.

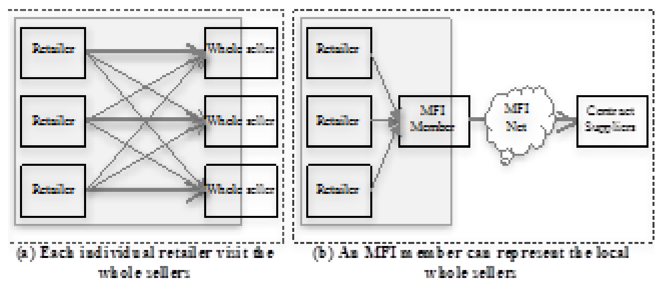


Fig. 6. Transportation cost saving for the individual retailers

E. Scope and Challenges

The objective of the proposed system is to introduce e-commerce services to the unreached community. To deliver the service, the proposed system places MFI officers at the center point of service delivery. Therefore, any person who is a member of an MFI is within the scope of this service model. Products to be handled in this system are selected according to the following features: (a) *Familiarity of the product*: Especially the branded items with the price tagged (b) *Transportability*: Products that are neither fragile nor perishable, and (c) *Affordability*: The optimum size of the product in an affordable range.

The proposed system will face following challenges:

(a) Business of the existing retailers: Presently, the retail business is channeled by two to three tiers of distributors. A large number of retailers are spread over the country. The new model of business would reduce their market share significantly, especially when we consider Bangladesh where every family in the BOP is attached to at least one MFI.

(b) Postpaid vs. prepaid: Uncertainty of income is a major problem for BOP people [8]. Hence they maintain a credit line with retailers. To address this problem, we propose that MFI can introduce a suitable loan product analyzing the members' credit and repayment history. The MFI would ensure a good bargain from the supplier, which would act as an incentive for advance payment.

(c) Home delivery: Home delivery might be a problem in low density, remote, and hard to reach parts of the country. Where residents used to walk or ride on small country boat to travel the long distance to the market place for the purchase of consumables.

IV. Conclusion and Future Works

Access to product information, online payment mechanism and product delivery channel are the major components to provide e-commerce services. Developing the necessary infrastructure can be a way to allow 4 billion people at the BOP to enjoy e-commerce benefits but it may take decades to make this happen. We proposed an alternative solution of using Microfinance resources and the ePassbook we have developed. MFI officers visit their clients once a week and have strong financial trust. The ePassbook allows a borrower to transfer money electronically. The proposed model brings benefits to all stakeholders. The first hand benefit goes to the villagers who have been deprived of e-commerce service. The microfinance industries will be able to keep more savings in hand. The suppliers can benefit from bulk orders from the microfinance institutions. The producers will be able to reach the unreached with their products. This will also open a new window for researchers to analyze the market trends and consumption patterns, including issues related to health. A concern remains about how the introduction of e-commerce through MFI in the BOP community will affect the local retailers.

Acknowledgment

This work has been supported by Kyushu University Research Superstar Program (SSP), Special Coordination Funds for Promoting Science and Technology, originating from the Ministry of Education, Culture, Sports, Science and Technology (MEXT), Japan.

References

[1] U.S. Census Bureau News, U.S. Department of Commerce, Washington, D.C. 20233, August 17, 2015

[2] ICT facts and figures, the world in 2015, ICT Data and Statistics Division, Telecommunication Development Bureau, International Telecommunication Union, Geneva, May 2015

[3] CK Prahlad, 2004. "The Fortune at the Bottom of the pyramid". Watson school Publishing, New Jersey, USA

[4] SMS Zabir, A Ahmed, H. Yasuura, "Digital Divided: The Amazing Fact at the BOP", Proceedings, IADIS International Conference ICT, Society and Human Beings (MCCSIS 2008), IADIS Press, July 2008

[5] Asifur Rahman, Ashir Ahmed, Osugi, Takuzou, "Key challenges to the expansion of micro finance institutions in Bangladesh: Case studies on Grameen, ASA, BRAC", Bulletin of Kyushu University Asia Center Vol. 4 March 2101, Page 85-93

[6] Yunus, Muhammad (1999). "Banker to the Poor (First ed.)". PublicAffairs Publishing, New York City, USA

[7] Ashir Ahmed, "An information production and ownership platform for BoPers", Proceedings. IADIS International Conference ICT, Society and Human Beings (MCCSIS 2009), IADIS Press, June 2009, pp. 147-154, ISBN: 978-972-8924-82-9

[8] Darly Collins, Jonathon Morduch, Stuart Rutherford, Orlanda Ruthven, 2009. "Portfolios of the Poor". Princeton University Press, New Jersey, USA

Modelling for Forest Fire Evolution Based on the Energy Accumulation and Release

Fan Yang
College of Computer
Hubei University of Education
Wuhan, China

Qing Yang *, Xingxing Liu
School of Management
Wuhan University of Technology
Wuhan, China

Pan Wang*
Institute of Systems Science and Engineering
Wuhan University of Technology
Wuhan, China

***Abstract*—Forest fire evolution plays an important role in the decision-making of controlling the forest fire. This paper aims to simulate the dynamics of the forest fire spread using a cellular automaton approach. Having analyzed the characteristics and evolution of forest fires, a simulation model for the forest fire evolution based on the energy accumulation and release is proposed. And, taking Australia's catastrophic forest fire in 2009 as an example, the fire's evolution closely to the reality is simulated. The results of the experiments are shown that if forest energy is released in a small scale before or during the fire, the fire would be better controlled even if it does not occur. Improving the efficiency of the fire extinguishing procedures and reducing the speed of the fire spread are also effective for controlling the forest fire.**

Keywords*—*forest fire evolution; energy accumulation and release; cellular automaton (CA); simulation

I. Introduction

This Development over the millennia have left the world in a grave state and it faces both complex and greater contemporary challenges. Therefore forest fire management is a subject that is worthy of investigation. A forest fire system is complicated and involves nature, society and economic development. Research on forest fire control mainly focuses upon forest fire evolution models and risk reduction following disaster.

The classical evolution model of forest fires proposed by Drossel and Scwhabl，is a type of cellular automata (CA) model, which simulates the growth of trees, the occurrence and extension of the fire and other processes with certain rules [1]. Based on the classical model, other more specific CA models [2-6] that have been introduced mostly change the system's conditions, such as the immune forest fire model [2], the limited scale effects of forest fires model [4], the integer type of forest fire model [5] and the heterogeneity of forest fire model [6].

Encinas et al. [7] proposed a hexagonal CA model for the forest fire evolution and discussed the impact of this six-edged structure on the forest fires spreading. Having considered the geological characteristics and hazard factors of fires, Yassemia et al. [8] proposed an integrated GIS-based CA model. Berjak et al. [9] presented a CA model that is capable of predicting the fire's spread in spatially heterogeneous Savanna systems. The physical basis of Rothermel's fire spread model (1972) was modified to a spatial context and used to improve the CA model introduced by Karafyllidis and Thanailakis (1997). Alexandridis et al. [10] presented and illustrated the simulation results of a CA model, thereby describing the dynamics of the spread of a forest fire on a mountainous landscape; having taken into account factors such as the type and density of vegetation, the wind speed and direction and how quickly the fire is spotted. Hui et al. [11] proposed a multi-state probability CA model of forest fires, which analyzed changes in the occupancy of forest trees under two sets of conditions; one being that they exist in spaces with no growth and are not susceptible to fires, the other being that the trees differ from their neighborhood due to deforestation. Through the improvement of CA probability, it is possible to stimulate the occurrence mechanism of forest fires. Subsequently conclusions were drawn that the correct type of spacing between trees and modest felling can prevent the spread of fires and realize effective tree growth.

In order to study the whole developing tendency and the evolvement rules of the forest fire system, Guangjun and Yaodong [12] introduced a pattern-oriented model based on an agent and proposed an agent-based forest fire simulating model. Furthermore their computer simulation was implemented by integrating the harmonizing nature and microscopic mechanism of society. Qinggui et al. [13] put forward a simple model of forest fires based on the power distribution of forest fire models, which can effectively reveal its self-organized criticality. A "frequency-scale" distribution is obtained by a numerical stimulation and the model satisfies the limited size effects. The changes of the average burned area are provided by adjusting the control parameters. The authors discuss the differences in "frequency-scale" distribution between their model and the original one, after the introduction of heterogeneity and wind factors. The results from their model that show how to control forest fires provide a good verification of their proposal.

In summary, the existing research lacks a discussion of the energy of forests. In order to understand the evolution of the forest fire and propose related methods for its management, a new evolution model is presented in this paper based on energy accumulation and release. The energy accumulation of forests is inevitable, and experiments show that the energy released in a suitable time and by a suitable release ratio could clearly reduce the frequency of forest fires occurrence. The controlling of forest fires could be realized following repeated practical tests to establish the optimal energy release time and ratio.

*Corresponding authors..

II. THE CHARACTERISTICS OF FOREST FIRES AND MODEL FACTORS

The common features of forest fires are continuous high temperatures and excessively strong winds that lead to the outbreak site of fire becoming out of control in a shorter time period, and eventually lead to large-scale fires in a large stricken area and the rapid spread of a fire, which can last for a few days or up to a month. Thus, the key elements of forest fires are taken as the important parameters for the model. The analogy between the features of forest fires and the model parameters is shown in Table 1.

TABLE I. THE CHARACTERISTICS OF FOREST FIRES AND THE MODEL PARAMETERS

Real-world	Modeling system
The forest area	The system space *M*
The number of fire points	Number *W*
Environmental factors: degree of drought and wind speed	The speed of the energy accumulation and the transfer rate
Trees in one unit (the affected unit)	Agent A_i
A state of the affected unit (latency, burning, extinguishing, overburning)	A state of the agents
The longest sunshine duration	The length $L_{(A)}$ of the agent gene $N_{(A)}$
The sunshine duration of an affected unit (sunlight exposure brings about the energy accumulation)	Latent period *q* of A_i
Time between the beginning and the end of the forest fire in an affected unit	Burning period of A_i
The burning speed of an affected unit	Changes in positional value of $N_{(A)}$
The fire spreading speed of an affected unit	Spreading speed *m* of A_i
The burning units	Total R_t of burning agents
Controlling measures for the forest fire	The algorithm of controlling agents
The efficiency of the fire extinguishing procedures	The efficiency of the fire extinguishing p_m

Moreover, the evolution of individuals will lead to demands for the state changes of the system. The status that might be produced during the evolution of the modeling system resembles real-world events. A detailed description is shown in Table 2.

TABLE II. AN ANALYSIS OF STATE OF THE FOREST FIRE

The state of the forest fire	Description in the model
Beginning time	Time the evolution begins (t=0)
Explosion point	Number of burning agents coming to a peak ($t=t_p$)
Expanding period	Period from t=0 to $t=t_p$
Declining period	Period from explosion to stability of the system
Vanishing period	Recovery to the stable situation

III. EVOLUTION MODEL

According to the above analysis, the model is built based on CA algorithm. Assume that each two-dimensional cell stands for a unit of a forest where there are a variety of trees; moreover there is a random distribution of the energy value and the energy is accumulating over time. From the perspective of energy, treating energy accumulation as the general term of tree growth, the accumulation of leaves, persistent drought and other factors, are all closer to reality than simply considering planting trees in a blank space. Additionally, the aim of this model is not to predict a fire but to simulate its evolution and search for controlling measures. Furthermore, assume that the number of fire points is known, and the probability that the trees catch fire is determined by the energy accumulation and the degree of the combustion of the surrounding trees. The extinguishing efficiency (p_m) , fire spreading speed (m) and other parameters, as well as the embedded energy release strategy algorithms, could all influence the simulation of the evolution of forest fires. The computational experimental process is shown in Figure1.

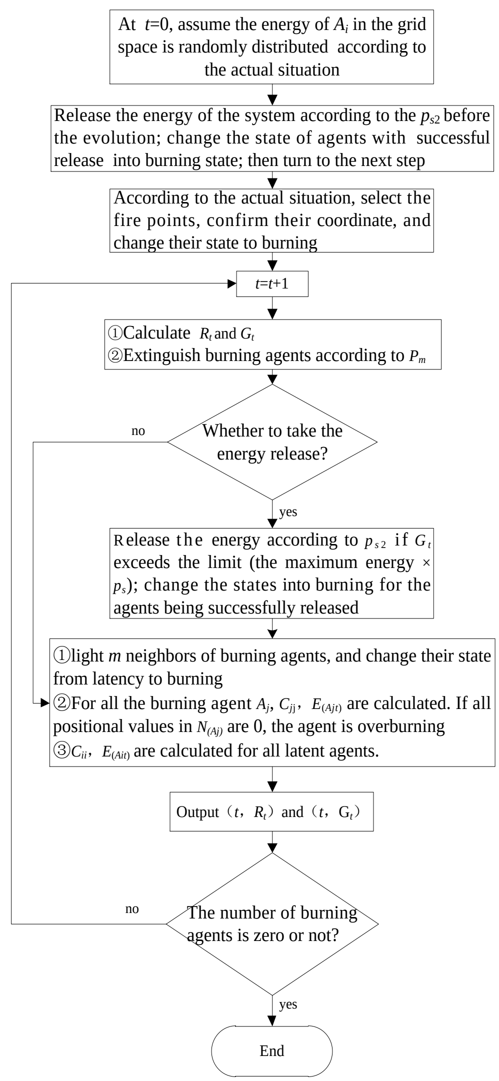


Fig. 1. The computational experimental process

A. A description of the agents

The different agents used in this model can be seen in Table 3.

TABLE III. THE AGENTS MAPPING TABLE OF THE FOREST FIRE SYSTEM AND THE MODEL SYSTEM

Forest fire system	Simulation system	Parameter explanation	Interaction
Fire environment	Environment agent	Systematic space M, systematic original state, agent neighbors	Providing space for agents to interact
Combustible trees per unit	Agent A_i	Evolution state$_{(A)}$, evolution period $N_{(A)}$, energy $E_{(A)}$, latent period q, the total burning time, the length $L_{(A)}$ of gene $N_{(A)}$.	Spreading speed m and the efficiency of the fire extinguishing p_m
Supervising institution	Observer agent	A systematic combustion value(the total of the burning agents) curve, a systematic energy curve, a control panel	Display of observed numbers, control of systematic speed
Evolution of the forest fire	Model agent	Evolution rule (C_{ii}, C_{jj}) of latent agent A_i and burning agent A_j, systematic evolution period, systematic burning number, systematic total energy	Interaction model of agents, model of accumulated energy, observed model of burning number

Subsequently, the simulation algorithm follows the rules of the systematic evolution in this model. In this way the CA itself will transfer energy to simulate the process of the outbreak of a fire.

Assume that A_i not only transfers energy but can also be transferred. Thus the adjacent agents' energy in the process of being transferred is gradually activated; moreover the total energy of the system would also gradually accumulate. A_i represents the affected unit of the forest, as described in Table 4.

TABLE IV. A COMPARISON OF THE AFFECTED UNIT AND THE AGENT

	State	The period of evolution	Interactions
Agent A_i	The state of the agent	Length of gene	Burning agents are transitive. The latent agents' energy accumulates every cycle automatically
The affected unit	Latency, burning, extinguishing, overburning	The maximum time of the latency of trees	The burning unit is transitive, triggering fire in neighboring forest units

B. The composition of the system

Suppose the system is a two-dimensional grid space. The coordinate of agent A_i is （x_i, y_i）， i=1, 2,…, M， where M is the sum of agents in the system. One and only one A is put into in each grid space unit. The original state（t = 0）refers to the fact that several random agents are in a state of burning (or some specific burning points are selected according to the actual situation), but other agents are in a latent state. The energy of agents is distributed randomly or is submitted to a certain distribution pattern according to actual situation.

C. The state parameter

A_i is the dynamic subsystem with a certain energy, whose state parameters include gene $N_{(Ai)}$ and the current state $state_{(Ai)}$. $N_{(Ai)}$ is composed of the binary numbers of a specific length ($L_{(A)}$). Its positional value 0 and 1 indicate the stability and disorder respectively, and the form of $N_{(Ai)}$ is as follows:

$$N_{(Ai)}=\begin{cases} 11100\ldots\ldots 000\ (q=3) & \text{latency, burning or extinguishing (state = 1 or 2 or 3)} \\ 11111\ldots\ldots 111\ (q=L_{(A)}) & \text{the maximal latency (state=1)} \\ 00000\ldots\ldots 000\ (q=0) & \text{overburning (state=4)} \end{cases} \quad (1)$$

In the formula above, the latent state of agents means that there is a state where energy is accumulating before burning; the agent in an extinguishing or overburning state should discontinue its evolution; and the positional value could be from 1 to 0, or 0 to 1. The former change means the agent is burning and the energy is declining; whereas the latter one means the agent is accumulating energy.

D. The rules of evolution

1) The energy accumulation and evolution rule

The self-evolution rule of all latent agents is that the number of 1 in $N_{(Ai)}$ adds k until all the position values are changed into 1.

$$C_{ii}=k \text{ positions change from 0 to 1 to the right in } N_{(Ai)}, \quad \text{if state}_{(Ai)} = 1 \quad (2)$$

2) Lighting rule

Burning agents could lead to their m latent neighbors catching fire. Furthermore, the state of the agents catching fire could change from latency to burning. The value of m is decided by the speed of fire spreading; the faster the fire spreads, the higher the m is.

3) Self-evolution rule

The self-evolution rule of A_j in a burning state is as follows: the number of 1 in $N_{(Aj)}$ subtracts k_2 until all positional values are 0. Then the state could be changed from burning to overburning, in which the state evolution discontinues.

$$C_{jj}= k_2 \text{ positions change from 0 to 1 to the left in } N_{(Ai)}, \quad \text{if state } A_j=2 \quad (3)$$

E. The efficiency of the fire extinguishing process

In the t-th cycle, the burning agents could be extinguished by the efficiency of the fire extinguishing p_m; its state changes from burning to extinguished. The agent evolution no longer occurs if the agent has been extinguished.

F. The observing value indicators of the evolution

At the *t*-th cycle (t ∈ [0, T]), assume R_t is the total of the burning agents, and G_t is the cumulative total energy of the system.

For agent A_i, assume $E_{(Ai)}$ is the current energy, which is determined by the number of 1 in $N_{(Ai)}$ at the *t*-th cycle. The formula of $E_{(Ai)}$ is shown below.

$$E_{(A_{it})} = 0.1\sum_{k=1}^{L_{(A)}} n_{ik}, n_{ik} = 0 \text{ or } 1 \tag{4}$$

n_{ik} means the positional value in $N_{(Ai)}$; and $L_{(A)}$ is the length of the agent gene $N_{(A)}$. When the state of A_i is burnt out, its energy is minimum and therefore zero; when A_i is at its maximum latency stage, its energy is the maximum for 0.1 $L_{(A)}$.

The total energy of the system at the *t*-th cycle is as follows:

$$G_t = \sum_{i=1}^{M_t} E_{(A_{it})} = 0.1\sum_{i=1}^{M_t}\sum_{k=1}^{L_{(A)}} n_{ik} \tag{5}$$

M_t is the number of agents that have energy at the *t*-th cycle. $M_t \leq M$.

IV. The Energy Release Algorithm

A lot of internal energy (including dry leaves, branches, and weeds) has accumulated within the forest system. If the initiative is taken in a planned manner to fell, lop, clean, set fire (and control the size of this fire), the internal energy in the forest system will be effectively released, and there may be no serious forest fires.

Embedded the energy release algorithm in the basic forest fire model, we can analyze its effect on management. If G_t and the maximum internal energy meets or exceeds the energy limit value (the limit ratio is p_s), the system begin to release some energy from the latent and extinguished agents in accordance with probability ps_2.

The related parameters are shown in Table 5.

TABLE V. The Related Parameters

parameters	meaning
R_t	the total number of burning agents
G_t	the cumulative total energy of the system
p_m	the efficiency of extinguishing procedures
v	the change rate of p_m
m	the spreading speed
p_s	the energy limit value ratio
p_{s2}	the energy release ratio

V. A Simulation Analysis

The simulation could be implemented after the model and the related parameters setting are completed. In this section, we analysis four kinds of simulations.

A. Case simulation

The case simulation takes the huge forest fire in Australia in 2009 as the prototype. This fire lasted for 35 days from February 7, 2009 to the end of March 14, 2009 and led to an area of 410000 hectares being burned. There were three fire points on February 7th after nearly a month of hot and dry days; furthermore following the outbreak, the local wind speed reached 96~115 km / h.

The setting of parameters refers to the case above; assume that it takes one day of actual time for the models to run a cycle, and the system space of model is M = 100 × 100. Due to nearly a month of hot and dry days, the amount of energy becomes larger, set q = 26, $L_{(A)}$ = 40, and the maximum energy = 0.1 × 40 × 10000 = 40000. The number of burning points is set up as the actual value w = 3; and considering that the actual fire spreads quickly, subsequently the spreading speed is set up at a larger value m = 24. According to a repeated trial, the extinguishing efficiency is set as p_m ∈ (0,0.5), and the change rate v increases by 0.0125 every cycle.

The simulation results are shown in Figure 2.

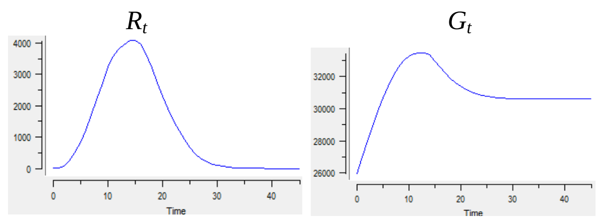


Fig. 2. The simulation results of the Australian large forest fire

The simulation result shows that R_t at the explosion point is 4094. If one grid represents 100 hectares, it can be converted into a burned area of 4094 × 100 = 40.94 million hectares, which is quite close to actual 410,000 hectares. Seen from the evolutionary cycle perspective, 39 cycles when R_t equals zero is close to the actual duration of the fire, which was 35 days. The model could restore the evolution of the fire to a higher degree.

From an analysis of the energy, it could have been as high as 26,000 at the start point, which takes up 26000 ÷ 40000, or 65% of the maximum energy; additionally the maximum energy in the evolution is up to 32,986, and 30,614 residual units of energy remained after the fire went out. Excessive energy can eventually lead to the primary cause of a large forest fire's outbreak. Since the remaining energy is higher than the initial energy, it may still lead to large forest fires later on.

B. A simulation for increasing the extinguishing efficiency

When the efficiency of extinguishing a fire is at a low level, the fire cannot be controlled effectively because of its high spread rate. A series of experiments are completed for increasing the extinguishing efficiency to v>0.0125. The evolution results are shown in Figures 3 and 4 when v=0.02 and v=0.1.

The results of the calculative experiments show that when the rate is up to v=0.02, R_t at the explosion point drops from 4094 to 2194, which is a decrease of 46.41%. Moreover, the duration of the fire is shortened from 39 to 35 days, which is a decrease of 10.26%. The highest energy of the evolution rose slightly to 35754, and the remaining energy rose to 33988.1; therefore the residual risk of fire would be higher.

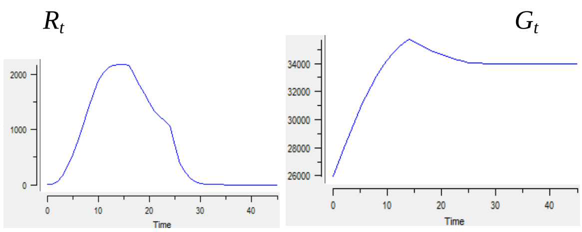


Fig. 3. A higher efficiency for extinguishing the fire (v=0.02)

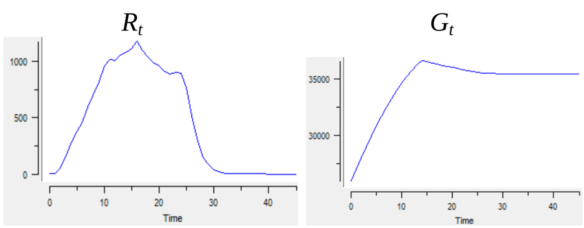


Fig. 4. A higher efficiency for extinguishing the fire (v=0.1)

When the efficiency of the fire extinguishing procedures are substantially improved to v=0.1, R_t at the explosion point would drop to 1185, a decrease of 71.06%, and the duration of fire would increase to 40 days. The highest energy of the evolution continues to rise to 36651.6, and the remaining energy further increases to 35464.3.

Thus, increasing the efficiency of the fire extinguishing procedures can decrease R_t greatly, but has no obvious effect on the duration of fire; and the duration would be extended if the efficiency of the fire extinguishing is excessively improved. Furthermore, increasing the efficiency of the fire extinguishing procedures will increase G_t and the remaining energy; this would perhaps increase the follow-up risks.

C. Reducing the speed of the fire spreading

A series of experiments are implemented by reducing the speed of the fire spreading when m<24, as another very important factor affecting the size of the fire is its spreading rate. Catastrophic fire is often accompanied by strong winds, resulting in a low efficiency of fire extinguishment, and meaning that the fire cannot be effectively controlled. If the speed of the fire spreading is reduced, the evolution of the results is shown in Figures 5 to 7.

Compared with Figure 2, Figure 5 shows that if *m* drops slightly from 24 to 20, R_t at the explosion point also drops. The evolution of the maximum energy value is slightly increased, whereas the overall value differs little. However, the evolution results in Figures 6 and 7 show that if the efficiency of the fire extinguishing procedures remains unchanged, reducing the speed of the fire spreading can effectively reduce R_t and increase the duration of the fire. Subsequently both the maximum energy and the energy remaining after the evolution could be increased.

Thus, R_t is decreased greatly, which increases the efficiency of the fire extinguishing procedures; however it has no obvious effect on the duration of the fire, which would be extended if it was excessively improved. Therefore improving the efficiency of the fire extinguishing procedures would increase G_t and the remaining energy, but this might increase the follow-up risks.

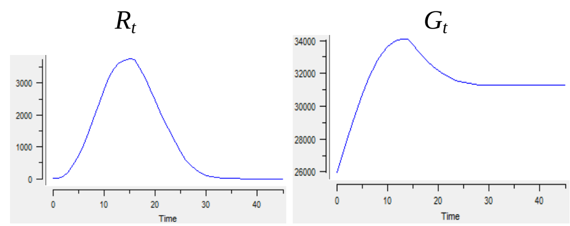


Fig. 5. Reducing the fire spreading speed (m=20)

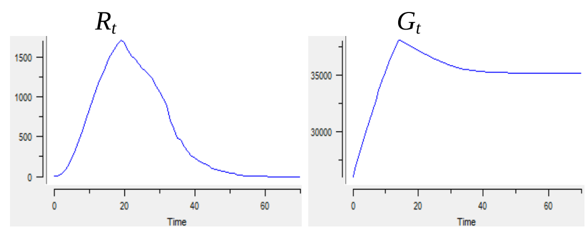


Fig. 6. Reducing the fire spreading speed (m=8)

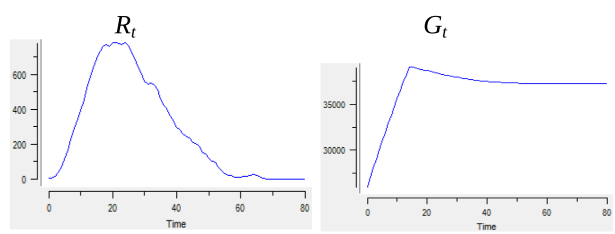


Fig. 7. Reducing the fire spreading speed (m=4)

D. The energy release model

The release of energy can be implemented before the forest fire occurs. Relevant activities would include as cutting down or pruning the trees that are too dense and clearing up the withered branches. Related measures may also be implemented after the fire, such as cutting down part of the forest zone which has not been affected by the fire to set up an isolation strip so as to control the fire.

1) Release the energy before the evolution

If the releasing ratio is 10%, it is known from figure 2 that the initial energy is 26000 × (1-10%) = 23400, and 58.5% (23400 ÷ 40000) of the maximum energy. The results of this evolution are shown in Figure 8.

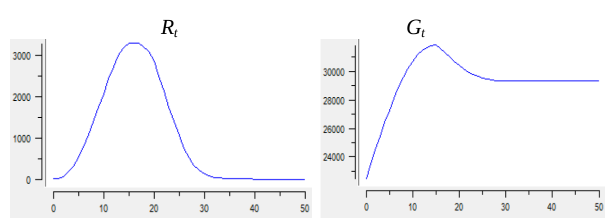


Fig. 8. Releasing 10% of the energy

Results show that R_t at the explosion point drops from 4094 to 3288, thereby reducing by 19.69%; moreover the fire duration is slightly extended from 39 days to 40 days.

If a huge amount of energy is released, the releasing ratio is set for 40%. Then the initial energy is 26000 × (1-40%) = 15600, and 39% (15600 ÷ 40000) of the maximum energy. The results of this evolution are shown in Figure 9.

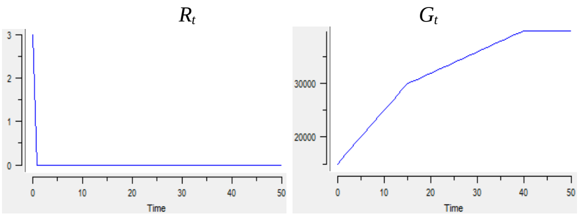


Fig. 9. Releasing 40% of the energy

From the calculation results in Figure 9, there is no outbreak of fire, and the R_t set at the first cycle quickly changes from three to zero. Additionally, after a series of computational experiments, the energy of the pre-release ratio is less than 40%, which could lead to a fire. When the ratio is 39%, the results of the evolution are shown in Figure 10.

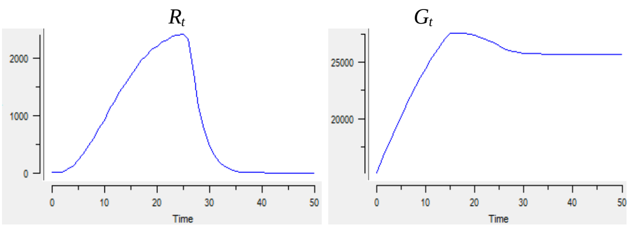


Fig. 10. Releasing 39% of the energy

When the releasing ratio is 39%, R_t at the explosion point drops from 4094 to 2429, a reduction of 19.69%; moreover the fire duration is slightly extended from 39 days to 40 days.

The above experiments show that the higher the proportions of energy released before the evolution, the more obvious the result.

2) Release the energy during the evolution

In this case the initial energy is as high as 26,000, accounting for 65% (26000 ÷ 40000) of the maximum energy. In order to control the fire effectively, the energy must be first released. Because p_s can only decide when to terminate the release and to re-release the energy, it cannot be too small; furthermore p_{s2} is the energy ratio for each release, and it cannot be too large. Thus $p_s \in [0.4, 0.65]$, $p_{s2} \in [0.1, 0.5]$ is set for a series of experiments. Some of the experimental results are shown in Figures 11 to 16; whereas all of the results are shown in Table 6.

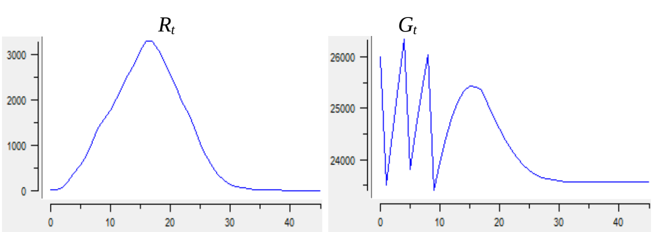


Fig. 11. Releasing the energy (ps =0.65，ps2=0.1)

R_t G_t

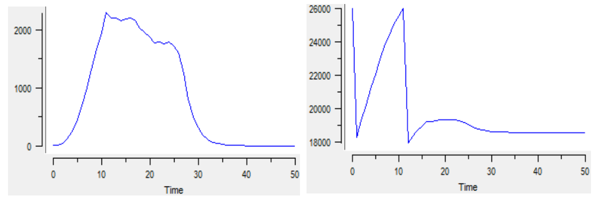


Fig. 12. Releasing the energy (ps =0.65，ps2=0.31)

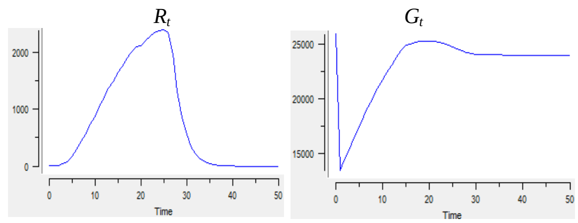


Fig. 13. Releasing the energy (ps =0.65，ps2=0.5)

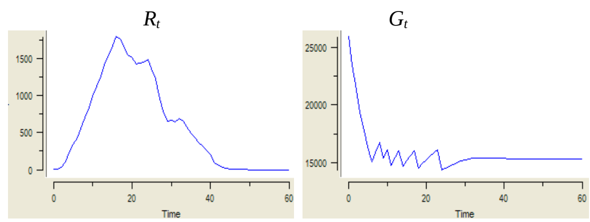


Fig. 14. Releasing the energy (ps =0.4，ps2=0.1)

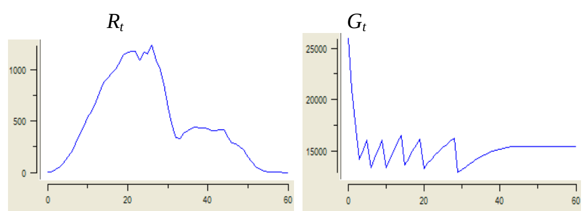


Fig. 15. Releasing the energy (ps =0.4，ps2=0.2)

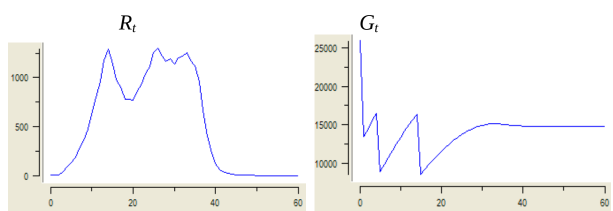


Fig. 16. Releasing the energy (ps =0.4，ps2=0.5)

The aforementioned series of computational results show that when the ratio of energy limitation reaches a higher point (p_s = 0.65), the best value of the probability of the energy release is p_{s2} = 0.31, and R_t at the explosion point decreases from 4094 to 2303, which is a decrease of 43.75%. When the ratio of energy limitation reaches a lower point (p_s = 0.4), the best value of the probability of the energy release is p_{s2} = 0.2, and R_t at the explosion point decreases from 4094 to 1177, which is a decrease of 71.25%. Therefore a lower ratio of energy limitation value could lead to more effective management.

TABLE VI. THE EFFECT COMPARISON OF THE ENERGY RELEASE

p_s	p_{s2}	R_t at the explosion point and the decrease ratio	The duration of the evolution
0.65	0.1	3298, 19.44%	39 cycles
0.65	0.2	2890, 29.41%	44 cycles
0.65	0.3	2312, 43.53%	41 cycles
0.65	0.31(the best)	2303, 43.75%	40 cycles
0.65	0.4	2949, 27.97%	39 cycles
0.65	0.5	2398, 41.43%	41 cycles
0.4	0.1	1804, 55.94%	50 cycles
0.4	0.2(the best)	1177, 71.25%	59 cycles
0.4	0.3	1209(943) , 70.47%	70 cycles
0.4	0.4	1439(776) , 64.85%	78 cycles
0.4	0.5	1291(1304,1258), 68.15%	50 cycles

3) Release the energy before the evolution and during the evolution

If the energy is released before the evolution, the energy is set to drop from 26,000 to 20,000 (that is 23.08% of the energy is released), which accounts for 50% of the maximal energy.

Then, the energy release is implemented during the evolution. A series of experiments are performed by selecting p_s= 0.4, $p_{s2} \in$ [0.1, 0.5]. Some of the experimental results are shown in Figures 17 to 19, and the effects of the experiment are shown in Table 7.

The aforementioned series of computational results show that when the ratio of the energy limit reaches a lower point (p_s = 0.4), the probability of energy release, p_{s2} , reaches 0.16, and R_t at the explosion point decreases rapidly from the three that was initially set to zero after six cycles; this makes it possible to completely control the fire. Thus the effect of the energy release before and during the fire is very distinct.

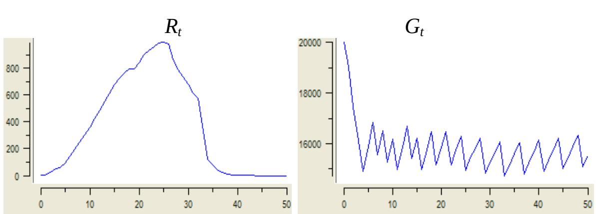


Fig. 17. Releasing the energy (ps =0.4，ps2=0.1)

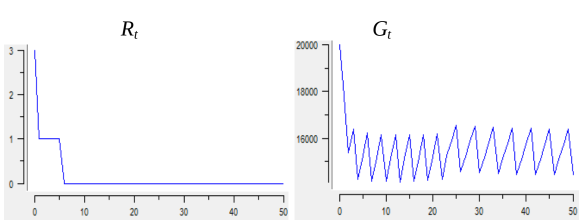


Fig. 18. Releasing the energy (ps =0.4，ps2=0.16)

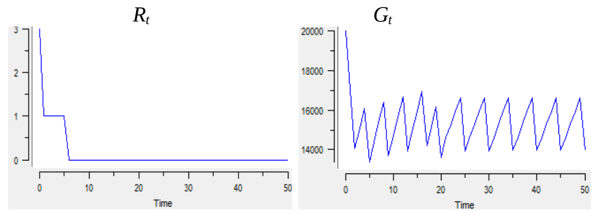


Fig. 19. Releasing the energy (ps =0.4，ps2=0.5)

TABLE VII. THE EFFECT COMPARISON OF THE ENERGY RELEASE

p_s	p_{s2}	R_t at the explosion point	The duration of the evolution
0.4	0.1	999	44 cycles
0.4	0.16	3	6 cycles
0.4	0.2	3	6 cycles
0.4	0.3	3	6 cycles
0.4	0.4	3	6 cycles
0.4	0.5	3	6 cycles

VI. CONCLUSIONS

The experiments have shown that the model proposed in this paper is suitable for analyzing the internal factors of the forest fire evolution and fires management practices. In order to control a fire, a scientific release of the energy could be considered to take. In addition, increasing the extinguishing efficiency and reducing the spread of the fire actually has an adverse effect on the management of the fire.

Following the simulations carried out in this paper, a number of suggestions can be proposed:

1) The method of releasing energy in a small scale before and during the disaster is scientific and feasible，and it can reduce the number of forest fires. It is crucial to scientifically determine the energy release time, energy limit value ratio p_s and the probability of the energy release p_{s2}; moreover it is necessary to find the most feasible solution in this area.

2) Improving the efficiency of the fire extinguishing procedures is the most direct and effective way to control forest fires. However, once a large-scale forest fire has broken out, it is hard to improve the firefighting efficiency and achieve better results. In addition, fire-fighting efficiency is a double-edged sword. The higher the efficiency, the smaller the burned area; however this leads to a larger residual energy, which may increase the risk of subsequent fires.

3) Reducing the speed of the fire spreading is another effective method. A significant reduction in the speed of the fire spreading can effectively reduce R_t at the explosion point (burned area). However, the fire spreading speed depends on the wind speed, wind direction, temperature, fuels, obstacles and other factors, which are generally difficult to control.

However, some factors of the forest fires, such as geologic structure, are rarely considered in this paper. And the action moment of the energy release need further research.

ACKNOWLEDGMENT

The This work was supported in part by the Chinese National Natural Science Foundation (No. 71371148); China postdoctoral Fund Projects (No. 2013M542080); China postdoctoral Fund Special projects (No.2014T70750) and Hubei province: humanities and social science project(No. 14G524).

REFERENCES

[1] S. Clar, B. Drossel, K. Schenk, F. Schwabl, "Self-organized criticality in forest-fire models," Physica A: Statistical Mechanics and its Applications, vol. 266, pp. 153-159, April 1999.

[2] B. Drossel, F. Schwabl, "Forest fire model with immune trees," Physica A, vol. 199, pp. 183-197, October 1993.

[3] Guisoni, Nara, Loscar, S. Ernesto, Albano, V. Ezequiel, "Phase diagram and critical behavior of a forest-fire model in a gradient of immunityGuisoni," Physical Review E - Statistical, Nonlinear, and Soft Matter Physics, vol. 83, pp. 1-9, January 2011.

[4] S. Yassemi, S. Dragićević, M. Schmidt, "Design and implementation of an integrated GIS-based cellular automata model to characterize forest fire behaviour," Ecological Modelling, vol. 210, pp. 71–84, January 2008.

[5] Thomas J. Duff, Derek M. Chong, Kevin G. Tolhurst, "Using Discrete Event Simulation Cellular Automata models to determine multi-mode travel times and routes of terrestrial suppression resources to wildland fires," European Journal of Operational Research, In Press, Accepted Manuscript.

[6] D.I. Iudin, Ya.D. Sergeyev, M. Hayakawa, "Infinity computations in cellular automaton forest-fire model," Communications in Nonlinear Science and Numerical Simulation, vol. 20, pp. 861–870, March 2015.

[7] L. Herna´ndez Encinas, S. Hoya White, A. Martı´n del Rey, G. Rodrı´guez Sa´nchez, "Modeling forest fire spread using hexagonal cellular automata," Applied Mathematical Modelling, vol. 31, pp. 1213–1227, June 2007.

[8] S. Yassemi, S. Dragićević, M. Schmidt, "Design and implementation of an integrated GIS-based cellular automata model to characterize forest fire behaviour," Ecological Modelling, vol. 210, pp. 71–84, January 2008.

[9] Stephen G Berjak, John W Hearne, "An improved cellular automaton model for simulating fire in a spatially heterogeneous Savanna system," Ecological Modelling, vol. 148, pp. 133–151, February 2002.

[10] A. Alexandridis, D. Vakalis, C.I. Siettos, G.V. Bafas, "A cellular automata model for forest fire spread prediction: The case of the wildfire that swept through Spetses Island in 1990," Applied Mathematics and Computation, vol. 204, pp. 191–201, October 2008.

[11] Z. Hui, W. Tao, W. Daimu, "Polymorphism forest fire probability cellular automata model and its application," Journal of FuYang normal college (Natural Sciences), vol. 27, pp. 23-26, January 2010.

[12] Z. Guangjun, L. Yaodong, "Forest fire system modeling and simulation based on Agent," Computer Engineering Design, vol. 31, pp. 4451-4454, October 2010.

[13] Z. Guiqing, Y. Zi, W. Lin, Z. Kaien, C. Tianlun, "Self Organized Criticality in a Simple Forest Fire Model," Journal of Nankai University (Natural Sciences), vol. 44, pp. 76-81, October 2011.

Community Perception of the Security and Acceptance of Mobile Banking Services in Bahrain: An Empirical Study

Ahmad S. Mashhour, PhD
IS Department,
University of Bahrain

Zakarya Saleh, PhD
IS Department,
University of Bahrain

***Abstract*—Bahraini banks and financial organizations have applied remote enabled service using the internet and a mobile device to increase efficiency, reduce costs and improve quality of services. There is need for these organizations to identify factors that persuade customers and raise their attitudes towards adoption and usage of these services.**

This study identifies the most important factors affecting customer attitudes towards mobile banking acceptance in Bahrain. The model formulated in this research presents and empirically examined the factors influencing mobile banking adoption behavior on customers. The model was tested with a survey sample of 300 banking customers. The findings of the study indicate that wireless connection quality, mobile banking awareness, the social influence, mobile self-efficacy, trust, and resistance to change have significant impact on the attitudes towards the likelihood of adopting mobile banking. Model developed is an extension to the Technology Acceptance Model (TAM). Data analysis is based on the Statistical Package for Social Science (SPSS).

Keywords—Adoption factors; Bahrain community; Mobile Banking Services; Perceived Usefulness (PU); Perceived Ease of Use (PEOU); Technology acceptance model (TAM)

I. Introduction

Mobile banking (m-banking) refers to the use of a smartphone or other cellular device such as tablet and Personal Digital Assistant (PDA) to perform online banking tasks from any place and any time. Mobile banking typically operates across all major mobile providers through one of three ways: SMS messaging; mobile web; or applications. Developed Mobile SMS text and alert is the simplest, allowing the user to transfer fund or access account information via text message. Mobile web is the second mobile banking option, which is similar to online account access from a home-based computer, this option allows for checking balances, bill payment and account transfers simply by logging into the user's account via a mobile web browser[1]. Mobile banking applications for Android, iPhone and Blackberry, connect the user directly to the bank server for complete banking functionality without having to navigate a mobile web browser.

Smartphone, Tablets and apps have spread the use of online banking and changed the way people bank. The number of mobile banking users has grown from 17.8 million in 2010 to 53.1 million in 2013 [2]. This increase can be recognized to the growth in smart phones industry and banking apps that have been developed by different banking organization. Advantages of mobile banking are numerous for both bankers and customers. For the bankers, mobile banking brings a range of benefits right from reducing costs, achieving greater customer satisfaction to bringing more customers into their crease. For the customer, it gives them an easy access to their account as they no longer have to go the actual banks to make their transactions. Service providers also benefit from mobile banking as it regarded as the best way of achieving growth. However, there are still issues facing banking organizations such as security and privacy [3, 4, 5].

Bahrain is considered a main center of the financial industry of the Arabian Gulf States which incents most Bahraini banks to adopt mobile banking (M-banking) services to satisfy the need of their customers. Bahrain's growing reputation as a center of financial excellence in the region is reflected by the steady increase of financial institutions registered in the Kingdom providing a variety of new and traditional banking services. There are 55 banks operating in Bahrain [6], and have increasingly adopted Internet and mobile devices in their services. Bahrain has the highest penetration Internet access rate in the area and rated 27th in the world out of 142 countries by the World Economic Forum's Network Readiness Index [6-7].

Although previous studies have addressed an extensive range of factors related to user adoption of information technology applications and products worldwide and including the Arabian Gulf states, developing a model that captures salient aspects of mobile banking in Bahrain and all factors affecting the adoption of mobile banking is suggested and in fact needed by both business and their customers. The main objective of this study is to understand the factors that affect users' adoption of mobile banking by developing a mobile banking adoption model (for Bahraini community) that raises their attitudes towards the usage of mobile banking services. To achieve the research objectives, one main research question was addressed: "What factors affect the adoption of mobile banking from the user's perspective?"

The remainder of the paper consists of the following sections: The next section presents literature review, followed by operation overview of online banking and security concerns. The next section presents research methodology which includes model development, and experiment design and implementation, followed by results discussion, and conclusions.

II. Literature Review and Theoretical Framework

According to survey by U.S Federal Reserve 2012 report prepared by Statista.com [8] and results shown in figure 1, a significant number of mobile phone users have already adopted mobile banking. The expected percentage of mobile owner who is planning to use mobile banking by 2017 will reach 51%. From the same survey, mobile banking is highly correlated with age and education; individuals between ages 18 and 29 account for approximately 44% of mobile banking users. 73 percent of all mobile banking users have at least some college education, but this education group represents only 60% of all mobile phone users, and the use of mobile banking is generally unrelated to household income. Undoubtedly, checking financial account balances or transaction inquiries were the most common mobile banking activity, with 90 percent of mobile banking users having performed this function in the last two years.

A study by Hassan et al. [9] investigated factors influencing the adoption of mobile banking services in Bangladesh and concluded that five factors affects user adoption. These are: perceived usefulness, subjective norm, perceived ease of use, perceived credibility, consumer awareness about mobile banking and perceived risks associated with mobile banking. A study by Soufi & Ali [10] concluded that the intention to adopt mobile banking in Bahrain is mainly affected by specific factors which are: Perceived Usefulness and Ease of Use.

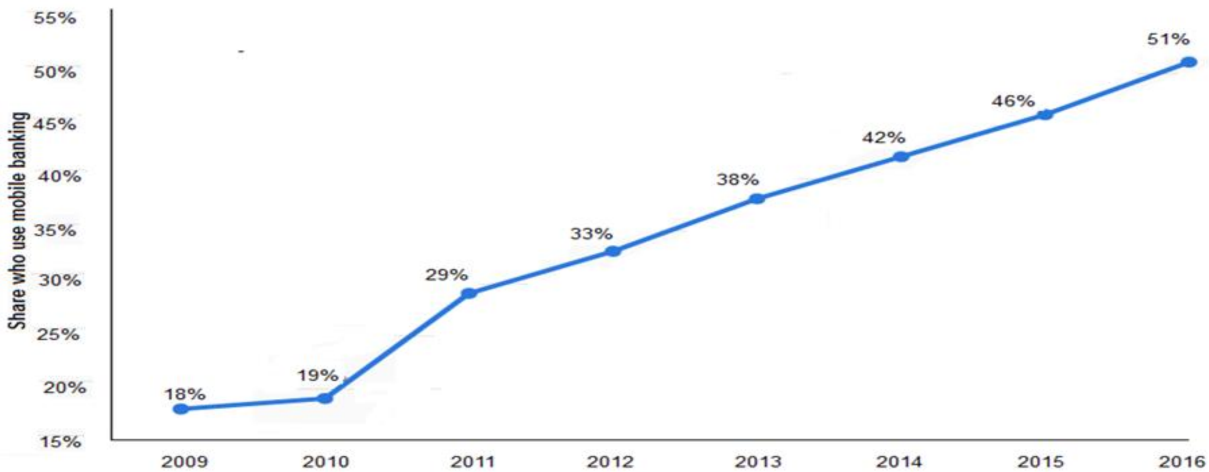


Fig. 1. Number of U.S. Mobile Users for the Period 2009-2011 [8]

A study by Bankole at al. [11] explores factors that influence adoption of mobile banking in Nigeria. Research results showed the existence of a causal relationship between perceived quality, satisfaction, and commitment in the context of mobile banking. His results showed that the perceived quality heavily influences the commitment of customers and its effect is direct and not mediated by satisfaction. A study by Al-Somali et al. [13] was aimed to identify the factors that encourage customers to adopt mobile banking in Saudi Arabia. It revealed that there are many factors that can influence the acceptance of mobile banking in Saudi Arabia, these factors include: quality of the Internet connection, awareness of services, trust, social influence, resistance to change, the technology self-efficacy and demographic characteristics. Alalwan et al. [14] studied predictive factors influencing customer intention and adoption of mobile banking in Jordan. The study concluded that trust is a crucial factor influencing behavioral intention to use mobile banking. Performance expectancy, hedonic motivation, and facilitating conditions are also positively influence the adoption of mobile banking.

III. Operation Overview

Mobile Banking is designed for mobile phone users and offers them services that enable them to conduct their financial transactions through a mobile device such as a mobile phone or tablet. The architecture of the Mobile Banking System is depicted in Figure 2, which shows the main functional components, their roles and contribution within the system.

The Mobile Banking Equipment is what is at the end–user's hand to access the information and services provided by the system. The Mobile Banking Equipment displays the menu and performs secure short message creation and transmission based on the user's selection. The Mobile Banking Platform is split into two functional blocks, which may be separated and operated by the Network Provider and the Service Provider respectively.

The Mobile Banking Platform transfers the short message received from the Mobile Banking Equipment into conformant commands of a selected banking protocol. Interaction between User and Service Provider system is supported by multilevel dialogs. The Bank Account Server as part of the system provides the respective banking support. It receives the instructions to provide the necessary functions to be performed on the bank accounts and communicates the results and status back to the Mobile Banking Platform. The Mobile Banking System supports communication with other servers, such as Internet Information Servers. These participate in the environment and contribute other services and information to enhance the service offering to the user.

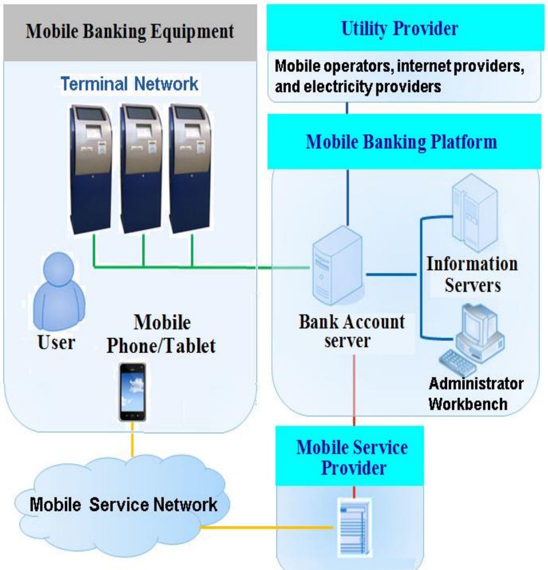


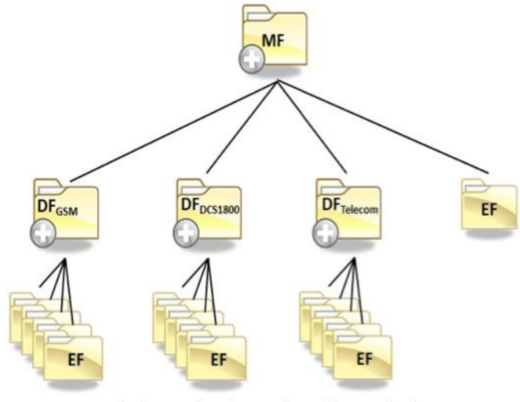
Fig. 2. Mobile Banking System Architecture

Besides viewing account balances and detailed account history, some of the banks in Bahrain (e.g. HSBC) provide several service to their customers which includes moving money between accounts, pay bills, check exchange rates and use the built-in currency calculator, receive secure messages from the bank and send requests from the mobile devices.

IV. Mobile Phones Security Concerns

Security of financial communications, where the transactions are performed remotely, then transmitting this sensitive information over the air, is a complicated challenge that needs to be the concern of the mobile application developers, the wireless network service providers and the banks' information technology departments. A PwC financial mobile services consumer survey of Canadian and US consumers reveals that security risk and fraud is a top concern for 78% of respondents when it comes to mobile payments. The survey also shows that 67% of those surveyed would prefer that their mobile payments be enabled by their banks [15]. IO Active security assessment company, published a report on the sort of security users can expect when conducting mobile banking on an iPhone or iPad, indicating that 70% of the apps offered no support at all for two-factor authentication and 40% of the apps did not validate the authenticity of SSL certificates presented, making them susceptible to Man in The Middle attack [16]. Someone performing a man-in-the-middle (MITM) attack on HTTPS traffic (i.e. HTTP over SSL) would be able to see all content of the encrypted communication, including transmitted usernames and passwords [17]. The fact is HTTPS certificates rely on a chain of trust, and validating that chain is important.

Identity modules (universally known as SIM cards), that interoperate with GSM cellular networks, incorporate a SIM File System (see figure 3), resulting in various types of digital evidence, including mobile banking transactions that could exist in elementary data files scattered throughout the file system and be recovered from the Universal Integrated Circuit Card (UICC).



MF - Master File (root and main container of DF and EF)
DF - Directory File
EF - Elementary File

Fig. 3. GSM SIM File System [18]

In addition, some of the same information held in the UICC may be maintained in the memory of the mobile device and encountered there as well [18]. Besides the standard files defined in the GSM specifications, a UICC may contain several general categories of data that could be found in standard elementary data files of a UICC. This information could include service-related information (e.g. the unique identifiers for the UICC), the Integrated Circuit Card Identification (ICCID) and the International Mobile Subscriber Identity (IMSI) (e.g. Phonebook, call information such as Abbreviated Dialing Numbers (ADN) and Last Numbers Dialed (LND)), and the messaging information including both Short Message Service (SMS) text messages and Enhanced Messaging Service (EMS) simple multimedia messages. The USIM application supports the storage of links to incoming (EFICI) and outgoing (EFOCI) calls (the EFICI and EFOCI are each stored using two bytes. The first byte points to a specific phone book and the second points to an abbreviated dialing number (EFADN) entry), as well as location information including Location Area Information (LAI) for voice communications and Routing Area Information (RAI) for data communications which indicates that mobile transactions data and information could be easily retrieved using some of the available tools (including commercial and open source tools) that are normally intended for device management, testing, and diagnostics. Example of the tools that can be used for the black box analysis would be otool (object file displaying tool), Burp pro (proxy tool), or SSH [16].

V. Development of the Research Model

The Technology Acceptance Model (TAM) proposed by Davis [19] is an information systems model used to explain or predict users' motivations to accept and use a technology. TAM, as illustrated in Figure 4, is one of the most utilized models used to determine Information Systems/Information Technology (IT/IS) acceptance. Many previous studies have adopted and expanded this model which was empirically proven to have high validity [20-28]. The model identifies Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) as key factors that influence acceptance of a certain technologies.

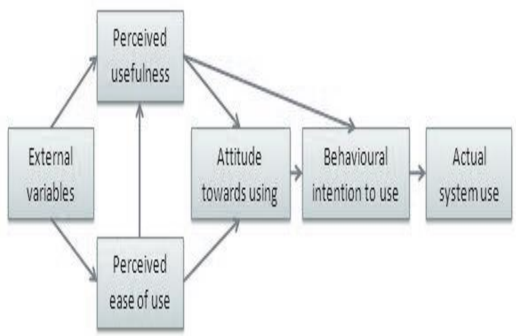


Fig. 4. Technology Acceptance Model, source: Davis et al. [22] 4

As defined by Davis [19], perceived ease of use and perceived usefulness are the two main factors that influence an individual's attitudes towards intention to use IT/IS (i.e., mobile banking system services).These attitudes will in turn influence the actual use of mobile banking. This research defines PU in the context of mobile banking as the degree to which a user believes that using a mobile banking system service would enhance banking services usability. We also assume that mobile banking is more likely to be adopted if they are easy to use. Therefore, PEOU is defined in this research as the degree to which a user believes that using a mobile banking system service or technology would be free from effort. However, TAM does not take into confederations the security aspects of the technology, and mobile banking is exposed to more security issues because wireless circuits are easier to tap than their hard-wired counterparts. In addition, despite the concerted efforts to secure the transmission of sensitive information over handheld devices, there is still the risk of physically loosing of the device. Accordingly, this study proposes an extended version of the Technology Acceptance Model (TAM). The proposed variables were tested and verified and the complete set of the variables are collected and tested on Bahraini community's acceptance of mobile banking. Several hypotheses have been constructed in the model for testing mobile banking adoption in Bahrain.

A. Demographic factors

Many studies recognized that demographic factors impact heavily on consumer attitudes and behavior regarding technology acceptance [29-31]. According to these studies young, educated, and wealthy consumers are the most likely to adapt the technologies. Therefore, the following hypotheses have been developed.

H1-A: Age positively affects customer's attitude towards using mobile banking.

H1-B: Gender has no impact on the customer's attitude towards using mobile banking.

H1-C: the level of Income has a significant impact on the customer's attitude towards using mobile banking.

H1-D: The level of education has a positive impact on the customer's attitude towards using mobile banking.

B. External Factors

1) The quality of the Internet connection (QI) is an essential component for any Internet-based application. Without a proper Internet connection the use of mobile banking is not possible. Some studies confirm that there is a significant relationship between the speed of Internet access and the use of mobile banking services [31-32].

H2: Perceived quality of the Internet connection (QI) has a positive impact on customer's perceived ease of use.

2) The technology self-efficacy (SE) is an individual's belief about his/her ability to successfully use the technological service to accomplish a specific task. Davis et al. [22] found that 'The technology self-efficacy' and 'perceived ease of use' are related. There is empirical evidence in previous studies that the technology self-efficacy has a positive impact on perceived usefulness and perceived ease of use [33-36].

H3: The technology self-efficacy (SE) has a positive impact on customer's perceived ease of use.

3) Awareness of services (AW): According to Sathye [30] & Al-Somali et al. [13], awareness of service has direct influence on user intention to use the technology.

H4: Awareness of services (AW) and benefits has a positive impact on customer's perceived usefulness.

4) Social Influence (SI) or (Image) is the degree to which a potential user perceives the usage of a technologically based innovation as adding prestige to his social image. Customers may have unfavorable or favorable perceptions towards mobile banking use because of the perceptions of a family member, acquaintances or peers influence. Davis et al. [22] believed that in some circumstances people might use a technology to comply with others' mandates rather than their own feelings and beliefs.

H5: Social Influence (SI) has a positive impact on customer's perceived usefulness.

5) Trust and security (TRS): Mobile banking services carry benefits as well as risks. Trust and security are related factors, and thus, are important in the acceptance of mobile banking. Trust has been accepted as a critical element in mobile banking services due to the fact that transactions are characterized as a process that involves uncertainty and risk and therefore, trust is considered as the most effective means of reducing uncertainty and risk [36]. Generally, consumer trust has been identified as a key to the development of Internet services [36-41].

H6: Customers Trust in secured (TRS) mobile banking has a positive impact on their attitudes towards using mobile banking.

6) Convenience is viewed as a very important advantage of mobile banking especially when users want to be able to have access to services anywhere at any time [39].

H7: Convenience (CNV) is Positively Related to perceived ease of use (PEOU).

7) Perceived ease of use (PEOU): This study suggests that mobile banking system requires less effort to use, learn, and train. According to Padachi et al., [42] ease of use is a significant factor in the adoption of e- Banking. Safeena et al. [43], and Liao and Wong [44] Stated that perceived ease of use has a strong and positive influence on customer's intention to adopt and use internet services.

H8: Customer's perceived ease of use in mobile banking system positively impact customer's attitude towards using mobile banking.

8) Perceived usefulness (PU) of mobile banking: Several studies showed that perceived usefulness influence customer interactions with internet banking [13,42,44], and these studies beleive that perceived usefulness affects the adoption of mobile banking services. Therefore a new hypothesis is added:

H9: Customer's Perceived Usefulness (PU) impacts positively the intention to use mobile banking.

9) Customer's attitude towards using mobile banking (ATT): Researchers found that users' attitude towards the acceptance of a new information system (IS) has a critical impact on its success [13, 45-46]. Celik [47] stated that perceived usefulness and perceived ease of use are direct determinants of customers' attitudes towards using the technology. Yap, et al. [48] stated that traditional service quality and website features such as PU, PEOU and PC (Perceived credibility) gives customer confidence and build trust in the technology. The following hypothesis is added:

H10: Customer's Attitude (ATT) towards using mobile banking has a positive impact on his/her behavioral intention to use it. Figure (4) next depicts the proposed model.

VI. Experiment Design

A sample of 300 participants was randomly chosen from the Bahrain community. All participants were bank customers selected randomly from universities, companies and Internet forums and are supposed to have some experience in using the Internet. Two hundred and forty six usable responses were collected, yielding a response rate of 82%.

The questionnaire is divided into three main sections according to Mobile banking service usage. The selection of the questionnaire items were collected form latest case studies and literature review which is considered the main source of information in developing the research questionnaire and then the research model [49, 50]. The questionnaire begins with general (demographic) section consist of questions which collect information about gender, age, level of education, income, preferred methods of performing banking transactions, computer literacy level, bank visiting frequency, user bank account, Internet knowledge a usage, and the type of users. The second set of questions are related services provided to users of mobile banking; it consists of several questions grouped into ten groups. The third set of questions belongs to the people who do not use the mobile banking services, and it includes challenges to mobile banking services.

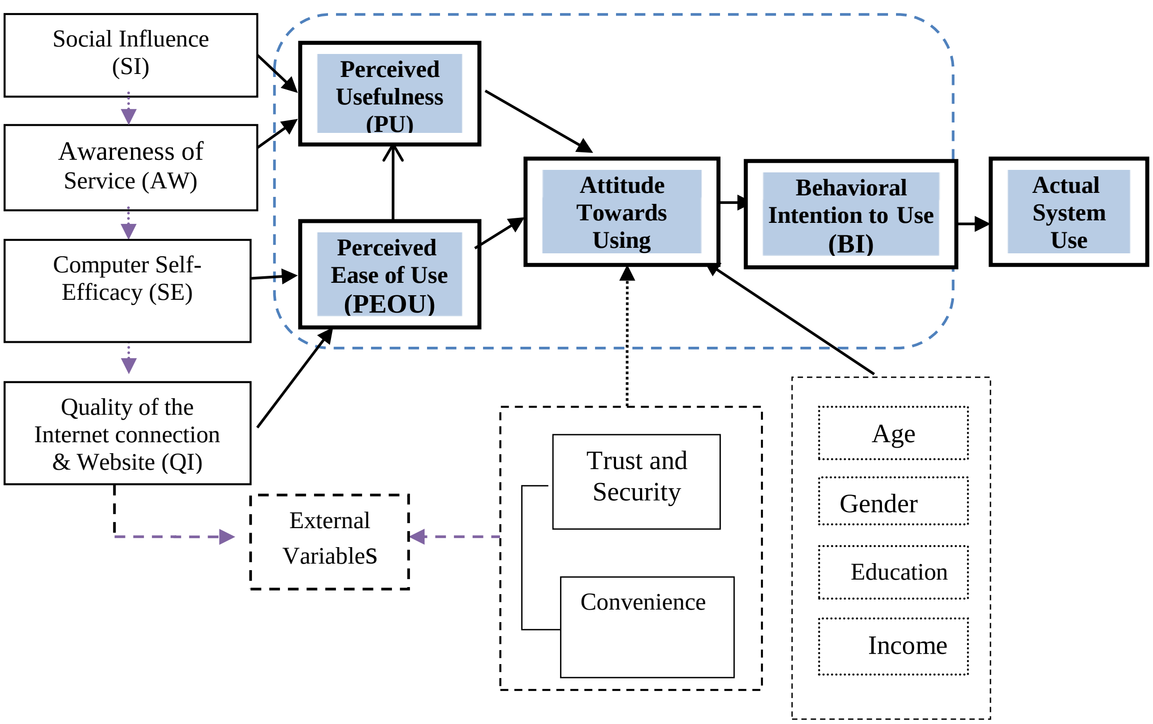


Fig. 5. The proposed extended TAM model

VII. Results and Discussion

The hypotheses were tested with an online survey involving 246 banking customers residing in the Kingdom of Bahrain. Collected data were analyzed using SPSS (Statistical Package for Social Science) Version 19 by applying several statistical tests including descriptive statistics and Chi-Square test. The descriptive statistics of the respondents' demographic characteristics were analyzed and presented first in table 1 shown below and summary of other hypothesis analysis are presented next.

A. Demographic Characteristics Analysis

43.92 percent of the respondents were male and the largest proportions (56.1%) of respondents were females. The largest proportion (65.9%) of respondents by age group, were those in the 18-25 years old category. The survey respondents were generally well educated with over 12.2 % holding an advanced degree and 64.2% having a 4-year first degree. The results indicate that the largest proportion (44.0%) of respondents had advanced computer literacy and only a tiny proportion claimed to have no or little computer ability. Based on the income more than half of the respondents (53.0%) earn less than 400 BD (1300 US dollar) monthly.

Chi-square test results for demographic factors are shown in table 2. From the table, the Sig. value is close to 0.000 for gender and income, 0.033 for Age (which is less than 0.05, the accepted criterion), and equal to 0.247 for education. Therefore the results are significant for gender, age, income and related to the intention to use mobile banking, while education is not significant and therefore does not affect intention to use the internet banking. Therefore, H1-A, H1-B and H1-D have been confirmed (not rejected) while H1-C is rejected.

TABLE I. Demographic Characteristics of Mobile Banking Usage

Demographic factor		Using mobile banking services	Do not use mobile banking	Total	Percent (%)
Gender	Male	60	48	108	43.91
	Female	28	110	138	56.09
	Total	**88**	**158**	**246**	**100.0**
Age	Between 18 – 25	44	118	162	65.84
	Between 25 – 35	24	16	40	16.26
	Between 35 – 45	12	15	27	11.38
	Above 45	8	9	17	06.52
	Total	**88**	**158**	**246**	**100**
Education	High school	11	19	30	12.20
	Bachelor's	38	110	158	64.23
	Master's	14	8	22	8.95
	Doctoral	2	2	4	3.25
	Others	14	18	32	11.83
		44	**79**	**246**	**100**
Income	less than 400 BD monthly	34	97	131	53.25
	Between 400 – 800 BD monthly	26	61	87	35.37
	over 800 BD monthly	14	14	28	11.38
Total		**74**	**172**	**246**	**100**

TABLE II. Pearson Chi-Square Tests for Demographic Variables

Factor	Value	df	Asymp. Sig. (2-sided)
H1. Gender	16.397	1	.000
H2. Age	8.735	3	.033
H3. Education	5.414	4	.247
H4. Income	37.457	3	.000

B. Significance Analysis of Research Hypotheses

First table 3 shows averages calculation for the tested variables, the correlation and Chi-Square tests between the hypotheses has been calculated and presented next. Tables 4 and 5 presents the results of asymptotic analysis and chi-square test analysis of the data collected from sample users' responses

TABLE III. Calculated Sample Averages of the Tested Variables

PU AVG	**PEOU AVG**	**BI AVG**	**ATT AVG**	**QI AVG**	**AW AVG**	**TRS AVG**	**SI AVG**	**CNV AVG**	**SE AVG**
1.8	1.5666	1.5854	1.6168	1.6877	1.7502	1.6488	1.6414	1.78	1.813
4.8	3.4833	3.7677	3.812	3.5134	3.4638	3.1849	3.1506	2.71	2.8797
4.4	4.3666	4.3604	4.2918	4.1266	4.1144	3.9638	3.9656	3.49	3.9486
4	3.9166	4.1198	4.2398	4.1954	4.2088	4.1535	4.0958	4.43	4.1468
4	3.9166	3.6823	3.6	3.3777	3.2444	3.0492	3.0968	3.11	3.0633

According to table 4 all the above hypothesizes (H2 - H10) have an Approx. Sig. close to 0.00 with perceived ease of use, perceived usefulness and behavioral intention to use (BI). So all the above hypothesizes are positively confirmed and are related.

Same conclusion can be obtained from table 5 where H8, H9, H10, have Asymptotic Significance close to 0.00 and an equal Asymptotic Significance for both H6 and H7 with 0.005. H2 and H3 have an Approx. Sig. with 0.02 and 0.010 respectively. From the table all results are significant, i.e. (chi-square is less than or equal to 0.05). This confirms with the results of frequency analysis of the hypotheses.

Table 6 summarizes the hypothesize result which shows that generally Bahraini citizen have a good awareness of mobile banking services.

TABLE IV. PEARSON SYMMETRIC MEASURES

Hypothesizes path	Value	Asymp. Std. Error	Approx. T	Approx. Sig.
H2: Quality of Internet (QI) AVERAGE → PEOU_AVG	.966	.013	24.181	.000
H3: The technologies self-efficacy (SE)_ AVG. → PEOU_AVG	.929	.025	16.103	.000
H4: Awareness of Service(AW)_ AVG. → PU_AVG	.834	.062	9.800	.000
H5: Social Influence (SI) _ AVG → PU_AVG	.822	.070	9.344	.000
H6: Trust & Security (TSR) _ AVG → ATT_AVG	.972	.012	26.712	.000
H7: Convenience (CNV)_AVG →ATT_AVG	.842	.0271	22.234	.000
H8: PEOU_AVG → ATT _ AVG .	.980	.007	32.140	.000
H9: PEOU_AVG → PU _ AVG	.913	.040	14.531	.000
H10: Attitudes toward using _ AVG (ATT)→ BI_AVG	.993	.003	53.530	.000

TABLE V. CHI-SQUARE TESTS

Hypothesis	Value	df	Asymp. Sig. (2-sided)
H2: QI _AVG → PEOU _AVG	1.232	1092	.002
H3: SE _AVG . → PEOU _AVG	1.204	1092	.010
H4: AW _AVG → PU _AVG	5.720	520	.057
H5: SI _AVG → PU _AVG	5.720	520	.057
H6: TRS _AVG → ATT _AVG	1.584	1440	.005
H7: CNV_AVG → ATT _AVG	1.324	1092	.012
H8: PEOU_AVG → ATT _ AVG	5.32	512	.000
H9: PEOU _AVG . → PU _AVG	5.679	364	.000
H10: ATT _AVG → BI _AVG	1.452	1188	.000

C. Correlation Analysis of Internal Variables

Pearson correlations were calculated to identify the correlations between the variables: Perceived Usefulness, Perceived Ease of Use, Behavior Intention, and Attitude towards using mobile banking and to test the hypothesis (H8-H11). Results are shown in table 6. Since the highest correlation coefficient is 0.513 which is less than 0.8, there is no multicollinearity problem in this research. Table 7 summarized the end results of the hypothesis testing.

TABLE VI. HYPOTHESIZES RESULT SUMMARY

Hypothesizes path	Approved
H1-A: Gender → ATT	✓
H1-B: Age → ATT	✓
H1-C: Education → ATT	×
H1-D: Income → ATT	✓
H2: Quality of Internet (QI) → PEOU	✓
H3: Self-Efficacy (SE) → PEOU	✓
H4: Awareness of Service (AW)→ PU	✓
H5: Social Influence(SI) → PU	✓
H6: Trust and Security (TRS) → ATT	✓
H7: Convenience (CNV) → ATT	✓
H8: Perceived Ease of Use (PEOU) → ATT	✓
H9: Perceived Ease of Use (PEOU) → PU	✓
H10: Attitudes towards using (ATT) → BI	✓

TABLE VII. CORRELATION ANALYSIS OF INTERNAL VARIABLES

Criteria	PU	PEOU	BI	ATT
Perceived Usefulness (PU)	1			
Perceived Ease of Use (PEOU)	.423	1		
Behavioral Intension (BI)	.513	.499	1	
Attitude towards (ATT)	-.251	-.356	-.474	1
Mean	2.44	2.34	2.233	1.843
Standard Deviation	.654	.792	.731	.258

VIII. CONCLUSIONS AND RECOMMENDATIONS

This research was carried out to study the user acceptance of mobile banking practice in the kingdom of Bahrain. The study examines the factors influencing user to adopt mobile banking technology services, as well as influencing users' intentions to adopt mobile banking service and technology. The study finds that mobile banking customers in Bahrain generally have a good awareness of the mobile services that have been provided. However, the study finds that the responders do not use mobile banking services due to many challenges including information security issues.

The study shows that the most effective challenges (variables) include: trust and lack of experience in using Internet enabled mobile applications. 68.4% respondents believe don't trust mobile banking, and 36.7% of them do not have the adequate skills to use the mobile banking technology. For security enhancements, banks and individuals may enhance their mobile devices with add-on security procedures or means.

A variety of login authentication mechanisms are available for mobile devices that could be used as a replacements or supplements to password mechanisms for mobile banking. Mobile banking should support a method to permanently delete all banking history from the mobile devices and all data relates to the transactions to prevent such data from being be recovered from the Universal Integrated Circuit Card. Mobile banking services carries benefits as well as risks. Hence, it is the responsibility of the bankers to recognize, manage and to address banking institutions in cautious and sensible way according to the fundamental characteristics and challenges of mobile banking services. The future of banking is driven by young professionals today who will be the significant drivers of retail banking revenues tomorrow by using their smart phones. Understanding what this group wants will differentiate the winners from the losers in the business of banking.

REFERENCES

[1] M. Monahan, "What Are The Three Big Trends In Mobile Banking In 2014? ", Javlin Strategy & Research,2014. Https://Www.Javelinstrategy.Com/Blog/2014/02/18/

[2] Monitise/Future, "Foundation, Emerging Trends In Mobile Banking" - Monitise, Americas, Inc. 2010. Www.Monitise.Com/Resources_Centre_Download/28/Money-O.

[3] J. Puschel, J. A. Mazzon, & J.M.C. Hernandez, "Mobile banking: Proposition of an integrated adoption intention framework. International Journal of Bank Marketing, 28(5), 389-409, 2010.

[4] Federal Reserve Board reports, "Consumers and Mobile Financial Services", 2014. http://www.federalreserve.gov/publications/default.htm.

[5] Juniper Research, "Mobile Banking: Handset & Tablet Market Strategies 2013-2017- the new juniper report", 2013, Hampshire, UK. http:// www.juniperresearch.com.

[6] Bank Association of Bahrain, 2012. http:// www.banksbahrain.org.

[7] World Economic Forum, "The Global Information Technology Report", 2014. http://www.weforum.org/ reports/ global information-technology-report-2014.

[8] Statista, the Statistics Portal, "Percentage of U.S. mobile phone users who use mobile banking from 2009 to 2016", 2015. http://www.statista.com/statistics/244414/percentage-of-us-mobile-phone

[9] M. Hassan, A. Rahman, S. Afrin, & M. Gulam Rabbany, "Factors Influencing the Adoption of Mobile Banking Services in Bangladesh: An Empirical Analysis". International Research Journal of Marketing, 9-20, 2014. DOI: 10.12966/irjm.02.02.2014

[10] A.Soufi, A., H. Ali, "Customers perception of m-banking adoption in Kingdom of Bahrain: an empirical assessment of an extended TAM model". International Journal of Managing Information Technology (IJMIT), Vol.6, No., 2014.

[11] F. O. Bankole, O. O. Bankole, & I. Brown, "Mobile banking adoption in Nigeria", The Electronic Journal on Information Systems in Developing Countries EJISDC, 47, 2, pp1-23, 2011.

[12] C. Hamadi, "The Impact of Quality of Online Banking on Customer Commitment". Communications of the IBIMA, IBIMA Publishing",Vol 2., Article ID 844230, 8 pages, 2010, DOI: 10.5171/2010.844230.

[13] S. A. Al-Somali, R. Gholami, & B. T. Clegg, "An investigation into the acceptance of mobile banking in Saudi Arabia". Technovation, 29(2), pp.130-141, 2009, Elsevier, DOI: 10.1016/j.tecnovation.2008.07.004.

[14] A. Al alwan, Y.K. Dwivedi, & M.D.Williams, M.D, "Examining Consumer Adoption of Mobile Banking in Jordan". Conference: Proceedings of Academy of Marketing Conference AM 2014. 7th -10th of July 2014, At Bournemouth.

[15] PwC, "Mobile payments: Is trust the key to consumer uptake?", Banking Review, Issue of Winter 2013.

[16] Ariel Sanchez, "Personal banking apps leak info through phone ", Insights, News & Discoveries from Ioactive Researchers, Issue of January 8, 2014. http://blog.ioactive.com/2014/01/personal-banking-apps-leak-info-through.html.

[17] NETRESEC (2011). "Network Forensic Analysis of SSL MITM Attacks". NETRESEC Network Security Blog. [Online] Available at http:// the WWW on October 2, 2014 at http://www.netresec.com/?page=Blog&month=2011-03 & post=Network-Forensic-Analysis-of-SSL-MITM-Attacks

[18] Wayne Jansen, and Rick Ayers, Guidelines on Mobile Device Forensics, NIST Special Publication 800-101, 2014.

[19] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology", MIS Quarterly, 13(3),1989, 319–339.

[20] P. Y. K. Chau, "An Empirical Assessment of a Modified Technology Acceptance Model", Journal of Management Information Systems, 12 (2), 1996, pp. 185-204.

[21] S. Al-Gahtani, "The applicability of TAM outside North America: An empirical test in the United Kingdom", Information Resources Manage Journal, 2001, 14(3), pp. 37-46.

[22] F. D. Davis, F.D., R. P. Bagozzi, & P. R. Warshaw, P.R., "User acceptance of computer technology: A comparison of two theoretical models", Management Science, 35(8), 1989, pp. 982-1003.

[23] Davis, F.D. and Venkatesh, V. A., "Critical Assessment of Potential Measurement. Biases in the Technology Acceptance Model: Three Experiments. International", Journal of Human-Computer Studies, 45, 1996, 19-45.

[24] V. Vinkatesh, M. G. Morris, G. B. Davis, F. D. Davis,). "User acceptance of Information Technology: Toward a Unified View", MIS Quarterly, Vol. 27 No. 3, 2003, pp. 425-478.

[25] Dishaw, M., Strong, Diane M., "Extending the technology acceptance model with Task-technology fit constructs", Information & Management 36 (1), 1999, pp. 9-21.URL http://dx.doi.org/10.1016/S0378-7206 (98)00101-3.

[26] V. Venkatesh, F. D. Davis, "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies", Management Science INFORMS, Vol. 46, No. 2, 2000, pp. 186–204

[27] Y. Malhotra, D. F. Galletta, "Extending the Technology Acceptance Model to Account for Social Influence", Theoretical Bases and Empirical Validation, HICSS, vol. 1, pp.1006, 1999, Thirty-Second Annual Hawaii International Conference on System Sciences-Volume 1.

[28] T. K. Pikkarainen, H. Karjaluoto, S. Pahnila, "Consumer acceptance of mobile banking: an extension of the technology acceptance model", Internet Research, Vol. 14 (3), pp. 224 – 235, 2014.

[29] I. Akman, A. Mishra, " Gender, age and income differences in internet usage among employees in organizations', Computers in Human Behavior, Elsevier, Volume 26, Issue 3, May 2010, Pages 482-490.

[30] M. Sathye, Adoption of Internet Banking by Australian consumer: an empirical investigation. International Journal of Bank Marketing 17(7), 2009, pp. 324-334.

[31] D. El- Kasheir, A. S. Ashour, & O. M. Yacout, "Factors affecting continued usage of mobile banking among Egyptian customers", Communications of the IBIMA, Vol. 9, 2009, pp 252-263.

[32] T. El-kiki, E. Lawrence, "Mobile User Satisfaction and Usage Analysis Model of m-Government Services", 2007. http://www.m4life.org/proceedings/2006/PDF/11_El-Kiki.pdf

[33] R. Agarwal, V. Sambamurthy, R.M. Stair, Research report: "The evolving relationship between general and specific, The technology self-

efficacy–An empirical assessment". Information System Research, 11(4), 2000, pp. 418-430.

[34] M. Igbaria, J. Livari, "The effect of self-efficacy on computer useage", Moega, Int. Mgmi Science, Vol.23, No. 6, 2005, pp. 587-606.

Econ. Res., Vol 2(2), 2013, Society of Interdisciplinary Business Research.http://www.sibresearch.org.

[36] Y. H. Kim, D. J. Kim, "A Study of Online Transaction Self-Efficacy, Consumer Trust, and Uncertainty Reduction in Electronic Commerce Transaction". Proceedings of the 38th Hawaii International Conference on System Sciences, 2005.

[37] A. Almogbil, "Security, perception, and practices: challenges facing adoption of mobile banking in Saudi", Unpublished PhD thesis, George Washington University, 2015.

[38] M. S. Shahibi , S. K. W. Fakeh, "Security Factor and Trust in E-Commerce Transactions", Australian Journal of Basic and Applied Sciences, 5(12), 2011: 2028-2033.

[39] A. Kagan R. N. Acharya, & L. S. Rao, "Does Internet Banking Affect the Performance of Community Banks?", Selected Paper prepared for presentation at the American Agricultural Economics Association Annual Meeting, No 19246, 2005. Annual meeting, July 24-27, Providence, RI from American Agricultural Economics Association (New Name 2008: Agricultural and Applied Economics Association). http://purl.umn.edu/19246.

[40] Yousafzai, S.Y., Pallister, J.G., Foxall, G.R. "A proposed model of e-trust for electronic banking", Technovation, 23 (11), 2003, pp. 847-860.

[41] Gefen, D., Karahanna, E. & Straub, D. W., "Trust and TAM in Online Shopping: An Integrated Model", MIS Quarterly, 27, 2003, pp 51-90.

[42] Rojid Padachi, A. Seetanah, " Analyzing the Factors that Influence the Adoption of Internet Banking in Mauritius", Proceedings of the 2007 Computer Science and IT Education Conference,

[35] M. S. M. Arrif, Y. S. Min, N. ZAkuan, N. Shak, "The Impact of Computer Self Efficacy and Technology Acceptance Model on Behavioral Intention in Internet Banking System. Rev.", Integr. Bus.

[43] Safeena, R., Abdullah, K., and Hema, D., "Customer Perspectives on E-business Value: Case Study on Internet Banking", Journal of Internet Banking and Commerce, vol. 15 (1), 2010.

[44] Liao, Z., and Wong, W., "The determinants of customer interactions with internet-enabled mobile banking services", Journal of the Operational Research Society, vol. 59 (9), 2008.

[45] V. Venkatesh, "Determinants of Perceived Ease of Use: Integrating Perceived Behavioral Control, Computer Anxiety and Enjoyment into the Technology Acceptance Model", Information Systems Research, 11, 2000, pp342-365.

[46] M. J. Succi, Z. D. Walter, "Theory of User Acceptance of Information Technologies: An Examination of Health Care Professionals", Proceedings of the 32nd Hawaii International Conference on System Sciences (HICSS), 1999, PP. 1-7.

[47] Celik, H., "Wh1at Determines Turkish customers' acceptance of internet banking?", International Journal of Bank Marketing. Vol. 26 (5), pp353-370, 2010.

[48] K. D.Yap, C. Wong, C. Loh, & R. Bak. "Offline and mobile banking - where to draw the line when building trust in e banking", International Journal of Bank Marketing, 28(1), 2010, pp.27-46.

[49] International Finance Corporation (IFC) on Mobile Banking Questionnaire – users http://www.ifc.org/wps/wcm/connect/571b Tool+3.9.+Market+Questionnaire++Users.pdf?MOD=AJPERES

Image Stitching System Based on ORB Feature-Based Technique and Compensation Blending

Ebtsam Adel
Information System Dept.,
Faculty of Computers and Information,
Mansoura University, Egypt

Mohammed Elmogy
Information Technology Dept.,
Faculty of Computers and Information,
Mansoura University, Egypt

Hazem Elbakry
Information System Dept.,
Faculty of Computers and Information,
Mansoura University, Egypt

***Abstract*—The construction of a high-resolution panoramic image from a sequence of input overlapping images of the same scene is called image stitching/mosaicing. It is considered as an important, challenging topic in computer vision, multimedia, and computer graphics. The quality of the mosaic image and the time cost are the two primary parameters for measuring the stitching performance. Therefore, the main objective of this paper is to introduce a high-quality image stitching system with least computation time. First, we compare many different features detectors. We test Harris corner detector, SIFT, SURF, FAST, GoodFeaturesToTrack, MSER, and ORB techniques to measure the detection rate of the corrected keypoints and processing time. Second, we manipulate the implementation of different common categories of image blending methods to increase the quality of the stitching process. From experimental results, we conclude that ORB algorithm is the fastest, more accurate, and with higher performance. In addition, Exposure Compensation is the highest stitching quality blending method. Finally, we have generated an image stitching system based on ORB using Exposure Compensation blending method.**

Keywords*—Image stitching; Image mosaicking; Feature-based approaches; Scale Invariant Feature Transform (SIFT); Speed-up Robust Feature detector (SURF); Oriented FAST and Rotated BRIEF (ORB); Exposure Compensation blending

I. Introduction

Image stitching is the construction process of a sequence of input overlapping images of the same scene into a single image with a high resolution. The use of the image stitching in real-time applications is a challenging topic for computer vision and computer graphics experts. The quality of stitching is measured by the similarity between the two adjacent stitched images that form the composite image. In addition, the seams visibility between the input overlapping images must be removed.

There are two essential approaches for image stitching: the direct approach and feature-based approach. The goal of the direct approach is to minimize pixel to pixel mismatching directly [1]. However, the feature-based techniques depend on extracting a set of features and matching them to each other [2].

Feature-based approaches begin by establishing similarity between points of the input images. The robust detectors must include some essential characteristics, such as invariance to noise, scale, translation, and rotation transformations. There are many feature-based techniques that are used in computer vision applications, such as HARRIS detector [3], Scale Invariant Feature Transform (SIFT) [2], Principal Component Analysis SIFT (PCA-SIFT) [4], Bag of Features (BOF) [5], Features from Accelerated Segment Test (FAST) [6], Speed-up Robust Feature detector (SURF) [7], and Oriented FAST and Rotated BRIEF (ORB) [8]. The choice of the convenient feature detector depends firstly on the nature of the problem. For example, for image stitching and pattern recognition applications, scale and rotation invariant detector is the best choice, such as ORB, SURF, and SIFT techniques.

For features-based approaches, there are two main processes: the registration process and the blending process. The registration step is the core of the stitching procedure, which aims at finding the transformations to align two or more input overlapping images. The blending step decides how to blend these input images to create an attractive looking panorama.

The main goal of this paper is to introduce a high-quality automatic image mosaicing and blending system with low computation time based on feature extraction approach. The proposed system consists of four main stages. These stages are feature detection, description and matching using ORB technique, image matching using RANSAC algorithm, and applying the Exposure Compensation blending method.

The remainder of this paper is structured in six sections. Section 2 presents an overview of some related work of image stitching research that tries to increase the quality of image blending. Section 3 contains the discussion of some common features detection and description techniques. Section 4 provides the discussion of some common blending methods that are used in image stitching systems. In Section 5, the proposed image stitching system is discussed. The experimental results are manipulated in Section 6. Finally, Section 7 contains the conclusion and the future work directions.

II. Related Work

There are many researchers that deal with the problem of image stitching and try to increase the quality of image blending. For example, Uyttendaele et al. [9] presented two main contributions of image stitching problems. The first one is a method for dealing with objects that move between different views of a dynamic scene. The other one is a method to eliminate visible shifts in brightness. They presented a method of block-based adjustment, which changes the pixel values using a weighted average of lookup tables from close parts of the image.

Rankov et al. [10] proposed an approach for establishing high resolution, edgeless, and composite image using cross-correlation and blending. One image is correlated at a time with a composite image. When the image is registered, the blending is performed. The presented method is fast because of using a lookup table technique.

Zomet and Peleg [11] studied the cost functions and compared their performance to different scenarios both theoretically and practically. Their approach can be used in many applications, such as building the panoramic images, object blending, and removing of compression artifacts.

Bind et al. [12] proposed a panoramic image stitching technique for three-dimensional, rotational images with a variation of the illumination. The input overlapping images are passed through two strong stitching algorithms, i.e. SIFT and SURF. SIFT algorithm is invariant towards scale and rotational variation. It is also robust towards the noisy environment. SURF algorithm has very similar properties as SIFT. However, it has the properties of illumination invariance and good computational speed. The blending process was done using Discrete Wavelet Transform (DWT).

Antony and Surendran [13] implemented a stitching technique to create panoramas of satellite images based on image registration. They geometrically aligned one input image into another. Then, image stitching algorithm takes the alignment estimation that is produced by the registration algorithm to blend the images in a seamless manner. Their image stitching system was well suited for all types of images including the satellite images. The system supported images of different formats, such as JPEG, TIFF, GIFF, and PNG. It did not perform very well on images with very different lighting conditions. To avoid this problem, the two images should be normalized before applying the method. The processing time of the proposed system varies with the size of the image. They also dialed with problems, such as blurring or ghosting caused by parallax and scene movement. The performance can be evaluated by comparing the execution time of various images with different size and formats.

Suen et al. [14] showed that how the curvature values can reject the effect of non-uniform inconsistency. They generated a method that is minimized the curvature value variations between the input images and the mosaicing image. The experiment showed that it could reduce conspicuous cutting curves. Moreover, even when there is severe geometric misalignment, by choosing an optimal cut between the input images, the induced artifacts become invisible. In addition, their methods provide an easy control of fidelity and transition smoothness by simply determining the area of using the minimization.

Finally, Adel et al. [15] compared many feature-based detectors that can be used in image stitching. They tested Harris corner detector, GoodFeaturesToTrack detector, SIFT, SURF, FAST, MSER detector, and ORB technique to measure the detection rate of the corrected keypoints, time, and accuracy of the detection process. The experimental result showed that the SIFT method is a robust algorithm, but it takes more time for computations. ORB and MSER algorithm is robust as well as SIFT algorithm, but ORB is the fastest technique. In addition, they introduced a real-time image stitching system based on ORB feature-based technique. They performed experiments that test the ORB relative to SIFT and SURF. ORB algorithm is the fastest, the highest performance, and with very low memory requirements.

III. Features Detection and Description

In image stitching systems that are based on the features approach, the features of the input images are extracted and then matched with each other based on correspondence “similarity” of their descriptors. This stage can be classified into three main steps: detection, description, and matching.

There are two main types of features descriptors: vector descriptor and the binary descriptor. SIFT, PCA-SIFT, and SURF are considered as vector descriptors while ORB and BRIEF are binary descriptors. In the following subsections, we will study briefly some of the most known feature detectors and descriptors.

1) SIFT

SIFT proposed by David Lowe [2] and then improved in 2004. Currently, it is the most common known vector descriptor. It consists of four essential stages: scale-space extrema detection, key points localization, orientation assignment, and generating keypoint descriptor. In the first stage, the key points are extracted based on their strength that are invariant to orientation and scale using Difference of Gaussian. In the second stage, the wrong points are removed. Then in the following stage, one or more orientations are assigned to each keypoint. In the final stage, a vector descriptor is made for each keypoint.

2) SURF

The SURF algorithm was proposed by Bay et al. [7]. It is built upon the SIFT, but it works by a different way for extracting features. SURF is based on multi-scale space theory and speeds up its computations by fast approximation of Hessian matrix and descriptor using “integral images”. Haar wavelets are used during the description stage.

3) FAST

FAST is a high-speed feature detector that is much suitable for real-time applications. The algorithm considers a circle of 16 pixels around the candidate corner p. A feature is specified when a set of n contiguous pixels in the circle are all darker or brighter than the candidate pixel p plus a threshold t [6].

4) Harris

Harris is a corner detector based on Moravec algorithm, which is proposed by Harris and Stephens in 1988 [3]. A detecting window in the image is designed. The average variation in intensity is determined by shifting the window by a small amount in a different direction. The center point of the window is extracted as a corner point.

5) Good Features to Track Detector

It expands the Harris detector to make its corners more uniformly distributed across the image. Shi and Tomasi [16] showed how to monitor the quality of image features during tracking. They investigated a measure of feature dissimilarity that quantifies how much the appearance of a feature changes between the first and the current frame.

6) ORB

ORB technique developed by Rublee et al. [8]. It is a combination of features from FAST keypoint detection and Binary Robust Independent Elementary Features (BRIEF) [17] descriptor. It describes the features of the input image in a binary string instead of the vector.

7) MSER

MSER stands for Maximally Stable Extremal Regions Detector. It was generated by Matas et al. [18] to find matching between image elements from two input images from different viewpoints. The 'maximally stable' in MSER describes the property optimized in the threshold selection process. The word 'extremal' refers to the property that all pixels inside the MSER may be either higher or lower intensity than all the pixels on its outer environment.

IV. Image Blending Methods

Image blending is an important stage when creating a panoramic image. During the stitching process, the seams between the input images may be generated because of many reasons, such as differences in camera response, lighting conditions changes, and due to geometrical alignment. To remove these seams, we must decide how to blend the input images. Image blending can hide these seams and reduce color differences between input images to create an attractive looking panorama. In this section, we will discuss some of the common methods of image blending that are used in image stitching.

1) Feathering (Alpha) Blending

Feathering blending is the simplest method to create a final composition "blending" of input images. It takes an average value simply at each pixel. The pixel values in the blended regions are a weighted average of the two overlapping images. The feathering blending approach works better if the image pixels have aligned well with each other [19].

2) Gradient Domain Blending

An alternative approach to multi-band image blending is to perform the operations in the gradient domain as the human visual system. It is very sensitive to the encode of the gradient. Here, instead of working with the initial color values, the image gradients from each source image are copied in a second pass. An image that best matches these gradients is reconstructed [19].

3) Laplacian Pyramid Blending

The pyramid is a multiple scale format of the image. It can be used in many different applications, such as image blending, image compression, image enhancement, and reduction of the noise. The image pyramid is a hierarchical representation of an image. It is a collection of images at different resolutions. The lowest level is the highest resolution, and the highest level is the lowest resolution [20].

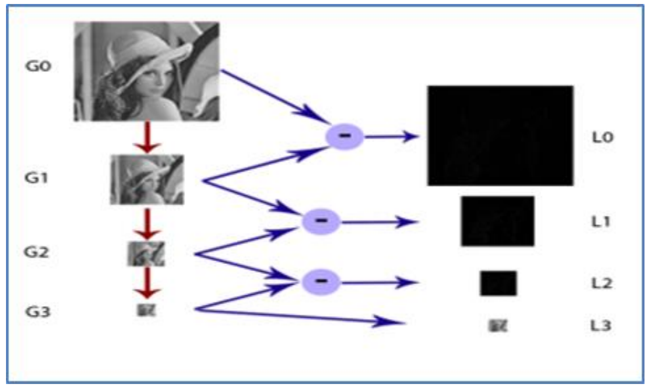


Fig. 1. The construction of the Laplacian pyramid for the Lena image [20]

The Laplacian pyramid has two primary repeated operations: Reduce and Expand. First, it downsizes the image into different sizes (Reduce) with Gaussian. Next, it expands the Gaussian into the lower level and subtracts from the image at that level (Expand) [20].

4) Exposure Compensation

Exposure compensation can do a better job of blending when the exposure differences become significant, and it can handle vignetting. It estimates a local correction between each source image and a blended composite. First, a block-based quadratic transfer function is fit between each source image and an initial feathered composite. Next, transfer functions are averaged with their neighbors to get a smoother mapping, and per pixel transfer functions are computed by splining between neighboring block values [9].

V. The Proposed Stitching System

In this paper, we propose a feature based system to create a panoramic image. First, we start with extracting and describing features from the input images by using one of the features extraction and description techniques. Then, we match the features using Homography RANSAC. Finally, the results are generated by applying one of the blending methods. In the proposed image stitching system, we apply the following steps:

1) We extract features from the overlapping input images using one of the different extraction techniques and then generating the descriptor of those features.

2) After extracting and describing the features, we match these features with each other based on their descriptors.

3) Then, we find out the correcting features by using the RANSAC (Random Sample Consensus), which removes unwanted feature points.

4) In the last step, we apply blending process to eliminate the seams between the processed images. With the help of image blending method, we get the final output panoramic image with a high stitching quality.

In the subsequent sections, we will speak in more detail about the main building steps of the proposed system.

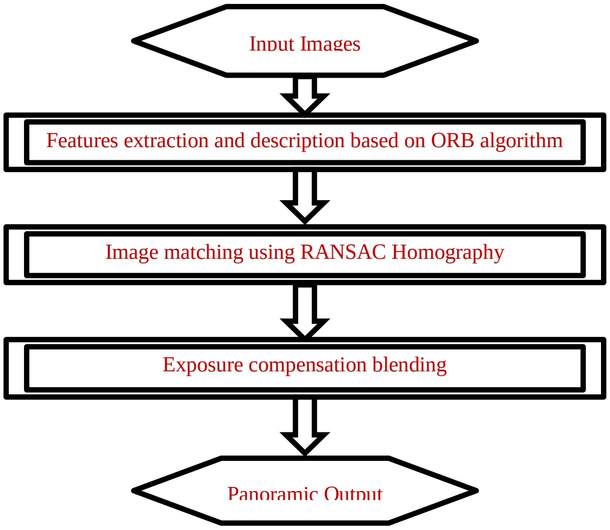


Fig. 2. The block diagram of the proposed panoramic image system

a) Features Extraction and Description

The aim of this step is to find out the unique features in the input images. It is compared with each other to determine "matching" relationships between processed images. Overlapping images will share an amount of features, and this information can be used to establish transformative relations. In this step, we will do firstly a comparative study between many different feature extraction detectors such as: Harris detector, SIFT, SURF, GoodFeaturesToTrack, FAST, MSER, and ORB to measure the number of the corrected detected feature points and the amount of the processing time.

b) Homography Using RANSAC (RANdom SAmple Consensus)

The next step of the image statching system is to estimate RANSAC Homography. To decrease the computation time through the Homography estimation, RANSAC method is used to delete the wrongly detecting points. It chooses the closest match between the two images by separating inliers and outliers. It determines the neighbor pictures. RANSAC loop involves selecting four feature pairs randomly. It computes Homography H (mapping between any two points with the same center of projection). For each key point, there may be more than one candidate matches in the other processed image. We choose the best matching based on the distance between their descriptors [21].

c) Image Blending

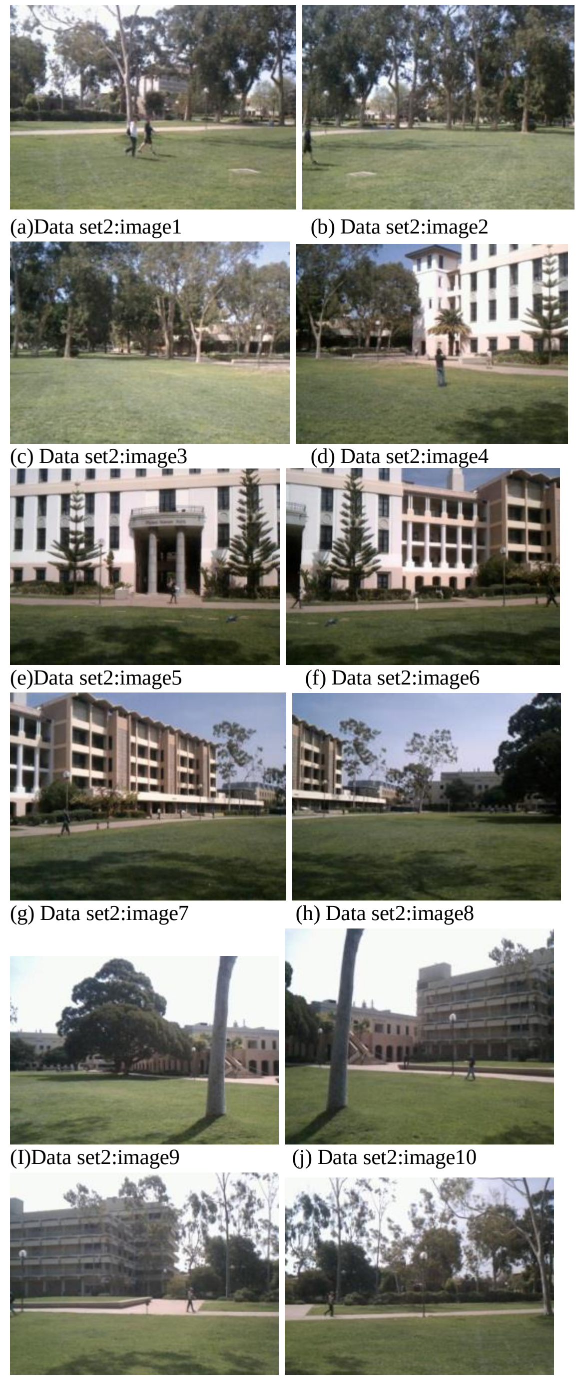
After alignment, the input overlapping images must be blended. Image blending is the final step in developing image stitching system that aims to blend the pixels colors in the overlapped region to avoid the seams between input images.

VI. Experiential Results

The experiments are performed on a laptop with CPU 2.6 GHz processor, 4 GB RAM, and Windows 7 as an operating system. We have implemented a complete image stitching system in Microsoft Visual Studio 2010 and OpenCV ver 2.4.9 library.

(a)Data set1:image1 (b) Data set1:image2

Fig. 3. The first group of 2 input images [22]



(a)Data set2:image1 (b) Data set2:image2

(c) Data set2:image3 (d) Data set2:image4

(e)Data set2:image5 (f) Data set2:image6

(g) Data set2:image7 (h) Data set2:image8

(I)Data set2:image9 (j) Data set2:image10

(k) Data set2:image11 (l) Data set2:image12

Fig. 4. The second group of 12 input images [22]

First, we have evaluated some known features extraction and description techniques to determine the highest performance and the least processing time. Also, We also evaluated some commonly used methods of the blending to determine the highest stitching quality. For the experiment purpose, we applied our system to many different groups of images. The first group contains two input images; each image is 320x225 resolutions, as shown in Figure 3. The second group contains twelve input images. Each image is 480x320 resolutions, as shown in Figure 4.

A. The responses of the extraction detectors

For the second dataset, Figure 5 shows the responses of the different techniques of the first input image.

Table 1 shows the number of detected features and detecting the time of the different detectors for the first and second image of the second dataset.

TABLE I. PERFORMANCE ANALYSIS OF FEATURE EXTRACTION DETECTORS FOR THE FIRST AND SECOND IMAGE OF THE SECOND DATASET

Extraction Detector	Detected features		Time (s)	
	Image1	*Image2*	*Image1*	*Image2*
Harris corner detector	1115	1015	0.52	0.43
SIFT	989	756	1.2	1.09
SURF	454	351	0.23	0.54
GoodFeaturesToTrack	623	680	0.76	0.74
FAST	912	863	0.1	0.12
MSER	261	266	0.68	0.55
ORB	175	125	0.06	0.05

From the results at this step, we found that Harris and SIFT detect the highest number of feature points, but the later took the longest processing time among all other features detectors. However, ORB satisfies the highest performance as well as SIFT but has the least computation time.

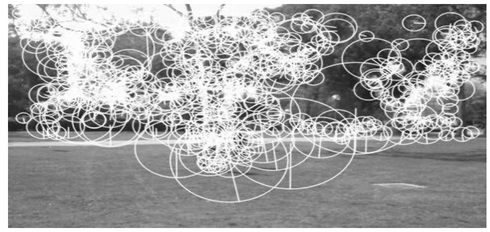
Table 2 shows the matching features number and the feature matching time of SIFT, SURF and ORB descriptors between the first and second images for the tested datasets.

TABLE II. THE FEATURE MATCHING TIME (SECONDS) OF SIFT, SURF, AND ORB DESCRIPTORS

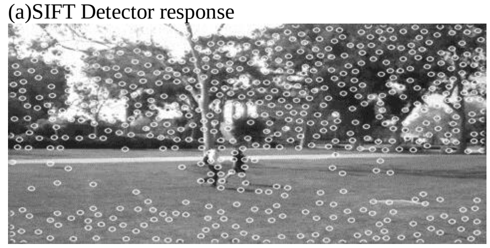
Dataset	Matching features			Matching time		
	SIFT	*SURF*	*ORB*	*SIFT*	*SURF*	*ORB*
DataSet1	256	143	89	1.245	0.564	0.326
DataSet2	235	156	78	1.749	0.75	0. 35

The results show that SIFT technique took the highest matching time, whereas ORB technique had the least matching time. Therefore, ORB is the most appropriate for real-time applications.

From the results at this step, we concluded that the number of extracted features is not a measure of the full success or performance of the detector by itself, but the performance and quality of these features in matching with the features in the other image. For example, SIFT may waste the time for detecting features that are not seemed to contain enough information for the matching step. The key points detected by ORB, although fewer, are more accurate than those detected by SIFT and SURF.

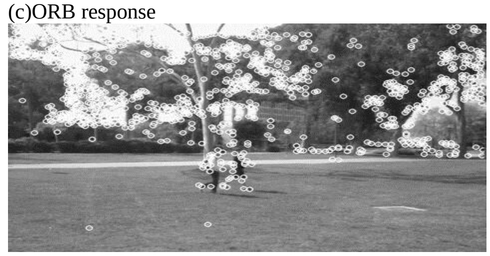


(a)SIFT Detector response

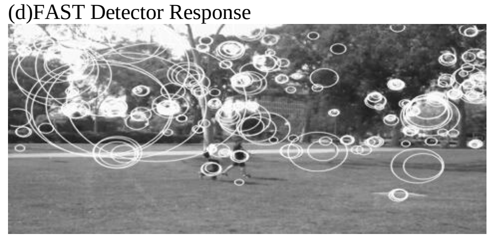


(b)GoodFeaturesToTrack response

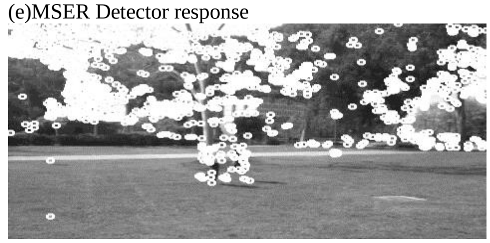
(c)ORB response



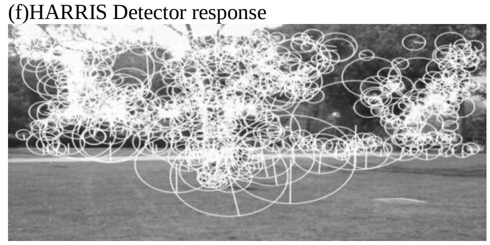
(d)FAST Detector Response



(e)MSER Detector response



(f)HARRIS Detector response



(g)SURF Detector response.

Fig. 5. The responses of the different features detectors for the first input image of the second dataset

B. Homography Using RANSAC

After extracting the features from all images, the next step is to match them with each other and discard the incorrect points. Figures 6 and 7 show the actually matched features between the first and second input images of the tested datasets.

Fig. 6. The matching pairs of the two images of the first dataset (32 matches)

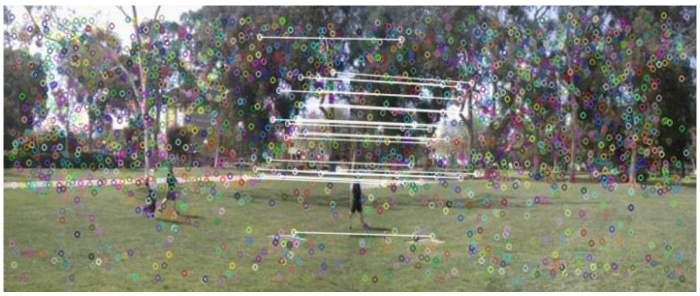


Fig. 7. The matching pairs between the image1 and image2 in the second dataset (44 matches)

After matching the input images, the last step of stitching system is to blend images with each other. There are many popular ways of blending the images, such as Alpha blending, Gaussian pyramid, Gradient Domain blending, and Exposure Compensation blending.

C. The responses of the blending methods

Figures 8, 9, 10, and 11 show the responses of the various blending methods in the proposed stitching system for the first dataset.

Fig. 8. The final panoramic image of the first dataset using Exposure Compensation blending

Fig. 9. The final panoramic image of the first dataset using pyramid blending

Fig. 10. The final panoramic image of the first dataset using Gradient Domain blending

Fig. 11. The final panoramic image of the first dataset using Alpha blending

Figures 12, 13, 14, and 15 show the responses of the different blending methods in the proposed stitching system for the second dataset.

Fig. 12. The final panoramic image of the dataset using Exposure Compensation blending

Fig. 13. The final panoramic image of the dataset using pyramid blending

Fig. 14. The final panoramic image of the dataset using gradient domain blending

Fig. 15. The final panoramic image of the dataset using alpha blending

D. The performance evaluation of the resulting panoramic images

Performance evaluation is a critical task in computer vision field. We test the performance of our system according to the following measures [12]: PSNR, Normalized Absolute Error, Enhancement performance measure, Feature similarity index and Mutual Information.

1) PSNR: It is defined as the peak signal to noise ratio. It is calculated to measure the quality of reconstruction [23]. The more the PSNR, the higher the quality of the reconstructed image.

2) FSIM: It is a method for measuring the similarity between two images.

3) Mutual Information: It measures the symmetry between two images as well as a fluctuation from its mean value [24].

4) Enhancement Performance Measure (EME): It is used for measuring the enhancement quality of the algorithm.

5) Normalized Absolute Error (NAE): The lower the value of NAE, the better is the blended output image.

TABLE III. THE PERFORMANCE ANALYSIS OF THE ORB TECHNIQUE AND DIFFERENT USED BLENDING METHODS FOR THE FIRST DATASET

Similarity Parameters	Exposure compensation	Laplacian pyramid	Gradient domain	Alpha blending
PSNR	43.876	42.657	41.675	41.06
FSIM	0.787	0.676	0.602	0.523
MI	1.324	1.3	1.22	1.2
EME	8.324	8.11	8.08	7.131
NAE	0.125	0.131	0.133	0.142

TABLE IV. THE PERFORMANCE ANALYSIS OF THE ORB TECHNIQUE AND DIFFERENT USED BLENDING METHODS FOR THE SECOND DATASET

Similarity Parameters	Exposure compensation	Laplacian pyramid	Gradient domain	Alpha blending
PSNR	41.234	40.12	40	38.6
FSIM	0.667	0.615	0.611	0.487
MI	0.667	0.63	0.57	0.5
EME	8.18	7.65	7.15	7.08
NAE	0.134	0.144	0.149	0.158

From the experimental results as shown in the two above tables, we notice that Exposure Compensation has the highest PSNR, higher FSIM, and the least NAE. It means that it is the highest similarity output blended image followed by Pyramid blending and then Gradient Domain blending.

VII. CONCLUSION

Image stitching is importantly required for many different applications, such as the construction of large satellite image from collections of input photographs. There are several problems while implementing the automatically image stitching system. For example, a change of camera rotation may lead to high parallax in the output image, which may decrease the stitching quality. In addition, a large number of overlapping images need a large processing time. The noisy input image may decrease the quality of stitching. The goal of this paper is to introduce a system for image stitching with high quality and in the same time with less processing time because time is a major factor in many applications. Therefore, we have compared many different features detectors and descriptors. We have concluded that ORB algorithm is the best one. Also, we have manipulated the implementation of four common categories of image fusion algorithms: Exposure Compensation, Alpha blending, Gradient domain blending, and Laplacian pyramid blending. The performance evaluation is done according to the following parameters: PSNR, FSIM, NAE, MI, and EME. Exposure Compensation blending produces the highest performance of the blending process since it has the highest similarity, and the least normalized error of the output blended image. However, Alpha blending produces the least performance. Finally, the system using ORB technique and Exposure Compensation shows the best results comparing to other methods of blending.

In the future work, we will test the implemented blending methods under some conditions, such as noisy input images, changes of the scale, and changes of illumination. In addition, we will stitch videos to create dynamic panoramas.

REFERENCES

[1] Szeliski Richard and Kang Sing Bing. Direct Methods for Visual Scene Reconstruction Conference In IEEE Workshop on Representations of Visual Scenes, pp. 26-33, 1995.

[2] Brown Matthew and Lowe David G. Automatic Panoramic Image Stitching using Invariant Features, 2007.

[3] Harris Chris and Stephens Mike. A combined corner and edge detector [Conference] In Proc. of Fourth Alvey Vision Conference, pp. 147-151, 1988.

[4] Yan Ke Rahul Sukthankar. PCA-SIFT:A More Distinctive Representation for Local Image Descriptors, Carnegie Mellon University, 2004.

[5] O'Hara Stephen and Draper Bruce A. Introduction to the Bag of Features Paradigm for Image Classification and Retrieval (CoRR), Vol. abs/1101.3354, 2011.

[6] Trajkovic Miroslav and Hedley Mark. Fast corner detection. Image Vision Comput, 2 : Vol. 16. - pp. 75-87, 1998.

[7] Bay, Herbert, Andreas Ess, Tinne Tuytelaars, and Luc Van Gool. Speeded-Up Robust Features (SURF) Comput. Vis. Image Underst. - New York, NY, USA: Elsevier Science Inc., - 3 : Vol. 110. - pp. 346-359. - ISSN: 1077-3142 DOI: 10.1016/j.cviu.2007.09.014, jun 2008.

[8] Rublee, Ethan, Vincent Rabaud, Kurt Konolige, and Gary Bradski. ORB: An Efficient Alternative to SIFT or SURF Proceedings of the 2011 International Conference on Computer Vision. - Washington, DC,

USA: IEEE Computer Society, pp. 2564-2571. - ISBN: 978-1-4577-1101-5 DOI: 10.1109/ICCV.2011.6126544, 2011.

[9] Matthew Uyttendaele , Ashley Eden and Szeliski Richard. Eliminating ghosting and exposure artifacts in image mosaics, pp. 509-516, 2001.

[10] Rankov, Vladan, Rosalind J. Locke, Richard J. Edens, Paul R. Barber, and Borivoj Vojnovic.An algorithm for image stitching and blending [Conference] Proceedings of SPIE. - 2005. - pp. 190-199.

[11] Assaf Zomet Shmuel Peleg. Seamless Image Stitching by Minimizing False Edges, 2005.

[12] Vimal Singh Bind Priya Ranjan Muduli, Umesh Chandra Pati. A Robust Technique for Feature-based Image Mosaicing using Image Fusion, 2013.

[13] Antony Dhanyamol and Surendran Subu. Satellite image registration and image stitching Satellite image registration and image stitching, 2013.

[14] Simon T.Y. Suen, Edmund Y. Lam, and Wong Kenneth K.Y. Photographic Mosaic for Camera Phones Based on Minimization of Curvature Value Variations, 2014.

[15] Adel ebtsam, Mohammed Elmogy, and Hazem Elbakry. "Real time image mosaicing system based on feature extraction techniques." Computer Engineering & Systems (ICCES), 2014 9th International Conference on. 2014. 339-345.

[16] Laganiere Robert. OpenCV 2 Computer Vision Application Programming Cookbook, 1st Ed., Packt Publishing, ISBN: 1849513244, 2011.

[17] Calonder, Michael, Vincent Lepetit, Christoph Strecha, and Pascal Fua. "BRIEF: Binary Robust Independent Elementary Features." Proceedings of the 11th European Conference on Computer Vision: Part IV. Berlin, Heidelberg: Springer-Verlag, 2010. 778-792.

[18] Matas, Jiri, Ondrej Chum, Martin Urban, and Toms Pajdla. Robust wide-baseline stereo from maximally stable extremal regions, Image Vision Comput., pp. 761-767, 2004.

[19] Szeliski Richard. Image Alignment and Stitching: Tech. rep.. - December 10, 2006.

[20] Adelson, E. H., C. H. Anderson, J. R. Bergen, P. J. Burt, and J. M. Ogden. Pyramid methods in image processing [Journal] RCA Engineer., 6 : Vol. 29. - pp. 33-41, 1984.

[21] Chandratre Rupali and Chakkarwar V. A Image Stitching using Harris and RANSAC, International Journal of Computer Applications., 15 : Vol. 89. - pp. 14-19. - Published by Foundation of Computer Science, New York, USA, March 2014.

[22] Visual Size: "http://www.visualsize.com/mosaic3d/index2.php" (Last accessed on 17/2/2015).

[23] Shivsubramani Krishnamoorthy, K P Soman. Implementation and Comparative Study of Image Fusion Algorithms, International Journal of Computer Applications., Vol. Volume 9, November 2010.

[24] Witkin Andrew P. Scale-space Filtering Conference Proceedings of the Eighth International Joint Conference on Artificial Intelligence - Volume 2. - San Francisco, CA, USA : Morgan Kaufmann Publishers Inc., pp. 1019-1022, 1983.

Systematic Literature Review of Agile Scalability for Large Scale Projects

Agile Scalability and Adoptability

Hina saeeda
Department of Computer Software Engineering
MCS, National University of Sciences and Technology,
Rawalpindi, Pakistan

Mukhtar Ahmed
Department of Computer Sciences
COMSATS Institute of Information Technology
Islamabad, Pakistan

Hannan Khalid
Department of Computer Sciences
COMSATS Institute of Information Technology
Islamabad, Pakistan

Abu Sameer
Department of Computer Sciences
COMSATS Institute of Information Technology
Islamabad, Pakistan

Fahim Arif
Department of Computer Software Engineering
MCS, National University of Sciences and Technology,
Rawalpindi, Pakistan

***Abstract*—In new methods, “agile” has come out as the top approach in software industry for the development of the soft wares. With different shapes agile is applied for handling the issues such as low cost, tight time to market schedule continuously changing requirements, Communication & Coordination, team size and distributed environment. Agile has proved to be successful in the small and medium size project, however, it have several limitations when applied on large size projects. The purpose of this study is to know agile techniques in detail, finding and highlighting its restrictions for large size projects with the help of systematic literature review. The systematic literature review is going to find answers for the Research questions: 1) How to make agile approaches scalable and adoptable for large projects?2) What are the existing methods, approaches, frameworks and practices support agile process in large scale projects? 3) What are limitations of existing agile approaches, methods, frameworks and practices with reference to large scale projects? This study will identify the current research problems of the agile scalability for large size projects by giving a detail literature review of the identified problems, existed work for providing solution to these problems and will find out limitations of the existing work for covering the identified problems in the agile scalability. All the results gathered will be summarized statistically based on these findings. Remedial work will be planned in future for handling the identified limitations of agile approaches for large scale projects.**

Keywords—Agility; large scale projects; agile scalability; SCRUM; XP; DSDM; Crystal; SLR; Statistical Analysis

I. INTRODUCTION

In market, different types of agile techniques such as SCRUM, DSDM, CRYSTAL, XP, XP2 are there each type of agile is having some different type of and specific property in it .While we talk about agile methods it is very good in the small and medium size project [1]. Agile are a combination of the characteristics that make the project successful these qualities make the project to have good properties according to the market [2]. The agile benefits such as minimum documentation, pair programming, and high teamwork produce good results for the small and medium level projects large size projects are also using the approaches but with certain limitations [3]. On the other hand, when we apply the agile approaches to large size projects it does not provide the same results.

When talking About scalability of agile two terminologies are in use “Scaling out” and “scaling up” Scaling up’ is dealing with using agile methods for developing large software systems that cannot be developed by a small team. Scaling out’ is concerned with how agile methods can be used in large size projects [4].

It is not the true that 100 percent its application is going to fail but like the small level and medium level projects results, it does not show the same for large size projects. The agile approaches such as crystal – blue are in use for large size projects but show less agile properties. [5]. Techniques of agility like SCRUM are applied for the large size project but it has also some restrictions [6].

The current research is about scaling of agile techniques for large size projects [7]. The discussion on ability of agile practices to scale to “large” software development efforts has been widely discussed [8][64]. Here the purpose of the research is to conduct detailed literature review on the agile scalability, identifying current work done for agile scalability and limitations faced by agility in large size projects. In a systematic way, In study proper research questions are built according to the PICOC structure against each question research strings are built for different search strings including, IEEE, ACM, GOOGLE SCHOLAR and SCIENCE DIRECT .

Data bases are created against each search strings and search protocol is applied on the data bases for final selection of papers, with help of data extraction forms data from each selected paper is extracted and reviewed statistically. Research Questions for Study

Research Question 1: How to make agile approaches scalable and adoptable for large projects?

Research Question 2: What are the existing methods, approaches, frameworks and practices support agile process in large scale projects?

Research Question 3: What are limitations of existing agile approaches, methods, frameworks and practices with reference to large scale projects?

II. Protocol for Search Process

After specifying research questions a review protocol is developed, this includes the definition of the following:

- The Search Process
- Inclusion And Exclusion Criteria
- The Selection Process
- The Data Extraction Process
- Data Synthesis

III. Sources (Digital Libraries) for Literature Search

The following databases are search out for primary studies Google Scholar, IEEE, Science Direct and ACM

IV. Research Questions in PICOC Structure

A. *RQ1: How to make agile approaches scalable and adoptable for large scale projects?*

- Population: Agile Approaches
- Intervention: Large scale projects
- Outcome: Parameters for scalability and adoptability

1) Search strings/Second Step: Synonyms

a) Population

"Agile Approaches "; "Agile software development approaches "; "Agile software development techniques "; "Agile software engineering"; "Agile software methodologies "; "Agile software engineering methodologies "; "Agile software development approaches "; "Agile software engineering methods "; "Agile software engineering methodologies "; "Agile software development processes "; "Agile software engineering practices".

b) Intervention

"Large scale Projects"; "Big scale Projects"; "Vast scale Projects"; "Large size Projects"; Big size Projects"; vast size Projects".

c) Outcome

"Parameters for scalability and adoptability"; "methods for scalability and adoptability"; ways for scalability and adoptability "; strategies for scalability and adoptability"

2) Search Strings Used for Primary Studies of Research question one

Database	Search String
IEEE	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND ("parameters for scalability and adoptability "OR "methods for scalability and adoptability "OR ways for scalability and adoptability "OR strategies for scalability and adoptability"'))
ACM	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND ("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND ("parameters for scalability and adoptability "OR "methods for scalability and adoptability "OR ways for scalability and adoptability "OR strategies for scalability and adoptability"'))
Science Direct	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND ("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND ("parameters for scalability and adoptability "OR "methods for scalability and adoptability "OR ways for scalability and adoptability "OR strategies for scalability and adoptability"'))
Google Scholar	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND ("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND ("parameters for scalability and adoptability "OR "methods for scalability and adoptability "OR ways for scalability and adoptability "OR strategies for scalability and adoptability"'))

B. RQ2: What are the existing methods, approaches, frameworks and practices support agile process in large scale projects?

1) Search strings/Second Step: Synonyms

a) Population

“Agile Approaches ”; “Agile software development approaches ”; “Agile software development techniques ”; “Agile software engineering”; “Agile software methodologies ”; “Agile software engineering methodologies ”; “Agile software development approaches ”; “Agile software engineering methods ”; “Agile software engineering methodologies ”; “Agile software development processes ”; “Agile software engineering practices”.

b) Intervention

“Large scale Projects”; “Big scale Projects”; “Vast scale Projects”; “Large size Projects”; Big size Projects”; vast size Projects”.

c) Outcome

“methods”; “approaches”; frameworks “; practices”.

2) Search Strings Used for Primary Studies of Research question Two

Database	Search String
IEEE	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“methods “OR “approaches “OR frameworks “OR practices ”’))
ACM	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“methods “OR “approaches “OR frameworks “OR practices ”’))
Science Direct	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“methods “OR “approaches “OR frameworks “OR practices ”’))
Google Scholar	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“methods “OR “approaches “OR frameworks “OR practices ”’))

C. RQ3: what are limitations of existing agile approaches, methods, frameworks and Practices with reference respect to large scale projects?

1) Search strings/Second Step: Synonyms

a) Population

“Agile Approaches ”; “Agile software development approaches ”; “Agile software development techniques ”; “Agile software engineering”; “Agile software methodologies ”; “Agile software engineering methodologies ”; “Agile software development approaches ”; “Agile software engineering methods ”; “Agile software engineering methodologies ”; “Agile software development processes ”; “Agile software engineering practices”.

b) Intervention

“Large scale Projects”; “Big scale Projects”; “Vast scale Projects”; “Large size Projects”; Big size Projects”; vast size Projects”.

c) Outcome

“Limitations of methods”; “limitations of approaches”;” limitations of frameworks “;” limitations of practices”.

2) Search Strings Used for Primary Studies Search Strings Used for Primary Studies of Research question Three

Database	Search String
IEEE	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“ limitations of methods “OR “ limitations of approaches “OR limitations of frameworks “OR limitations of practices ”’))
ACM	((““Agile Approaches ”OR “Agile software development approaches ”OR “Agile software development techniques ”OR “Agile software engineering “OR “Agile software methodologies ”OR “Agile software engineering methodologies ”OR “Agile software development approaches ”OR “Agile software engineering methods ”OR “Agile software engineering methodologies ”OR “Agile software development processes OR “Agile software engineering practices” AND (“Large scale Projects” OR “Big scale Projects ” OR “Vast scale Projects” OR “Large size Projects” OR Big size Projects” OR vast size Projects”) AND (“ limitations of

	methods "OR " limitations of approaches "OR limitations of frameworks "OR limitations of practices ""))
Science Direct	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND ("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND (" limitations of methods "OR " limitations of approaches "OR limitations of frameworks "OR limitations of practices ""))
Google Scholar	((""Agile Approaches "OR "Agile software development approaches "OR "Agile software development techniques "OR "Agile software engineering "OR "Agile software methodologies "OR "Agile software engineering methodologies "OR "Agile software development approaches "OR "Agile software engineering methods "OR "Agile software engineering methodologies "OR "Agile software development processes OR "Agile software engineering practices" AND ("Large scale Projects" OR "Big scale Projects " OR "Vast scale Projects" OR "Large size Projects" OR Big size Projects" OR vast size Projects") AND (" limitations of methods "OR " limitations of approaches "OR limitations of frameworks "OR limitations of practices ""))

V. Publication Quality Assessment

The data extraction form is designed as it will extract the data form finally selected papers assessing their quality and searching answers for research questions.

Detail of quality assessment 1-5:

Study provides detailed description of agile scalability? The possible answers to this question are: ''Yes (+1)'' if the paper provides detail description of agile scalability; ''partially (0)'' if the paper provides partial or not detail information about agile scalability; and ''No (_1)'' if the paper does not provide any information about agile scalability.

The study provides the guideline as how the agile techniques are used in large size projects? The possible answers to this question are: ''Yes (+1)'' if the paper provides information as how the agile techniques are used in large size projects; ''partially (0)'' if the paper provides partial or not detail information as how the agile techniques are used in large size projects; and ''No (_1)'' if the paper does not provide any information as how the agile techniques are used in large size projects.

The study provides clear results after application of agile techniques in large size projects?

The possible answers to this question are: ''Yes (+1)'' if the paper provides clear results; ''partially (0)'' if the paper provides partial or not detail results; and ''No (_1)'' if the paper does not provide any results.

The study has been published in a relevant journal or conference proceedings. The possible answers to this question are: ''Very relevant'' (+1), ''Relevant (0)'', and ''Not so relevant (_1)''.

This question will be rated by considering the order of relevance provided by the digital library, the CORE conference ranking (A, B and C conferences), and the Journal Citation Reports (JCR) lists.

The study has been cited by other authors. The possible answers to this question are: ''Yes (+1)'' if the paper has been cited by more than five authors; ''partially (0)'' if the paper has been cited by 1–5 authors; and ''No (_1)'' if the paper has not been cited. This question was rated by considering the Google scholar citations count.

TABLE I. Data Extraction form

Paper Title:	
Authors:	Year of Publication:
Reference Type: Journal/Conference/Thesis/Unpublished	Publisher: IEEE/ACM/Google Scholar/Science Direct
Quality Assessment	**(1)** **(0)** **(-1)**
Study provides detailed description of agile scalability?	
The study provides the guideline as how the agile techniques are used in large size projects?	
The study provides clear results after application of agile techniques in large size projects?	
The study has been published in a relevant journal or conference?	
The study has been cited by other authors?	
Data extraction for Questions	Answers
What methods have been employed by researchers to make Agile scalable for large size projects?	
1.1. Phase(s) of software process in which the Agile techniques are applied for scalability?	Requirement Design Implementation Testing Maintenance
1.2. Which Agile technique has been reported in this study?	Technique Name
1.3. Data characteristics	Academia mixed Industrial

	Government
Research detects agile limitations for large size project?	Documentation Time period Budget Human resources Coordination Distributed environment others
Empirical Validation of the agile techniques applied in large size projects.	Case Study Experiment Survey experience reports observational study, survey action research No
Remarks:	

VI. General Information Regarding Research Paper

The below table represent the general information of papers studied in the SLR process all these papers were finalized for study process, so that the specific information from theses papers can be gathered according to the research questions designed.

TABLE II. General Information Regarding Research Paper

Sr. No	General information regarding research papers				
	Title	**Author(s)**	**Database**	**Journal ./Conf./ Work.**	**Year**
1	Identifying some important success factors in adopting agile software development practices	Subhas Chandra Misra a, Vinod Kumar b, Uma Kumar b	ACM	Journal	2009
2	Strengths and barriers behind the successful agile deployment—insights from the three software intensive companies in Finland	Minna Pikkarainen & Outi Salo & Raija Kuusela & Pekka Abrahamsson	ACM	Journal	2011
3	Acceptance of agile methodologies: A critical review and conceptual framework	Frank K.Y. Chan, James Y.L. Thong	Google Scholar	Journal	2008
4	A Study of the Agile Software Development Methods, Applicability and Implications in Industry	Kuda Nageswara Rao, G. Kavita Naidu, Praneeth Chakka	Google Scholar	Conference	2011
5	‘State of the Art’ in Using Agile Methods for Embedded Systems Development	Jayakanth Srinivasan, Radu Dobrin, Kristina Lundqvist	Google Scholar	Journal	2009
6	An Empirical Study: Understanding Factors and Barriers for Implementing Agile Methods in Malaysia	Ani Liza Asnawi, Andrew M Gravell, Gary B Wills	Google Scholar	Conference	2010
7	Distributed Scrum: Agile Project Management with Outsourced Development Teams	Jeff Sutherland, Anton Viktorov, Jack Blount,Nikolai Puntikov	Google Scholar	Conference	2007
8	Agile methods in European embedded software development organizations: a survey on the actual use and usefulness of Extreme Programming and Scrum	O. Salo and P. Abrahamsson	Google Scholar	Conference	2007
9	The Impact of Scaling on Planning Activities in an Agile Software Development Context	Hubert Smits	Google Scholar	Conference	2007
10	Rolling out Agile in a Large Enterprise	Gabrielle Benefield	Google Scholar	Conference	2008
11	An Appraisal of Existing Evaluation Frameworks for Agile Methodologies	Masoumeh Taromirad, Raman Ramsin	Google Scholar	Conference	2008
12	Implementing Program Model with Agile Principles in a Large Software Development Organization	Maarit Laanti	Google Scholar	Conference	2008
13	A Soft-Structured Agile Framework for Larger Scale Systems Development	Shvetha Soundararajan and James D. Arthur	Google Scholar	Conference	2009
14	FORMAL VERSUS AGILE: SURVIVAL OF THE FITTEST?	Sue Black, Paul P. Boca, Jonathan P. Bowen, Jason Gorman, Mike Hinchey,	Google Scholar	Conference	2009
15	Agile Adoption Experience : A Case	Hassan Hajjdiab and	Google Scholar	Thesis	2011

	Study in the U.A.E	Al Shaima Taleb			
16	Agile Method to Improve Delivery of Large-Scale Software Projects	Mary Wu	Google Scholar	Journal	2011
17	IBM agility @scale™: Become as Agile as You Can Be	By Scott W. Ambler Chief Methodologist for Agile and Lean, IBM Rational	Google Scholar	Conference	2010
18	Agile Framework for Globally Distributed Development Environment (The DAD Model)	Rehan Akbar , Muhammad Haris , Majid Naem	Google Scholar	Journal	2008
19	Complex software project development: agile methods adoption	Deepti Mishra?,† and Alok Mishra-fan Dai and Ming-li Wang	Google Scholar	Journal	2011
20	Designing an Information Systems Development Course to Incorporate Agility, Flexibility, and Adaptability	Chuan-Hoo Tan Wee-Kek Tan Hock-Hai Teo	Google Scholar	Journal	2009
21	Innovation and Scaling up Agile Software Engineering Projects	Sita Ramakrishnan	Google Scholar	Thesis	2009
22	Agile Software Development in the Large	Jutta Eckstein	Google Scholar	Conference	2008
23	Agile Framework for Globally Distributed Development Environment (The DAD Model)	Reahan Akbar, Muhammad Haris and MajidNaeem	Google Scholar	Conference	2008
24	Scrum Practices in Global Software Development: A Research Framework	Mohammed Abdullah Alnuem, Arshad Ahmad and Hashim Khan	Google Scholar	Conference	2009
25	Usage and Perceptions of Agile Software Development in an Industrial Context: An Exploratory Study Agile methods for cloud computing	Emam Hossain, Paul L. Bannerman, and D. Ross Jeffery	IEEE	Conference	2008
26	Agile Software Product Lines - A Working Session Designing an information systems development course to incorporate agility, flexibility, and adaptability	Andrew Begel, Nachiappan Nagappan	IEEE	Conference	2009
27	Using XP in Telecommunication Software Development	John D. McGregor	IEEE	Conference	2009
28	Experiences Applying Agile Practices to Large Systems	Ensar Gul Multitek Arge Istanbul,Turkey	IEEE	Conference	2009
29	A Heavy Weight IT Project Management Framework based on Agile Theory	Harry Koehnemann,	IEEE	Conference	2010
30	ESCAPE THE WATERFALL: AGILE FOR AEROSPACE	Chen jianbin Business	IEEE	Conference	2010
31	Enterprise Scrum: Scaling Scrum to the Executive Level	Steven H. VanderLeest,	IEEE	Conference	2011
32	Agility in a Large-Scale System Engineering Project: A Case-Study of an Advanced Communication System Project	Daniel R. Greening	IEEE	Conference	2009
33	Software Development as a Service: Agile Experiences	Amir Shatil Haifa, Israel	IEEE	Conference	2012
34	Agile Way of BI Implementation	Tobin J. Lehman	IEEE	Conference	2012

35	The Many Lives of an Agile Story: Design Processes, Design Products, and Understandings in a Large-Scale Agile Development Project	Bhawna Rehani	IEEE	Conference	2011
36	Understanding the Impact of Pair Programming on Developers Attention A Case Study on a Large Industrial Experimentation	Aaron Nebraska Omaha	IEEE	Conference	2013
37	Scrum Goes Formal: Agile Methods for Safety-Critical Systems Distributed agile development: using Scrum in a large project	Alberto Sillitti, Bozen Bozen	IEEE	Conference	2013
38	Agile Software Development Methodology for Medium and large size projects	Sune Wolff Terma A/S	IEEE	Conference	2013
39	Agile Methods for Cloud Computing	M.Rizwan Jameel Quereshi	IEEE	Conference	2012
40	Extreme Programming Applied in a Large-scale Distributed System	S. Kalem, D. Donko and D. Boskovic	IEEE	Conference	2014
41	The impact of agile principles and practices on large- scale software development projects A multiple-case study of two projects at Ericsson	Elmuntasir Abdullah, El-Tigani B. Abdelsatir	IEEE	Conference	2014
42	Towards an Agile Feature Composition for a Large Scale Software Product Lines	Lina Lagerberg, Tor Skude, Pär Emanuelsson and Kristian	IEEE	Journal	2007
43	Categorization of risk factors for distributed agile projects	Ikram Dehmouch Mohammed V Souissi	Science Direct	Journal	2008
44	Process fusion: An industrial case study on agile software product line engineering	Suprika V. Shrivastava ?, Urvashi Rathod 1	Science Direct	Journal	2011
45	A framework to support the evaluation, adoption and improvement of agile methods in practice	Geir K. Hanssen a, b,*, Tor E. Fægri	Science Direct	Journal	2012
46	"Leagile" software development: An experience report analysis of the application of lean approaches in agile software development	A. Qumer, B. Henderson-Sellers *	Science Direct	Journal	2013
47	Agile requirements prioritization in large-scale outsourced system projects: An empirical study	Xiaofeng Wanga? Kieran Conboyb , Oisin Cawleyc	Science Direct	Journal	2014
48	A critical examination of recent industrial surveys on agile method usage	Maya Danevaa, Egbert van der Veena, Amrita,?, Smita Ghaisasb, Klaas Sikkela, Ramesh	Science Direct	Journal	2013
49	When agile meets the enterprise	Stavros Stavru?	Science Direct	Journal	2014
50	Towards a governance framework for chains of Scrum teams	Guus van Waardenburg b, Hans van Vliet a,?	Science Direct	Journal	2013
51	Operational release planning in large-scale Scrum with multiple stakeholders – A longitudinal case study at F-Secure Corporation	Jan Vlietland a, Hans van Vliet b?	Science Direct	Journal	2014

The above information and the graphical results are gathered from the references.[9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64].

VII. Graphical Representation of Results (SLR) and Specific Information Regarding Research Paper

Q# 4: Source of publication

Options	Response Percentage	Responses
Journal	35%	18
Conference	61%	31
Thesis	4%	2
Unpublished	0%	0

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.686 Std. Deviation: 0.542 Satisfaction Rate:22.876 Variance: 0.294 Std. Error: 0.076

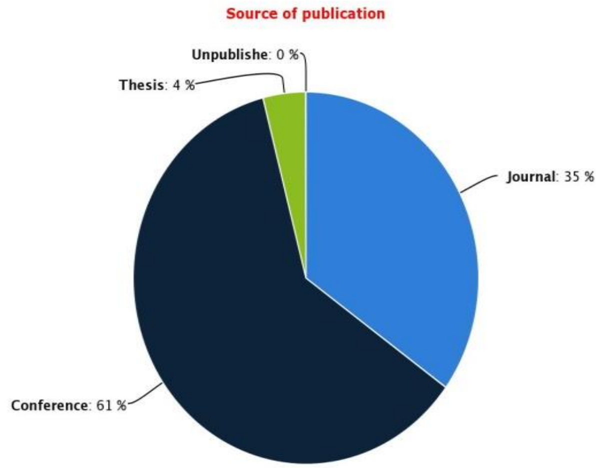


Fig. 1. Source of publication of the paper is?

Q# 5: Publisher:

Options	Response Percentage	Responses
IEEE	37%	19
ACM	4%	2
Science Direct	18%	9
Google Schoolor	43%	22

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 2.706 Std. Deviation: 1.344 Satisfaction Rate:55.128 Variance: 1.806 Std. Error: 0.186

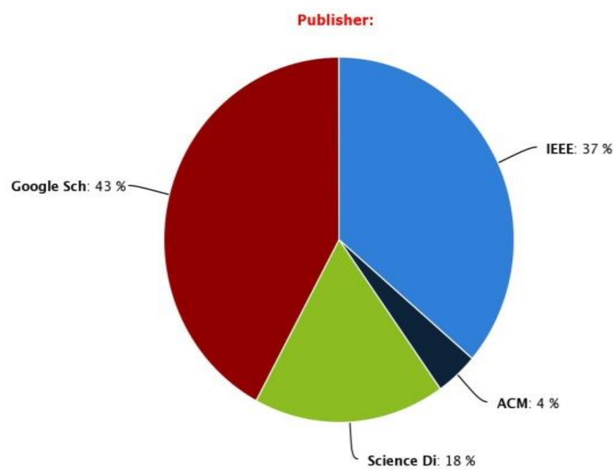


Fig. 2. The study provides information about the publisher of the research papers

Q# 6: Study provides detailed description of agile scalability?

Options	Response Percentage	Responses
1	67%	34
0	33%	17
-1	0%	0

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.333 Std. Deviation: 0.471 Satisfaction Rate:16.667 Variance: 0.222 Std. Error: 0.066

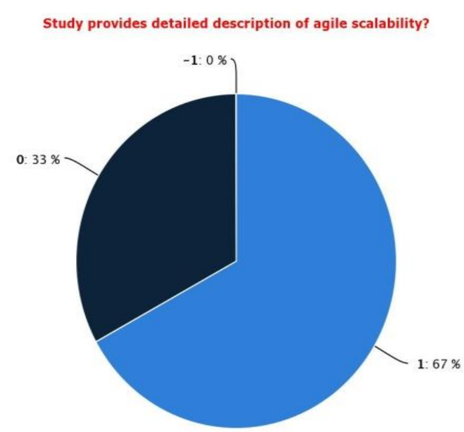


Fig. 3. Study provides detail description of agile scalability

Q# 7: The study provides guideline as how Agile techniques are used in large size projects?

Options	Response Percentage	Responses
1	71%	36
0	27%	14
-1	2%	1

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.314 Std. Deviation: 0.505 Satisfaction Rate:15.686 Variance: 0.255 Std. Error: 0.071

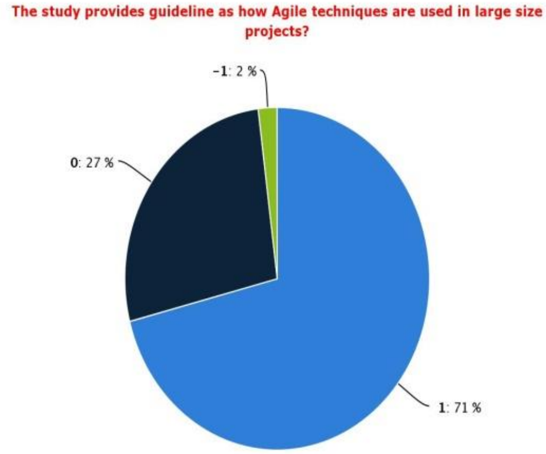


Fig. 4. The study provides guideline as how agile techniques are used in large size projects

Q# 8: The study provides clear results after application of agile techniques in large size projects?

Options	Response Percentage	Responses
1	71%	36
0	29%	15
-1	0%	0

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.294 Std. Deviation: 0.456 Satisfaction Rate:14.706 Variance: 0.208 Std. Error: 0.064

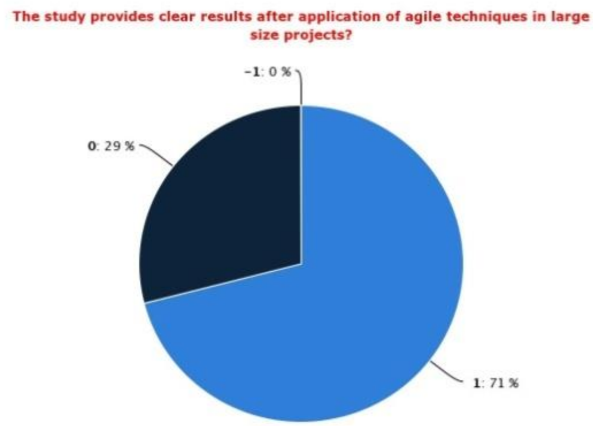


Fig. 5. The study provides clear results after application of agile techniques in large size projects

Q# 9: The study has been published in a relevant journal or conference?

Options	Response Percentage	Responses
1	98%	50
0	2%	1
-1	0%	0

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.02 Std. Deviation: 0.138 Satisfaction Rate:0.98 Variance: 0.019 Std. Error: 0.019

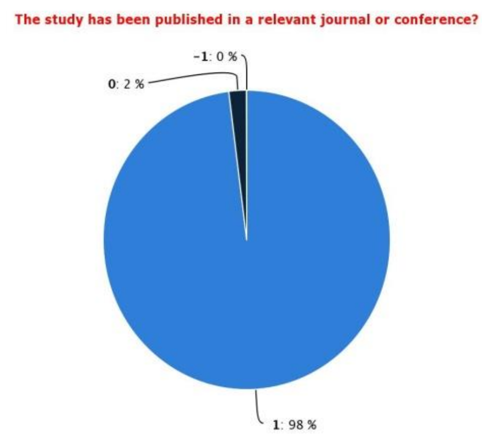


Fig. 6. The study has been published in a relevant journal or conference

Q# 10: The study has been cited by other authors?

Options	Response Percentage	Responses
1	96%	49
0	4%	2
-1	0%	0

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 1.039 Std. Deviation: 0.195 Satisfaction Rate:1.961 Variance: 0.038 Std. Error: 0.027

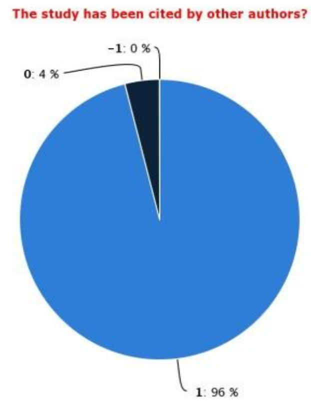


Fig. 7. The study has been cited by authors

Q# 15: Empirical Validation of the agile techniques applied in large size projects.

Options	Response Percentage	Responses
Case study	51%	26
Experiment	6%	3
Survey	16%	8
Experience Report	22%	11
Observational Study	31%	16
Action Research	0%	0
Other	4%	2

Total Responses: 51 Answered Responses: 51 Skipped Responses: 0

Mean: 3.804 Std. Deviation: 1.996 Satisfaction Rate:32.323 Variance: 3.986 Std. Error: 0.246

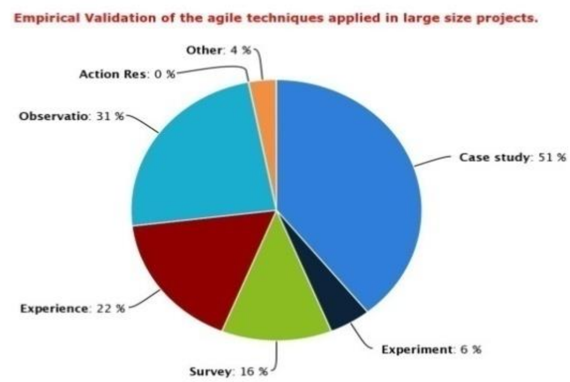


Fig. 8. Empirical validation of agile techniques in large sized projects

VIII. Conclusion

In this SLR performed on agile scalability and adaptability three research questions were made on basis of these three questions research strings were designed using PICOC structure to extract research papers from different data bases including IEEE, Google Scholar, ACM and Science Direct .Search protocol was designed for setting studies rules regulations to follow for summarize and concrete results after analysis.

Inclusion and Exclusion criteria was applied on these selected data bases of papers on basis of set protocol .Papers were selected iteration wise against each research question from these finalized data bases 51 papers were selected ,these selected papers were analysed , reviewed and data was extracted based on questions designed in data extraction form.

The study summarized that different researchers made efforts for agile scalability; different techniques of agile scalability are applied for covering agile limitations for scalability limitations.

The gathered data is statistically analysed and according to this analysis research papers selected for study were taken between 2009 -2011 ,out of 100 percent 35 percent papers were published in journal 61 percent in conference and 4 percent were thesis publications.

While 37 percent paper's publisher was IEEE, 4 percent ACM, Science Direct was publisher of 18 percent and 43 percent papers were published by Google Scholar.

Form all these selected papers 67 percent papers in detail describe agile adoptability and scalability, 33 percent papers partially discussed the issue .From papers that were answering about agile techniques application 71 percent studies in detail describe the agile techniques application on large scale projects, 27 percent studies partially describe the techniques application and just 2 percent papers are not describing any technique at all.

In SLR 79 percent studies provide clear results of agile application on large size projects, 29 percent are partially providing results of applications, according to analysis, main factor we found was that 88 percent techniques were applied in implementation phase for agile scalability.

Research detect agile limitations for large size projects this question was answered by different researchers and 24 percent researchers said documentation is a limitation for agile practices in large scale projects, 22 percent were saying about time period as a limitation for agile approaches in large scale projects, 14 percent were saying about budget overflow issues in large scale projects while applied agile techniques,14 percent were talking about human resources related problems in large scale projects while applied agile approaches.

In SLR conducted 33 percent were talking about team coordination and communication issues and 25 percent were saying that distributed teams are creating limitation for agile applications in large size projects. From these results it is clear that researchers are working on agile scalability and adaptability for large size projects.They are trying to find the exiting limitations as faced by large scale projects while agile approaches are used. They are also working on remedial strategies for agile scalability problems compensation ion large projects.

The aim of this SLR conducted was performing a detailed analysis of the limitations of agility in large size projects and analyzing the existing remedial work and its limitations. From here we extract detail problems analysis, current strategies presents their limitations.We are statistically able to judge the problems, their nature and affect on large size projects

IX. Future Work

In future on the basis of these detailed limitations identified in SLR faced by agile approaches some remedial work has to be proposed to handle the highlighted limitations.

References

[1] Hamed, A.M.M.; Abushama, H., (Aug. 2013). Popular agile approaches in software development: Review and analysis. Computing, Electrical and Electronics Engineering (ICCEEE), 2013 International Conference. pp.160,166, 26-28 .

[2] Miller, (2011). The Characteristics of Agile Software Processes. Granville Together Soft. Proceedings of the 39th Int'l Conf. and Exhibition on Technology of Object-Oriented Languages and Systems (TOOLS'01),1530-2067/01 $10.00 © 2001 IEEE

[3] Dot Tudor and George A. Walte, (2006). Using an Agile Approach in a Large, Traditional Project. Proceedings of the conference on AGILE ,

[4] Alistair Cockburn, (2001). Book Software Engineering. 1st ed.: Editors copyright Alistair Cockburn.

[5] Dan Turk and Robert France, (2002). Limitations of Agile Software Processes. IN PROCEEDINGS OF THE THIRD INTERNATIONAL CONFERENCE ON EXTREME PROGRAMMING AND FLEXIBLE PROCESSES IN SOFTWARE ENGINEERING (XP).

[6] ProjectVille T. Heikkil¨a, Maria Paasivaara and Casper Lassenius , (2013). Scrum But, but Does It Matter? A Mixed-Method Study of the Planning Process of a Multi-Team Scrum. ACM / IEEE International Symposium on Empirical Software Engineering and Measurement..

[7] Brian Fitzgerald_, Klaas-Jan Stol_, Ryan O'Sullivan†, and Donal O'Brien† _Lero, (2013). Scaling Agile Methods to Regulated Environments: An Industry Case Study . The Irish Software Engineering Research Centre, University of Limerick, Ireland †QUMAS, Cleve Business Park, Monahan Road, Cork, Ireland.

[8] Moore, E.; Spens, J, (Aug. 2008). Scaling Agile: Finding your Agile Tribe. Agile, 2008. AGILE '08. Conference. pp.121, 124.

[9] N. Maiden, (2013). Extending Agile Processes with Creativity Techniques. IEEE Computer Society, B. Hollis , City Univ. London, London, UK. 30, pp.: 78-84

[10] David Bustard , George Wilkie, Des Greer, (2013). The Maturation of Agile Software Development Principles and Practice. ECBS '13 Proceedings of the 20th Annual IEEE International Conference and Workshops on the Engineering of Computer Based Systems IEEE Computer Society Washington, DC, USA.

[11] Aziz Nanthaamornphong, Karla Morris, Damian W. I. Rouson, Hope A. Michelsen, (2013). A case study: agile development in the community laser-induced incandescence modeling environment (CLiiME). Proceeding SE-CSE '13 Proceedings of the 5th International Workshop on Software Engineering for Computational Science and Engineering . ISBN: 978-1-4673-6261-0 , pp.9-18

[12] Lagerberg, L. Skude, T. ; Emanuelsson, P. ; Sandahl, K. ; Stahl, D., (2013). The impact of agile principles and practices on large scale software development projects A multiple-case study of two projects at Ericsson . ACM / IEEE International Symposium on Empirical Software Engineering and Measurement..

[13] Ben Othmane, L.; Angin, P.; Weffers, H.; Bhargava, B., , (2014). Extending the Agile Development Process to Develop Acceptably Secure Software,. Dependable and Secure Computing, IEEE Transactions. 11 (6), pp.497,509

[14] Antinyan, V.; Staron, M.; Meding, W.; Osterstrom, P.; Wikstrom, E.; Wranker, J.; Henriksson, A.; Hansson, J, (2014). Identifying risky areas of software code in Agile/Lean software development: An industrial experience report. Software Maintenance, Reengineering and Reverse Engineering (CSMR-WCRE), 2014 Software Evolution Week - IEEE Conference . (), pp.154,163

[15] Scheerer, A.; Hildenbrand, T.; Kude, T., (2014). Coordination in Large-Scale Agile Software Development: A Multiteam Systems Perspective. System Sciences (HICSS), 2014 47th Hawaii International Conference ..pp.4780,4788,

[16] Olsson, H.H.; Bosch, J.; Alahyari, H.,, (2013). Customer-Specific Teams for Agile Evolution of Large-Scale Embedded Systems. Software Engineering and Advanced Applications (SEAA), 2013 39th EUROMICRO Conference,pp.82,89.

[17] Farrow, A.; Greene, S, (2008). Fast & Predictable A Lightweight Release Framework Promotes Agility through Rhythm and Flow. Agile, 2008. AGILE '08. Conference , pp.224,228.

[18] Blau, B.; Hildenbrand, T, (2011). Product Line Engineering in Large-Scale Lean and Agile Software Product Development Environments - Towards a Hybrid Approach to Decentral Control and Managed Reuse. Availability, Reliability and Security (ARES), 2011 Sixth International Conference , pp.404,408 .

[19] Khan, M.I.; Qureshi, M.A.; Abbas, Q.(2010). Agile methodology in software development (SMEs) of Pakistan software industry for successful software projects (CMM framework). (ICENT), 2010 International Conference, pp.576, 580.

[20] Pearl Brereton a,*, Barbara A. Kitchenham a, David Budgen b,Mark Turner a, Mohamed Khalil c, (2006). Lessons from applying the systematic literature review process within the software engineering domain. Department of Computer Science, Durham University, Durham, Science Laboratories, South Road, Durham City, DH1 3LE, UKc Department of Computer Sciences, University of Khartoum, P.O. Box 321, Khartoum, Sudan.

[21] Subhas C. Misra, Vinod Kumar, Uma Kumar, (2009). Identifying some important success factors in adopting agile software development practices. Journal of Systems and Software. 82 pp.1869-1890

[22] Minna Pikkarainen & Outi Salo & Raija Kuusela & Pekka Abrahamsson, (2011). Strengths and barriers behind the successful agile deployment—insights from the three software intensive companies in Finland. Springer Science+Business Media.

[23] Frank K.Y. Chan, James Y.L. Thong , (2009). Acceptance of agile methodologies: A critical review and conceptual framework. Department of Information Systems, Business Statistics and Operations Management, School of Business and Management, Hong Kong University of Science and Technology, Clear Water Bay, Kowloon, Hong Kong .

[24] Kuda Nageswara Rao, G. Kavita Naidu, Praneeth Chakka , (2011). A Study of the Agile Software Development Methods, Applicability and Implications in Industry . International Journal of Software Engineering and Its Applications. 5.

[25] [Mengjiao Shen; Wenrong Yang; Guoping Rong; Dong Shao, (2012). Applying agile methods to embedded software development: A systematic review," Software Engineering for Embedded Systems (SEES),. 2nd International Workshop. Pp.30-36.

[26] Smits, H, (2007). The Impact of Scaling on Planning Activities in an Agile Software Development Center,. 40th Annual Hawaii International Conference , pp.274c.

[27] Salo, O.; Abrahamsson, P, (2008). Agile methods in European embedded software development organizations: a survey on the actual

use and usefulness of Extreme Programming and Scrum, Software, IET. 2 pp.58 and 64.

[28] Gabrielle Benefield, (2008). Rolling out Agile in a Large Enterprise. Proceedings of the 41st Hawaii International Conference on System Sciences.

[29] Taromirad, M.; Ramsin, R, (2008), An Appraisal of Existing Evaluation Frameworks for Agile Methodologies, Engineering of Computer Based Systems, ECBS 2008. 15th Annual IEEE International Conference and Workshop pp.418, 427.

[30] Laanti, M, (2008) Implementing Program Model with Agile Principles in a Large Software Development Organization,Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International, pp.1383, 1391.

[31] Soundararajan, S.; Arthur, J.D.,(2009) A Soft-Structured Agile Framework for Larger Scale Systems Development," Engineering of Computer Based Systems,. ECBS 2009. 16th Annual IEEE International Conference and Workshop pp.187, 195.

[32] E. Murphy-Hill, L. Williams, (2003), Agile software development: it's about feedback and change, North Carolina State University; Computer; 36(6): DOI: 10.1109/MC.2003.1204373 Source: IEEE Xplore, pp. 39-43.

[33] Hajjdiab, H.; Taleb, A.S.,(2011) , Agile adoption experience: A case study in the U.A.E, Software Engineering and Service Science (ICSESS), 2011 IEEE 2nd International Conference on , vol., no., pp.31,34, 15-17 July 2011 doi: 10.1109/ICSESS.2011.5982247

[34] Mary Wu, (2011), Agile Method to Improve Delivery of Large-Scale Software Projects, Presented to The Faculty of the Department of General Engineering Son Jose State University.

[35] W. Ambler , (2011). Methodologist for Agile and Lean, IBM Rational IBM agility@scale™: Become as Agile as You Can Be . 1st ed.

[36] Deepti Mishra∗,† and Alok Mishra, (2011). Complex software project development: agile methods adoption . JOURNAL OF SOFTWARE MAINTENANCE AND EVOLUTION: RESEARCH AND PRACTICE J. Softw. Maint. Evol.: Res. Pract. (2011) . (), pp.

[37] Reifer, D.J, (2003). XP and the CMM," Software. IEEE. 20 , pp.e.g. 14-15.

[38] Paulk, M.C,(2011) , Extreme programming from a CMM perspective, Software, IEEE , vol.18, no.6, pp.19,26.

[39] Elssamadisy A, (2001), XP on a large project—A developer's view, Proceedings of XP/Agile Universe, Raleigh NC, 2001.

[40] Petersen K, Wohlin C, (2009), A comparison of issues and advantages in agile and incremental development between state of the art and an industrial case, Journal of Systems and Software 2009; 82(9), pp. 1479–1490.

[41] Soundararajan S, Arthur JD, (2009). A soft-structured agile framework for larger scale systems development.. Proceedings of the 2009 16th Annual IEEE international Conference and Workshop on the Engineering of Computer Based Systems.ECBS. IEEE Computer Society: Washington DC, 2009; 187195.

[42] Sidky A, Arthur J, (2007). Determining the applicability of agile practices to mission and life-critical systems. Proceedings of the 31st IEEE Software Engineering Workshop,(SEW 2007). IEEE Computer Society: Reading MA, 2007; 3–12. DOI: 10.1109/SEW.2007.61.

[43] Chuan-Hoo Tan , Wee-Kek Tan , Hock-Hai Teo Hock-Hai Teo , (2013). Designing an Information Systems Development Course to Incorporate Agility, Flexibility, and Adaptability . Volume 26 Article 10 . (), pp.

[44] Jutta Eckstein , (2009). Agile Software Development in the Large Encontro Ágil . Large Encontro Ágile. ISBN 0-932633-57-9 (), pp.233

[45] REHAN AKBAR, MUHAMMAD HARIS, MAJID NAEEM, (2008). Agile Framework for Globally Distributed Development Environment (The DAD Model) . 8th WSEAS International Conference on APPLIED INFORMATICS AND COMMUNICATIONS (AIC'08) . (), pp.

[46] Abbass Ghanbary , (2010). Success of Agile Environment in Complex Projects. Edith Cowan University Research Online Australian Information Warfare and Security Conference.. (), pp.

[47] Begel, A.; Nagappan, N, (2007). Usage and Perceptions of Agile Software Development in an Industrial Context: An Exploratory Study. Empirical Software Engineering and Measurement, 2007. ESEM 2007. First International Symposium. (), pp.255-264 , doi: 10.1109/ESEM.2007.12 .

[48] Isham M, (2008). Agile Architecture IS Possible You First Have to Believe. Agile, 2008. AGILE '08. Conference. (), pp.484,489 , doi: 10.1109/Agile.2008.16.

[49] John D. McGregor , (2008). Agile Software Product Lines - A Working Session. 12th International Software Product Line Conference IEEE Computer Society Washington, DC, USA ©2008. ISBN: 978-0-7695-3303-2 , doi:10.1109/SPLC.2008.60.

[50] Gul, E.; Sekerci, T.; Yuceturk, A.C.; Yildirim, U, (2008). Using XP in Telecommunication Software Development. Software Engineering Advances, 2008. ICSEA '08. The Third International Conference . e.g. 32 (), pp.258,263. doi: 10.1109/ICSEA.2008.11

[51] Jianbin; Shi Tong; Fang Deying, (2009). A Heavy Weight IT Project Management Framework Based on Agile Theory. Management and Service Science, 2009. MASS '09. International Conference . (), pp.1-5 , doi: 10.1109/ICMSS.2009.5301737.

[52] VanderLeest, S.H.; Buter, A, (2009). Escape the waterfall: Agile for aerospace. Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th. (), pp.6 doi: 10.1109/DASC.2009.5347438.

[53] Lehman, T.J.; Sharma, A, (2011) , Software Development as a Service: Agile Experiences, SRII Global Conference (RII), 2011 Annual , vol., no., pp.749,758, March 29 2011-April 2 2011 doi: 10.1109/SRII.2011.82.

[54] Read, A.; Briggs, R.O, (2012) , The Many Lives of an Agile Story: Design Processes, Design Products, and Understandings in a Large-Scale Agile Development Project, System Science (HICSS), 2012 45th Hawaii International Conference on , vol., no., pp.5319,5328, 4-7 Jan. 2012 , doi: 10.1109/HICSS.2012.684.

[55] S. Kalem, D. Donko and D. Boskovic , (2013). Agile Methods for Cloud Computing . Faculty of Electrical Engineering, University of Sarajevo, Bosnia and Herzegovina . (), pp.

[56] Suprika V. Shrivastava ⇑, Urvashi Rathod , (2015). Categorization of risk factors for distributed agile projects. Symbiosis Centre for Information Technology (SCIT), Symbiosis International University (SIU), Rajiv Gandhi Infotech Park, Hinjewadi, Pune 411 057, Maharashtra, India. Information and Software Technology journal homepage. 58 (), pp.

[57] Geir K. Hanssen a,b,*, Tor E. Fægri a , (2007). Process fusion: An industrial case study on agile software product line engineering . SINTEF ICT, NO-7465 Trondheim, Norway b Norwegian University of Science and Technology, Department of Computer and Information Science, NO-7491 Trondheim, Norway . (), pp.

[58] A. Qumer, B. Henderson-Sellers , (2008). A framework to support the evaluation, adoption and improvement of agile methods in practice. Faculty of Information Technology, University of Technology, Sydney, P.O. Box 123, Broadway 2007, Australia. (), pp.

[59] Xiaofeng Wanga,∗, Kieran Conboyb, (2012). Leagile" software development: An experience report analysis of the applicationof lean approaches in agile software development. Oisin Cawleyca Free University of Bozen/Bolzano, Italyb School of Information Systems, Technology and Management, UNSW, Sydney 2052, Australiac Lero, The Irish Software Engineering Research Centre, Ireland The Journal of Systems and Software . 85 (), pp.

[60] Stavros Stavru∗,St. Kliment Ohridski, (2014). A critical examination of recent industrial surveys on agile method usage . The Journal of Systems and Software 94 (2014) 87–97 , pp.

[61] Guus van Waardenburg b, Hans van Vliet a, (2013). When agile meets the enterprise . a VU University Amsterdam, De Boelelaan 1081, 1081 HV Amsterdam, The Netherlands b Avanade Netherlands, Versterkerstraat 6, 1322 AP Almere, The Netherlands Information and Software Technology 55 (2013) 2154–2171.. (), pp.

[62] Jan Vlietland a, Hans van Vliet b,⇑, (2015). Towards a governance framework for chains of Scrum teams. The Netherlands b Department of Computer Science, VU University Amsterdam, Amsterdam, the Netherlands. Information and Software Technology 57 (2015) 52–65.. (), pp.

[63] Hina Saeeda , Fahim Arif (20150 Agile Scalability for Large Scale Projects: Lessons Learned. Computer Software Department MCS NUST, JSW 2015 Vol.10(7):893-903ISSN:1796-217X doi: 10.17706//jsw.10.7.893-903

[64] HINA SAEEDA , FAHIM ARIF (20150 AGILE SCALABILITY FOR LARGE SCALE PROJECTS: LESSONS LEARNED. COMPUTER SOFTWARE DEPARTMENT MCS NUST, JSW 2015 VOL.10(7):893-903ISSN:1796-217X DOI: 10.17706//JSW.10.7.893-903

AUTHOR PROFILE

Hina Saeeda received her BS (CS) degree in 2011 from the Arid Agriculture University and received MS in Software Engineering degree from NUST, Pakistan in 2015. Her current research interests include agile software Engineering, and usability engineering. She is a lecturer of Computer Sciences by profession.

Hannan Khalid received his BS (hons) degree in Computer Science in 2012 from the Arid Agriculture University and is now conducting research towards completion of his Masters' degree in Software Engineering from COMSATS Institute of Information technology, Islamabad, Pakistan. His current research interests include information system theories, and techniques for requirement engineering. He started his professional career in 2013 as a software quality assurance engineer and has worked with multiple projects since then.

Mukhtar Ahmed is doing MS in Software Engineering from COMSATS Institute Of Information Technology, Islamabad, Pakistan. He did his BS in Software Engineering from university of Azad Jammu and Kashmir in 2011. His allegiance to work and preeminent nature guided him to learn different research issues from different platforms. His research interests are information system, and Global software development (GSD).

Abu Sameer earned his Bachelor's in Software Engineering in 2013 from University Of Sargodha Pakistan. He completed his MS degree in Software Engineering form COMSATS Institute of Information Technology, Islamabad, Pakistan in 2015. He has an affirm attitude towards research and is working as a research assistant. Moreover he is an active adroit member of Agile Software Development research committee at COMSATS Institute Of Information Technology Islamabad Pakistan.

Fahim Arif was born in 1967, is currently professor at MCS-NUST Pakistan. He received Master in Sciences in Computer Software Engineering degree from National University Science and Technology, Islamabad in 2003. He has completed his PhD degree from National University Science and Technology in 2009.His research interest is quality assurances, software engineering and image processing.

The Apsidal Precession for Low Earth Sun Synchronized Orbits

Shkelzen Cakaj
Faculty of Electrical and Computing Engineering,
University of Prishtina,
Prishtina, Kosovo

Bexhet Kamo, Algenti Lala, Ilir Shinko, Elson Agastra
Faculty of Information Technology,
Polytechnic University of Tirana,
Tirana, Albania

***Abstract*—By nodal regression and apsidal precession, the Earth flattering at satellite low Earth orbits (LEO) is manifested. Nodal regression refers to the shift of the orbit's line of nodes over time as Earth revolves around the Sun. Nodal regression is orbit feature utilized for circular orbits to be Sun synchronized. A sun-synchronized orbit lies in a plane that maintains a fixed angle with respect to the Earth-Sun direction. In the low Earth Sun synchronized circular orbits are suited the satellites that accomplish their photo imagery missions. Nodal regression depends on orbital altitude and orbital inclination angle. For the respective orbital altitudes the inclination window for the Sun synchronization to be attained is determined. The apsidal precession represents major axis shift, respectively the argument of perigee deviation. The apsidal precession simulation, for inclination window of sun synchronized orbital altitudes, is provided through this paper.**

Keywords—LEO; satellite; orbit; apsidal precession

I. INTRODUCTION

Orbital perturbation analyzes consider the satellite's orbit behavior under real space-ambient circumstances compared with ideal orbit mathematical model defined by Kepler parameters. Due to the gravitational forces of the Sun, other celestial bodies and also due to the Earth's flattering at both poles the perturbations are caused. Based on geopotential model the effect of the Earth flattering is determined as a sum of spherical harmonics, where the most dominated term is "J2-term" [1].

The Earth flattering is manifested by the nodal regression and apsidal precession. The apsidal precession is too early considered by Newton for celestial bodies, and lately the apsidal theorem is further more analytically considered, among them by authors under [2]. For satellites orbiting the Earth, the laws of celestial bodies' movement are applied. This concept is applied for the apsidal precession analysis of the Sun synchronized low Earth orbiting (LEO) satellites.

Under the second section, the nodal regression is considered and followed by terms the orbit Sun synchronization to be accomplished. Considering different initial low Earth orbit altitudes the inclination window for orbit Sun synchronization is determined. For the determined inclination window, the apsidal precession is simulated.

II. NODAL REGRESSION

The Earth rotates eastward. An orbit where the satellite moves in the same direction as the Earth's rotation is known as *prograde* or *direct orbit.* The inclination of a prograde orbit lies between 0º and 90º. Most satellites are launched in a prograde orbit because the Earth's rotational velocity provides part of the orbital velocity with a consequent saving in launch energy. An orbit where the satellite moves in opposite direction to the Earth rotation is called *retrograde orbit*. The inclination of a retrograde orbit always lies between 90º and 180º [3], [4].

The Earth is not the spherical homogeneous body. Earth is characterized with a bulge at the equator, and a slight flattening at the both poles. The terrestrial potential at a point in space (in our case the point indicates a satellite) depends not only on the distance *r* to the Earth's centre but also on the longitude and latitude of the point and the time. This happens due to irregularities of Earth's rotation and not homogenous Earth's mass distribution. This terrestrial potential depends much more on latitude than longitude, and it through geopotential coefficients J_n is expressed. The J_2 term due to flattering of the Earth (about 20km) dominate all other terms. The values of these coefficients are given by different models. Based on GEM4 model it is [1]:

$$J_2 = 1.0827 \cdot 10^{-3} \quad (1)$$

To a first approximation, the orbital plane is fixed in space as the satellite orbits around the Earth. But, the potential generated by the non-spherical Earth causes variations of the orbital elements. Most effected orbital elements are the *right ascension* and the *argument of perigee*, as presented in Figure.1 [3], [4]. The *right ascension* of the ascending node (Ω) defines the location of the ascending and descending orbital crossing nodes (these two nodes make a *line of nodes*) with respect to a fixed direction in space. The fixed direction is Vernal Equinox. The Vernal Equinox is the direction of the line joining the Earth's center and the Sun on the first day of spring. The *argument of perigee* (ω) is the angle taken positively from 0º to 360º in the direction of the satellite's motion, between the direction of the ascending node and the perigee direction [3], [4].

Under the effect of terrestrial potential variation, the right ascension of the ascending node Ω, shifts its position, so, the line of nodes which is in equatorial plane rotates about the center of the Earth, consequently shifting the orbital plane. *Nodal regression* refers to the shift of the orbital plane over time as Earth revolves around the Sun. Nodal regression is a very useful feature that is especially utilized for Low Earth circular orbits providing to them the *Sun synchronization*.

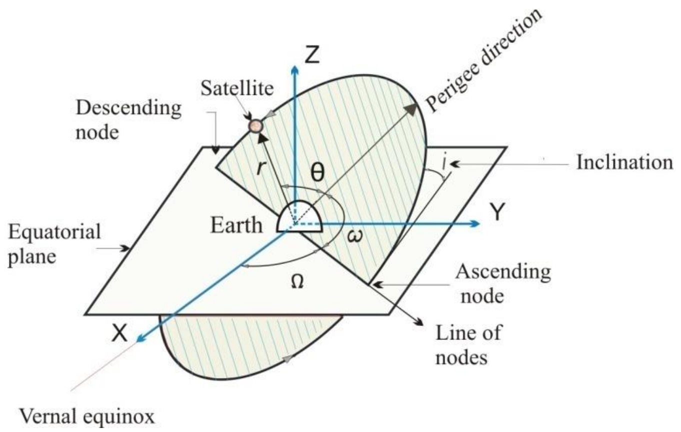


Fig. 1. Space orbital parameters

An approximate expression for the nodal rate regression of *Ω* due to time is expressed as [1]:

$$\frac{d\Omega}{dt} = -(\frac{3}{2})n_0 A J_2 \cos i \tag{2}$$

Where:

$$A = \frac{R_E^2}{a^2(1-e^2)^2} \tag{3}$$

$R_E = 6378$ km is Earth's radius, e is orbital eccentricity, i is the inclination, a is a semimajor axis of satellite's orbit and n_0 is mean movement of the satellite, as:

$$n_0 = \frac{2\pi}{T} \tag{4}$$

Where T is the orbital period. For circular orbits it is $e = 0$ and $a = r$, where r is orbital radius of circular orbit. Orbital period for circular orbits is expressed as:

$$T = 2\pi\sqrt{\frac{r^3}{\mu}} \tag{5}$$

where $\mu = 3.986005 \cdot 10^5\ \text{km}^3/\text{s}^2$ is Earth's geocentric gravitational constant. For circular orbit yields:

$$A = \frac{R_E^2}{r^2} \tag{6}$$

Substituting Eqn. (4), Eqn. (5), and Eqn. (6) at Eqn. (2) and then considering values of R_E, μ and J_2, finally stems nodal regression expressed by inclination i and orbital radius r. The nodal regression expressed in (°/day) is [5]:

$$\Delta\Omega = -2.06474 \cdot 10^{14} \cdot \frac{\cos i}{r^{7/2}} \quad [°/\text{day}] \tag{7}$$

The nodal regression for circular orbits depends upon orbit inclination and orbital altitude (radius). The nodal regression is zero in the case of the inclination angle being 90°.

When the orbit inclination angle is $i < 90^\circ$ than deviation is negative, so according to Eqn. 2 the satellite orbital plane rotates in a direction opposite to the direction of the Earth's rotation. When the orbit inclination angle is $i > 90^\circ$, then deviation is positive, so the satellite orbital plane rotates in the same direction as the direction of the Earth's rotation. From this stems that if the orbit is prograde the nodes slide westward, and if it is retrograde, the nodes slide eastward. This means that nodes (line of nodes) because of this effect move in opposite direction to the direction of satellite motion, hence the term *nodal regression*.

III. ORBITAL SUN SYNCHRONIZATION

LEO (Low Earth Orbiting) satellites have very wide applications, from astronomical purposes, remote sensing of oceans, Earth's climate changes or Earth's imagery with high resolution [6]. For photo imagery missions from satellites, in order the observed area to be treated under the same lighting (illumination) conditions, the observed area's position related to the Sun it is too important [7]. For these purposes the satellites are suited in LEO sun synchronized orbits [8].

A sun–synchronous orbit is one that lies in a plane that maintains a fixed angle with respect to the Earth-Sun direction. In other words, the orbital plane has a fixed orientation with respect to the Earth-Sun direction. Consequently, the angle between normal orbital plane vector and normal Sun vector is always kept constant throughout the year, as shown in Figure 2 [8].

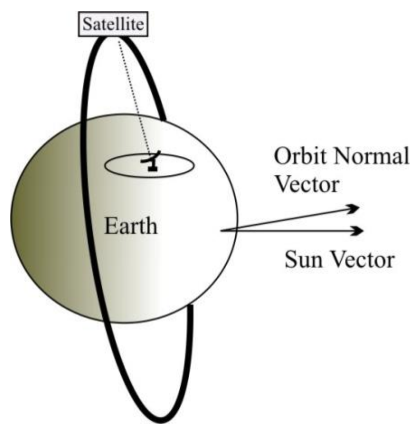


Fig. 2. Orbital Sun synchronization concept

As a result of this property, sun-synchronous orbits ensure that the satellite passes over a given location on Earth every time at the same local solar time, thereby guaranteeing almost the same illumination conditions, varying only with seasons. The satellite in sun-synchronized orbit ensures coverage of the whole surface of the Earth, since the appropriate orbit is quasi-polar in nature [9]. The shift control method to keep the local time shift within an allowance range is given by [10].

The nodal regression effect is typical for LEO orbits. The further goal of this paper is to conclude about the inclination window of the nodal regression for different LEO orbit altitudes ensuring to be attained the orbital Sun synchronization. For simulation purposes are considered low Earth orbit altitudes from 600km up to 1200km. LEOs have too low eccentricity which one can be considered $e \approx 0$ and then $a = r$. Thus, for altitudes from 600km up to 1200km and considering Earth's radius as $R_E \approx 6400$ km yields out the orbits' radius range from 7000km up to 7600km. Considering Eqn. 7, for this orbits' radius range it is calculated the nodal regression [º/day] for different inclination angles i. Results confirm that nodal regression for altitudes form 600km up to 1200km may range from 0º up to 6.7º as a function of inclination angle. Lower inclination causes higher deviation. For inclination of 90 º there is no nodal deviation [11].

The further step is inclination window determination for Sun synchronized feature. An orbital plane fixed with respect to the Earth effectively makes a 360º rotation in space in a year (about 365.25 days) since the Earth itself rotates by 360º around the Sun. This rate is equivalent to a rotation of the orbital plane of about 0.986 [º/day]. By choosing a pair of particular values of i and r, it is possible to obtain an orbit for which the nodal regression varies each day by a quantity equal to the rotation of the Earth around the Sun [8]. Mathematically this is expressed as:

$$\frac{d\Omega}{dt} = 0.9856^{\circ} / day \tag{8}$$

$$\Delta\Omega = -2.06474 \cdot 10^{14} \cdot \frac{\cos i}{r^{7/2}} = 0.9856 \text{ °/day} \tag{9}$$

The angle between line of nodes of the orbits and the mean direction of the Sun obtained in this way remains constant throughout the year as presented in Figure 3.

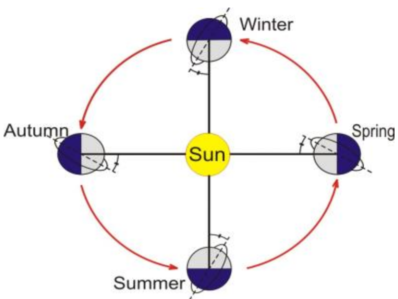


Fig. 3. Sun synchronization throughout seasons

So, the orbit normal vector and Sun vector keep the same angularity during the year. These orbits are known as *Sun synchronized orbits*.

Sun-synchronous orbits are a function of altitude, eccentricity and inclination. By solving the Eqn, 9 for orbital altitude of 600km consequently for $a = r = 7000$ km under no eccentricity ($e = 0$) will get inclination for sun synchronization as:

$$i_1 = 97.9^{\circ} \tag{10}$$

and for orbital attitude of 1200km consequently for $a = r = 7600$ km under no eccentricity ($e = 0$) will get inclination for sun synchronization as:

$$i_2 = 100.5^{\circ} \tag{11}$$

Considering these values of inclination, and the range for lower and higher orbital attitudes, the nodal regression for the inclination range from 97º up to 101 º it is presented in Table 1 and Figure 4 [11]. For the range of low Earth altitudes from 600km up to 1200km *the inclination window* for the orbital Sun synchronization is:

$$97.9^{\circ} < i < 100.5^{\circ} \tag{12}$$

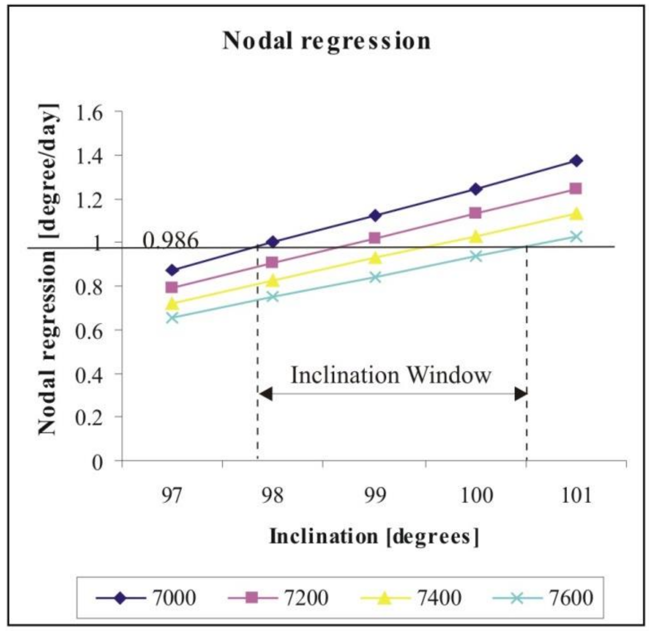


Fig. 4. Inclination window

IV. Apsidal Precession

The position of the orbit major axis is defined by the argument of perigee. This parameter like the right ascension of the ascending node also undergoes natural perturbation due to equatorial bulge of Earth. The phenomenon is known as *apsidal precession.*

An approximate expression for the apsidal precession of perigee's argument (ω) over the time is expressed as [1]:

$$\frac{d\omega}{dt} = (\frac{3}{4}) n_0 A J_2 (5\cos^2 i - 1) \tag{13}$$

where all parameters on the right side of Eqn. (11) have the same meaning as for nodal regression expressed through Eqn. (1) up to Eqn. (6).

The aim of this paper is to conclude about the apsidal range which corresponds to inclination window for orbit Sun synchronization. This calculation leads toward the thrust vector to be applied in order to keep argument of perigee under in advance defined value, consequently keeping the health of the appropriate satellite link. Considering Eqn. (13), there is no apsidal precession if the orbital inclination fulfills the feature expressed as follows,

$$5\cos^2 i - 1 = 0 \tag{14}$$

This happens under the inclination of 63°43'. This is exactly the inclination applied for Molnya elliptic orbit. The rotation of the perigee occurs in the direction opposite to the satellite motion if the inclination is greater than 63°43' and in the same direction as the satellite motion if the inclination angle is less than 63°43' [9].

Substituting Eqn. (4), Eqn. (5), and Eqn. (6) at Eqn. (11) and then considering values of R_E, μ and J_2, finally stems the apsidal precession expressed by inclination i and orbital radius r. The apsidal precession expressed in (°/day) is:

$$\Delta\omega = 1.03237 \cdot 10^{14} \cdot \frac{\left(5\cos^2 i - 1\right)}{r^{7/2}} \text{[°/day]} \qquad (15)$$

The apsidal precession for circular orbits depends upon orbit inclination and orbit altitude (radius). The closer the satellite to Earth center, it is the larger apsidal precession. The apsidal precession is zero in the case of the inclination angle being 63°43'. Considering Eqn. (13), and orbits' radius range from 7000km up to 7600km, it is calculated the apsidal precession [°/day] for inclination window which ensures low Earth Sun- synchronization. These results are given in Table I and Figure 5.

TABLE I. APSIDAL PRECESSION [°/DAY]

Inclination [°]	Orbital radius [km]			
	7000	7200	7400	7600
97	3.329	3.014	2.738	2.494
98	3.248	2.943	2.673	2.435
99	3.156	2.858	2.596	2.365
100	3.054	2.766	2.513	2.289
101	2.942	2.662	2.419	2.203

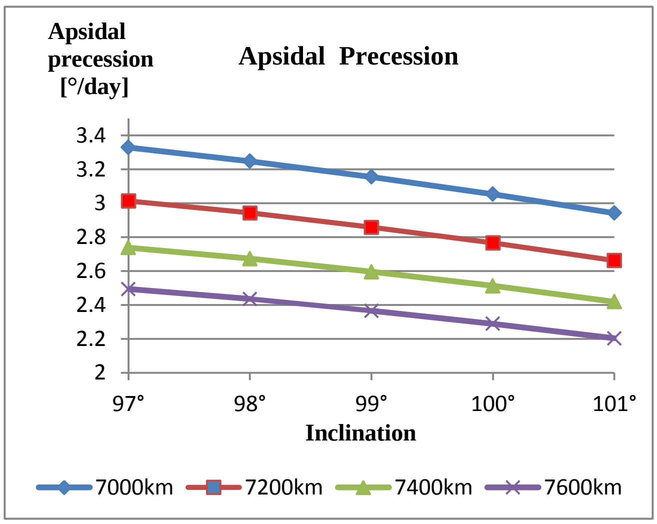


Fig. 5. Apsidal precession

V. CONCLUSIONS

Satellites dedicated for photo imagery missions are suited in low Earth Sun synchronized circular orbits. Nodal regression is the typical feature of low Earth circular orbits which enables orbital Sun synchronization. Sun synchronized orbits are retrograde orbits. Sun synchronization is achieved only for inclination within inclination window.

The apsidal precession for circular orbits depends upon orbit inclination and orbit altitude. The closer the satellite to the Earth center, it is the larger apsidal precession. For the Sun synchronization inclination window for altitudes from 600km to 1200km, the low Earth circular orbits are faced with apsidal precession in the range of 2.2° - 3.3°.

REFERENCES

[1] G. Maral and M. Bousquet, "*Satellite communication systems*," John Willey & Sons, Ltd, Chichester, England, 2002.

[2] S.R. Valluri, P.Yu, G..E. Smith and P.A. Wiegert, "An extension of Newtons apsodal precession theorem", *Momthly Notices of Rolyal Astronomical Society (MNRAS)*, Vol. 358, No. 4, pp. 1273-1284, 2005.

[3] D. Roddy, "Satellite communications", McGraw Hill, New York, 2006.

[4] M. Richharia, (1999), "Satellite communication systems", McGraw Hill, New York, 1999.

[5] Basics of space flight: Orbital mechanics, pg. 14, www.braeunig.us/space/orbmech.htm, 12/4/2011

[6] J.E. Oberright, *Satellite artificial*, World Book Online Reference Center, World Book, Inc, 2004.

[7] S. Cakaj, W. Keim, K. Malaric, "Sun Noise Measurement at Low Earth Orbiting Satellite Ground Station", *47th International Symposium ELMAR 2005 focused on Multimedia Systems and Applications*, IEEE, 8-10 June 2005, Zadar , Croatia, pp. 345 - 348.

[8] S. Cakaj, M. Fischer, A. L. Schotlz, "Sun synchronization of Low Earth Orbits (LEO) through inclination angle", *28th IASTED International Conference on Modelling, Identification and Control*, MIC 2009, Feb. 16 –18, 2009, Innsbruck, Austria, pp. 155-161.

[9] A.K. Maini and V. Agrawal, "Satellite Technology-Principles and Applications", Wiley, UK, 2011.

[10] Y.Yong'an, et al., "Shift control method for the local time at descending node based on sun-synchronous orbit satellite", *Journal of Systems Engineering and Electronics*, Vol.20, No.1, pp.141-145, BIAI, 2009.

[11] S. Cakaj, B. Kamo, K. Malaric, "The Inclination Window for Low Earth Sun Synchronized Satellite Orbits", *Transactions on Maritime Science* Volume 2, Number 1, April 2013, Split, Croatia, pp. 15-19.

Developing Computer Network Based on EIGRP Performance Comparison and OSPF

Lalu Zazuli Azhar Mardedi
Academy of Information Management and Computer
AIMC Mataram
Mataram, Indonesia

Abidarin Rosidi
School of Information Management and Computer
STMIK Yogyakarta
Yogyakarta, Indonesia

***Abstract*—One of the computer network systems technologies that are growing rapidly at this time is internet. In building the networks, a routing mechanism is needed to integrate the entire computer with a high degree of flexibility. Routing is a major part in giving a performance to the network. With many existing routing protocols, network administrators need a reference comparison of the performance of each type of the routing protocol. One such routing is Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF). This paper only focuses on the performance of both the routing protocol on the network topology hybrid. Network services existing internet access speeds average of 8.0 KB/sec and 2 MB bandwidth. A backbone network is used by two academies, they are Academy of Information Management and Computer (AIMC) and Academy of Secretary and Management (ASM), with 2041 clients and it caused slow internet access. To solve the problems, the analysis and comparison of performance between the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) will be applied. Simulation software Cisco Packet Tracer 6.0.1 is used to get the value and to verify the results of its use.**

***Keywords*—Network; EIGRP; OSPF; based; simulator; performance**

I. Introduction

The use of computer networks in everyday lives is increasingly high. It is due to the various facilities offered by the network, ranging from the ease of communicating to the possibility of sharing resources. The use of the requires a variety of tools, such as routers and switches as well as an understanding of the various techniques (addressing technique using the IP address and routing techniques. Routing is the process of sending data packets from the host of origin to the destination host, which is performed by the routers [1].

One form of computer network system usage is an internet connection. To build an internet network, it requires some hardware, software, and protocols. TCP / IP is a protocol standard that is applied to the Internet. The existence of a router in the network TCP / IP is very important. It is due to a large number of hosts and differences in the devices used on the network TCP / IP. As a result, it takes a routing mechanism that can integrate millions of computers with a high degree of flexibility. Routing is divided into two categories; they are static routing and dynamic routing [2].

Computer network expansion will certainly have an impact on the quality of the Internet connection service and connection of existing data exchange [3]. In 2003 the existing Internet connection is only used by the Academic Unit and the Finance Department at the Academy of Information Management and Computer (AIMC) and Academy of Secretary and Management (ASM). However, in 2015 1 backbone and bandwidth 2 MB with Mikrotik routers, computer network services are already used by these academies. Computer network service at those academies is faculty, students and staff with 1021 clients that accesses the computer network, while the other can be accessed by a client in 1020 is comprised of faculty, students, and staff. The uses of computer networks by these two academies reach 2041 clients that access the computer network service every day.

With the conditions of using one backbone by two academies of speed in accessing the Internet an average of 8.0 KB/sec if the network was accessed by a client in 2041. The needs to be a strategy that is mature in conducting development by reference to the comparison of performance between EIGRP to OSPF about which one is better, so that each user gets good access to share and access the data to the internet with the best connection. EIGRP and OSPF routing protocol is a kind of underdog this time [3]. To determine the effectiveness of the distribution of bandwidth, this paper will discuss on a better performance comparison between EIGRP and OSPF on computer network services at AIMC and ASM. With the goal of producing a best development design system of computer networks, it can be implemented in existing computer networks at those academies.

II. Literature Review

A. Routing Protocol

A routing protocol is a set of rules or standards that determine how the router on the network to communicate and exchange information with one another, allowing them to choose the best route to the destination network. Routing protocols perform several activities, including:

1) *Network discovery.*
2) *Update and maintain the routing table.*

There are three types of methods used by the routing protocol, they are:

1) *Distance Vector (Path Vector) Protocol*

It is known as the determination of distance vector routing protocol based on distance or the shortest distance between the points of origin of the package with the destination point. [2]

2) *Link State Protocol*

It is called link state routing protocol for the determination made based on information obtained from other routers. [2]

3) Ring

Ring protocol uses aspects of distance-vector routing protocol types and link state. Examples ring is EIGRP. [2]

B. Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol (LS), which is based on open standards. Each router is configured to use a link-state routing protocol will send two kinds of packages, namely:

1) LSR (Link-State Refreshment) are sent periodically to the router that are around to see if the router is still active and still form a link to the router.

2) LSA (Link-State Advertisement) or routing updates are sent only when there is a change on the network and at the start (initialization).

At first, OSPF router is turned on, and then the router will send a multicast LSA. The router that receives the LSA will copy the information it carries, then pass (forward) of the LSA. Information obtained from the LSA will be stored in the topological (link-state) database. Based on LSA and also the topological database that contains all existing routers on the network, each router will run the SPF algorithm and form the SPF Tree. [1]

C. Enhanced Interior Gateway Routing Protocol (EIGRP)

A routing protocol owned by Cisco that works on routers and the internal route processors contained in the core layer switches and distribution layer switches Cisco. EIGRP is a distance vector protocol that classes and enhanced.

EIGRP has the following characteristics:

1) Using the cost of load balancing are not the same.

2) Using a combination of a distance-vector algorithm with link-state.

3) Using Diffusing Update Algorithm (DUAL) to calculate the shortest path.

4) Supporting IP, IPX, and AppleTalk through modules that are dependent protocol. [2]

D. Switch

It is a device that filters and missed packets of an LAN. Switcher works at the data link layer (layer 2) and sometimes in the Network Layer (Layer 3) based on the OSI reference model that can work for any protocol packets. LANs that use switches to communicate on the network then called Switched LAN or in the physical Ethernet network called Switched Ethernet LANs.

The switch has almost the same function as a hub. The difference is that the switch can operate in a full-duplex mode and can track and filter information transferred to and from specific destinations, while the hub cannot filter and divert the path of relationships. [1]

III. Research Method

A. Development Method

1) Need Analysis

It is a process of finding the problem and generates alternative solutions to problems that are relevant.

2) Designing

It is the first step in manufacturing phase and or development of systems for each product system. At this stage of the design will be produced which will be built.

3) Modeling

At this stage, it will do the design that was made on a limited scale so that it becomes integrated into more useful work.

4) Examination

This stage is the most critical element of the overall process design and process modeling that has been done. At this stage will be discussed basic - basic trial design and the model that essentially is a collection of techniques used to conduct trials according issues tailored to the problems and objectives as a whole.

B. Research Setting

This research was conducted at the Academy of Information Management and Computer and Academy Management Secretary Mataram. This study begins with an ongoing problem, namely 1 backbone with bandwidth of 2 MB is accessible by 2 colleges such as Academy of Management Computer and Academy of Secretary and Management Mataram.

C. Data Collecting Techniques

1) Observation

Direct observation and attention to and examine the computer network services in the Academy of Information Management and Computer and Academy of Secretary and Management Mataram. Observations were done on the computer network and the data collected are as follows:

a) Computer network conditions,

b) Computer network data used,

c) Data traffic of computer networks by observing the delay and timing parameters such as convergence.

d) Computer network development plan.

The data above will be used as the basis for developing the computer network at the Academy of Information Management and Computer and Academy of Secretary and Management Mataram.

D. Need Analysis

In this phase, the basis or foundation of research on the development of computer network design at the Academy of Information Management and Computer (AIMC) and Academy of Secretary and Management (ASM) Mataram. In this case, an analysis of all the data that already collected in finding the problem and generate alternative solutions to the existing problems in order to achieve the ultimate goal of this research is to meet the needs of users in making interactions within the computer network at those colleges. Problems and alternative solutions resulting in this stage will be used as a basis for the next research step.

E. Stage Design

1) Old Schematic

In the old scheme, the writer will explain the existing network at Academy of Information Management and Computer (AIMC) and Academy of Secretary and Management (ASM) Mataram. A backbone network access service is used by these two academies. The number of clients who access the internet, namely 2041 client so that the speed of access reached 8.0 KB/sec. Fig 1 is an old schematic network.

The network use at the Academy of Information Management and Computer (AIMC) and Academy of Secretary and Management (ASM) Mataram, includes the overall activities or academic activities such as students, staff, faculty and leadership. Where network services accessed by the client in 2041 consisting of those academies in order that the speed in accessing such downloads reached 8.0 KB/sec. Figure 2 is showed a schematic end user.

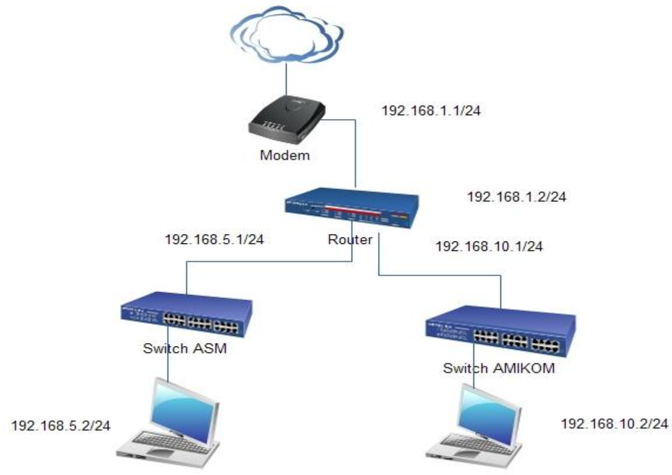


Fig. 1. Old Schematic

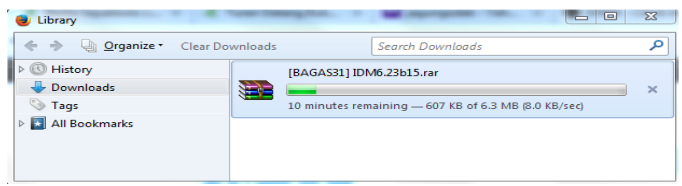


Fig. 2. End user

2) New Scheme

The need for network implementation that can vary in each location to make a difference in the type and amount of equipment needed. Differences in the type and number of these tools as well that ultimately make the difference in techniques and methods to obtain the information required by the router, as one of the tools for routing in the network. The use of many routers make network administrators choose to use a routing protocol as a way for the router to get the information to do the routing.

a) Network Design Flowchart

In this study explained how the simulation system design and configuration of the data communication network based on ring topology using EIGRP and OSPF routing protocol. Fig. 3 showed a flowchart network design.

Fig. 3 showed the stages in the design and simulation performance of EIGRP and OSPF in a ring topology. This simulation is done on a Packet Tracer 6.0.1 software and configure the network begins with the manufacture of the network topology is a ring topology, setting IP Address, and IP settings on each interface. Each topology configured by the EIGRP and OSPF routing protocol then conducted tests ping to every existing PCs after work then proceed to the analysis.

a) Network Topology

In this study, the software used for the simulation is a Cisco Packet Tracer 6.0.1 provides a development environment performance communications networks. On this design will be applied a backbone that is used by the two academies (AIMC and ASM) Mataram. Networks that want to implement only comparing the performance of the OSPF with EIGRP routing protocol.

The topology to be used in this simulation is by using a ring topology with 3 pieces each router, 4 pieces of switches, and eight PCs for every topology and routing protocol. Fig. 4 showed a network topology.

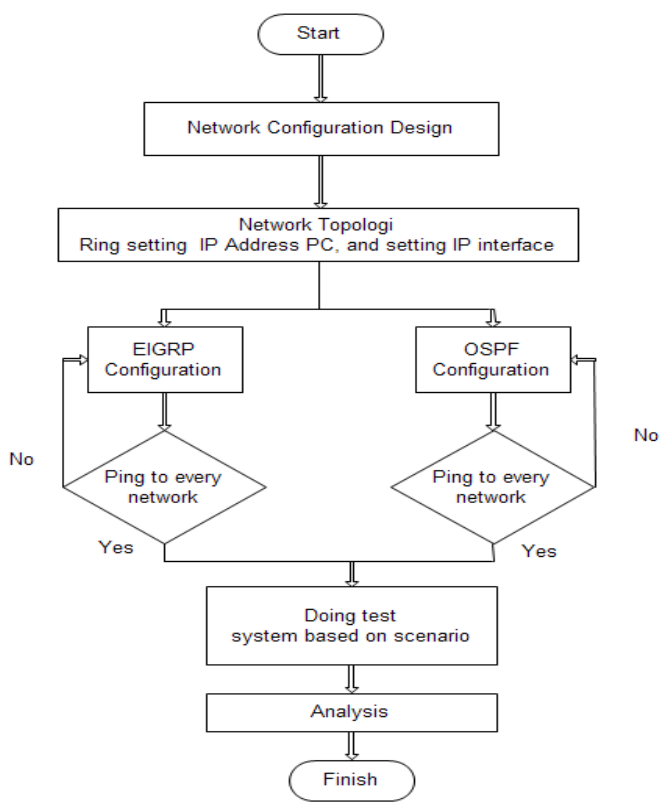


Fig. 3. Flowchart network design

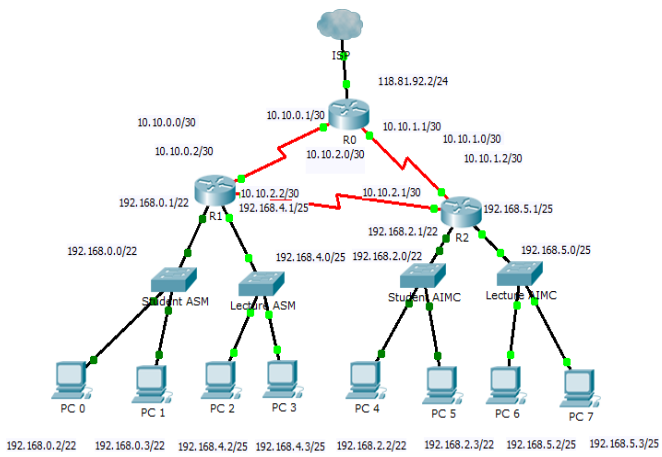


Fig. 4. Network topology

b) IP Address Calculation

At this stage, it will be sub netting based on the number of existing networks as much as 7 network i.e. from R0 to R1, R0 to R2, R1 to R2, students' networks for ASM, lecturers' network, and students and lecturers of AIMC. The network address of each network is as follows:

TABLE I. NETWORK ADDRESS

Network Name	Network Address
R0 to R1	10.10.0.0/30
R0 to R2	10.10.1.0/30
R1 to R2	10.10.2.0/30
ASM Student Network	192.168.0.0/22
ASM Lecture Network	192.168.1.0/25
AIMC Student Network	192.168.2.0/22
AIMC Lecture Network	192.168.3.0/25

- Ring topology

$2^n \geq \times$, n is the number of binary 1 in the subnet mask that must be added in order to exceed or equal the number of required network whereas x is the number of the required number of subnets on a network so that the equation becomes:

$2^n \geq \times$
$2^n \geq 8$
If n = 3 then,
$8 \geq 8$
By adding 3 bits in the subnet mask 255.255.255.0/24
11111111. 11111111. 11111111. 11100000/27

255 . 255 . 255 . 254 /27

The total amount deducted hosts 256 224 of the amount above calculation becomes the difference or range of IP addresses that can be used for each subnet, 256-224 = 32.

TABLE II. CALCULATION IP ADDRESS

Subnet Number	IP Address	Network Address	Broadcast Address	Subnet mask
SN 1	10.10.0.1-10.0.0.2	10.10.0.0	10.10.0.3	255.255.255.252
SN 2	10.10.1.1-10.0.0.2	10.10.1.0	10.10.1.3	255.255.255.252
SN 3	10.10.2.1-10.0.0.2	10.10.2.0	10.10.2.3	255.255.255.252
SN 4	192.168.0.1-192.168.3.254	192.168.0.0	192.168.3.255	255.255.252.0
SN 5	192.168.1.1-192.168.1.126	192.168.1.0	192.168.1.127	255.255.255.128
SN 6	192.168.2.1-192.168.3.254	192.168.2.0	192.168.3.255	255.255.252.0
SN 7	192.168.3.1-192.168.3.126	192.168.3.0	192.168.3.127	255.255.255.128

IV. RESULTS AND DISCUSSION

Simulations were obtained from this study were performed on a Cisco Packet Tracer 6.0.1 for each routing protocol. Scenario testing is made by using the following ways:

1) Observing delay delivery of data packets from a PC to another PC when traffic is busy.

2) Observing the usual trace route path pass data packets during transmission, and then break the link that bypassed the usual data packets to determine these differences are skipped.

B. First Scenario

The first scenario testing done by sending the package Internet Control Message Protocol (ICMP) traffic is busy at the moment as many as five cases and every case the experiment is repeated five times, to increase the traffic on the network added four ICMP packets with the same conditions for each case. 5 cases were simulated apply to a ring topology.

Scenario sending data from PC to PC are shown in the following tables.

TABLE III. SCENARIO OF SENDING DATA PACKETS

Subject 1		Subject 2		Subject 3		Subject 4		Subject 5	
Sender	Receiver	Sender	Receiver	Sender	Receiver	Sender	Receiver	Sender	Receiver
PC 0	PC 5	PC 1	PC 2	PC 2	PC 4	PC 4	PC 7	PC 6	PC 5
PC 1	PC 2	PC 2	PC 4	PC 4	PC 7	PC 6	PC 5	PC 0	PC 5
PC 2	PC 4	PC 4	PC 7	PC 6	PC 5	PC 0	PC 5	PC 1	PC 2
PC 4	PC 7	PC 6	PC 5	PC 0	PC 5	PC 1	PC 2	PC 2	PC 4
PC 6	PC 5	PC 0	PC 5	PC 1	PC 2	PC 2	PC 4	PC 4	PC 7

The examined packet is the first packet in table 3 or grayscale line. Other packets are packets sent to improve traffic on the network.

The topology tested using EIGRP and OSPF routing protocol. A delay on the results of these observations is obtained by dividing the second time resulting from the simulation. The chart comparisons of the average delay with these cases are used are as shown below:

TABLE IV. THE AVERAGE SCORE OF THE RING DELAY EIGRP AND OSPF

Comparison of the average value of delay (seconds)					
Topology and routing protocol	Cases				
	1	2	3	4	5
Ring EIGRP	0,012505	0,01033	0,010325	0,01008	0,010715
Ring OSPF	0,01305	0,01061	0,010715	0,010405	0,011105

If the averaged value of delay each routing protocol for each case is then obtained:

1) Topology Ring EIGRP

Average delay EIGRP topology Ring.

$$\frac{0{,}012505 + 0{,}01033 + 0{,}010325 + 0{,}01008 + 0{,}010715}{5} = 0{,}010791\ seconds$$

2) Ring Topology OSPF

Average delay OSPF topology Ring.

$$\frac{0{,}01305 + 0{,}01061 + 0{,}010715 + 0{,}010405 + 0{,}011105}{5} = 0{,}011177\ seconds$$

Ring EIGRP value better than the value 0.000386 seconds Ring OSPF.

C. Second Scenario

The second scenario testing is done by looking at the data packet router that passed before the termination of the link, and then decide on a few links that pass the package to determine changes in the path of the data packet.

1) The results of the second scenario testing prior to the termination link

- EIGRP topology Ring

A route to be taken by ICMP packets for delivery from PC 0 to PC 5 is PC 0 - Switch Student ASM - Router 1, Router 0 - Router 2 - Switch Student AIMC - PC 5. It is due to the EIGRP route selection performed by the parameter value different metrics for each track. Metric value calculated from the total path or interface that is passed from source router to the destination router by the following equation:

$$metric = 256 * \left(\frac{10^7}{\text{The minimum bandwidth}} + \frac{total\ delay}{10}\right)$$

Further explanation of the metric value will be described in Fig. 5 as follows.

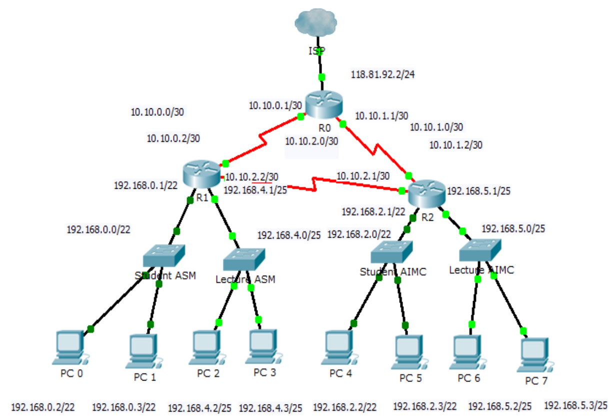


Fig. 5. This packet transmission towards the network from the router 0 Address in a ring topology EIGRP router 1

From fig. 5 above can be seen from the packet transmission path in a router network address 0 towards network address in the router 1 via the router 2 with a minimum bandwidth of 100 kbps, delay 20000µs serial interface and fast Ethernet interface 100µs delay. Metri-value calculation is as follows:

$$metric = 256 * \left(\frac{10^7}{100\ kbps} + \frac{20000\mu s + 20000\mu s + 100\mu s}{10}\right) = 26626560$$

Meanwhile, if the delivery of network packets at the router address 0 towards the network address in the router 2 via the router 1 with 50 kbps bandwidth, delay 20000µs serial interface and fast Ethernet interface 100µs delay. His metric value calculation is as follows:

$$metric = 256 * \left(\frac{10^7}{50\ kbps} + \frac{20000\mu s + 20000\mu s + 100\mu s}{10}\right) = 52226560$$

Of the metric calculations can be proven that the data packet will pass 26626560 smallest metric values to reach to the goal than passing the metric value 52226560 larger than the other metrics.

- OSPF topology Ring

A route to be taken by ICMP packets for delivery from PC 0 to PC 5 is PC 0 - Switch Student ASM - Router 1, Router 0 - Router 2 - Switch Student AIMC - PC 5. This is because the OSPF route selection parameter is done by the value of cost which is different for each individual track, cost value is calculated from each or a router interface that is passed from the source to the destination router by the following equation:

$$Cost = \frac{100\ Mbps}{Bandwidth}$$

Further explanation of the calculation of the cost will be explained in Fig. 6 as follows:

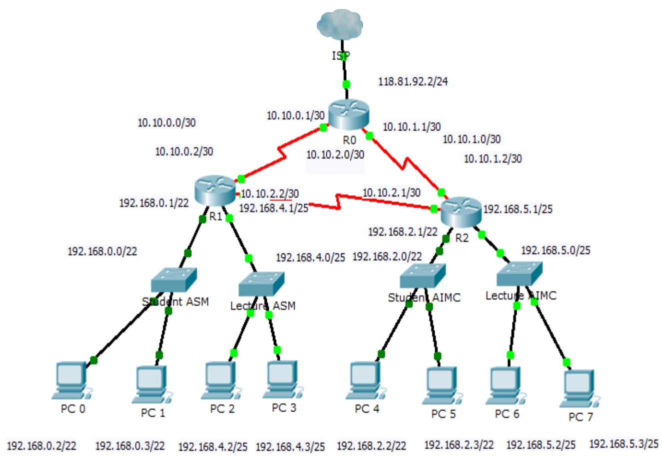


Fig. 6. These routers are sending packets from 0 towards the Ring topology OSPF router 1

From Figure 6 can be seen above the delivery path of network packets at the router address 0 towards network address via the router 1 router 2 with a bandwidth of 100 kbps respectively, its cost value calculation is as follows:

$$Cost\ (total) = \frac{100\ Mbps}{100\ kbps} + \frac{100\ Mbps}{100\ kbps} + \frac{100\ Mbps}{100\ Mbps} = 2001$$

So the cost is the interface into the router 1, 2001. Meanwhile, if the deliveries of network packets at the router address 0 towards network address via the router 1 router 2 with each interface bandwidth of 50 kbps, its cost value calculation is as follows:

$$Cost\ (total) = \frac{100\ Mbps}{50\ kbps} + \frac{100\ Mbps}{50\ kbps} + \frac{100\ Mbps}{100\ Mbps} = 4001$$

So the cost towards the router interface 2 is 4001. From the calculation of the cost can be proved that the data packets passing through the smallest cost value in 2001 to reach to the destination of the passing greater cost that is worth 4001.

2) The second scenario test results after the termination of the link

After knowing the path data packets Ping ICMP data on the usual channels bypassed disconnected to determine the backup path of each routing protocol at each topology. Disconnected paths are paths that connect the router to router 2. 0. The result is as follows:

- EIGRP topology Ring

Once the link is decided on the route that bypassed the PC 0 to PC 5 is PC 0 - Switch Student ASM - Router 1, Router 0 - Router 2 - Switch Student AIMC - PC 5. The data packet will pass 52.22656 million metric values.

- OSPF topology Ring

Once the link is decided on the route that bypassed the PC 0 to PC 5 is PC 0 - Switch Student ASM - Router 1, Router 0 - Router 2 - Switch Student AIMC - PC 5. The data packet will pass the cost value of 4001.

D. Convergence Time

In the third scenario, it will be examined i.e. the convergence time for each router to get the information from other routers and ready to transmit data packets.

1) Time ring topology convergence EIGRP

To determine the Ring EIGRP convergence time can be done by the command "show ip EIGRP neighbors" in the CLI command in every router that result as fig. 7 below:

```
IP-EIGRP neighbors for process 1
H   Address      Interface   Hold Uptime    SRTT   RTO   Q    Seq
                             (sec)          (ms)         Cnt  Num
0   10.10.0.2    Se0/1/0     13   00:00:49  40     1000  0    12
1   10.10.1.2    Se0/1/1     14   00:00:10  40     1000  1    0
```

Fig. 7. Time convergence of simulation results EIGRP topology Ring

Column Hold (sec) which indicates the Hold Time column on the router to wait for the Hello packet from the router to another time when convergence is what underlies every router where the Hello interval by default 5 seconds and Hold / Dead default interval is 15 seconds. So that the average convergence for each router is:

$$Average\ Convergence\ Time = \frac{13 + 14 + 14}{3} = 13{,}66\ seconds$$

2) Time ring topology convergence OSPF

To determine the Ring OSPF convergence time can be done by the command "show ip OSPF neighbors" on each router CLI Command that the results as follows:

```
Neighbor ID    Pri   State       Dead Time   Address      Interface
118.81.92.2      0   FULL/  -    00:00:33    10.10.0.1    Serial0/1/0
192.168.5.1      0   FULL/  -    00:00:31    10.10.2.1    Serial0/1/1
```

Fig. 8. Left Ring topology convergence of simulation results OSPF

Dead Time column where the column shows Dead Time on the router to wait for the Hello packet from another router by default Hello interval is 10 seconds and Hold/Dead interval by default 40 seconds. So that the average times for each router convergence are:

$$Average\ Convergence\ Time = \frac{30 + 33 + 37}{3} = 33{,}33\ seconds$$

V. Conclusion and Suggestions

A. Conclusion

The results of testing Ring network topology on EIGRP and OSPF routing protocol has the following conclusions.

1) In a ring topology testing the score of total delay EIGRP better than 386µ seconds delay value in OSPF.

2) OSPF is a link-state so that at the same cost value of the package to be delivered is not always the shortest route but also the longest route.

3) The average convergence time in a ring topology is 12.75 seconds EIGRP and OSPF Ring topology is 35.25 seconds.

4) The dead-time interval is 15 seconds while the EIGRP OSPF so time is 40 seconds faster than the convergence EIGRP OSPF.

B. Suggestions

Based on the research results, there are some suggestions:

1) Other researcher

Other researchers can conduct the same field with different setting and subjects. They also can use it as reference.

2) Simulation computer network is one way to design a computer network before building a computer network in real.

REFERENCES

[1] A. Setiawan and N. Sevani, "Perbandingan Quality Of Service Antara Routing Information Protocol (Rip) Dengan Open Shortest Path First (Ospf)," pp. 196–207.

[2] E. Menggunakan, S. Jaringan, and O. Modeler, "Simulasi Kinerja Routing Protokol Open Shortest Path First (Ospf) Dan Enhanced Interior Gateway Routing Protocol (Eigrp) Menggunakan Simulator Jaringan Opnet Modeler v. 14.5," pp. 1–6.

[3] "Pengembangan Jaringan Komputer Universitas Surakarta Berdasarkan Perbandingan Protokol Routing Information Protokol (RIP) Dan Protokol Open Shortest Path First (OSPF) Prawido Utomo, Bambang Eka Purnama ABSTRAKSI," vol. 1, no. November, pp. 8–25, 2012.

[4] "Desain Implementasi Routing Jaringan Komputer," vol. 3, no. 1, 2009.

[5] B. A. Y. Tampi, M. E. I. Najoan, A. A. E. Sinsuw, A. S. M. Lumenta, and A. P. J. Komputer, "Implementasi Routing Pada IP Camera Untuk Monitoring Ruang di Universitas Sam Ratulangi," pp. 1–8, 2013.

[6] D. B. Saptonugroho, D. B. P, and B. Santosa, "Analisis Pengaruh Konfigurasi Eigrp Equal Dan Unequal Cost Load Balancing Terhadap Kinerja Router."

[7] J. Jenderal, A. Yani, and N. Palembang, "Analisis Kinerja Routing Protocol Rip Pada Jaringan IPV4 DAN IPV6," vol. 6, no. 12, pp. 1–10.

[8] D. S. Bataona, G. C. Manulangga, and K. Kunci, "Analisis dan Perancangan Metode Subnetting : Hybrid Fixed Length Subnet Masking (HFLSM)," vol. 2, no. 2, pp. 7–15, 2014.

[9] Tina Fajrin, Bambang Eka Purnama, Analisis Sistem Penyimpanan Data Menggunakan Sistem Cloud Computing Studi Kasus SMK N 2 Karanganyar, Seruni 2012 - Seminar Riset Unggulan Nasional Informatika dan Komputer

[10] Wiji Suhardjo, Bambang Eka Purnama (2013), Pemanfaatan Local Area Network Dan Program Netop School Sebagai Media Pembelajaran Interaktif Pada Jurusan Teknik Komputer Jaringan Smk N 1 Klaten, IJNS – Indonesian Journal on Networking and Security, Vol 2 No 3 – Juli 2013, ijns.org, ISSN: 2302-5700

[11] Muchamad Arifin, Ramadhian Agus Triyono, Rekayasa dan Manajemen Jaringan WAN SMK Alhikmah Tanon, IJNS – Indonesian Journal on Networking and Security, Vol 2 No 1 – Januari 2013, ijns.org, ISSN: 2302-5700

[12] Muhammad Taufiq Muslih, Bambang Eka Purnama, Pengembangan Aplikasi Sms Gateway Untuk Informasi Pendaftaran Peserta Didik Baru Di SMAN 1 Jepara, IJNS – Indonesian Journal on Networking and Security, Vol 2 No 1 – Januari 2013, ijns.org, ISSN: 2302-5700

A New Algorithm for Balancing Group Population in Collaborative Leaning Sessions

Aiman Turani
Faculty of Computer Science and Engineering
Taibah University
Media, KSA

Jawad Alkhatib
Faculty of Computer Science and Engineering
Taibah University
Media, KSA

***Abstract*—Proper group formation is essential in conducting a productive collaborative learning session. It specifies the internal structure that the collaborating groups should have based on roles. The Group formation is a dynamic and a challenging component. In some cases, more than one group formation is made during a single session and more than one role a single participant undertakes. Group population is another essential process that follows group formation. Group population is concerned with the process of assigning participants to groups and roles. There are several group population methods that are used in Computer Support for Collaborative Learning environment.**

The main challenge in group population is the partial filling situation. Partial filling is happened when some participants fail to attend their assigned groups at the start of a session. Partial filling could be caused by various reasons. It could be caused by human's mistakes or by technical faults. In this paper, a correction algorithm is described to balance back the groups' participation levels. This algorithm is based on three main phases: Group Elimination, External Transfer, and Internal Transfer phase. The algorithms of these phases are fully described in this paper.

Keywords—Group formation; Group Population; CSCL; Collaboration Techniques

I. Introduction

Usually, the initial step at the start of any collaborative learning session is to allocate participants into groups and to explain them the nature of roles that they need to do [1]. A session could be composed from a single group or from multi-groups. In the corporate and business environment, a specialized team's members are usually allocated in a single group. In the educational environment, large learning sessions such as workshops, seminars, courses, etc., usually distribute their participants into multi-groups to perform group-based activities. Group collaboration is considered an effective way to transfer valuable knowledge among learners [2]. There are many collaboration techniques, such as Brainstorming, Debate, etc. that are widely used, which are based on defining certain roles and groups' settings [3].

Assigning participants to their groups and roles is a challenging task. Instructor needs to decide how and when roles and group should be populated with participants. Some methods are based on participants themselves to choose, or on instructors or even systemically where participants are chosen randomly or selectively based on their characteristics such as age, sex, level of education, expertise, etc.

It is even a more challenging task when forming these groups in a virtual environment [4]. In face-to-face it is easier for an instructor to direct participants during groups' construction and to engage directly in fixing any grouping issue if it occurs.

II. Group Population

Not many Computer Support for Collaborative Learning (CSCL) tools specify how participants will be actually populated in their groups. Some tools allow instructors to create groups based on their students' profile [5]. Other tools assign participants randomly to groups on the base of first come first assigned. Usually, these group formation tools do not take in consideration roles found within collaboration sessions [6]. In addition, they tend to limit the selection flexibility by relying on certain algorithms, such as genetic algorithm [7], and excluding students and instructors from making their own selection.

To clarify the complexity nature of group population, three key issues are listed: population assigner, population time, and population mode. Firstly, the assigning method should be specified early by the owner of the session. In general, there are three common approaches in assigning participants to groups. The assignment could be done by either the participant himself, by the facilitator, or by the system. In the first approach, a participant will simply choose his role and group [8]. In the second approach, the facilitator or the instructor will assign participants to groups. In the last approach, there are two means for the system that it could take, randomly based on first come first assigned, or selectively based participants' profiles data (age, sex, education level, specialties, friendship, geographical background, etc.) [9].

In addition to the assignment method, there are also different population timings. Population could happen just before the session starts or sometime before the session starts. In some cases, the instructor may need longer time to manually allocate participants in their groups especially at large classes. In other cases, he wants participants to know their roles and groups in advance to prepare themselves, or to be able to accommodate any request of changing roles or groups [10].

Finally, there are two identified population modes which are sequential and parallel. In the sequential mode, the system would open up groups for population one by one. In the

Taibah University- Computer Science & Computer Engineering

parallel mode, all groups would be opened at once. Many CSCL systems use the sequential population at the start of a session allowing arriving participants to join their session in a linear manner. The parallel mode in the other hand provides more selection's flexibility. For example, instructor could start filling groups by first assigning the most critical role at all groups to key-participants and then turns to another role. In another example, a participant would like to select a certain group to join his friends for instance.

III. POPULATION RISKS

There are several populating risks that lead to the groups' partially-filled situation. The partially-filled situation usually causes undesired events to occur. Examples of these events could be the inability to start a session due a large number of absentees, a certain group cannot function properly due to a critical role that is missing or that suddenly leaves, unbalanced group's outputs due to some groups have maximum attendants while other suffers from shortages in attendants, etc.

The focus in this section is on the reasons that might cause partial groups' filling. Firstly, it starts with the last-group partial filling scenario. Even in case of a complete attendance, there is a still high chance that the number of attending participants will not match exactly the default groups' sizes. In other word, the division result will not be always an integer causing the last group to be in short. Another common reason is when some participants fail to join their groups. This can be caused by various reasons such as, carelessness, forgetting, emergencies, technical fault, etc. These undesired incidents could leave some groups with some vacancies or even in extreme cases a scattered population throughout all groups. Late comers issue also needs to be addressed. Would the system allow them to join and if they join, which group and role they could have, and after what point in time they should be banned.

IV. FLEXIBLE GROUP STRUCTURE

There is a need to design a flexible group structure that could tolerate population faults. A group structure within collaborative learning environments depends heavily on roles. What types of roles that are needed to carry out collaborative activities, how many participants should be assigned to a specific role, etc.? These questions should be addressed by an instructor during group's formation phase [11]. To enable flexibility, a further question should be asked, that is which roles are critical and which roles are flexible. To answer this question, the group structures of common collaboration techniques should be analyzed. A certain role is considered a flexible role if its size could vary otherwise it is a critical role. So in order to enable role's flexibility, a maximum and a minimum size should be also defined. For instance, instead of defining a rigid structure for a Brainstorming technique that may include 1 chairperson and 4 participants, it could have this flexible setting: (1 chairperson, 2-7 (5) participant). In this setting the participant role default size is 5 but this size could range from minimum 2 to maximum 7. A simple flexibility ratio could be obtained by using this formula:

Fr = (max group size - min group size)/ default group size

For the above Brainstorming technique the Fr would equal 0.8 (7-2 /6). The following table includes the flexibility ratios for some common collaborative techniques with suggested roles and sizes.

TABLE I. FLEXIBILITY RATIO FOR SOME COMMON COLLABORATIVE TECHNIQUES

Collaboration Technique	**Role1**	**Role2**	**Role3**	**Role4**	**Flexi ratio**
Brainstorming Group Nomination	Chairperson 1	Participant 2 -7 (5)			0.83
Group Discussion Buzz group Round Table Discussion Case study Jigsaw	Participant 2 -7 (5)				1.0
Debate	Prosper 1	Opposer 1	Chairper 1	Audience 2 -7 (5)	0.62
Pyramid Team pair-solo Think-pair-share Panel	Participant 4 -14 (10)				1.0
Pro/Contra	Side1 2 -14 (7)	Side 2 2 -14 (7)			1.7

As shown in this table, most techniques have good flexibility ratios allowing for an appropriate opportunity for group populating correction.

V. POPULATING CORRECTION

A populating correction is needed if one the following cases occur:

- If the attending participants as a total number is not sufficient to fill all groups according to their minimum sizes. --- Group Elimination
- If there is an unbalanced group attendance (highest attendance group - lowest attendance group is more than one). --- External transfer
- If any critical role that is not fulfilled. --- Internal transfer
- If there is an unbalanced roles attendance at a certain group (the difference between [a flexible role attendants – its min size] and [any other flexible role attendants – its min size] is more than one). --- Internal transfer

In this paper, the general correction algorithm that depends on the flexibility within the groups' structure was proposed. There are three correction phases in this process which are: the Elimination phase, the External Correction phase, and the Internal Correction phase. The Elimination phase is started by checking if there are no enough attendants to cover all groups' minimum requirements. In this case, the lowest group in attendance is eliminated and its member are transferred to another group. The External Transfer phase is performed to balance participants' distribution. Groups with extra attendants will donate to groups with lower attendants. The last correction phase is the Internal Transfer phase where attendants of a flexible role are used to replace unattended critical roles or to balance other flexible roles if required.

The following correction algorithm would be carried out just before the start of a collaboration session.

1) Groups will be sorted according to their attendance sizes.

2) The system will calculate the Participation index.

3) If the index has a negative value, then the lowest group will be eliminated and its members will be assigned to the next lowest group.

4) Step 3 and 4 will be repeated until the index value becomes zero or more.

5) To allow a balanced participants' distribution, the system will sort groups again and check if the difference between the lowest group and the highest group is equal to one.

6) If the difference is greater than one, then the highest group will donate one member form its flexible roles to the lowest group.

7) Steps 6 and 7 will be repeated until difference between the lowest group and the highest group is only one.

8) For internal group correction, the system will check if all critical roles are populated and also if there is a balanced distribution between its flexible roles.

The Participation index is computed according the difference between the total number of attendants and the total groups' minimum hosting capability. The following formula is used to compute the Participation index

$$Pi = \sum_{i=1}^{All\ Group} \text{Group Att.} - \text{Min G Size}$$

For instance, suppose you have 31 participants that are joining Group Nomination technique out of 40 learners. They joined in 6 groups as shown in the first column at the following table.

TABLE II. GROUP NOMINATION ATTENDANCE EXAMPLE

	Sort	**Elimi**	**Sort**	**Ex.T**	**Sort**	**Ex.T**	**Sort**
5	7	7	**8**	**7**	**7**	**6**	**7**
7	6	6	7	7	7	7	6
4	5	5	6	6	6	6	6
6	5	5	5	5	6	6	6
5	**4**	**8**	**5**	**6**	**5**	**6**	**6**
4	**4 ***						Finish

According to the Group Nomination setting, the default group size is 6. The Pi = 31- 6*6 = -5. Since this is a negative index, the lowest group's participants will be eliminated. As shown in the second column, a descending sorting is done then and the lowest group which contains 4 participants is eliminated and donates its participants to the next lowest group as shown in the third column. The index will be checked again, which becomes positive this time (31-6*5). A new sorting will follow and since the size of the highest (8) – lowest(5) > 1, an external transfer from max group to min group will happen as shown in columns 4 and 5. Still, since the difference between the highest and lowest is more than one, a new round of external transfer will happen.

To clarify internal transfer process, suppose that there is a collaboration session that is based on Pro/Contra technique with this group formation structure: (1 chairperson, 1-5(2) side1, 1-5(2) side2) and one of the groups has this population: (3 side1, 6 side2). Since the critical role is missing, the critical role will first be populated from the flexible role side2 (1 chairperson, 3 side1, 5 side2). The absolute value of (3-2) – (5-2) > 1 therefore another internal transfer is needed for balancing roles' distribution. The new population arrangement would look like this (1 chairperson, 4 side1, 4 side2). No further correction is needed since the critical role is fulfilled and the difference between the flexible roles is not more than one.

VI. CONCLUSION

Proper group formation and population is essential in conducting collaborative learning sessions. Random population can lead to unbalanced grouping and is unlikely to produce effective groups. Not many CSCL tools support group formation and even less supports group population. In addition, collaborative learning sessions usually have their groups' structure based on roles. Many populating tools do not consider roles and also assume that all participants will attend.

Many population risks were discussed in this paper which causes serious difficulty in conducting a proper collaboration session. These risks cause groups to suffer or even to do not function as required (for instance critical roles are missing). To overcome these risks a new populating correction algorithm was introduced in this paper. The correction algorithm has three main phases. The Elimination phase, External Transfer phase, and Internal Transfer phase. The Elimination phase was used to eliminate some groups if there are no enough attendants. An External Transfer phase was used to provide proper group balancing if needed, where groups with extra attendants would transfer some of its members to groups with less attendants. The Internal Transfer phase was used to balance roles' attendance and to fill unattended critical roles within a particular group. A list of eight steps was introduced in this paper to describe the full population correction algorithm.

This correction algorithm did not specify how the system should handle late comers. In the future, a more comprehensive algorithm will include solving late comers' issue. That correction algorithm will not only keep balancing groups after late comers are arriving but also specifies associated policies within, such as, until what point in time or participation percentage the system should allow late comers to join. Will they construct new groups or distribute them in existing groups using non-critical roles, etc.

ACKNOWLEDGMENT

We would like to owe thanks to TAIBAH University, College of Computer Science and Engineering (CCSE), Kingdom of Saudi Arabia for supporting this research.

REFERENCES

[1] W. Martin, P. Hans-Rüdiger, "Group formation in computer-supported collaborative learning," ACM., pp. 24-31, 2001 [In: Proceedings of the 2001 international ACM SIGGROUP conference on supporting group work].

[2] T. Tobin, R. Daniel, Re-educating the corporation: foundations for the learning organization, John Wiley & Sons, 1994.

[3] G. Peter, "Educational design and networked learning: Patterns, pattern languages and design practice," Australasian Journal of Educational Technology, vol. 21, 2005, pp.82-101.

[4] M. Townsen, M. Samuel, and R. Anthony, "Virtual teams: Technology and the workplace of the future," The Academy of Management Executive, 3th ed, vol. 12, 1998, pp. 17-29.

[5] C. Marreiro, I. Seiji, "Group Formation Algorithms in Collaborative Learning Contexts: A Systematic Mapping of the Literature Wilmax," Collaboration and Technology Lecture Notes in Computer Science, vol 8658, 2014, pp. 199-214.

[6] J. Strijbo, L. Rob, W. Martens, M. Wim, and B. Nick, "The effect of functional roles on group efficiency using multilevel modeling and content analysis to investigate computer-supported collaboration in small groups," Small Group Research 2nd ed, vol.35, 2004, pp. 195-229.

[7] R. Tyson, R. Henry, "Forming Productive Student Groups Using a Massively Parallel Brute-Force Algorithm," WCECS 2013, vol. 1 pp. 23-25, October 2013 [Proceedings of the World Congress on Engineering and Computer Science USA, 2013.

[8] Andersena, D., and G. Richardsona. "Scripts for group model building." *System Dynamics Review* 13, no. 2,1997, pp. 107-129.

[9] Chow, Bob Eng Po. "Regulation of motivation in undergraduate business students learning with the case method: examining an underemphasized aspect of self-regulated learning." PhD diss., Education: Faculty of Education, 2011.

[10] Mezirow, Jack. "Last Gamble on Education: Dynamics of Adult Basic Education." (1975).

[11] P. Dillenbourg, "Over-scripting CSCL: The risks of blending collaborative learning with instructional design," Three worlds of CSCL. Can we support CSCL? ,2002, pp. 61-91.

An Approach to Calculate the Efficiency for an N-Receiver Wireless Power Transfer System

Thabat Thabet
School of Computer science and Electronic Engineering
University of Essex, Colchester, Uk
Technical Collage, Mosul, Iraq

Dr. John Woods
School of Computer science and Electronic Engineering
University of Essex
Colchester, Uk

***Abstract*—A wireless power transfer system with more than one receiver is a realistic proposition for charging multiple devices such as phones and a tablets. Therefore, it is necessary to consider systems with single transmitters and multiple receivers in terms of efficiency. Current offerings only consider single device charging systems. A problem encountered is the efficiency of one receiver can be affected by another because of the mutual inductance between them. In this paper, an efficiency calculation method is presented for a wireless power transfer system with one to N-receivers. The mutual inductance between coils is implicitly calculated for different spatial positions and verified by practical experimentation. The effect of changing parameters, such as resonant frequency, coil size and distance between coils, on the efficiency has been studied. A clarification of the special performance of a wireless power transfer system at a specific point has been presented.**

Keywords—wireless power transfer; multiple receivers

I. Introduction

Wireless power transfer by magnetic resonant frequency coupling is a new version of the classic theory presented by [1]. Wireless charging is more convenient and has a number of advantages over wired connections. In wireless charging there is no physical connection between the load and the source encouraging its use for no spark applications. Wireless power transfer depends on the near field and is convenient, safe, and simple [2]. Due to its dependence on magnetic resonance, Witricity is also safe from a biological point of view i.e. environmentally friendly [3]. The seminal work of this technique was conducted by Nikola Tesla in the late 19th century, he was one of the wireless power transmission pioneers [1].

In 2007 scientists at Massachusetts Institute of Technology (MIT) revisited the concept of wireless power transfer by announcing a testbed which wirelessly transferred tens of watts over a distance of greater than two meters. Following this, research in this area has received increased attention by many large multinational companies such as Apple, Duracell and Qualcomm [4]. Researchers have tended to study wireless power transfer systems with a single transmitter and a single receiver. It is clear that the performance of wireless power transfer changes according to factors such as the distance between the transmitter and the receiver [5-7].

In [8] the authors explained how one can express inductive coupling or magnetic resonance with the same analytic form as used in coupled mode theory. However, according to [9] this method is undesirable and inconvenient. Therefore researchers tend to use the equivalent circuit for a magnetic coupled system. For example, in [5] the researchers analysed an equivalent circuit wireless system and found its efficiency at different distances between the transmitter and the receiver demonstrating optimum performance at a specific point. In their analysis, s-parameters have been employed because they are more convenient for practical experiments at high frequency. In spite of the wealth of research to study efficiency for single receiver wireless systems, there is still a shortage of similar studies about multiple receivers.

In this paper, the equivalent circuit of the magnetic coupling system is proposed with some modification to study the efficiency of wireless power transfer with multiple receivers. An essential part of this study is the calculation of the mutual inductance between coils. Resonant frequency, coil size and distance between coils, and the effect of these parameters on efficiency has been considered. The optimum performance of the wireless power transfer system has been demonstrated for various cases.

The findings of our study can be used to form the basis of any multiple receiver system. The proposed method can also be applied analytically at different frequencies. To investigate the results practically, experiments have been conducted inside a Faraday cage at frequencies of 2.07MHz and 2.5MHz. Choosing these frequencies is due to practical considerations such as a.c. signal sources and practical dimensions of the coils.

II. Wireless Power Transmission Using Magnetic Resonance

The principle of the mutual induction phenomena, which happens between two coils, is the passing of a continuous time varying current through one of the coils called the primary coil leading to the production of a magnetic field around it. The interaction of this magnetic field with the second coil called secondary, leads to an induced current in it as shown in Fig.1. The maximum interaction happens when the two coils work at the same frequency and the mutual induction here is called magnetic resonance [3, 10].

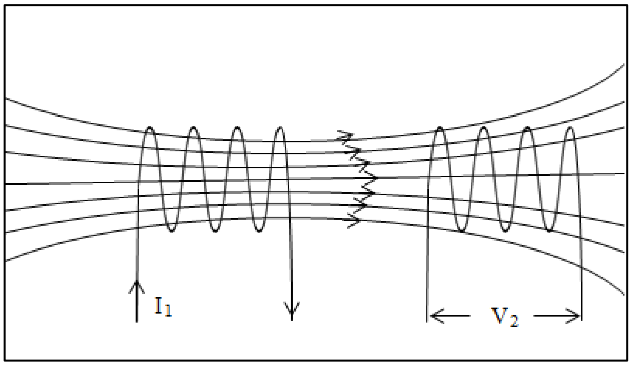


Fig. 1. Mutual Induction Process

III. Resonance Coupled System Representation

A. One load system representation

A simple wireless power transmission system consists of a transmitter and a receiver as shown in Fig.2. The transmitter is represented by the source *Vs* and its internal resistor *Rs*, the capacitor C_1 and the inductor L_1. While C_2 and L_2 are the capacitor and the inductor that achieve the resonance to transfer the power to the load resistor R_2.

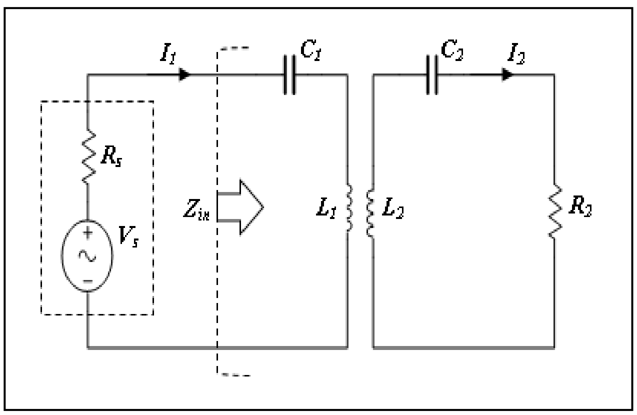


Fig. 2. Equivalent Circuit of a Wireless Power Transfer System

Due to the inductance value of each coil, capacitor values are chosen to achieve the resonance condition $X_L=X_C$, through the resonance frequency equation [11]:

$$f_o = \frac{1}{2\pi\sqrt{L_1C_1}} = \frac{1}{2\pi\sqrt{L_2C_2}} \qquad (1)$$

B. Two load system representation

The same principle can be used to represent a system with two receivers or more. Fig.3 shows a schematic circuit of a resonant coupled system which consists of a transmitter and two receivers. It shows the basic variables which are used in the calculation of mutual inductance. The variables *A* and *a* are the radius of the transmitter and each receiver, respectively. The distance between the transmitter and each receiver or between the two receivers are represented by *b* and *D*, respectively. Finally, *p* is the pitch between any two turns in any of the coils. It is clear from this circuit that the calculation method of mutual inductance between the transmitter and each receiver is different for the two receiver case due to variation in location. Different methods are proposed to calculate the mutual inductance for each case [12, 13].

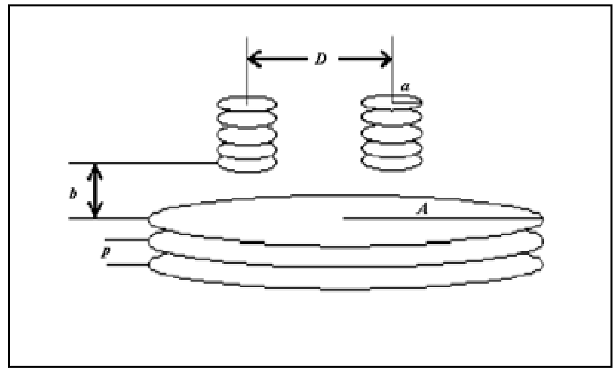


Fig. 3. Schematic Circuit of a Resonant coupled system

The equivalent circuit of a wireless power transfer system with two receivers is shown in Fig.4. In the figure, the source V_s drives a transmitter coil and its internal resistor is R_s. L_1 and C_1 are the inductor and the capacitor of the transmitter. On the other side of the circuit, the first receiver is represented by L_2, C_2, and R_2 as an inductor, capacitor and load resistor, respectively. Similarly, L_3, C_3, and R_3 form the second receiver.

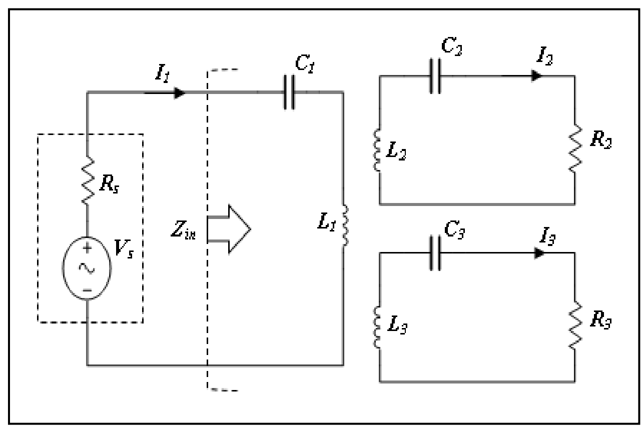


Fig. 4. Equivalent Circuit of a Wireless Power Transfer System with Two Receivers

The second receiver should be under the resonance condition with the same resonance frequency.

$$f_o = \frac{1}{2\pi\sqrt{L_3C_3}} \qquad (2)$$

IV. Basics of Theoretical Analysis

Applying Kirchhoff's law of voltage on each loop [14] (the transmitter and the receiver) is the start of the analysis. M_{12} or M_{21} is the mutual inductance between the transmitter and the receiver.

$$V_s = \left(R_s + jwL_1 + \frac{1}{jwC_1}\right) I_1 - jwM_{12}I_2 \quad \text{(3-a)}$$

$$0 = -jwM_{21}I_1 + \left(R_2 + jwL_2 + \frac{1}{jwC_2}\right) I_2 \quad \text{(3-b)}$$

Where w=2πf

I_1 and I_2 : The loops currents.

Applying Z-parameters on this set of equations leads to:

$$\begin{bmatrix} V_s \\ 0 \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} \\ Z_{21} & Z_{22} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \end{bmatrix} = [Z] \begin{bmatrix} I_1 \\ I_2 \end{bmatrix} \quad (4)$$

The previous equation can be written as:

$$\begin{bmatrix} I_1 \\ I_2 \end{bmatrix} = inv\ [Z] \begin{bmatrix} V_s \\ 0 \end{bmatrix} \quad (5)$$

So

$$I_1 = inv\ Z(1,1)\ V_s \quad (6\text{-a})$$
$$I_2 = inv\ Z(2,1)\ V_s \quad (6\text{-b})$$

It is concluded from (6-a) that:

$$Z_{in} = inv\ Z(1,1) - R_s \quad (7)$$

Here, the output and input power can be calculated:

$$P_{out} = I_2^2\ R_2 \quad (8)$$
$$P_{in} = \left(\frac{V_s}{R_s+Z_{in}}\right)^2 Z_{in} \quad (9)$$

Under the condition of maximum transfer of power, the efficiency can be calculated as:

$$eff = inv\ Z(2,1)^2\ (R_s + R_2)^2 * 100\% \quad (10)$$

V. Theoretical Analysis of Multiple Receivers

Following the same theoretical analysis as for a single receiver system we extend the method for a number of the receivers; this is the main contribution of this paper.

A. Two Receivers

For the circuit shown in Fig.3, Kirchhoff's law of voltage is applied on each loop (the transmitter and the two receivers) with regard to the mutual inductance between each pair of coils [14]. The mutual inductance between the transmitter and the first, second receiver are M_{12} and M_{13}, respectively. Both of them follow the same calculation method because of their relation to the transmitter. As a special case, M_{12} is equal to M_{13} if the two receivers are identical. While M_{23}, the mutual inductance between the two receivers has to be calculated using another method due to their parallel nature.

$$V_s = \left(R_s + jwL_1 + \frac{1}{jwC_1}\right) I_1 - jwM_{12}I_2 - jwM_{13}I_3 \quad (11\text{-a})$$
$$0 = -jwM_{21}I_1 + \left(R_2 + jwL_2 + \frac{1}{jwC_2}\right) I_2 + jwM_{23}I_3 \quad (11\text{-b})$$
$$0 = -jwM_{31}I_1 + jwM_{32}I_2 + \left(R_3 + jwL_3 + \frac{1}{jwC_3}\right) I_3 \quad (11\text{-c})$$

Where $w=2\pi f$

I_1, I_2 and I_3 : The loops currents.

Applying Z-parameters on this set of equations leads to:

$$\begin{bmatrix} V_s \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} & Z_{13} \\ Z_{21} & Z_{22} & Z_{23} \\ Z_{31} & Z_{32} & Z_{33} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} = [Z] \begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} \quad (12)$$

The previous equation can be written as:

$$\begin{bmatrix} I_1 \\ I_2 \\ I_3 \end{bmatrix} = inv\ [Z] \begin{bmatrix} V_s \\ 0 \\ 0 \end{bmatrix} \quad (13)$$

So

$$I_1 = inv\ Z(1,1)V_s \quad (14\text{-a})$$
$$I_2 = inv\ Z(2,1)V_s \quad (14\text{-b})$$
$$I_3 = inv\ Z(3,1)V_s \quad (14\text{-c})$$

It is concluded from (14-a) that:

$$Z_{in} = inv\ Z(1,1) - R_s \quad (15)$$

Here, the output power for each receiver can be calculated:

$$P_{out1} = I_2^2\ R_2 \quad (16\text{-a})$$
$$P_{out2} = I_3^2\ R_3 \quad (16\text{-b})$$

And the input power is:

$$P_{in} = \left(\frac{V_s}{R_s+Z_{in}}\right)^2 Z_{in} \quad (17)$$

Under the condition of maximum transfer of power, the efficiency for each receiver can be calculated as:

$$eff_1 = inv\ Z(2,1)^2\ (R_s + R_2)^2 * 100\% \quad (18\text{-a})$$
$$eff_2 = inv\ Z(3,1)^2\ (R_s + R_3)^2 * 100\% \quad (18\text{-b})$$

B. Three Receivers

Similar representation for the two receivers system can be applied on the three receivers system:

$$V_s = \left(R_s + jwL_1 + \frac{1}{jwC_1}\right) I_1 - jwM_{12}I_2 - jwM_{13}I_3 - jwM_{14}I_4 \quad (19\text{-a})$$
$$0 = -jwM_{21}I_1 + \left(R_2 + jwL_2 + \frac{1}{jwC_2}\right) I_2 + jwM_{23}I_3 + jwM_{24}I_4 \quad (19\text{-b})$$
$$0 = -jwM_{31}I_1 + jwM_{32}I_2 + \left(R_3 + jwL_3 + \frac{1}{jwC_3}\right) I_3 + jwM_{34}I_4 \quad (19\text{-c})$$
$$0 = -jwM_{41}I_1 + jwM_{42}I_2 + jwM_{43}I_3 + \left(R_4 + jwL_4 + \frac{1}{jwC_4}\right) I_4 \quad (19\text{-d})$$

Where w=2πf

I_1, I_2 and I_3 : The loops currents.

Applying Z-parameters on this set of equations leads to:

$$\begin{bmatrix} V_s \\ 0 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} & Z_{13} & Z_{14} \\ Z_{21} & Z_{22} & Z_{23} & Z_{24} \\ Z_{31} & Z_{32} & Z_{33} & Z_{34} \\ Z_{41} & Z_{42} & Z_{43} & Z_{44} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix} = [Z] \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix} \quad (20)$$

The previous equation can be written as:

$$\begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ I_4 \end{bmatrix} = inv\ [Z] \begin{bmatrix} V_s \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad (21)$$

So

$$I_1 = inv\ Z(1,1)V_s \quad (22\text{-a})$$
$$I_2 = inv\ Z(2,1)V_s \quad (22\text{-b})$$
$$I_3 = inv\ Z(3,1)V_s \quad (22\text{-c})$$
$$I_4 = inv\ Z(4,1)V_s \quad (22\text{-d})$$

It is concluded from (22-a) that:

$$Z_{in} = inv\ Z(1,1) - R_s \quad (23)$$

Here, the output power for each receiver can be calculated:

$$P_{out1} = I_2^2\, R_2 \qquad (24\text{-a})$$
$$P_{out2} = I_3^2\, R_3 \qquad (24\text{-b})$$
$$P_{out3} = I_4^2\, R_4 \qquad (24\text{-c})$$

And the input power is:

$$P_{in} = \left(\frac{V_s}{R_s+Z_{in}}\right)^2 Z_{in} \qquad (25)$$

Under the condition of maximum transfer of power, the efficiency for each receiver can be calculated as:

$$eff_1 = inv\, Z(2,1)^2\, (R_s + R_2)^2 * 100\% \qquad (26\text{-a})$$
$$eff_2 = inv\, Z(3,1)^2\, (R_s + R_3)^2 * 100\% \qquad (26\text{-b})$$
$$eff_3 = inv\, Z(2,1)^2\, (R_s + R_2)^2 * 100\% \qquad (26\text{-c})$$

C. N- Receivers

The method can be applied in the general case for an N-receiver system and the general equation for any system is:

$$\begin{bmatrix} V_s \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = \begin{bmatrix} Z_{11} & Z_{12} & Z_{13} & \dots & Z_{1n} \\ Z_{21} & Z_{22} & Z_{23} & \dots & Z_{2n} \\ Z_{31} & Z_{32} & Z_{33} & \dots & Z_{3n} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ Z_{n1} & Z_{n2} & Z_{n3} & \dots & Z_{nn} \end{bmatrix} \begin{bmatrix} I_1 \\ I_2 \\ I_3 \\ \vdots \\ I_n \end{bmatrix} \qquad (27)$$

VI. Mutual Inductance Methods

A. Concentrical Coils

According to [5], The Neumunn formula can be applied to find the mutual inductance between two concentric turns:

$$M = \frac{\mu_o}{4\pi} \iint \frac{dl_1 dl_2}{D} \qquad (28)$$

Where $\mu_o = 4\pi * 10^{-7}\, H/m$

D: the distance between dl_1 and dl_2

The same solution for this integral can be achieved by the Maxwell equation [12]:

$$M_{12} = \mu_o \sqrt{Aa}\, \left(\frac{2}{k} - k\right) K(k) - \frac{2}{k}\, E(k) \qquad (29)$$

Where *A*, *a*: the radius of what is regarded as two concentric turns as shown in Fig.2

$$k = \frac{2\sqrt{Aa}}{\sqrt{(A+a)^2 + D^2}} \qquad (30)$$

K and *E*: the first and second kind of the complete elliptic integral and they are defined as:

$$K = \int_0^{\pi/2} \frac{d\varphi}{\sqrt{1 - k^2 sin^2\varphi}}$$

$$E = \int_0^{\pi/2} \sqrt{1 - k^2 sin^2\varphi}\, d\varphi$$

As a modification to deal with a coil of more than one turn, the following expression was used instead of *D* in (30):

$$D \to D + (j-1)p + (i-1)p \qquad (31)$$

Where $i = 1 \to N_1$

$j = 1 \to N_2$

N_1 and N_2: the number of turns for each coil.

P: the pitch between turns

Finally, the total mutual inductance between two concentric coils with multiple turns can be found by [12]:

$$M_{total} = \sum_{i=1}^{N_1} \sum_{j=1}^{N_2} M_{ij} \qquad (32)$$

B. Parallel Coils

Mutual inductance calculation between two parallel coils needs another formula instead of the Maxwell equation. In [13], the researchers presented two formulas to express the mutual inductance between two turns at the same level and two turns with lateral misalignment.

1) Two turns at the same level

The following formula can be applied to calculate the mutual inductance between two turns at the same level:

$$M = \frac{\mu_o a_p}{2\pi} \int_0^{\pi} \sqrt{(1-\alpha V)^2 + \beta^2}\, \left[\left(1 - \frac{k^2}{2}\right) K(k) - E(k)\right] d\varphi \qquad (33)$$

Where

$$\alpha = \frac{a_s}{a_p} \qquad \beta = \frac{C}{a_p}$$

$$k^2 = \frac{4\alpha V}{(1+\alpha V)^2 + \beta^2}$$

$$V = \sqrt{1 + \frac{d^2}{a_s^2} - \frac{2d}{a_s}\cos\varphi}$$

In this case *C* equals zero because the two turns are in the same level

2) Lateral Misalignment

If the two turns are allocated at different levels, the mutual inductance between them can be calculated by:

$$M = \frac{\mu_o}{\pi} \sqrt{a_p a_s} \int_0^{\pi} \frac{\left(1 - \frac{d}{a_s}\cos\varphi\right)}{\sqrt{V^3}} \left(\frac{2}{k} - k\right) K(k) - \frac{2}{k} E(k) d \qquad (34)$$

Again the mutual inductance between each of the two turns of the two parallel coils can be summed by (32) to find the total mutual inductance.

VII. Results and Discussion

The representation of a wireless power transfer system with one to n-receivers is programmed in Matlab to calculate the mutual inductance between coils and then the efficiency.

A. Single Receiver System

As a starting point to investigate the previous analysis, a wireless power transfer system with two identical coils is practically implemented. Each coil, with 3cm radius, 21 turns and 3mm pitch between the turns, has an inductance equal to 18.6µH. One of them is the transmitter and the other is the receiver. Choosing specific parameters such as resonance frequency at 2.07 MHz, load resistor 50Ω, $C_1 = C_2 = 330pF$ (which includes the natural capacitance of the coil) and the distance between the two coils is 3cm. Next, finding the efficiency over a range of frequencies was achieved as shown in Fig.5. The theoretical results are compared with the experimental in the figure.

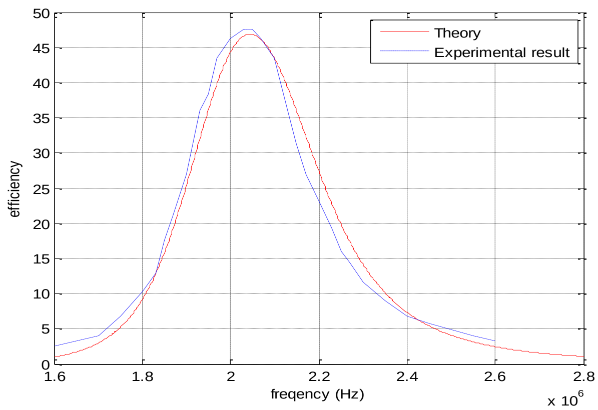


Fig. 5. Efficiency versus frequency at 3cm distance and f_o= 2.07MHz

It is clear from Fig.5 that the higher efficiency of 46% for wireless transfer happens at the resonance frequency and there is a good match between the theoretical and practical results. However, the efficiency here is relatively low, that is because of the small value of mutual inductance between the two coils. It is equal to 1.5468μH.

Replacing the two coils with another set of coils, which have higher inductance and higher mutual inductance between them, gives higher efficiency over larger distances at the same frequency as shown in Fig.6. In this experiment, each coil has 12.25cm radius, 8 turns and 3mm pitch between the turns, and 31.3 μH inductance. Working at the same frequency of 2.07MHz, 188pF capacitors are required for the transmitter and receiver. The system has an efficiency of 72% at 15.5 cm. This is as a result of the 2.1583 μH mutual inductance, which is larger compared to the previous experiment.

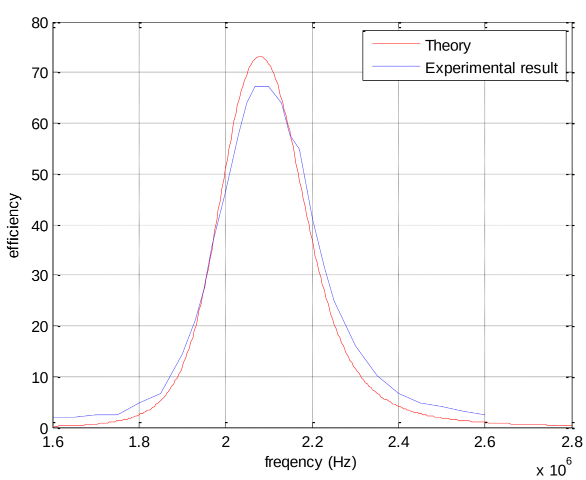


Fig. 6. Efficiency versus frequency at 15.5cm distance and f_o= 2.07MHz (Mutual Inductance Effect)

It was explained in section 6 that mutual inductance increases when the two coils approach. Fig.7 shows the effect of changing the distance between these two coils on the mutual inductance.

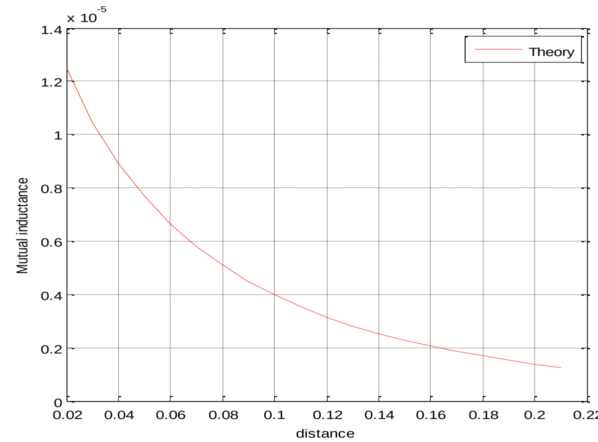


Fig. 7. Mutual inductance versus distance

Using the larger coils as in Fig.6, at smaller distances, the efficiency at the same resonant frequency gradually increases until it approaches the maximum value of 100% at a distance of 10cm as shown in Fig.8.

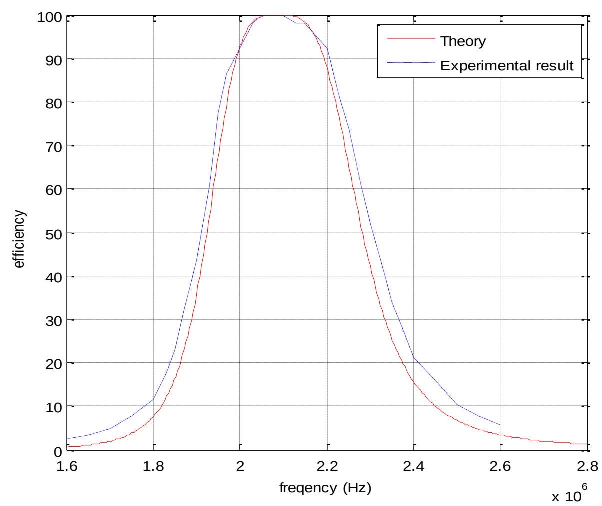


Fig. 8. Efficiency versus frequency at 10cm distance and f_o= 2.07MHz (Distance Effect)

A further decrease in the distance surprisingly leads to a decrease in efficiency of the system. As shown in Fig.9, there is a splitting in the efficiency of the system at a distance of 3.5cm. This splitting starts to appear as the mutual inductance increases between the two coils (the transmitter and the receiver), increasing when the two coils are approaching. This effect shifts the maximum efficiency to two distinct frequencies around the resonance frequency. This means that there is a perfect point to transfer the maximum power in the wireless system as shown in Fig.10 from the relation between the efficiency and the distance at the resonant frequency.

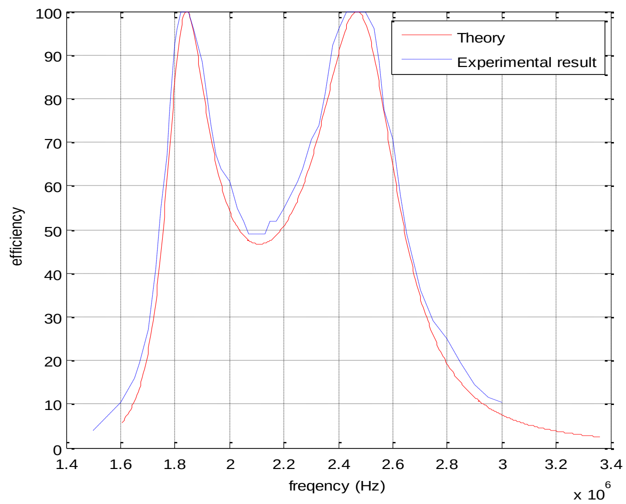


Fig. 9. Efficiency versus frequency at 3.5cm distance and f_o= 2.07MHz

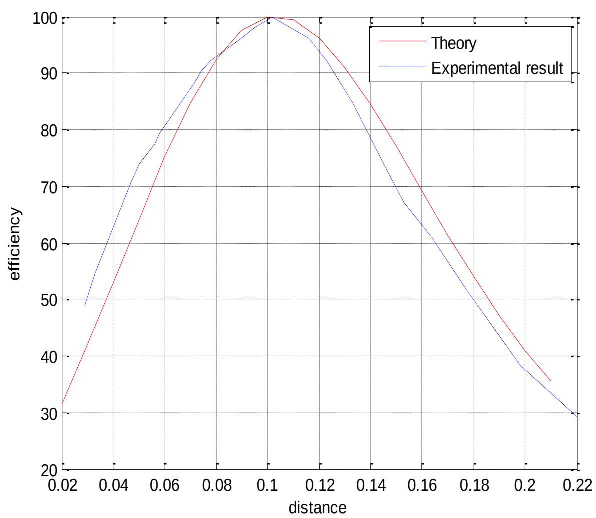


Fig. 10. Efficiency versus distance at resonant frequency

The reason for this point is shown in Fig.11, where the input resistance of the system, which changes with the distance, equals 50Ω at this point. The 50Ω value is equal to the input resistance of the source Z_{in} which leads to maximum transfer of power.

Working at a different frequency will also affect the efficiency of the wireless power transfer system. To show this effect, the capacitors of the transmitter and the receiver are changed from 188pF to 128pF. The results are shown in Fig.12. The efficiency of the system is shown at the resonant frequency of 2.5MHz with 15.5cm distance between coils. Compared to Fig.6 and Fig.8, the higher frequency enables the system to transfer more power through a larger distance. It can be concluded that the distance of the perfect point increases at higher frequency but is ultimately limited by the frequency and mutual inductance in both coils.

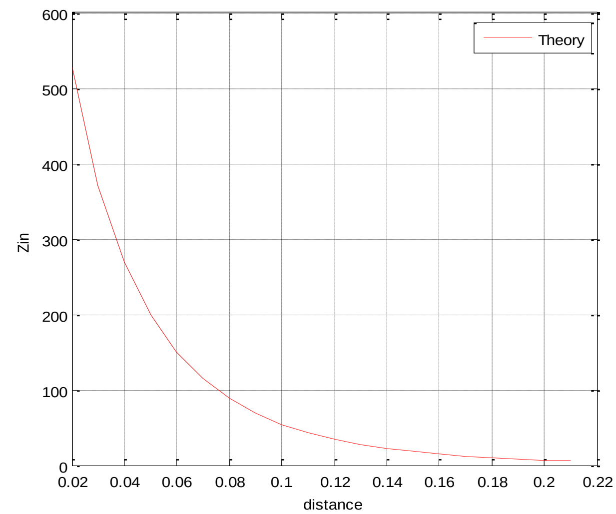


Fig. 11. Input resistance versus distance at resonant frequency

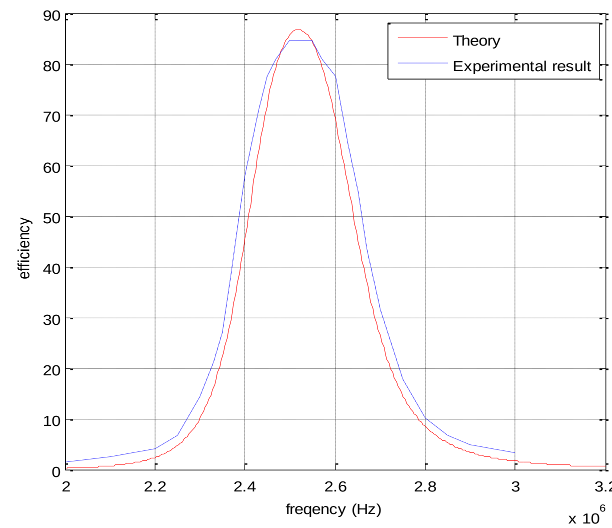


Fig. 12. Efficiency versus frequency at 15.5cm distance and f_o=2.5MHz (Resonance Frequency Effect)

Before studying multiple receivers it is necessary to study the efficiency of a small receiver with a large transmitter. The efficiency of a system with the large coil of 12.25cm and the small coil of 3cm is shown in Fig.13 at a resonant frequency of 2.07MHz and a distance of 3cm.

A. Two Receiver System

Using two identical receivers of 3cm radius and a transmitter of 12cm the efficiency of a two coil system is studied. The efficiency of a receiver can be affected by the presence of another receiver in the same field. Fig.14 shows the efficiency of each one of two closed receivers in the same transmitter field. The distance between their centres is 7cm. It appears from the figure that the efficiency here is less than it is in case of just one receiver as shown in Fig.13.

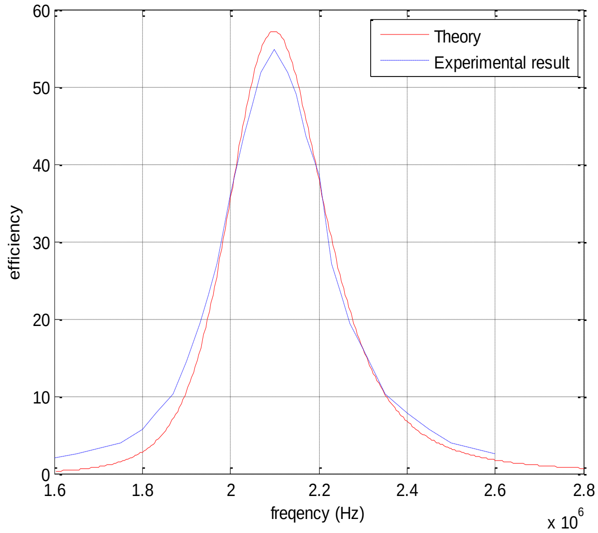


Fig. 13. Efficiency versus frequency at 3cm distance

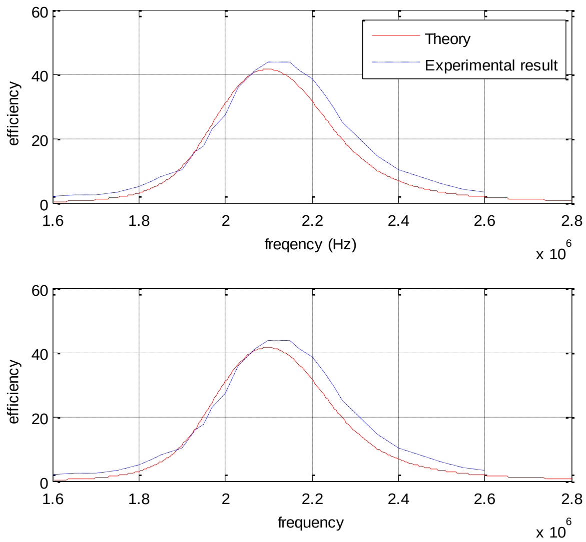


Fig. 14. Efficiency versus frequency for two receivers system

B. Three Receiver System

It is possible to apply our modelling and simulation approach for the case of more than two receivers, i.e. three to N. Fig.15 shows the efficiency of one of the three receivers if all three are together inside the field of the same transmitter. In this part the three identical receivers form a triangular shape at the same level. This means that the mutual inductance between any two of them are equal, which is 0.21076µH. Moreover, the mutual inductance between the transmitter and any one of the receivers are also equal which is 1.7358µH. Moving a receiver to another location in the same field requires a new calculation for the mutual inductance between coils.

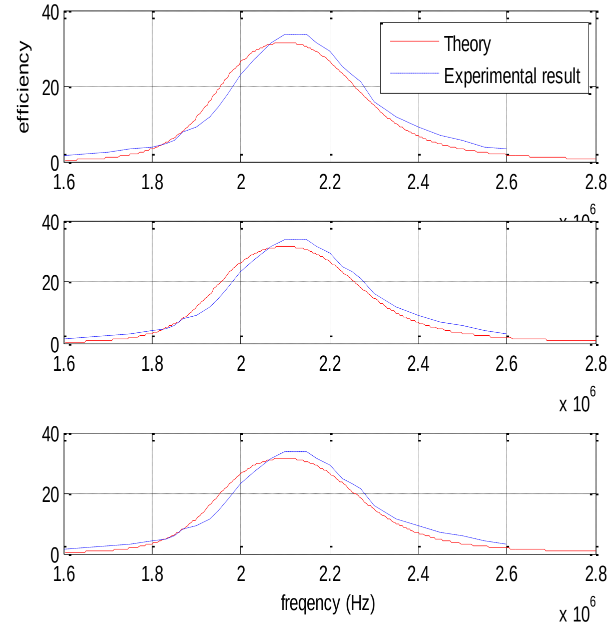


Fig. 15. Efficiency versus frequency for three receivers system

VIII. CONCLUSION

The mutual inductance between any two coils depends on their shape, their location and the distance between them. This study presented a method for the calculation of mutual inductance between any solenoid coils with a different location and distance.

The efficiency of a wireless power transfer system is dependent on factors such as: the resonance frequency; the size of the coils; the mutual inductance between them; the distance between coils and the presence of more than one receiver in the transmitter area. The following observations can be made:

- There is a specific distance, where the input resistance of the system equals the internal resistor of the source, at which point the system has the maximum efficiency and can transfer maximum power to the load.
- Higher frequency leads to an increase in the distance at which the system has the maximum efficiency subject to frequency and mutual inductance limitations.
- A Larger transmitter size, produces more flux around it, and also leads to an increase in the distance at which the system has the maximum efficiency.
- The Presence of more than one receiver gives decreased efficiency for each individual (compared to the larger coil), but the sum is greater than the efficiency of the same individual coil
- There are a number of practical limitations observed at higher frequencies regarding measurements

Applying the proposed method is an efficient and compact way to calculate the efficiency for a wireless power transfer system with one to N- receivers.

REFERENCES

[1] T. W. Versloot, D. J. Barker, and X. O. One, "Optimization of Near-Field Wireless Power Transfer Using Evolutionary Strategies," The 8th European Conference on Antennas and Propagation, Netherlands, 2014.

[2] J. Wang, S. Ho, W. Fu, and M. Sun, "Analytical design study of a novel WiTricity charger with lateral and angular misalignments for efficient wireless energy transmission," Magnetics, IEEE Transactions on, vol. 47, no. 10, pp. 2616-2619, 2011.

[3] A. Mahmood, A. Ismail, Z. Zaman, H. Fakhar, Z. Najam, M. Hasan, and S. Ahmed, "A Comparative Study of Wireless Power Transmission Techniques," Journal of Basic and Applied Scientific Research, vol. 4, no. 1, pp. 321-326, 2014.

[4] O. Rönnbäck, "Optimization of Wireless Power," 2013.

[5] T. Imura, and Y. Hori, "Maximizing air gap and efficiency of magnetic resonant coupling for wireless power transfer using equivalent circuit and neumann formula," Industrial Electronics, IEEE Transactions on, vol. 58, no. 10, pp. 4746-4752, 2011.

[6] V. Jiwariyavej, T. Imura, and Y. Hori, "Coupling Coefficients Estimation of Wireless Power Transfer System via Magnetic Resonance Coupling using Information from Either Side of the System," in Proc. International Conference on Broadband and Biomedical Communication, Australia, 2012.

[7] D. Chaurasia, and S. Ahirwar, "An Optimal Parameter Estimation Technique for Wireless Electricity Transmission," Research India Publications, vol. 3, no. 1, pp. 1-9, 2013.

[8] H. Shim, J. Park, S. Nam, and B. Lee, "A criterion Proposed for Inductive Coupling and Magnetic Resonance Coupling in Wireless Power Transfer System, " Microwave Conference (APMC), 2014 Asia-Pacific. IEEE, 2014.

[9] T. Beh, M. Kato, T. Imura, and Y. Hori, "Wireless Power Transfer System via Magnetic Resonant Coupling at Fixed Resonance Frequency―Power Transfer System Based on Impedance Matching―," EVS-25 Shenzhen, China, 2010.

[10] J. Gozalvez, "WiTricity-the wireless power transfer [Mobile radio]," Vehicular Technology Magazine, IEEE, vol. 2, no. 2, pp. 38-44, 2007.

[11] M. Yasir, and M. S. Haque, "The Witricity: Revolution in Power Transmission Technology," International Journal of Scientific & Engineering Research, vol. 4, no. 8, pp. 565-570, 2013.

[12] A. C. M. de Queiroz, "Mutual inductance and inductance calculations by Maxwell's Method," Home page of Dr. Antonio Carlos M. de Queiroz, 2005.

[13] C. Akyel, S. I. Babic, and M.-M. Mahmoudi, "Mutual inductance calculation for non-coaxial circular air coils with parallel axes," Progress In Electromagnetics Research, vol. 91, pp. 287-301, 2009.

[14] Y. Zhang, Z. Zhao, and K. Chen, "Frequency-Splitting Analysis of Four-Coil Resonant Wireless Power Transfer," Industry Applications, IEEE Transactions on, vol. 50, no. 4, pp. 2436-2445, 2014.

Grid Color Moment Features in Glaucoma Classification

Abir Ghosh
St Xavier's College, Kolkata, INDIA

Anurag Sarkar
St Xavier's College, Kolkata, INDIA

Amira S. Ashour
Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University, EGYPT

Dana Bălas-Timar
Aurel Vlaicu University of Arad, ROMANIA

Nilanjan Dey
Department of Information Technology,
Techno India College of Technology, Kolkata, INDIA

Valentina E. Balas
Faculty of Engineering
Aurel Vlaicu University of Arad, ROMANIA

***Abstract*—Automated diagnosis of glaucoma disease is focused on the analysis of the retinal images to localize, perceive and evaluate the optic disc. Clinical decision support system (CDSS) is used for glaucoma classification in human eyes. This process depends mainly on the feature type that can be morphological or non-morphological. It is originated in the retinal image analysis technique that used color feature, texture features, extract structure, or contextual. This work proposes an empirical study on a narrative automated glaucoma diagnosis, classification system based on both Grid Color Moment method as a feature vector to extract the color features (non-morphological) and neural network classifier. Consequently, these features are fed to the back propagation neural network (BPNN) classifier for automated diagnosis. The proposed system was tested using an open RIM-ONE database with accurate gold standards of the optic nerve head. This work classifies both normal and abnormal defected retina with glaucoma images. The experimental results achieved an accuracy of 87.47%. Thus, the proposed system can detect the early glaucoma stage with good accuracy.**

***Keywords*—Glaucoma; Clinical decision support system; RIM-ONE image database; Classifier; Back Propagation Neural Network; color feature extraction; Grid Color Moment**

I. Introduction

Medical image processing is a promising domain that various researches try to develop as in [1-10]. Since, Glaucoma is one of the main reasons for blindness worldwide that affect around 80 million people by 2020. It is a disease that damages the optic nerve (ON) due to incessant increase in the intraocular pressure (IOP) in the eye, which can lead to vision loss and cause blindness. Thus, early diagnosis of glaucoma is necessary to prevent vision loss. Globally, glaucoma is a significant cause of vision loss that excessively affects women and Asians [11]. Additionally, glaucoma enlarges the cup size, which affects the optic disc (OD). Where the Optic disc is the observable portion of the optic nerve from which the nerve fibers exit the eye [12].

Hence, early diagnosis, detection and treatment of glaucoma are the only ways to prevent vision impairment and blindness. There are three well-established standard tests used by ophthalmologists to diagnose glaucoma: i) the IOP measurements [13, 14], ii) the assessments of the optic nerve (stereoscopic) [15], iii) Visual field tests.

Moreover, other measurements that calculate the changes in the retinal nerve fiber layer (RNFL) thickness or the ocular blood flow can be performed for glaucoma diagnosis. Jointly, these methods afford information on both structural and functional defects that require digital image analysis for recognizing the natural growth of the disease. This relies on qualitative assessments of the eye using computational techniques. Where, conventional ophthalmologist manufactures diagnoses are based on the doctor’s experience and individual judgment. Therefore, automatic retina image analysis is considered a screening tool [16] for early detection of diseases. Thus, the main parameter that can be used with the screening programs is the OD [17] for diagnosis and to identify glaucoma.

Generally, automated CDSSs in ophthalmology are designed mainly for the identification of the disease pathology in human eyes. It is used to facilitate clinicians in diagnosis, support clinical decision-making and to reduce variability/ time. These systems are used for automated pattern recognition and image analysis that requires feature extraction.

Since, the feature is an attribute that can capture a definite visual image property, either locally for objects or globally for the whole image. Thus, texture feature classification is used for glaucoma diagnosis. An assortment of approaches can be derived from texture features such as: signal processing (Gabor and Wavelet transformation) [18, 19], co-occurrence matrices [20], Fourier power spectrum [21] and correlation features, neural networks [22], etc.

Meanwhile, color is invariance with regard to image translation, scaling, and rotation. Therefore, color is considered a significant feature for image representation that is extensively used in image recovery and analysis.

Recent studies are concerned with the automatic feature extraction procedures in retinal images for automatic glaucoma detection. Typically, detection/ classification of the glaucoma by means of retinal image are controlled by the features selection and feature extraction approaches. The extracted features are then used as input to a classifier to determine the glaucoma class.

The feature type is divided into two categories, namely: I) morphological (requires segmentation process before measuring the geometric parameters), and II) non-morphological (doesn't require segmentation process and considers image-based features). Texture, shape, and color are features captured from the image without segmentation.

Through the CDSSs, features extracted are sorted into two types: structural features and texture features. Structural features commonly include the disk diameter, disk area, cup diameter, cup-to-disk ratio, rim area, and the topological features extracted from the image [23]. Approaches using non-morphological features such as color feature extraction for classification are promising at medical image classification tasks. That is based on Grid color moment, which represents the feature vector of the image.

Since, classification plays a significant role in the detection of some diseases in their early phases, such as diabetes that can be accomplished via comparison of the states of retinal blood vessels. Thus, our research is focused on a novel automated classification system for glaucoma. The extracted features can then be fed to the Back propagation neural network (BPNN) classifier to distinguish between normal and glaucomatous images accurately. To test the proposed system, the RIM-ONE database, a fundus image database is used for glaucoma disease.

The remaining part of this paper is organized as follows. Section II includes related work, followed by section III that represents the methodology via data acquisition and the proposed system. In section IV, the color feature extraction concept is presented, while the BPNN network classifier used for the glaucoma automated diagnosis is discussed in section V. The results obtained and the discussion is introduced in section VI. Finally, the paper is concluded and goes through the future work in section VII.

II. Related Work

Numerous studies focused on early detection of glaucoma, the objective/ quantitative measurements of the RNFL are calculated. Some of the prominent existing modalities for eye imaging are such as optical coherence tomography (OCT), Multifocal electroretinograph (mfERG), etc. have been used for the thickness and phase retardation; respectively. The application of OCT technology in clinical glaucoma practice has largely centered on imaging the peripapillary RNFL. This approach proved its sufficiency for assisting the clinician in both diagnosing glaucoma and detecting disease progression [24, 25].

Bock *et a*l. [26] used non-morphological features that carried out via feature extraction methods such as Gabor Filter (textures), pixels intensity values, histogram model and Fourier Transform (FFT). The results achieved 86% accuracy with 2-stage classification and Support vector machine (SVM) classification methods. Archana in [27] initiated the Computer Based Diagnosis of glaucoma using digital fundus images. Where, images with different color variation inside the eye were compared using images taken by high definition laser camera. To identify whether the eye is suffering from glaucoma, a test is made using the image of a normal eye that is kept as a reference (zero) and then compared to the clinical observations of the person's image.

Matsopoulos *et al*. used 127 blood vessels fundus image database of the optic nerve head (ONH) a feature to detect glaucoma based on the blood vessel shape [28]. For classification the authors used multilayered Artificial Neural Network (ANN), which achieved 87.5% accuracy. A narrative glaucoma detection system via an arrangement of texture and higher order spectra features suggested by Rajendra *et al*. provided accuracy of more than 91% [29].

Yogesh and Sasikala illustrated texture analysis of the retinal layers in spectral domain OCT images to diagnosis the retinal disorders [30]. A method for automated segmentation of the SD-OCT images was presented with the texture analysis for the diagnosis of fluid filled regions associated with retinal disorders. Surfaces and features were extracted in each surface locally to distinguish texture properties across the macula. Classification was done based on 22 texture feature values. If the feature value deviates from the preset normal range, this indicates detected abnormalities. This work aimed to extract textural information from the SD-OCT scans that can be used for clinically important applications.

The authors in [31] developed a method for the RNFL texture classification based on Markov random fields. Two supervised classifiers named linear Ho-Kashyap rule and nonlinear Bayesian classifier based on Gaussian mixture model (GMM) were implemented. The experiments showed that the proposed textural features were reliable for RNFL texture descriptors using the fundus-OCT data pairs.

While, in [32] a glaucomatous image classification using texture features within images and efficient glaucoma classification based on Probabilistic Neural Network (PNN) of examining the efficiency of the features extracted was proposed. A wavelet-based texture feature set has been used for feature extraction.

Energy distribution over wavelet sub bands was applied to compute these texture features. Wavelet features were attained from the daubechies (db3), symlets (sym3), and biorthogonal (bio3.3, bio3.5, and bio3.7) wavelet filters. It uses to distinguish between normal and glaucomatous images through the proposed technique to extract energy signatures obtained using 2-D discrete wavelet transform and the energy obtained from the detailed coefficients. The observed accuracy, using features by DWT was around 95%, this demonstrates the effectiveness of these methods.

In order to early detection of glaucoma progression, the authors in [33] introduced a solution for the retinal nerve fiber layer loss estimation using fractal dimension (FD) and texture feature.

This enabled more comprehensive assessment of the retinal nerve fiber layer and was performing glaucoma detection using RNFL loss determining. Spearman correlation co-efficient was estimated for FD and texture feature for healthy, medium loss, and severe loss RNFL were 0.85, 56, and 35 respectively.

The proposed features can be used as a part of feature vector in glaucoma risk. The authors suggested that these features can be used in the glaucoma screening program together with other features such as RNFL thickness, etc. based on different methods.

In [34] a modified spatial fuzzy C-means for glaucoma detection has been applied using retinal images. The authors deployed both the K-Means clustering and C-Means clustering which provided accurate results.

Therefore, the proposed study employed a non-morphological feature extraction via Grid Color Moment method, that to be the input to the BPNN classifier to distinguish between the normal and glaucoma cases.

III. Methodology and Proposed System

A. Data Acquisition

There are numerous public databases for retinal fundus images that are available for glaucoma research to automatically extract the features for glaucoma detection. An Open Retinal Image Database for Optic Nerve Evaluation (RIM-ONE) is a fundus image database that is related to glaucoma disease. I

It consists of 169 ONH images, where the images are divided into several classes as follows: normal 118 images, early glaucoma 12 images, moderate glaucoma 14 images, deep glaucoma 14 images and ocular hypertension (OHT) 11 images [35, 36]. In this study the RIM-ONE database is employed as it is considered precise gold standards of the ONH.

Fig. 1 demonstrates normal and abnormal glaucomatous images taken from the RIM-ONE database. Even if the images are clear, using the naked eye one can’t distinguish between the normal (healthy) images and the abnormal (glaucoma) images, which necessities the automated system development. In recent years, the progress in digital imaging technologies generated a large growth in the number of digital images taken.

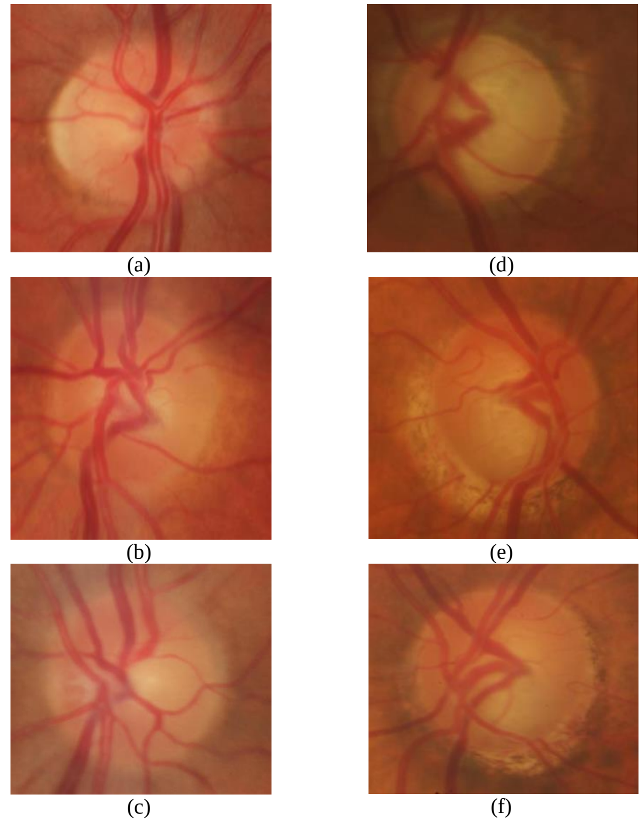


Fig. 1. Eye RIM-ONE database images: (a, b, c) Normal image, (d, e, f) Glaucoma image (abnormal)

B. Proposed System

The block diagram of the proposed system is illustrated in Fig. 2. It is divided into two subsystems, namely offline and real time systems. This work distinguishes between normal and glaucoma affected retina. Several features are required to be extracted using the Grid color moment that provides obvious results for distinct identification and classification. The classification method proposed is the use of a neural network classifier with the help of texture feature extraction of the localized area of the optic cup of images. The entire set of the RIM-ONE images (normal, abnormal) are attained in the first step in the offline mode. The Grid color moment features are then extracted from the RIM-ONE database images. Then, the extracted features are fed into the back-propagation neural network (BPNN) classifier. In the real time mode, the database images are used to extract the significant features and fed to the trained classifier for classification. It then performs the classification into normal and abnormal glaucoma classes based on the extracted significant colored texture features.

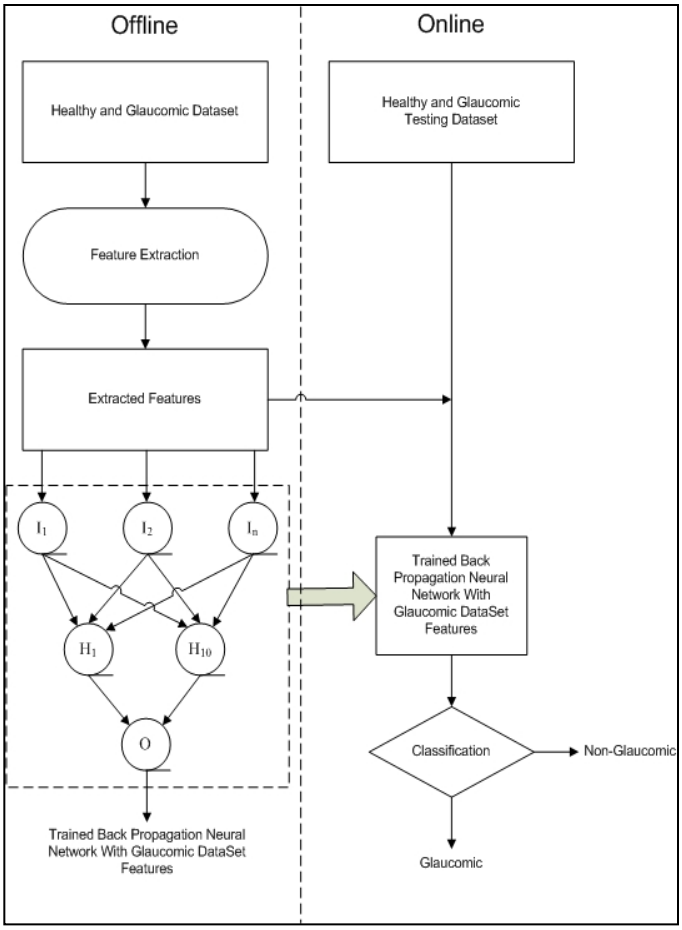


Fig. 2. The Automated Glaucoma Diagnosis Proposed System

IV. Color Feature Concept

Typically, morphological feature extraction methods can produce features such as the disc diameter, cup diameter, and the neuroretinal rim. While, the features that can be formed with non-morphological feature extraction methods are such as parapapillary atrophy (PPA), RNFL and blood vessels. Septiarini and Harjoko recommended using non-morphological features for glaucoma detection as it yields higher accuracy than using morphological features [37]. Visual indexing procedures can be categorized into: pixel domain and compressed domain. The former is based on features as texture, color/histogram, shape, while the compressed domain indexing procedures can be generally classified into spatial domain and transform domain techniques.

Based on [37] this study is based on color features (non-morphological features) for glaucoma classification. Color feature is one of the broadly used features in low level feature. Compared with texture- and shape- feature, color feature provides superior stability and is further insensitive to the zoom of image and the rotation. There are several color descriptors such as color moment, Color Coherence Vector (CCV), and color histogram.

Color histogram is used to describe the color distribution in an image. However, since there is no local association between information on the color histograms, thus it cannot differentiate between objects [38]. To compensate this disadvantage, grid color moment can be used. Color moment represents the color distribution using standard deviation, mean and the third root of the skewness of each color channel [39].

The mean, variance, and standard deviation are described for an image of size $N \times M$ pixels as follows:

$$\bar{z} = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} z_{ij}}{NM} \quad (1)$$

$$\gamma^2 = \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(z_{ij} - \bar{z}\right)^2 \quad (2)$$

Where z_{ij} is the pixel intensity in H/S/V channels of the pixel in row i and column j. In addition, the skewness (H/S/V) is computed by:

$$\eta = \frac{\frac{1}{nm}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(z_{ij} - \bar{z}\right)^3}{\left(\frac{1}{nm}\sum_{i=1}^{N}\sum_{j=1}^{M}\left(z_{ij} - \bar{z}\right)^2\right)^{3/2}} \quad (3)$$

Using the Grid Color Moment which is the feature vector for a given image, the algorithm used is [40]:

Algorithm: Grid color moment

Start
Input: colored RGB (Red-Green-Blue) image
Procedure:
Convert the image from RGB for HSV color space
Divide uniformly the image into 3x3 blocks
Compute the mean color (H/S/V) using equation (1) for each of these nine blocks
Compute its variance (H/S/V) using equation (2)
Compute its skewness (H/S/V) using equation (3)
Perform normalization for each of the 81 features by:

1- ***Compute*** the mean and standard deviation from the training dataset

$$\lambda = \frac{1}{G}\sum_{k=1}^{G} R_k \quad (4)$$

$$\sigma = \sqrt{\frac{1}{G}\sum_{k=1}^{G}\sum_{j=1}^{M}\left(R_k - \lambda\right)^2} \quad (5)$$

Where, G is the number of images in the training database, and R_k is the feature of the k^{th} training sample.

2- ***Perform*** the "whitening" transform for all the data (including both the training data and the testing data), and get the normalized feature value:

$$R_k^{'} = \frac{R_k - \lambda}{\sigma} \quad (6)$$

Output: normalized color feature vector
End

Where, each block 9 features, and thus the entire image will have 9x9=81 features. It is noted that the normalization step is done for the 81 features to achieve good numerical behavior before performing the classification that will be discussed in the next section.

V. Neural Network Classifier

Color feature analysis is imperative in numerous applications of computer image analysis for classification/ segmentation of medical images based on local spatial variations of intensity or color. The objective of the color classification is to allocate an indefinite sample image to one of a set of recognized color classes. A significant application area in classifications based color are industrial and biomedical surface examination, such as discovering the defects and disease, satellite or aerial imagery classification, etc.

The classification of color features is useful to an ophthalmologist's clinical analysis and engages separating the selected feature space according to the glaucoma class. Image classification is the facility to split normal and abnormal (glaucoma affected) regions by applying feature based image extraction methods. Classification is classically achieved using an assessment function.

In the proposed system, the Neural Network based back-propagation (BPNN) classifier is used for the automated diagnosis of glaucoma. The BPNN is briefly clarified below:

A. *Neural Network*

A significant tool for the classification is the Neural networks (NN). Recent neural classification has ascertained that NN is a capable alternative to diverse conventional classification methods. The neural network improvement appeared in [41], as it's used for medical application. Neural networks have various features as follows:

- Are data driven, self-adaptive techniques that can adjust themselves to the data, without any clear specification of with the underlying model.
- Can approximate any function with arbitrary accuracy.
- Are nonlinear models that are able to modeling complex real world applications.
- Provide the basis in set up the classification rules and achieve statistical analysis.
- Are successfully applied to an extensive variety of real world classification such as speech recognition, medical diagnosis, etc.
- Play a vital role in classifications using its supervised and unsupervised techniques.

The NN architecture is made up from input, output and one or more hidden layers. Input layer represents the raw information that is fed into the network. Each neuron in a particular layer is connected with all neurons in the next layer. The connection between the i^{th} and j^{th} neuron is characterized by the weight coefficient W_{ij} and the i^{th} neuron by the threshold coefficient ϑ_i. The weight coefficient replicates the degree of significance of the given connection in the neural network. The output value (activity) of the i^{th} neuron x_i is determined as follows [42]:

$$x_i = q(\psi_i) \tag{7}$$

$$\psi_i = \vartheta_i + \sum_{j \in \Gamma_i^{-1}} W_{ij} x_j \tag{8}$$

Here, ψ_i is the i^{th} neuron potential and the function $q(\psi_i)$ is the transfer function.

The supervised adaptation process varies the threshold coefficients and weight coefficients to minimize the sum of the squared differences between the computed and required output values. This is achieved by minimization of the objective function p:

$$P = \sum_o \frac{1}{2}\left(x_o - \hat{x}_o\right)^2 \tag{9}$$

x_o and $\hat{x}_o$ are the computed and required activity vectors of the output neurons; respectively.

B. *Back-propagation Neural Network (BPNN)*

One of the trendiest NN algorithms is back propagation algorithm. Rojas in [43] declared that the BP algorithm could be broken down to four main steps. After choosing the weights of the network randomly, the back propagation algorithm is used to compute the compulsory corrections. The algorithm can be decomposed in the following four steps: i) Feed-forward computation ii) Back propagation to the output layer iii) Back-propagation to the hidden layer iv) Weight updates. The algorithm stops when the value of the error function has become adequately small.

The steepest-descent minimization method is used in the back-propagation algorithm. For adjustment of the weight and threshold coefficients it holds that:

$$W_{ij}^{(k+1)} = W_{ij}^{(k)} - \lambda\left(\frac{\partial P}{\partial W_{ij}}\right)^{(k)} \tag{10}$$

$$\vartheta_{ij}^{(k+1)} = \vartheta_{ij}^{(k)} - \lambda\left(\frac{\partial P}{\partial \vartheta_{ij}}\right)^{(k)} \tag{11}$$

λ is the learning rate. The calculation of the derivatives $\left(\frac{\partial P}{\partial \vartheta_{ij}}\right)$ and $\lambda\left(\frac{\partial P}{\partial W_{ij}}\right)$ is the key parameter of the algorithm.

For cluster based classification of medical images, neural networks are constructive. This method can be used in computer-aided diagnostic decision making.

C. Performance measures

To perform the classification using the extracted features, the entire dataset is divided into parts. The experimental dataset contains both normal and glaucoma images. The process begins with the training of 80% of the data and 10% for testing. Then, the validation was done using the remaining 10% part. The accuracy, PPV (positive predictive value), sensitivity and specificity are computed for each iteration. The average of all ten folds gives the actual accuracy, PPV, sensitivity and specificity.

VI. Results and Discussion

In this study, Grid color moment feature based glaucoma classification using back propagation network has been proposed.

A. Classification Results

In the current study, features were computed. Individually, if these features are considered using the proposed model, then the corresponding classification obtained accuracies were shown in Table 1. Table 1 reported the effective classification accuracy (87%) with the Grid color moment feature.

In this work, high risk of the proposed system signifies the glaucoma and low risk of the proposed system signifies non-glaucoma (normal) cases. While, defining the standard performance metrics, four parameters were adapted for performance analysis named the True Negative (TN), True Positive (TP), False Negative (FN) and False Positive (FP).

TN involves the total number of non-Glaucomic cases in the proposed system that is classified as Glaucomic cases. TP is the total number of Glaucomic cases in proposed system that is classified as Glaucomic cases.

FN indicates the total number of non-Glaucomic cases in the proposed system that is classified as Glaucomic cases. FP is the total number of Glaucomic cases in proposed systems that are classified as non-Glaucomic cases.

These metrics are shown in the confusion matrix illustrated in Fig. 3.

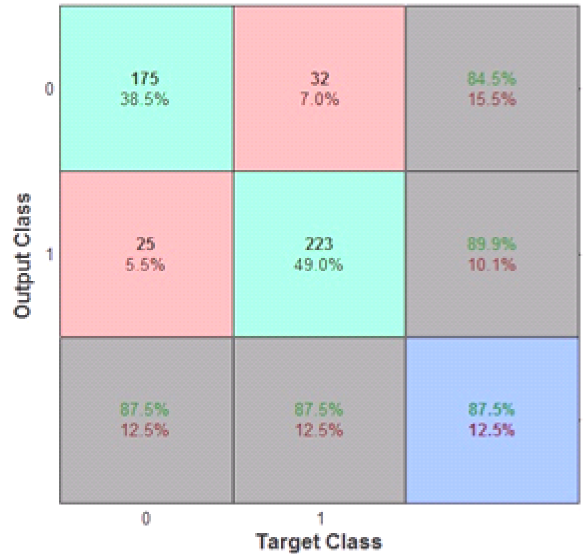


Fig. 3. Confusion Matrix

From Figure 3, it is clear that in case of Grid color moment analysis, the TP and TN values are 38.5% and 7% and FP and FN are 49% and 5.5%; respectively. Supplementary metric measures are computed using the previous four parameters as follows.

1) Sensitivity: is identified as the probability that a classifier will mark a Glaucomic label for Glaucomatous dataset, and is computed as:

$$\text{Sensitivity}=\frac{\text{TP}}{(\text{TP+FN})} \tag{12}$$

2) Specificity: is a measure of the probability that the classifier will result in a non-Glaucomic label when used on low risk Glaucomic patients and is calculated as:

$$\text{Specificity}=\frac{\text{TN}}{(\text{TN+FP})} \tag{13}$$

3) Positive predictive value (PPV): is described as the probability of patient's label as Glaucomic correctly diagnosed, is denoted as:

$$\text{PPV}=\frac{\text{TP}}{(\text{TP+FP})} \tag{14}$$

4) Negative predictive value (NPV): is the probability of patient's label as Glaucomic incorrectly diagnosed and is calculated as:

$$\text{NPV}=\frac{\text{TN}}{(\text{TN+FN})} \tag{15}$$

5) Accuracy: is the ratio of the number of correctly classified Glaucomic patients to the Glaucomic patients, and is calculated as:

$$\text{Accuracy}=\frac{\text{TP+TN}}{(\text{TP+TN+FP+FN})} \tag{16}$$

Since, a high specificity and high sensitivity indicate an ideal test scenario. A positive outcome in this case means the condition is likely and a negative outcome in this case means the condition is unlikely. The proposed Grid color moment approach achieved 87.50% Sensitivity, 87.45% Specificity, PPV of 84.54% value, NPV of 89.92%, and 87.47% accuracy.

In fig. 4, the regression curves are shown for the different features used. It demonstrates the network outputs with respect to targets for training, validation, and test sets. The dashed line indicates the perfect result – outputs = targets. The solid line specifies the best fit linear waning line between the outputs and targets. The linear regression (R) value identifies the connection between the outputs and the targets. If R = 1, this characterizes an exact linear relationship between the outputs and targets. If R is near to zero, then there exists no linear relationship between outputs and targets. In this study, R=0.78, which denotes some linear relationship between outputs and targets, where (output=0.65*Target+0.18).

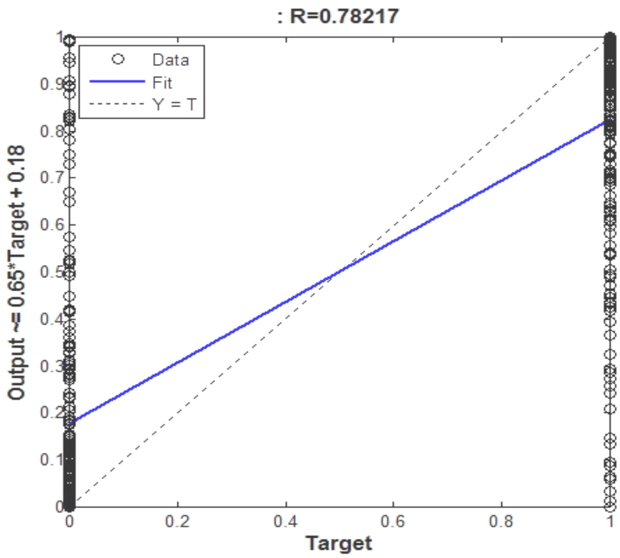


Fig. 4. Regression curve

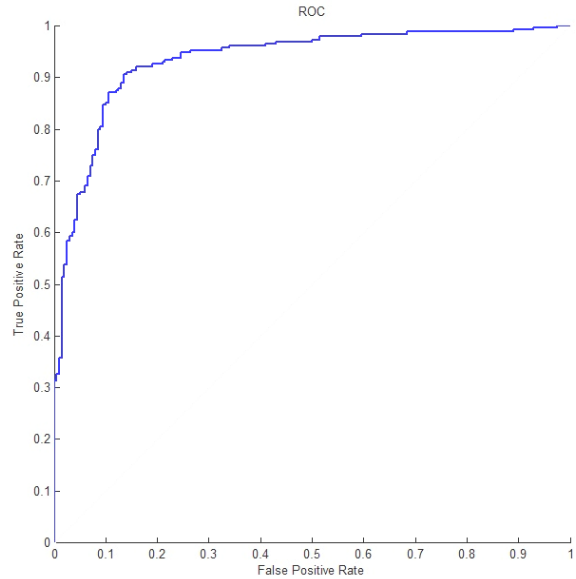


Fig. 5. The ROC curve

The Receiver Operating Characteristic (ROC) curve shown in Fig. 5 facilitates the classifiers' performance measurement. This graph has a plot that indicates the false positive rate on the X axis and the true positive rate on the Y axis. The point (0,1) indicates the perfect classifier. It performs accurate classification for all the positive cases and negative cases correctly. The (0,1) point denotes that the false positive rate is 0 (none) and the true positive rate is 1 (all). The (0,0) point denotes a classifier that predicts all the cases to be negative, whereas the point (1,1) corresponds to a classifier that predicts each and every case to be positive. Point (1,0) is the classifier which represents that it is incorrect for all the classifications. From Fig. 5, it is clear that the Grid color moment RCO curve has decreased error slowly, which yields to improved RCO.

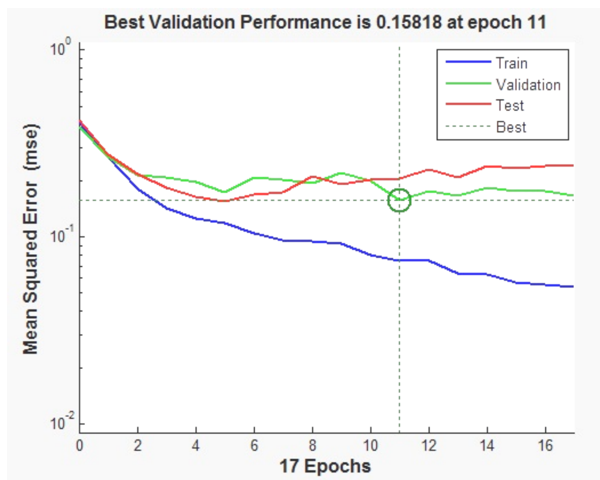


Fig. 6. Performance validation

Figure 6 designates the Performance validation, as it includes all information concerning the training of the neural network. The trace of a matrix (tr) structure assists in tracking different variables during the training, such as the gradient magnitude, the value of the performance function, etc. The property (tr) best epoch finds the number of iterations for which the validation performance has a minimum value.

In this study, best validation performance is 0.158 at the 11th using the Grid color moment approach. The neural network model which performs a function approximation task will be using a continuous error metric such as mean squared error (MSE). All the errors will be summed up over the validation set of inputs and outputs, and then normalized by the size of the validation set.

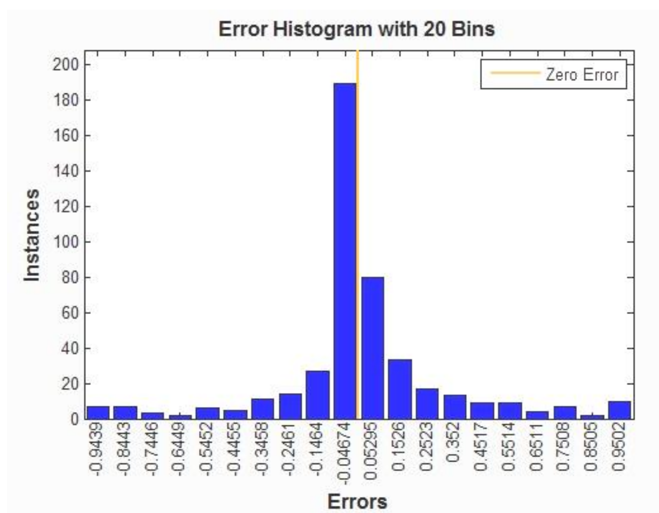


Fig. 7. Error histogram

Fig. 7 illustrates the error histogram with the 20th bin. It is used to attain additional verification of network performance. In figure 7, the blue bars represent training data. The histogram can provide an indication of outliers, which are data points where the fit is extensively worse than the majority of data. The error is calculated as the (Target-network output). The large center peak specifies very small errors that refer to output that is very close to the targeted value.

Commonly, numerous studies have been conducted on the classification of normal and glaucoma classes. Further, most of the work carried out in the literature classifies the RIM-ONE database images into normal and glaucomatous classes. Classification of normal and glaucoma images using Grid color moment feature vector provided 87.47% accuracy.

The main contribution of this current study has been achieved as:

1) Developed an algorithm that automatically analyzes the retina images and classifies normal images and diseased glaucoma images with indicating the defected portions.

2) Neural Network is used to automatically classify the images as normal or abnormal eye images. The proposed system automatically extracts features and uses them with the BPNN classifier to predict the class (normal, glaucoma).

3) The proposed system is able to automatically identify the abnormal subjects as abnormal with an NPV of 89.92%, as the Specificity of the system is 87.45% and accuracy.

4) From all the previous experimental results, the proposed method is able to diagnose the early stage of glaucoma with an accuracy of 87.47%.

5) Using the color features based Grid color moment approach to detect the early stage of glaucoma is the novelty of this paper.

VII. Conclusion and Future Work

Glaucoma is a disease which arises by the deterioration of the optic nerves (optic disc). It is an optic neuropathy that causes the loss of retinal ganglion cells and damage to the retinal nerve fiber layer (RNFL). The CDSS is based on the retinal image analysis techniques to extract structural, textural or contextual features from the images. Therefore, it is able to effectively differentiate between normal and glaucoma diseased samples. Retinal image analysis is based on computational techniques to make a qualitative inspection of the eye more objectively.

Therefore, enormous studies have been working in the domain of the automated diagnosis of glaucoma disease. These studies have been focused on the analysis of retinal database images to localize, detect and evaluate the optic disc. An open RIM-ONE database images with accurate gold standards of the optic nerve head is implemented in the current study. Classification of the glaucoma affected eye has been performed via training the BPN.

Widespread research has been carried out for efficient eye disorder and glaucoma treatment and a number of research reports have been submitted with different accuracy levels for different diagnostic methods. In this paper, a CDSS system based on color features and a multiple NN classification scheme is presented. The major goal of this method is to reduce the changeability that is arising between different clinical diagnoses of the structural characteristics of the human eye. As well as preventing the vision loss with the early identification and diagnosis of glaucoma.

In the proposed system, the back propagation neural network classifier is used to classify normal and abnormal glaucoma retinal images. The Grid color moment that indicates the feature vector extracted from the whole image for the region of interest (ROI) proves its efficiency as it provides 87.47% accuracy that shows the effectiveness of the proposed system.

As a suggested future work:

1) Design a complete, integrated, automated system to classify all different types of glaucoma namely: Primary Open-Angle Glaucoma, Normal Tension Glaucoma, Angle-Closure Glaucoma, Acute Glaucoma, Pigmentary Glaucoma, Exfoliation Syndrome and Trauma-Related Glaucoma.

*2) Develop a system that combines the three test parameters for diagnosis**.** For example, features extracted from cup to disk ratio and RFNL can be used for classification and can be used to develop a glaucoma risk index (GRI) which can classify the different stages of glaucoma with just a single number.*

3) Make ranking for the features discrimination index.

4) Add pre-processing step, for de-noising.

5) Combine both color and texture feature extraction: contribute to determine the visual appearance of images in a different way.

6) Use another modified NN instead of the BP, and compare with the current. Also, use different classifiers and compare the results.

7) Make test on various fundus databases to prove the proposed system robustness. Also, to increase the accuracy of the system further using huge databases with diverse images, another nonlinear feature and better classifiers.

8) Measure the complexity and the convergence time for each feature.

9) In order to obtain high performance, clinically significant features essential to be extracted from diverse huge database. This will necessitate a huge storage space for the CAD system.

10) Use a combination of different features for automatic glaucoma detection/ classification.

11) Perform classification of glaucoma that is not only distinguished as normal or glaucoma, but the several stages of glaucoma (early, mild and advance).

References

[1] N. Dey, and A. Das, "Shape & Size Analysis of Mineral Grains From photomicrographs Using Harris Corner Detection," International Journal of Advances in Engineering, Science and Technology (IJAEST), vol.2, no. 2, 2012.

[2] N. Dey, B. Nandi, A. B. Roy, D. Biswas, A. Das, and S. S. Chaudhuri, "Analysis of Blood Cell Smears using Stationary Wavelet Transform & Harris Corner Detection," Recent Advances in Computer Vision and Image Processing: ethodologies and Applications, pp-357-370, 2013.

[3] N. Dey, M. Pal, and A. Das, "A Session Based Watermarking technique Within the NROI of Retinal Fundus Images for Authencation Using DWT, Spread Spectrum and Harris Corner Detection," International Journal of Modern Engineering Research, vol. 2, no.3, pp.749-757, 2012.

[4] N. Dey, A. B. Roy, and A. Das, "Detection and Measurement of Bimalleolar Fractures Using Harris Corner," ICACCI-2012 Chennai, India, pp.3-5, 2012.

[5] N. Dey, A. S. Ashour, A.S. Ashour, and A.Singh, "Digital Analysis of Microscopic Images in Medicine," Journal of Advanced Microscopy Research, vol.10, pp.1-13, 2015.

[6] S. Hore, S. Chakroborty, A. S. Ashour, N. Dey, A. S. Ashour, D. sifaki-pistolla, T. Bhattacharya, and S. R. Chaudhuri, "Finding contours of Hippocampus Brain Cell using Microscopic Image Analysis," Journal of Advanced Microscopy Research, vol.10, no.2, pp. 93-103, 2015.

[7] N. Dey, S. Samanta, S. Chakraborty, A. Das, S. Chaudhuri, and J. Suri, "Firefly Algorithm for Optimization of Scaling Factors during Embedding of Manifold Medical Information: An Application in Ophthalmology Imaging," Journal of Medical Imaging and Health Informatics, vol. 4, pp. 384–394, 2014.

[8] N. Dey, S. Acharjee, D. Biswas, A. Das, and S. Chaudhuri, "Medical Information Embedding in Compressed Watermarked Intravascular Ultrasound Video," Transactions on Electronics and Communication, vol. 57, 2012.

[9] N. Dey, S. Chaudhuri, S. Chakraborty, S. Ahmed, G. Dey, and P. Maji, "Effect of Trigonometric Functions based Watermarking on Blood Vessel Extraction: an Application in Ophthalmology Imaging," International Journal of Embedding Systems, 2014.

[10] T. Araki, N. Ikeda, N. Dey, *et al*, "A comparative approach of four different image registration techniques for quantitative assessment of coronary artery calcium lesions using intravascular ultrasound," Computer Methods and Programs in Biomedicine, vol. 118, pp. 158–172, 2015.

[11] H. A. Quigley, and A.T. Broman, "The number of people with glaucoma worldwide in 2010 and 2020," Br J Ophthalmol, vol. 90, pp. 262–267, 2006.

[12] P. N. Schacknow, J. R. Samples, The Glaucoma Book (First Edition). Portland, USA:Springer Publication, 2010.

[13] AGIS Investigators, "The Advanced Glaucoma Intervention Study (AGIS); The AGIS Investigators, The relationship between control of intraocular pressure and visual field deterioration," Am J Ophthalmol, vol.130, no.4, pp.429–40, 2000.

[14] S. S. Sandhu, S. Chattopadhyay, M. K. Birch, *et al*., "Frequency of Goldmannapplanation tonometer calibration error checks," J Glaucoma, vol. 14, no. 3, pp. 215–18, 2005.

[15] N.J. Reus, M. de Graaf, H.G. Lemij, "Accuracy of GDx VCC, HRT I and clinical assessment of stereoscopic optic nerve head photographs for diagnosing glaucoma," Br J Ophthalmol, vol. 91, no. 3, pp. 313–18, 2007.

[16] R. L. Cooper Fracs, G. C. Grose Bee, and I. J. Constable Fraco, "Mass Screening Of The Optic Disc For Glaucoma: A Follow-Up Study," Australian and New Zealand Journal of Ophthalmology, vol.14, no.1, pp.1–96, 1986.

[17] V. Mahalakshmi, S. Karthikeyan, "Clustering Based Optic Disc and Optic Cup Segmentation for Glaucoma Detection," International Journal of Innovative Research in Computer and Communication Engineering,vol. 2, no. 4, 2014.

[18] T. R. Reed, and H. Wechsler, "Segmentation of textured images and Gestalt organization using spatiavspatial-frequency representations," IEEE Trans. Pattern Anal. and Machine Intell., vol. 12, pp. 1-12, 1990.

[19] L. Shen, and L. Bai, "A review of Gabor wavelets for face recognition," Patt.Anal. Appl., vol. 9, pp. 273-292, 2006.

[20] V. Sebastian, A. Unnikrishnan, and K. Balakrishnan, "Grey Level Co-Occurrence Matrices: Generalisation and Some New Features," International Journal of Computer Science, Engineering and Information Technology (IJCSEIT), vol.2, no.2, 2012.

[21] A. Rosenfeld, and J. Weszka, "Picture Recognition" in Digital Pattern Recognition, K. Fu (Ed.), Springer-Verlag, pp.135-166, 1980.

[22] N. Sharma, A.K. Ray, S. Sharma, K.K. Shukla, S. Pradhan, L. M. Aggarwal, "Segmentation and classification of medical images using texture-primitive features: Application of BAM-type artificial neural network," J Med Phys., vol. 33, no. 3, pp. 119-26, 2008.

[23] B. Brown, "Structural and functional imaging of the retina: New ways to diagnose and assess retinal disease," Clin. Exp. Optometry, vol. 91, pp. 504–514, 2008.

[24] K. Nouri-Mahdavi, D. Hoffman, D. P. Tannenbaum, S.K. Law, J. Caprioli, "Identifying early glaucoma with optical coherence tomography," Am J Ophthalmol, vol.137, pp. 228–235, 2004.

[25] D. L. Budenz, A. Michael, R.T. Chang, J. McSoley, J. Katz, "Sensitivity and specificity of the Stratus OCT for perimetric glaucoma," Ophthalmology, vol. 112, pp. 3–9, 2005.

[26] R. Bock, J. Meier, G. Michelson, L. Nyul, and J. Hornegger, "Classifying Glaucoma with Image-Based Features from Fundus Photographs", Springer-Verlag, pp. 355–364, 2007.

[27] K. Huang, and S. Aviyente, "Wavelet feature selection for image classifi-cation," IEEE Trans. Image Process., vol. 17, no. 9, pp. 1709–1720, Sep. 2008

[28] G. K. Matsopoulos, P. A. Asvestas, K. K. Delibasis, N. A. Mouravliansky, and T. G.Zeyen, "Detection of Glaucomatous Change based on Vessel Shape Analysis", Computerized Medical Imaging and Graphics, vol. 32, pp. 183–192, 2008.

[29] A.U. Rajendra, S. Dua, X. Du, S.V. Sree, and C.K. Chua, "Automated diagnosis of glaucoma using texture and higher order spectra features," IEEE Trans. Inf. Technol. Biomed., vol. 15, pp.449-455, 2011.

[30] K.A. Yogesh, and M. Sasikala, "Texture analysis of retinal layers in spectral domain OCT images," Int. J. Emerg. Technol. Adv. Eng., vol.2, pp. 296-300, 2012.

[31] J. Odstrcilik, R. Kolar, J. Jan, J. Gazarek, Z. Kuna, M. Vodakova, "Analysis Of Retinal Nerve Fiber Layer Via Markov Random Fields In Color Fundus Images," IWSSIP 2012, Vienna, Austria, ISBN 978-3-200-02328-4

[32] N. Annu, and J. Justin, "Automated Classification of Glaucoma Images by Wavelet Energy Features," International Journal of Engineering and Technology (IJET), vol 5, no. 2, pp. 1716-1721, 2013.

[33] D. Lamani, T. C. Manjunath, M. Mahesh, Y. S. Nijagunarya, "Early Detection of Glaucoma Through Retinal Nerve Fiber Layer Analysis Using Fractal Dimension And Texture Feature," International Journal of Research in Engineering and Technology (IJRET), vol. 3, no. 10, 2014.

[34] S. J. G. Shoba, and A. B. Therese, "A Modified Spatial Fuzzy C-Means Clustering Algorithm for Detecting Glaucoma in Retinal Fundus Images," Journal of Computer Science, vol. 10, no. 8, pp. 1362–1372, 2014.

[35] F. Fumero, S. Alayon, J. L. Sanchez, J. Sigut, and G. M. Hernandez, "RIM-ONE :An Open Retinal Image Database for Optic Nerve Evaluation", Proc. 24th Int. Symp. Comput. Med. Syst., pp. 2–7, 2011.

[36] F. Fumero, S. Alayon, J. L. Sanchez, J. Sigut, and M. Gonzalez-Hernandez, "RIM-ONE: An open retinal image database for optic nerve evaluation," in 2011 24th International Symposium on Computer-Based Medical Systems (CBMS), pp. 1–6, 2011.

[37] A. Septiarini, A. Harjoko, "Automatic Glaucoma Detection Based on the Type Of Features Used: A Review," Journal of Theoretical and Applied Information Technology 28th February 2015, vol.72, no.3, pp. 366-375, 2015.

[38] A. Yanagawa, W. Hsu, and S. Chang, "Brief Descriptions of Visual Features for Baseline TRECVID Concept Detectors," Columbia University ADVENT, Technical Report #219, 2006 -5, 2006.

[39] M. A. Stricker, and M. Orengo, "Similarity of color images," Proceedings of SPIE, Storage and Retrieval for Image and Video Databases III, vol. 2420, pp. 381-392, 1995.

[40] Y. Jiang, J. Yang, C. Ngo, A. G. Hauptmann, "Representations of Key point-Based Semantic Concept Detection: A Comprehensive Study," IEEE, 2008.

[41] K.V.Ramana, and R..B. Korrapati, "Neural Network Based Classification and Diagnosis of Brain Hemorrhages," International Journal of Artificial Intelligence and Expert Systems (IJAE), vol 1, no. 2, 2009.

[42] D. Svozil, V. KvasniEka, J. Pospichal, Introduction to multi-layer feed-forward neural networks, Tutorial, Chemometrics and Intelligent Laboratory Systems, vol. 39, pp. 43-62, 1997.

[43] Raul Rojas. Neural Networks:A Systematic Introduction. Springer, 2005.

Hybrid Method and Similarity to Recognize Javanese Keris

Halim Budi Santoso
Faculty of Information Technology
Duta Wacana Christian University
Yogyakarta, Indonesia

Ryan Peterzon Hadjon
Faculty of Information Technology
STIKOM Uyelindo
Kupang, Indonesia

***Abstract*—This paper describes Hybrid method and Similarity for recoginizing Javanese Keris. Javanese Keris is one of traditional javanese weapon. It is one of the Indonesia Cultural Heritage. Keris is famous for its distinctive wavy blade. But some of the keris has straight blades. There are many kinds of Keris and every Keris has its own unique pattern. The algorithm to recognize several types of Javanese Keris is made by using Edge Detection method with Image Segmentation and combine with Similarity. By using these three methods, it will bring more exact results.**

The method combines Canny Algorithm and Basic Morphological for image segmentation. The result of edge detection and image segmentation are compared with the sample pictures using similarity. Ten (10) images of traditional javanese keris are being used as samples. The final result for this study is recognizing the kind of keris. These techniques is carried out with an experiment by using MATLAB 6.0.1 software.

Keywords—Edge Detection; Similarity; Canny Algorithm; Basic Morphological; Image Recognition; Javanese Keris

I. INTRODUCTION

Edge detection is one of the image processing techniques to identify the real edge of an image. The purpose is to get detail information of an object in an image by detecting the edge of the object and separating the image background with the object [1].

The edges of an image are the boundary for every different texture [2]. Many algorithms have been developed in various research to detect edge [2] [3] [11] [12]. One of the edge detection algorithms is Canny Algorithm.

Canny Algorithm is an effective algorithm to detect the edge of an object because the result of this method can produce single pixel thick.Using this method also can detect continous edge, comparing with other edge detection algorithms [3]. This algorithm can be used to recognize the object within an image. In his research, Allam Mouse [4] develop an alogorithm to recognize license number plate using Canny Algorithm for edge detection.

In this research, Canny algorithm is combined with the basic morphological method for image segmentation. Image segmentation is a process to divide an image into smaller segment (collection of pixel or superpixel). The objective of image segmentation is to identify relevant objects in digital image [5] [6]. Image segmentation has been used in many image processing application or computer vision. Using combination of edge detection and image segmentation can produce more exact results comparing with only one algorithm, either edge detection or image segmentation.

The result of image segmentation and edge detection is combined by using similarity models to recognize image of javanese keris. Many studies have been conducted to find the similarity of two or more images [13][14][19]. One of the study was did by C.M. Christopher [7]. C.M. Christopher, et al. study about recognizing 3D objects using graf approach and similarity. As the result, they found an effective method to recognize 3D objects using similarity model.

The arrangement of this paper as follows. In the second section, the edge detection using Canny Algorithm and image segmentation using Basic Morphological are discussed.. Similarity models is also discussed in this section. Following the literature review is literature study about Javanese Keris and its kind. In the fourth section, analyzing the image using the selected methods. The result of this study is discussed in this section. Following the result, the conclusion is written in the last section.

II. LITERATURE REVIEW

A. *Keris as Indonesian Cultural Heritage*

Keris is one of the Indonesian traditional weapon. In the past, Keris was the heritage from Dongson and South China Culture [1]. Based on the literature, Dong Son civilization brought metal work knowledge to the Malay World. It is known for its elaborative bronze working, especially its drum. People called it Keris Sajen since the leaf shaped blades of the Dong Son Daggers looked like a Keris.

In the Empire age of Indonesia, such as Majapahit, Keris was used as a weapon for civil society. Keris was well known as a weapon which had strong, tough, and light blade. In the era of Demak – Mataram kingdom, the most famous Keris was Keris Nagasasra Sabukinten.

Nowadays, Keris has totally different function comparing in the past time. People think that Keris is "*Tosan Aji*"[2] not a weapon. Different regions in Indonesia has a different perspective about Keris and the usage of Keris. Javanese culture thinks that Keris is a *dhuwung* or a relic.

[1] http://old.blades.free.fr/keris/introduction/origin/history2.htm. Data accessed on 8th August 2015.
[2] Tosan aji is a kind of metal which is glorious and honorable.

Keris has unique pattern comparing with other traditional weapon. Keris looks like a dagger. Some of Keris have wavy blades and the other have straight blade. Many kinds of Keris comes from different region of Indonesia. There are two main parts of Keris, Warangka and Wilah.

Warangka is a Keris Sheath. Warangka is made from various kind of materials, but most of them are made from wood to hold the blade which can be coated with metals, such as brass, iron, silver,or gold. The upper part of sheath formed a broad curved handle made from wood or sometimes ivory. It could be adorned with precious and semi-precious stones. One of the Javanese keris in 1881, the Shealth is made from silver and the front have leaf and floral shaped chasing [20].

Another part of Keris is Wilah. Wilah is the Keris blade. Keris blades are ussually narrow with a wide, asymmetrical base. It has Luk. Luk is a wave in Keris. Common Keris has odd number of luk, range from three to thirteen waves, but some blades have up to 29. [3] One of the examples is North Java Keris that have eleven curves in its blade [20].

The last part of Keris is Hulu Keris or it is called Hilt. Hilt is the object of art, often craved in meticulous details and made from various materials; precious rare types of wood to gold or ivory[4]. They were often craved to resemble demons coated in gold and adorned with semi precious and precious stone, such as rubies. In Yogyakarta, one of its keris has hilt based on the face of the owner [20].

B. Canny Algorithm

One of the algorithm to detect image edge in image processing is Canny Algorithm or Canny Edge Detector. Canny Algorithm is known as one of the optimal algorithm to detect edge in digital image. This algorithm was introduced by John Canny in 1986 on his thesis to finish his master degree in MIT [10]. Canny Algorithm was developed to make a new optimal method to detect edge by modifying the existing algorithm [2] [6].

Canny Algorithm is specified to optimize edge detection method in two (2) criteria specific which has to be fulfilled. The first criteria is edge detection method has to have an appropiate signal – to – noise ratio in order to be implemented in bad quality image. In other word, an Edge Detection method should have low error ratio. Every edge in digital image has not to be missed and every non edge shape has not to be responded [2].

The second criteria that every edge in image has to be located properly. It means that distance between edge pixels has to be detected and the real edge should be minimized well. There are some steps to use Canny Algorithm :

- Reduce all of noises using Gaussian Filter in the following equation:

$$\boldsymbol{g(m,n) = G\sigma(m,n) * f(m,n)}$$

Where $\boldsymbol{G\sigma(m,n)}$ can be expressed as follows:

$$\boldsymbol{G\sigma(m,n) = \frac{1}{\sqrt{2\pi\sigma^2}} exp\left[\frac{-m^2+n^2}{2\sigma^2}\right]}$$

- Calculate gradient g(m,n) using one of the existing gradient operators to get:

$$\boldsymbol{M(m,n) = \sqrt{gm^2(m,n) + gn^2(m,n)}}$$

and

$$\boldsymbol{\theta(m,n) = arctan\left[\frac{gn(m,n)}{gm(m,n)}\right]}$$

- Define threshold M using the following equation:

$$\boldsymbol{M_T(m,n)} = \begin{cases} \boldsymbol{M(m,n)}, & M(\boldsymbol{m,n}) > T \\ \boldsymbol{0}, & M(\boldsymbol{m,n}) < T \end{cases}$$

Where T is defined in order to save all of the edge and only reduce the noise.

- Surpress Non-Maxima pixel on the $\mathbf{M_T}$ edge which is got from (3) equation to thin the edge line.
- Hysteresis: apply the threshold to supressed image. Canny algorithm is able to use two (2) thresholds, upper and lower threshold.
  - If gradient of pixel is bigger than upper threshold then pixel is detected as an edge.
  - If gradient of pixel is lower than lower threshold then pixel cannot be accepted / is refused as an edge.
  - If the value of pixel gradient between those two thresholds, this pixel is not detected as an edge unless the edge is connected to the pixel which is in above the upper threshold.

C. Basic Morphological Method

In the digital image processing, morphology is one of the methods to analyze the geometrical structure which stick on the image. Morphology is based on the association theory in mathematics [9][15]. In general, morphological method can be used as an image segmentation method. The goal of this method is to change the original image into new image through an interaction with another image which has specific shape and size. Image geometric feature which has the same size and shape will be saved. The rest of them will be neglected. This process is known as structuring element. In the digital image, collection of pixel which is similar (geometric feature with the same shape and size) is known as "foreground" (pixel structure has value one (1)) [8] and collection of pixel which is the complement is known as background (pixel structure has value 0) [8]. According to Basic Morphological or Morphology, there are some basic arithmetic which can be used for image segmentation [9][16].

1) Dilation : if A and B is the element of Z2 association then dilation of A by B (A⊕B) can be expressed as follow:

$$\mathbf{A \oplus B = \{z \in Z^2 \mid z = a + b, \text{ for some } a \in A \text{ and } b \in B\}}$$

Or

$$\mathbf{A \oplus B} = \bigcup_{b \in B} (A)_b$$

Dilation is the process to expand the image so if there are some holes in the foreground will be filled.

[3] http://www.karatonsurakarta.com/keris.html. Data accessed in 10th August 2015.

[4] http://www.javakeris.com/?mode=viewid&post_id=61. Data accessed in 10th August 2015.

2) Erosion : Erotion of image A by structuring element B can be denoted AΘB is:

$$\mathbf{A\Theta B = \{z \mid z + b \in A, \text{ for all } b \in B\}}$$

Or

$$\mathbf{A\Theta B} = \bigcap_{b\in B}(A)_{-b}{}^{c}$$

The result of erotion process is the opposite of the dilation where erotion will make the original picture smaller and eliminate small noises which is not required in "foreground".

3) Opening : Opening of image A by structuring element B can be denoted A◦B is expressed as follows:

$$\mathbf{A\circ B = (A\Theta B) \oplus B}$$

The result of opening process is smoothing image processing and reduce the noise from quantitation or extra structure in the original image.

4) Closing : Closing of image A by stucturing element B can be denoted $A\cdot B$ is expressed as follows:

$$\mathbf{A\cdot B = (A\oplus B)\ \Theta\ B}$$

The result of closing process is the additional pixel on the holes in the original image and smoothing process like in the opening process.

D. Similarity Concept

Similarity concept is the basic geometric concept in mathematics that expressed the similarity of two (2) objects. Two (2) objects are similar if those two objects has the same shape. In other words, there is no significant differences between the two objects geometrically [18][19]. Calculating similarity between two objects is one of the key objectives in the image recognizition. To calculate the similarity degree, there is an involvement with resemblance within the two objects using similarity measure. [17].

Shape similarity measure or distance function in the shape association S is the function of d∶S×S→R. There are some conditions that have to be fulfilled for the shape A,B, or C in S as follows [18]:

1) (Non-negativity): d(A,B)⩾0
2) (Identity): d(A,A)=0,for all of the shape A
3) (Uniqueness): d(A,B)=0,so A=B
4) (Strong triangle inequality): d(A,B)+d(A,C)⩾d(B,C).
5) (Triangle inequality): d(A,B)+d(B,C)⩾d(A,C).
6) (Relaxed triangle inequality): c(d(A,B)+d(B,C)) ⩾ d(A,C),for c⩾1
7) (Symmetry): d(A,B)=d(B,A)
8) (Invariance): g ∈G,d(g(A),g(B))=d(A,B).
9) (Pertubation robustness): d(f(A),A)< ∈d(B,A) for all f ∈F.
10)(Crack robustness): A-U=B-U,where d(A,B)< ∈
11)(Blur robustness): d(A,B)< ∈for all B that B-U=A-U and d(A,B)< ∈.
12)(Noise robustness): for all x ∈R^2 dan ∈ >0 , there is U from x in order for every B this formula is valid B-U=A-U,where d(A,B)< ∈.
13)(Distributivity): for every A and decomposition B ∪C, d(A,B ∪C)⩽d(A,B)+d(A,C).
14)(Endlessness): for every A,B there is C where d(A,C)>d(A,B).
15)(Discernment): for every transformation association G which is chosen, d(A,A ∪B)⩽d(g(A),A ∪B) where g ∈G.
16)(Sensitivity): for every A,B with A ∩B=B ∩A,B-U=C-U, and B ∩U≠C ∩Ufor every U⊂R^2, then d(A,B)<d(A,C).
17)(Proportionality): for every A ∩B=∅ and A ∩C=∅, if B⊂C, then d(A,A ∪B)<d(A,A ∪C).
18)(Monotonicity): for all A⊂B⊂C,d(A,C)>d(A,B), or d(A,C)>d(B,C).

III. PROPOSED ALGORITHM

In this study, the writers try to develop a hybrid algorithm as a combination between Canny Edge Detection and Image Segmentation using the Basic Morphological Method. After using the hybrid method, the segmented image will be compared with the sample pictures of keris.

In order to use this algorithm, some preparation should be done to change the original image into the same dimensions. These ten (10) images will be used as a reference to be compared with the tested image:

1) Take 10 samples of Keris from different regions in Java
2) Normalize these ten (10) samples of keris, including resize the image to get desired pixel and crop some background
3) Rotate the picture in order to get the image in a vertical position with Wilah is in the top position and hulu is under the blade.
4) Use the Canny Algorithm for image detection.
5) Use the Basic Morphological Algorithm to segment the image.

The sample of preparation can be seen in figure 1 below:

Keris 1 Original Image	Keris 2 Original Image
	
Rotated Image Keris 1 (*Same Image*) It is not neccessary to rotate the image 1 because it is already in vertical position	Rotated Image Keris 2 

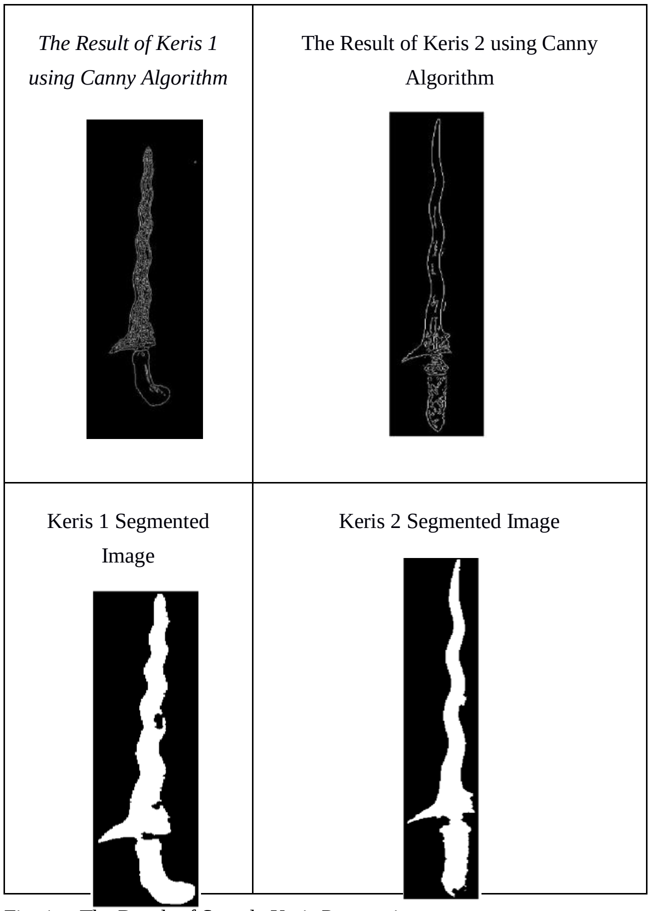


Fig. 1. The Result of Sample Keris Preparation

After some steps to prepare ten (10) samples picture of Keris, here is the algorithm which is used to recognize Javanese Keris.

1) *Do the preparation steps as mention above*
2) *Similarity testing by comparing the vector of tested image with sample image*
3) *Calculate the total pixel which has same value between tested image and sample image*
4) *Calculate the total pixel of every picture*
5) *Calculate the percentage similarity between tested image and sample image*
6) *Define the keris using the highest percentage*

IV. IMAGE SIMULATION

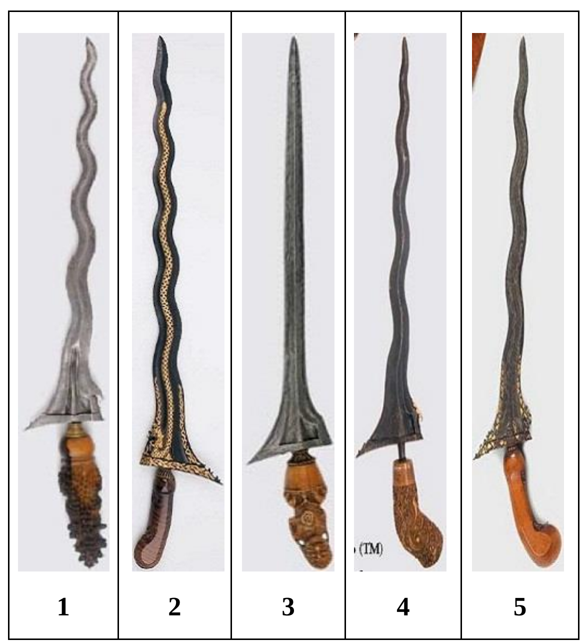
In this study, ten (10) sample of keris images are used. All of those Keris have been known the origin. Based on Groneman [20] there are some Keris from different parts of Java Island. The ten (10) samples are taken from book [20]. The research is conducted by using those ten (10) samples. As tested images, three (3) unknown Keris are taken. Recognizition keris process is done using some primary steps based on algorithm above mentioned in section three (3).

A. Normalize the Image to get the same dimension.

Normalization is done to ease the similarity process since it is required the same dimension to be compared. Image normalization is done by changing the image size and tested image. The result is the same dimension of the sample and tested image. The image size is 85 pixel for width and 507 pixel for length.

In figure 2, it shows the three tested Keris Image. In Figure 3, it shows the ten sample Keris image.

Fig. 2. Unknown Tested Keris image A, B, and C



6	7	8	9	10

Notes :

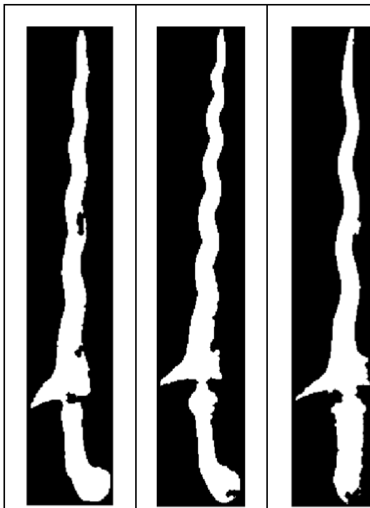
1. Origin central Java – 3139 WM
2. Origin Central Java – 1789 WM
3. Origin Central Java – 13005 WM
4. Origin Cirebon, West Java
5. Origin East Java
6. Origin Madura East Java
7. Origin Surakarta
8. Origin Tegal Central Java
9. **9.** Origin Yogya
10. Origin Yogya

Fig. 3. Ten Sample Keris Image

After the rotation (if needed), the next step is to make the same dimensions for every Keris Image. Each Keris Image in Figure 2 and Figure 3 has the same dimensions. 85 x 507 pixels. Keris image has been standardized to make the same dimension for every picture.

B. Edge Detection and Image Segmentation for every Keris Image

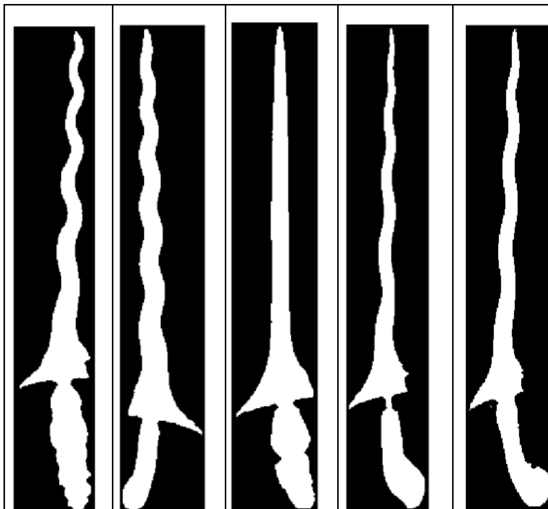
Before doing this step, canny edge detection algorithm and basic morphological image segmentation is done for ten (10) sample keris images and three (3) tested keris image.



A	B	C

Fig. 4. Tested Image A, B, and C after Edge Detection and Image Segmentation

Figure 4 above gives the result of tested image A, B, and C after two operations: Edge Detection and Image Segmentation were conducted. On the other hand, Figure 5 below shows the result of sample image keris 1 to 10 after Edge Detection and Image Segmentation has been done to the Images.



1	2	3	4	5

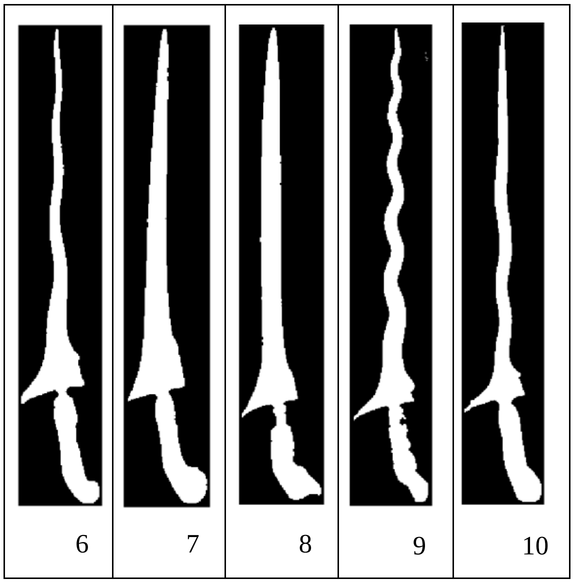


Fig. 5. After Image Detection of Keris Sample Image 1-10

C. Image Similarity to compare between two similar images.

In this process, sample and tested images are into a single vector which has value 0 (black) or 1 (white). It is to ease the comparison for every pixel in the image, either sample or tested image. Every pixel in image A, B, and C has to be converted into a vector. There is a counter for every testing which shows the total pixel has the same value within two images, tested and sample image. The result will be used to calculate image similarity. The result is an input for the next process, calculating the image similarity percentage.

After the total same pixel is derived, the calculation of similarity percentage is the next step. Percentage of image similarity within two image is the total same pixel (number of pixel between two images, tested and sample image which have same value) is divided by the total pixel.

The result of calculation using similarity percentage can be seen in Table 1 below. From the table 1, it can be seen that the highest percentage for every image will be different.

TABLE I. SIMILARITY RESULT BETWEEN TESTED IMAGE AND SAMPLE IMAGE

Similarity Percentage		Tested Image		
		Image A	**Image B**	**Image C**
Sample Image	**Image 1**	74.50	80.87	**88.17**
	Image 2	65.34	65.34	58.35
	Image 3	86.47	83.11	79.68
	Image 4	**88.35**	83.24	71.46
	Image 5	86.05	81.62	67.38
	Image 6	83.58	82.16	72.74
	Image 7	76.85	75.45	64.39
	Image 8	73.78	71.67	61.85
	Image 9	87.88	**85.12**	75.61
	Image 10	65.34	82.42	73.25

D. Intrepret the Result of Calculation

In this step, the highest percentage is taken to define the kind of Keris. Based on table 1, it can be concluded that:

1) Image A has the highest percentage value (88.35%) with Image 4. It means that Image A is most similar with Image 4. It can be concluded that Keris A is most similar with Keris sample 4 (Keris from Cirebon, West Java). This number also shows that Keris A is possibly recognized as Keris from Cirebon, West Java.

Image A only has 73.78% with Keris image 8. It means that Image A is less similar to Keris image 8 (Keris from Tegal, Central Java)

2) Image B has the highest percentage value (85.12%) with Image 9. It means that Image B is similar to Image 9. It can be concluded that Keris B is similar with Keris 9 (Keris from Yogyakarta).

Image B only has 75.45% with Keris image 7. It means that Image B is less similar to Keris image 7 (Keris from Surakarta, Central Java).

3) Image C has the highest percentage value (88.17%) with Keris image 1. It can be concluded that Keris C is most similar with Keris 1 (Keris from Central Java) and possibly can be recognized as Keris from Central Java.

V. CONCLUSION

Keris recognition is one of the image recognition applications. Proposed algorithm that is used in this research is able to recognize the kind of Keris based on the calculation of every single pixel on the Keris's image after being converted into a single vector. The higher similarity percentage value, more accurate the possibility of the keris recognizition. The higher similarity percentage value will give more confident result.

On the other hand, the result of similarity calculation depends on the result of image segmentation. Better result of image segmentation will bring better result to the calculation for image similarity. Basic Morphological methods is one of the suitable image segmentation method to Keris segmentation. In the next research, it is suggested to use another image segmentation to compare the result with Basic Morphological Methods.

Some limitation in this study also need to be fixed. The similarity percentage still lower than 90%. It is needed to be higher than 90%. The other algorithm can be implemented to test the Javanese Keris.

For further research, some improvement can be done. It is better to test the image from the picture taken from the original Keris. There are many museum that has Keris collections, such as Museum Pusaka in Jakarta, Museum Sonobudoyo in Yogyakarta, Keris Museum in Surakarta. The algorithm can be tested to test the photograph taken from those museum. It is suggested to combine with the mobile application to recognize Javanese Keris. The reader can also have the history of the Keris from those mobile application.

Indonesia has many traditional weapons. It is also applicable that this algorithm can be test to recognize other traditional weapons, such as Mandau from Borneo.

REFERENCES

[1] Al-amri, S. Salem, N.V. Kalyankar, S.D. Khamitkar (2010). “Image Segmentation by Using Edge Detection”. *International Journal on Computer Science and Engineering*, vol. 2(3), 804-807.

[2] Juneja, M., P. Singh Sandhu (2009). “Performance Evaluation of Edge Detection Techniques for Images in Spatial Domain”. *International Journal of Computer Theory and Engineering*, vol. 1 (5), 1793-8201.

[3] Nadernejad, E., S.Sharifzadeh, and H. Hassanpour (2008). “Edge Detection Techniques : Evaluations and Comparisons”. *Applied Mathematical Sciences*, vol. 2 (31), 1507-1521.

[4] Allam, M (2012). “Canny-Edge Detection Based Vehicle Recognition”, *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 5 (3).

[5] Nagaraju, C., S. NagaMani, G.rakesh Prasad, and S.Sunitha (2011). “Morphological Edge Detection Algorithm Based on Multi-Structure Elements of Different Directions”. *International Journal of Information and Communication Technology Research*, vol. 1 (1).

[6] Muthukrishnan, R., M. Radha (2011). “Edge Detection Techniques for Image Segmentation”. *International Journal of Computer Science and Information Technology*, vol. 3 (6).

[7] Christopher, C.M., K.B. Benjamin (2004). “A Similarity-Based Aspect-Graph Approach to 3D Object Rrecognition”. *International Journal of Computer Vision*, vol. 57 (1), 5-22.

[8] Peter, T (2007). “Morphology Image Pre-processing for Thinning Algorithms”. *Journal of Information, Control and Management Systems*, vol. 5 (7).

[9] Shaosheng, F., W. Hainan (2011). “Multi-direction Fuzzy Morphology Algorithm for Image Edge Detection”. *Journal of Networks*, vol. 6 (6).

[10] Canny, J. F (1986). “A computational approach to edge detection”, .*IEEE Trans. Pattern Analysis and Machine Intelligence*, pages 679-698.

[11] Manisha, K., S. Arjan, S. Baljit (2010). “Adaptive Thresholding for Edge Detection in Gray Scale Images”. *International Journal of Engineering Science and Technology*, vol. 2 (6), 2077-2082.

[12] Luo, W (2006). “Comparison for Edge Detection of Colony Images”. *IJCSNS International Journal of Computer Science and Network Security*, vol. 6 (9A).

[13] Hua, S., G. Chen, H. Wei, and Q. Jiang (2012). “Similarity Measure for Image Resizing using SIFT feature”. *EURASIP Journal on Image and Video Processing*.

[14] Chary, R.V.R., D.R. Lakshmi, and K.V.N Sunitha (2012). “Feature Extraction Method for Color Image Similarity”. *Advanced Computing : An International Journal* , vol. 3 (2).

[15] Meyer, F (2001). “An overview of morphological segmentation”. *International Journal of Pattern Recognition and Artifcial Intelligence*, Vol. 15 (7), 1089-1118.

[16] Kumar, S.H., S. Pooja, and S. Khushboo (2012). “Morphological Segmentation and Gradient of Multispectral Image of Bareilly Region”. In *IJCA Proceedings on National Conference on Recent Trends in Computing NCRT* (3) ,May 7-10.

[17] Veltkamp, R. C. (2001). Shape matching: Similarity measures and algorithms. In Shape Modeling and Applications, SMI International Conference on. (pp. 188-197). IEEE.

[18] Cheong, O., Gudmundsson, J., Kim, H. S., Schymura, D., & Stehn, F. (2009, June). Measuring the Similarity of Geometric Graphs. In Proceedings of the 8th International Symposium on Experimental Algorithms (pp. 101-112). Springer-Verlag.

[19] Veltkamp, R. C., & Hagedoorn, M. (2000, November). Shape Similarity Measures, Properties and Constructions. In Proceedings of the 4th International Conference on Advances in Visual Information Systems (pp. 467-476). Springer-Verlag.

[20] Groneman, Isaäc, 2009: ‘*The Javanese Kris*‘. Leiden: KITLV Press

Cryptocurrency Mining – Transition to Cloud

Hari Krishnan R.1
Department of Computer Science and Engineering
SRM University, Chennai, India

Sai Saketh Y. 2
Department of Computer Science and Engineering
SRM University, Chennai, India

Venkata Tej Vaibhav M.3
Department of Computer Science and Engineering
SRM University, Chennai, India

***Abstract*—Cryptocurrency, a form of digital currency that has an open and decentralized system and uses cryptography to enhance security and control the creation of new units, is touted to be the next step from conventional monetary transactions. Many cryptocurrencies exist today, with Bitcoin being the most prominent of them. Cryptocurrencies are generated by mining, as a fee for validating any transaction. The rate of generating hashes, which validate any transaction, has been increased by the use of specialized machines such as FPGAs and ASICs, running complex hashing algorithms like SHA-256 and Scrypt, thereby leading to faster generation of cryptocurrencies. This arms race for cheaper-yet-efficient machines has been on since the day the first cryptocurrency, Bitcoin, was introduced in 2009. However, with more people venturing into the world of virtual currency, generating hashes for this validation has become far more complex over the years, with miners having to invest huge sums of money on employing multiple high performance ASICs. Thus the value of the currency obtained for finding a hash did not justify the amount of money spent on setting up the machines, the cooling facilities to overcome the enormous amount of heat they produce and electricity required to run them. The next logical step in this is to utilize the power of cloud computing. Miners leasing super computers that generate hashes at astonishing rates that have a high probability of profits, with the same machine being leased to more than one person on a time bound basis is a win-win situation to both the miners, as well as the cloud service providers. This paper throws light on the nuances of cryptocurrency mining process, the traditional machines used for mining, their limitations, about how cloud based mining is the logical next step and the advantage that cloud platform offers over the traditional machines.**

***Keywords*—Cryptocurrency; Bitcoin mining; Cloud mining; Double Spending; Profitability**

I. Introduction To Mining

Mining is the integral process wherein generation, transmission and validation of transactions of cryptocurrencies is done. It ensures stable, secure and safe propagation of the currency from the payer to payee. Unlike fiat currency, where a centralized authority controls and regulates the transactions, cryptocurrencies are decentralized and work on a peer-to-peer system. Banks that generate physical currency and monitor the transactions require huge infrastructure to function and operate. Cryptocurrencies overcome this need by implementing a mining system where people in the network, called 'miners' or 'nodes', monitor and validate transactions which generates currency.

In cryptocurrency, a transaction is a transfer of coins from one wallet to another. When a transaction is made, the details of the transaction will be broadcast to every node in the network. The transactions made over a set period of time are collected to form a 'Block'. To incorporate transparency in the system, it is designed in such a way that all the transactions made from the inception of the currency are recorded and maintained in a general ledger called the 'Block chain' which, as the name suggests, is a list of blocks created from the beginning.

Miners play a predominant role in mining. Miners process transactions by verifying the ownership of the currency from source to destination. Every transaction contains the hash of the previous transaction made by the owner through which authenticity of a present transaction is tested, thereby validating it. Miners also inhibit double spending of the currency through this validation process.

The main purpose of mining is to generate and release coins into its coin economy. Whenever a transaction takes place and is validated, miners collect these transactions and include them into the block they are currently solving. Every block has to be solved before being broadcasted and put in the block chain. Solving of a block involves mathematical puzzles which are difficult to unlock and crack provided there will be some constraints on the output generated. Only on solving the mathematical puzzle is one allowed to add the block to the ledger and a reward of coins is given in return. Thus mining eventually boils down to a competition of mathematical puzzles to solve for the reward of coins. This mechanism prevents miners from easily procuring coins and thus maintains the fairness of the system. [1][2][3][4]

II. Mining Machines

Mining of crypto currency is done through purpose specific designed machines called as 'Mining machines'. The history of mining machines starts from CPU to the currently widely used ASICs. The periodic growth of mining difficulty led to evolution of new machines with higher efficiency than previously designed machines. The cost and performance of the mining machine determine its mining profitability, hence the design and its implementation is very crucial in mining. The various machines used in mining are:

A. CPU

During initial days of mining, CPU was used to mine the coins effectively with hash rates less than or equal to 10MH/sec. A personal PC with mining software installed in it was enough to cope with the mining process. But, due to the constant increase of difficulty in mining, usage of CPU's as mining machine became irrelevant to the evolving machines with higher hashing rates. A popular mining software for CPU mining was cpuminer.

cpuminer is a simple client program that performs Pooled Mining or solo mining. The program receives proposed block data from the server, for which it tries to guess a nonce value that will result in a valid block. If a block hash with at least 32 consecutive zero bits is found, the block data containing the guessed nonce value is sent back to the server. If used in Pooled Mining mode, this block is called a "share" because the server is supposed to credit the registered user's account, according to the number of shares that user has contributed, and eventually transfer an amount of Bitcoins to the registered user's address.

B. GPU

As the power of CPU mining didn't meet the growing demands, CPU with Graphic cards are used to mine the coins. Graphic cards contain Graphical Processing Units (GPU's), which are used to solve high mathematical calculation functions and complex polygons used in gaming. Different cryptocurrencies uses different hash-proof based algorithms to solve transaction blocks which require high mathematical lifting, hence GPU's were seen as a credible alternative to the CPU mining.

A CPU core can execute 4 32-bit instructions per clock (using a 128-bit SSE instruction) or 8 via AVX (256-Bit), whereas a GPU like the Radeon HD 5970 can execute 3200 32-bit instructions per clock (using its 3200 ALUs or shaders). This is a difference of 800 (or 400 in case of AVX) times more instructions per clock. As of now, the fastest CPUs have up to 6, 8, or 12 cores and a somewhat higher frequency clock (2000-3000 MHz vs. 725 MHz for the Radeon HD 5970), but one HD5970 is still more than five times faster than four 12-core CPUs at 2.3GHz (which is also costlier at $4700 when compared to $350 for the HD5970).

In October 2010 an open-source OpenCL miner was released on the web which was rapidly optimized and adapted by miners. These miners would typically implement the SHA protocol in languages such as Java or Python which was compiled down by the hidden ISA of the GPU.

Since these rigs are left to mine for many months the users aggressively tweak the voltages (to lower in order to reduce mining costs, or higher, with frequency, to increase Gh/s) and operating frequencies of video ram (lower to save energy, since memory is unused) and the GPU core itself, as well as parameters of the code such as the number of threads that are enqueued at a given instance, so as to maximize throughput within reasonable bounds of stability and temperature. Since the Bitcoin computation does not exercise the memory system, many of the critical paths and bottlenecks in the GPU are not exercised, which means that the system can be pushed beyond the normal bounds of reliability. Over time it often becomes necessary to retune the parameters as fans and power delivery system wear eventually causes the GPU core to run too slowly.

GPUs tend to be much more accessible than FPGAs for end users, requiring PC-building skills and avid forum reading but no formal training in parallel programming or FPGA tools. The goal of scaling BTC hash rate through GPUs pushes the limits of consumer computing in amazing and novel ways. Despite such benefits GPU have some limitations.

Limitations:

- Though Graphic cards can give over 800 MH/sec, but they are of high cost than normal CPU's.
- The GPUs cannot be used standalone. Each GPU has to be plugged into a PCI-E 8x or 16x slot, of which there are relatively few on commercial motherboards.
- All the components like motherboard, hard-drive and RAM are not used in GPU mining which ultimately increases the cost of mining.
- GPU's require high additional power of 200-300W for mining effectively.
- GPU's normally takes two slots in a case or motherboard which makes it difficult to attach two or more GPU's to a single computer for greater performance.

GPU mining is largely inactive these days as the mining difficulty has exceeded the levels it can compete and further, with the advent of FPGAs and ASICs into the field of mining which vouched for good mining profitability.

C. FPGA (Field Programmable Gate Array)

June 2011 brought the first open-source FPGA Bitcoin miner implementations. With the constant increase of mining cost against the coins earned as a result of mining, it impacted mining profitability in a negative sense. GPU mining with its high mining cost and low $ per day return was incompetent to mine any more. There was an immediate need for an emergence of machines which could make the mining profitable for the miners to continue with the mining.

FPGA known as Field Programmable Gate Array is a reprogrammable IC which can be configured or designed after manufacturing. FPGAs contain individual programmable logic blocks commonly called as Configurable Logic Blocks (CLB). These logic blocks are inter-connected in a manner that can be reconfigured. FPGAs contain large resources of logic gates and RAM's for complex digital computation.

FPGAs are flexibly configurable and reprogrammable, hence a designer can design and implement any digital function. FPGAs are easier to synthesize than its other counterparts which made FPGAs a good option for Bitcoin mining. FPGAs are reusable as they can be reprogrammed very easily. FPGAs consume energy one-fifth less than that of GPU, which was a major issue with GPU mining. FPGAs are also good at rotate-by-constant operations and at bit-level operations used in hash-proof based algorithms like SHA256 used in Bitcoin transactions.

A Butterfly labs mini rig FPGA mines at around 25,200Mh/s with efficiency 20.26Mhash/J consuming 1,250Watts of power I contrast to the GPU's which mine at 800MH/s in general.

Limitations:

- Though BTC FPGAs are easily synthesizable, they consume high power than typical FPGAs.
- FPGAs are good for low quantity production, otherwise cost per product increases with the required quantity increment which less efficient than its competitors like ASICs.

D. ASIC (Application Specific Integrated Circuit)

Mining coins with time became hard to come by with the upgraded machines available at cheaper prices made huge competition among the miners to achieve more gains through mining. FPGAs designed for mining purpose though are flexible to program and manufacture, consumes a lot of power against the return it gets. With the use of ASICs for mining, these offered an improved performance than FPGAs when used for large scale mining. ASICs are a logical progression of this trend: circuits are specifically designed to calculate hashes as fast as possible, while consuming as little energy as possible. The best ASICs on the market today are capable of well over 1,000 Mhash (1 billion hashes) per joule of energy.

ASICs are Application Specific Integrated Circuits used for various types of specified applications. They are microchips built for single purpose though its applications are implemented in various fields. Bitcoin ASICs which are designed specifically to mine Bitcoins, are good at complex mathematical tasks that mining needs, as fast and efficiently as possible. Although FPGAs dominated only a short time, its development efforts served as a quick stepping stone to ASICs. ASIC Verilog are similar to FPGA Verilog in its design and implementation that came before it.

Advanced ASICs in the present market are capable of producing more than or equal to 1,000Mhash per joule of energy consumed. An ASIC Ant-Miner S5 costing up to $370 typically gives 1957Mhash/J and consumes around 590 Watts, which makes ASICs the most profitable privately owned machine available in the market for mining as of today.

The disadvantages faced through ASICs is its cost and the speed with which the entire field is developing. The pace with which the field is updating with improved hardware achieving high hash rates than previously designed economically makes the ASIC mining profitable only for a short period of time until a new machine with higher performance emerges.

Due to its obvious advantages when compared to the other mining machines available, ASICs are currently reigning the mining field with their performance, though it remains to be seen how much it will withstand and sustain with the ever emerging improved machines. [2][8]

III. COMPARISON OF HARDWARE

Mining machines characterize the whole mining process with their action and output. Mining difficulty and mining profitability are dependent on the machines used at the respective times in the history of mining. Figure 1 shows the revenue per GH/s that bit coin network generated since 2010. The horizontal lines depict the energy costs per GH/s of CPU'S, GPU'S, FPGAS and ASICS. When revenue per GH/s goes below these costs the profits will turn negative and rig should turn off.

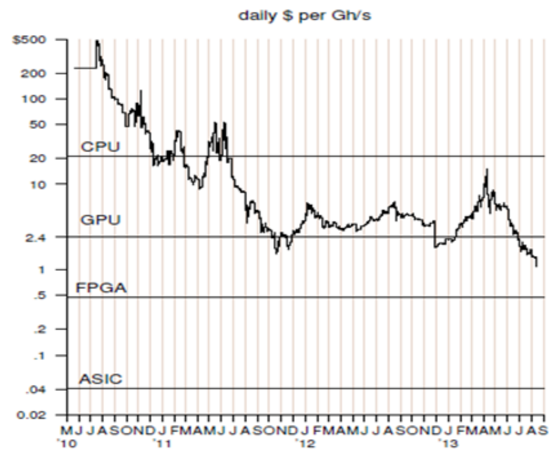


Fig. 1. Revenue per GH/s vs. Energy costs [8]

The above graph also suggests that ASICs have the highest returns/capital spent on energy requirement in comparison to the other three mining systems.

The general comparison between ASICs, FPGAs, GPUs and CPUs against various parameters is shown below:

TABLE I. PERFORMANCE CHARACTERISTICS OF VARIOUS MACHINES [9]

NAME	TYPE	HASH RATE 'R' (Mhash/S)	POWER 'P' (WATTS)	ENERGY EFFICIENCY 'E' (Mhash/J)	COST ($)
CORE i7 950	CPU	18.9	150	0.126	350
Atom N450	CPU	1.6	6.5	0.31	169
ATI 4850	GPU	101.0	110	0.918	45
ATI 5770	GPU	214.5	108	1.95	80
DIGILENT NEXYS 2 500K	FPGA	5.0	5.0	1	189
MONARCH BPU 600 C	ASIC	600000.0	350	1714	2196
BLOCK ERUPTER SAPPHIRE	ASIC	333.0	2.55	130	34.99

IV. PROFITABILITY

Profitability is a major criterion when we consider performing Bitcoin mining operations. The profitability of mining depends on factors like:

- The initial cost of the mining rigs like the ASICs
- The hashing rate of the machine
- The total network hashing power and the current difficulty of hashing problems.
- The cost of electricity consumption.
- The current and future value of Bitcoins.

A traditional mining technique requires miners to purchase large and multiple highly powered ASICs machines to perform hashing operations which yields Bitcoins. However such a technique is not practical to a new or even an experienced miner with respect to profitability. This is because as the number of miners increases, greater amount of processing power is being added to the Bitcoin network. This requires vast amount of electricity to keep the machines running at constant rate and thereby not only resulting in a higher carbon footprint that has environmental consequences but also increasing the cost of electricity consumption per machines, thereby reducing the profit obtained by mining of Bitcoins.

A. *Efficiency calculations*

Mining requires a lot of electricity. If we are building a DIY system then we will be getting an ATX power supply unit (PSU). Therefore it's worth investing in the most efficient supply you can get.

Let us consider the following two cases for determining efficiency of rigs: A PSU that is guaranteed to supply 860W and is 93% efficient would actually draw 925W (860W/0.93). By contrast, a 750W power supply that is only 80% efficient would actually draw 937.5 W (750/0.8) - thus using more power, but supplying less. When building a mining rig, miners will need to take account of the power requirements of all the components they are using, especially all the graphics cards. Also it is a good idea to provide some excess capacity to deal with unexpected events and provide the potential to overclock the system. ASICs, on the other hand, can do far more calculations with far less power because they are highly specialized devices. And since they ship with an appropriate power adapter, miners do not have to worry about doing all the math to find one that is up to the task. The mining efficiency of different systems can be compared by taking the ratio of the number of hashes it can perform in a second, divided by the power it consumes:

Hashing speed / power consumption = mining efficiency.

The profitability calculators like the Genesis block ask for the electricity costs and the initial investments in the hardware. Effectively the miners are being asked for their ongoing and one-off investments. The conversion process isn't completely straightforward; In the case of hardware miners, the monthly running cost can be worked out by multiplying the electricity charge (i.e., $ per KWh) by the power consumption of the unit and by a conversion factor of 0.744 (the ratio of seconds per month to joules of energy per KWh).

However the main question is: Has profitability increased or decreased over the years?

Recent data, table 2, pertaining to difficulty of mining and corresponding hash rates clearly indicate that traditional mining techniques can lead to losses or reduce profitability substantially. From the data we can conclude that over period of 11 months the difficulty and hashing rate has increased by 7.5% and 346.81331% respectively. Additionally, there is not guarantee that the value of Bitcoins and other cryptocurrencies will remain stable or even rise. Speculations and increasing regulation constantly encourage different parties to join in or exit the market. While the picture is one of increasing adoption, major developments can still affect the price markedly.

TABLE II. BITCOIN DIFFICULTY AND HASH RATE HISTORY (11 MONTHS) [25]

Date	Difficulty	Change	Hash Rate
Mar 22 2015	46,717,549,645	-1.50%	334,417,246 GH/s
Mar 08 2015	47,427,554,951	1.59%	339,449,662 GH/s
Feb 22 2015	46,684,376,317	5.01%	334,179,783 GH/s
Feb 09 2015	44,455,415,962	7.71%	318,224,263 GH/s
Jan 27 2015	41,272,873,895	-6.14%	295,442,739 GH/s
Jan 12 2015	43,971,662,056	8.20%	314,761,417 GH/s
Dec 30 2014	40,640,955,017	3.00%	290,919,288 GH/s
Dec 17 2014	39,457,671,307	-1.37%	282,449,013 GH/s
Dec 02 2014	40,007,470,271	-0.73%	286,384,627 GH/s
Nov 18 2014	40,300,030,328	1.76%	288,478,854 GH/s
Nov 05 2014	39,603,666,252	10.05%	283,494,086 GH/s
Oct 23 2014	35,985,640,265	2.81%	257,595,247 GH/s
Oct 09 2014	35,002,482,026	0.98%	250,557,526 GH/s
Sep 25 2014	34,661,425,924	16.20%	248,116,151 GH/s
Sep 13 2014	29,829,733,124	8.75%	213,529,547 GH/s
Aug 31 2014	27,428,630,902	15.03%	196,341,788 GH/s
Aug 19 2014	23,844,670,039	20.86%	170.686.797 GH/s
Aug 08 2014	19,729,645,941	5.30%	141.230.307 GH/s
Jul 25 2014	18,736,441,558	8.08%	134.120.673 GH/s
Jul 12 2014	17,336,316,979	3.08%	124,098,191 GH/s
Jun 29 2014	16,818,461,371	24.93%	120,391,236 GH/s
Jun 18 2014	13,462,580,115	14.51%	96,368,902 GH/s
Jun 05 2014	11,756,551,917	12.44%	84,156,677 GH/s
May 24 2014	10,455,720,138	18.10%	74,844,960 GH/s

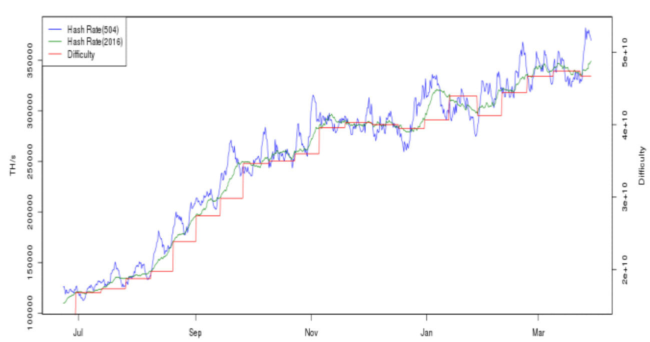


Fig. 2. Bitcoin Hash Rate vs Difficulty (9 months)

V. Issues in Traditional Mining

A. Double spending problem

Double spending as the name goes suggests is a successful spending of a money more than once. Double spending is a unique problem associated with digital currencies because the digital data can be reproduced easily unlike physical currency.

Crypto currency network involves mining which is a Proof of Work (PoW) based. Users do the transactions by digitally signing their transactions over the network through a distributed time stamp service to prevent double spending of coins. In double spending, any digital currency holder can make a copy of the currency and might send it to any merchant or any other party while retaining the original.

For example, a popular digital currency like Bitcoin takes an average 10 to 15 minutes for conformation of a transaction and which is why is not efficient for fast payments. But this process is essential for the detection of double spending of coins. Since all digital currency users are anonymous and hold multiple accounts, it is practically very difficult to trace out the fraudsters. This problem was acknowledged by the Bitcoin developers and suggested a mechanism such that merchants don't have to wait for the conformation if the transaction amount is not a huge sum. But this proposal doesn't remove the double spending problem of the network theoretically since Bitcoin is increasingly used in fast payments like ATM transaction, restaurant bills etc…

Understanding the conditions for double spending needs a knowledge about the types of payments involved in digital currencies. Generally, two types of payments namely slow and fast payments are present.

Slow Payments: Slow payments are the conventional way of transaction mechanism. Slow payments are accepted after the conformation of the transaction by the network. Since confirmed transactions are accepted by the honest peers, any malicious attempts will have negligible advantage.

The study shows that 64% of the transactions in Bitcoin network are confirmed under or below 10 min whereas remaining 36% took 10-40 min time for conformation.

Fast Payments: When payments are done in a quick time, they cannot operate on the basis of conformations of the transactions like supermarkets, vending machines etc…These kind of payments comes under fast payments where exchange of currency and goods are done in a shorter time.

In Bitcoin transactions to enable faster payments, merchants are suggested to approve the transaction without any conformation if it's not of a higher value. But the measure can't avoid the vulnerability of the Bitcoin network.

Necessary conditions for successful Double-spending:

To successfully double spend the money, the attacker needs to make the vendor accept the transaction (TRv) that will not be redeemed afterwards. An attacker creates a transaction (TRa) which will have same inputs as TRv but the recipient address will be an address which under his control or any other vendor or merchant.

The conditions which help an attacker to have a successful double-spending are:

- When the time taken by the vendor to accept the transaction TRv is less than the time taken by vendor to acknowledge the transaction TRa. Since network doesn't support multiple transactions that share common inputs, the transaction TRv cannot be redeemed.
- When the transaction TRa is already confirmed in any other block, then the transaction TRv is never confirmed by the network.

Types of attacks:

- Race Attack: Immediate acceptance of a 0/unconfirmed transaction by the vendor or the merchant leads to race attack. The coins in the transaction showed to the merchant might have been used in different transaction that would be first to make into the block. So, the transaction done to the merchant by the attacker has high chances of getting rejected and cannot be redeemed by the merchant.
- Finney Attack: Finnely attack is a fraudulent double-spending which requires the participation of a miner. A miner will have to include a non-broadcasted transaction which is deceiving in his block generation to achieve double-spending. But this attack is irrelevant for a smaller amounts and will not make any profit for the risk involved in it.
- >50% attack: When the attacker maintains or controls more than 50% of the network hash rate then this attack is possible. So, there will be higher chances of making a false transaction getting conformed across the network. Only high profits can make an attacker to resort to such an attack but since the mining is gaining popularity day by day it becomes practically impossible now.

Though, double-spending is theoretically possible, practically only a negligible amount of fraud is done through this mechanism. Now-a-days much of the fraud is done due to the insecurity of the wallets present at each node.

B. Malware

Malware, also called ransom-ware, is a hacker-controlled bot-net that directly attacks the PC or encrypts files stored in the drives. A type of such malware is 'Trojan-Ransom.Win32.Linkup' which blocks the internet access by modifying the DNS and turning the computer into a Bitcoin mining bot at the same time.

In addition to messing around with the DNS, Linkup can also link up to a remote server and pressgang the PC into service as a Bitcoin-mining bot. This is carried out via a downloader called 'pts2.exe', which extracts a second file, named 'j.exe', onto a computer. This is, in fact, a popular piece of mining software called 'jhProtominer'.

The damage that is likely to be inflicted by the Trojan is limited. jhProtominer only works on 64-bit operating systems, but even so, it still leaves plenty of computers around the globe to infect.

How do does the malware (also miners) get into mining systems?

BKDR_BTMINE.MNR may arrive on users' systems as part of a malware package. It may either be dropped or downloaded by other malware/ grayware/spyware from malicious sites. These may also be unknowingly downloaded by users while visiting malicious sites. BKDR_BTMINE.DDOS may also arrive as part of a malware package. These may be downloaded by other malware/grayware/ spyware from malicious sites or may be unknowingly downloaded by users while visiting malicious sites. Cybercriminals use social media to infect users' systems with Bitcoin-mining malware. They have, for instance, used Tweets with malicious links to trick users into downloading WORM_KOLAB.SMQX, which subsequently download HKTL_BITCOINMINE onto infected systems. Some cybercriminals also used WORM_OTORUN.ASH to exploit a certain network vulnerability to force systems to participate in a Bitcoin pool. It may also be dropped or downloaded by other malware/spyware/ grayware from malicious sites.

What happens to Bitcoin-mining-infected systems?

Bitcoin-mining malware primarily aim to force systems to generate Bitcoins for cybercriminals use.

BKDR_BTMINE.MNR accesses malicious URLs to procure certain IP addresses. It then accesses the IP addresses to send and receive information, to download other malware, and to get an updated list of IP addresses. It also downloads and uses one of three different Bitcoin-mining software, depending on the infected system's specifications.

BKDR_BTMINE.DDOS comes with a list of IP addresses that it tries to access in order to send and receive information, to download other malware, to get an updated list of IP addresses, and to obtain a list of sites to target via distributed denial-of-service (DDoS) attacks. Upon execution, WORM_KOLAB.SMQX creates a directory that contains HKTL_BITCOINMINE—a Bitcoin-mining-mining grayware, in an infected system. WORM_KOLAB.SMQX uses this grayware to generate Bitcoins without the users' knowledge. During analysis, the grayware tried but failed to access a malicious link using a specific user name and password. WORM_OTORUN.ASH attempts to force infected systems to participate in a Bitcoin-mining pool service known as Deepbit. A Bitcoin mining pool refers to a network of Bitcoin miners that process the same block for faster payout. The Bitcoins generated through such a pool are then divided among the participants.

C. Energy footprint

Bitcoin mining network is stuck in a cycle which is driving up its power usage. Miners tend to put more computing power on the network so that they can make more and more Bitcoins. The software underpinning the network reacts by changing a parameter that makes it more difficult to solve the mathematical problem needed to solve a Bitcoin block. Therefore, because it is harder to solve the problem, miners add even more computing power. As this cycle increases, it takes more electricity to mine a Bitcoin. The hashing power of the network surpassed the world's top 500 supercomputers almost a year ago. So the higher the value of one Bitcoin, the higher the value of mining rewards and transaction fees, the higher the energy consumption of the Bitcoin network in the long run.

Energy consumption and Bitcoin mining relation can be described as follows:

More efficient mining gear does not reduce energy use of the Bitcoin network. It will only raise the network difficulty

Cheaper energy linearly increases mining energy use of the Bitcoin network

The same conclusions apply to all proof of work based currencies.

A Bitcoin miner is part of Bitcoin's peer-to-peer network that collects recent transactions and aims to complete a proof of work scheme. In this scheme, there is a current target value T, which is periodically recalculated by the network. The miner's aim is to find a nonce value so that:

$$H(B.N) < T \quad (1)$$

where B is the string representing the recent transactions, N is the nonce value, '.' is the concatenation operator and H is the Bitcoin hash function, in this case:

$$H(S) := SHA256\,(SHA256(S))$$

The proof of work can be achieved by choosing values for N randomly or systematically until eq.1 is satisfied. When an N is found, the resulting block can be sent to the Bitcoin network and added to the Bitcoin blockchain. Finding a block results in a reward of extra Bitcoins for the block's finder.

Thus, the process of finding a suitable N value is referred to as Bitcoin mining.

The major limiting factors in Bitcoin mining are the hash rate of hardware and the cost of running this hardware. The hash rate, R, is typically measured in millions of hashes per second or Megahashes (Mhash/s). This is combined with the power usage, P, of the hardware to get the energy efficiency of the hardware $E = R/P$ (Mhash/J) which serves as a helpful statistic to compare hardware.

Initially mining took place on normal computers. As Bitcoin gained popularity, there was something akin to an arms race as miners attempted to increase their hash rate. Graphics Processing Units (GPUs) which can perform many parallel calculations are well-adapted to Bitcoin mining. Standard programming interfaces, such as OpenCL and CUDA, made GPUs popular among Bitcoin miners. Their higher hash rate compared with their lower energy footprint made them better suited to mining than normal CPUs. As the use of GPUs became more widespread, people were forced to look for alternatives to keep ahead of the crowd. Field Programmable Gate Arrays (FPGA) came into vogue for a brief period before Application Specific Integrated Circuits (ASIC) came onto the scene. ASICS can perform the Bitcoin hash at higher rates but with a much smaller energy requirement.

Bitcoin is similar to other currencies, in that the exchange rate between Bitcoin and other currencies fluctuates over time. This in turn impacts on the viability of Bitcoin mining; if the value of a Bitcoin is less than the cost of the energy required to generate it then there is a disincentive to continue mining. On the other hand, as the number of people mining Bitcoin increases, difficulty of mining follows suit, so the likelihood of discovering a valid block decreases. To overcome this, more powerful hardware is required to achieve the same success rate. However, since the cost of energy is a limiting factor, newer hardware will have to have a higher hash rate and a lower energy footprint. [11]

VI. What is Cloud and Why is it an Alternative

The key to the definition of cloud computing is "cloud" itself. Cloud is, by definition, a large group of interconnected computers. These computers can be personal computers or network servers and they can be public or private. For example, Google hosts a cloud that consists of both small PCs and large servers. Googles cloud is a private one which means it is accessible only by google users.

Cloud computing goes beyond a single company or enterprise. The applications and data served by the cloud are available to a broad group of users, across enterprises and across platforms. The access is via internet. Any authorized user can access these docs and apps from any computer over any Internet connection.

Cloud computing should not be confused with network computing where all the information are hosted on the company's single network and it can be accessed by members on that network only. Cloud is much bigger than that and it encompasses multiple companies, servers and networks.

In order to first think about implementing cloud technology with Bitcoin mining, it is essential to understand why a Cloud network based application is important. This can be explained by considering advantages of cloud computing, which are many but a few significant ones are listed as:

- Low-Cost Computers for Users: You do not need a high powered and highly priced computer to run cloud computing's web based applications. Because the application runs in cloud and not on the desktop PC, that PC does not need any processing power and Hard-disk space.
- Improvement in performance of computers: Because the desktop PC does not require to store and run tons of software applications, users will see better performance from their PC's. Put simply, computers on cloud network boot up faster and run faster because they have fewer programs and processes loaded in memory.
- Lower IT infrastructure cost: Instead of investing in larger numbers of more powerful servers, the staff of an IT company can use the computing power of the cloud to supplement or replace internal computing resources. These companies that have peak needs no longer have to purchase equipment to handle peaks in traffic.
- Lower software costs: Instead of purchasing separate software packages for each computer in the organization, only those employees actually using an application need access to that application in the cloud. Even if it costs the same to use similar desktop software, IT staffs are saved the cost of installing and maintaining those programs on every PC in the organization. Thus the costs of the software offered by cloud technology firms are much less than non-cloud firms.
- Fewer maintenance issues: Cloud computing substantially reduces both hardware and software maintenance cost for organizations. With less hardware in the form of fewer servers, the maintenance costs are immediately lowered. In the software front all applications are based on cloud servers, so maintenance practically zero.
- Cloud technology also offers unlimited storage capacity, increased data safety (as the data is not present directly on desktop it can be difficult for third party users to gain access), increased computing power and instant software updates (that is, when an application is updated by the owner or cloud service provider, this update is accessible to the users the next time they log in).

As a result of such attractive advantages pertaining to cloud services, Bitcoin mining can be made more efficient and cost-effective by exploiting various cloud technology services like:

- Infrastructure as a Service (IaaS)
- Software as a Service (SaaS)
- Platform as a Service (PaaS)

VII. Bitcoin Cloud Implementation

Since the Bitcoin industry is very erratic in nature, it may not be feasible to own and operate costly ASICs and therefore the need to introduce cloud-technology to help reduce and recoup losses associated with high electricity consumption and maintenance cost for the users/customers. The term 'Cloud Mining' is coined for carrying out mining operations, associated with various cryptocurrencies like Bitcoins, on a cloud network.

The basic idea is that the miners can carry-out mining operations without requiring owning an ASIC but renting one. The renting of these machines provides easier exit opportunities to the miner in times when losses due to falling Bitcoin prices or increased difficulty in mining network are inevitable. This is an example of Infrastructure as a Service. The miners can also use platforms like amazon EC2 and Digital Ocean for mining, which is Platform as a Service. Finally the miners can simple rent/lease the hashing power of ASICs owned by large hardware companies that specialize in the development of integrated circuits (ICs).

To elaborate, there are three forms of cloud mining techniques miners can exploit for better profitability:

A. Hosted mining machines

This scheme can refer to hosted Bitcoin ASIC mining also where the miners, clients, can lease or rent ASICs. The clients are required to pay monthly rental rates for a large range of Bitcoin ASIC mining systems and can also rent a dedicated physical machine for their personal use. The advantages of such a scheme are obvious; for instance, clients can eliminate the electricity costs pertaining to running such machines at home as well as reduce carbon footprint. Further, miners need not worry about re-selling the machines at reasonable prices.

Many companies are working on their own hosted mining facilities, for example, KnC Miner, a Sweden based company is planning to introduce such a scheme in Stockholm and at the same time use renewable energy sources to power up the machines. A range of ASIC machines from ‘Nano Fury NF2’ with 3700 million/sec hash rate and 5 watts consumption to ‘Hash Coins- Zeus v3’ that has hash rate of 4.5 million/sec , electricity consumption of 3000 watts with USB COMM ports can be used under this scheme. The selection of the rigs depends on the client’s budget and requirements.

B. Hosted platform mining

Under this scheme, a Client is required to rent virtual computers on which they can run their applications.

The Amazon EC2 platform:

The EC2 platform provides virtual services, also known as Compute Instances in the cloud quickly and inexpensively. The client is required to choose the instance type they want, selecting the templates which can be based on Windows or Linux and finally choosing the quantity of services (or virtual servers). This can be done by using the AWS management console or automate the entire process by an API using SDK in any programming language. After implementing the API code, client’s instances will begin running and they will have full access and administrative control just like any other server. The EC2 provides a range of instance type designed for different use cases. These range from small and economical instances for low volume applications all the way up-to clustered computer systems for high performance computing workload and cloud based super-computing on demand. The amazon EC2 provides instances optimized for compute, memory, storage, GPU processing and also high performance ASICs. This enables clients to choose the right price and performance combination for whatever workloads to be run. It is also easy to resize the instance as the requirements of the clients change. For instance during time when the hashing rates and difficulty of the network are very high the user can adjust the instance to obtain high performance and vice-versa. The user will pay according to the degree of requirements of instances.

The important feature of Amazon EC2, it comes to determining the profitability of the platform, is the flexibility of the pricing options available to miners. With on-demand prices the clients pay for what they use that is if the instances are stopped the miners stop paying as well. Thereby, helping cut losses given the erratic nature of Bitcoin prices. The reserved instance price provides significant demand over the on-demand prices in return for low one-time payment. Spot instance prices lets the miners to name the prices they want to pay for instances using market based pricing and allows computing capacity at a significant discount compared to on demand pricing.

The spot instances prices are the most economical of the three models, whereby the miners can bid for computing time at a price they are willing to pay. When amazon has spare capacity, it will grant the computing power to the highest bidder and if the bid prices are too low then the mining system may never come online.

Further, EC2 mining provides a number of built-in security features to provide protection from Malware and Trojan attacks. The instances are located in a Virtual private cloud or VPC, which is a logically isolated network that the miners control. The VPC provides a number of network security tools, like Network ACLS and Security Groups, to determine who can access your instances.

A Security Group acts as a virtual firewall that controls the traffic for one or more instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that allow traffic to or from its associated instances. Clients can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group. When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

A Network access control list (ACL) is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet. Clients might set up network ACLs with rules similar to the security groups in order to add an additional layer of security to the VPC.[12][13][14]

DigitalOcean:

Another type of such service is provided by DigitalOcean. It is a provider of virtual private servers (VPS). These servers are not actual computers, but simulated computers – several of which run simultaneously on powerful server computers at once. This is a cost effective way for any business providing online hosting services whether it be virtual private servers or web hosts.

Usually, a group of virtual servers hosted on single (or across a network of) physical servers do not all need the CPU and network resources at once. Therefore, having several simulated computers contained within one physical computer is more efficient as one set of hardware can be active all the time, providing resources to all of the virtual machines it hosts. The whole business of virtual hosting is somewhat like fractional reserve banking in that it relies upon most of its users not requiring its resources at any particular moment.

C. Leasing hashing power

Under the scheme, the miners can rent Hashing power of multiple, highly powered ASICs machines owned by mining companies. The hashing rate depends on the plan chosen by miners. The plan must be selected while considering the profitability factor. The various service providers are:

- Cloud Hashing: A one year contract specifying the hashing power required is awarded to the clients under this service. Contracts can range from 30Gh/s to as much as 350Gh/s.

- Hash Rack: A single payment for an indefinite time is made by the clients (i.e., until the hardware breaks), a percentage of which can be reinvested to increase hashing power. Additionally, users can move ‘hashpacks’ between multiple rigs owned by them.

- Bit Miner: Offers collective mining on a rent sharing basis. For instance, the Ant Miner rig (6x180 GH/s) is divided into 10,000 shares, each of which is priced at $5.50. Several such rigs are rented at such competitive pricing.

- E-Pickaxe: Contracts vary from one year to indefinite length of time, payments for which are done using Bitcoins. However, the amount of GH per contract is not fixed because, as they put it “as we add more hardware, your contracts have access to that too, meaning as we grow and invest in more hardware, you benefit from this throughout the term of the contract”.

- Bit of Glory: This firm offers 12-month contracts at 100 GH/sec, 500GH/sec and 1TH/sec.

- Cex.io: Clients using Cex.io can both mine as well as trade hashing speeds (GH/s). Profits are shared using the PPLNS (pay per last N shares) scheme and all hash-rates are guaranteed.

- Nimbus Mining: Nimbus Mining offers 12-month contracts of varying hashing powers, using ‘off-the-shelf’ hardware from various manufacturers, which can be chosen by the clients.

- eBay contracts: Several eBay users are currently offering mining contracts for a period of 24 hours for as little as £1 ($1.67). However, since these contracts are fulfilled on old USB Block Erupter rigs, the hashing power is limited. That said, this could set off a positive trend with powerful mining contracts being offered in the future.

VIII. Cloud Mining Efficiency Calculations

We have previously covered ways to calculate mining profitability for traditional mining methods. The difference is that the services offered are designed to work with the hardware parameters and not cloud-mining parameters.

Even so, we can still use these calculators by taking into account the costs involved. We had taken the example of Genesis block in determining profitability of hardware mining by multiplying the electricity charge ($ per KWh) by the power consumption of the unit and by a conversion factor of 0.744 (the ratio of seconds per month to joules of energy per KWh). But for cloud mining calculations we have to perform the opposite, mainly because the provider gives the miner an (effective) monthly running cost. Hence, we have to calculate the cost per kilowatt hour to feed into the mining calculator. This can be done by dividing the monthly running cost by the conversion factor (0.744) mentioned earlier. For example, if prospective/existing miners were to use these numbers into a Bitcoin mining calculator, they would enter ‘0’ for the cost of hardware, shipping costs and miscellaneous costs, and enter ‘1’ for power usage, and then enter the equivalent electricity cost into the electricity costs line.

However this type of calculation does not apply to all cloud mining service providers because some have a significantly different cost structure. Services provided by Hash Rack or Cex.io cloud mining companies, for example, would not be suitable for the calculations mentioned above.

IX. Limitations of Cloud

Engaging in any type of cryptocurrency mining can lead to risks but profits are possible if miners can make the right choices with regard to the factors mentioned earlier. While calculating profitability it is quite clear that some cloud mining services will be profitable for a few months, but as the difficulty level of the Bitcoin increases it is highly possible that miners start to make loses four to six months beyond.

Cloud Mining has been taking a beating with the precipitous drop in Bitcoin price over the past year. The profit margins have become thinner and thinner, and also non-existent for many miners and service providers. The value of less valuable altcoins has seen a corresponding tumble in value. On January 13, 2015 GHash.io reported that many as 30,000 miners are leaving the industry since BTC had entered the $300-and-below range.

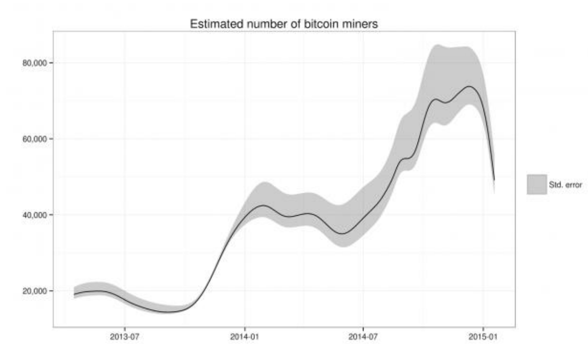


Fig. 3. Representation of the fall in Bitcoin miners [15]

The main reason for the mass exodus can be attributed to issues with paying off large loans for computer equipment, hosting services, rent and location leasing costs, all while keeping up with the latest in digital mining software and tech. These short-term costs can reach into the millions in dollars. As the price of Bitcoin has continued to drop, even the World’s largest mining operations are unable to cover their costs at this time. In early 2015 CEX.IO, the second-largest Bitcoin mining pool extant, had temporarily suspended operations due to an inability to run their operation profitably. Another Bitcoin mining firm that has had to change with the times is GAW Miners. They moved into cloud mining in summer of 2014, and the company recently launched its virtual currency called Paycoin. Many customers who continue to mine using GAW’s cloud-based “hashlets” have witnessed their operating fees starting to exceed the returns from mining. If the market is having this much of an effect on the major player it is easy to estimate the effect on smaller service providers. Many have had to halt operations and payouts, including ZeusHash and PB Mining.

X. Conclusion

Since the start of the virtual currency revolution, the rate of evolution of mining techniques to maximize hashing rates (in turn maximizing profits) has been staggering. With mining machines and technologies becoming redundant at amazingly quick rates, stability has always been a question. It took only three years since the introduction of Bitcoins for miners to move from using their CPUs to buying mining specific ASIC machines. To make matters worse, the fluctuating values of the various cryptocurrencies make it impossible for any long term investment that does not involve considerable risks. The amount of computation required to validate transactions has been increasing exponentially because of two reasons – the complexity increases with each hash generated and the number of people entering the world of Bitcoin mining, which in turn increases the hash rate. Given the perilous scenario, where mining with privately owned ASICs and similar machines has the odds stacked against it when it comes to profitability, cloud mining by leasing machines seems to be the way forward, as it offers greater chances of profit and easier exit options with a very low initial investment.

The flipside is that even for many of the cloud mining providers, this initial short term investment to buy large and powerful mining machines, security features, space, air conditioning for the systems and electricity to power them is way too high, as can be seen from the temporary suspension of operations of key players such as cex.io. With stringent government regulations, and a general negative outlook on cryptocurrencies, sudden drops and rises in the value of Bitcoins is bound to happen time and again and miners need to be braced for it. What one needs to keep in mind is that, such sudden drops notwithstanding, value of Bitcoins, and cryptocurrencies in general would rise proportionally to the increase in hashing difficulty.

For cloud mining to be successful, miners need to move from private mining techniques and adopt cloud mining on a larger scale, which would only then justify the initial expenses of these cloud service providers. A dangerous scenario that may arise when this does not happen is that several of these providers would face losses and ultimately quit, leaving only few giants such as Amazon or Digital Ocean in business, who would then gain complete dominance over the mining network, leading to monopoly. Not only is this unhealthy to the mining network, it is against its fundamental nature that the system is decentralized and provides equal opportunities to all miners.

This paper provided an in depth view of types of cryptocurrencies currently in operation, the types of mining algorithms and the history of machines used for mining process, which led us to the next logical step of cloud based mining. But of course, this is definitely not the final solution. As complexity and competition increases, faster and more efficient machines are bound to be designed. However, at present, cloud mining presents the most viable route to maximizing profits.

References

[1] Morgan E. Peck - The Bitcoin Arms Race is on! Spectrum, IEEE, vol.50 (2013), Issue: 6, pp. 11-13.

[2] Allied Control – Analysis of Large-Scale Bitcoin Mining Operations (White Paper), URL: http://www.allied-control.com/publications/Analysis_of_Large-Scale_Bitcoin_Mining_Operations.pdf.

[3] Brito, J. & Castillo, A. (2013). Bitcoin: A Primer for Policymakers.

[4] S. Nakamoto. “Bitcoin: A Peer-to-Peer Electronic Cash System,” URL: https://bitcoin.org/bitcoin.pdf, 2008.

[5] The cryptographic hash function SHA-256, URL: http://www.researchgate.net/publictopics.PublicPostFileLoader.html?id=534b393ad3df3e04508b45ad&key=50463534b393ab994e.

[6] Evans-Pughe, C.; Novikov, A.; Vitaliev, V.-“To bit or not to bit?”. Engineering & Technology, vol. 9 (2014), Issue: 4, pp. 82-85

[7] Hurlburt, G. F; Bojanova I. - “Bitcoin: Benefit or Curse”. IT Professional, vol. 16(2014), Issue: 3, pp. 10-15.

[8] Taylor, M. B - “Bitcoin and the age of Bespoke Silicon”. Compilers, Architecture and Synthesis for Embedded Systems (CASES), 2013 International Conference, 2013, pp. 1-10

[9] Mining Hardware Comparison, URL:https://en.Bitcoin.it/wiki/Mining_hardware_comparison

[10] Bitcoin Difficulty. URL: https://Bitcoinwisdom.com/Bitcoin/difficulty

[11] O’Dwyer, K. J.; Malone, D. - “Bitcoin Mining and its energy footprint”. Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014). 25th IET, pp. 280-285

[12] Amazon EC2. URL: http://aws.amazon.com/ec2/

[13] Amazon Elastic Compute Cloud. URL: http://en.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud

[14] Amazon EC2 Security Groups for Linux Instances. URL: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-network-security.html

[15] January 18th 2015 Network Statistics. URL: http://organofcorti.blogspot.com.au/2015/01/january-18th-2015-network-statistics.html

Development of Prediction Model for Endocrine Disorders in the Korean Elderly Using CART Algorithm

Results from a Population-Based Study

Haewon Byeon
Department of Speech Language Pathology & Audiology
Nambu University
Gwangju, Republic of Korea

***Abstract*—The aim of the present cross-sectional study was to analyze the factors that affect endocrine disorders in the Korean elderly. The data were taken from the A Study of the Seoul Welfare Panel Study 2010. The subjects were 2111 people (879 males, 1,232 females) aged 60 and older living in the community. The dependent variable was defined as the prevalence of endocrine disorders. The explanatory variables were gender, level of education, household income, employment status, marital status, drinking, smoking, BMI, subjective health status, physical activity, experience of stress, and depression. In the Classification and Regression Tree (CART) algorithm analysis, subjective health status, BMI, education level, and household income were significantly associated with endocrine disorders in the Korean elderly. The most preferentially involved predictor was subjective health status. The development of guidelines and health education to prevent endocrine disorders is required for taking multiple risk factors into account.**

Keywords—data-mining; CART; elderly; health behavior; endocrine disorders

I. Introduction

One of the biggest difficulties in old age is health problems [1]. Among them, endocrine disorders, such as diabetes, are known as typical old-age chronic diseases [2]. According to a survey on causes of death by Statistics Korea, diabetes is the fifth major cause of death as of 2013, and fatalities from diabetes increase dramatically by over 40 times from 3.3 to 135.4 out of every 100,000 people in the population of those in their 40s to those in their 70s, respectively [3]. Given that diabetes is related to various complications, such as cerebrovascular diseases, its actual effect on death is predicted to be much greater. In addition, endocrine disorders add to the psychological and economic burden on a patient's family as well as the patient themselves in that they require consistent self-management to prevent complications after treatment.

The endocrine system is a generic term that refers to hormone secretion organs, and, based on its structure, the system consists of the pituitary, pineal, thyroid, parathyroid, and adrenal glands and the pancreas and gonads [4]. Hormones secreted from the endocrine system move to the target organs through the blood and play important roles in the growth and development of the body and the maintenance of the metabolism and homeostasis [5]. Therefore, although an imbalance of hormones does not manifest symptoms immediately, sustained hormonal problems ultimately cause metabolic disorders and fatal complications by destroying the balance of metabolic activities in the body [6, 7]. In particular, when managed poorly, diabetes, an endocrine disease, has a high possibility of causing complications, such as cerebrovascular diseases (e.g. stroke) or microvascular diseases (e.g. diabetic retinopathy) [8]; therefore, the ultimate treatment goal of endocrine disorders is controlling the disease process.

As it is necessary to manage risk factors, such as life habits, to prevent endocrine disorders and complications, it is important to elucidate related factors that affect endocrine disorders to ensure healthy aging, especially in old age. So far, a high level of education and income, participation in social activities, and positive social recognition have been reported as protective factors against endocrine disorders [2, 4, 9]. These protective factors play a role in decreasing the risk of endocrine disorders by promoting positive health-related behaviors.

On the other hand, depression, stress, irregular eating patterns, smoking, drinking, obesity, and lack of exercise have been reported as risk factors that increase the risk of endocrine disorders [10–13]. The majority of preceding studies, however, have researched risk factors on an individual basis by using regression analysis, and there is still a lack of studies that have explored various related factors in an integrated manner. In particular, a regression model requires assumptions, such as linearity, normality, and homoscedasticity, and as the distributions of some disease data are non-linear, the normality and homoscedasticity of this regression model are not suitable.

Recently, as data-mining has been used as a method of predicting diseases, complex exploration is being used for risk factors [14]. In particular, among the data-mining methods, the Classification And Regression Tree (CART) has several advantages; first, it enables nonparametric analysis; second, it enables easy understanding of disorders, as its analysis process is expressed in the tree structure; third, it enables understanding of the most closely-related factors.

Endocrine disorders frequently elude complete recoveries. In addition, since practical management must be performed by the patient themselves even when the treatment is in progress, complications should be prevented or postponed through elimination of risk factors and sustained management [1]. Therefore, a vital theme in maintaining health in old age is determining complex factors related to old-age endocrine disorders and predicting high-risk groups.

This study developed a prediction model of endocrine disorders for the Korean elderly by using data-mining and provides basic material for the prevention of old-age endocrine disorders. This paper is organized as follows: the study population and measurements are described in section 2. CART Algorithm is described in section 3. I conducted a series of experiments to verify proper performance of CART Algorithm in section 4 and the conclusions are presented in section 5.

II. Methods

A. Study population

This study analyzed raw data from Seoul Welfare Panel Study (SWPS) conducted by Seoul Welfare Foundation on citizens of Seoul from June 1, 2010 through August 31, 2010. Having acquired authorization of Statistics Korea (no. 20113) in 2009, SWPS was conducted for the purpose of investigating the level of welfare of the households and reality of vulnerable classes in Seoul and estimating the demand of welfare services [15]. The population of the study was households in Seoul at the time of 2005 Population and Housing Census and sampling was conducted on 25 districts of Seoul using stratified cluster sampling. Major survey items were income, economic level, health, living condition and demand for welfare services and survey method was Computer Assisted Personal Interviewing in which interviewers visited target households and entered responses answered according to the structured questions in notebook computers.

This study analyzed 2,111 senior citizens (879 males, 1,232 females) over the age of 60 among 7,761 people who completed SWPS.

B. Measurements

Outcome was defined as prevalence of endocrine disorders (diabetes, hypothyroidism, thyroid hyperactivity). Explanatory variables were included as sex, final education (elementary school and lower, middle, high school, over college), whether or not being engaged in economic activities (yes, no), the average monthly income of households (less than 2 million won, 2-4 million won, more than 4 million won), marital status (living with spouse, living without spouse, unmarried person), binge drinking (yes, no), smoking (non-smoker, past smoker, current smoker), BMI (underweight, normal, overweight), subjective health status (good, fair, poor), regular exercise (no, yes), experience of stress in the last 1 months, depressive symptoms in the last 1 months (yes, no). Binge drinking was defined as five or more drinks ($\geqslant$ 61 g of alcohol) per episode for men and as four or more drinks per episode ($\geqslant$ 41 g of alcohol) for women, with reference to the International Center for Alcohol Policies [16].

III. Statistical Analysis

A. Exploration on factors related to the endocrine disorders

For general characteristics, mean and percentage were presented and difference between groups based on endocrine disorders was analyzed by Chi-square test.

B. CART Algorithm

When the related factors of endocrine disorders were identified in the chi-square test, the related factors of endocrine disorders were statistically classified and a prediction model was established, using CART (Classification And Regression Tree) Algorithm.

Classification And Regression Tree (CART) is a data-mining algorithm suggested by Breiman in 1984 which measures impurities by using Gini Index and performs binary split that only forms 2 children nodes from the parent's node [17].

CART has the advantage that it enables easy interpretation of created rules and it can use both continuous variables and categorical ones. Continuous variables creates separation rules in the form of “X≤C?” or “X≥C?” while categorical binary creates separation rules in the form of “X∈{A, B}”.

Gini's coefficient is a probability of two extracted elements' belonging to two different groups when the two elements are extracted from n number of elements [18]. First, misclassification probability is calculated in each node and the statistic equation runs as formula 1.

$$Gini\ Index\,(t) = 1 - \sum_j [P(j/t)]^2 \qquad (1)$$

Next, all misclassification probabilities are added and the estimate of misclassification probability is calculated with formula 2.

$$G = \sum_{j=1}^{c} \sum_{i \neq j} P(i)P(j) \qquad (2)$$

After the decrement of Gini's coefficient is calculated, the predictor which reduces Gini's coefficient the most is chosen as child node as the last step of the algorithm formula 3.

$$G = \sum_{j=1}^{c} P(i)(1-P(j)) = 1 - \sum_{j=1}^{c} P(j)^2 = 1 - \sum_{j=1}^{c} (n_j/n) \qquad (3)$$

In the CART, the Alpha value for the criteria of splitting and merging was set at 0.05. The number of parent nodes was 200 and that of child nodes was 100, and the number of branches was limited to 5. The validity of the model was tested using the 10-fold cross-validation.

IV. Results

A. General characteristics of subjects and factors related to endocrine disorders

General characteristics of subjects and factors related to endocrine disorders are presented in Table 1.

TABLE I. GENERAL CHARACTERISTICS OF THE SUBJECTS BASED ON ENDOCRINE DISORDERS, N (%)

Variables	**Endocrine disorders** *No (n=1,738)*	*Yes (n=373)*	***p***
Sex			0.098
Male	738 (84.0)	141 (16.0)	
Female	1,000 (81.2)	232 (18.8)	
Final education			0.170
≤ Elementary school	735 (80.4)	179 (19.6)	
Middle school	309 (82.8)	64 (17.2)	
High school	422 (85.1)	74 (14.9)	
≥ College	272 (82.9)	56 (17.1)	
Economic activities			0.007
Yes	309 (87.3)	45 (12.7)	
No	1,429 (81.3)	328 (18.7)	
Average monthly income of households			0.388
< 2 million won	1,113 (81.5)	253 (18.5)	
2-4 million won	409 (84.2)	77 (15.8)	
> 4 million won	75 (80.6)	18 (19.4)	
Marital status			0.978
Living with spouse	1,167 (82.2)	252 (17.8)	
Living without spouse	35 (83.3)	7 (16.7)	
Unmarried person	536 (82.5)	114 (17.5)	
Binge drinking			<0.001
Yes	438 (87.8)	61 (12.2)	
No	1,300 (80.6)	312 (19.4)	
Smoking			0.565
Current smoker	180 (84.1)	34 (15.9)	
Past smoker	373 (80.9)	88 (19.1)	
Non smoker	1,185 (82.5)	251 (17.5)	
BMI			0.059
Underweight	410 (82.5)	87 (17.5)	
Normal	1,034 (83.5)	204 (16.5)	
Overweight	294 (78.2)	82 (21.8)	
Subjective health status			<0.001
Good	533 (91.3)	51 (8.7)	
Fair	584 (83.7)	114 (16.3)	
Poor	621 (74.9)	208 (25.1)	
Regular exercise			0.842
Yes	773 (82.1)	168 (17.9)	
No	965 (82.5)	205 (17.5)	
Experience of stress in the last 1 months			0.022
Yes	472 (78.9)	126 (21.1)	
No	868 (84.4)	161 (15.6)	
Depressive symptoms in the last 1 months			0.001
Yes	421 (77.8)	120 (22.2)	
No	1,317 (83.9)	253 (16.1)	

Among the total of 2,111 subjects, number of those who have endocrine disorders was 373 (17.7%).

As the result of chi-square test, prevalence of endocrine disorders has statistically significant difference in conomic activities, alcohol drinking, BMI, subjective health status, experience of Stress, depressive symptom ($p<0.05$).

The prevalence of endocrine disorders was higher in unemployed(18.7%), non-drinkers(19.4%), obesity(21.8%) those with bad subjective health(25.1%), those who are under stress (21.1%), those with depression symptoms (22.2%), unemployed (18.7%), non-drinkers (19.4%), obesity (21.8%) and subjective poor health (25.1%), stress received (21.1%), that depressive symptoms (22.2%).

B. *Prediction model for endocrine disorders using CART algorithm*

Prediction model for endocrine disorders using CART algorithm is presented in Figure 1.

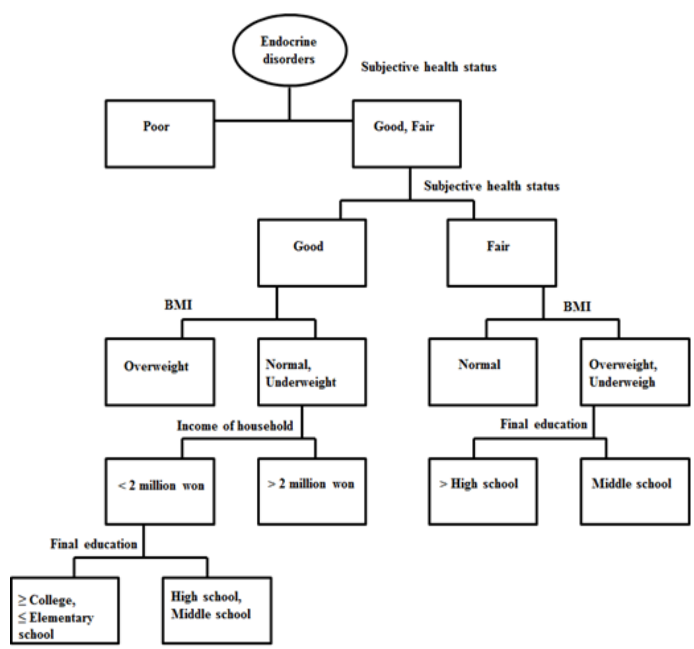


Fig. 1. Prediction model for endocrine disorders

As the result of constructing statistical classification model using CART algorithm after including variables set as factors related to endocrine disorders through chi-squared test, factors having significant effect were subjective health status, BMI, education level, and household income. The most preferentially involved predictor was subjective health status.

Table 2 is a profit chart of prediction model for endocrine disorders by CART algorithm suggested in the higher order of path for subjects' improved gain. In CART algorithm, the paths with improved gain of less than 100% are regarded as insignificant.

When this study drew out profit indicator for each node to seek out prediction paths for endocrine disorders, 2 nodes were confirmed as significant paths which effectively predict the endocrine disorders.

TABLE II. PROFIT CHART OF PREDICTION MODEL FOR ENDOCRINE DISORDERS BY CART ALGORITHM

Node no	Subjects (%)[a]	Gain n (%)[b]	Response %[c]	Gain Index %[d]	Description
12	88 (4.2)	24 (6.4)	27.3	154.4	The elderly who are middle school graduates with average subjective health and BMI which is either obese or underweight
1	829 (39.3)	208 (55.8)	25.1	142.0	The elderly who perceive their health status as poor

a. Node n(%); node number, % to 2,111

b. Gain n(%); gain number, % to 373

c. Response (%): The fraction of the endocrine disorders in the elderly

d. Gain index (%):=154.4 in total 8 node

The first path with the biggest profit indicator for the prediction of the endocrine disorders was the elderly who are middle school graduates with average subjective health and BMI which is either obese or underweight and its profit indicator was 154.4%.

The second path was the elderly who perceive their health status as poor and its profit indicator was 142.0%.

When the analysis on the prediction model by CART algorithm was completed, this study conducted 10-fold cross-validation test to assess developed prediction model. As the result of the 10-fold cross-validation test to compare stability of drawn-out model, drawn-out risk index was 0.287 and misclassification rate was 29% for cross classification model, showing the same risk index 0.288 and misclassification rate 29% of prediction model.

Surface area of Receiver Operation Characteristic (ROC) Curve (AUROC) which presents explanatory power of prediction model was 0.71, demonstrating that explanatory power of prediction model is average or medium level (Figure 2, Figure 3).

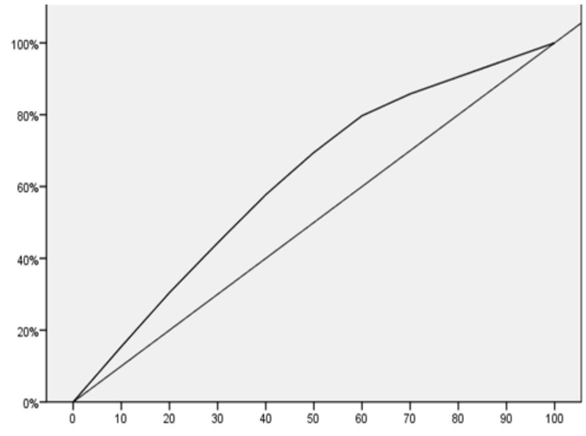


Fig. 1. Gains percentile of final model

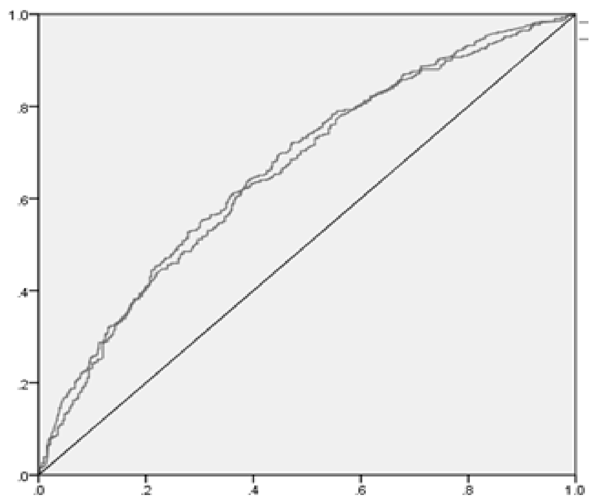


Fig. 2. ROC curve of final model

V. CONCLUSION

In order to investigate the potential factors related to endocrine disorders in the elderly over the age of 60 in local communities, this study developed a prediction model based on the CART algorithm by using epidemiological data, which represent the general Korean population.

In the prediction of endocrine disorders in old age in this study, the overriding factor was subjective health status. Subjective health is known to recognize physiological and biological changes more correctly and have a greater effect on interactions among the nerve system, endocrine system, and immune system than the objective measurement of health [19]. Additionally, the 2008 National Survey on Living Conditions and Welfare Needs of the Elderly conducted by the Korea Institute for Health and Social Affairs reported that 90.0% of the elderly who perceive their health as poor had more than one chronic disease [20]. Therefore, the reason why subjective health is highlighted as the most compelling factor for endocrine disorders in this study is because the elderly with poor subjective health may have perceived problems of the endocrine system by responding to physical problems more sensitively than the elderly with good subjective health; second, in contrast, the elderly with endocrine disorders might have perceived their health as poor. As subjective health is a major motivating factor that influences health-promoting behaviors [21], in order to prevent endocrine disorders, it is necessary to implement regular check-ups and health education for the elderly with poor subjective health.

This study identified two high-risk groups who are vulnerable to old-age endocrine diseases. According to this prediction model, "the elderly who are middle school graduates with average subjective health and are either obese or underweight" and "the elderly who perceive their health status as poor" are at a high-risk for endocrine disorders.

According to preceding studies that investigated factors related to endocrine diseases, a high level of education was a protective factor against endocrine disorders, and, in contrast, a low level of education increased the risk of endocrine disorders [1]. Moreover, in elderly people, not only was there a relationship between health-promoting living habits and subjective health status and were socio-demographic variables, such as education, major variables of living habits [22], but the elderly with subjectively good health also practice positive living habits more [23], which demonstrates that the results of preceding studies support those of this study.

Furthermore, this study implies that the risk factors identified in preceding studies, such as socio-demographic characteristics and living habits, not only affect endocrine diseases on an individual basis, but work in synergy with other risk factors as well. Considering that subjective health status, health-promoting behaviors, and desirable living habits are correlated, it is necessary to develop programs for preventing endocrine diseases that take level of education, subjective level of health, and living habits into consideration.

The limitations of this study are as follows; first, there is a possibility that potential factors exist that may influence endocrine disorders other than the factors included in the study model. Second, as this study is based on cross-sectional research, the results of the study cannot be interpreted as causal relationships.

The elderly who are middle school graduates with average subjective health, who are either obese or underweight, and who perceive their health status as poor were high-risk groups for endocrine disorders. The development of guidelines and health education for preventing endocrine disorders is required for taking multiple risk factors into account. Furthermore, longitudinal studies to explore the causal relationship between multiple risk factors and endocrine disorders are required.

Acknowledgment

The author wish to thank the Seoul Welfare Foundation on citizens of Seoul that provided the raw data for analysis.

References

[1] A. Steptoe, C. Wright, S. R. Kunz-Ebrecht, and S. Iliffe, Dispositional optimism and health behaviour in community-dwelling older people: associations with healthy ageing. British Journal of Health Psychology, vol. 11, no. 1, pp.71–84, 2006.

[2] D. Kapoor, and T. H. Jones, Smoking and hormones in health and endocrine disorders. European Journal of Endocrinology, vol. 152, no. 4, pp. 491–499, 2005.

[3] Available at: http://kostat.go.kr/portal/korea/index.action, accessed in 15/8/2015

[4] S. H. Golden, K. A. Robinson, I, Saldanha, B, Anton, and P. W. Ladenson, Prevalence and incidence of endocrine and metabolic disorders in the United States: a comprehensive review. The Journal of Clinical Endocrinology & Metabolism, vol. 94, no. 6, pp. 1853–1878, 2009.

[5] U. Meier, and A. M. Gressner, Endocrine regulation of energy metabolism: review of pathobiochemical and clinical chemical aspects of leptin, ghrelin, adiponectin, and resistin. Clinical Chemistry, vol. 50, no. 9, pp. 1511–1525, 2004.

[6] C. G. Campbell, S. E. Borglin, F. B. Green, A. Grayson, E. Wozei, and W. T. Stringfellow, Biologically directed environmental monitoring, fate, and transport of estrogenic endocrine disrupting compounds in water: a review. Chemosphere, vol. 65, no. 8, pp. 1265–1280, 2006.

[7] L. Adorini, G. Penna, Control of autoimmune diseases by the vitamin D endocrine system. Nature Clinical Practice Rheumatology, vol. 4, no. 8, pp. 404–412, 2008.

[8] J. M. Forbes, and M. E. Cooper, Mechanisms of diabetic complications. Physiological reviews, vol. 93, no. 1, pp. 137–188, 2013.

[9] A. Monzani, F. Prodam, A. Rapa, S. Moia, V. Agarla, S. Bellone, and G. Bona, Endocrine disorders in childhood and adolescence: natural history of subclinical hypothyroidism in children and adolescents and potential effects of replacement therapy: a review. European Journal of Endocrinology, vol. 168, no. 1, pp. 1–11, 2013.

[10] D. L. Musselman, and C. B. Nemeroff, Depression and endocrine disorders: focus on the thyroid and adrenal system. British Journal of Psychiatry, vol. 168, no. 30, pp. 123–128, 1996.

[11] S. Safea, Endocrine disruptors and human health: is there a problem. Toxicology, vol. 205, no. 1, pp. 3–10, 2004.

[12] S. H. Golden, A. Brown, J. A.Cauley, M. H. Chin, T. L. Gary-Webb, C. Kim, J. A. Sosa, A. E. Sumner, and B. Anton, Health disparities in endocrine disorders: biological, clinical, and nonclinical factors—an Endocrine Society scientific statement. The Journal of Clinical Endocrinology & Metabolism, vol. 97, no. 9, pp.1579–1639, 2012.

[13] S. Melmed, K. S. Polonsky, P. R. Larsen, and H. M. Kronenberg, Williams textbook of endocrinology. PA: Elsevier & Saunders, 2011.

[14] H. Byeon, The risk factors of laryngeal pathology in Korean adults using a decision tree model. Journal of Voice, vol. 29, no. 1, pp. 59–64, 2015.

[15] Seoul Welfare Foundation, Seoul Welfare Panel Study 2010. Seoul, Seoul Welfare Foundation, 2010.

[16] International Center for Alcohol Policies. ICAP blue book: practical guides for alcohol policy and prevention approaches. Available at: http://www.icap.org/PolicyTools/ICAPBlueBook/ accessed in 15/8/2015

[17] C. El Moucary, Data Mining for Engineering Schools: Predicting Students' Performance and Enrollment in Masters Programs. International Journal of Advanced Computer Science and Applications, vol. 2, no. 10, pp. 1–9, 2011.

[18] H. Byeon, and R. Lee, Prediction model for the smoking in Korean adolescent using CART algorism. Information-An International Interdisciplinary Journal, vol. 17, no. 12A, pp. 6273–6278, 2014.

[19] N. J. Kim, The effect of regular exercise on the subjective health and social activity of the elderly. Journal of Korean Physical Education, vol. 39, no. 1, pp. 149–158, 2000.

[20] Korea Institute for Health and Social Affairs, A study of 2008 living profiles and welfare service needs of older persons in Korea Survey. Seoul, Korea Institute for Health and Social Affairs, 2010.

[21] C. N. Wei, K. Harada, K. Ueda, K. Fukumoto, K. Minamoto, and A. Ueda, Assessment of health-promoting lifestyle profile in Japanese university students. Environmental health and preventive medicine, vol. 17, no. 3, pp. 222–227, 2012.

[22] O. Simsekoglu, and N. Aydemir, Health-seeking practices and psycho-social factors related to health behaviors in a Turkish sample. Journal of Behavioral Health, vol. 3, no. 1, pp. 17–24, 2014.

[23] J. Ogden, Health psychology. Berkshire, McGraw-Hill Education, 2012.

An Approach to Improve Classification Accuracy of Leaf Images using Dorsal and Ventral Features

Arun Kumar
Dept. of Computer Science & Engineering
Sir Padampat Singhania University
Udaipur, India

Deepak Khazanachi
School of Information Technology
University of Nebraska
Omaha, USA

Vinod Patidar
Department of Physics
Sir Padampat Singhania University
Udaipur, India

Poonam Saini
Dept. of Computer Science & Engineering
Sir Padampat Singhania University
Udaipur, India

***Abstract*—This paper proposes to improve the classification accuracy of the leaf images by extracting texture and statistical features by utilizing the presence of striking features on the dorsal and ventral sides of the leaves, which on other types of objects may not be that prominent. The texture features have been extracted from dorsal, ventral and a combination of dorsal-ventral sides of leaf images using Gray level co-occurrence matrix. In addition to this, this work also uses certain general statistical features for discriminating them into various classes. The feature selection work has been performed separately for the dorsal, ventral and combined data sets (for both texture and statistical features) using the most common feature selection algorithms. After selecting the relevant features, the classification has been done using the classification algorithms: K-Nearest Neighbor, J48, Naïve Bayes, Partial Least Square (PLS), Classification and Regression Tree (CART), Classification Tree(CT). The classification accuracy has been calculated and compared to find which side of the leaf image (dorsal or ventral) gives better results with which type of features(texture or statistical). This study reveals that the ventral leaf features can be another alternative in discriminating the leaf images into various classes.**

***Keywords*—Leaf image; Leaf classification; Texture features; Statistical features; Dorsal and ventral sides of leaves; Gray level co-occurrence matrix**

I. INTRODUCTION

The plants play an integral role in the ecological balance by providing shelter, improving the atmosphere, providing medicinal values etc. Therefore, there is a dire necessity to preserve and conserve them. Plants have also been studied for increasing food production, bringing forth new varieties of fruits, flowers and plant species. Several attempts have been made to classify the plants on the basis of flowers, arrangement of leaves on the plants, shapes, color and texture, to name a few. Such studies are essential for the ecological balance as some of the plants are on the verge of the extinction. For a layman, the characteristics features of a digital image are texture, shape, color and size. But, for a computer system there must be a computer recognizable feature set which could be stored, refined and analysed for appropriate classification. The human quest for finding the image textural features dates back to 1970's when Haralick [1], Rosenfeld and Troy [2] have obtained textural coarseness of digital images by finding the difference of the gray values of the adjacent pixels and then performing autocorrelation of the image values. The texture based properties of digital images have also been used in medical images [3] and in tomography based images [4], analysis of ultrasound images [5] and classification of food items like Italian pasta and plum cakes [6,7].

Some common approaches for plant leaf classification using digital images are based on geometrical properties [8], texture and shape based features [9] and color features [10].

Nature has given two faces to the leaves: the dorsal (or the face up side) and the ventral (or the back side facing the substratum). The dorsal sides are generally smooth with texture, absorbing sunlight whereas the ventral sides have prominent vein structure. The fine line present on the leaf is called the mid rib or the prominent vein and other hair like lines are called secondary veins. The pattern of leaf venation is an important characteristic for the identification of a plant.

The texture is an integral property of every surface: patterns of tiles, wood, fabric or crops in the field. A texture contains important information regarding structural arrangement of surface and its relationships with the surroundings. The human eyes can interpret texture features for a surface which is fine, coarse, rough or smooth, rippled or irregular. In the case of digital images, the texture represents the arrangement of pixels and their distribution, which is very helpful in classifying the images into various categories. A digital image data structure is represented through pixels expressing the relative brightness values. All the pixels in a digital image form the population and in statistical jargon, a sample is a subset of values taken out from a digital image to draw appropriate conclusions about the characteristic properties exhibited by the population. A statistical sample drawn from a large population can be represented through frequency distribution or correlation curves can be drawn, through which detailed statistical analysis can be performed.

Therefore, the univariate image statistics like mean, mode, median or standard deviation etc. can be utilized in studying and discriminating one class of digital image from the other.

The present study proposes to improve the classification accuracy of the leaf images by extracting texture and statistical features by utilizing the presence of striking features on the dorsal and ventral sides of the leaves, which on other types of objects may not be that prominent. The texture features have been extracted from dorsal, ventral and a combination of dorsal-ventral sides of leaf images using Gray level co-occurrence matrix. In addition to this, certain general statistical properties [11] like Mean, Median, Integrated Density, Skewness, Kurtosis, Minimum value, Standard Deviation, Raw-Integrated Density, XM and YM of leaf images for discriminating them into various classes have been used. The most important task for achieving higher degree of classification accuracy is to extract relevant features which can improve the overall accuracy of the classifier. Hence, the selection of an appropriate set of features is very important in pattern recognition problems. The feature extraction algorithms help in reducing the storage space requirement for the data, the visualization of the small dataset improves, the features and their relation can be better understood, and further, the training phase is greatly reduced. This work performs the feature selection task for the dorsal, ventral and combined data sets (for both texture and statistical features) using the most common feature selection algorithms. After selecting the relevant features, the leaf images are classified using the classification algorithms: K-Nearest Neighbor, J48, Naïve Bayes, Partial Least Square (PLS), Classification and Regression Tree (CART), Classification Tree (CT) and then the classification accuracy for each algorithm with each feature data set is calculated. One of the objectives behind the study of dorsal and ventral sides of leaf images using texture and statistical features is to find which side (dorsal or ventral or dorsal-ventral) gives best classification results and with which type of classification approach: texture or statistical. The rest of the paper has been divided into four sections, the Section II highlights the proposed methodology (Creation of colored leaf Image data set, Preprocessing of the Digital images, Generation of texture features, Generation of statistical features, Feature Selection process in different data sets, Application of classification algorithms), the Section III describes the results obtained through the proposed methodology and their comparison with the similar recent work and in Section IV, the conclusion follows.

II. Proposed Methodology

This work proposes to use the dorsal and ventral sides of the leaf images using texture and statistical approaches for leaf discrimination into classes. The proposed approach involves the following steps:

A. Creation of colored leaf Image data set

The leaf image data set is available from several sources (Data Banks) including that of [12, 13, 14]. But the images that are stored in the data set are that of dorsal leaf images. But, this work proposes to utilize both the dorsal and the ventral faces of the leaf images. This necessitated the creation of a new data set with both the faces of the leaf images. For the purpose of creating the required database, the 24-bit RGB images of dorsal and ventral faces of leaves of the Helianthus annuus L.(Sunflower), Psidium guajava (Guava) and Alcia rosea (Hollyhock) have been captured as shown in Fig. 1 using Sony Cybershot HX200V with 18.2MP "Exmor R™" CMOS Sensor with extra high sensitivity technology, 30x optical zoom. The captured images include 100 dorsal side and 100 ventral side images for each of the above mentioned leaf categories totaling a sample size of 600 images with a pixel size of 1080 X 920.

Fig. 1. Colored sample of dorsal and ventral leaf images

B. Preprocessing of the Digital images

The leaf images were extracted using background removal technique. In order to find out the texture features and to reduce the computational complexity, all the colored images were converted to 8-bit gray level and reduced to the pixel size of 256X256. All the image processing tasks have been performed through ImageJ (Version 1.44) [11]. The gray stack of the slices of the dorsal, ventral and dorsal-ventral combined images have been prepared for further feature extraction using Gray Level Co-occurrence Matrix and statistical techniques [11] in a batch processing mode in ImageJ.

C. Generation of texture features

For batch processing, the gray stacks of the slices of the leaf images are processed through the texture extraction techniques given by Haralick [1] which provides the probability of gray level i occurring in the neighborhood of gray level j given distance d and angle Θ and total number of gray levels N (in the present case 256). The gray level co-occurrence matrix GM can be expressed mathematically as follows:

$$GM = \Pr(i, j \mid d, \theta, N) \tag{1}$$

In order to reduce the complexity, the inter pixel distance d is kept unity. Normally, in the case of Gray level co-occurrence matrix based methods, the calculations for feature extraction are carried out at unit pixel distance with Θ =0° and 45°, but this work has gone further in extracting the image texture features for the dorsal and ventral sides of the leaf images using Gray level co-occurrence matrix based method at unit pixel distance with angular pixel positions at Θ =0°, 45°, 90° and 135° independently and then combining them together using ImageJ software. The remaining angular positions of 225°, 270° and 315° are just the mirror images, therefore not considered.

Haralick [1], has described 14 texture properties out of which, the study uses the following 11 texture properties: Angular Second Moment(TF_1), Inverse Difference

Moment(TF_2), Contrast(TF_3), Energy(TF_4), Entropy(TF_5), Homogeneity(TF_6), Variance(TF_7), Shade(TF_8), Prominence(TF_9), Inertia(TF_{10}), Correlation(TF_{11}) [1,11,23] for preparing the texture feature values at different angular values of Θ for dorsal, ventral and dorsal-ventral combined leaf images.

The texture features dataset at the angular pixel position Θ is represented in the following manner:

$$TFD_\theta = \left(TF_1, TF_2, ..., TF_{11}\right)_\theta \quad (2)$$

Here $TF_1, TF_2, ..., TF_{11}$ indicate that all the 11 different values of texture features (mentioned above) measured at a particular value of Θ which is one of the values 0°, 45°, 90° and 135°.

The following three texture feature datasets have been prepared in this study: Image Texture Dorsal Dataset (ITDD), Image Texture Ventral Dataset (ITVD) and Combined Image Texture Dorsal-Ventral Dataset (CITDVD) using the equations (3), (4) and (5) respectively.

$$ITDD = \left\{TFD_{0^0}, TFD_{45^0}, TFD_{90^0}, TFD_{135^0}\right\}_{Dorsal} \quad (3)$$

$$ITVD = \left\{TFD_{0^0}, TFD_{45^0}, TFD_{90^0}, TFD_{135^0}\right\}_{Ventral} \quad (4)$$

$$CITDVD = \left\{TFD_{0^0}, TFD_{45^0}, TFD_{90^0}, TFD_{135^0}\right\}_{Dorsal\&Ventral} \quad (5)$$

D. Generation of statistical features

The 10 statistical features extracted from the leaf image dataset are Mean Gray value(SF_1), Median value(SF_2), Integrated Density(SF_3), Standard Deviation(SF_4), Minimum value(SF_5), XM(SF_6), YM(SF_7), Skewness(SF_8), Kurtosis(SF_9), Raw Integrated Density(SF_{10}).

The scale of calibration has been set to millimeter (mm). The statistical features datasets have also been prepared using ImageJ software [11].

The statistical features dataset is represented in the following manner:

$$SFD = \left\{SF_1, SF_2, ..., SF_{10}\right\} \quad (6)$$

Here $SF_1, SF_2, ..., SF_{10}$ indicate that all the 10 different values of statistical features (mentioned above).

The following three statistical feature datasets have been prepared: Image Statistical Dorsal Dataset (ISDD), Image Statistical Ventral Dataset (ISVD) and Combined Image Statistical Dorsal-Ventral Dataset (CISDVD) using the equations (7), (8) and (9) respectively:

$$ISDD = SFD_{Dorsal} \quad (7)$$

$$ISVD = SFD_{Ventral} \quad (8)$$

$$CISDVD = SFD_{Dorsal\&Ventral} \quad (9)$$

E. Feature Selection process in different data sets

Feature selection process involves selecting those features in the data set that are most useful and in simpler words most relevant and which shall provide better predictive accuracy and remove redundancy from the dataset. In addition to that, feature selection process also provides better understanding of the features.

In this study for the feature selection process, following seven feature selection algorithms have been used: Best First Search (BFS), Correlation Based Feature Selection (CFS), Chi-square (Chisq), OneR, Randomforest (RForest), ReliefF and Hill Climbing (HC). In addition to this one more method which includes all the features extracted from the image set i.e. No Feature Selection Algorithm (No Algo. Used) has also been used.

The algorithms mentioned above have been applied on the texture feature data sets: ITDD, ITVD, CITDVD and statistical feature data sets: ISDD, ISVD, CISDVD which generates a total of 48 different data sets comprising of 24 texture based and 24 statistical based data sets. The Tables I, II and III describe the number and names of texture features selected by each of the feature selection algorithm used in the present analysis. Similar results are given in Tables IV, V and VI for the statistical features.

TABLE I. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON ITDD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	4	TF_1, TF_5, TF_7, TF_8
2	CFS	4	TF_1, TF_3, TF_6, TF_7
3	Chisq	5	TF_7, TF_2, TF_9, TF_3, TF_{10}
4	OneR	5	TF_1, TF_4, TF_5, TF_6, TF_2
5	RForest	5	TF_9, TF_8, TF_7, TF_5, TF_{11}
6	ReliefF	2	TF_3, TF_{10}
7	HC	5	TF_1, TF_4, TF_5, TF_7, TF_8
8	No Algo. Used	11	TF_1, ..., TF_{11}

TABLE II. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON ITVD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	4	TF_1, TF_6, TF_7 ,TF_8
2	CFS	6	TF_2, TF_3,TF_5, TF_6, TF_7, TF_9
3	Chisq	3	TF_9, TF_5, TF_6
4	OneR	5	TF_7, TF_6, TF_2, TF_5 , TF_{11}
5	RForest	5	TF_9, TF_8, TF_7, TF_5 TF_{11}
6	ReliefF	2	TF_2,TF_1
7	HC	4	TF_2, TF_6, TF_9 , TF_{11}
8	No Algo. Used	11	TF_1, ..., TF_{11}

F. Application of classification algorithms

To discriminate the features obtained in section 2.5 into various classes (using 48 different data sets), the following six classification algorithms have been used: K-Nearest Neighbor (KNN), J48, Naïve Bayes, Partial Least Square (PLS), Classification and Regression Trees (CART), Classification Tree (CT) using "caret" package under RStudio [15]. Each data set was split into two groups (Training and Test sets) in the ratio 75:25. The training data set contains the class labels, whereas the testing dataset does not contain the class labels.

The preprocessing of the data involved centering and the scaling of the data matrix. In the classification procedure, a 10-fold cross validation technique has been applied which is repeated three times for validating any predictive model. Predictive accuracy and kappa values have been adopted as a measurable parameter for the classification process. Kappa is defined as the degree of right predictions of a model. This is originally a measure of agreement between two classifiers and is calculated as:

$$\kappa = \frac{\Pr(a) - \Pr(e)}{1 - \Pr(e)} \tag{10}$$

In broad terms a kappa below 0.2 indicates poor agreement and a kappa above 0.8 indicates very good agreement or beyond chance [17, 18].

TABLE III. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON CITDVD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	8	TF_3, TF_4, TF_5, TF_6, TF_8, TF_9, TF_{10}, TF_{11}
2	CFS	4	TF_1, TF_3, TF_6, TF_7
3	Chisq	5	TF_7, TF_5, TF_8, TF_6, TF_7
4	OneR	5	TF_1, TF_4, TF_5, TF_6, TF_3
5	RForest	5	TF_9, TF_8, TF_7, TF_5, TF_{11}
6	ReliefF	2	TF_6, TF_2
7	HC	8	TF_1, TF_3, TF_5, TF_6, TF_7, TF_8, TF_9, TF_{11}
8	No Algo. Used	11	$TF_{1,\ldots\ldots\ldots,}TF_{11}$

TABLE IV. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON ISDD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	3	SF_5, SF_7, SF_{10}
2	CFS	4	SF_5, SF_6, SF_7, SF_1
3	Chisq	5	SF_7, SF_6, SF_1, SF_3, SF_{10}
4	OneR	5	SF_4, SF_1, SF_3, SF_{10}, SF_8
5	RForest	5	SF_7, SF_5, SF_6, SF_4,SF_{10}
6	ReliefF	2	SF_7, SF_5
7	HC	5	SF_4, SF_5, SF_6, SF_7, SF_3
8	No Algo. Used	10	SF_1,………….., SF_{10}

TABLE V. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON ISVD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	4	SF_4 , SF_5 , SF_7 , SF_9
2	CFS	6	SF_1 , SF_4 , SF_5 , SF_6 , SF_7, SF_8
3	Chisq	3	SF_7 , SF_8 , SF_1
4	OneR	5	SF_9 , SF_8 , SF_1 , SF_3 , SF_{10}
5	RForest	5	SF_7 , SF_5 , SF_4 , SF_6 , SF_8
6	ReliefF	2	SF_7 , SF_6
7	HC	7	SF_1 , SF_4 , SF_6 , SF_7 ,SF_3 , SF_2 , SF_{10}
8	No Algo. Used	10	SF_1,………….., SF_{10}

TABLE VI. FEATURE SELECTION ALGORITHM AND FEATURES SELECTED ON CISDVD

S. No.	Feature Selection Algorithm	No. of Features Extracted	Name of the Features Extracted
1	BFS	5	SF_4, SF_5, SF_6, SF_7, SF_9
2	CFS	4	SF_5, SF_6, SF_7, SF_8
3	Chisq	5	SF_7, SF_8, SF_6, SF_5, SF_4
4	OneR	5	SF_4, SF_8, SF_2, SF_7, SF_9
5	RForest	5	SF_7, SF_5, SF_6, SF_4, SF_9
6	ReliefF	2	SF_7, SF_5
7	HC	7	SF_1, SF_5, SF_6, SF_7, SF_3, SF_2, SF_9
8	No Algo. Used	10	SF_1,………….., SF_{10}

TABLE VII. CLASSIFICATION ACCURACY FOR ITDD

Classification Algorithms	Feature Selection Algorithms								
	BFS	*CFS*	*Chisq*	*OneR*	*RForest*	*ReliefF*	*HC*	*No Algo. Used*	*Average Accuracy Across*
KNN	93.11	84.29	84.88	85.07	91.96	61.29	93.62	86.14	85.05
J48	96.00	90.92	91.00	87.25	94.00	59.96	95.18	93.55	88.48
Naïve Bayes	73.03	76.77	78.74	61.70	76.37	59.59	71.11	77.77	71.89
PLS	73.55	71.55	71.74	75.07	71.92	54.44	77.85	88.55	73.08
CART	89.85	85.48	86.25	81.03	87.51	61.81	90.37	88.11	83.80
CT	91.00	82.77	84.59	80.96	87.81	59.92	90.55	86.51	83.01
Average	86.09	81.96	82.87	78.51	84.93	59.50	86.45	86.77	80.89

TABLE VIII. CLASSIFICATION ACCURACY FOR ITVD

Classification Algorithms	Feature Selection Algorithms								
	BFS	*CFS*	*Chisq*	*OneR*	*RForest*	*ReliefF*	*HC*	*No Algo. Used*	*Average Accuracy Across*
KNN	93.81	85.22	90.51	83.92	95.37	76.74	87.88	85.66	87.39
J48	97.18	94.77	95.07	93.37	95.88	80.22	94.85	95.29	93.33
Naïve Bayes	74.74	78.03	69.67	73.81	76.00	62.66	74.48	79.88	73.66
PLS	71.14	84.14	63.14	81.55	64.62	58.22	69.00	89.88	72.71
CART	93.22	90.40	90.07	87.66	89.07	76.59	90.18	90.18	88.42
CT	86.37	87.18	85.88	80.92	90.85	76.44	86.81	89.03	85.44
Average	86.08	86.62	82.39	83.54	85.30	71.81	83.87	88.32	83.49

TABLE IX. CLASSIFICATION ACCURACY FOR CITDVD

Classification Algorithms	Feature Selection Algorithms								
	BFS	*CFS*	*Chisq*	*OneR*	*RForest*	*ReliefF*	*HC*	*No Algo. Used*	*Average Accuracy Across*
KNN	84.35	80.16	90.39	82.18	81.61	66.90	83.77	84.27	81.70
J48	94.37	90.85	93.87	88.42	94.42	66.77	94.25	94.85	89.73
Naïve Bayes	75.96	72.12	70.20	69.92	76.64	60.25	75.50	75.16	71.97
PLS	83.20	69.11	79.44	76.92	70.90	59.68	85.18	85.20	76.20
CART	89.37	83.83	86.81	82.27	87.62	66.74	86.96	89.70	84.16
CT	85.92	81.75	87.27	81.5	84.90	66.66	85.64	86.70	82.54
Average	85.53	79.64	84.66	80.20	82.68	64.50	85.22	85.98	81.05

III. RESULTS AND DISCUSSION

The quantitative results, obtained by following the methodology proposed in Section II, for the predictive accuracy for texture feature data sets: ITDD, ITVD, CITDVD and statistical feature data sets: ISDD, ISVD, CISDVD are given in Tables VII, VIII, IX and Tables X, XI, XII respectively. However the pictorial representations of the kappa values for ITDD, ITVD, CITDVD texture feature data sets and ISDD, ISVD, CISDVD statistical feature data sets have been represented in Fig. 2((a),(b),(c)) and 3((a),(b),(c)) respectively.

TABLE X. CLASSIFICATION ACCURACY FOR ISDD

Classification Algorithms	Feature Selection Algorithms								
	BFS	***CFS***	***Chisq***	***OneR***	***RForest***	***ReliefF***	***HC***	***No Algo. Used***	***Average Accuracy Across***
KNN	89.47	95.13	86.51	68.54	93.48	87.35	93.48	90.15	88.01
J48	89.88	92.16	85.91	72.99	91.86	86.31	91.86	92.04	87.88
Naïve Bayes	88.03	94.80	83.80	58.97	94.64	83.29	94.64	90.33	86.06
PLS	87.09	93.06	84.75	65.42	92.39	64.73	92.39	93.61	84.18
CART	92.58	90.20	83.57	53.91	89.31	90.45	89.31	89.06	84.80
CT	92.39	99.00	85.62	70.89	90.10	87.92	90.10	89.50	88.19
Average	89.91	94.06	85.03	65.12	91.96	83.34	91.96	90.78	86.52

TABLE XI. CLASSIFICATION ACCURACY FOR ISVD

Classification Algorithms	Feature Selection Algorithms								
	BFS	***CFS***	***Chisq***	***OneR***	***RForest***	***ReliefF***	***HC***	***No Algo. Used***	***Average Accuracy Across***
KNN	85.54	87.72	84.53	70.79	88.87	80.58	79.19	85.13	82.79
J48	87.24	85.02	79.52	72.07	87.25	82.45	86.52	87.49	83.45
Naïve Bayes	83.06	84.93	79.68	53.39	87.96	78.84	78.60	82.86	78.67
PLS	73.69	79.77	75.00	53.17	80.09	61.77	76.31	84.95	73.09
CART	87.08	85.28	79.95	65.00	85.65	79.40	83.99	86.07	81.55
CT	83.28	85.98	75.91	58.67	84.85	81.28	84.17	85.83	80.00
Average	83.32	84.78	79.10	62.18	85.78	77.39	81.46	85.39	79.92

TABLE XII. CLASSIFICATION ACCURACY FOR CISDVD

Classification Algorithms	Feature Selection Algorithms								
	BFS	***CFS***	***Chisq***	***OneR***	***RForest***	***ReliefF***	***HC***	***No Algo. Used***	***Average Accuracy Across***
KNN	91.40	89.11	91.77	81.48	91.40	77.55	89.037	88.22	87.50
J48	89.40	86.37	89.48	80.44	89.40	76.44	86.518	89.11	85.89
Naïve Bayes	89.62	84.59	88.29	79.25	89.62	77.92	85.55	84.88	84.97
PLS	87.03	83.18	85.7	71.55	87.03	63.55	86.81	87.40	81.53
CART	85.48	86.29	86.81	78.00	85.48	63.03	83.037	85.77	81.74
CT	84.37	83.40	86.00	78.29	84.37	78.14	82.29	84.00	82.61
Average	87.88	85.49	88.01	78.17	87.88	72.77	85.54	86.56	84.04

A. Analysis on the basis of Texture feature data sets

It has been observed from the values for predictive accuracy for the texture feature dataset, the ITVD feature data model has the highest value for the average predictive accuracy (83.49%) amongst all the texture based data models (CITDVD(81.05%),ITDD(80.89%)) studied in this work. The comparison of the present results with the results of [9] are not directly comparable due to the differences in the datasets used. Despite of this fact this work compares its results with the results of [9]. In [9] two classification algorithms Neuro Fuzzy Controller(NFC) and Multi-Layer Perceptron(MLP) have been used for the texture based model with only dorsal side images and the average predictive accuracy achieved is 81.6% and 87% respectively. In the proposed ITVD model, ventral based texture feature model provides average predictive accuracy value of 83.49% and J48 classification algorithm gives 97.18% accuracy value using Best First Search(BFS) algorithm for feature selection, which is comparable with the results of [9] as shown in the Fig. 4.

While observing the accuracy values for texture feature based models, ITDD model provides accuracy value of 96% using Best First Search(BFS) algorithm for feature selection applied to dorsal leaf images and J48 as the classification algorithm. When CITDVD model is used, an accuracy value of 94.85% for J48 algorithm has been observed when all the textures features are used (No feature selection algo. used) as shown in the Tables VII, VIII and IX. On comparing results with textures segmentation model [19], which used Brodatz album (each image size 256 X 256) prepared the gray level co-occurrence matrix at unit pixel distance with angular pixel positions at $\Theta = 0°$, 45, has achieved predictive accuracy as high as 90% (approx.). However this work has prepared the gray level co-occurrence matrix at unit pixel distance with angular pixel positions at $\Theta = 0°$, 45°, 90° and 135° and have achieved better predictive accuracy in all the texture based (ITDD, ITVD, CITDVD) models as shown in Table XIII.

B. Analysis on the basis of Statistical feature data Sets

On observing the values for predictive accuracy for the statistical feature model, the ISDD feature model has the highest value for the average predictive accuracy (86.52%) amongst all the statistical based feature data models (CISDVD(84.04%), ISVD(79.92%)) studied in this work, as shown in the Fig. 4.

On comparing the results for statistical based feature models proposed in this work with [9], which is based on the dorsal based image sets only, two of the proposed statistical based feature models (ISDD and CISDVD) have fared better by giving more values for average predictive accuracy. Now, on comparing the texture based (ITDD, ITVD, CITDVD) and statistical based feature models (ISDD, ISVD, CISDVD) proposed in this work, the statistical based model ISDD fares the best amongst all the models proposed in this work in achieving the average predictive accuracy, as shown in the Fig. 5. While observing the classification using statistical features, by using K-Nearest Neighbor algorithm with correlation based feature selection algorithm has given the highest accuracy value of 95.13%. The ISVD model has achieved highest accuracy value of 88.87% with K-Nearest Neighbor algorithm with Random Forest based feature selection algorithm. On combining the dorsal and ventral images together and it has been observed that the predictive accuracy achieved is 91.77% with K-Nearest Neighbor algorithm with chi-square as the feature selection algorithm as shown in the Tables X, XI and XII.

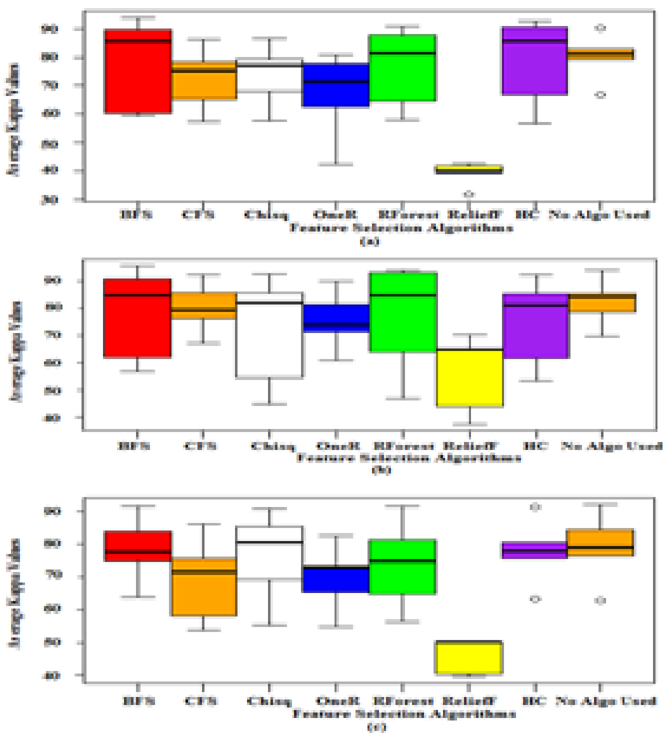


Fig. 2. Average kappa values versus feature selection algorithms for (a)ITDD (b) ITVD (c) CITDVD respectively

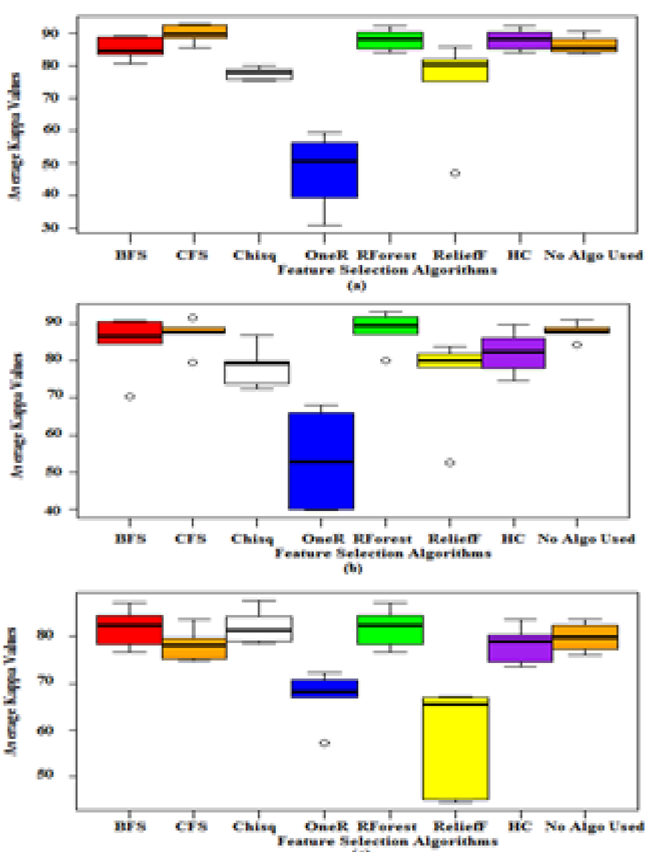


Fig. 3. Average kappa values versus feature selection algorithms for (a) ISDD (b) ISVD (c) CISDVD respectively

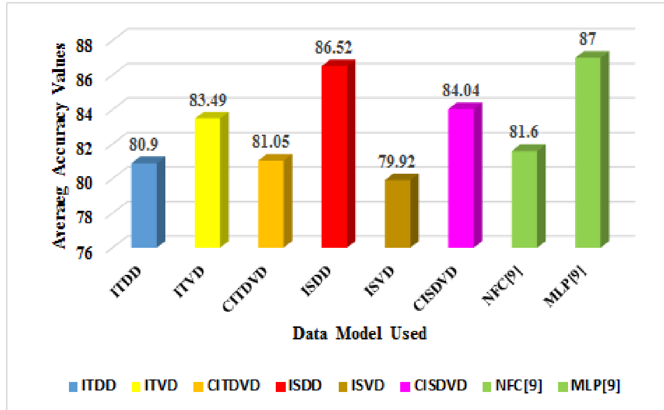


Fig. 4. Comparison of average accuracy of different data models with [9]

TABLE XIII. SUMMARY CHART FOR THE COMPLETE WORK CARRIED OUT

Model Type	**Model Name**	**Average Predictive Accuracy (%)**	**Best Classification Algorithm on the basis of Predictive Accuracy Values**	**Feature Selection Algorithm used**	**Number of Features Used**	**Predictive Accuracy Values for Best Classification Algorithm (%)**
Dorsal Leaf Image Models	ITDD	80.89	J48	BFS	4	96
	ISDD	86.52	KNN	CFS	4	95.13
Ventral Leaf Image Model	ITVD	83.49	J48	BFS	4	97.18
	ISVD	79.92	KNN	RForest	5	88.87
Combined Dorsal& Ventral Leaf Image Model	CITDVD	81.05	J48	No Algo. Used	11	94.85
	CISDVD	84.04	KNN	CFS	4	91.77

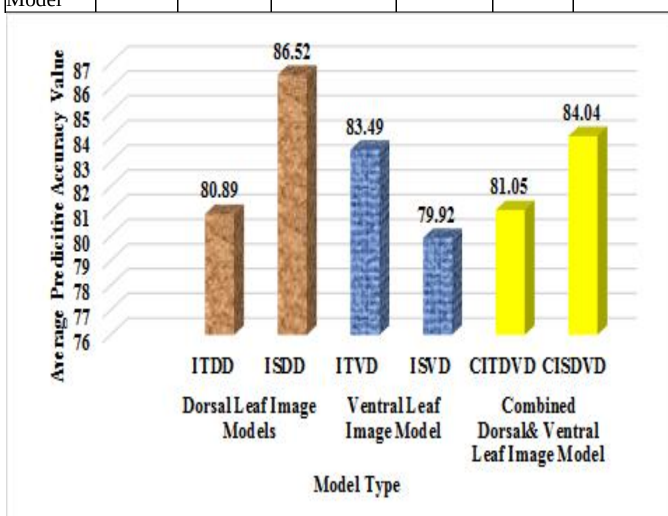


Fig. 5. Comparison of average predictive accuracy of different data models

C. Analysis on the basis of number of texture features used and the Average Misclassification results

In ITDD based models, when features are selected using Hill Climb algorithm (5 features selected) the average misclassification rate is the 13.55% and when no feature selection algorithm is used (all the 11 features used), the average misclassification rate is the 13.23% as shown in the Fig. 6(a). In ITVD based model, when the features are selected using Correlation based feature selection algorithm (6 features selected), the average misclassification rate is the 13.88%, and when no feature selection algorithm is used (all the 11 features used), the average misclassification rate is the 11.68% as shown in the Fig. 6(b). In CITDVD based model, when the features are selected using Best First Search algorithm (8 features selected) the average misclassification rate is the 14.47%, and when no feature selection algorithm is used (all the 11 features used), the average misclassification rate is the 14.02% as shown in the Fig. 6(c).

D. *Analysis on the basis of number of statistical features used and the Average Misclassification results*

In ISDD based models, when features are selected using Correlation based algorithm (4 features selected) , the average misclassification rate is the 5.94% and when Hill Climb and Random Forest based algorithms are used with 5 features, the average misclassification rate is the 8.04% as shown in the Fig. 7(a). In ISVD based model, when the features are selected using Random Forest algorithm (5 features selected), the average misclassification rate is the 14.22%, as shown in the Fig. 7(b). In CISDVD based model, when the features are selected using Chi-square (5 features selected) the average misclassification rate is the 11.59%, as shown in the Fig. 7(c).

E. *Analysis on the basis of Number of features selected for classification*

On comparing the results of this work with the [19, 20] as shown in Fig. 8, [19] has the highest predictive accuracy of 90% with 32 features and the highest predictive accuracy achieved is 93.29% for 10 features on Lung Cancer Data [20], whereas in the present study, when 10 features are used, the accuracy achieved is 95.13% using Correlation based feature selection (CFS) for ISDD based model. In the case of ISDD model proposed in this study has achieved the highest accuracy values for 10 features.

The feature selection and misclassification method is not directly comparable due to different datasets used, but with the 10 features selection as the criteria for classification, this work has compared its results with [19,20].

F. *Analysis on the basis of dorsal and ventral features*

The summary of the results, presented quantitatively in Table XIII and graphically in Fig. 5, clearly demonstrate the supremacy of ventral features over the dorsal features. The highest predictive accuracy (97.18%) is achievable through classification algorithm J48 using Best First Search algorithm applied over texture features obtained from ventral side leaf images. The statistical features are giving the best average predictive accuracy (86.52%) amongst all the models proposed in this work.

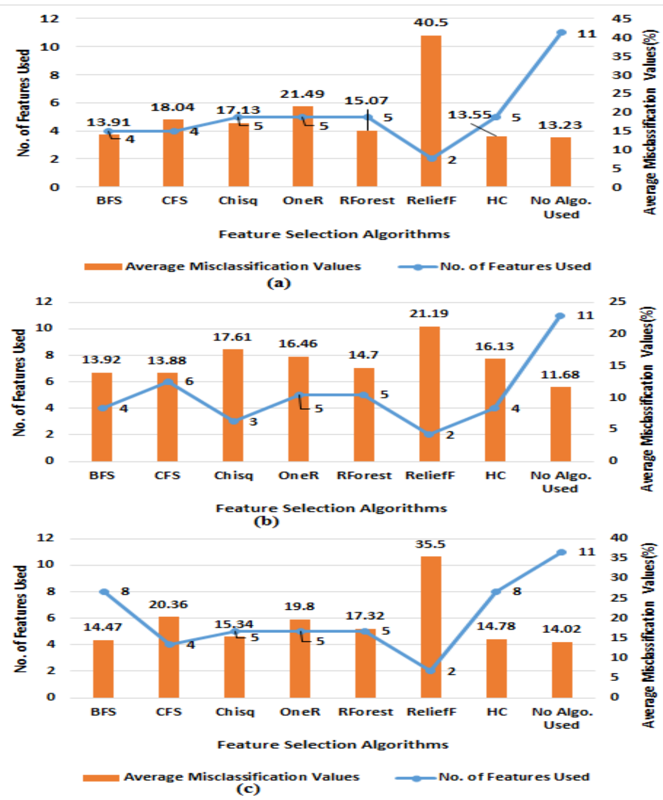


Fig. 6. Average misclassification rate vs. no. of features selected using (a) ITDD (b) ITVD (c) CITDVD respectively

IV. CONCLUSIONS

This paper proposes to utilize the concept of striking features present on both the dorsal and the ventral sides of the leaves and has been modeled around texture and statistical features for dorsal, ventral and dorsal-ventral leaf images. It has been observed that the texture based model, the ITVD model, is giving better average predictive accuracy as compared to other texture based models. This strengthens the proposition of this work that ventral sides of leaf images can be another alternative for extracting and discriminating features. Based on the results of all the statistical feature based models, it is inferred that the ISDD model is the best amongst all the texture and statistical based models used in this work.

The statistical feature set is providing much better predictive accuracy as compared to the models with texture based feature sets owing to the fact that the mutual information (MI) which is based on entropy, provided by the two or more random variables in the dataset is more in the case of statistical feature sets as compared to the texture based feature sets. Based on the extensive analysis, performed in this work, it is proposed that the statistical model (ISDD) which is purely based on calculating the statistical feature values can be applied for studying any object of interest with dorsal side of the image.

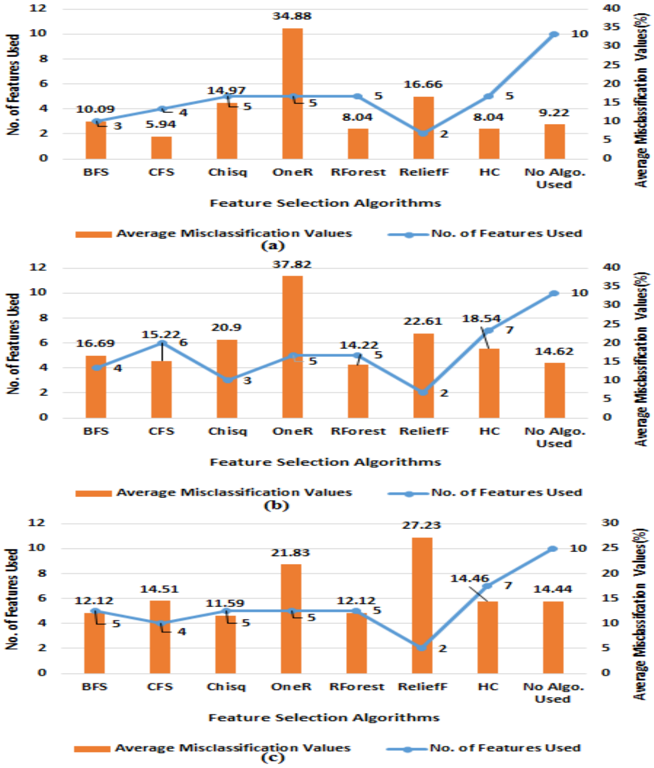


Fig. 7. Average misclassification rate versus no. of features selected using (a) ISDD (b) ISVD (c) CISDVD respectively

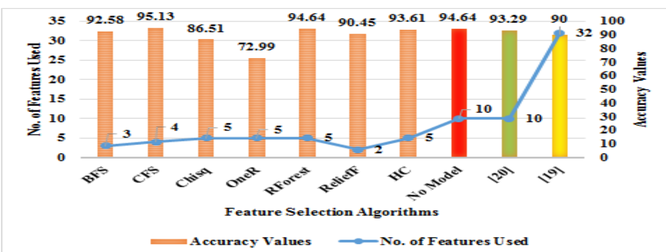


Fig. 8. Comparison of accuracy values versus no. of features used in ISDD with [19, 20]

REFERENCES

[1] Robert M Haralick et al., “Texture features for image classiifcation”, IEEE Transactions on Systems, Man and Cybernetics, Vol. 3, No. 6, pp. 610-621, 1973.

[2] Rosenfeld, E. Troy, “Visual texture analysis”, Computer Sci. Cent., University of MaryLand, College Park, Technical Report, pp. 70-116, 1970.

[3] G. Castellano et al., “Texture analysis of medical images”, Clinical Radiology, Vol. 59, pp. 1061–1069, 2004.

[4] M.S. Oliveira et al., “Texture analysis of computed tomography images of acute ischemic stroke patients”, Braz. J. Med. Biol. Research, Vol. 42, No. 11, pp. 1076-1079, 2009.

[5] Igor Pantic et al., “ Nuclear entropy, angular second moment, variance and texture correlation of thymus cortical and medullar lymphocytes: Gray level co-occurrence matrix analysis”, Annals of the Brazilian Academy of Sciences, Vol. 85, No. 3, pp. 1063-1072, 2012.

[6] Fongaro L. et al., “Assesment of surface aspects of foods using ImageJ plugins”, In proceedings of the ImageJ User and Developer Conference, Luxembourg: Centre de Recherche Public Henri Tudor, ISBN: 2-919941-18-6, pp. 245-248, 2012.

[7] Lorenzo Fongaro, Knut Kvaal, “Surface texture characterization of an Italian pasta by means of univariate and multivariate feature extraction from their texture images”, Food Research International, Vol. 51, No. 2, pp. 693-705, 2013.

[8] Cem Kalyoncu, Onsen Toygar, “Geometric leaf classification”, Computer Vision and Image Understanding, Vol. 133, pp. 102-109, 2015.

[9] Jyotismita chaki et al., “Plant leaf recognition using texture and shape features with neural classifier”, Pattern Recognition Letter, Vol. 58, pp. 61-68, 2015.

[10] A.J. Perez et al., “Color and shape analysis techniques for weed detection in cereal fields”, Comput. Electron. Agric. Vol. 25, pp. 197-212, 2000.

[11] Rasband, W.S., ImageJ, 1997-2014, U. S. National Institutes of Health, Bethesda, Maryland, USA.

[12] http://imagej.nih.gov/ij/http://www.vision.caltech.edu/Image_Datasets /leaves/leaves.tar (Web page last visited on Aug., 2015)

[13] Database from Oxford, http://www.plant-phenotyping.org/ CVPPP2014-dataset, (Web page last visited on Aug., 2015)

[14] https://archive.ics.uci.edu/ml/machine-learning-databases/00288/leaf.zip ,(Web page last visited on Aug., 2015)

[15] R Development Core Team, R:A language and environment for statistical computing, R Foundation for Statistical Computing, Vienna, Austria. ISBN 3-900051-07-0., 2008.

[16] Piotr Romanski, FSelector: Selecting attributes. R package version 0.19, 2013, http://CRAN.R-project.org/package=FSelector

[17] Anthony J. Viera, Joanne M. Garrett, “Understanding interobserver agreement:The Kappa statistic”, Family Medicine, Vol. 37, No. 5, pp. 360-363, 2015.

[18] Julius Sim , Chris C Wright, “The Kappa statistic in reliability studies: use, interpretation, and sample size requirements”, Physical Therapy, Vol. 85, No. 3, pp. 257-268, 2005.

[19] Andrik Rampun et al., “Texture segmentation using different orientations of GLCM features”, Mirage 6th International Conference on Computer Vision / Computer Graphics Collaboration Techniques and Applications, 2013.

[20] Matthew Shardlow, “An analysis of feature selection techniques”, https://studentnet.cs.manchester.ac.uk/pgt/COMP61011/goodProjects/Shardlow.pdf (Web Pages last visited on May 5, 2015).

Electrooculogram Signals Analysis for Process Control Operator Based on Fuzzy c-Means

Jiangwen Song
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

Chaoxing Xiong
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

Raofen Wang*
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

Leyan Zhang
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

Guanghua Zhang
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

Cunbang Sun
School of Electronic and Electrical Engineering
Shanghai University of Engineering Science
Shanghai, China, 201620

***Abstract*—Biomedical signals of human can reflect the body's task load, fatigue and other psychological information. Compared with other biomedical signals, electrooculogram (EOG) has higher amplitude, less interference, and is easy to detect. In this paper, the EOG signals of operator's were analyzed. Wavelet transform was used to remove the high-frequency artifacts. Then fuzzy c-means was adopted to detect the eye blink peak points of EOG. After that, eye blink interval (EBI) of operator was calculated. Four EOG features (the average of EBI, variance of EBI, standard deviation of EBI and variation coefficient of EBI) were extracted. Finally, the relationship between EOG features and operator's fatigue, effort, anxiety and task load were analyzed. The experimental results illustrate that EOG features had some relation to the operator's fatigue, effort, anxiety and task load respectively.**

Keywords—electrooculogram; fuzzy c-means; operator functional state; fatigue

I. Introduction

Fatigue is a natural physiological phenomenon, which is related to the operator's labor intensity, work environment, health, mood and so on. It is a kind of self-adjustment and protection function of human body. In recent years, with the rapid development of economy and the faster pace of life, many of the operators continue to work in the state of fatigue [1,2]. Consequently, many accidents occurred because of operator fatigue. And also the anxiety and effort level of the operators can affect their work performance. The operator's performance degradation may be the reason of some serious disasters, particularly in safety-critical applications. The assessment of operator mental workload would help predict the operator's periods of high operational risk. Early warning based on prediction of the operator's mental workload is one of the effective methods to prevent such accidents. Therefore, the accurate assessment of operator mental workload is the key to provide early warning successfully.

Current scientific research found that, the human body contains many types of biological signals which can reflect in parts the operator's fatigue, anxiety, mental workload, etc. [3-5] After comparing the characteristics of electroencephalogram (EEG), electrocardiogram (ECG) and electrooculogram (EOG), the authors analyzed EOG signals of operator's. Features of EOG signals contain eye blink rate, eye blink amplitude, closing time, eye blink variability, etc. [6] The researchers thought that EOG is associated with operator's mental workload because eye blink is associated with facial nerve and the awakening is associated with central nerve. When task load increases, the visual demand is likely to increase which may lead to eye blink rate decrease. Simultaneously, the eye activity may increase. When the operator focuses on the tasks, his/her eyes blink rate may decrease and the eye blink interval may increase [7,8]. In [9,10], the authors analyzed the driver's eye blink interval. It is illustrated that when the driver is fatigue, his/her eyelid ptosis arises, eye blink amplitude decreases. In other words eye blink interval decreases while closing time increases.

This paper is to investigate the EOG signals associated with the operator functional state (OFS), like fatigue, anxiety, effort and task load. The experimental environment of process control was designed, and the EOG signals of operators under multi-level of task loads were sampled. Fuzzy c-means (FCM) was adopted to detect the eye blink peak points of EOG. And then EOG features to assess the human fatigue, anxiety, effort and task load were found through the study of EOG. Thereby, these indices will be used to predict the functional state of the operator. Early warning system can be constructed to prevent accidents which are caused by human factors.

The rest of the paper is arranged as follows. Section 2 described the data acquisition experiment in details. In section 3, the Fuzzy c-means algorithm is presented. In section 4, the EOG signal analyzing process and results are illustrated, and the discussions are presented. Section 5 makes the conclusions and gives the future works.

II. Experiment

A. Data Acquisition

The experiments were carried out on Automation-enhanced cabin air management system (AUTOCAMS), developed by Hockey and his colleagues [11] and modified by Lorenz [12]. AUTOCAMS simulates a life support system of a spacecraft. It requires the subject to manage a semi-automatic system which is to maintain comfortable atmospheric condition of the cabin. There are four sub-systems corresponding to four critical parameters of atmospheric condition (oxygen concentration, carbon dioxide concentration, temperature, pressure). The subject was instructed to control some of the sub-systems manually according to the experimental design.

Subjects were trained on the manual process control tasks for over 7 hours, followed by a further 5 hour experience of controlling the system under a range of conditions. After that, the subjects are regarded as the adept at operating AUTOCAMS. Three subjects (SA, SB, and SC) participated in this experiment.

The task of the subject was defined to control some of the four subsystems so as to maintain their relevant variables within target ranges. There are 8 control conditions (C1~C8) in the experiment. The first (C1) and last (C8) conditions are five minute baseline testing conditions in which the subjects' task was to monitor the operation of AUTOCAMS. The amount of manually controlled subsystems in other control conditions (C2~C7) is 1, 3, 4, 4, 3, 1, respectively and each condition lasts for 15 minutes. For an experimental session, the cyclic loading method resulted in a loading phase (C2~C4) and an unloading phase (C5~C7).

Every subject was required to do the experiment for three times (e.g. SA1, SA2, SA3) at the same time on different days to avoid circadian effect.

B. EOG Data

The subjects' vertical EOG signals were recorded by Nihon-Koden EEG 1100 physiological recorder from 2 sites, which are placed above and under the subject's right eye and referenced to linked earlobes. The EOG data were sampled at 500 Hz.

III. Methods

A. Fuzzy c-Means

Fuzzy c-means is a data clustering method in which each data point belongs to a cluster, with a degree specified by a membership grade [13-15]. FCM partitions a collection of *n* vectors $X = \{x_1, x_2, \cdots, x_n\}$, where $x_k = (x_{k1}, x_{k2}, \cdots, x_{ks})$ is the *k*th vector of *X*. FCM is based on minimizing an objective function, which respects to fuzzy membership '*U*', and set of cluster centroids, '*V*'. The FCM objective function can be described as,

$$\begin{cases} J_m(U,V) = \sum_{k=1}^{n}\sum_{i=1}^{c} \mu_{ik}{}^{m} d_{ik}{}^{2} \\ s.t. \quad \sum_{i=1}^{c} \mu_{ik} = 1;\ \mu_{ik} \in [0,1];\ 0 < \sum_{k=1}^{n} \mu_{ik} < n \end{cases} \tag{1}$$

where, '*c*' is the number of clusters. μ_{ik} is the membership function of vector x_k to the *i*th cluster. $d_{ik}{}^2 = \|x_k - v_i\|^2$ can be either Euclidean distance or one of its generalizations such as Mahalanobis distance. Euclidean distance is used in this study.

The steps of the FCM method are explained in brief:

- Firstly, the centers of each cluster $V(0)$, fuzzy coefficient '*m*', number of cluster '*c*' and termination threshold 'ε' are randomly selected.
- Secondly, the membership matrix $U^{(t)}$ is computed with the following equation:

$$\mu_{ik}(t) = 1 \Big/ \sum_{j=1}^{c} \left(d_{ik}(t) / d_{jk}(t) \right)^{2/m-1}. \tag{2}$$

- Thirdly, the *c*th cluster centroid is calculated with the following equation:

$$v_i(t+1) = \sum_{k=1}^{n} \mu_{ik}(t)^m x_k \Big/ \sum_{k=1}^{n} \mu_{ik}(t)^m. \tag{3}$$

- The process is stopped if $\|V^{(t+1)} - V^{(t)}\| < \varepsilon$.

In this paper, the FCM algorithm was used to separate EOG signals into 2 subsets, i.e. the higher amplitude subset and the lower amplitude subset. Then the eye blink peak of EOG can be identified.

IV. Results and Discussion

The process of EOG analysis is as follows:

1) Denoising. Wavelet Transform was used to remove the high frequency artifacts of EOG signal. The parameter settings of wavelet denoising method are: wavelet base: DB4, decomposition level: 3. Soft threshold denoising method and unbiased threshold estimation method was adopted.

2) Fuzzy c-means. The EOG signal was divided into two clusters. The eye blink peak was found in the higher amplitude cluster. Figure 1 shows the eye blink peak point of EOG signals. It can be seen that the proposed method can find the eye blink peak correctly. The eye blink peaks for all the EOG signals were detected by using the same method.

3) Feature extraction. The eye blink interval was calculated. Figure 2 shows the mean eye blink interval of 1 minute of SC2. The EBI tends to decrease (increase) when task load increase (decrease). For the purpose of analyzing the relation of EOG to OFS, four features of EBI, i.e. average of EBI (AEBI), variance of EBI (VEBI), standard deviation of EBI (SDEBI) and variation coefficient of EBI (VCEBI), were extracted. The value of each feature in each condition was calculated to observe its changes in the whole experiment. Figure 3-6 show the changes of these four features in the whole experiment of SC2. Figure 7 shows the number of subsystems under manual control and subjective measurements in eight control conditions of SC2, respectively.

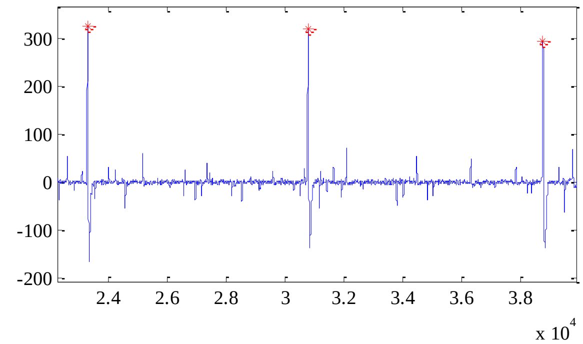


Fig. 1. The results of fuzzy c-means: line—EOG signal;*—eye blink peak point

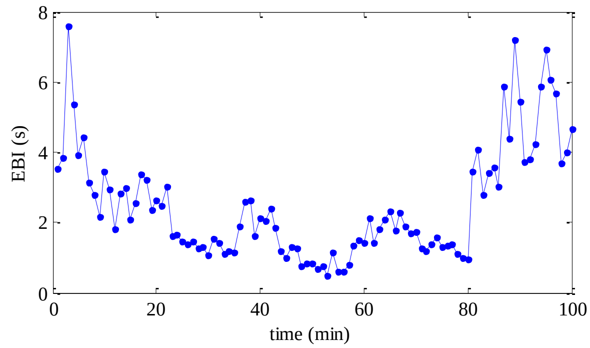


Fig. 2. EBI per minute

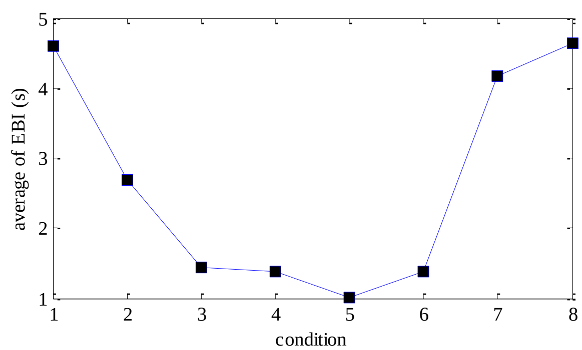


Fig. 3. Average of EBI

The average of EBI, variance of EBI and standard deviation of EBI decrease when the operator's task load increases from C1 to C4. And these features show the same changes when the operator's task load decrease from C5-C8. It is clear that the average of EBI, variance of EBI and standard deviation of EBI has a significant relation to operator's task load.

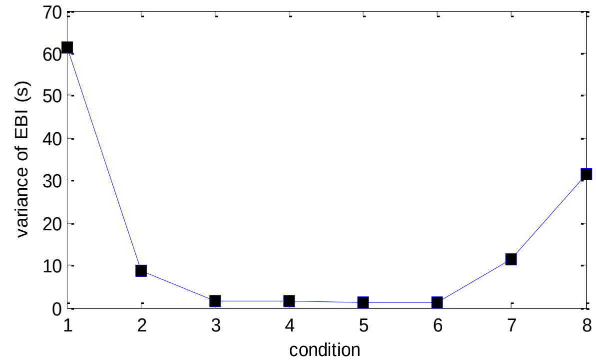


Fig. 4. Variance of EBI

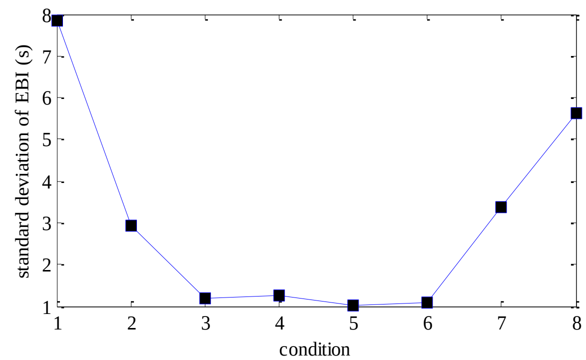


Fig. 5. Standard deviation of EBI

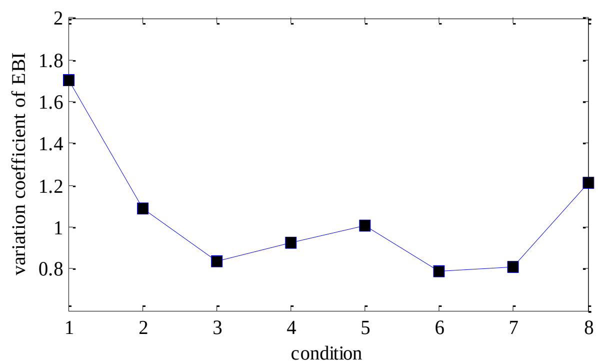


Fig. 6. Variation coefficient of EBI

The variation coefficient of EBI increases from C3-C5, which may be influenced by the operator's increasing effort and anxiety. In C1 and C8, AUTOCAMS runs automatically.

The operator was required to monitor the system. Thus there wasn't any task load for the operator. In C2-C7, the operator needs to control some of the subsystems. From all the four features, it could be seen that there are significant differences between no-load conditions (C1 and C8) and under load conditions (C2-C7). The difference of features between C1 and C8 may be caused by the subject's fatigue.

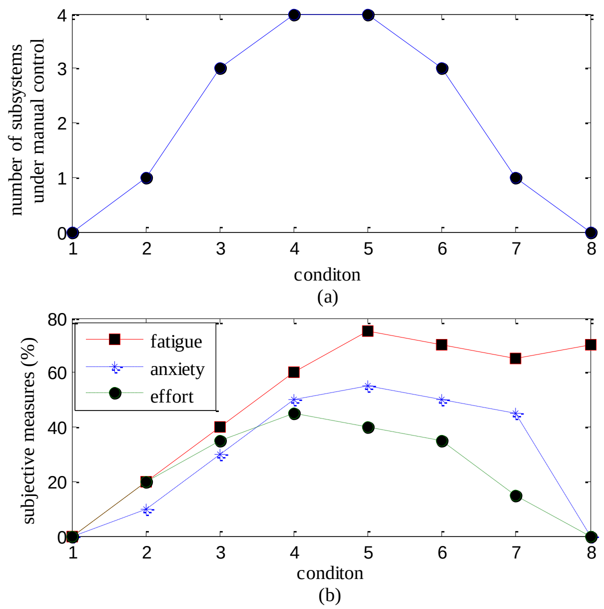


Fig. 7. The number of subsystems under manual control and subjective measurements

These finds indicate that the changes of task load and mental workload can be reflected by features of EOG. The correlative analysis is used to quantitatively analyze the relationship between EOG features and operator task load, anxiety, effort and fatigue. Table 1 shows the results of correlative analysis between EOG features and operator fatigue, anxiety, effort and task load of SC2. Operator's fatigue can be reflected by variation coefficient of EBI. All these four features can be indices of operator's anxiety. Average of EBI, variance of EBI and standard deviation of EBI have significant relations with operator's effort and task.

TABLE I. CORRELATION ANALYSIS BETWEEN EOG FEATURES AND OPERATOR FUNCTIONAL STATE

Operator Functional State	Average of EBI	Variance of EBI	Standard Deviation of EBI	Variation Coefficient of EBI
Fatigue	-0.34	-0.6	-0.56	-0.68
Anxiety	-0.72	-0.77	-0.82	-0.76
Effort	-0.97	-0.85	-0.93	-0.69
Task	-0.95	-0.78	-0.89	-0.62

TABLE II. SIGNIFICANT EOG FEATURES RELATED TO OPERATOR FUNCTIONAL STATE

No.	Fatigue	Anxiety	Effort	Task load
SA1		SDEBI, VCEBI	SDEBI, VCEBI	SDEBI, VCEBI
SA2		VEBI, SDEBI	SDEBI, VCEBI	VEBI, SDEBI
SA3		AEBI, SDEBI	AEBI, SDEBI	AEBI, SDEBI
SB1	VEBI, SDEBI	SDEBI, VCEBI		
SB2	AEBI,VEBI		AEBI	
SB3	VEBI, SDEBI	AEBI,VEBI		
SC1	VEBI,VCEBI	VEBI,VCEBI	VEBI,VCEBI	VEBI, SDEBI
SC2	VEBI,VCEBI	VEBI, SDEBI	AEBI, SDEBI	AEBI, SDEBI
SC3	VEBI,VCEBI	AEBI,VCEBI	AEBI,VCEBI	AEBI,VCEBI

The same analysis was done to the EOG signals for all the subjects. Table 2 shows the top 2 significant EOG features ($P<0.05$) for each subject. Variance of EBI is a good index of operator fatigue. Standard deviation of EBI can reflect the operator's anxiety, effort and task load. It could be seen that the salient features for different subjects are different owing to individual difference. For subject SA, standard deviation of EBI is a salient feature of operator anxiety, effort and task load. For subject SB, variance of EBI can significantly reflect the changes of operator fatigue. For subject SC, variance of EBI and variation coefficient of EBI are significant features of fatigue and anxiety. Average of EBI can reflect the changes of effort and task load.

V. CONCLUSION

This paper analyzed the EOG signal of operator. Fuzzy c-means was used to detect the eye blink peak of EOG. Average of EBI, variance of EBI, standard deviation of EBI and variation coefficient of EBI were extracted. The relation of EOG features and operators fatigue, anxiety, effort and task load was analyzed. Salient EOG features for each subject are successfully extracted. The experiment results show that it's necessary to assess the operator functional state using personal salient features. The results of this paper could be used to identify operator functional sate in future works. Future works will focus on two areas. First, the authors will do more experiments and further analysis on EOG, in order to evaluate the individual differences. Second, models that describe the relation between EOG features and operator functional state will be constructed.

ACKNOWLEDGMENTS

This work is partially supported by the Shanghai University Young Teachers' Training Scheme Funds ZZGJD12011, the National Nature Science Foundation under Grant No. 61403249 and No. 61403248.

REFERENCES

[1] G. Borghini, L. Astolfi, G. Vecchiato, D. Mattia, F. Babiloni, "Measuring neurophysiological signals in aircraft pilots and car drivers for the assessment of mental workload, fatigue and drowsiness", Neurosci. Biobehav. R. Kidlington, vol. 44, pp. 58-75, July 2014.

[2] R. Wang, J. Zhang, Y. Zhang, X. Wang, "Assessment of human operator functional state using a novel differential evolution optimization based adaptive fuzzy model", Biomed. Signal Process. Control, Kidlington, vol. 7, pp. 490-498, September 2012.

[3] K. L. Saroj, C. Ashley, "Driver fatigue : electroencephalography and psychological assessment", Psychophysiol. Malden MA, vol. 39, pp. 313-321, May 2002.

[4] I. Kathner, S. C. Wriessnegger, G. R. Muller-Putz, A. Kubler, S. Halder, "Effects of mental workload and fatigue on the P300, alpha and theta band power during operation of an ERP (P300) brain–computer interface", Biol. Psychol. Amsterdam, vol. 102, pp. 118-129, October 2014.

[5] S. Rodriguez-Ruiz, P. M. Guerra, S. Moreno, M. Carmen Fernandez, J. Vila, "Heart rate variability modulates eye-blink startle in women with bulimic symptoms", J. Psychophysiol. Gottingen, vol. 26, pp. 10-19, October 2012.

[6] H. A. Slagter, K. Georgopoulou, M. J. Frank, "Spontaneous eye blink rate predicts learning from negative, but not positive, outcomes", Neuropsychologia, Kidlington, vol. 71, pp. 126-132, May 2015.

[7] M. J. Doughty, "Further assessment of gender- and blink patternrelated differences in the spontaneous eyeblink activity in primary gaze in

young adult humans", Optometry Vision Sci. Philadelphia, vol. 79, pp. 439-447, July 2002.

[8] P. L. Kaufman, A. ALM, "Adler's physiology of the eye", 10th ed. St. Louis: Mosby, 2003.

[9] M. A. Recarte, L. M. Nunes, "Mental workload while driving: effects on visual search, discrimination, and decision making", J. Exp. Psychol. Appl. Washington, vol. 9, no. 2, pp. 119-137, June 2003.

[10] M. Boyer, M. L. Cummings, L. B. Spence, E. T. Solovey, "Investigating mental workload changes in a long duration supervisory control task", Interact. Comput. Oxford, May 2015.

[11] G. R. J. Hockey, D. G. Wastell, J. Sauer, "Effects of sleep deprivation and user-interface on complex performance: a multilevel analysis of compensatory control", Human Factors. vol. 40, no. 2, pp. 233-253, June 1998.

[12] B. Lorenz, F. DiNocera, S. Rottger, R. Parasuraman, "Automated fault-management in a simulated spaceflight micro-world", Aviat. Space Environ. Med. Washington, vol. 73, 886-897, September 2002.

[13] J.C. Bezdek, "Pattern recognition with fuzzy objective function algorithms", New York: Plenum Press, 1981.

[14] J. C. Bezdek, Pattern Recognition with Fuzzy Objective Function Algorithms. Springer Science & Business Media, 2013.

[15] N. R. Pal, K. Pal, J. M. Keller, J. C. Bezdek, "A possibilistic fuzzy c-means clustering algorithm", IEEE Trans. Fuzzy Syst. vol. 13, pp. 517-530, August 2005.

How to Model a Likely Behavior of a Pedagogical Agent from a Real Situation

Mohamedade Farouk NANNE
Assistant Professor, Research Unit "Digital Documents and Interaction", Dept. Mathematics and Computer Science, Faculty of Sciences and Techniques, University of Sciences Technology and Medicine, Nouakchott - Mauritania

***Abstract*—The aim of this work is to model the behavior verbal and nonverbal behavior of a Pedagogical Agent (PA) can be integrated into an Intelligent Tutoring System. The following research questions were posed: what is the nonverbal component of an educational communication? How to study this component for a computational model of plausible behavior of a virtual agent? What correlations between educational actions and the direction of gaze of a human agent? To carry out exploratory work, a methodological approach based on multi-modal video corpus study was adopted. Within a multidisciplinary team consisting of computer scientists and didactics of mathematics, an educational situation in which a virtual pedagogical agent is likely was developed. Dyadic interactions between teachers and learners late second early third (15-16 years) in a skills assessment interview in mathematics following the resolution of exercises by students with a mathematics software was filmed. A multi-level annotation scheme to annotate the observed behavior was proposed. The multidisciplinary research subject (ITS, Human-Machine Interfaces, Educational sciences, educational, linguistic etc.) due to the development of the coding scheme a delicate but important work given the wealth of knowledge from different disciplines. After a portion of the collected work annotation corpus statistical measures derived from annotations carried out suggest different strategies for teachers in terms of gaze direction depending on the learner profile and pedagogical actions. These measures have enabled to extract rules to control the nonverbal behavior of a PA.**

Keywords—pedagogical agent; nonverbal communication; behavior; corpus analysis

I. Introduction

The general theme of this work is the integration of a pedagogical agent in a Computing Environment for Human Learning (ILE). This theme, very extensive, can itself give rise to many research directions in computer science but also in Education Sciences, in Cognitive Sciences or Psychology. Set in this context requires a research topic to restrict and specialize this vast field of research. It was decided to focus this work on modeling the behavior of a pedagogical agent. This work should provide answers to a number of questions. In particular: in what situations a pedagogical agent can it improve communication between a student and an ITS? How to model these situations and interactions to specify the behavior of an agent?

To answer these questions, an empirical approach based on video corpus analysis compiled from situations of communication between humans was followed. The objective of this analysis is to evidence rules of behavior to model the behavior of the pedagogical agent.

In the field of educational agents, multimodal behavior of the agent is often limited expressiveness and is not based on a detailed analysis of multimodal behaviors of teachers, but rather on general rules derived for example from the literature in sociolinguistics. Although the use of educational videos developed in the field of ITS, they are rarely used as a resource for annotating and understanding of multimodal communication in the educational context. It was decided to follow a methodology that takes into account the sociolinguistic literature but especially to data from real situations. This methodology for annotating videos corpus and statistical analysis of these annotations was developed in the field of Human-Machine Interfaces.

A key objective of this work is to explore the application of this methodology to the field of ILE and specifically pedagogical agents. We were taken for this to be a video corpus based annotation analysis targets, define a schema and a markup annotation protocol, to analyze these annotations to finally provide a set of rules to control certain elements of non-verbal behavior of the agent.

II. Methodology

The multimodal behavior varies depending on the context and therefore must be routed so situated. The nonverbal behavior literature is rich in experimental methods and studies. However, from the perspective of human-machine interface design, it provides little specific enough knowledge to be used in a relevant way in a given situation. Approaches type digital corpus aim to provide such specific and detailed knowledge to a particular situation for building computational models. This methodology recommends starting with defining questions that wants answers using this method and also the definition of basic concepts. Then comes the development of an encoding scheme involving these and these concepts. The next step is to collect video footage from which the behavior will be defined. Once these sequences are recorded, an encoding scheme according to the already determined to be performed. This coding must be validated and after validation, statistical measures should be implemented to draw lessons for defining control rules of the pedagogical agent.

The particular methodology developed for modeling the behavior of a pedagogical agent located based on that general methodology. The main difference is that, according to general methodology, the coding scheme directs corpus of the collection and the concepts which are based on this scheme are fixed in advance, upstream of the collection. In the case of this work, exploratory work communication actual data collection in a learning situation served prior to the definition of many of the concepts. Given the very precise contextualization of this work, some of the underlying concepts to this particular study could not be determined a priori. These were extracted from viewing videos in preparatory work for the establishment of the coding scheme. The steps of the video corpus annotation methodology which underpins our research methodology will be detailed later.

A. Define the research questions and basic concepts

To achieve satisfactory results, it is important to define research questions. Their definition requires the determination of concepts and definitions which they refer.

B. Coding Scheme

A coding scheme is a set of parameters and indicators to be considered when observing sequence to annotate. It contains all the elements that could provide answers to research questions. It is therefore linked to the concepts and definitions which research questions refer. A coding scheme consists of annotation values. An annotation value is the means by which the annotator to describe his observation of an event. Those annotation values can be arranged in sets or groups of sets. These annotations values may be exclusive or not. The development of a coding scheme is a difficult task. [1] proposes to answer the following questions before developing a coding scheme: what are the coding schemes already defined in other studies that are similar or close enough to study to achieve? Do annotations values of these patterns are naturally defined and clearly structured? The links between these annotation values, research questions and the underlying concepts are they outstanding? If the answers to these questions are affirmative, [2] believe that there is a strong chance that the use of such encoding schemes as they are or by making changes would have a positive contribution.

C. Registration and behavior coding

Once the coding scheme defined, the annotator has methodological tools needed to describe his observations a series of practical and technical questions arise. These questions relate to how annotators will work and save their decisions (observations). Managing to combine the human and material resources in order to make observations and record them is the goal of this stage of the method.

[2] propose recording sequences of behavior observed in real time for later annotation. The advantage of video is the ability to perform multiple viewings but also the opportunity to review the event by slowing down the movements. Records can be stored for later use. They can also be seen by different observers and / or with different objectives. For example, different annotators can annotate different behaviors recorded. The same sequences can also be seen by an observer same but in different time for it confirms previous observations or for it to work in a progressive manner. The videos provide a literal observation of behavior , that does not allow the vision in real time. The recording tools are becoming relatively inexpensive, easy to use and information loss risks are minimal.

D. Representation of initial data

Whatever the technical tools used during annotation (paper and pencil tool, recordings involving cameras connected to laptops ...), annotations will ultimately processed by computer.

The use of an approach based on technology often has many advantages. Many computer systems have been developed for this purpose. One example is the software Anvil Mr. Kipp [3], the system developed by The James Long Company [4], the system developed by L. Procoder Noldus [5] and the system ObsWin developed by N. Martin, C. Oliver and S. Hall [6].

Generally, computer-coding systems are used to define the codes, their use and their characteristics. These systems safeguard the codes and the time associated with these codes in files. Annotators can edit these files and change them if they find that the initial codes are wrong. With appropriate equipment, video recordings can be controlled with the mouse. The annotator can then select episodes that appear interesting to him and watching them repeatedly.

The annotated data are stored in files for their computer processing (statistical calculations). Software has been developed can process these data such as SAS and SPSS but that these data are processed by the software, it must be organized according to forms required by that software. Depending on the desired treatment, it may be the other need to develop its own statistical analysis programs.

[7] defined a standard organization of annotation data to make them shareable. This standard is called SDIS.

E. Study of reliability of annotations

The records must be validated. In other words, it is necessary to assess the reliability of decisions made by annotator in his annotation. This step of the method of verifying the implementation of coding scheme by the annotator and prudence in decision-making. Several methods can be used to make this verification. If there is a standard that is supposed to correct, annotators can compare their observations with respect to this standard.

A set of video sequences is selected to serve as support for the validation step. Several annotators annotate these sequences independently of each other. A measure to calculate a coefficient of inter-judge agreement among different observers is then applied. This is the Kappa [8]. It can be applied to an isolated annotation value, or to a set of annotation values. The agreement is considered perfect if the coefficient is 1. If the agreement is greater than 0.75, it is considered excellent. If it is between 0.60 and 0.75, it is considered good. For agreements that are less than 0.60, the agreement is inadequate.

F. Statistical calculation on annotations

Statistical calculations on annotations enable a comprehensive and detailed view (depending on the nature of the calculations) of the studied indicators, their possible occurrences and co-occurrences. This step allows to define the elements constituting the studied behaviors and assembling these elements model the behavior will be defined.

III. Constitution of the Corpus and Annotation

Habert defines a corpus as a collection of language data that are selected and organized along linguistic lines and extralinguistic explicit job to serve as determined sample of a language [9]. Such corpus may be textual, audio, video or multimedia. The corpus can be used in several areas: language, interactional linguistics, ergonomic psychology, sociology, etc. A body is considered well-formed if some elements are taken into account in its constitution. These criteria vary according to the area studied.

A corpus should reach a critical size to be representative [10], but also to the statistical measures are reliable. A well-trained corpus must cover one language and more specifically one variation of this language. It is clear that this condition is applicable only on language use in corpus, because for example if we want to compare the gestures used by the French and those used by Anglo-Saxon in a given circumstance, we are obliged to collect videos two different languages. Two other criteria, like the previous criterion concerning the linguistic corpus. This is the time covered by the text corpus and language register.

For computer applications, we distinguish the corpus for learning and corpus for the test [11]. The corpus for learning are the corpus for study of indicator values (learn what the values of these indicators). The corpus for the test are the corpus collected while indicator values are defined in advance, the purpose of their incorporation is to validate or invalidate these values. In no way do the results or implement models from a training corpus on the same corpus as a test because if the values of the indicators sought are defined by the act of a body back to the same corpus could validate that attributed values are well within the corpus, which would validate the annotation process but would not validate the fact that these values are the most appropriate for the studied indicators.

The constitution of a corpus depends on the objective motivating the constitution both in terms of the situation at the level of collection itself. At the end of this constitution [2], a corpus can be considered sufficient to meet the aims of its constitution or not to be, which can result in a new collection. Out of all the footage, it often happens that all is not relevant in relation to the objectives of the corpus. Filter is then performed to select the data for the annotation. Filtering can also be applied in the case where the annotation means are not equal to the data collected such as the number of annotators or time devoted to the annotation work. Other reasons may lead filtering data collected such as the volume indicators looking. When using hundreds of indicators, the volume of data that can be mark up is different than when a few indicators are used. The indicators used in this work are detailed in the "coding scheme" section. A compromise feasibility and "reliability" appears. More data is annotated many more indicator values are confirmed which increases the reliability of values assigned to the indicators but the question of the feasibility intervenes quickly because it is expensive to annotate a number of important data.

This section describes how the corpus was collected and annotated. It describes the status of the data collection, the data collection, the selection of data on which the work is done, the coding scheme which has been developed and the annotation work.

A. Constitution of corpus

The annotation and corpus analysis are very time consuming. To select the most informative sequences with respect to the research questions, a fairly large number of videos was collected. In addition to this large size of the corpus, the other three criteria for a corpus is well formed (see the introduction to this section) are verified. The interviews are all recorded in French, in the same period (the period that covers all records is less than two months) and all components (textual, audio and visual) are recorded as part of post-resolution of interviews mathematical exercises for school students late third and early second intended to be applied in the same frame.

The communication situation that was filmed is that of interpersonal communication between a teacher and a student. The student before performing the test (which is individually performed on a computer). The cognitive profile and all Student Answer the exercises are then printed and sent to the teacher. The teacher had a few days to study these documents and prepare for the personal interview. At the beginning of each interview, the teacher prepared students to the situation of record so that it is not too tight and to reduce the influence of the presence of cameras so that this presence has no effect its possible interventions. The purpose of this interview is twofold. On the side of the student's goal is to help him overcome his difficulties in algebra and meet their specific questions by explaining its fragility and its levers and advising him to improve his level. The goal is to collect a corpus allowing us to specify the behavior of a pedagogical agent from real situations.

The teacher and student are sitting next to each other, facing a low table on which documents are placed. The table height is an important factor. Indeed, the two players must keep complete freedom of movement, at least as regards the upper body, so as not to force the use of different communication modes. This interview situation that the teacher and student are naturally positioned slightly turned towards each other. Two cameras were used, one positioned in the axis of the teacher and the other in the axis of the pupil, forming a triangle with approximately 60 degrees. Each camera records the entire scene but can effectively capture facial expressions, gaze and human gestures and postures on which it focuses. The height of the cameras have been set so as to properly observe both the facial expressions of people filmed (including when they look at printed material placed on the coffee table) and, with sufficient accuracy, the pointed places these documents (when a deictic gesture to a printed document is used).

Preliminary work viewing was conducted in order to identify a priori, informally, episodes considered particularly rich and interesting, firstly in terms of multimodal communication and, secondly, in terms of instructional events made by the teacher.

B. Coding Scheme

Like any experimental approach, an approach based on the corpus of study begins with the identification of one or more theoretical questions that wants answers. These questions and theoretical objectives and the study of existing work should direct the collection of video data and constitution of the coding scheme.

A multi-level encoding scheme from the collected corpus and theoretical elements from the literature was formed. This scheme has been retouched and validated by a team of researchers who come from many disciplines including linguistics, teaching and IT.

Many taxonomies to manually annotate observed behaviors have been developed at different levels, from the physical signs in different ways to more subjective levels related to the interpretation of such messages related to acts of dialogues or emotions [12] [13] [14] [15].

Before discussing the development of the coding scheme, it would be good to discuss the taxonomy of Pariès and DAMSL scheme whose application areas overlap that of this work.

The work of Pariès focus on the classroom teacher's communication. They are therefore different from this work since it is interested in the communication between two people (teacher-student) and not to the communication between a person and a group of people (teachers and students). This work is nevertheless interesting because most of the functions of the speech defined by Pariès remain relevant in the context of this study. Pariès defines two types of functions in the teacher talk: cognitive function and non-cognitive functions. Cognitive functions are related to the task to solve and mathematical knowledge. Cognitive functions are mentioned by Pariès: Distribution tasks Introduction of a sub-task, balance, Evaluation, Justification, Structuring. The non-cognitive functions are independent of the task in their formulation even though they may have an effect on the resolution. In this function category, Pariès class the following functions: Commitment in the job, Mobilizing students' attention, encouragement, Pooling the student's response.

Pariès taxonomy was developed using a corpus of six sessions recorded in four different classes of fifth, a refresher class in sixth and during a particular lesson in fourth class [16].

In this taxonomy, several functions will not be transposed to this study because the context is different. The communication between a teacher and a class is different from the communication between a teacher and a student. Thus functions such as "Mobilizing the attention of the student" for managing noise in a class and the "Pooling of student response" that allows to share the answer to all of a student by repeating, are not relevant in this situation.

Another taxonomy attracted the attention. This is DAMSL which was proposed by Core and Allen [17]. The first version of DAMSL was developed using the TRAINS corpus which gathers oral dialogues between two participants working together to solve a planning task. This corpus has 18 dialogs for 1524 set annotated by two people. This project was then used as the basis for other such body COCONUT [18], Monroe [19] and SWBD [20].

DAMSL has four main dimensions annotation :

- Communicative status: specifies if the statement is understandable and if it was completed and if the speaker seems able to convey what he meant. For example, a statement can be annotated as "self-talk", meaning that the speaker seems unable to transmit the information contained.
- Information-level: represents the semantic scope of the statement. In this category, four types of statements can be classified: statements that are interested in performing a task, those who speak of the management of a task and those interested in the management of communication. The fourth type includes statements that are not part of the first three types.
- Forward looking functions: defines how the statement will influence the discourse, context, actions of the speakers. In this category are the words of the speaker on the next actions to take, the effects on the statement following the conversation and statements containing requests.
- Backward looking functions: shows the relationship between the statement and previous statements of the speech. Such a statement could have a goal to meet, accept, reject, correct a previous speech. To do this it is necessary to specify the type of function that contains the statement and the previous part of speech to which the statement refers.

These categories are not mutually exclusive.

[21] defines two types of statements of a speaker: the locutionary acts and speech acts. By locutionary acts, it refers to what is said by the speaker, that is to say the fact to produce sounds. It defines the illocutionary act by the social act performed by producing a statement (producing a promise, an application, a statement ...). This work was pursued by linguists such as [22] offering four types of acts (act of utterance, propositional act, and perlocutionary act illocution) or [23] that mention five different functions the speech acts (assertive, the directive, the promissifs, expressive and statements). As part of this work, only the first level of analysis provided by Austin was used. This study focuses on speech acts represented by the speaker's intention, in this case, the teacher.

Taking into account existing studies mentioned above, and the particular situation that is the object of this study, a multi-level annotation scheme was developed. This scheme consists of five main levels: the intention expressed by the teacher, the means used by the teacher to express this intention, the strategies used by the teacher, emotional parameters and the nonverbal behavior. These levels will be detailed later.

Intention

In this level of annotation scheme, the illocutionary goals of the teacher are placed. [24] distinguishes three intentions of the teacher talk. These intentions are: information, evaluation and animation. These intentions have been identified in the corpus that was collected. Annotation values in this category are divided between the three types of intention.

It is inspired by the division made by Pariès into two types of functions: cognitive and non-cognitive. Among the non-cognitive functions, it is classified everything relating to the entertainment. For cognitive function, it is classified everything concerning information and evaluation.

All DAMSL categorization levels are present in the intention category. The Animate part is very close to the level "Information-level" of DAMSL and specifically the sub category "Communication-management". Other DAMSL levels are also present. This is "Forward looking functions" and "Backward looking functions" because some functions refer to functions related to the previous parts of speech (eg, "show cause") and other functions influencing the Following of the conversation (eg, "to ask"). The fourth level DAMSL (Communicative status) is also present in the annotation value "interrupt point"), especially with his "Abandoned" value. For parties to assess and advise on the most appropriate DAMSL level is that of "information-level" in its parts "Task" and "Task management".

Means

In this level of annotation scheme, the means used by the teacher to express an intention are classified. This is essentially linguistic means but also other resources that was identified in the corpus. The annotation values classified at this level three overlapping levels of DAMSL taxonomy. Some values can influence the continuity of the conversation (eg, "ask a question") and this is how they intersect the level "Forward looking functions". Others refer to previous parts (eg, the annotation value "sum") and thus overlapping the level "Backward looking functions". Some values relate to the management of the task and the task itself (eg, "read part of a support" and "focus on educational support") and the management of communication (for example, the annotation value "be humorous." These overlapping level "information-level" of DAMSL.

Strategies

In this category all the strategies used by the teacher to achieve a given objective are classified. Annotations values placed here cut across levels DAMSL. In particular level of duties "Forward looking functions" (eg, incitement affects the continuity of the conversation) and "Backward looking functions" (eg, the value annotation "correct errors" which refers to the past learning) and "information-level" in its part related to the management of the task and the task itself. We also note the similarity between the "Introduction of a sub task" of the taxonomy Pariès and annotation value "cut a complex question into sub-questions" that level of our annotation scheme.

Affective parameters

At this level of annotation scheme, the emotional parameters observed in the corpus are classified. This level intersects the DAMSL schema diagram for the functions "Forward looking functions" (eg annotation value "motivate learners" that would affect the rest of the conversation) and "Backward looking functions" (eg "mitigate speech" which refers to a previous part of speech). The annotation value "Encourage the learner" is found in Pariès in the "Encouragement" function.

Nonverbal behavior

This category includes the direction of gaze, gestures and facial expressions.

The gaze direction and mutual eye contact are very important in human-human interactions. The look not only helps manage practical tasks such as the exchange of turn in the conversation, but it also conveys a broad spectrum of information about the speaker, such as sociability, personality, culture . In Western culture, people often establish eye contact are perceived as more attentive, friendly, cooperative, confident, mature and sincere; while those who avoid the gaze of others are perceived as cold people pessimistic, defensive, evasive, indifferent and submitted. Several experiments have also highlighted the role persuasive than the eye can play [25] conducted a number of studies on human-agent interaction. They showed that the look is very important to make the plausible speech. It was also shown that individuals who cooperate mutually longer look than those in competition with each other [29]. People using eye contact receive more job offers after an interview, more help when they request it, and teachers who watch over the students make them more productive.

Pedagogical agents can use gestures to encourage, blame, empathy, praise (facial expressions, hand gestures), encourage them to ask questions (gesticulate, scratching their heads), etc. They can also show how to perform a physical action in a simulated 3D environment (hand gestures, postures).

Facial expressions are located not only in the geometry of the face, but also in terms of the texture of the face, and particularly the color (e.g., reddening) and brightness (tears, sweat etc.). The first model of blood vessels (including facial color depends) was developed by [26]. In this model, the authors define emotion as a function of two parameters: a parameter to control the muscle model, and a parameter to indicate the face of the texture variations.

IV. Annotation and Validation of Annotations

[27] defines a video annotation by the establishment of a textual description or digital video content, regardless of the part of the document in question. [28] defines the video annotation by the process by which textual or other information is associated with specific segments of documents. This information does not alter the original document, but are simply mapped therewith. Defined as an annotation is a generic term that includes both the addition of information without specific constraints, such as an exchange of e-mail about a video, or addition of information that must meet a defined format.

The objective of the annotation work is to apply statistical calculations on annotations. These annotations must be organized in a structure that allows for these calculations a robust, reliable and systematic. A tool has been chosen to organize these annotations in XML files which were then assembled in order to apply the desired statistical calculations.

Two annotation types can be distinguished: the manual annotation and automatic annotation. Automatic annotation proceeds by computer processing of video or audio signal to extract the elements. The software to use depends on the level of annotation to lead.

For example, the fact of calculating the size or duration of a video does not require complex treatments whereas the detection of specific elements in a video or comparing two images is complex. The manual annotation is necessary when automatic annotation cannot meet the objectives of the annotation work. For example, to extract the educational process initiated by a teacher, there is need to use this type of annotation.

The corpus analytical work was started by a transcription job of the teacher's speech with Praat, sound analysis software. The audio signal from the video has been imported into Praat then was manually segmented on the basis of the auditory content. After completing the transcript of the speech, it was imperative to use annotation software to import the files resulting from the transcription.

The annotations are defined in a hierarchical manner. There is need to use a tool that supports a multi-level coding scheme. According to the study [30], only Anvil tools, Media & Text Editors and Elan support this kind of coding scheme. But among these tools, only Anvil can import Praat transcription files.

The video selected was annotated with the Anvil software. This annotation work began with defining the specification file that contains the coding scheme described in the previous section. The TextGrid files produced by transcription with the Praat software was imported in Anvil. In these files, the teacher's speech is transcribed and is segmented into blocks. The blocks was analyzed one by one, and in the analysis, the annotation values constituting the scheme was checked one by one and each time the analyzed part of speech corresponded to an annotation value, the time to this correspondence and the interval marked on the appropriate track was defined.

The total duration of annotated sequences represents 54 minutes and 55 seconds. The duration annotation work of each part of speech is a function of its density. Part of speech tagged with multiple tags, takes longer to annotate a portion having a single label. It took us the final 54 hours and a half to complete the annotation work, what makes a average time was devoted to annotate a minute of video.

For now this work was limited to the gaze direction with respect nonverbal component of communication. This choice is explained partly by the importance of eyes in human communication, and secondly by a greater simplicity of this annotation component relative to other components of nonverbal communication such as such gestures. Working on the look has allowed carrying out the test work and methodological development which was the first. The annotation of this track was different from the other tracks in the coding scheme because it did not based on the blocks of the speech provided with importing files Praat but only watching videos. Other annotation work including gestures and facial expressions are underway.

The annotation work is a very costly process in terms of time. It was therefore impossible to validate all annotated sequences. It was decided to test the annotations on an extract of three minutes. The choice of this extract was adopted after viewing annotated excerpts. The first criterion was the annotation density values. Other criteria were also taken into account, such as the agreement between the annotation values for each block and the teacher talk.

This extract three minutes is not a lot for an annotated total of 54 minutes, but as in the case of exploratory work and given the available resources, the validation work should be limited. A second annotator took four hours to annotate this extract. This is not surprising given the density of the chosen extract.

To support the testing, this extract has been annotated by the teacher who gave back to the learner. In addition to its expertise in didactics and pedagogy, it is best placed to explain his speech, that is to say through this discourse determine the pedagogical act she wanted to accomplish.

Having entered this excerpt the two annotations were compared using the Kappa statistical measure.

Kappa is a statistical measure proposed by Cohen [8]. The agreement found between qualitative judgments or not, is the sum of a "random" component and a component of agreement "true". The Kappa coefficient, denoted κ, proposes to quantify the intensity or quality of the actual agreement between paired qualitative judgments. It expresses a relative difference between the proportion of observed agreement and the proportion of random agreement that is to say the likelihood of annotators agree luckily that is the expected value under the null hypothesis of independence judgments, divided by the amount available beyond random agreement. k corresponds to the maximum of that agreement that it would be corrected under the simple effect of chance.

The application of the statistical test of interrater agreement kappa gave very good results. The results are between 0.75 and 1, which corresponds according to the classification of [31] a good agreement to excellent. It is evident that this first validation is very limited. In a subsequent phase, these annotations may be validated using several annotators and more meaningful recording times. This work is exploratory work and seeks to highlight control rules that make the probable agent. This initial check shows that the coding process is relevant, if not actually validated.

V. Modeling and Implementation

The annotated corpus was the subject of a study by statistical analysis of annotations. Annotations are stored by ANVIL in XML files. A Java program into taking these XML files and to obtain a share of simple statistical evidence about the annotations (number of hits, average duration, etc.) and, secondly, the probability co-occurrence between the annotations and the direction of gaze was developed. These have allowed studying the correlation between the direction of gaze and other annotation values. In other words a search for every act done by the teacher, what is the probability of focusing the gaze to each of the centers of attention was performed. Thereafter the analysis algorithm implemented will be detailed.

The files from the annotation and whose extension is .anvil are XML files. The parser used to extract data from these files based on the library JAXP (Java API for XML Processing) which is used to parse XML documents through a Java program. After parsing the data are stored in arrays of vectors. Each annotation value is presented by an array of vector, vectors and a hundred paintings was created (number of annotation values encoding scheme). The size of the array is the number of annotation files passed to the parser. Following this step for each value of annotation all occurrences are stored in a table of vectors. The data on the occurrence of an annotation value are the start time, the end time of the period, the index of the event, the name of the annotation track.

Statistical measures applied to these vectors boards are explained below. Following these overall results and detailed calculations are stored in HTML files.

The steps of calculating the annotations are as follows:

Step 1: For each annotation value we calculated the total time of agreement with a single point of focus look. Eg for annotation value "Ask a question" we observe that the teacher focuses his gaze on the student for 40% of the time.

Step 2: The results of the preceding step may not be relevant in case of superposition of strongly linked annotation values. For example, if an annotation value A often appears simultaneously with an annotation value B, and if calculations show that these two annotation values have the same focal point of the eye, we can not distinguish whether this is the result of the performance of A or the completion of B. It is therefore necessary to study the dependence of the two values and it is the objective of this step.

Step 3: It is also possible that the influence is not that of an annotation value to another, but that of a block of annotation values on the value studied. For this we calculated all intersections annotation values were encountered in the annotated episodes. Specifically for each value annotation we studied its intersection with the blocks of annotation values that overlap.

Step 4: We also calculated for each annotation value, the focal point of the corresponding eye if there is no intersection with other annotation values which can be called "exclusive intersection "between a focusing point of view and an annotation value.

We distinguish annotations in three broad categories: those for which the co-occurrence values are stable from one student to another, those that seem to be related to the cognitive level of the student and those for which these values vary independently of the cognitive level of the student. Cognitive profiles of products allow students to place students in relation to the knowledge expected at this level of competence in elementary algebra. We hypothesize that this "level" of the student is an important factor explaining some differences in the analysis of the corpus. This hypothesis will of course be consolidated by a study on a larger panel of students.

VI. Conclusion and Perspectives

In this work the role of the agent to conceive is that of a teacher giving a feedback to a learner on a mathematical evaluation. Not to miss elements that may be essential, it was useful to make use of scenes back and coordinate this information coming from real situations with theoretical knowledge from the scientific literature. Thus these sessions were organized with students the school level at which the application that will host the agent is intended. There is no question here of a noted work but rather a work that helps the student to better understand his knowledge of algebra. These sessions involved two teachers and eight students. Thus corpus of teaching communication situations with strong emotional charge was collected.

Once the corpus is collected, the question that arose was how to study nonverbal component in educational communication for a plausible computational model of a pedagogical agent. To study this component, the context of ILE video corpus analysis methodology developed for the HMI was adopted. This methodology begins with the definition of objectives. To secure these objectives, the screenings of videos from the collection of the corpus and a study of existing taxonomies and annotation schemes were made. A multi-level annotation diagram modeling the actions of the teacher as the general level of ordinary communication at the level of educational communication was developed. Teacher's intentions, linguistic or other means he uses to express themselves, teaching strategies implemented, the teacher's emotional parameters were taken into account in establishing this pattern of annotation. For non-verbal communication, work is limited to the gaze direction. The viewing was carried out by several people from several disciplines: computer science, pedagogy, didactics and linguistics. This work was also used to select the set of episodes judged interesting for the annotation. Following this scheme annotation all selected sections were annotated. Given the time and energy that takes such work, validation could be made only on a limited sample. But this symbolic validation has given excellent results.

The next stage of work was to provide answers to the question what correlations between verbal communicative behavior and the viewing direction of a human agent. The communicative behavior in its verbal aspect was annotated, and the direction of gaze of the teacher. Just make calculations to study the correlation between this component of nonverbal behavior and different values constituting verbal behavior. A Java program was conducted for this purpose.

At the end of this step we get for each annotation value the probability that the light of the teaching points towards one of the focal points of the eyes. Thus, a model has been proposed to control the pedagogical agent. A working implementation of the rules defined in this research is underway on the agent litebody [32]. After setting these rules and those that will result from the annotation of gestures and facial expressions, a validation work will be done and guidance to struggling learners is planned.

ACKNOWLEDGMENT

Most of this work was conducted as part of a doctoral thesis at the University Paris 8 in collaboration with Jean-Hugues Réty, Elisabeth Delozanne, Jean-Claude Martin, Brigitte Grugeon, Catherine Pelachaud and Nelly Bensimon.

REFERENCES

[1] BAKEMAN R. Behavioral Observations and Coding. In H. T. Reis & C. K. Judd (Eds.), Handbook of research methods in social psychology (pp. 138-159). New York: Cambridge University Press, 2000.

[2] BAKEMAN R., DECKNER D.F, Analysis for Behavioral Streams, In Teti, D. M. (Ed.), Handbook of Research Methods in Developmental Psychology. Oxford, UK: Blackwell Publishers, 2004..

[3] KIPP M. Gesture Generation by Imitation. From Human Behavior to Computer Character Animation. Florida, Boca Raton, Dissertation.com, 2004. http://www.dfki.de/~kipp/dissertation.html

[4] LONG J. Video coding system reference guide. Caroga Lake, NY: James, Long Company, 1996..

[5] NOLDUS L.P.J., TRIENES R. J. H., HENRIKSEN A. H. M., JANSEN H., et JANSEN R. G. The Observer Video-Pro : New software for the collection, management, and presentation of time-structured data from videotapes and digital media files. Behavior Research Methods, Instruments, and Computers, 32, 197-206, 2000.

[6] MARTIN N., OLIVIER C., et HALL S. ObsWin: Observational data collection and analysis for Windows. CTI Psychology Software News, 9, 14-16, 1999 .

[7] BAKEMAN R., and QUERA V. Analyzing Interaction: Sequential Analysis with SDIS and GSEQ. New York: Cambridge University Press, 1995.

[8] COHEN J., (1960). A coefficient of agreement for nominal scales", Educ. Psychol. Meas.: 20, 27-46.

[9] HABERT, B. 'Representative corpus, what,why and how ?', Des corpus représentatifs : de quoi, pour quoi, comment ?, in M. Bilger (éd.),Linguistique sur corpus. Études et réflexions, Perpignan, Presses Universitaires de Perpignan, pp.11-58, 2000.

[10] HABERT B., FABRE C. et ISAAC F. 'From the writing to digital: build, standardize and exploit the electronic corpus', De l'écrit au numérique : constituer, normaliser et exploiter les corpus électroniques, Paris, InterEditions, 1998.

[11] RASTIER F. 'Epistemological stakes of corpus linguistics', Enjeux épistémologiques de la linguistique de corpus. In G. Williams, Acte des deuxièmes Journées de Linguistique de Corpus, Presses Universitaires de Renne, Lorient, 2002.

[12] BAKEMAN R., et GOTTMAN J. M., (1997). Observing Interaction. An introduction to sequential analysis. Second edition., Cambridge University Press 1997.

[13] POGGI I. Mind Markers. In M. Rector, I. Poggi and N. Trigo. Meaning and Use. Oporto, Portugal University Fernando Pessoa Press: 119-132. 2002

[14] HARRIGAN J.A., ROSENTHAL R. and SCHERER K. The new handbook of methods in nonverbal behavior research, Oxford University Press, 2005.

[15] MARTIN, J. C. Multimodal Human-Computer Interfaces and Individual Differences. Annotation, perception, representation and generation of situated multimodal behaviors. Habilitation à diriger des recherches en Informatique. Université Paris XI, 2006.

[16] PARIES C. M. 'Comparing practices of teachers of mathematical relationships between teachers and speech potential student activities', Comparaison de pratiques d'enseignants de mathématiques relations entre discours des professeurs et activités potentielles des élèves. In Recherches en didactique des mathématiques : vol. 24, no2-3, pages 251-284, 2004.

[17] CORE M. G. and ALLEN J. F. (1997). Coding Dialogues with the DAMSL Annotation Scheme. AAAI Fall Symposium on Communicative Action in Humans and Machines, Menlo Park, California,American Association for Artificial Intelligence. citeseer.ist.psu.edu/ core97 coding. Html

[18] EUGENIO B.D., JORDAN P., et PYLKKANEN L. The coconut project: dialogue annotation manual. Technical report, University of Pittsburgh, 1998.

[19] STENT A. The monroe corpus. Technical Report 728, University of Rochester. 2000.

[20] JURAFSKY D., BATES R., COCCARO N., MARTIN R., METEER M., RIES K., SHRIBERG E., STOLCKE A., TAYLOR P., et ESS-DYKEMA C.V. Switchboard discourse language modeling project final report. Rapport Technique Summer Research Workshop Technical Reports 30, Johns, Hopkins University, Baltimore, 1997.

[21] AUSTIN J.L. How to Do Things with Words. Cambridge (Mass.) 1962.

[22] SEARLE J. Speech Acts. Cambridge University Press. 1969.

[23] SEARLE J. et VANDERVEKEN D. Foundations of Illocutionary Logic. Cambridge: Cambridge University Press, 1985.

[24] DABENE, L. 'For a taxonomy of meta-communicative operations in foreign language classroom', Pour une taxinomie des opérations métacommunicatives en classe de langue étrangère. COSTE, D. (éd.) Interactions et enseignement/apprentissage des langues étrangères, Etudes de Linguistiques Appliquée, 55, 39-46, 1984.

[25] CASSELL J., THORISSON K.R. The power of a nod and a glance: Envelope versus emotional feedback in animated conversational agents. Applied Artificial Intelligence, 13, 519-538, 1999

[26] KALRA P., MAGNENAT-THALMANN N. Modeling of Vascular Expressions in facial Animation, Computer Animation, pp. 50-58, 1994.

[27] ASSFALG J., BERTINI M., COLOMBO C., DELBIMBO A. Semantic Annotation of Sports Videos. IEEE MultiMedia 9(2): 52-60, 2002.

[28] EMOND B., BARFURTH M.A., COMEAU G., BROOKS M. 'Video annotation technologies and pedagogical applications' , Technologies d'annotation vidéo et leurs applications à la pédagogie du Piano. In : Recherche en Education Musicale. 2006.

[29] ARGYLE M. Bodily Communication. New York:Methuen & Co. Ltd. 1988.

[30] ROHLFING K., LOEHR D., DUNCAN S., BROWN A., FRANKLIN A., KIMBARA I., MILDE J.-T., PARRILL F., ROSE T., SCHMIDT T., SLOETJES H., THIES A., WELLINGHOFF S. Comparison of multimodal annotation tools – workshop report. Second Congress of the International Society for Gesture Studies, Lyon. 15-18 Juin 2005 http://www.gespraechsforschung-ozs.de/heft2006/tb-rohlfing.pdf

[31] LANDIS J. R., et KOCH G. G. The measurement of observer agreement for categorical data. Biometrics 33: 159–174, 1977.

[32] Bickmore, T.W., Schulman D., Shaw, G., DTask & LiteBody: Open Source, Standards-based Tools for Building Web-deployed Embodied Conversational Agents, Intelligent Virtual Agents, PP. 425-431 2009.

An Analysis of Information Technology on Data Processing by using Cobit Framework

Surni Erniwati
Academy of Information Management and Computer
AMIKOM Mataram
Mataram, Indonesia

Nina Kurnia Hikmawati
Telkom University Bandung
Universitas Telkom Bandung
Bandung, Indonesian

***Abstract*—Information technology and processes is inter connected, directing and controlling the company in achieving corporate goals through value-added and balancing the risks and benefits of information technology. This study is aimed to analyze the level of maturity (maturity level) on the data process and produced information technology recommendations that can be made as regards the management of IT to support the academic performance of the service to be better. Maturity level calculation was done by analyzing questionnaires on the state of information technology. The results of this study obtainable that the governance of information technology in data processing in Mataram ASM currently quite good. Current maturity value for the data processing has the value 2.69. This means that the company / organization already has a pattern of repeatedly done in managing the activities related to data management processes. Based on the data analysis, there is an effect on the current conditions and expected conditions can be taken solution or corrective actions to improve IT governance in the process of data management at ASM Mataram gradually.**

Keywords—Cobit; Data Processing; Information Technology; Level of Maturity; Management Awareness

I. Introduction

Information technology is a very important requirement for all enterprise organizations because it is proved to help in improving the effectiveness and efficiency of enterprise business processes as well as colleges. To achieve effectiveness and efficiency in the college needed a good management of information technology so that the technology used to support the organization's success in achieving its objectives. The success of information technology depends on how far the governance of IT is done [1].

Information technology governance structures and processes are an interrelated, directing and controlling the company in achieving corporate goals through value-added and balancing the risks and benefits of information technology [2].

Academy of Secretary dan Management (ASM) Mataram is one of the educational institutions of higher education held in Mataram. The main function is as an organizer college education or academic services. In education or academic services necessary for the use of information technology that is able to support the speed, ease of data processing.

In conducting its main activities, ASM as universities that provide education services that are supported by an academic bureaus namely Administrative Bureau of Academic and Student Affairs (ABASA) that function of providing administrative services and academic information quickly and accurately. ABASA already supported by IT in data processing, which for the procurement of IT is implemented by a separate division, namely division BPSI. However, research has not been done to measure the maturity level data processing and mapping the information technology process maturity level of the institution cannot be measured, in addition to these problems relating to data processing, how to maintain the completeness, accuracy and availability of data through the efforts of data backup, data storage or deletion of data. Based on those problems, this study is aimed to make a recommendation proper management of information technology so that it can be used as a reference that can be used wearer and can increase the data processing optimally.

In the information technology management of the study using the framework COBIT (Control Objectives for Information and Related Technology), the basic concept of the COBIT is the determination of control on IT based on the information that is required to support the business objectives and the information derived from the combined application of information technology and resource? The benefit of the research is that the information technology management can be used as recommendations for the management of IT to support the academic performance of the service to be better.

II. Review of Related Literature

A. Information Technology Governance

IT Governance is a combination of structural mechanisms, processes, and relational applied by the Organization [3]. According to the IT, Governance provides a structure associated with IT processes, IT resources and information to enterprise strategies and objectives [4]. How to integrate IT governance and optimization of the company is through the planning and organization (PO), acquisition and implementation (AI), the delivery and support (DS) and monitoring and evaluation (ME) on the performance of IT.

Generally, IT governance has the following definition "IT governance is responsibility executive and council directors, and consists of leadership, structure organization and processes which ensures that company IT prop and expand strategy organization and purpose "[11].

IT Governance is an integral part of the success of enterprise governance through improvements in effectiveness and efficiency in company processes related. IT governance provides the structure that connects the IT processes, IT resources and information to enterprise strategies and objectives. Furthermore, IT Governance combines good (best) practice of planning and the IT organization, and implementation development, delivery and support, and monitoring IT performance to ensure that information about the company and related technology to support business objectives.

B. Control Objectives For Information and Related Technologi (COBIT)

A comprehensive tool for creating the IT Governance in organizations is the use of COBIT (Control Objectives For Information And Related Technology) that bring together the diverse needs of management by bridging the gap between business risks, control needs and technical issues of IT. COBIT provides best business practice reference that covers the entire business process organization and expose the logical structure of activities that can be managed and controlled effectively.

COBIT main goal is to provide clear policy and good practice for IT governance for organizations around the world to help senior management to understand and manage the risks associated with IT. COBIT do so by providing a framework for IT governance and control objectives detailed instructions for management, business process owners, users and auditors.

C. COBIT Management Guidelines

Guidelines for the management of COBIT, which consists of a maturity model, KGI, and KPI, which then provides management with tools to assess and measure the organization's IT environment against 34 identified COBIT IT processes. Currently IT-related risk management is understood as a core part of the organizational arrangements. IT arrangements that are part of the organizational arrangements become more pronounced role in achieving organizational objectives by adding value through balancing risk on the value of IT and its processes.

IT arrangement is an addition element for the success of management organization through increasing the effectiveness and the more efficiency of organization process. IT arrangements provide a structure that is related to the IT process, IT sources, and strategy information and organizations goals. Further, IT arrangements integrate related practices.

D. COBITS' Framework

COBIT (Control Objectives For Information And Related Technology) is a framework of IT Governance, addressed to the management, staff IT services, control department t, the audit function and more importantly for owners of business processes (business process owner's), to ensure CONFIDENCIALITY, integrity and availability data as well as sensitive and critical information.

The basic concept of the COBIT framework is that the determination of control in IT based information needed to support the business objectives and the information generated from the combined application of IT processes and related resources. In the application of IT management, there are two types of control models, namely the model of business control (controls business model) and IT control models (IT focused control models), COBIT try to bridge the gap of the two types of controls.

Basically the COBIT framework consists of three levels of control objectives, namely activities and tasks, processes, domains. Activities and tasks are routine activities that have the concept of life cycle, while the task is an activity undertaken separately. Furthermore, activity and task collection is grouped into IT processes that have the same IT management issues are grouped into domains [11].

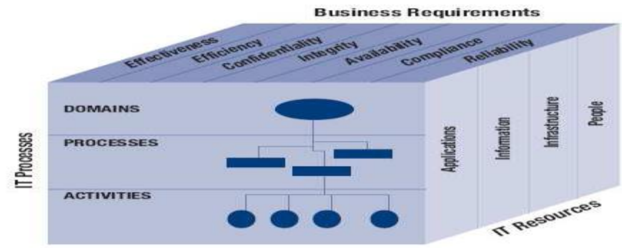


Fig. 1. COBIT cube

COBIT is designed that consists of 34 high-level control objectives that describe the IT process consisting of four domains, namely: Plan and organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The framework consists of the 34 COBIT IT processes divided into 4 management domain [11] namely:

E. Domain Plan and Organize (PO)

PO domain covers strategy and tactics, and focus on the identification of the way IT can contribute best to achieve organizational goals. Furthermore, the realization of the vision of the strategy needs to be planned, communicated and managed from several perspectives. Finally, good organization.

Domain is an emphasis on the application of IT planning process and its alignment with the objectives to be achieved by the company in general. This domain covers the tactics and strategies, as well as a matter of identifying the best way to deliver IT maximum contribution to the achievement of business objectives. The realization of the strategy needs to be planned, communicated and managed by a variety of different viewpoints. Implementation of the strategy should be accompanied by an adequate infrastructure and could support the company's business activities.

IT processes of PO Domain include:

- PO1 – Define a strategic IT plan.
- PO2 – Define the information architecture.
- PO3 – Determine the technological direction.
- PO4 – Define the IT Processes, Organization and Relationships
- PO5 – Manage the investment.
- PO6 – Communicate management aims and direction.
- PO7 – Manage IT human resources.
- PO8 – Manage quality.

- PO9 – Assess and Manage IT risks.
- PO10 – Manage projects.
- PO8 – Ensure compliance with external requirements.

F. Domain Acquire and Implement (AI)

Domains with an emphasis on the process of selecting the technology to be used and the process of implementation. To realize the IT strategy that has been established must be accompanied by appropriate solutions, IT solutions and then held and implemented and integrated into business processes. IT processes in the domain of AI are:

- AI1 – Identify automated solution.
- AI2 – Acquire and maintain application software.
- AI3 – Acquire and maintain technology infrastructure.
- AI4 – Enable Operation and Use
- AI5 – Procedure IT Resources
- AI6 – Manage change.
- AI7 – Install and accredit Solutions and changes systems.

G. Deliver and Support (DS)

This domain focuses on the process of IT service and technical support that includes security system, continuity of care, training and education for users, and ongoing data management. DS domain consists of 13 control objectives, namely:

- DS1 Define and manage service levels (assign and manage service levels).
- DS2 Manage third-party services (managing the services of a third party).
- DS3 Manage performance and capacity (set of performance and capacity).
- DS4 Ensure continuous service (guarantee continuity of service).
- DS5 Ensure systems security (guarantee the security of the system).
- DS6 Identify and allocate costs (identifying and allocating costs).
- DS7 Educate and train users (educate and train the user).
- DS8 Manage service desk and incidents (managing service desk and problem).
- DS9 Manage the configuration (configuring).
- DS10 Manage problems (managing problems).
- DS11 Manage Data (organizing data).
- DS12 Manage the physical environment (arranging the physical environment).
- DS13 Manage operations (set operations).

H. Monitor and Evaluate(ME)

This domain focuses on the regulatory process on the organization's entire IT management controls are applied every IT process must be monitored and assessed for feasibility regularly. These domains focus on the problem of controls that are applied within the organization, internal and external examinations. The following IT processes in the domain of monitoring and Evaluate:

- ME1 Monitor and Evaluate IT Performance (monitor and evaluate the performance of IT).
- ME2 Monitor and Evaluate internal control (monitoring and evaluating internal controls).
- ME3 Ensure regulatory compliance (ensuring compliance with the law).
- ME4 Provide IT Governance (providing IT governance).

I. Model Maturity

COBIT has a maturity model to control IT processes using the methods of assessment / scoring so organizations can assess IT processes are incorporated (a scale of 0 to 5). Maturity Models that exist in COBIT can be seen in the following table [11]:

TABLE I. GENERIC MATURITY MODEL

0 - Existent	The company does not care about the importance of information technology to be managed either by the management
1 Initial	Company reactively perform application and implementation of information technology in accordance with the needs of existing sudden, without preceded by prior planning.
2 Repeatable	The Company has a pattern that is repeatedly performed in conducting activities related to the management of information technology governance, but its existence has not been well defined and that is still happening formal inconsistency.
3 Define	The Company has had a formal and written standard operating procedures that have been socialized to all levels of management and employees to be obeyed and worked in daily activities.
4 Manage	The company has had a number of indicators or quantitative measures that serve as targets and objective performance of every application of information technology applications.
5 Optimized	The Company has implemented the information technology governance refers to "best practice"

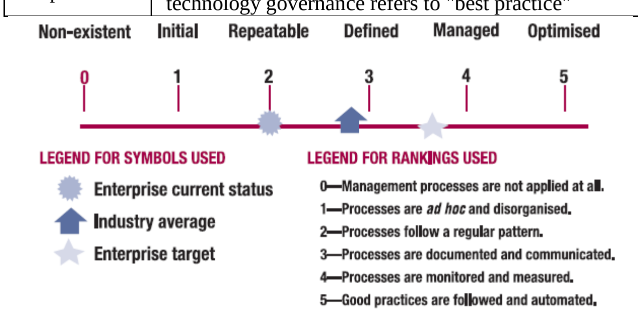


Fig. 2. Maturity Model (ITGI; 2005: p18)

With the maturity level models, the organization will be able to know the position of the current maturity, and continuous and sustainable should strive to increase the level to the highest level so that aspect of the information technology governance can work effectively.

III. Research Methods

The stages are implemented in making information technology governance recommendations as follows:

- The field study in determining the use of information technology is running and collecting the necessary documents, such as vision, mission, objectives, strategies and institutional structure.
- Analyzing the data relating to data processing.
- Making a priority scale questionnaire which is responsible for data processing and BPSI responsible for IT management at ASM Mataram.
- After creating a questionnaire, analyze the data results of the questionnaire results of direct observation and calculation of priorities each control objective.
- Objective data analysis and control of the level of compliance that gained DCO (Detail Control Objectivities) and level of maturity, as well as the gap analysis and research implications.

IV. Result of the Study

a) Data Analysis

In this study, the data can be processed from the questionnaires by respondents are filled according to the data by means of questionnaires, while data is not in accordance with the instructions questionnaires will not be processed further.

Based on the questionnaire that was distributed to respondents selected for filling out the questionnaire in this study were 14 respondents. Respondents were selected that has the ability to assess the current use of IT related to process the data and recapitulated processed for the calculation of the degree of fulfillment Detailed Control Objectives (DCO) and maturity level in ASM Mataram obtained from the calculation results of questionnaires 1 Management Awareness, while the level of maturity (maturity level) ontainable based on calculations questionnaire II maturity level. The software used for data processing by using Microsoft Excel software.

The identification of respondents is done by consistently referring to diagrams responsible, accountable, consulted and / or informed (RACI).

Roles are defined in the diagram RACI main stakeholders (key stakeholders that are directly related to the processing of such data, hereinafter interpreted (mapped in the functional structure in ASM Mataram that shown in the table below.

TABLE II. RESPONDENTS AT ASM MATARAM

No.	Functional Structure Of Cobit		Functional Structure Of Asm Mataram	Number
1	Chief Information Officer	CIO	Head of Planning and Information Systems (BPSI)	1
2	Business Process Owner	BPO	Director ASM Mataram	1
3	Chief Architect	CA	• Admin BPSI • Head of Laboratory	1 1
4	Head Operations	HO	• Program Chairman tudi • Secretary Studies Program	1 1
5	Head Development	HD	Assistant Director for Academic Affairs	1
6	Head of IT Administration	HITA	• Head of Academic Administration Bureau (BAAK) • Head of General Administration Bureau (BAU) • Head Bureau of Financial Administration (BAKeu)	1 1 1
7	Compliance, Audit, Risk and Security	CARS	• Lecturer • Chairman of the Quality Assurance Agency	3 1
Number				1 4

b) Scale Manufacturing Tecniques

The questionnaire in this study treated with the calculation of the degree of fulfillment Detailed Control Objectives (DCO) and Maturity Level. to be able to clearly describe the results of a study of the performance data processing on the fulfillment of criteria-criteria in the processing of existing data in the DCO, the mapping of the responses to questionnaires with values that reflect the performance of the quantitative level of performance, as shown in the table below.

TABLE III. VALUE LEVELS

No.	Answer	Value	Information
1	L (Low)	1.00	Less
2	M (Medium)	2.00	Moderate
3	H (High)	3.00	Good

While the value for the level of maturity of each attribute that contributes directly to the level of maturity for the overall data processing is the value of maturity model can be seen in the following table:

TABLE IV. VALUE MATURITY LEVEL

No.	Answer	Value	Information
1	a	0,00	Non -Existent 0 (None)
2	b	1.00	1 Initial / Ad Hoc
3	c	2.00	2 Repeatable but intuitive
4	d	3.00	3 Defined Process
5	e	4.00	4 Managed and Measurable (Set)
6	f	5.00	5 Optimized

While the scale of the manufacturing index for the level of maturity model mapping contained in the following table.

TABLE V. ROUNDING SCALE INDEX

Rounding scale	Level of Maturity Model
4.51 to 5.00	5 - optimized
3.51 to 4.50	4 - Set
2.51 to 3.50	3 - Defined
1.51 to 2.50	2 - Repeatable
0.51 to 1.50	1 - Initialization
0.00 to 0.50	0 - No

c) The Result of Quetionnaire I Management Awareness

Based on the identification of risk analysis carried out on collecting data on the results of questionnaires that have been carried out, the number of respondents as many as 14 respondents, obtained the answers as much as the number of questionnaires that have been distributed to the respondents. From the respondents, it is made a recapitulation that describes the tendency of the level of compliance, performance, or achievements that are now in ASM Mataram against some object questions, both the fulfillment of the DCO and other indicators related to the processing of data, in general, can be seen in the following table:

Recapitulation of respondents' answers to questionnaires Management Awareness.

TABLE VI. MANAGEMENT AWARENESS

No.	Objects Question	Distribution of Answers		
		L (%)	*M (%)*	*H (%)*
1	Business requirements for data management	7.14	78.57	14.29
2	Storage Settings	14.29	57.14	28.57
3	Media Library	7.14	50.00	42.86
4	Data deletion / Disposal	7.14	78.57	14.29
5	Backup and Restore	21.43	71.43	7.14
6	Data management security needs	21.43	57.14	21.43
7	Tests on the backup media	28.57	50.00	21.43
8	Speed restoration process	14.29	57.14	28.57
9	The success of the restoration process	21.43	57.14	21.43
10	Security of sensitive data after the deleted	14.29	28.57	57.14
11	Incident handling storage capacity	14.29	57.14	28.57
12	The reliability of the system because the recovery process	0.00	57.14	42.86
13	User satisfaction over the availability of data	0.00	64.29	35.71
14	Compliance with the legal aspects / rules	28.57	35.71	35.71
Total		14.29	57.14	28.57

From the results of the recapitulation, can be delivered the following matters:

- Respondents who expressed the opinion that the performance data management processes are still low or less (Low) of 14:29% of respondents.
- 57.14 Respondents who expressed opinions, opinions that the level of performance in the data processing need to be improved or Medium (M).
- Respondents who expressed the opinion that the current data management practices already well underway and the relative has met the expectations of as much as 28.57 respondent.

In accordance with the reference to the recapitulation table answers the questionnaire respondents Management Awareness, can be obtained on the fulfillment of the performance value of the DCO quantitatively as follows:

TABLE VII. DETAILED PERFORMANCE LEVEL CONTROL OBJECTIVES (DCO)

No.	Objects Question	Performance Value
1	Business requirements for data management	2.07
2	Storage Settings	2.14
3	Media Library	2.36
4	Data deletion / Disposal	2.07
5	Backup and Restore	1.86
6	Data management security needs	2.00
	Average	2.08

Based on the performance level table Detailed Control Objectives (DCO) can be concluded that the degree of fulfillment of the DCO in the processing of the data is good enough but needs to be improved, with the average value of the performance of the data processing is 2:08, can be seen in the following diagram:

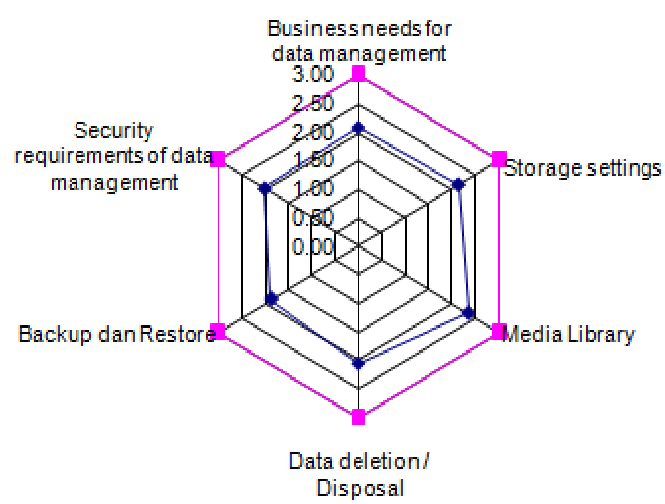


Fig. 3. Representation Diagram Level Compliance DCO

d) Maturity Level II Quuestionnaire Result

Based on the results of the survey questionnaire II maturity level in ontainable answers to the questionnaire as many as the number of questionnaires were distributed to the respondents, the results of respondents' answers are then made recapitulation in the table and is expressed in the following graph:

Table Summary of the distribution of answers to the questionnaire II Maturity Level

TABLE VIII. MATURITY LEVEL II

No.	Attribute	Status	Distribution of Answers					
			a (%)	*b (%)*	*c (%)*	*d (%)*	*e (%)*	*f (%)*
1	Air conditioning	as is	0.00	14.3	35.7	14.3	21.4	14.3
		to be	0.00	0.00	7.14	28.5	14.3	50.0
2	PSP	as is	7.14	21.4	21.4	21.4	14.29	14.3
		to be	0.00	0.00	14.3	0.00	35.71	50.0
3	TA	as is	7.14	28.5	14.3	28.5	14.3	7.14
		to be	0.00	0.00	0.00	21.4	0.00	78.5
4	SE	as is	0.00	14.3	42.8	14.3	21.43	7.14
		to be	0.00	0.00	7.14	7.14	28.57	57.1
5	RA	as is	0.00	14.3	28.5	14.3	14.29	28.5
		to be	0.00	0.00	0.00	7.14	35.71	57.14
6	GSM	as is	0.00	14.3	35.7	35.7	7.14	7.14
		to be	0.00	7.14	0.00	7.14	42.86	42.8
As Is			2.38	17.8	29.7	21.4	15.48	13.1
To Be			0.00	1.19	4.76	11.9	26.19	55.95

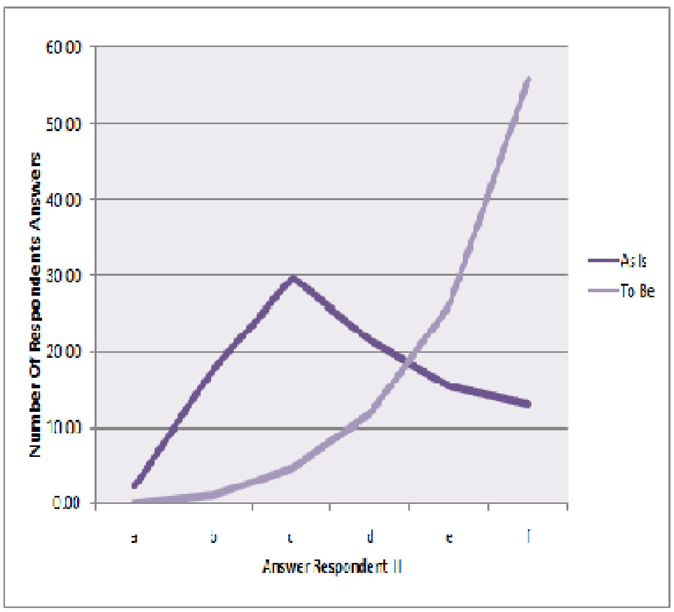


Fig. 4. Refresentasi Distribution Maturity Level II questionnaire answers

Based on the analysis of the current maturity level (as is) and the expected level of maturity, there are attributes air-conditioning, PSP, SE, RA and GSM refers to the level 4 and TA refers to level 5, as shown in the table and graph below:

TABLE IX. VALUE AND PROCESS MATURITY LEVEL

No.	Attribute	Value Maturity		Maturity Level	
		as is	*to be*	*as is*	*to be*
1	Air conditioning	2.86	4.07	3	4
2	PSP	2.57	4.21	3	4
3	TA	2.36	4.57	2	5
4	SE	2.64	4.36	3	4
5	RA	3.14	4.50	3	4
6	GSM	2.57	4.14	3	4
Average		2.69	4.31	2.8	4.2

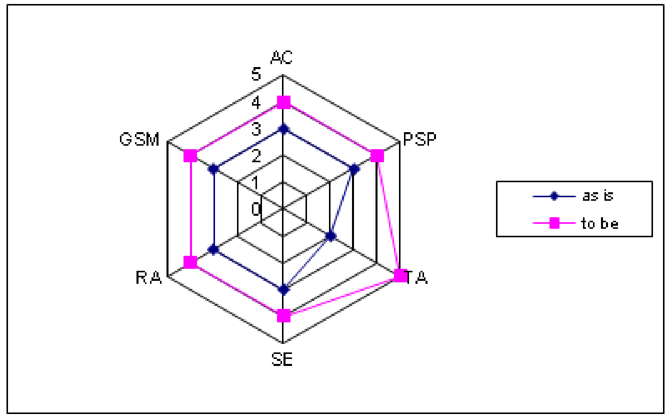


Fig. 5. Value and Process Maturity Level DS11

V. CONCLUSION AND SUGGESTION

a) The Conclusions of the Study are:

- The software used for data processing by using Microsoft Excel software.
- The identification of respondents is done by consistently referring to diagrams responsible, accountable, consulted and / or informed (RACI).
- Based on the results of the questionnaire I Management Awareness in which the degree of fulfillment of the DCO in the process of data management with an average value of performance on data management processes is 2.08. These results are based on the 3 scale is 1 as the condition of "low", 2 as a condition of "being" and 3 as conditions are "good".
- Current maturity value for the data processing has the value 2.69. It means that the company / organization has a pattern of repeatedly done in managing the activities related to data management processes.
- Maturity Level II questionnaire results both for current conditions and expected conditions can be taken solution or corrective actions to improve IT governance in the process of data management at ASM Mataram gradually into 3 groups, namely the corrective action corrective actions to achieve maturity level 4 and level of maturity 5.
- Repairs carried out based on priority, starting from the lowest level of maturity that auxiliary devices and automation (TA), skills and expertise (SE), internal and external accountability (RA), standards and procedures (PSP), goal setting and measurement (GSM) and awareness and communication (AC).

b) The Suggestions of the Study are:

- ASM Mataram

To reach a level of maturity at 5, hard work and committed to work together is required to realize the corrective actions recommended in this study.

- Other researchers

A gradual evaluation is needed after corrective action in accordance with the recommendations for the improvements of this study.

REFERENCES

[1] Agus Prasetyo Utomo and Novita Mariana,"Analisis Tata Kelola Teknologi Informasi (IT Governance) pada Bidang Akademik dengan Cobit Frame Work Studi Kasus pada Universitas Stikubank Semarang",*Jurnal Teknologi Informasi DINAMI,* Volume 16, No 2, Juli 2011: 139-149.

[2] ITGI. (2000). *COBIT 4.1*. IT Governance Institute. [Online]. Available: www.itgi.org

[3] Risma bayu and Dana Indra Sensuse,"Rancangan Tata Kelola IT untuk Institusi Pemerintah Studi Kasus Bappenas", *Jurnal Sistem Informasi MTI-U,* Volume 4, No 1, pp. 7-25

[4] Herri Setiawan,"IT Governance dan Penggunaan Cobit Framework", *Jurnal Sistem Informasi (JSI),* Volume 2, No 2 Oktober 2010, pp. 219-237

[5] Budi Widjajanto, Novi Rijati and Purwanti Kusumaningrum,"Strategi Peningkatan Proses Tata Kelola Teknologi Informasi Universitas XYZ Domain Deliver and Support (DS) Framework Cobit 4.0", *Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2012 (Semantik 2012),* Semarang 23 Juni 2012.

[6] Azhari Shouni Barkah and Melia Dianingrum,"Evaluasi Penerapan Sistem Informasi dan Teknologi Informasi Menggunakan COBIT Frame Work di STMIK AMIKOM Purwokerto", *Jurnal Probisnis,* Vol 8 No.1 Februari 201, pp. 22-30.

[7] Diana Trivena Yulianti and Michel Canggih Patria, "Audit Sistem Informasi Sumber Daya Manusia pada PT X Menggunakan COBIT Framework 4.1", *Jurnal Sistem Informasi,* Vol 6, No.1, Maret 2011, pp. 15-33.

[8] Meliana Christianti, Billy Bobby A.B," Kontrol dan Audit Kinerja Management Information System PT.X Pemrograman di Bidang Marketing Menggunakan COBIT 4.1". *Jurnal Sistem Informasi,* Vol.6, No. 1, Maret 2011, pp. 35-50

[9] Shengnan Zhang and Hans Le Fever, " An Examination of the Practicability of COBIT Framework and the Proposal of a COBIT-BSC Model, *Journal of Economics, Business and Management, Vol. 1, No. 4, November 2013,* pp. 391-395.

[10] Indra Dwi Hartanto and Aries Tjahyanto,"Analisa Kesenjangan Tata Kelola Teknologi Informasi untuk Proses Pengelolaan Data menggunakan COBIT (Studi Kasus Badan Pemeriksa Keuangan Republik Indonesia)", *Prosiding Seminar Nasional Manajemen Teknologi XI,* Program Studi MMT-ITS, Surabaya 6 Pebruari 2010.

[11] ITGI. (2005). *COBIT 4.1*. IT Governance Institute. [Online]. Available: www.itgi.org

[12] ISACA. (2012). COBIT *Document*. Retrieved 2013. [Online].Available: http://www.isaca.org/COBIT/Documents/Compare-with-4.1.pdf

MCIP Client Application for SCADA in Iiot Environment

Nicoleta Cristina GAITAN[1,2]
[1]Faculty of Electrical Engineering and Computer Science, Integrated Center for Research, [2]Development and Innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for Fabrication and Control (MANSiD)
[1,2]Stefan cel Mare University of Suceava
Suceava, Romania

***Abstract*—Modern automation systems architectures which include several subsystems for which an adequate burden sharing is required. These subsystems must work together to fulfil the tasks imposed by the common function, given by the business purpose to be fulfilled. These subsystems or components, in order to perform these tasks, must communicate with each other, this being the critical function of the architecture of such a system. This article presents a MCIP (Monitoring and Control of the Industrial Processes) client application which allows the monitoring and control of the industrial processes and which is object-oriented. As a novelty, the paper presents the architecture of the user object, which is actually a wrapper that allows the connection to Communication Standard Interface bus, the characteristics of the IIoT (Industrial Internet of Things) object and the correspondence between a server's address space and the address space of MCIP.**

***Keywords*—SCADA; OPC DA; OPC.NET; OPC UA; DDS**

I. Introduction

SCADA (Supervisory Control and Data Acquisition) systems are those hardware/software systems that allow data acquisition from sensors or field devices used in the industrial process monitoring and control, and also allow the transmission of command/instructions to the remote field devices or actuators [1].

SCADA systems are usually distributed applications on a local network or WAN. The main elements of the SCADA architecture and security are presented in [2]. Usually in process control, the typical information architecture is hierarchically organized. A simplified model contains the following levels: process and business management; process control; management of field devices. These levels are not clearly defined, but the vertical communication up to the process component level is always necessary.

This communication requires solving the following requirements: to provide an adequate level of reliability; to comply with the time limits for delays; to support a diverse communication infrastructure; to use the standards specific for the producers in order to access the data from the process; the communication architecture must use open solutions (independent of the producers) for further development; to provide a uniform model for data presentation. An innovative idea is to solve the problem of system integration using a homogeneous architecture and a real-time process level.

The architecture must be based on the international standards for data exchange which allow data sharing from the devices placed on the hierarchical levels of the enterprises by the control and management systems of the processes. This architecture is a virtual level model which offers an overview of the underlying process level consisting of data units accessible randomly by means of a standardized and unified interface. As a result, the structure of the links becomes systematic and, more than that, the superior levels can be preserved.

The architecture must also ensure an optimum transfer of data based on a simple but generally accepted rule that the most important data must be transferred only once at any given time. To achieve this goal, the acquisition of the data contained by the process must be performed using appropriate communication technologies. This functionality is very important in order to achieve communication in the systems using remotely-controlled terminals spread over a large geographical area, such as heat and electricity meters.

Examples of such overall architectures were presented in [3] and [4] for the Classic OPC based on architecture for servers starting from standards [5] and [6] and in [7] based on a general architecture for servers named OPC Unified Architecture (OPC UA) [8].

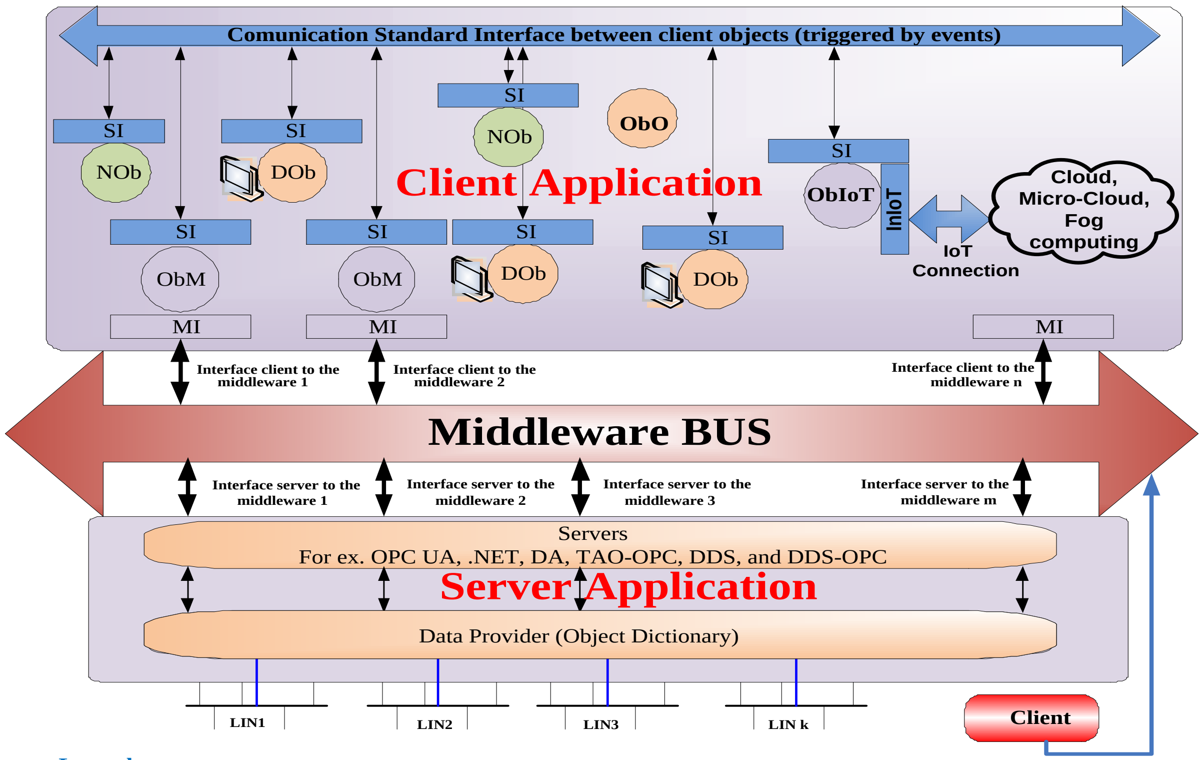
An idea related to the standardization of the data is the use of gateways which work in real time and which standardize the access to various local industrial networks that implement different algorithms [9][10].

The MCIP application, originally submitted in [11], is object-oriented, the objects implementing the standard interface of the client application which allows the communication between the application objects. In addition to this standard interface, each object may implement other interfaces for the communication with other applications (middleware interface) or user interaction (graphical interface). The acronyms MCPI (Monitoring and control industrial processes) in [11] and MCIP are equivalent.

Further, this article is structured as follows: Section II presents the client application and its objects, in Section III the processing triggered by events is presented, Section IV presents the IoT (Internet of Things) object, Section V presents the future development of the proposed solution. The conclusions are drawn in Section VI.

II. THE MCIP CLIENT APPLICATION AND ITS OBJECTS

This application was developed to allow the monitoring and control of the industrial processes. The MCIP application is an executable software module which is part of a complex architecture (see Fig.1). MCIP has the following types of objects: ornament objects (background or fonts for windows or objects), graphical objects (display values from other objects or expressions with values from other objects – window, scale, trend, button, input box, etc.), expression-type objects which produce value based on the evaluation of an expression that has as an input values from other objects, middleware-type objects which have two interfaces, one with the MCIP application's internal bus and one with a middleware bus (the bus has well defined API functions, see Fig. 1), a middleware interface specific for a server (OPC UA, .NET, Classic, TAO_OPC and DDS_OPC) and the Internet of Things-type objects such as DDS (ObIoT from Fig. 1). The TAO_OPC and DDS_OPC servers are based on a set of interface functions defined by the OPC DA 2.05 specification, while the middleware is specific (CORBA for TAO_OPC and DDS for DDS_OPC). The items marked in italics surpass the MCPI described in [11]. The middleware objects define the MCIP application's local address space, while the DDS server defines the MCIP application's global space IIoT.



Legenda

NOb - Normal Object **DOb** - Display Object **ObM** - Object interface to middleware
SI - Standard Interface **MI** - Middleware Interface **ObIoT**- Object Internet of Things
LIN - Local Industrial Network **InIoT** - Industrial Internet of Things **ObO** - Object Ornamental

Fig. 1. The architecture of the MCIP application

When designing the client application, the following important features were taken into account from the beginning:

- The MCIP application is fully object-oriented. By object we understand, in its most general meaning, a software module with internal functioning, which has a set of input sizes - binary or analogue, internal memory and a set of output sizes - binary or analogue, resulting from internal processing.
- The objects' space is called Project. In a project there can be several window-type objects, depending on the application's complexity.
- The mcip.exe application supports a single project. If more than one project needs to be implemented, more mcip.exe applications will be left running.
- Only within a project can all the objects communicate among themselves.
- Only the middleware-type objects, OPC (Classic, NET and UA), TAO_OPC (The ACE (Advanced Collaborative Environment) ORB), DDS_OPC (Distributed Data Services) and DDS can create the connection to the data servers, histories and alarms and events.

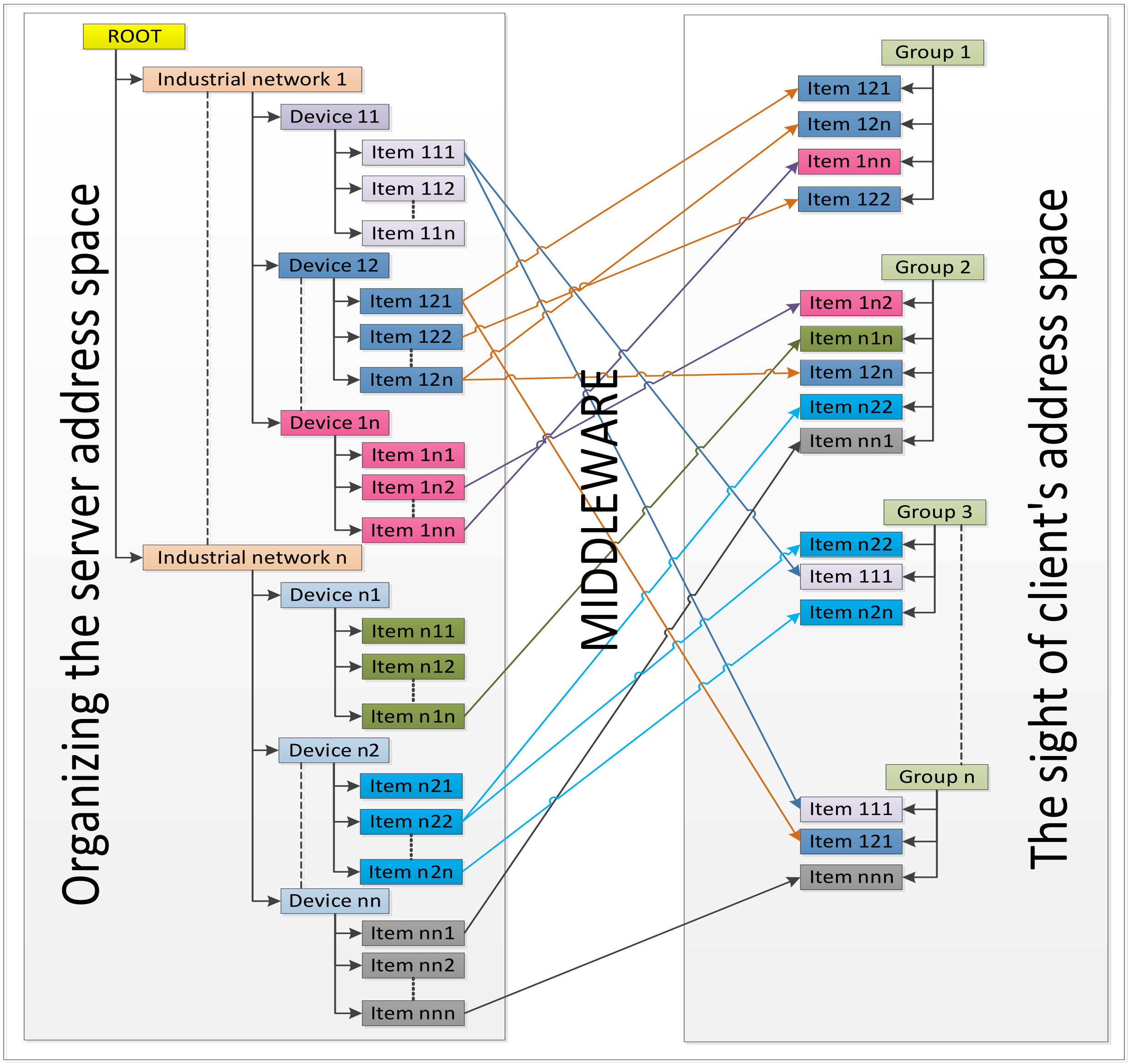


Fig. 2. The correspondence between the server's address spaces and MCIP

The middleware objects are designed to create groups with common features (only pressures, only temperatures, a complete installation, a control loop with parameters and the connected orders, etc.) or any type of group depending on the user's needs.

- A middleware object can be connected to a single server placed on the same computer as the application or on another computer in the network.
- A value exposed (supplied) by the server can be taken up by any number of local middleware objects (from the same computer) or placed at a distance.
- The MCIP application is secured with a set of passwords which allow only its use or both its use and modification.
- The MCIP application has two working modes, namely:
  - ✓ The *editing mode* when it is disconnected from the servers and it allows the implementation or modification of the project, and
  - ✓ The *execution mode*, when the application runs what it was designed to run.
- The mcip.exe application has a basic set of objects to which, by loading some dynamic *.dll type libraries, one can add other objects supplied by the producer or objects can be added on demand or programmed by the user. This is possible because the objects have a standardized interface.

A. The objects of the MCIP application

As shown in Fig. 1, objects always have a standard interface but they can also have other ones such as the interfaces with the servers described and a user-defined interface. From this point of view, we can distinguish the following types of objects: a) general form, producer-consumer object; b) empty object (text or image); c) an object which is only a producer; d) an object which is only a consumer. The graphical objects always have an expression in the form of text or image in the window. For non-graphical objects, it is not mandatory for their expression in the window to be text or image (they are hidden). The software module attached to the object runs only when the trigger is activated which is achieved only on events (for example, changing the value of a quantity).The MCIP application consists of an ensemble made up of a project, objects and connections, the user's being to create, configure, and connect the objects among together. In this subsection, the objects made available by the application (the MCIP client) will be presented. A project is a group of independent or interconnected objects. The user creates projects (separate MCIP applications) in order to perform certain tasks. The user can open and close projects without affecting the other projects running in parallel. Each object will have among its resources the parameter setup window and other windows needed to display the object's information and configuration. It is possible for an object to have multiple functions (for example, an object which can calculate either the minimum or the maximum for a given input variable). The middleware-type objects are the only objects which allow the connection to the middleware servers. Because the architecture of the MCIP application is based on objects and on the connections between objects, once a middleware objects is created, any other object within a project will be able to connect to it. These objects can be graphic displays, control objects through which the human operator has access to the process values.

This is the usual mode of communication with the physical devices part of the process, but, if necessary, communication objects internal to the application can be developed (for serial communication, Ethernet, wireless – with specific interfaces). Each object has the "BaseObject" interface and can optionally have a middleware or a specific interface.

The entirety of a project's objects forms the project's address space which will always be displayed in the window named "Manager of objects". There is an exception here, namely that the graphical objects, those displaying a text or image, are not included in a project's address space being managed only as information display elements at window level (those objects which do not produce outputs and, therefore, to which other objects cannot connect).

The user will be able to create multiple windows in the same project and will be able to connect the objects from the same window or different windows but will not be able to connect objects belonging to different projects. The client application will allow the users to access take over and manage the data displayed by the server. The user will be able to view and browse the server's address space, creating groups which will contain a series of items available at this address space.

In other words, the customer will create his own vision of the address space exhibited by the server. This concept is illustrated in Fig. 2.

B. The user object

What is represented in Fig. 3 is an object adaptor (an instance of a class) to which a base object is attached which implements the standard interface), when created by the user. Under this form can the objects from the application's object directory be found (of the project) [11]. This is an artifice for the implementation of the connections between objects, because the object's common functionalities would have otherwise implemented themselves repeatedly in each base object's case. The adapter automatically attaches the client application whenever an object is created and, as a result, at the dll level which implements new base objects, only the standard interface must be implemented (CSI – Communication Standard Interface of the Object Client).

The directory of the user objects is a set of objects and subdirectories used to group the project's user objects in various categories. It will handle the management of the component user objects. It consists of:

- List of directories;
- List of user objects.

The connection. Objects can be interconnected, allowing signals to pass from one object to another. Thus, an object's data members can connect to the data members of another object. A connection is described by the following information:

- A data member/alias handle which has connections (that enter into an expression associated with a parameter, or to which another object's data member is connected (directly or through an expression), or which is displayed on a form (directly or through an expression);
- A list of objects to be notified when the above-mentioned data member/alias changes. Each listed item will be a structure containing an object handle and a handler list of data members or parameters to be notified for that object.

User object name. Each object must have a unique name within the project/directory (each object will belong to a project/directory). The name of the object will be indicated in the properties window, from where the parameters will be configured. A set of rules must also be defined and must be followed in order to give an object a name.

Alias. An alias for a data member is a generic name which can be used in a project even if the connection with other objects has changed (even if used a thousand times, there is no need to change the name in a thousand places in the project). It contains information such as:

- Data member handle;
- Alias name (optional). If a name for the alias is given, it creates a new instance of the data member. Afterwards, the alias can be configured with a different configuration from that of the original data member. The aliases are used to isolate the process from the

hardware changes. Thus, supposing that for a multichannel indicator, called IUM04, IUM04.Ch1 (Channel 1) has the alias Pressure and that everywhere in the process it is referred to through this alias instead of the data member, as IUM04.Pressure. Later, for some reason, the pressure is acquired on Ch2 (Channel 2). In this case, the alias will simply be changed to refer to IUM04.Ch2 instead of IUM04.Ch1. If only the parameters are changed and a name for the alias is not given, all the connections towards the data member will take into account these parameters.

- Description;
- The following information depends on the data type of the data member for which the alias is given:
  - ✓ Numeric: linear scaling from one domain to another; deviation – in order not to take into account the insignificant variations of the data members (if the difference between the last and the current value does not exceed the deviation, it is considered that the amount did not change); a forced value – the data member will have this value no matter what happens in the process. Usually, it is used when a sensor breaks or when a sensor is being repaired, or when a PLC receives erroneous signals.
  - ✓ Logic: The possibility of reversing the logic signal.
  - ✓ Text: It has no additional particularity.

Attribute. The generic term of attribute will be used for any parameter, data member or alias of a base object. Where this term appears, when it does not refer to all the properties, what it refers to will, in principle, be listed (for example, through an attribute only the parameters and the data members can be determined in certain contexts). Attribute = data member = properties.

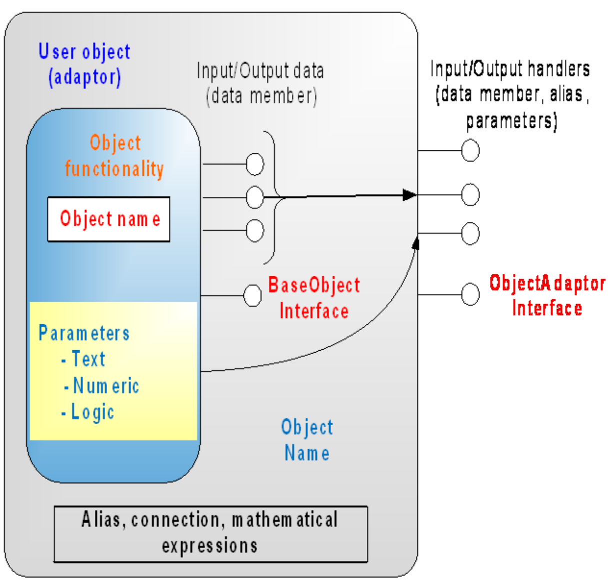


Fig. 3. The architecture of the user object

C. *The interface of the object implemented in dll*

To access the object implemented in the dll a standard interface is defined. The term object described above in the terminology section refers to an object in the project which is actually an adapter for the object in dll (because, for an object, additional information is needed – aliases, filters, connections – which do not need to be doubled, tripled in dlls). A standard interface will be created (or a base class containing all the virtual methods) to be implemented by all the objects defined as independent components in dlls and by the possible objects implemented in the application. The code implementation has been done in C#. For the fast access to the information about the data member and about the reading and writing methods of the data members, a Hash table is used. The objects within the hash tables are name_data_member–object_type_MemberInfo pairs. For each data member exposed by the by the current object, there will be a pair in the hash table.

III. Processing Triggered by Events

At process level, the code is only executed when an event is activated. The characteristics referring to the events are as follows:

- The functioning of the client application is entirely driven by events.
- A particular code sequence is executed only when an input variable changes.
- The execution of the code in an infinite loop is avoided in order to save processor time.
- The update loops are avoided (the events which generate themselves recursively).
- Each object remains inactive until an event occurs on one of its connections.
- When an input signal changes, the object processes the value according to the internal logic (given by the type of object).
- The objects emit events only when the processing result has changed.

This application's approach will consume much less processor time than a solution based on waiting in a loop until the input signal changes.

IV. IoT Objects

Several current technologies have revolutionized everyday life. One of them is the Internet that has led to a new era of information, available for everyone. Other technologies, such as Radio-Frequency Identification (RFID), or Wireless Sensors Network increased the ability to communicate among things. Internet Protocol Version 6 (IPv6) removed the address depletion problem existing in the Internet Protocol (IPv4). In this context, it is only natural that the next wave in the development of the Internet does not refer to people, but to interconnected smart devices. The mobile revolution, with more than 5 billion smart phones connected to various mobile networks, provides the population with the possibility to access the Internet.

DDS RTS (Data Distribution Service for Real-Time Systems) is a middleware standard based on the publish/subscribe paradigm for distributing data between heterogeneous applications developed by OMG consortium [12]. An important feature of this protocol is that it has facilities for implementing QoS (Quality of Service) parameters in order to achieve real-time performance. It is also data centric and allows the anonymous dissemination of information. Due to real-time facilities, this protocol is used in critical systems to the detriment of OPC based solutions. An interesting comparison between DDS and OPC can be found in [13]. There are several open source implementations of the DDS standard [14], namely OpenDDS and OpenSpice, and commercial implementations, for example, RTI-DDS.

The DDS standard can be used in two ways: as an object in the MCIP application and as a "DDS server" type application which instantiates the data provider. For both versions, the IDL interface is used, in which the topics to be published are defined. For this reason, data can be transmitted between the MCIP applications, between the DDS server applications or between the MCIP applications and the DDS servers. In MCPI, the DDS object actually creates an interface between the DDS topics defined in IDL and in the MCIP internal communication bus and in the DDS server an interface is created between the API provided by the data provider and the DDS topics defined in IDL. The DDS will define the IoT workspace.

The OpenDDS object is currently in the development and implementation stage. This object will expose the address space of the DDS domain in the MCIP environment on which it can connect. Each instance of the OpenDDS objects can connect to only one DDS domain in terms of available QoS parameters. In order to develop this object, the OpenDDS implementation of the DDS standard was chosen because it is an open-source solution and it is developed based on the TAO middleware.

V. Conclusion

In this article, we have detailed aspects related to the MCIP client. Thus, new MCIP objects were defined, the adapter structure for user objects was presented, and a new object was added which allows it to connect to the IIoT-type (Industrial Internet of Things) applications. The object is based on the DDS protocol from OMG because of the existence of a free implementation called OpenDDS.

VI. Future Work

In the future, other IoT-type objects based on protocols will be taken into account such as XMPP (Extensible Messaging and Presence Protocol, AMPQ (Advanced Message Queuing Protocol), MQTT (Message Queuing Telemetry Transport (MQTT), OPC UA (OPC Unified Architecture), REST (Representational State Transfer) and, CoAP (Constrained Application Protocol).

Acknowledgment

This paper was partially supported from the project „Integrated Center for research, development and innovation in Advanced Materials, Nanotechnologies, and Distributed Systems for fabrication and control", Contract No. 671/09.04.2015, Sectorial Operational Program for Increase of the Economic Competitiveness co-funded from the European Regional Development Fund..

References

[1] S. A. Boyer, SCADA: supervisory control and data acquisition, 4rd ed., International Society of Automation, ISBN-10: 19360070962009, June 15, 2009.

[2] R. Krutz, Securing SCADA Systems, ISBN-10: 0-7645-9787-6, Wiley, 2006.

[3] Nicoleta-Cristina GĂITAN, Vasile Gheorghiţă GĂITAN, Ştefan Gheorghe PENTIUC,Ioan UNGUREAN, Eugen DODIU, Middleware Based Model of Heterogeneous Systems for SCADA Distributed Applications, pag. 121-124, ISSN: 1582-7445 e-ISSN: 1844-7600, Advances in Electrical and Computer Engineering Volume 10, Number 2, 2010.

[4] Iwanitz, Franz şi Lange, Jurgen. OPC - Fundamentals, Implementation, and Application, third rev. Ed. [ed.] Softing. 3. Munich : Huthig, ISBN 3-7785-2904-8, 2005.

[5] OPC Foundation - DA 3.0. 2003. OPC Data Access Custom Interface Standard Version 3.0. 2003.

[6] OPC Foundation- DA 2.05. 2002. OPC Data Access Custom Interface Standard Version 2.05. 2002.

[7] Lange, Jurgen, Iwanitz, Frank şi Burke, Thomas J. 2010. OPC From Data Access To Unified Architecture. [ed.] Softing. Berlin : VDE VERLAG GMBH,ISBN 3-978-3-8007-5, 2010.

[8] OPC Foundation: Home Page, https://opcfoundation.org/

[9] V.G. Gaitan, N. C. Gaitan, I. Ungurean, A flexible acquisition cycle for incompletely defined fieldbus protocols, ISA Transactions, Volume 53, Issue 3, Pages 776-786, ISSN 0019-0578, http://dx.doi.org/10.1016/j.isatra.2014.02.006, May 2014.

[10] Gaitan, N. C. Real–time Acquisition of the Distributed Data by using an Intelligent System. Electronics and Electrical Engineering.–Kaunas: Technologija 8 (2010): 104, 2010.

[11] Vasile Gaitan, Valentin Popa, Nicoleta Cristina Gaitan, Mihai Gabriel Danila, A scalable Human-Computer Interaction (HCI), Proceedings of ED-MEDIA 2008 – World Conference on Educational Multimedia, Hypermedia & Telecomunications, , pag. 1522-1527, ISBN 1-880094-62-2, Viena, Austria, (http://www.editlib.org/), June 30- July 4 2008.

[12] Object Management Group, http://www.omg.org/ H. Perez, J.J. Gutierrez, "A survey on Standards for real-time distribution middleware" Journal ACM Computing Surveys, vol. 46, issue 4, March 2014.

[13] Comparison of OPC and DDS – RTI, https://www.rti.com/docs/RTI_DDS_and_OPC.pdf.

[14] Best-Practices Data-Centric Programming: Using DDS to Integrate Real-World Systems, https://www.rti.com/docs/DDS_Best_Practices_WP.pdf.

Intrusion Detection Techniques in Wireless Sensor Network using Data Mining Algorithms: Comparative Evaluation Based on Attacks Detection

YOUSEF EL MOURABIT
Equipe Signaux, Systèmes et Informatique (ESSI)
National School of Applied Sciences, Ibn Zohr University
AGADIR, MOROCCO

ANOUAR BOUIRDEN
Laboratoire Thermodynamique et Energétique
Faculty of Sciences, Ibn Zohr University
AGADIR, MOROCCO

AHMED TOUMANARI
Equipe Signaux, Systèmes et Informatique (ESSI)
National School of Applied Sciences, Ibn Zohr University
AGADIR, MOROCCO

NADYA EL MOUSSAID
Equipe Signaux, Systèmes et Informatique (ESSI)
National School of Applied Sciences, Ibn Zohr University
AGADIR, MOROCCO

***Abstract*—Wireless sensor network (WSN) consists of sensor nodes. Deployed in the open area, and characterized by constrained resources, WSN *suffers* from several *attacks, intrusion and security vulnerabilities.* Intrusion detection system (IDS) *is one of the essential* security mechanism against attacks in WSN. In this paper we present a comparative evaluation of the most performant detection techniques in IDS for WSNs, the analyzes and comparisons of the approaches are represented technically, followed by a brief. Attacks in WSN also are presented and classified into several criteria. To implement and measure the performance of detection techniques we prepare our dataset, based on KDD'99, into five steps, after normalizing our dataset, we determined normal class and 4 types of attacks, and used the most relevant attributes for the classification process. We propose applying CfsSubsetEval with BestFirst approach as an attribute selection algorithm for removing the redundant attributes. The experimental results show that the random forest methods provide high detection rate and reduce false alarm rate. Finally, a set of principles is concluded, which have to be satisfied in future research for implementing IDS in WSNs. To help researchers in the selection of IDS for WSNs, several recommendations are provided with future directions for this research.**

Keywords—Keyword: Wireless sensor network; Anomaly Detection; Intrusion detection system; classification; KDD'99; Weka

I. INTRODUCTION

Wireless sensor networks are composed of several sensors deployed in areas where the aim is to collect data and forward it for the analysis. It has become an increasingly interesting field of research in solving such challenging real-world problem, as environmental monitoring [1], military applications, geographical sensing, traffic control, and home automation. The properties of WSN show that that sensor node is completely restricted by resources, including memory, energy, computing, communication and bandwidth. [2]. Therefore, the deployment of these kinds of networks with their resource restrictions makes their security issue essential, and vulnerable to various security threats. Key management and authentication have been used to protect WSNs from different attacks, encryption and authentication are the first security measures as the first line of defense for protecting WSN [3]. But cryptography based on secret key management are not enough to protect the WSN, because even in the presence of this first line of defense, several attacks may extract sensitive information, and use them for malicious reason. However, Detection-based approaches are then proposed to protect WSNs from intrusion and attacks, as a second line defense, after the failure of the cryptographic techniques [4], Intrusion detection system (IDS) observes and analyzes the events generated in the network system to identify maximum security problems. IDSs are used to monitor the network to detect anything unusual. [5]. This concept was originally proposed by Anderson [6]. There are two principal approaches for detection, intrusion: Misuse detection based on rules, these rules will look for signatures on the network and then system operations try to catch known attack that should be considered as Misuse [7] [8]. Anomaly detection [9], which based on the normal behavior of a system, it compares normal activities against observed events to identify significant deviations. The main scope of this paper is to improve that random forest technique is an efficient anomaly detection technique for IDS in WSN, with a comparative evaluation study for the most recent and performants anomaly detection technique used in IDS for WSN. In Section 2 we present a classification of existing attacks in WSN by several criteria. Section 3 introduces a survey of ids in WSN, and analyzes four recent anomaly intrusion detection techniques using in IDS for WSN: (K-means, Naives Bayesian, SVM, Random Forest), showing their principles, advantages and drawbacks.

Simulation environment and results are presented in section 4, we simulated last techniques on KDD dataset using Weka tool, and results are based on matrices of confusion, detection rate, time of execution and memory consumption. At the end of the paper a conclusion is introduced, and a set of recommendations are suggested to boosting the performance of intrusion detection in WSN for future researches.

II. Attacks Classification in WSN

An attack is a set of techniques, used to cause damage to a network by exploiting flaws in it. Attacks know several possible classification, the most used are grouped into the following categories:

A. According to the origin or source attacks:

Two categories are distinguished: internal and external attacks: An external attack is triggered by a node that does not belong to the network or does not have access permission. The aim of this attack is to cause congestion in the network, the spread of incorrect routing information, or completely close the network. The internal attack is done by a malicious internal node. Defense strategies generally aim to protect the network against external attacks. However, internal attacks are the most serious threats that can disturb the WSN [10][11].

B. Based on the nature of attacks:

We can distinguish between passive and active attacks, the passive attack is limited to listening and analyzes exchanged traffic. This kind of attacks is difficult to detect and easier to realize, because the attacker does not make any modification on exchanged information.

The aims of the attacker can be the knowledge of the significant nodes in the network (cluster head node), or knowledge of confidential information by analyzing routing information. In the active attacks, an attacker tries to modify or remove the messages transmitted on the network, inject his own traffic or replay of old messages to disturbing the operation of the network. [12].

C. Classification by attacks techniques:

The spoofed, altered, or replayed routing information attack, and sinkhole attack: need to make a probe step before starting to attack, thereforeattack we can classified these attack as probe attacks. Selected forwarding, jamming, tampering: which uses illegitimate data forwarding to make attack, is known as a dos attacks? Hello floods caused by internal attacks, is classified as U2R attack. Sybil, wormholes, hello floods, and acknowledgment spoofing make the attack through the weakness of the system then they would be classified as R2L attack. In the table below we present the following main types of attacks, sorted by four principals attack classes.

TABLE I. ATTACKS CLASSES

Attack class	Attack techniques
Probe	Spoofed Routing Information attack, Altered Routing Information Attacks, Replayed Routing Information, Sinkhole
DOSS	Selected Forwarding, Jamming, Tampering
U2R	Hello Floods
R2L	Sybil, Wormholes, Achnowledgement Spoofing

D. According to the various protocol layers and proposed mechanism defense:

The following main types of attacks, are sorted by their assignments to the relevant layers of the protocol stack. For each attack, a list of proposed mechanism defense is presented [13][14]:

TABLE II. ATTACKS, PROTOCOL LAYER AND DEFENSE MECHANISM

Protocol layer	Attacks	Defenses
physical	Jamming	Priority messages, monitoring, authorization, redundancy, encryption[14] Spread-spectrum, priority message, lower Duty cycle, region mapping, mode change Tamper-proofing, hiding
	Tampering	
Data link	Collision	Error-correction code
	Exhaustion	Rate limitation
	Unfairness	Small frames
network	Spoofed, Altered or relayed routing information	Detection on MintRoute[4]
	Selective forwarding	
	Sinkhole	
	Sybil attack	Identity certificates[11]
	Wormholes	Dawwsen proactive routing rotocol[13] suspicious node detection by signal strength,[10]
	Hello flood attacks	Suspicious node detection by signal strength[10]
	Achnowledgment spoofing	Encryption,authentication, monitoring
Transport	Flooding	Client puzzles
	De-Synchronization	Authentication

III. Related Work

It has become clear that we cannot achieve the satisfactory level of security in WSN only by using cryptographic techniques, as these techniques fall prey to insider attacks. The attacker can compromise and retrieve the cryptographic material of a number of nodes [15]. In order to counter this threat some additional techniques such as intrusion detection system (IDS) has to be deployed. Any kind of unauthorized or unapproved activities are called intrusions. An IDS is a collection of the resources, methods and tools to help identify, evaluate, and report intrusions [16]. WSN led researchers develop strategies about providing stable networking and communications, and also about how to secure these strategies with limited resources.

In [17], a hierarchical framework for intrusion detection as well as data processing is proposed. Throughout the experiments on the proposed framework, they stressed the significance of one hop clustering. The authors believed that their hierarchical framework was useful for securing industrial applications of WSNs with regard to two lines of defense. Krontiris et al. [18] proposed a distributed IDS for WSNs based on collaborative neighborhood watching. In a simulation environment, the authors evaluated the effectiveness of their IDS scheme against blackhole and selective forwarding attacks. In [19] provided an IDS for WSNs that was based on detection of packet level receive power anomalies. The detection scheme was focused on transceiver behaviors and packet arrival rates of the neighboring nodes of a particular node. In [20], a distributed cluster based anomaly detection algorithm was proposed. They minimized the communication overhead by clustering the sensor measurements and merging clusters before sending a description of the clusters to the other nodes. The authors implemented their proposed model in a real-world project. They demonstrated that their scheme achieves comparable accuracy when compared to centralized schemes with a significant reduction in communication overhead. The table below presents a brief list of constraints and the corresponding requirements of IDS in WSN:

TABLE III. IDS REQUIREMENT FOR WSN

Constraints and challenges of WSN	Requirement of IDS
• *N*o infrastructure in WSNs to support operations such as communications, routing, real time traffic analysis, encryption, etc. • Nodes are prone to physical capture, tampering or hijacking which compromises network operations. • Compromised nodes may provide misleading routing information to the rest of the WSN leaving the network un-operational (blackhole, wormhole, sinkhole attacks). • Wireless communication is susceptible to eavesdropping, which would reveal important data to adversaries and/or to jamming/interfering, which would cause DoS in the WSN. • There is no trusted authority; decisions have to be concluded in a collaborative manner.	• *N*ot introduce new weaknesses to the system, • Need little system resources and should not degrade overall system performance by introducing overheads, • Run continuously and remain transparent to the system and the users, • Use standards to be cooperative and open, • Be reliable and minimize false positives and false negatives in the detection phase.

There are two basic approaches in IDS according to the used detection techniques [21]:

Misuse detection technique compares the observed behavior with known attack patterns (signatures). Action patterns that may pose a security threat have to be defined and stored in the system. The advantage of this technique is that it can accurately and efficiently detect instances of known attacks, but it lacks an ability to detect an unknown type of attack.

Anomaly detection: The detection is based on monitoring changes in behavior, rather than searching for some known attack signatures. Before the anomaly detection based system is deployed, it usually must be taught to recognize normal system activity (usually by automated training). The system then watches for activities that differ from the learned behavior by a statistically significant amount. The main disadvantage of this type of system is high false positive rate. The system also assumes that there are no intruders during the learning phase.

Anomaly may be caused by security threats, or faulty sensor nodes in the network or unusual phenomena in the monitoring zone [22]. Isolated node failures can bring down the whole network, which is malicious to reliability of WSN. Researches in this field are yet absent to present the latest progress of developing anomaly detection in WSN. However, our paper expects acting as a guideline of selecting efficient and appropriate anomaly detection techniques, not just based on analyzing, comparing, and evaluating those particular approaches, but also according to the results of simulation, which shows the classification rate, confusion matrix, consumption of memory, and time to build every approach.

IV. RSTUDY ANALYSIS AND EVALUATION OF ANOMALY DETECTION TECHNIQUES IN WSN

A. *Clustering approach*

With K-means clustering algorithm, Rajasegarar et al [20] design a distributed detection scheme. Each common sensor node locally collects the input dataset to work out a normal profile. Then the cluster head collects all local normal profiles to accomplish the procedure of data processing, where a global normal profile is produced. After received the global normal profile, each common sensor node initiates the analysis and decision procedure to perform detection. In order to fit in distance-based clustering, the input dataset is normalized at each common sensor node with a preprocessing procedure.

Given a dataset v_{kj} , k=1…m, it is transformed to $u_{kj=(v_{kj}-\mu_{vj})/\delta_{vj}}$

Where μ_{vj} and δ_{vj} stand for the mean and standard deviation of the jth attribute in v_{kj}. Subsequently u_{kj} is normalized in the interval [0,1], according to

$$\overline{u}_{kj} = (u_{kj} - minu_j)/(maxu_j - minu_j).$$

Given a common sensor node s_i collecting a dataset X_i, s_i sends the local normal profile.

$$(\sum_{k=1}^{m} x_k^i \sum_{k=1}^{m} (x_k^i)^2, m, x_{max}^i, x_{min}^i)$$

to the cluster head, where m stands for $|X_i|$. After the global normal profile is computed,

$(\mu_j, \delta_G^2, x_{max}^G, x_{min}^G)$. The cluster head sends it back to the common sensor nodes. After receiving the global normal profile, each common sensor node initiates detection locally, using a fixed-width clustering algorithm. If the Euclidean distance between a data point and its closest cluster centroid is larger than a user-specified radius o, a new cluster is organized with this data point as centroid. For reducing the number of resulting clusters, a cluster merging process is then conducted, through measuring the inner- cluster distances[35]. The clusters c1 and c2 merge if their inner- cluster distance d(c1,c2) is less than o. Finally, the average inter- cluster distance of K nearest neighbor (KNN) clusters is applied to identify anomalous clusters. Let ICDi be the average inter-cluster distance (KNN) of cluster i, AVG (ICD) and SD(ICD) be the mean and standard deviation of all inter-cluster distances respectively. If : ICDi>SD(ICD) + AVG(ICD), cluster i is viewed as anomalous[35].

B. Support Vector Machine Classifier

Support Vector Machines (SVMs) are supervised learning algorithms [24], which have been applied increasingly to anomaly detection in the last decade. One of the primary benefits of SVMs is that they learn very effectively from high dimensional data [25]. In WSN SVM is used to investigate spatial and temporal correlations of data for detecting suspect behavior of a node. Many researchers have tried to find possible methods to apply SVM classification for large data sets. Sequential Minimal Optimization (SMO) is a fast method to train SVM [26], which breaks the large Quadratic Programming (QP) problem into a series of smallest possible QP problems. In [27] Kim et all applied SVMs to host based anomaly detection of masquerades. One-class quarter-sphere SVM, as a representative algorithm of SVM, is also suited to distribute anomaly detection [28]. First, the local quarter-sphere is computed at each common sensor node. Second, the cluster heads collects these locally computed radii to work out a global radius. Detection is then launched at each common sensor node with the global normal profile.

C. Naïve Bayes Classifier

The naive Bayes classifier is usually used in WSN because of its simplicity, elegance, and robustness. A large number of modifications have been introduced, by the statistical, data mining, machine learning, and pattern recognition communities, in an attempt to make it more flexible. Novel approach was proposed in [29] to identify the faulty sensor node using Naïve Bayes classifier. The proposed Naïve Bayes framework was deployed for performing WSN faulty node(s) detection. A new attribute, the end-to-end transmission time of each packet arrived at the sink is analyzed using Naïve Bayesian classifier for determining the network status. This technique doesn't involve any additional protocol and extra resource consumption of sensor node, it suggests a list of suspicious faulty nodes to the user [29]. In the same context, based on mobile agent and using naïve Bayesian classifier an IDS is presented in [23]. The figure below presents the principal of naive Bayesian classifier.

m Number of classes C1, C2,….,Cm

d_{ct} Dimentional vector for class t d_{ct}= {dct1,dct1,…….,dctn} where $\sum_i d_{cti}$=1

K total ksenses of network operation S = {S_1, S_2,….., S_k}

S_1 Is a product of the data that appear in the scene:

$$P(S_1|d_{ct})=\frac{(\sum_i N_i)!}{\prod_i N_i!}\prod_i (d_{cti})^{N_i} \qquad (1)$$

Where N_i is the number of data I in sceneS_1.

$$L= \arg max_c\ [\ \log P(D_{ct})+\sum_i N_i\ log d_{cti}] \qquad (2)$$

D. Random Forest Classifier :

Random forests are based on collection learning method for classification, that operate by constructing a multitude of decision trees, at training time and outputting the class, that is the mode of the classes output by individual trees. Random tree, on the other hand, involves construction of multiple decision trees randomly [30]. Each tree is constructed using the following algorithm:

Step1: Let the number of training cases be *N*, and the number of variables in the classifier be *M*. ***Step2***: We are told the number *m* of input variables to be used to determine the decision at a node of the tree; *m* should be much less than *M*. ***Step3***: Choose a training set for this tree by choosing *n* times with replacement from all *N* available training cases (i.e. take a bootstrap sample). Use the rest of the cases to estimate the error of the tree, by predicting their classes. ***Step4***: For each node of the tree, randomly choose *m* variables on which to base the decision at that node. Calculate the best split based on these *m* variables in the training set. ***Step5***: Each tree is fully grown and not pruned (as may be done in constructing a normal tree classifier). A novel data mining approach based on random forests was proposed to characterize and classify a similar large scale physical environment in [31]. The proposed data mining formulation, allows better performance in terms of tradeoff between energy efficiency and accuracy. Compared to a single decision tree algorithm, RFs runs efficiently on large datasets with a better performance. In [30] Random Forests (RF) is used as a classifier for the proposed intrusion detection framework. RF gives better performance in designing IDS that is efficient and effective for network intrusion detection. the advantages and inconveniences of the studied techniques are presented in the following table:

TABLE IV. ADVANTAGES AND INCONVENIENCIES OF STUDIED TECHNIQUES

approach	advantages	inconveniences
K-means	-Fast and easier to understand. -Gives best result when data set are distinct.	-Sensitive to initialization -Low detection accuracy
Naïve-bayes	-Low computation complexity -High detection accuracy	-Increased communication overhead required for sending full data from common nodes to cluster heads. -Central point of failure as anomalous detection is accomplished only at cluster heads
SVM	-No central points of failure, all nodes have the same capability of detection -Reduced energy consumption by transmitting support vectors between nodes instead of all captured data	There must be an efficient way to select relevant features instead of delete one at a time and rank the important one the biggest limitation of the support vector approach lies in choice of the kernel
Random Forest	-Runs efficiently on large databases -Provides effective methods for estimating missing data -High detection accuracy and low false positive rate.	have been observed to over fit for some datasets with noisy classification/regression tasks the variable importance scores from random forest are not reliable for all types of data

V. EXPERIMENT RESULTS

A series of experiments were conducted to simulate and evaluate each approach, to define the efficient detection technique for ids in WSN. We used several critical evaluation metrics: Confusion matrix, general classification rate, time to build model, memory consumption. We prepared our data set, based on the standard KDDCup'99 intrusion detection dataset [32], into following five step, using Weka tool:

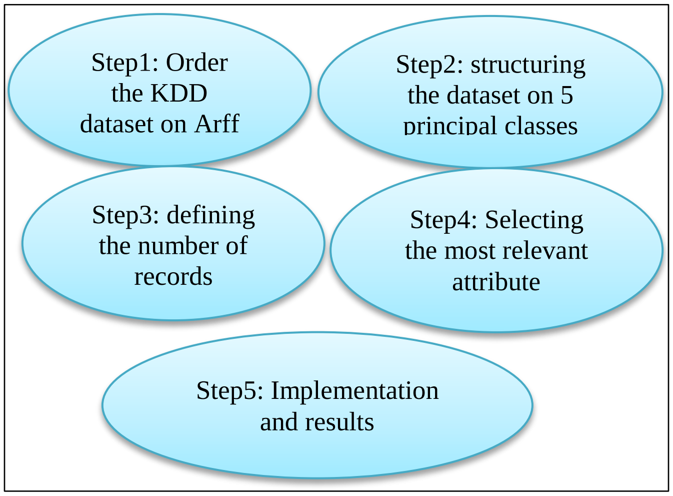


Fig. 1. Preparing dataset steps

Step1: in this step we structured all records on Attribute-Relation File Format (ARFF), which is an input file format used by the machine learning tool WEKA [33].

Step2: In this step we classed all types of attacks, on four principal categories. As shown the table [2].

Step 3: the main aims of this step is defining the number of records treated for each class as presented in table below, we used 70% in training stage and 30% in the test stage for each class.

TABLE V. NUMBER OF RECORDS

Class	Instances Number
Normal	10233
Dos	41748
Probe	441
R2L	96
U2R	92

Step4: In general, a characteristic is good if it is relevant to the concept of class but not redundant to one of the other functions. Reduction of the attributes is a process of choosing a subset of the original attributes which feature space is reduced optimally at an endpoint.

In our experiment, Weka tool is used for reduction function. **CfsSubsetEval** with **BestFirst** approach is applied to the set of training data to obtain the relevant features for the classification process. Each subset was analyzed using correlation analysis to identify important features. The best known Measuring correlation is the linear correlation coefficient. For a pair of variables (x, y), the linear correlation coefficient r (x, y) is given by the expression below:

$$r(x,y) = \frac{n\sum xy - \sum x \sum y}{\sqrt{(n\sum x^4 - (\sum x)^4)(n\sum y^4 - (\sum y)^4)}} \ldots$$

The main principle of CfsSubsetEval method is evaluating the value of a subset of attributes by considering the individual predictive ability of each element as well as the degree of redundancy between them. It generates subsets of features that are highly correlated with the class while having a low cross correlation [34]. The results are presented in the table below:

TABLE VI. MOST RELEVANT ATTRIBUTES

Search Method	CFS Subset Evaluator + Best first
Selected attributes	5,6,9,11,12,14,31,32
Attributes names	src_bytes; dst_bytes; urgent; num_failed_logins; logged_in; root_shell; srv_diff_host_rate; dst_host_count

Step5: In this step we implemented each technique on our dataset, using Weka tool. Below the result obtained based on confusion matrix, detection rate, time of execution and memory consumption.

A. Confusion Matrix:

In order to assess these techniques we take the confusion matrix, illustrated below:

TABLE VII. CONFUSION MATRIX APPROACHES

K-means confusion matrix

Classified / Attacks	a	b	c	e	f
Normal	4090	6106	0	0	37
Dos	4808	31254	0	0	5686
U2r	37	55	0	0	1
R2L	38	58	0	0	1
Probe	148	151	0	0	142

Naïve Bayes confusion matrix

Classified / Attacks	a	b	c	e	f
Normal	8253	150	36	709	1085
Dos	309	39189	4	10	2236
U2r	0	0	92	1	0
R2L	4	0	8	82	3
Probe	9	5	0	15	412

SMO confusion matrix

Classified / Attacks	a	b	c	e	f
Normal	10207	15	2	9	0
Dos	13	41735	0	0	0
U2r	1	0	92	0	0
R2L	14	0	0	83	0
Probe	23	0	0	0	418

Random forest confusion matrix

Classified / Attacks	a	b	c	e	f
Normal	10230	0	0	3	0
Dos	2	41745	0	0	1
U2r	1	0	92	0	0
R2L	8	0	0	89	0
Probe	7	2	0	0	432

Generally each column of the matrix represents the number of occurrences of an estimated class, while each row represents the number of occurrences of a real class (or reference). The results are presented in the following figures:

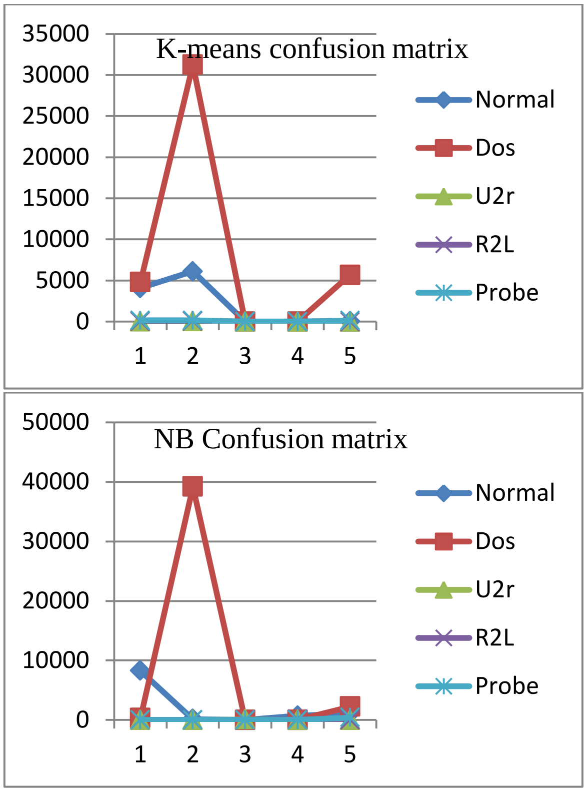
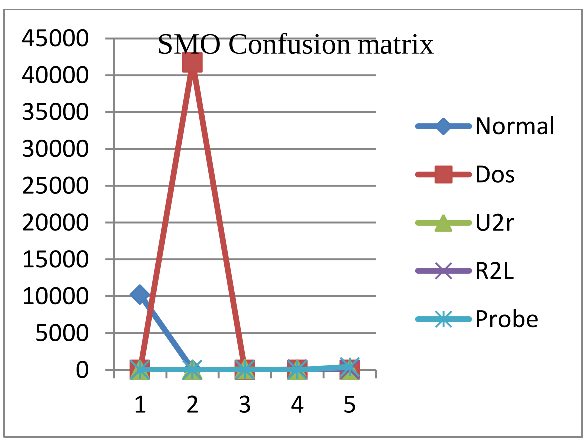


Fig. 2. Confusion Matrix Approach



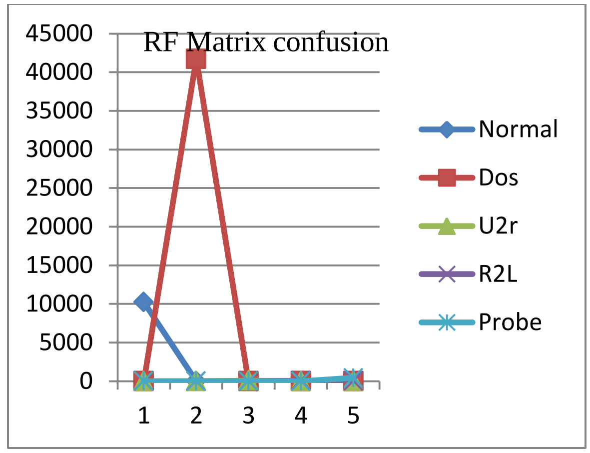


Fig. 3. Confusion Matrix Approach

According to results above and Based on Dos attack: K-means a classify 31254 Dos attack from 41749 real dos attack (74,86%), however 6106 instances are classified into normal class, 55 as U2R attack, 58 as R2L attack and 151 as Probe attack. Naïve bayes is able to classify 39189 Dos attacks from 41749 real Dos Doss attack (93.87%), while 150 instances is classified as normal attack, and 5 as Probe. SMO classified 41735 Dos attack from 41749 (99,96%), and 15 instances into normal class. Finally random forest classified 41745 Dos attack from 41749 real Dos attack (99,99%), and 2 instances as a Probe attack.

B. Classification Rate

The purpose of classification is to minimize the probability of error Detection algorithms are usually evaluated using the detection rate. A simple way to perform an intrusion detection, is to use a classifier to determine whether certain traffic data observed is normal or attacks. We present the classification rate on two sides: Global records classification and general rate classification.

Global records classification: The table below presents for each technique the global number of correctly and incorrectly classified records:

TABLE VIII. INSTANCES CLASSIFICATION

Approach	Correctly Classified Instances	Incorrectly Classified Instances
K-means	35486	17126
Naive bayes	48028	4584
SMO	52535	77
Random forest	52588	24

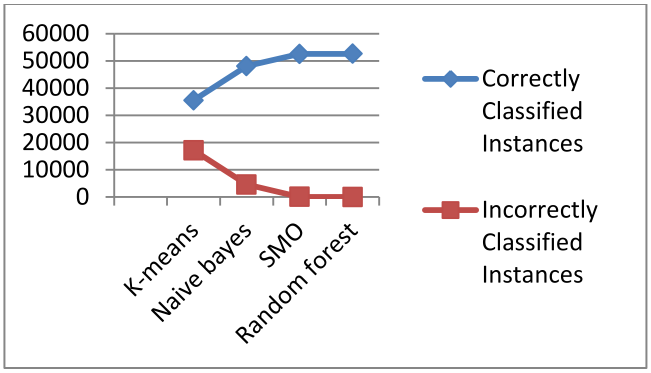


Fig. 4. Instance Classification

As shown in figure above, we note that random forest has the higher number of correctly classified instances and the lower number of incorrectly classified instances, however we observe the complete opposite for K-means technique.

General rate classification: The following figures represents the rate classification of each class, normal class is represented by the Blue color, Red for Doss class, U2R Blue sky, green for R2L class, and pink color for the Probe class. A better classification is obtained if the represented classes are well separated. According to the results we deduce that the Random Forest classifier is more effective and efficient than other approaches with a classification rate of 99.9544%.

Below the Complexity variables: (**N**: instances number, **M**: Attribute number, **C:** Classes number, **V**:attribute value).

According to the results, the SVM method is the most complex [0((NM)^2] , which explains its high memory consumption with 38,444KB, and his long time compilation.

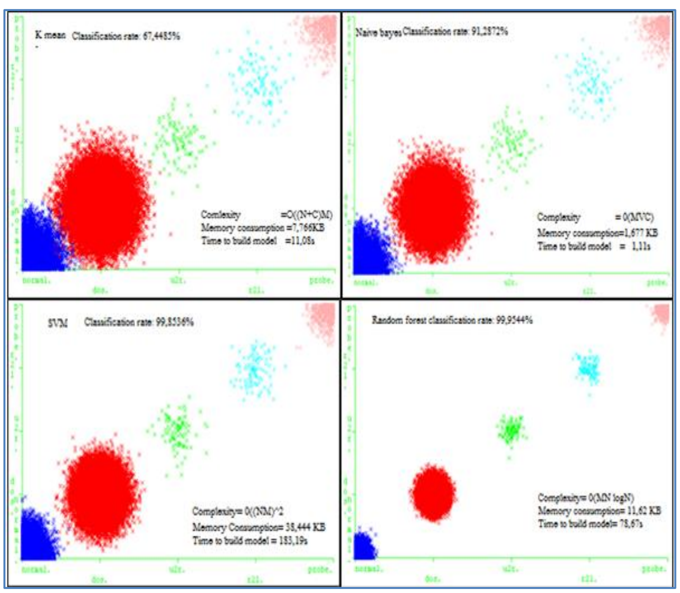


Fig. 5. Classification rate

The memory consumption of these techniques are compared with properties of sensor node that we can use in deployment of wireless sensor network, we choose MICA2 and Telosb. Knowing that MICA2 is equipped with a processor running at 7.37 MHz, 4KB of RAM, 128KB of flash memory and a radio transmitter on 433 MHz. For Telosb, is equipped with an 8 MHz clock processor, 10K RAM, 48K of program memory, and 1024K flash storage.

In the figure 5, we compare the memory consumption of studied techniques and node sensor ability. Time to build the approaches is presented in figure 6.

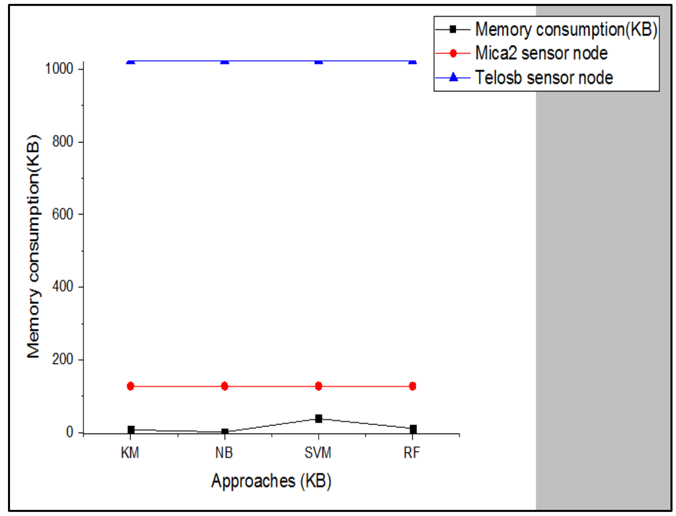


Fig. 6. Memory Consumption

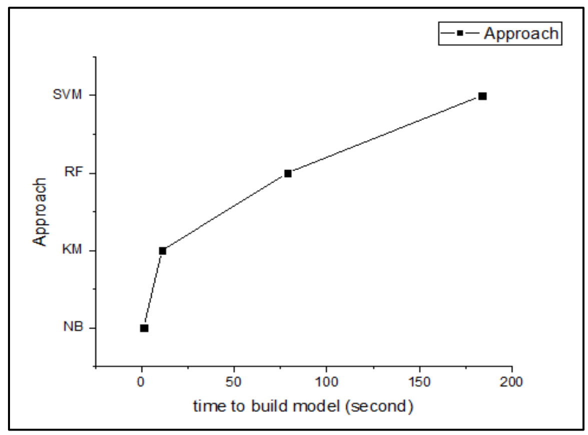


Fig. 7. Approaches building time

According to results, it is clear that memory is enough to compile each approach on Mica2 node or Telosb node, but for increasing the lifetime of the node, and taken on consideration the main aims of these techniques, detecting the different attacks (classification rate),we can say that Random forest technique is the efficient technique for detecting intrusion in wireless sensor network, with a higher rate classification (99.9544 %), reasonable required memory (11,62 KB), and building time(78,67 s). Indeed, the superiority of Random Forest intrusion detection technique, SVM, Naïve Bayes and K-means respectively, can be clearly deduced, in this order, according to confusion matrix, classification rate, memory, complexity, building time and memory consumption we can classify these techniques, from the higher to lower performant technique. Classification based on suitable feature selection is one of the main factors which reach the performance of IDS, especially in WSN.

VI. CONCLUSION

The key challenge of evolving intrusion detection system in WSN is to identify attacks with high accuracy, and satisfied the required constraints and challenges, to prolong the lifetime of the entire network. This aims could be attained from several ways. Firstly paying much more attention to detection techniques used for attacks detection is characterized by efficiency and ability. Secondly, reconstructing detection mechanism with a distributed manner, to reducing the communication overhead. This paper has compared and evaluated the newest anomaly detection intrusion techniques used in wireless sensor network, to improve the efficient technique for IDS in WSN. According to the results, it is highly recommended to use the data mining techniques to detect effectively the intrusions and attacks in WSN. The decision of choosing efficient IDS is a compromise between technique employed and performance metrics. However, many issues are still open and need further research efforts such as hierarchical clustering patterns, using machine learning in resource management problem of wireless sensor networks, developing a classifier that is trained well with network patterns, selecting and preprocessing an appropriate dataset. In addition, taking smart strategies into account such as compressing the input dataset, narrowing the scale of attributes set and simplifying the procedure of analysis and decision could make lots of progress for IDS to satisfy the requirement constraint of WSN without losing the security and reliability.

REFERENCES

[1] Akyildiz,I.F.,Su,W.,Sankarasubramaniam,Y.,Cayirci,E.,2002.Wirelessse nsor networks: asurvey. Comput Networks 38,393–422.

[2] Lopez J, Zhou J. Overview of wireless sensor network security. In: Wireless sensor network security. IOS Press, incorporated; May 2008. p. 1–21.

[3] Perrig A, et al. SPINS: security protocols for sensor networks .Presented at the 17th ACM international conference on mobile computing and networks, 2001.

[4] Xiao Y, Rayi VK, Sun B, Du X, Hu F, Galloway M. A survey of key management schemes in wireless sensor networks. Comput Commun 2007;P: 30-23,14–41.

[5] Jaiganesh, V., Mangayarkarasi, S., & Sumathi, P.(2013). Intrusion Detection Systems: A Survey and Analysis of Classification Techniques. International Journal of Advanced Research in Computer and communication Engineering ,Vol. 2, Issue 4, April 2013

[6] Anderson JP. Computer security threat monitoring and surveillance. Fort Washing- ton, Pennsylvania: James P Anderson Co; April 1980.

[7] Kuperman, Benjamin A. "CERIAS Tech Report 2004-26 A CATEGORIZATION OF COMPUTER SECURITY MONITORING SYSTEMS AND THE IMPACT ON THE DESIGN OF AUDIT SOURCES." (2004).

[8] Govindarajan, M. "Hybrid Intrusion Detection Using Ensemble of Classification Methods." International Journal of Computer Network & Information Security 6.2 (2014).

[9] Hu J. Host-based anomaly IDS. In: Springer handbook of information and com- munication security. Springer Verlag; 2010.

[10] K. Sharma and M. K. Ghose; Wireless Sensor Networks: An Overview on its Security Threats; IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs; CSE Department, SMIT, Sikkim, India; 2010.

[11] Y. Zhou, Y. Fang and Y. Zhang; Security Wireless Sensor Networks: A Survey; IEEE Communication Surveys; 2008.

[12] David Boyle, Thomas Newe. “Securing Wireless Sensor Networks: Security Architectures”, Journal of networks, Volume 3, No. 1, 2008.

[13] Rouba El Kaissi, Ayman Kayssi, Ali Chehab and Zaher Dawy, (2005)” DAWWSEN: A Defense Mechanism against Wormhole ttack In Wireless Sensor Network”,Proceedings of the Second International Conference on Innovations in Information Technology (IIT”05).

[14] A. D. Wood and J. A. Stankovic,(2002) “Denial of service in sensor networks”,Computer, 35(10):54–62, 2002.

[15] Ioannis Krontiris, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos. Intrusion detection of sinkhole attacks in wireless sensor networks. In Miroslaw Kutylowski, Jacek Cichon, and Przemyslaw Kubiak, editors, ALGOSENSORS, volume 4837 of Lecture Notes in Computer Science, pages 150–161. Springer, 2007.

[16] Richard Heady, George Lugar, Mark Servilla, and Arthur Maccabe. The architecture of a network level intrusion detection system. Technical report, University of New Mexico, Albuquerque, NM, August 1990.

[17] S. Shin, T. Kwon, G.Y. Jo, Y. Park, H. Rhy, “An experimental study of hierarchical intrusion detection for wireless industrial sensor networks”, IEEE Trans. Ind. Informat., volume 6, number 4, pages 744-757, 2010.

[18] I. Krontiris, T. Dimitriou and F.C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”, Proc. 13th European Wireless Conference, 2007

[19] I. Onat and A. Miri, “An Intrusion Detection System for Wireless Sensor Networks”, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2005.

[20] S. Rajasegarar, C. Leckie, M. Palaniswami, J.C. Bezdek, “Distributed Anomaly Detection in Wireless Sensor Networks”, 10th IEEE Singapore International Conference on Communication systems, 2006.

[21] A. Patcha and J.M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological trends”, Elsevier J. Computer Networks, volume 51, number 12, pages 3448-3470, 2007.

[22] Rajasegarar S, et al. Anomaly detection in wireless sensor networks. IEEE Wireless Communications 2008;15:34–40.

[23] Y.EL Mourabit, A. Toumanari, H.Zougagh, “A Mobile Agent Approach for IDS in Mobile Ad Hoc Network”, International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1, January 2014

[24] M. Burgess. Computer immunology. In LISA ’98: Proceedings of the 12th USENIX conference on System administration, pages 283–298, Berkeley, CA, USA, 1998. USENIX Association.

[25] B.E Boser, I.M. Guyon and V.N. Vapnik. A training algorithm for optimal margin classifiers. In COLT ’92:Proceedings of the fifth annual workshop on Computational learning theory, pages 144–152, New York, NY, USA, 1992. ACM. ISBN 0-89791-497-X.

[26] J.Platt, “Fast training of support vector machine using sequential minimal optimization,” Advances in Kernel Methods: support vector machine, MIT Press, Cambridge, MA, 1998.

[27] H-S. Kim and S-D. Cha. 2004. Efficient masquerade detection using svm based on common command frequency in sliding windows.IEICE Transactions On Information And Systems Volume, E87-D, 2446–2452.

[28] S. Rajasegarar, C. Leckie, M. Palaniswami and J.C. Bezdek, “Quarter Sphere Based Distributed Anomaly Detection in Wireless Sensor Networks”, IEEE ICC ’07, Glasgow, U.K., June 2007.

[29] Bill C.P. Lau a, Eden W.M. Maa, Tommy W.S. Chow, “Probabilistic fault detector for Wireless Sensor Network”, Expert Systems with Applications 41 (2014) 3703–3711.

[30] Hastie, T., et al., The elements of statistical learning: data mining, inference and prediction. The Mathematical Intelligencer, 2005. 27(2): p. 83-85.

[31] Abebe Tesfahun, D. Lalitha Bhaskari, “Intrusion Detection using Random Forests Classifier with SMOTE and Feature Reduction”, 2013 International Conference on Cloud & Ubiquitous Computing & Emerging Technologies.

[32] http://kdd.ics.uci.edu/databases/kddcup99/ kddcup.

[33] Zdrayko Markov, Ingrid Russel, “An introduction to the WEKA data mining system”, ITICSE '06 Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, Pages 367-368.

[34] I. H. Witten and E. Frank. Data Mining: Practical Machine Learning Tools and Techniques, Second Edition (Morgan Kaufmann Series in Data Management Systems). Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2005.

[35] M. Xie et al. "Anomaly detection in wireless sensor networks: A survey", Journal of Network and Computer Applications 34 (2011) 1302–1325.

A Multi-Attribute Decision Making for Electrician Selection using Triangular Fuzzy Numbers Arithmetic Approach

Wiwien Hadikurniawati
Faculty of Information Technology
Universitas Stikubank
Semarang, Indonesia

Retantyo Wardoyo
Department of Computer Science and Electronics
Universitas Gadjah Mada
Yogyakarta, Indonesia

***Abstract*—This study uses an approach of fuzzy multi attribute decision making in determining alternatives to solve the selection problem of the electrician through a competency test. Competency test consists of several tests of knowledge, skills and work attitude. The parameters of decision making is used to choose the best alternative written test, test of theoretical knowledge, practice knowledge test and oral test. Linguistic values expressed by triangular fuzzy numbers is used to represent the preferences of decision makers so that the uncertainty and imprecision in the selection process can be minimized. Aggregation results are represented using triangular fuzzy numbers. The output of this selection process is the best alternative obtained using triangular fuzzy numbers arithmetic approach.**

Keywords*—multi-attribute decision making; triangular fuzzy number; fuzzy arithmetic; electrician

I. Introduction

National development will boost economic growth and competitiveness in the world market. The developments affect the increased needs of the elements associated with infrastructure development, one of which is the human resources in the form of labor. Indonesia has a large number of workers. For this purpose, the quality of Indonesian human resources in various sectors and regions, need to be improved and optimized for utilization [1]. Improving the quality of human resources is very important for experts in construction industry. Labor skills are important part in the implementation of a construction project. Job skills suitability possessed by workers with job skills required by the labor service user is needed to increase employment opportunities [2]. Professional construction sector worker has a reliable ability, ethical, and highly competitive.

The government realizes the importance of human resource competencies in the field of electricity. The government creates it through Law No. 15 on Electricity. The government has drawn up Government Regulation No. 3 of 2005 as an amendment to Government Regulation No. 10 of 1989 About the Provision and Use of Electric Power, which in Article 21 paragraph 9 states that "Every technician who worked in the electricity business is required to have a certificate of competence". The electrician should do several competency tests to obtain a certificate of competence. Competency test consists of knowledge, skills and attitude tests. The tests of knowledge, skill, and attitude obtained from several tests, both written and oral tests as well as practice of skill [2].

The decision-making is a research group developed over the last twenty years, while research on the theory and method of group decision-making has always received attention from researchers in the world [3,4]. Multi attribute decision making (MADM) is used to solve the problem in selecting the optimal alternative out of several alternatives related to attributes. The decision maker in the MADM process often takes the form of the linguistic variables. It occurs because of the complexity and uncertainty of the objective things and the ambiguity of human thinking [5]. Multi-attribute decision making method makes the decision maker to be able to determine the appropriate alternative. MADM technique is a popular technique and widely used in many fields of science, namely engineering, economics, management, transportation planning, etc [6].

The fuzzy set theory has been applied in many fields, for example operation research, management theory etc. The fuzzy numbers and fuzzy values are suitable for representing uncertain information; they are used in many applications [7].

At present, if decision information, often refers to attribute value, is given in the form of precise value, the multi attribute decision methods is relatively perfect.

The complexity and uncertainty of objective things and fuzziness of human thinking in many actual decision making are difficult to give the explicit attribute weight, this kind of multi attribute decision making having incomplete information has been worth studying.

The process of selecting a qualified electrician must be precise, accurate and qualified to be able to achieve the expected outcome is to get the best electrician appropriate to their parameters. Decision making method can solve that problem. Based on the idea, decision making approach is proposed to identify qualified electricians according to their parameters.

In this paper, attribute value are given in the form of Triangular Fuzzy Numbers (TFN), calculate the rank of alternatives according to arithmetic approximation.

The rest of the papers are organized as follows, section 2 describes related works of the research. In the section 3 triangular fuzzy numbers and fuzzy multi-attribute approach are summarized. In this section, methodology for each technique is also given. Section 4 discusses a case study, analysis, and result of this research. The conclusions are presented in Section 5.

II. Related Work

The purpose of multi attribute decision making is reaching a decision by choosing the best alternative from many candidates [8]. The attribute or criteria can be the one causes some benefits or the one that causes cost. Decision making comprised of four steps: 1. Acquisition of information, 2. Decision making model, 3. Acquisition of decision results, 4. Ranking alternatives in a sequence [9]. Hopfe [10] proposed design assessment uncertainty in decision making. This decision making using AHP approach and the case is focused on discrete decision. The key performance indicators are used as a preference in this case.

Dongjing [11] proposed method for decision making, compute the distance between each alternative and positive, negative ideal point of interval numbers, then finds out each alternative's closeness degree for ideal point.

Wibowo [12] used a fuzzy multi-criteria approach in the group decision making to increase the confidence level of the decision maker or the decision maker in solving the problem of selection of suppliers. Fuzzy linguistic variables are used to represent subjective assessment decision makers. The uncertainty can be minimized by fuzzy linguistic variable. Hegazy [13] explained how to solve the problem of uncertainty in the medical world, especially mental health issues using a fuzzy set approach.

Fuzzy multi attribute decision making (FMADM) is used to resolve the problems with the appropriate decision-making approach. FMADM describes rational decisions in situations of uncertainty given in the form of linguistic values. Fuzzy numbers represent the values of linguistic. Researchers typically use triangular fuzzy numbers or trapeziodal [14]. Bekheet [14] proposed polygon fuzzy number (PFN) for decision makers to express their own linguistic. FMADM methods based on comprehensive satisfaction evaluatives that are derived from the preferences of decision maker, is presented to solve the decision data sampling problems in a fuzzy situation. The decision data and weights of all attributes take the form of generalized trapezoidal fuzzy numbers (GTFN) [15].

In this paper, selection of the best alternative is obtained using fuzzy multi attribute decision making methods. The proposed methods use triangular fuzzy numbers and fuzzy arithmetic approach to select electrician.

III. Methods

A. Fuzzy Number

A fuzzy number is a generalization of a regular, real number in the sense that it does not refer to one single value but rather to a connected set of possible values, where each possible value has its own weight between 0 and 1. Fuzzy number is expressed as a fuzzy set a fuzzy interval in real number. The boundary of this interval is ambiguous; the interval is also a fuzzy set. Generally a fuzzy interval is represented by two end points a_1 and a_2 and a peak point a_2 as $[a_1, a_2, a_3]$ [16-18].

B. Triangular Fuzzy Number

Triangular fuzzy number is more popular because of its ease of the arithmetic operations. The arithmetic operations are addition, subtraction, multiplication, division, reciprocal, geometric mean, etc. Such operations enable the decision makers to determine the rank of alternative [16].

Triangular Fuzzy Numbers (TFN) is a fuzzy number represented by three values, namely $A = (a_1, a_2, a_3)$. It can be defined as shown in (1).

$$\mu_{(A)}(x) = \begin{cases} 0, & x < a_1 \\ \frac{x-a_1}{a_2-a_1}, & a_1 \le x \le a_2 \\ \frac{a_3-x}{a_3-a_2}, & a_2 \le x \le a_3 \\ 0, & x > a_3 \end{cases} \tag{1}$$

This presentation is expressed as membership functions as shown in the Fig.1.

The crisp interval got by α-cut operation, interval A_a is obtained as follows $\forall\alpha \in [0,1]$ from

$$\frac{a_1^{(\propto)}-a_1}{a_2-a_1} = a\,, \quad \frac{a_3-a_3^{(\propto)}}{a_3-a_2} = \propto \tag{2}$$

And then obtained :

$$a_1^{(\propto)} = (a_2 - a_1)\propto + a_1 \tag{3}$$

The formula of A_α obtained as shown in (4).

$$A\propto \; = \; [a_1^{(\propto)}, a_3^{(\propto)}]$$
$$A\propto \; = \; [(a_2 - a_1)\propto + a_1, -(a_3 - a_2)\propto + a_3] \tag{4}$$

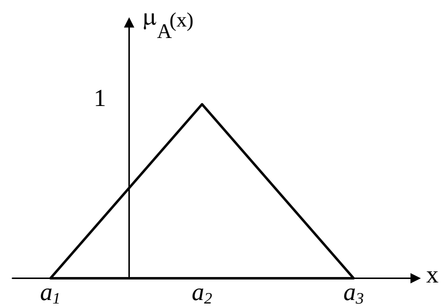


Fig. 1. Triangular Fuzzy Number A = (a1, a2, a3)

C. Fuzzy Arithmetic

Basic arithmetic operation on fuzzy number is an extension of the concept of basic arithmetic operations in general by using the degree of membership. Some important properties of operations on the triangular fuzzy number are [17,18]

1) The result of the addition or subtraction between the triangular fuzzy numbers is in the form of triangular fuzzy numbers

2) The result of multiplication or division between the triangular fuzzy numbers is not a form of triangular fuzzy numbers. Operations of multiplication or division results can be converted into triangular fuzzy numbers through value approach.

3) Operation max or min did not produce the form of triangular fuzzy numbers

Triangular Fuzzy Numbers Operation

1) Addition

This operation does not use the membership function. For example, A and B are triangular fuzzy number $A = (a_1, a_2, a_3)$, $B = (b_1, b_2, b_3)$. A + B are calculated using (5).

$$A + B = (a_1, a_2, a_3) (+) (b_1, b_2, b_3)$$
$$A + B = (a_1+b_1, a_2+b_2, a_3+b_3) \quad (5)$$

2) Substraction

If $A = (a_1, a_2, a_3)$ and $B = (b_1, b_2, b_3)$. A – B are calculated using (6)

$$A - B = (a_1, a_2, a_3) (-) (b_1, b_2, b_3)$$
$$A - B = (a_1-b_1, a_2-b_2, a_3-b_3) \quad (6)$$

3) Approximation of Multiplication

There are triangular fuzzy number $A = (a_1, a_2, a_3)$ and $B = (b_1, b_2, b_3)$.

The main concern is α-cuts of two fuzzy numbers,

$$A_\alpha = [(a_2 - a_1)\alpha + a_1, -(a_3 - a_2)\alpha + a_3]$$
$$B_\alpha = [(b_2 - b_1)\alpha + b_1, -(b_3 - b_2)\alpha + b_3] \quad (7)$$

Multiply A_α with B_α which are 2 crisp intervals, where for all $\alpha \in [0, 1]$, that elements of each interval are positive numbers. The formula of multiplication approximation as shown in (8).

$$A_\alpha (\cdot) B_\alpha = [(a_2 - a_1)\alpha + a_1, -(a_3 - a_2)\alpha + a_3] (\cdot) [(b_2 - b_1)\alpha + b_1, -(b_3 - b_2)\alpha + b_3] \quad (8)$$

The result of multiplication approximation $A_\alpha (\cdot) B_\alpha$ determined by $\alpha = 0$ and $\alpha = 1$.

4) Approximation of Division

Value of A (/) B can be expressed in a triangular fuzzy number. The way to determine the division is similar with the multiplication. First step is divide interval A_α by B_α.

For $\alpha \in [0, 1]$, the formula is shown in (9).

$$A_\alpha (/) B_\alpha = [(a_2 - a_1)\alpha + a_1 / -(b_3 - b_2)\alpha + b_3, -(b_3 - b_2)\alpha + b_3 / (b_2 - b_1)\alpha + b_1] \quad (9)$$

The result of division approximation $A_\alpha (\cdot) B_\alpha$ determined by $\alpha = 0$ and $\alpha = 1$.

D. Fuzzy Multi Attribute Approach

Decision makers often face doubt and uncertainty in expressing subjective perceptions or judgments, uncertainty in decision making. Fuzzy set theory is used to express the linguistic terms of decision-makers to resolve the uncertainty, ambiguity and subjectivity of human judgment [19].

The decision makers are influenced by uncertainties and imprecision in giving their subjective assessment. This uncertainty occurs because the decision makers are not fully confident in their assessments so that their judgments are represented by fuzzy numbers in linguistic form [20]. Linguistic variables represented by fuzzy numbers, which represent a subjective assessment decision to minimize the uncertainty and imprecision in the selection process. The steps of fuzzy multi attribute decision making (FADM) are:

1) Problem Representation

a) Identification of goals and decision alternative is determining the highest rank of alternative.

b) Parameter Identification

c) Building a hierarchical structure of these problems.

2) Evaluation of Fuzzy Set

a) Choosing the rating set for the weights parameter and the degree of fitness for each alternative with its parameters. W_i is the weight for parameter P_t. S_{it} is a fuzzy rating for the fitness degree of decision alternative A and parameter P_t. F_i is a fuzzy match index of alternative Ai which represents the fitness degree of alternative decisions. F_i is derived from the aggregation S_{it} and W_t, where i = 1,2,3, ... n and t = 1,2,3, ... k

b) Evaluating parameter weights and fitness degrees of any alternative parameters.

Aggregating the parameter weights and the fitness degree of each alternative with its parameters using fuzzy arithmetic, as shown in (10).

$$F_i = [(S_{1i} \otimes W_1) \oplus (S_{2i} \otimes W_2) \oplus \ldots \oplus (S_{ik} \otimes W_k)] \quad (10)$$

3) Selecting Alternatives

a) Prioritizing decision alternative based on the results of aggregation. Priority aggregation results are used to determine the ranking of decision alternatives. This aggregation results represented as triangular fuzzy numbers.

b) Choose a decision alternative with the highest priority as the optimal alternative.

IV. CASE STUDY

The proposed model is applied to solve the problem of the electrician selection.

A. Problem Representation

The problems in the selection of electrician aim to get experts who have parameters as per the requirements of the Agency for Construction Services. The electricians fulfill the administrative requirements before taking the competency test. The competency test consists of 4 exam materials and they are parameter of decision making. These parameters include P1 (written test), P2 (test of theoretical knowledge), P3 (practice knowledge test), and P4 (oral test). The electricians will receive a certificate of competence after they have passed a competency test. The problem in the selection of electrician can be represented in Fig. 2.

B. Evaluation of Fuzzy Set

There are linguistic variables that represent the importance weight for each parameter. Each weight represented by a triangular fuzzy numbers as follows:

$T_{(importance)}$ W = {VL, L, M, H, VH}

VL = Very Low, L = Low, M = Medium, H = High, VH = Very High. Each weight represented by a triangular fuzzy numbers as follows:

- VL = (0, 0, 0.25)
- L = (0, 0.25, 0.5)
- M = (0.25, 0.5, 0.75)
- H = (0.5, 0.75, 1)
- VH = (0.75, 1, 1)

The fitness degree of alternatives and decision parameter as follows :

$T_{\{fitness\}}$ S = {VP, P, M, G, VG}

VP = Very Poor, P = Poor, M = Medium, G = Good, VG = Very Good. Each weight represented by a triangular fuzzy numbers as follows:

- VP = (0, 0, 0.25)
- P = (0, 0.25, 0.5)
- M = (0.25, 0.5, 1)
- G = (0.5, 0.75, 1)
- VG = (0.75, 1, 1)

The rating for each decision parameter is shown in Table 1. The fitness degree of decision parameter and alterative are shown in Table 2

The next step is to determine the value of a fuzzy fitness. The values obtained by aggregating the alternative weight of importance degree on each parameter as shown in Tables 1 and Table 2

TABLE I. IMPORTANCE RATE FOR EACH PARAMETER

Parameter	P1	P2	P3	P4
Importance rate	L	H	VH	M

TABLE II. FITNESS RATE OF EACH ALTERNATIVE TOWARD PARAMETERS

Alternative	Parameter			
	P1	*P2*	*P3*	*P4*
Electrician 1	M	G	P	P
Electrician 2	P	P	M	G
Electrician 3	G	VG	G	G
Electrician 4	M	M	P	M
Electrician 5	P	G	G	M
Electrician 6	G	G	G	G
Electrician 7	P	M	VP	VP
Electrician 8	VP	G	G	G
Electrician 9	VG	M	G	G
Electrician 10	P	G	G	G

Alternative 1 (Electrician 1)

- Alternative fitness rating A1 (electrician 1) of the first parameter is Medium (M) = (0.25, 0.5, 0.75) and the importance rate for parameter 1 is Low (L) = (0, 0.25, 0.50).

Fuzzy fitness value is determined using approximation of multiplication on fuzzy arithmetic, as follows:

A = (0.25, 0.5, 0.75) B = (0, 0.25, 0.5)

A_α = [(0.5–0.25)α+0.25, – (0.75-0.5)α+0.75]
= [0.25α+0.25, - 0.25α+0.75]

B_α = [(0.25-0)α+0, - (0.5-0.25)α+0.5]
= [0.25α+0, - 0.25α+0.5]

A_α (·) B_α = [0.25α+0.25, - 0.25α+0.75] (·)[0.25α+0, - 0.25α+0.5]
= [(0.25α+0.25)(0.25α+0), (-0.25α+0.75)(-0.25α+0.5)]
= [0.0625α^2+0.0625α,0.0625α^2-0.125α+0.1875]

If α = 0, then A_α (·) B_α = [0, 0.1875]

If α = 1, then A_α (·) B_α = [0.125, 0.125] = 0.125

Triangular Fuzzy Number (TFN) of A_α (·) B_α ≅ (0, 0.125, 0,1875).

- Alternative fitness rating A1 (electrician 1) of the second parameter is Good (G) = (0.5, 0.75, 1) and the importance rate for parameter 2 is High (H) = (0.5, 0.75, 1).

Fuzzy fitness value is determined using approximation of multiplication on fuzzy arithmetic, as follows:

A = (0.5, 0.75, 1) B = (0.5, 0.75, 1)

A_α = [(0.75-0.5)α+0.5, - (1-0.75)α+1]
= [0.25α+0.5, - 0.25α+1]

B_α = [(0.75-0.5)α+0.5, - (1-0.75)α+1]
= [0.25α+0.5, - 0.25α+1]

A_α (·) B_α = [0.25α+0.5, - 0.25α+1] (·)[0.25α+0.5, - 0.25α+1]
=[(0.25α+0.5)(0.25α+0.5),(-0.25α+1)(-0.25α+1)]
= [0.0625α^2+0.025α+0.25, 0.0625α^2-0.5α+1]

If α = 0, then A_α (·) B_α = [0.25, 1]

If α = 1, then A_α (·) B_α = [0.5625, 0.5625] = 0.5625

Triangular Fuzzy Number (TFN) of A_α (·) B_α ≅ (0.25, 1, 0,5625).

- Alternative fitness rating A1 (electrician 1) of the third parameter is Poor (P) = (0, 0.25, 0.5) and the importance rate for parameter 3 is Very High (VH) = (0.75, 1, 1).

Fuzzy fitness value is determined using approximation of multiplication on fuzzy arithmetic, as follows:

A = (0, 0.25, 0.5) B = (0.75, 1, 1)

A_α = [(0.25-0)α+0, - (0.5-0.25)α+0.5]
= [0.25α+0, - 0.25α+0.5]

B_α = [(1-0.75)α+0.75, - (1-1)α+1]
= [0.25α+0.75, - 0α+1]

A_α (·) B_α = [0.25α+0, - 0.25α+0.5](·)[0.25α+0.75, - 0α+1]

$= [(0.25\alpha+0)(0.25\alpha+0.75),\ (-0.25\alpha+0.5)(-0\alpha+1)]$

$= [0.0625\alpha^2+0.1875, -0.25\alpha+0.5]$

If $\alpha = 0$, then $A_\alpha\ (\cdot)\ B_\alpha = [0.1875, 0.5]$

If $\alpha = 1$, then $A_\alpha\ (\cdot)\ B_\alpha = [0.25, 0,25] = 0.25$

Triangular Fuzzy Number (TFN) of $A_\alpha\ (\cdot)\ B_\alpha \cong$ (0.1875, 0,25, 0,5).

- Alternative fitness rating A1 (electrician 1) of the fourth parameter is Poor (P) = (0, 0.25, 0.5) and the importance rate for parameter 4 is Medium (M) = (0.25, 0.5, 0.75).

Fuzzy fitness value is determined using approximation of multiplication on fuzzy arithmetic, as follows:

A = (0, 0.25, 0.5) B = (0.25, 0.5, 0.75)

$A_\alpha = [(0.25-0)\alpha+0, - (0.5-0.25)\alpha+0.5]$

$= [0.25\alpha+0, - 0.25\alpha+0.5]$

$B_\alpha = [(0.5-0.25)\alpha+0.25, - (0.75-0.5)\alpha+0.75]$

$= [0.25\alpha+0.25, - 0.25\alpha+0.75]$

$A_\alpha\ (\cdot)\ B_\alpha = [0.25\alpha+0, - 0.25\alpha+0.5]\ (\cdot)[0.25\alpha+0.25, - 0.25\alpha+0.75]$

$= [(0.25\alpha+0)(0.25\alpha+0.5),\ (-0.25\alpha+0.5)(-0.25\alpha+0.75)]$

$= [0.0625\alpha^2+0.0625\alpha,\ 0.0625\alpha^2-0.3125\alpha+0.375]$

If $\alpha = 0$, then $A_\alpha\ (\cdot)\ B_\alpha = [0, 0.375]$

If $\alpha = 1$, then $A_\alpha\ (\cdot)\ B_\alpha = [0.125, 0.125] = 0.125$

Triangular Fuzzy Number (TFN) of $A_\alpha\ (\cdot)\ B_\alpha \cong$ (0, 0.125, 0,375).

Triangular Fuzzy Number (TFN) of the alternative weight to other parameters can be determined with the same steps as the previous calculation. The fuzzy fitness value calculation results of all alternative towards parameter can be seen in Table 3.

C. Ranking of Alternatives

The ranking is determined from the alternatives that have the largest parameter to the smallest alternatives. The result obtained is shown in Table 4.

Based on the results from the calculation, it is obtained that an electrician 3 has the highest value and has top rank.

V. Conclusion

The process of evaluating and determining an electrician in the competency test involves many parameters. This study uses triangular fuzzy number arithmetic approach for decision-making to solve the problem of determining an electrician in the competency test. Linguistic values expressed by triangular fuzzy number is used to represent the preferences of decision makers so that the uncertainty and imprecision in the selection process can be minimized. Aggregation results are represented using triangular fuzzy numbers. The selection results are obtained in the form of ranking the final value of the electrician. They are used to recommend experts in electrical field who has the highest level of competence.

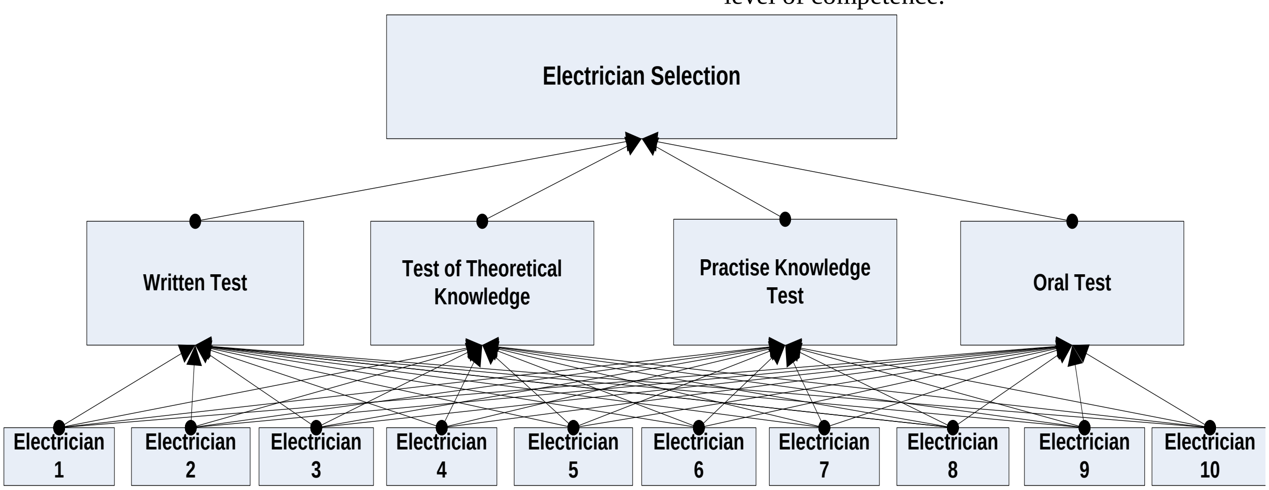


Fig. 2. Structure to select electrician

TABLE III. THE FUZZY FITNESS VALUE

Alternative	**Parameter**			
	P1	***P2***	***P3***	***P4***
Electrician 1	(0, 0.125, 0.1875)	(0.25, 0.5625, 1)	(0.1875, 0.25, 0.5)	(0, 0.125, 0.375)
Electrician 2	(0, 0.0625, 0.25)	(0, 0.1875, 0.5)	(0.1875, 0.5, 0.75)	(0.125, 0.375, 0.75)
Electrician 3	(0.125, 0.1875, 0.5)	(0.375, 0.75, 1)	(0.375, 0.75, 1)	(0.125, 0.375, 0.75)
Electrician 4	(0, 0.125, 0.375)	(0.25, 0.5625, 1)	(0.1875, 0.25, 0.5)	(0.0625, 0.25, 0.5625)
Electrician 5	(0, 0.0625, 0.25)	(0.25, 0.5625, 1)	(0.375, 0.75, 1)	(0.125, 0.375, 0.75)
Electrician 6	(0, 0.1875, 0.5)	(0.25, 0.5625, 1)	(0.375, 0.75, 1)	(0, 0, 0.1875)
Electrician 7	(0, 0.0625, 0.25)	(0.125, 0.375, 0.75)	(0, 0, 0.25)	(0.125, 0.375, 0.75)
Electrician 8	(0, 0, 0.125)	(0.25, 0.5625, 1)	(0.375, 0.75, 1)	(0.125, 0.375, 0.75)
Electrician 9	(0.875, 0.25, 0.75)	(0.125, 0.375, 0.75)	(0.375, 0.75, 1)	(0.125, 0.375, 0.75)
Electrician 10	(0, 0.0625, 0.25)	(0.25, 0.5625, 1)	(0.375, 0.75, 1)	(0.125, 0.375, 0.75)

TABLE IV. THE RESULT OF ALTERNATIVE RANKING

Alternative	Weight	Rank
Electrician 1	(0.109375, 0.265625, 0.515625)	7
Electrician 2	(0.078125, 0.28125, 0.5625)	8
Electrician 3	(0.25, 0.515625, 0.8125)	1
Electrician 4	(0.125, 0.296875, 0.609375)	6
Electrician 5	(0.1875, 0.4375, 0.75)	3
Electrician 6	(0.15625, 0.375, 0.671875)	5
Electrician 7	(0.0625, 0.203125, 0.5)	9
Electrician 8	(0.1875, 0.421875, 0.71875)	4
Electrician 9	(0.203125, 0.4375, 0.8125)	2
Electrician 10	(0.1875, 0.4275, 0.75)	3

REFERENCES

[1] Direktorat Jenderal Pembinaan Pelatihan dan Produktivitas, Departemen Tenaga Kerja dan Transmigrasi, “Pedoman Penyelenggaraan Sistem Pelatihan Kerja Nasional di Daerah,” 2000.

[2] Lembaga Pengembangan Jasa Konstruksi Nasional, “Rancangan Standar Kompetensi Kerja Khusus”, 2010.

[3] X. Chen and L. Ma, “An Analytic Method far Consensus Analyisis in Group Experts’Judgments Based on Numerical Decision Matrix Preference Information”, Fifth International Conference on Fuzzy Systems and Knowledge Discovery, IEEE, doi:10.1109/FSKD.2008.502, 2008, pp. 176-180.

[4] P. Liu and Y. Su, “Multiple Attribute Decision Making Method Based on the Trapezoid Fuzzy Linguistic Hybrid Harmonic Averaging Operator”, Informatica, Vol. 36, 2012, pp. 83-90.

[5] P. Dongjing, “A New Method for Fuzzy Multiple Attribute Decision Making based on Interval Numbers”, International Forum on Information Technology and Applications, IEEE Computer Society, doi:10.1109/IFITA.2009.141, 2009, pp. 408-411,

[6] L. Fan and F. Zuo, “Research on Multi-Attribute Decision Making Method Based on AHP and Outranking Relation”, Workshop on Power Electronics and Intelligent Transportation System, IEEE, doi:10.1109/PEITS.2008.42, 2008, pp. 227-232.

[7] A.N. Gani and S.N.M. Assarudeen, “A New Operation on Triangular Fuzzy Number for Solving Fuzzy Linear Programming Problem”, Applied Mathematical Sciences, Vol.6, No. 11, 2012, pp. 525-532.

[8] K.T. Cho, “Multicriteria Decision Methods : An Attempt to Evaluate and Unify”, Mathematical and Computer Modelling, Elsevier, 2003, pp. 1099-1119.

[9] Y. Dong and H. Zhang, “Multiperson Decision Making with Different Preference Representation Structures : A Direct Consensus Framework and Its Properties”. Knowledge Based System, doi:10.1016/j.knosys.2013.09.021, Elsevier, 2013.

[10] C.J. Hopfe, G.L.M. Augenbroe, J.L.M Hensen, “Multi-Criteria Decision Making Uncertainty in Building Performance Assesment”, Building and Environment, Elsevier, vol.69, doi:10.1016/j.buildenv.2013.07.019 , 2013, pp. 81-90.

[11] P. Dongjing, “A New Method for Fuzzy Multiple Attribute Decision Making based on Interval Numbers”, Internatioal Forum on Information Technology and Applications, doi: 10.1109/IFITA.2009.141, IEEE Computer Society, 2009, pp. 408-411.

[12] S. Wibowo, “A Fuzzy Multicriteria Group Decision Making Approach for Improving the Degree of Confidence in Supplier Selection”, Fourth International Symposium on Computational Intelligence and Design, doi: 001.10.1109/ISCID.2011.122. IEEE Computer Society, 2011, pp. 83-86.

[13] S. Hegazy, et.al, “Modulating Membership Grades to Gain Consensus for Fuzzy Set Uncertainty Values in Clinical Decision Support System”, Third International Conference on Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services, IEEE Computer Society, doi: 10.1109/CENTRIC.2010.27, 2010, pp. 40-45.

[14] S. Bekheet, “An Enhanced Fuzzy Multi Criteria Decision Making Model with a proposed Polygon Fuzzy Number”, International Journal of Advanced Computer Sience and Applications (IJACSA), Vol. 5, No. 5, 2014, pp. 118-121.

[15] X. Yu, M. Li, Z. Ping, “Multi-Attribute Group Decision Making Based on Biased Informaton Sampling Model and Generalized Trapezoidal Fuzzy Numbers”, 12th International Conference on Computer and Information Technology, doi: 10.1109/CIT.2012.44, 2012, pp. 109-114.

[16] F. Herrera, E.H.Viedma, “Linguistic Decision Analysis : Steps for Solving Decision Problems Under Linguistik Information”, Fuzzy Sets and Systems 115, PII: S0165-0114(99)00024-X, 2000, pp. 67-82.

[17] K.H. Lee, “First Course on Fuzzy Theory and Applications”, Springer, ISSN.16-15-3871, 2005.

[18] L.X. Wang, “A Course in Fuzzy Systems and Control”, Prentice-Hall International Inc, 1997.

[19] A. Sanayei, S.F. Mousavi, C.A. Shahmirzadi, “A Group Based Fuzzy MCDM for Selecting Knowledge Portal System”, World Academy of Science, Engineering and Technology 52, 2009, pp. 455-452.

[20] M. Tavana, M.A. Sodenkamp, “A Fuzzy multi-criteria Decision Analysis Model for Advanced Technology Assesment at Kennedy Space Center”, Jounal Operational Research Soc, DOI. 10.1057/jors. 2009.107. Vol.61, 2010, pp. 1459-1470.

A Modified Heuristic-Block Protocol Model for Privacy and Concurrency in Cloud

Akhilesh Kumar Bhardwaj
Research Scholar
Punjab Technical University
India

Dr. Surinder
Associate Professor
H.C.T.M, Kaithal
India

Dr. Rajiv Mahajan
Professor & Principal
C.T.I.T., Jalandhar
India

***Abstract*—With boost in the figure of cloud users and the magnitude of sensitive data on cloud, shielding of cloud has become more important. Competent methods are consistently desirable to ensure the information privacy and load management of outsource data on un-trusted cloud servers. The base of our proposed idea is the chronological display of metaheuristic firefly algorithm and blocks based Merkle hash tree protocol. This pool of combination significantly reduces the communication delay and I/O costs. The projected scheme in addition considers the dynamic data operations at block level while maintaining the equivalent security assurance. Our method makes use of third party auditor to periodically verify the data stored at cloud provider side. Our elucidation removes the burden of verification from the user side and alleviates both the user's and storage service's fear about data outburst and data corruptions.**

***Keywords*—Cloud Computing; TPA; Firefly; MHT; NTRU; LZW**

I. Introduction

Cloud computing is a network-dependent environment, which aims to share computations or resources. The most vital negative aspect, as observed by the organizations looking ahead to transfer to the cloud is confidential data protection and application safekeeping along with communication interlude. In this paper, a simple data protection and load management protocol model has been proposed to overcome the existing negativities coupled with cloud.

The idea behind cloud computing has been introduced after the emergence of distributed computing, parallel computing and grid computing [5]. During the past few years, cloud computing has been widely adopted because the corporate require an increasingly proficient means of exploiting its IT investment [3].

In fact, clouds are dependent on Internet and they attempt to mask the complexity for the clients [1]. Cloud computing usage has become more prevalent and most of the companies have started utilizing the services from cloud computing [2].

The cloud computing model is widely accepted because it offers access to computing as well as storage as per requirement, in addition to boundless resources [4]. Some of the features of cloud computing include ubiquity, increased reliability, being virtual, adaptability, scalability, quick suppleness, abundant tendency, planned service, increased intelligence, autonomic efficient control and high quality of service "QoS" [7].

The cloud model provides numerous advantages to each and every cloud stakeholders such as cloud providers (CPs), cloud consumers (CCs) and service providers (SPs). Yet, there are also several unlocked issues available in this model, which affects the reliability to a greater extent [6].

The data residing in a cloud is subjected to severe problems and hence, currently, more number of researchers and projects has given utmost interest towards providing improved data security in cloud computing [10].

More recently, it is highly essential to learn and examine the way the cloud computing and its applications operate on clouds. In addition, it is also necessary to observe the level of privacy offered by the cloud computing services and the determination of the kind of cloud computing service to be used by the users becomes more vital. Examining the performance and the security issues of real cloud environments seems to be difficult because testing in real environments can be more costly, unrepeatable and time-consuming [8].

The security and performance associated with the entire system are also affected by the novel data storage paradigm in Cloud [12]. The cloud provider is responsible for preventing the unauthorized insiders or the malicious outsiders from accessing the data and personal information that is available in the host database and to assure data security [13].

Data that is securely stored in the server will be also under problem, when a hacker attacks several servers for obtaining the information. One security mechanism of cloud computing, which can avoid security violations, is the management reliability [14]. Safe access to the cloud services can be rendered by cloud authentication systems that utilize various methods such as simple text password, third party authentication, graphical password, biometric and 3D password object [11].

Of the serious challenges posed in cloud computing, mutual authentication is more important. With mutual authentication, both the parties involved in communication can authenticate each other prior to the initiation of communication. Several authentication methods can be used for authenticating the user.

Few authentication methods like, plain password authentication can be implemented without much difficulty. But, they are commonly feeble and primitive [9]. Making use of a reliable third party auditor, who serves as the user for evaluating and revealing the risk of cloud storage services as per user request, can be a better way of assuring data security [10].

Third Party Authentication can be considered as a form of scrutiny. Private audit-ability and public audit-ability are the two classifications of third party authentication. The private audit-ability may result in large scheme efficiency. But, the public audit-ability only enables everyone including the client, who is the owner of data, to insist the cloud server for the rightness of data storage without owning private information. Third - party auditor (TPA) aids in auditing the data of the client, so that the trouble of the data owner in handling the data can be eliminated. TPA audits to see if the data stored in the cloud is unharmed or not and thus, avoids the client from taking part. This audit performed by TPA is more essential because it accomplishes economies of scale for Cloud Computing. The released audit assists the owners in assessing the risks that are related with the cloud data services accessed. The report can be advantageous to the cloud service provider for enhancing their cloud-dependent service platform [15].

II. Related Work

The current technological advancements have led cloud computing to be more popular and successful. Yet, severe problems in security and privacy may arise, if the data and business applications are outsourced to a third person.

Zhifeng Xiao and Yang Xiao [16] have suggested plenty of methodologies for third party authentication that help in handling storage and data transaction in a secure way. The objective of all their works is to give a complete review of all the security and privacy issues in cloud environments.

The users can make a choice of the third-party auditor (TPA), if the public auditability for cloud storage is enabled. This step is more essential for the users because the TPA, who they choose, would verify the integrity of the outsourced data and they need not bother about it. More secure and successful way of introducing TPA can be accomplished, only if the auditing process does not cause vulnerabilities to data security, in addition to not increasing user's burden further. **Cong Wang [17]** has put forward a more protective cloud storage system that supports public auditing with privacy-preserving ability. They have also broadened their outcomes in a way that the TPA is rendered with the power to carry out audits for multiple users at the same time

In a distributed storage system that lacks central authority, it is difficult to provide security along with multiple function support**. Hsiao-Ying Lin *et al*. [18]** have presented a threshold proxy re-encryption scheme, which is integrated with a decentralized erasure code for developing a secure distributed storage system. Technically, their chief contribution is that the proxy re-encryption system would assist both the encoding operations, which are carried out on the encrypted messages, and the forwarding operations that are performed on the encoded and the encrypted messages.

The cost associated with handling data can be lowered by outsourcing the data backups from off-site to third-party cloud storage services. But, security assurance for the outsourced data is highly essential and at the present moment, the third party does this job. Hence **Yang Tang *et al.* [19]** have dealt with the design and implementation of FADE, which is a protected overlay cloud storage system that is capable of realizing fine-grained, policy-based access control and file assured deletion.

Cloud computing is turning out to be a novel computing model in the healthcare zones, though they have flourished in the other business areas. Most of the healthcare organizations have begun transferring their electronic health information to the cloud environment. **Assad Abbas *et al.* [20]** have proposed a cloud service in the health sector, wherein, the cloud serves as a medical record storage center along with the ability to perform the transfer of electronic medical records between various hospitals and health centers.

In cloud computing, the major issue of concern is that the cloud providers should be more certain about the protection of their infrastructure. This issue needs more consideration because the outsiders, other clients or any of the unauthorized cloud employees may have access to the data in an unlawful manner. **Ching-Nung Yang [21]** have proposed a cloud security services, which incorporates key agreement and authentication. Here, the secure cloud computing (SCC) has been developed with the utilization of Elliptic Curve Diffie-Hellman (ECDH) and symmetric bivariate polynomial based secret sharing. The SCC that is employed can be of two classes. The former uses a trusted third party (TTP) and the latter does not make use of a TTP.

The need for ensuring data security is rising constantly and in particular, the hybrid cloud computing model requires data protection to a larger extent. **Jingxin K. Wang [22]** have put forth a number of methods for providing user data security that comprises of single encryption, multi-level virtualization and authentication interface. This work can be widened to the state, where CA system is either lacked or crashed.

A two layer encryption based approach has been suggested by **Mohamed Nabeel and Elisa Bertino [23]** in order to work out the problem by delegating as much of the access control enforcement responsibilities as feasible to the cloud while decreasing the information exposure risks due to colluding users and cloud. They have demonstrated that this problem was NP-complete and furthermore have suggested new optimization algorithms. By utilizing partial relationships among ACPs, they had furthermore plan to further decrease the computational cost.

Faraz Fatemi [24] have offered an efficient and scalable user authentication scheme for cloud computing environment. A client-based user authentication agent has been introduced to confirm identity of the user in client-side. Furthermore, a cloud-based software-as-a-service application has been used to confirm the process of authentication for unregistered devices.

G. Jai Arul Jose [25] has offered an security system providing authentication, confidentiality and data integrity of user's data by joining the cloud computing framework with cluster load balancing, SSL over AES and secure session.

E.M. Mohamad [26] has provided on-demand security options by making selection from different encryption algorithms. They are examined based on NIST statistical testing and implemented as pseudo random number generator (PRNG). Performance calculation is done by testing encryption speed.

V. Nirmala [27] has proposed user authentication scheme in which data is divided into blocks and applied with AES encryption after the generation of hash value for each block. Further, the Hash code is also implemented to check the data integrity. The cloud here is used to storing encrypted data and generating hash while rest of work takes place at user side.

The paper [22] suggests that making use of user data at the time of commercialization can end up in a great issue. The security and privacy of commercial data of the user is much preferred than other factors, while the user wants to establish cloud computing in their company. Certain problems of security in cloud computing still persist, in particular, the inter-cloud operations. The cloud providers need to meet the standard of inter-cloud operation interfaces.

The data security ensured through Privacy-Preserving Public Auditing is stated in [17], wherein, TPA is employed to achieve greater efficiency. Yet, the efficiency of their work during multiple auditing tasks seems to be lower. It is also found that the security and efficiency obtained from their work is not that much better, when an extensive investigation is made.

When a cloud system is being developed, several issues (that reduce the level of security) need to be considered with utmost care. People may find difficulty in accessing all their data of interest from the cloud data center. This is because various cloud service providers store the required data. Hence, a state of uncertainty arises amid the users, if they access data through cloud service providers.

The data privacy issue that is encountered during third party auditing cannot be cleared entirely with the introduction of the encryption method. But, it can simply be transformed into the complex key management domain. The cloud model brings about a lot of latest security confronts, which have not been fine tacit. To overcome these drawbacks of privacy and concurrency, the proposed article presents a modified firefly – merkle hash tree protocol model. The model can be further extended for different communication scenario in the future.

III. Proposed Model

Cloud computing configuration contains two foundation layers: a virtualization layer and a management layer [30]. In the virtualization layer, we catch the actual platforms and servers that host the virtual machines and have virtualization enabled hardware. In the management layer, we come across the modules accountable for enabling the complete operations detailed for the cloud.. Ensuring the integrity of data storage is the primary difficulty in Cloud Computing. Hence, to overcome this difficulty, a simple data protection and load management protocol model (where data is encrypted using Advanced Encryption Standard before it is launched in the cloud) has been proposed.

In the proposed FMHP (Firefly-Merkle Hash Tree Protocol) model, the firefly algorithm is implemented for file encryption and integrity verification, while MHT helps in load management and files compression.

Here, a third party auditor (TPA) would assist the cloud client for ensuring the integrity of the dynamic data placed in the cloud. During the auditing period, the client's participation is considered by the TPA to check whether the client data is left undamaged or not. By doing so, the levels of economy of cloud computing can be achieved.

The proposed cloud computing model could fix the serious problems, namely public authentication, load balancing and dynamic data integrity. The effort is divided into different modules including design and execution of a FMH protocol to overcome the problem of public authentication and load management (while maintaining file server based data integrity), assessment of various threats on the security of cloud environment, evaluation and analysis of security and performance parameter like encryption time, decryption time, throughput and network delay and ensuring appropriate load balancing with metrics like throughput, response time, migration time, scalability and fault tolerance.

A. Proposed Algorithm

Step 1

User Login from the Client Software

Step 2

Establishment of Validation

TPA Registration - Main Server Login: Username, Password, MAC address will send to the Main Server.

Step 3

First Encryption of Username, Password and MAC address using AES and fully Homomorphic Algorithm

*1) Input of A; SK (username, password, MAC)) /*SK – Signature Name*/*

2) Input of B; BK (where BK is the apply AES algo first and then apply gates operation to convert plain SK text to cipher text)

*3) Output; LK+ 1(output of signature in cipher text form) /*LK – Final Signature*/*

Step 4

TPA Server will verify the Signature in the Database: If signature gets match then reply to user with success message as well as to main server with success message.

Step 5

TPA Server will perform Handshaking procedure 10 times with recently authorize client based on the specific format in which TPA server send message to client 10 times asking "Show Your Identity". In respect the client reply, TPA communicates with following format to server "Yes Authenticated: IP, MAC, Name of OS, Hardisk Address". If out of 10, 9 responses are found true then TPA issues Session Number to Main server respect to the Client.

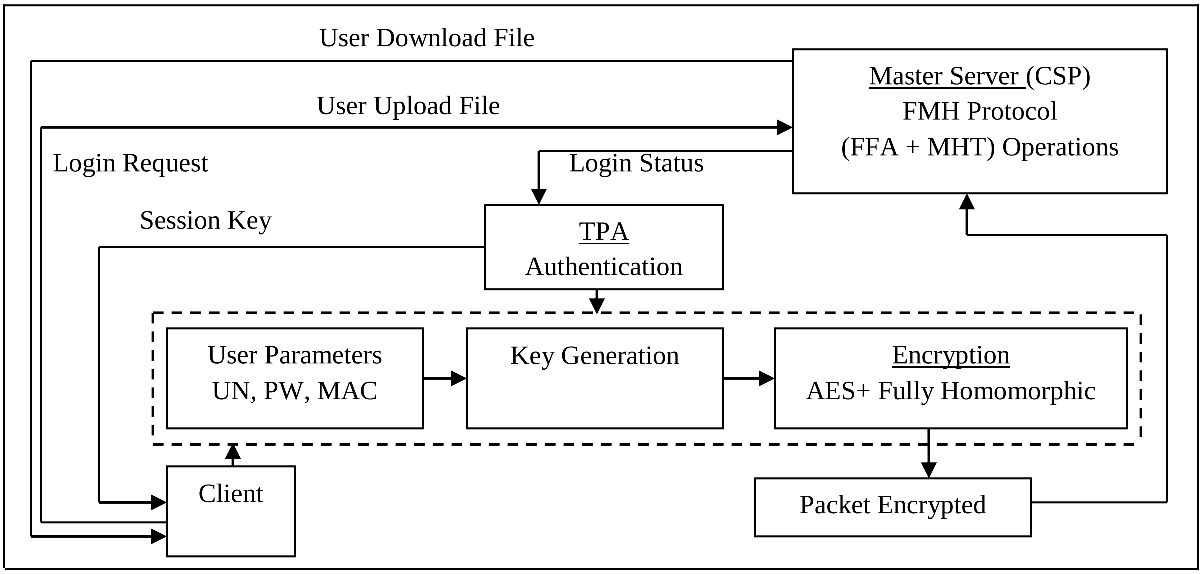


Fig. 1. TPA-FMHP based Proposed Cloud Security Model

Step 6

a) TPA sends prime number to the client who is going to upload the file.

b) Client receives the public and private key (computed by MS using NTRU algorithm)

/*NTRU (N-th degree Truncated Polynomial Ring Unit Algorithm) is based on polynomial arithmetic and provides very fast computation for the encryption and decryption of the message*/

1) The operations are based on objects that are in a polynomial ring: R = Z [X] / (XN - 1)

2) The polynomials, present in the ring have integer coefficients and degree N – 1:

Key Generation:

/*NTRU involves a public key and a private key. The public key is used for encrypting message and can be known to everyone. Messages encrypted with this key can only be decrypted in a reasonable amount of time using the private key*/

*1) For the encryption, let m be the polynomial representing a message. We choose a small polynomial r as the random blinding polynomial, and compute the ciphertext c = p*r*h + m mod q.*

*2) For the decryption of c, a = f*c mod q is computed firstly, where the modulo q operation is done in an appropriate interval. Then the plaintext m = a mod p is recovered.*

/*NTRU based convolution product computation algorithm is widely used in software implementation [28] */

Both A and B

PK1 + 1 ← generate an initial key of fireflies (LK)

/*pass Generated key from NTRU to initiate Firefly as well as convert plain text to cipher on every rotation*/

For (A + 1) do (where A would 1 to n value)

A (plaintext)

ω4←count (n) apply encryption till of n

TK← ω4

αB ← E_{PK} (plaintext)(conversion of plaintext into ciphertext)

Step 7

Compression Process

a) Take ciphertext file generated on above steps.

b) Convert the file into the binary form using MHT hash function algorithm.

c) Split the binary content in 32 bit blocks using MHT.

d) Pass these 32 bit blocks into LZW string compression algorithm. It returns compressed blocks.

e) Arrange the blocks in tree format.

f) Assemble various chunks starting from the root till all blocks are covered using DFS support.

g) All blocks are then converted into string and write a new file.

/* LZW sting Compression algorithm is dictionary based algorithm which output a code for a character. Input data to compress is read from the file. Output codes have less number of bits than input data [29]*/

String s, char c;
s- Get input character
While (there is still input character)
ch- transfer input string to ch.
If (ch is in dictionary)
Generate its codeword;
Else
Update ch and get next character to ch and
Again search data in dictionary;

If (it is not present in dictionary) then
Add that string to dictionary;
End if;

Decompression process

/*In LZW decompression algorithm, it needs to take the stream of code output from the compression algorithm, and use them to exactly recreate the input stream*/

ch = output code
While (there is still data to read)
Code =get input character;
If (code is not in the dictionary)
Entry =get translation of code;
Else
Entry=get translation of output code;
Output entry;
ch =first character in entry
Add output code + c to the dictionary
Output code = code;

/*In decompression algorithm, code will be searched in dictionary and its character will be output*/

Step 8

Decryption using firefly algorithm

B
A←D_{SK} (B) /* only B can decrypt the result. Here B will generate hash and send back to A*/
If R= 1 then /*1=true 0=false*/
TK=D_{SK} (put cipher text)/* convert cipher text to plain*/
End if
End for
End.

Step 9

Concurrency Management using MHT algorithm

a) Initiate from the root. Root will update all the child nodes (connected to the parent node) using Merkle hash tree algorithm.

b) The process terminates as all nodes of the network are updated.

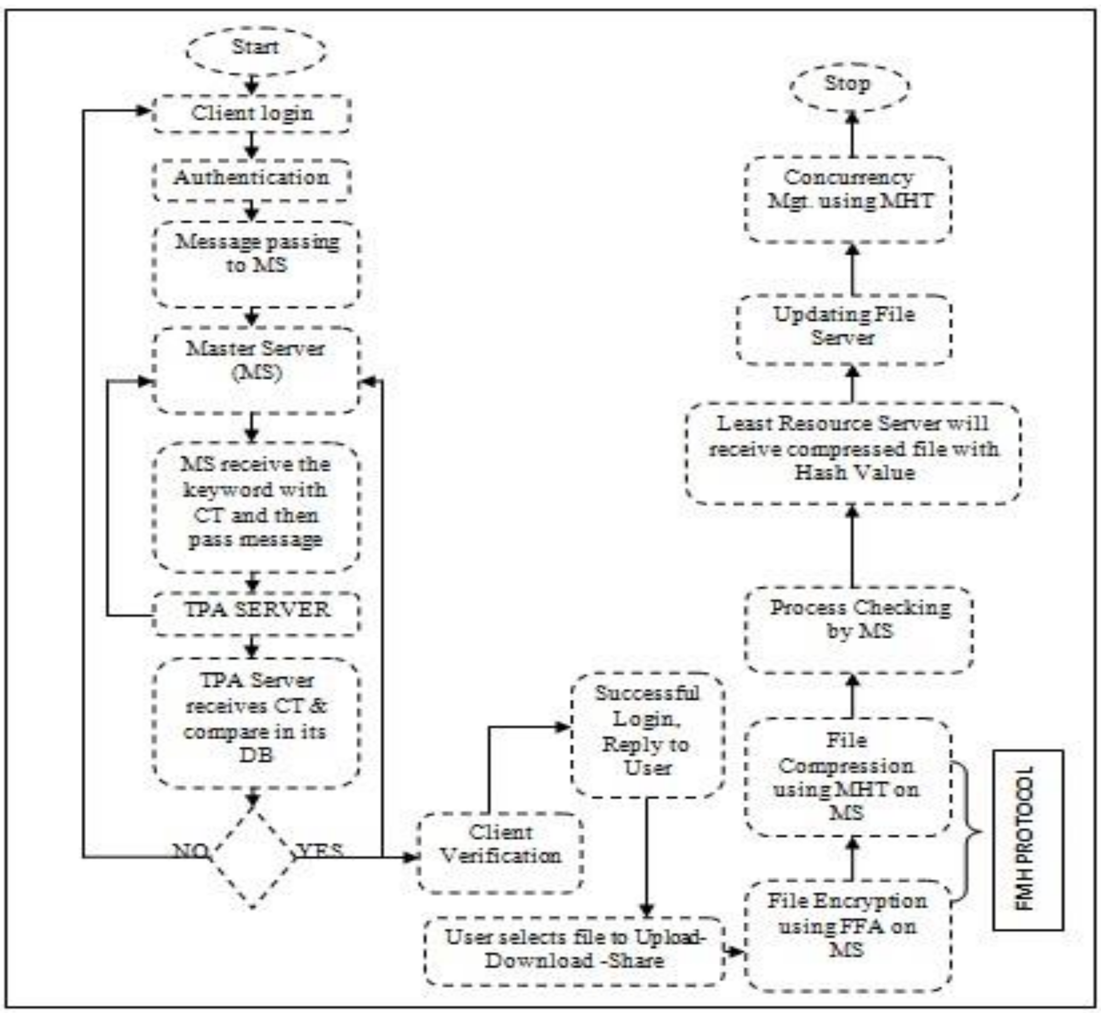


Fig. 2. Flow Chart of the Proposed System

I. CONCLUSION

The payback of the clouds computing is to accomplish the economics of scale, diminish the expenses on technology infrastructure, improves ease of access and monitoring the projects more efficiently. In addition, ensuring the security of client's data is the prime focus. In this paper, the cloud computing key issues are discussed and new integrated protocol model for information protection and load management is suggested.

The performance of the proposed system will be evaluated and justified in preventing anxious attacks on the security of cloud environment. Assessment and investigation of security and performance parameters will be the part of the apprehension along with ensuring suitable load balancing.

The potential work can be constructive to expand the security and performance of cloud computing during different communication modules.

REFERENCES

[1] Farzad Sabahi, "Cloud Computing Security Threats and Responses", In the Proceeding of IEEE 3rd International Conference on Communication Software and Network, pp. 245-249, May 2011.

[2] Xiang Tana, Bo Aib, "The Issues of Cloud Computing Security in High-speed Railway ", In the Proceeding of IEEE International Conference on Electronic & Mechanical and Engineering and Information Technology, pp. 4358-4363, Aug 2011.

[3] Yanuarizki Amanatullah, and Heru Purnomo Ipung, "Toward Cloud Computing Reference Architecture: Cloud Service Management Perspective", In the Proceeding of IEEE International Conference on ICT for Smart Society (ICISS), pp. 1-4, June 2013.

[4] Qiang Guan, Chi-Chen Chiu and Song Fu, "CDA: A Cloud Dependability Analysis Framework for Characterizing System Dependability in Cloud Computing Infrastructures", In the Proceeding of IEEE 18th International Conference on Dependable Computing, pp. 11-20, Nov 2012.

[5] WANG En Dong WU Nan, LI Xu, "QoS-oriented Monitoring Model of Cloud Computing Resources Availability", In the Proceeding of IEEE International Conference on Computational and Information Sciences, pp. 1537-1540, June 2013.

[6] Mohemed Almorsy, John Grundy and Amani S. Ibrahim, "Collaboration-Based Cloud Computing Security Management Framework", In the Proceeding of IEEE International Conference on Clouding Computing (CLOUD), pp. 364-371, July 2011.

[7] Maha Attia Hana, "E-Government Cloud Computing Proposed Model: Egyptian E_Government Cloud Computing", In the Proceeding of IEEE International Conference on Advanced in Computing Communication and Information (ICACCI), pp. 847-852, Aug 2013.

[8] Wei Zhao, Yong Peng, Feng Xie, and Zhonghua Dai, "Modeling and Simulation of Cloud Computing: A Review ", In the Proceeding of IEEE International Conference on Asia Pacific Cloud Computing Congress (AP Cloud CC), pp. 20-24, Nov 2012.

[9] Nimmy K., M. Sethumadhavan, "Novel Mutual Authentication Protocol for Cloud Computing using Secret Sharing and Steganography", In the Proceeding of IEEE fifth International Conference on Application of Digital Information and Web Technologies (ICADIWT), pp.101-106, Feb 2014.

[10] Shuai Han, Jianchuan Xing, "Ensuring Data Storage Security Through a Novel Third Party Auditor Scheme in Cloud Computing", In the Proceeding of IEEE International Conference on Cloud Computing and Intelligence System (CCIS), pp. 264-268, Sept 2011.

[11] Dinesha H A, Agrawal V K, "Multi-level Authentication Technique for Accessing Cloud Services", In the Proceeding of IEEE International Conference on Computing Communication and Application (ICCCA), pp. 1-4, Feb 2012.

[12] Qian Wang, Cong Wang, and Kui Ren, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing", In the Proceeding of IEEE Transaction on Parallel and Distributed Systems, Vol. 22, No. 5, pp. 847-859, May 2011.

[13] Ching-Nung Yang, Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", In the Proceeding of IEEE International Conference on Biometric and security Technology, pp. 259-266, July 2013.

[14] Sue-Chen Hsueh, Jing-Yan Lin, and Ming-Yen Lin, "Secure Cloud Storage For Convenient Data Archive Of Smart Phones", In the Proceeding of IEEE International Conference on Consumer Electronics, pp. 156-161, June 2011.

[15] Bhavna Makhija, VinitKumar Gupta, and Indrajit Rajput, "Enhanced Data Security in Cloud Computing with Third Party Auditor", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 3, No. 2, Feb 2013.

[16] Zhifeng Xiao and Yang Xiao, "Security and Privacy in Cloud Computing" In the Proceeding of IEEE Conference on Communication Surveys & Tutorials, Vol. 15, No. 2, pp. 843-859, May 2013.

[17] Cong Wang, Sherman S.M. Chow, and Qian Wang, "Privacy-Preserving Public Auditing for Secure Cloud Storage", In the Proceeding of IEEE Transaction on Computers, Vol. 62, No. 2, pp. 362-375, Feb 2013.

[18] Hsiao-Ying Lin, and Wen-Guey Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding", In the Proceeding of IEEE Transaction on Parallel and Distributed Systems, Vol. 23, No. 6, pp. 995-1003, June 2012.

[19] Yang Tang, Patrick P.C. Lee, and John C.S. Lui, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", In the Proceeding of IEEE Transaction on Dependable and Secure Computing, Vol. 9, No. 6, pp. 903-916, Nov 2012.

[20] Assad Abbas and Samee U. Khan, "A Review on the State-of-the-Art Privacy-Preserving Approaches in the e-Health Clouds", Journal of Biomedical and Health Information, Vol. 18, No. 4, pp. 1431-1441, July 2014.

[21] Ching-Nung Yang, and Jia-Bin Lai, "Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing", In the Proceeding of IEEE Transaction on Biometrics and Security Technologies (ISBAST), pp. 259-266, July 2013.

[22] Jingxin K. Wang, Xinpei Jia, "Data Security and Authentication in Hybrid Cloud Computing Model" In the Proceeding of IEEE International Conference on Global High Tech Congress on Electronic (GHTCE), pp. 117-120, Nov 2012.

[23] Mohamed Nabeel and Elisa Bertino, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transaction on Knowledge and Data Engineering, Vol. 26, No. 9, pp. 2268-2280, Sep 2014.

[24] Moghaddam, Faraz Fatemi, Shiva Gerayeli ; Rouzbeh, Sohrab ; Araghi, Sagheb Kohpayeh ; Alibeigi, Nima Morad ; Varnosfaderani, Shirin Dabbaghi, "A Scalable and Efficient User Authentication Scheme for Cloud Computing Environments", IEEE symposium, Kuala Lumpur, Malaysia, pp. 508-513, 2014.

[25] G. Jai Arul Jose, C. Sajeev, Dr. C. Suyambulingom, "Implementation of Data Security in Cloud Computing", International Journal of P2P Network trends and Technology, Volume 1, Issue 1, pp 18-22, 2011.

[26] E. M. Mohamed, H.S. Abdelkadar, S.E. Etriby, "Enhanced Data Security Model for Cloud Computing", International Conference on Informatics and Systems, 2012.

[27] V. Nirmala, R. K. Shivanadhan, R. S..Lakshmi,"Data Confidentiality and Integrity Verification using User Authentication Scheme in Cloud", International Conference on Green High Computing, IEEE, pp 1-5, 2013.

[28] Xuexin Zheng, An Wang, Wei Wei, "First-order collision attack on protected NTRU cryptosystem", Microprocessors and Microsystems, Elsevier, pp 601–609, 2013.

[29] S. Kaur, V.S. Verma, "Design and Implementation of LZW Data Compression Algorithm", International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[30] Patrascu, V.V. Patriciu, "Logging for Cloud Computing Forensic Systems", International Journal of Computer Communication and Control, ISSN 1841-9836, 10(2):222-229, April, 2015.

Modeling Knowledge Bases for Automated Decision Making Systems – A Literature Review

Franz Felix Füssl, Detlef Streitferdt
Institute for Computer and Systems Engineering
Technische Universität Ilmenau
Ilmenau, Germany

Anne Triebel
Institute for Business Information Systems Engineering
Technische Universität Ilmenau
Ilmenau, Germany

***Abstract*—Developing automated decision making systems means dealing with knowledge in every possible manner. One of the most important points of developing artificial intelligent systems is developing a precise knowledge base with integrating self-learning mechanisms. Moreover using knowledge in expert systems or decision support systems it is necessary to document knowledge and make it visible for managing it. Main goal of this work is finding a suitable solution for modeling knowledge bases in automated decision making systems concerning both illustrating specific knowledge and learning mechanisms. There are a lot of different terms describing this kind of research, such as knowledge modeling, knowledge engineering or ontology engineering. For that reason this paper provides a comparison of the technical terms in this domain by illustrating similarities, specifics and how they are used in literature.**

***Keywords*—Knowledge Base; Knowledge Modeling; Knowledge Engineering; Ontology Engineering; Artificial Neural Network; Expert System**

I. Introduction

An automated decision making system (ADMS) is software that is used to make decisions application-specific and mostly autonomous. Based on rules and a consistent knowledge base such a system is able to provide solutions for different issues. The underlying knowledge is one of the most significant components and has to be modeled in a specific way. There are different options for modeling the knowledge base, especially for ADMS in the topic of large software development projects. Regarding to [1] it is necessary to identify ADMS for software development projects and in that context to reveal existing knowledge models. Therefor a comprehensive literature review according to Webster and Watson [2] will be conducted. Moreover the terms 'modeling knowledge' and 'automated decision making system' will be analyzed for distinction.

The paper addresses concretely an analysis of literature about modeling knowledge bases for ADMS that could be used for choosing toolsets in large software development projects.

As methodological approach a literature review according to Webster and Watson was selected. It can be used as basis for researching and analyzing current standards of information technology issues. Webster and Watson [2] categorize two intentions for literature reviews. For one thing it serves to specify or extend a given topic by reference to existing publications. Otherwise it can be used for developing new concepts or models by analyzing theoretical principles and previous works. Accordingly this paper presents a literature review with the first described intention about modeling knowledge bases for ADMS concerning toolsets for large software development projects. First of all the concepts or rather the keywords based on the issue to be edited have to be determined. A simple mind map is very suitable for this and will be pictured. When all relevant literatures are selected by forwards and backwards searches, the concept-matrix will demonstrate all publications identified and their affiliation to the concepts. Subsequently the topic can be analyzed and important facts will have to be presented.

This document is structured as follows: After the introduction the procedure of identifying relevant literatures are detailed in chapter II. The chapter describes the used publication databases and the searched keywords. TABLE I. contains the identified literature combined with their connection to the settled concepts and summarizes the research findings. Chapter III shows different definitions of the authors about the concepts and centralizes the important results of the literature review. Finally a conclusion is displayed with main facts of the analysis and an outline for further investigations.

II. Identifying of Literature

The main facts of the analysis to be created are due to the topic 'modeling knowledge bases for automated decision making systems'. Webster and Watson [2] describe the concepts as segments of the main issue with partially similar meaning or completely various facets. The authors of this paper concretized the concepts through brainstorming as Fig. 1 shows.

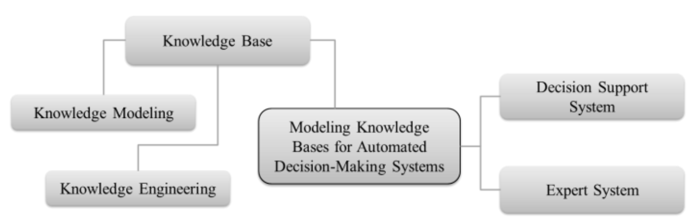


Fig. 1. Mindmap about relevant items

'Knowledge base' is deemed to be a superordinate term for knowledge modeling and knowledge engineering and will not be used for this research. The specific year range for the publications is defined from 2000 to 2015 with focus on the last 5 years based on the importance of actuality of contributions. Another reason is to generate a restrictive number of significant publications for analyzing. The following publication databases were used for identifying literatures due to the settled concepts: ACM Digital Library, AIS Electronic Library, EBSCO, ELSEVIER and IEEE Xplore Digital Library. In total the research aggregates to 58 papers. After examining for relevance there are 26 publications for analyzing the topic to be edited.

TABLE I. shows the concept matrix with the settled keywords and the leading authors who discuss the topics. The certain fields of application will not be displayed in this matrix but the following chapter will constitute the different range of subjects.

TABLE I. CONCEPT MATRIX

References	Knowledge Modeling	Knowledge Engineering	Decision Support System	Expert System
Chan (2002)	x	x		x
Colloc et al. (2000)			x	
Gerards et al. (2011)				x
Ghoniemy et al. (2013)		x		x
Guaglianone et al. (2011)		x		
Guan et al. (2012)				x
Guo et al. (2008)				x
Hall (2012)		x		
Hwang et al. (2011)				x
Kulinich (2012)				x
Liu et al. (2010)	x			x
Lu et al. (2001)			x	
Mendis et al. (2007)	x			
Mistrík et al. (2014)		x		
Moawad et al. (2013)		x		
Nguyen et al. (2000)				x
Oguntimilehin et al. (2014)			x	
Paul et al. (2012)			x	
Popescu et al. (2014)			x	
Prat et al. (2010)			x	
Ramirez et al. (2011)	x			
Sheng et al. (2010)			x	
Tang (2014)				
Wang et al. (2011)				x
Wu et al. (2015)		x		

The table displays the occurrence of the concepts dependent on the combination of the terms within the research. Expert system (ES) and decision support system (DSS) are established keywords that will be often used in publication databases. Knowledge engineering or knowledge modeling combined with DSS or ES were less found in articles as shown in the concept matrix. The keyword 'knowledge modeling' is currently used very rare in combination with an ADMS. It could indicate that knowledge modeling is rather called knowledge engineering and it could probably mean the same. The research implies that there are representative contexts between the settled concepts and knowledge engineering is more acknowledged than knowledge modeling. In the following chapter the settled subjects must be defined and made distinguishable.

III. ANALYSIS AND DISCUSSIONS

At first the terms knowledge engineering and knowledge modeling will be investigated by analyzing the founded articles and their definitions. Afterwards the major differences between DSS and ES will be investigated. Consequently based on these descriptions the areas of application where knowledge models are used for ADMS will be described. In particular it will be examined if there are existing researches on the subject of large software development projects.

A. Knowledge Modeling vs. Knowledge Engineering

Knowledge engineering and knowledge modeling are used by most of the authors in a similar manner depending on the target domain [3], [4], [5], [6], [7], [8], [9], [10], [11] and [12]. Chan et al. considered in [13] the process of knowledge acquisition and modeling for structuring the knowledge base of an ES. In fields of product redesign and mechanical engineering, an ontology based knowledge model and reuse approach was studied by Liu et al. [7]. Here an ontology modeling method was considered for solving redesign problems based on an existing knowledge design that must be used in an effective and efficient way. According to Mendis et al. [8] knowledge modeling addresses languages, tools, techniques and methods to develop abstract models of some target domain or problem solving behavior. Some examples for tools and methods, that are serving to structure and represent knowledge, are semantic nets, topic maps or ontologies. A semantic net constitutes concepts and their relations with the aid of equivalent structures in terms of a graph with nodes and edges [15]. Topic maps, also called as knowledge maps, consist of subjects (topics, associations and occurrences) that are depicted in a human way of knowledge processing. Their description as XML enables for topic maps to be machine-readable. In the first place topic maps serve to a better navigation and search in internet resources and also for exchanging of metadata [16]. According to Chan [3] ontology offers a set of concepts and terms to describe a domain and those terms are used by knowledge bases for representing true about some real or imaginary world. It is a symmetric representation of knowledge with mechanism of inheritance to generate an ambiguous communication, for instance based on the Web Ontology Language.

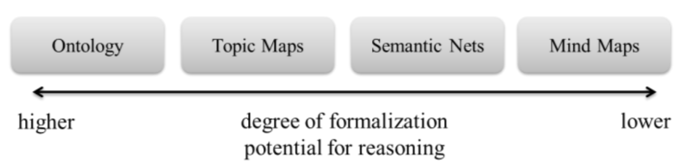


Fig. 2. Tools for knowledge modeling

According to [17] Fig. 2 shows the described tools dependent on their respective degree of formalization and thus their potential for reasoning. As brainstorming tool mind map symbolizes at this point just an arbitrary description of information in a specific use case.

Knowledge modeling is also used in the domain of intelligent personalization of cognitive learning activities as Ramirez et al. [11] described. Here it is demonstrated how to associate main body units of knowledge to previous and future learned knowledge referring to basic of semantic net. Chan [3] defines knowledge models as problem-solving models of real world application domains for increasing effectiveness of knowledge based systems. In addition to developing effective knowledge bases, knowledge models serve to enable sharing and reuse of knowledge. Thus modeling knowledge bases can be used for structuring their information, data and associations by using methods of ontology and additionally generate sharing and reuse knowledge.

Chan [3] speaks of knowledge engineering as "process of eliciting expertise, organizing it into a computational structure, and building knowledge bases. This is a process that addresses directly internal information processing mechanisms and processes of human experts." Furthermore Chan issues that ontology engineering is deemed to be the successor of knowledge engineering. Ontology engineering shall improve a long-term efficiency of a knowledge based system development process, even in distributed environments. The authors Matta et al. [14] and Guaglianone et al. [5] describe knowledge engineering likewise for acquiring and modeling knowledge and for developing ES. It can be adapted to answer to aims of knowledge management. Hall [6] attends to the question concerning knowledge engineering in which way knowledge has to be integrated into a computer system. The knowledge in engineering design varies from that one in science. In particular modeling knowledge in science includes topics of decision making, reasoning, problem solving and the nature of thought itself. Whereas engineering knowledge for instance in an ES involves heuristics, theories, tools and techniques.

Ontology engineering as machine-readable method for modeling ontology-based knowledge bases to develop ES needs to be analyzed in more detail. According to [17] and [18] an ontology model is a purposeful created engineering artifact that serves for extensive declarative description of decision making models to reduce false reasoning and increase useful automatic interpretations and processing. Thereby it is difficult to afford a temporal stability of the ontology and most of all in cases of great and various ontologies to have a consistent formality and integrity of modeling. Moreover the scalable reasoning in ontology engineering is still not investigated for instance as an abstract model.

There are a range of tools for constructing ontologies for instance to model products and processes or to manage ontologies. Ontology maps attempt to automatically manage different ontologies for the purpose of information integration. However there also is given a lack of consistent formality and integrity of modeling [18].

The subject 'expert system' is still used in combination with knowledge engineering or ontology engineering. In the following it has to be defined where are the differences between DSS and ES.

B. Decision Support System

First time it was spoken about DDS was introduced by Morton [19] in terms of managing decision systems. Fick and Sprague [20] define a DSS as computerized planning and information system that presents useful information from raw data, documents or personal knowledge for helping to solve problems and make decisions, sometime in a graphical way. Based on comprehensive databases and settled rules such a knowledge-based system for decision making are applied to analyze, plan, budget as well as calculate data for strategic activities. According to [21], [22] and [23] DSS are often used for clinical and medical diagnoses and therapy decisions. Lu et al. [24] developed a prototype of a multi-objective group decision support system that addresses interactive applications for decision making by a group of participants which are not staying at the same place. Another group decision support system was used for railway construction decisions by Sheng et al. [25]. In most of these fields of application for DSS a simple decision tree was evolved to set the rules and thus to aggregate information or knowledge for presenting.

When a system is used to generate new knowledge, it is usually an ES, not a DDS. So the main difference between DSS and ES is in the fact of acquiring new knowledge, for instance an ES with a well modeled ontology-based knowledge base or an ES with a self-learning component such as artificial neural network.

C. Expert System

According to Russell et al. [26] "an expert system can be defined as an intelligent system that can mimic some part of human intelligence". To develop an artificial intelligence system it needs to be identified how intelligent behavior of human experts can be replicated by a computer system [27], [31]. ES are built by acquiring the knowledge from human experts and coding it into a machine-readable form. In combination with inference rules, e.g. cause/effect, situation/ action, if-then-else, it is used for problem solving, decision making, designing, planning, monitoring, diagnosing and training activities [27]. The literature has reported that people have difficulty in solving multi-dimensional problems of unknown issues fastest possible. In these cases human cognition reaches their limits [28]. An ES bunches expert and experience knowledge and supports decision makers in problem solving as a human expert of each specific domain at any time.

Guan et al. [29] also describe a weakness of traditional ES. It lies in the fact that there could be a lack of completeness in terms of covering various types of different knowledge (expert knowledge and knowledge acquisition), for instance in his field of application 'financial internal control systems'. According to Chan [3] constructing an ES is a knowledge intensive process and knowledge engineering or modeling is often adopted for building the knowledge base. Accordingly the modeled knowledge base and its continuous enhancement by knowledge acquisition, using the ES, is one of the most important points.

As said by Tian et al. [30] and Qian et al. [32] artificial neural networks combined with knowledge bases can be used for developing ES and could give the possibility to construct a self-learning ES. An artificial neural network is, in accordance with [32], “a collection of basic units to compute a non-linear function of their input. Every input has an assigned weight that determines [its] impact […] on the overall output of the node.” Thus an ES is able to access a knowledge base that will be trained by artificial neural networks based on user input as well as the acquired and expert knowledge.

Fig. 3 illustrates in a simple way components and relations of ES and the acquiring knowledge process. Also it shows the relationship between knowledge modeling, knowledge engineering and ontology engineering. Decision makers can use an ES for solving problems. Based on rules and inference mechanism an inference system communicates to the knowledge base that can be modeled with methods of ontologies engineering. Knowledge bases of ES consist human-specific domain knowledge (expert knowledge) as well as experience knowledge, which is acquired from the ES itself. Artificial neural networks can be included in developing the knowledge base and for training the system. As result represented knowledge is made based on the inference system combined with the ontology-based knowledge base and/or for instance on the basis of artificial neural networks, as [30] investigated.

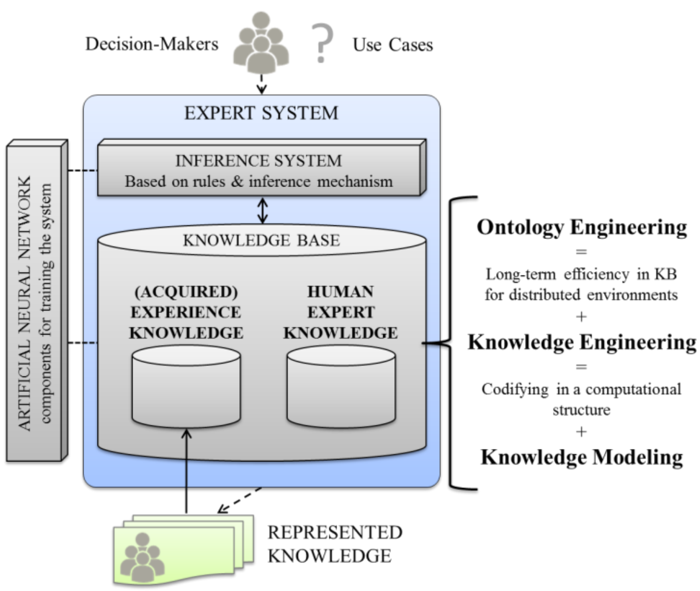


Fig. 3. Components and relations of Expert Systems

As described above inference methods and knowledge base provide the foundation of ES. Major problem of splitting these components is differentiating between human readable illustrating of knowledge and machine learning creating of knowledge. A model that combines visualization knowledge and inference mechanism would serve as better approach for building knowledge bases in ES.

D. *Fields of application*

The literature review has shown that DSS and ES are often used in the domain of medicine and therapy. Furthermore decision making systems are integrated in control or detecting failure systems for example in finance. Also in the fields of economics such as analyzing customer needs or designing industrial or service products ES are increasingly used. During the study of the identified literature it was not found any ES or DSS within the subject of large software development projects and their toolsets. These listed fields of application are just examples and no claim is raised on completeness.

IV. Conclusion

Elaboration of this paper has shown that the manner of modeling knowledge bases of any decision making system is an important step to develop an ES. The tools for knowledge modeling are different dependent on their potential for reasoning. Ontology engineering is the successor of knowledge engineering and enables long-term efficient knowledge within the knowledge base. The limits of ontology engineering lie in combining various ontologies and creating a consistent formality and integrity of modeling as well as scalable reasoning. Artificial neural networks combined with ontology engineering and topic maps as methods for modeling a knowledge base of an ES can be appointed to build a self-learning ADMS.

By the example of choosing the ideal toolset in large software development projects, that may consist of project management, development or administration tools, an abstract knowledge model can be investigated and hence to fill the gaps of ontology engineering additionally. For this reason techniques of ontology engineering and artificial neural networks should be combined for developing a self-learning human-readable ES in the future.

Ackknowledgments

We acknowledge support for the Article Processing Charge by the German Research Foundation and the Open Access Publication Fund of the Technische Universität Ilmenau.

References

[1] F.F. Fuessl, J. Ciemala, "Variable Factors of Influence in Product Line Development", Computer Software and Applications Conference Workshops (COMPSACW), Vasteras, Sweden, 21-25 July, 2014, pp. 390-395

[2] J. Webster, R.T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review”, MIS Quarterly Vol. 26 No. 2, pp. xiii-xxiii, 2002

[3] C.W Chan, “Cognitive informatics: a knowledge engineering perspective”, Cognitive Informatics, pp. 49-56, 2002

[4] S. Ghoniemy, O.H. Karam, “Semantic Network-based Digital Optical Computer Algorithms for Expert Systems and Massively Parallel Knowledge Base Applications”, Journal of Next Generation Information Technology; Vol. 4 Issue 5, pp.133-146, 2013

[5] M.T. Guaglianone, R. Guarasci, N. Matta, J. Cahier, A. Benel, “Comparison and evaluation of knowledge modeling techniques towards the definition of a global approach: MNEMO (Methodology for kNowledgE acquisition and MOdelling)”, Computer Sciences and Convergence Information Technology (ICCIT), pp. 777-782, 2011

[6] J.G. Hall, “Engineering knowledge engineering”, Expert Systems: International Journal of Knowledge Engineering and Neural Networks, Vol 29(5), pp. 427-428, 2012

[7] X. Liu, D. Rosen, Z. Yu, “Ontology based Knowledge Modeling and Reuse Approach in Product Redesig”, Information Reuse and Integration (IRI), pp. 270-273, 2010

[8] D.S.K. Mendis, A.S. Karunananda, U. Samaratunga, U. Ratnayake, “Tacit knowledge modeling in Intelligent Hybrid systems”, Industrial and Information Systems - ICIIS, pp. 279-284, 2007

[9] I. Mistrík, S. Beecham, I. Richardson, A. Avritzer, “Knowledge engineering in global software development environments”, Expert Systems: International Journal of Knowledge Engineering and Neural Networks, Vol 31(3), pp. 232-233, 2014

[10] N. Moawad, K. Liu, M. El-Helly, “Integrating Activity Theory and Semiotics as Knowledge Elicitation Technique”, Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), pp. 137-142, 2013

[11] C. Ramirez, B. Valdes, “Memory Map of a Knowledge Representation model used for intelligent personalization of learning activities sequences”, Cognitive Informatics & Cognitive Computing, pp. 423-431, 2011

[12] X. Wu, H. Chen, G. Wu, J. Liu, Q. Zheng, X. He, A. zhou, Z. Zhao, B. Wei, Y. Li, Q. Zhang, S. Zhang:, “Knowledge Engineering with Big Data”, Intelligent Systems, IEEE, pp. 1-19, 2015

[13] C.W. Chan, Y. Peng, L. Chen, “Knowledge acquisition and ontology modeling for construction of a control and monitoring expert system”, International Journal of Systems Science, 33(6), pp. 485-503, 2002

[14] N. Matta, J.L. Ermine, G. Aubertin, J.Y. Trivin, “Knowledge capitalization with a knowledge engineering approach: the MASK method”, Knowledge management and organizational memories, R. Dieng-Kuntz,N. Matta, Kluwer Academic Publishers, 2002

[15] T. Berners-Lee, J.A. Hendler, O. Lassila, “The Semantic Web”, Scientific American, 284(5), pp. 34-43, 2001

[16] S. Pepper, “The TAO of Topic Maps” http://www.ontopia.net/ topicmaps/materials/tao.html, 2002

[17] C. Brewster, Y. Wilks, “Ontologies, Taxonomies, Thesauri: Learning from Texts”, Deegan, M. (Hrsg.): The Use of Computational Linguistics in the Extraction of Keyword Information, Proceedings from Digital Library Content Workshop, Centre for Computing in the Humanities, 2004

[18] M. Hepp, “Possible Ontologies: How Reality Constrains the Development of Relevant Ontologies”, IEEE Internet Computing 11(1), pp. 90-96, 2007

[19] M.S.S. Morton, “Management Decision Systems: Computer Based Support for Decision Making”, Division of Research, Harvard University, Cambridge, MA, 1971

[20] G. Fick, R.H. Sprague, “Decision support systems: issues and challenges”, Pergamon Press, Oxford, 1980

[21] D. Popescu, D. Lăptoiu, A. Hadăr, “Intelligent collaborative platform for development of personalized surgical orthopedic guides”, Key Engineering Materials, Vol. 638, p303-309, 2014

[22] A. Oguntimilehin, A.O. Adetunmbi, K.A. Olatunji, “A Machine Learning Based Clinical Decision Support System for Diagnosis and Treatment of Typhoid Fever”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol 4,Issue 6, p961-969, 2014

[23] J. Colloc, L. Bouzidi, “A Framework for Clinical Decision Making and Medical Experience Storing”, ECIS 2000 Proceedings, Paper 125

[24] J. Lu, M. Quaddus, “A Prototype of Multi-Objective Group Decision Support System with a Group AggregationMethod base”, ACIS 2001 Proceedings, Paper 48

[25] Q. Sheng, Z. Lei-shan, Y. Yi-xiang, “A web-based distributed group decision support system for railway construction organization”, Informatics in Control, Automation and Robotics (CAR), pp. 362-365, 2010

[26] S. Russell, P. Norvig, “Artificial Intelligence: A Modern Approach”, 3rd Ed., Prentice Hall, 2010

[27] G. Hwang, C. Chen, P. Tsai, C. Tsai, “An expert system for improving web-based problem-solving ability of students”, Expert Systems with Applications, Vol. 38 Issue 7, pp.8664-8672, 2011

[28] D. Nguyen, D.S. Kira, “Designing Optimal Knowledge Base for Integrated Neural Expert Systems”, AMCIS 2000 Proceedings, Paper 89

[29] J. Guan, A.S. Levitan, “A Model for Investigating Internal Control Weaknesses”, Communications of the Association for Information Systems: Vol. 31, Article 3, 2012

[30] T. Tian, M. Zhu, B. Zhang, “An artificial neural network-based expert system for network topological error identification”, Neural Networks 1995, Vol.2, pp. 882-886

[31] A. Kulinich, “Computer systems for cognitive maps simulation: Approaches and methods”, Automation & Remote Control. Vol. 73 Issue 9, p1553-1571, 2012

[32] F. Qian, L. Xu, “Improving customer satisfaction by the expert system using artificial neural networks”, Intelligent Control and Automation 2008, pp. 8303-8306

Developing a New Integrated Model to improve the using of Classical Approach in Designing Management Information Systems

[1] Mohammad M M Abu Omar, [2] Khairul Anuar Abdullah
Limkokwing University of Creative Technology
Malaysia

***Abstract*—Management information system (MIS) is used to solve management problems in the practical life, the designing and building of the management information systems is done by using one of the systems development methodologies. Classical approach is one of these methodologies which still suffer from some critical problems when it is used in designing and building the management information systems, it consumes more time and cost during its life cycle. This paper develops a new integrated model to minimize the classical approach life cycle in designing and building the management information systems in order to avoid the additional consume in time and cost.**

***Keywords*—Management Information System; MIS; Systems Development Methodologies; Classical Approach; Information System Life Cycle; ISLC**

I. Introduction

The classical approach or (traditional approach) includes the series of stages that are used in building the management information systems [9], these stages are known as classical approach life cycle or the information system life cycle (ISLC) of the classical approach. The work of classical approach always uses the all stages of its life cycle in building the management information systems (MIS's), but this paper develops and presents a new integrated model that leads in many cases to partially use of the classical approach life cycle stages, so this new integrated model will help in solving the classical approach problems which are consuming additional time and cost.

The classical approach life cycle stages are main five sequential steps which are:

1) Planning Stage: it is the first stage in the information system life cycle, the responsibilities of this stage are:

- Defining the problem and collecting the required information about the problem which the system will solve it.[1],[2]
- Determining the user's requirements, which the developed system will solve them. .[1],[2]
- Determining the estimated budget and time to accomplish the system.[1] ,[2]
- Suggesting a solution or list of solutions to the problem.[1],[2]

2) Analysis Stage: it is the second stage in the information system life cycle. In this stage the system analyzer will study each solution in the list of the suggested solutions that is obtained from the previous stage (planning stage) and then choose the best solution. [1],[2]

3) Design Stage: it is the third stage in the information system life cycle. Here, the designer's team will provide all the design necessary requirements such as: input screens, output screens, reports, database and system algorithms. [1] ,[2]

4) Development Stage: it is the fourth stage in the information system life cycle. Here the system will be programmed and operated. [1],[2]

5) Test and Maintenance Stage: it is the fifth (final) stage in the information system life cycle. Here, the system will be tested if it includes some errors or if it needs some improvements to be better and effective in achieving the users' requirements. [1],[2]

The weakness of the classical approach is coming from the permanent use of these all five stages in all cases; because there are many cases which actually need to use some of these stages not to all of them, so this research will solve these problems by developing the integrated model, which will organize the using of the classical approach in building the MIS's in order to solve the management problems.

II. Research Methodologies

The classical approach (traditional approach) life cycle consists sequential steps which makes this methodology simple, easy to use, and simple to implement in building the information systems [6], but at the same time, it still suffers from critical weakness; because of its additional consuming in time [6], which leads also to additional consuming in cost, so this research will help the classical approach to reduce from these problems, by the following research methodologies:

The first main methodology: is to develop a new classification for management problems.

The second main methodology: is to develop a new integrated model which will minimize the classical approach life cycle stages in many cases, this integrated model is designed according to the classification of the management problems in the first main methodology.

A. The first main methodology:

This paper develops a new classification for the management problems; this classification has two main categories:

1) The first Category: in this category, the management problems are divided according to its nature and to its corresponding solutions, as in the following:

a) First order problem: the solution of this problem is clear, and it is usually one, you need only to collect the required information about this problem in order to implement it. So the solution for this type of problems will be defined as: direct solution. [2]

b) Second order problem: The solution of this problem is also clear, but it isn't determined by one solution, there are usually a list of multiple solutions. So the solution for this type of problems will be defined as: indirect solution. [2]

2) The second Category: in this category, the management problems are divided according to the type and nature of computer program (software) that will be used to solve these management problems. In this issue, the research divides the computer programs (software) which will be used by (MIS) in order to solve the management problems into two main types: [1]

a) First level problem: Here, the management problem needs software, which can be founded as s software package, and this means that management problem doesn't need to build and develop new software, but it needs software package which is ready software, that is available directly in the markets.[1]

b) Second level problem: In this case, management problem needs to build and develop its own special software, which (MIS) will use it to solve this problem. [1]

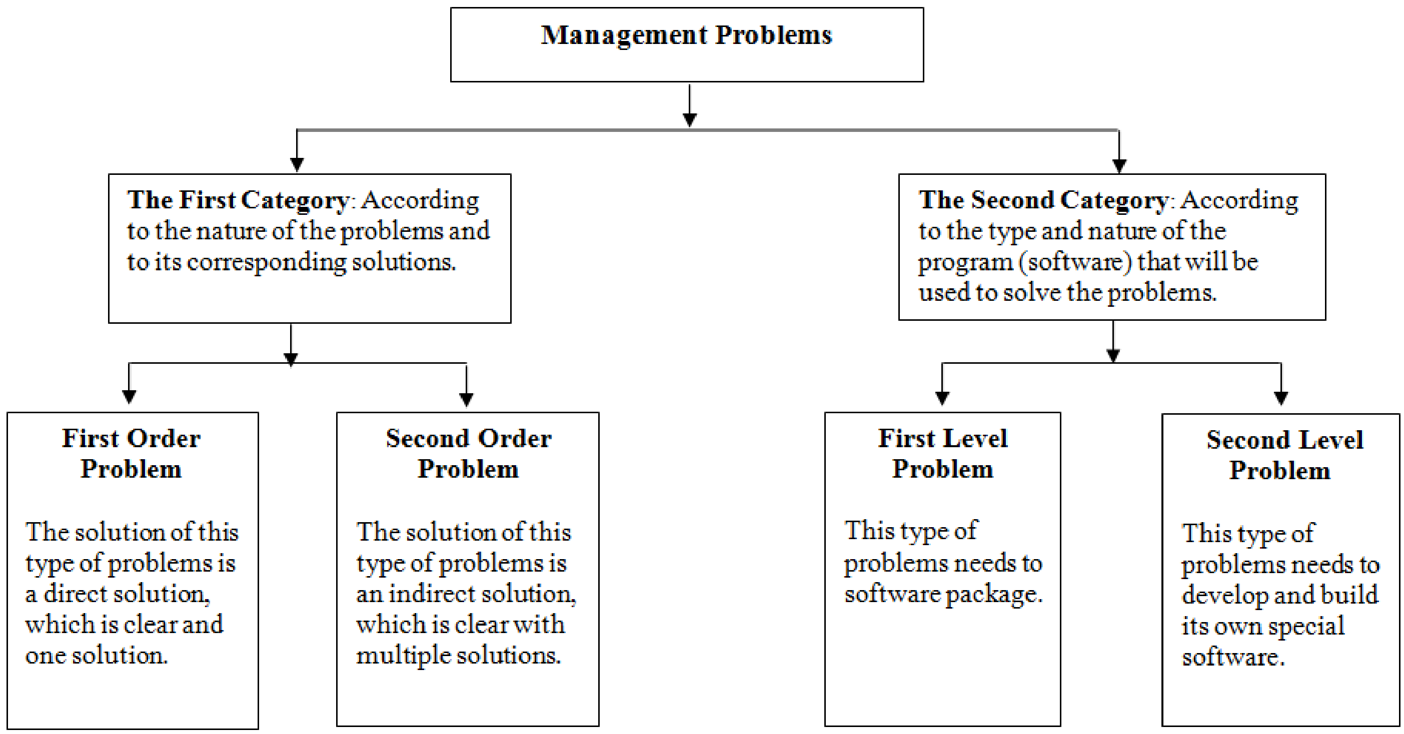


Fig. 1. The Research First Main Methodology

B. The second main methodology:

This research develops and introduces a new integrated model, in order to minimize the classical approach life cycle during the building of management information systems (MIS's), so this integrated model will help the classical approach to reduce the additional consuming in time and cost, and this will increase the efficiency of classical approach in building the MIS's.

The integrated model is developed step by step by finding sub approaches according to the management problems classification, which the research develops and introduces through the first main methodology in the previous section 2.1

1) Analysis the Effect of Management Problems Classification on the Information System Life Cycle (ISLC) of the Classical Approach:

The research will study the effect of each type of management problems on the information system life cycle (ISLC) which is a adopted by classical approach. The analysis will include all types of the management problems that are mentioned in section (2) through the management problems classification, which are: the first category (first order problem, second order problem) and the second category (first level problem, second level problem).

needed in this case, but also must be avoided, since if it is used, this will consume more time, effort and cost through using of the analysis stage, which the determined problem doesn't need, due to its nature and properties.[2]

a) Analysis the Effect of the First Order Management Problems on the ISLC of the Classical Approach:

The research defines the management problem as: first order management problem, when its solution is: direct solution; which is clear, and it is usually one, you need only to collect the required information about this problem in order to implement it.[2]

In this case, there is no need to find multiple solutions to the problem and choose the best solution. This means that there is no need to consume more time, effort and cost in using analysis stage, which is the second stage in the information system life cycle that is adopted by classical approach.[2]

Now, and according to the analysis of the effect of the first order management problem to the (ISLC) of the classical approach, the research develops the MIS approach (1) to build the management information systems which will be used to solve this type of problems. This approach (MIS New approach (1)) will avoid the using of analyses stage through building the management information system by using classical approach. Using this stage is not only

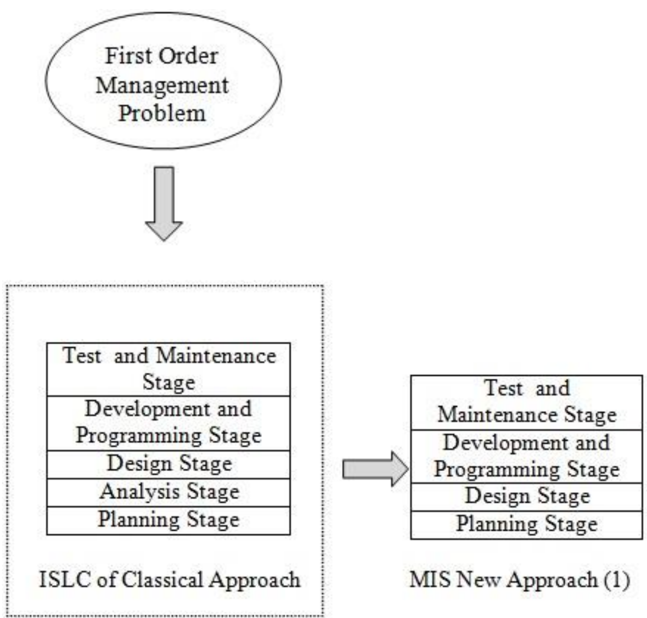


Fig. 2. Finding the MIS New Approach (1)

b) Analysis the Effect of the Second Order Management Problems on the ISLC of the Classical Approach:

The research defines the management problem as: second order management problem, when its solution is: indirect solution; there are usually list of multiple solutions for this type of problems, so this type of problems needs to clarify its solution by finding a list of the suggested solutions, then, the best solution will be chosen, and this will confirm the necessary of using the analysis stage, which is the second stage in the information system life cycle that is adopted by classical approach.[2]

The use of analysis stage in the ISLC of the classical approach will help these problems to change from second order management problem to be first order management problem.[2]

In this case, the research agrees with the current approach which classical approach uses in designing and building management information systems which includes all stages of information system life cycle (ISLC), and defines it as: MIS classical approach, so there is no skip to the second stage in the information system life cycle as in MIS approach (1), all stages must be used, this is because of the properties of this type of problems which are:

a- Solution of this type of problems is clear but it is an indirect solution; since it is not determined by one solution, on the contrary, there is a list of multiple solutions.

b- The existence of multiple solutions for this type of problems, will lead to the need to study each of these solutions in order to detect the best, this means that this type of problems needs (analysis stage) which is the second stage in information system life cycle that is adopted by classical approach.[2]

Test and Maintenance Stage
Development and Programming Stage
Design Stage
Analysis Stage
Planning Stage

Fig. 3. The MIS classical approach which uses all stages of classical approach

c) Analysis the Effect of the First Level Management Problems on the ISLC of the Classical Approach:

Here, management problem needs software, which can be founded as s software package, and this means that management problem doesn't need to build and develop new software, but it needs software package which is ready software, that is available directly in the markets. [1]

If we return to the information system life cycle that is adopted by classical approach, and which has been explained through the introduction in this paper, we will find that the building of the computer program (software), which the management information system (MIS) will use it to solve the management problems, is related directly with the third stage (Design Stage) in the information system life cycle, because the building of the computer program (software) includes already to the building of: algorithms, database, input and output screens, reports,….etc, and these are the responsibilities of the (Design Stage) in the information system life cycle.[1]

Hence, this research provides a scientific contribution which is: the building of computer program (software) will cause the need to use the design stage, and vice versa. So, if there isn't need to build a computer program (software), design stage in the information system life cycle will be skipped. [1]

Now, and according to the analysis of the first level management problems, the research develops a new approach (MIS New Approach (2)) to build the management information system (MIS) which will be used to solve this type of problems.[1]

The MIS new approach will skip the third stage (Design Stage) in the information system life cycle that is adopted by classical approach. this means that this new approach will minimize the information system life cycle to be four stages instead of five stages, and this will cause to reduce the number of employees that will work in the project team, in addition, the use of this new approach will help to save time, effort and cost, and this will lead to increase the efficiency in building and designing the management information systems by using classical approach.[1]

The MIS new approach will use the classical approach and skip the design stage (third stage) in building the management information system (MIS) which will be used to solve the first type of management problems. [1]

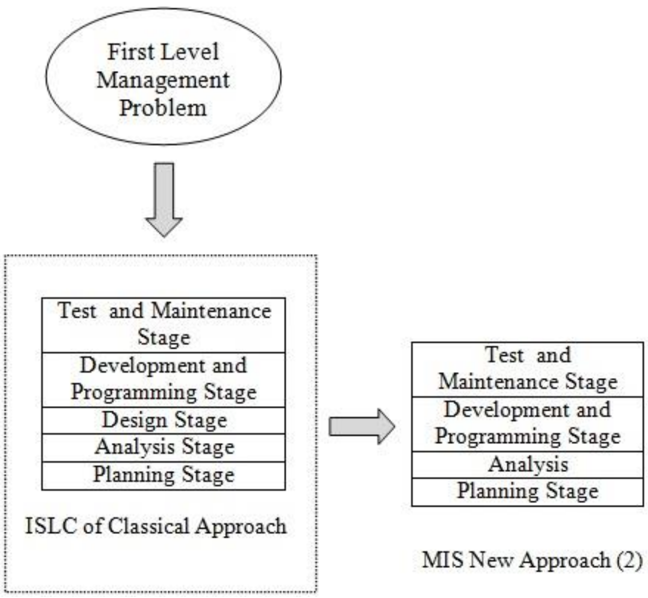


Fig. 4. Finding the MIS New Approach (2)

d) Analysis the Effect of the Second Level Management Problems on the ISLC of the Classical Approach:

In this case, the research agrees with the current approach which classical approach uses in designing and building management information systems, which includes all stages of information system life cycle, and defines it as: MIS classical approach, so in this case, there is no skip to the third stage (Design Stage) in the information system life cycle, as in MIS new approach(2); because and as it is mentioned in the section (2),this type of management problems needs to build its own special software, and this requires the use of design stage in the information system life cycle.[1]

Test and Maintenance Stage
Development and Programming Stage
Design Stage
Analysis Stage
Planning Stage

Fig. 5. The MIS classical approach which uses all stages of classical approach

III. The Combined Management Problems

This research reaches to the new types of management problems and defines these problems as: (Combined Management Problems), these problems are appeared by the combination of two different problems from the problems that research defines them in the research methodology through two main categories which are: the first category (first order problem, second order problem) and the second category (first level problem, second level problem).

A. Finding the Combined Management Problems:

As it is mentioned in the previous section; the combined management problems are appeared by the combination of two different management problems which the research defines them in the research methodology, now we will number each one of these problems as mathematical equations numbering:

* First category ……………………………(1)
 - First order management problem……….(1.a)
 - Second order management problem……(1.b)
* Second Category………………………....(2)
 - First level management problem……….(2.a)
 - Second level management problem…….(2.b)

Now, we will apply the distributed operation between the previous equations:

(1) * (2)…………………….….(X)

Equation (X) implies that:

((1.a) , (1.b)) * ((2.a) , (2.b))………(X^1)

Now, we will list all the results probabilities which will be obtained from the applying of the distributive operation in equation (X^1) :

First probability: (1.a) , (2.a)
Second probability: (1.a) , (2.b)
Third probability: (1.b) , (2.a)
Fourth probability: (1.b) , (2.b)

The previous results will be interpreted, in order to find the new combined management problems:

1) The first combined management problem:

It comes from the first previous probability {(1.a) , (2.a)}, this means that the first combined management problem is a first order management problem and a first level management problem at the same time.

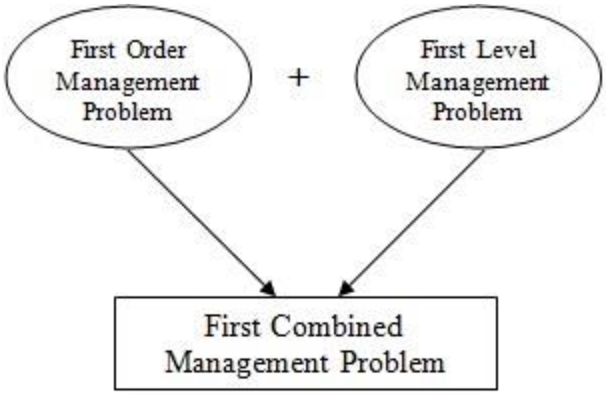


Fig. 6. First Combined Management Problem

and if we return to section 2.2, we can note that the first order management problem leads to use the MIS new approach (1), which skips the analysis stage in the ISLC of the classical approach, on the other hand, the first level management problem leads to use the MIS new approach (2), which skips the design stage in the ISLC of classical approach, and thus, the first combined management problem will combine between the skipping of the two stages: analysis and design.

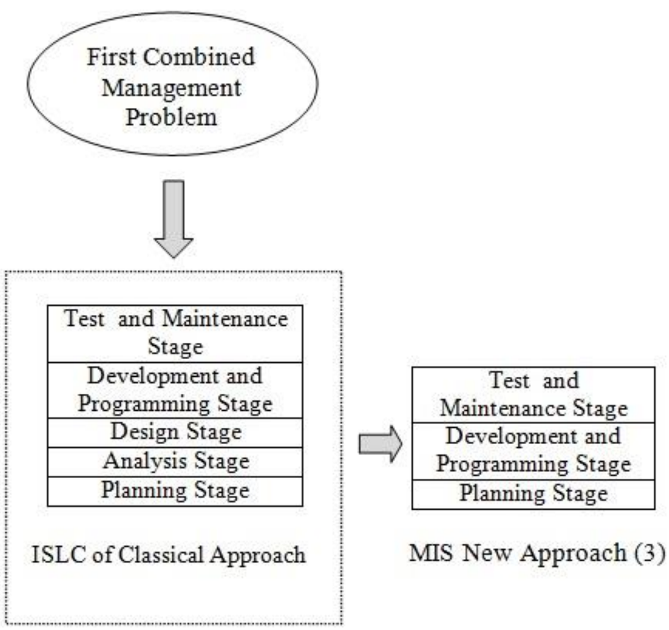


Fig. 7. Finding the MIS New Approach (3)

2) The second combined management problem:

It comes from the second probability {(1.a) , (2.b)}, which means that the second combined management problem is a first order management problem and a second level management problem at the same time.

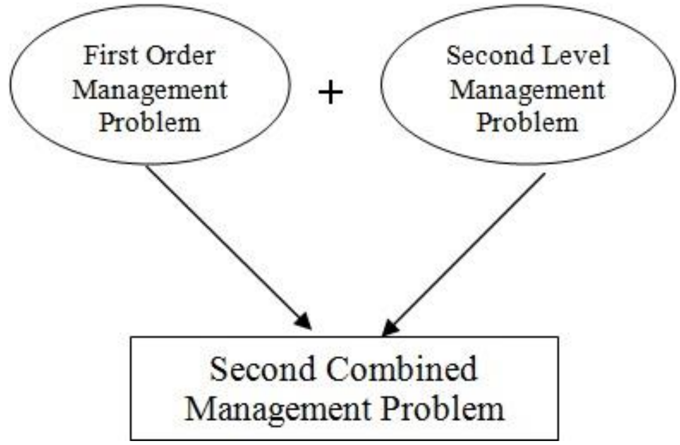


Fig. 8. Second Combined Management Problem

As the research has mentioned, the first order management problem leads to use the MIS new approach (1), which skips the analysis stage in the ISLC of the classical approach, but the second level management problem will use the current life cycle of the classical approach which uses all stages of the INSLC of the classical approach, so the second combined management problem will inherit only the skipping of the analysis stage, and hence, the second combined management problem will not generate a new approach to build the MIS, and instead of this, the research recommends to use the MIS new approach (1) to build the required MIS in order to solve the second combined management problem.

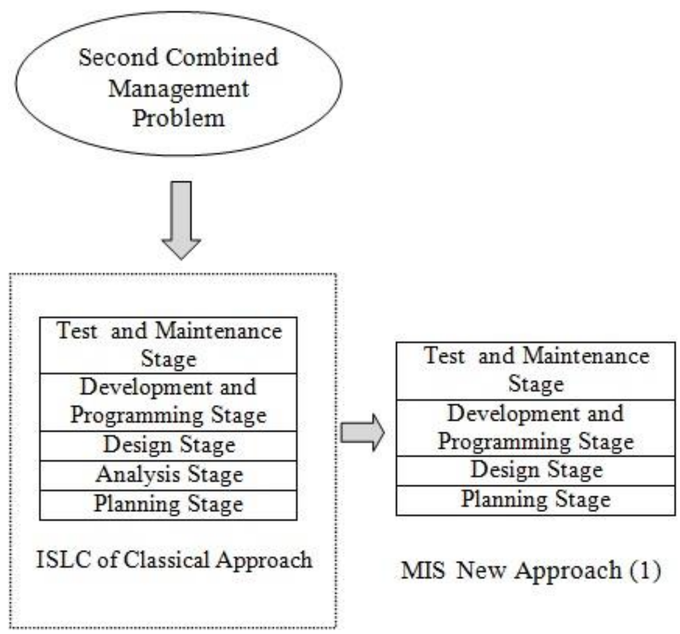


Fig. 9. Using the MIS New Approach (1) to Solve the Second Combined Management Problem

3) The third combined management problem:

It comes from the third probability {(1.b) , (2.a)}, which means that the third combined management problem is a second order management problem and a first level management problem at the same time.

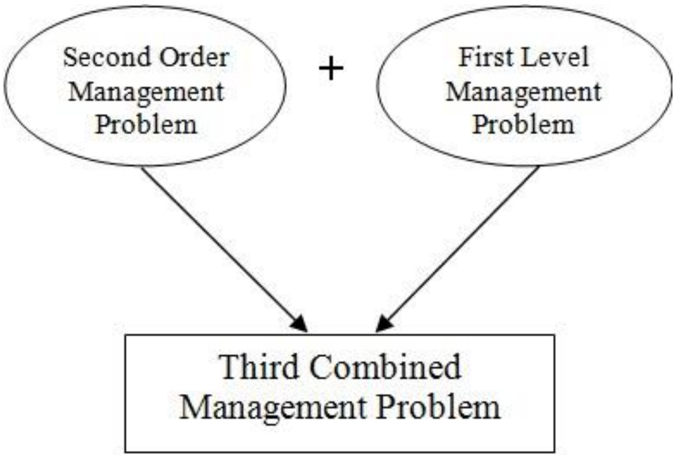


Fig. 10. Third Combined Management Problem

According to the research methodologies, the using of classical approach to build the MIS in order to solve the problems from the type of second order management problem, there is a need to use all stages of the ISLC of the classical approach, but the second level management problems lead to use the MIS new approach (2), which skips the design stage in the ISLC of classical approach, and thus, the third combined management problem will inherit only the skipping of the design stage, and this implies that the third combined management problem will not generate a new approach to build the MIS, and instead of this, the research recommends to use the MIS new approach (2) to build the required MIS in order to solve the third combined management problem.

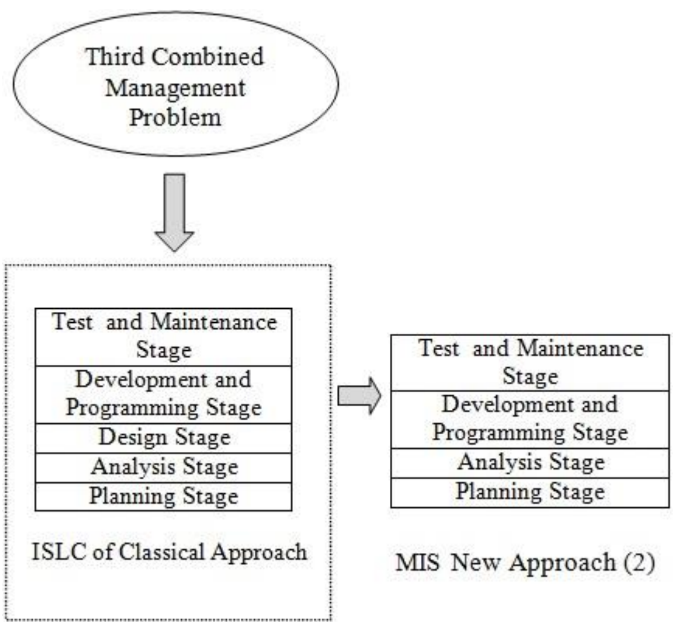


Fig. 11. Using the MIS New Approach (2) to Solve the Third Combined Management Problem

4) The fourth combined management problem:

This is the last one of the combined management problems, which comes from the fourth probability: {(1.b) , (2.b)}, so the components of this problem are: the second order management problem and the second level management problem.

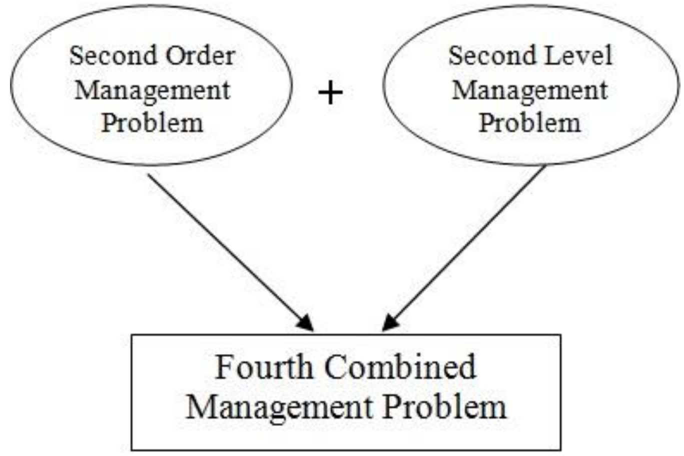


Fig. 12. Fourth Combined Management Problem

This research mentions in its methodologies to use the all stages in the ISLC of classical approach, when we want to solve the both two problems: second order management problem and second level management problem, which are the components of the fourth combined management problem, so building the MIS by using classical approach to solve the fourth combined management problem will lead to use the MIS classical approach which uses the all stages of the ISLC of classical approach, without any skipping to any stage.

Test and Maintenance Stage
Development and Programming Stage
Design Stage
Analysis Stage
Planning Stage

Fig. 13. The MIS classical approach which uses all stages of classical approach to solve the fourth combined management problem

IV. The NewIntegrated Model to Build and Design the MIS by Using Classical Approach

Now, and after the finding of the sub approaches for solving the different management problems, these sub approaches will be the components of the new integrated model, so the research will combine all these sub approaches in order to build and find the new integrated model.

The new integrated model will implement a general and clear procedure in order to solve all types of the management problems which are defined and founded by this research; which provides suitable approaches to solve each one of these problems by using the classical approach.

The integrated model will increase the efficiency of the used of classical approach in building the required MIS that will be used to solve the management problems. Increasing the efficiency of the classical approach comes from the minimizing of the ISLC of the classical approach, in many different cases, which will help the classical approach to overcome to its problems by decreasing the additional consuming in time and cost.

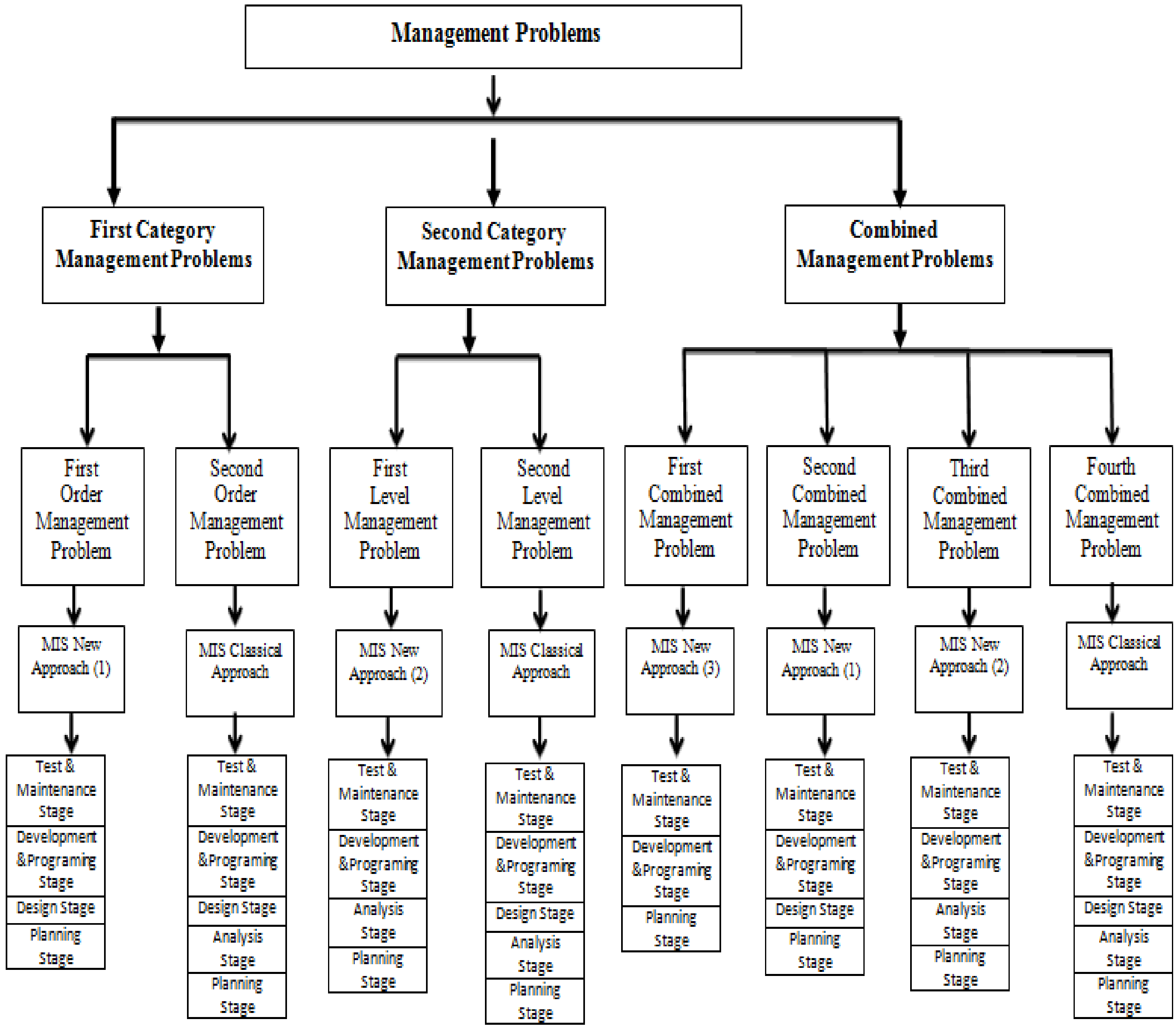


Fig. 14. The New Integrated Model

V. Conclusion

Classical approach is one of the information systems methodologies that is used to design and build the management information systems (MIS's). The classical approach suffers from critical problems; which are the long time and high cost in many different cases while building MIS. These problems come from the classical approach method, which always uses the all stages in its life cycle, although some of these stages are not necessary to be used in many different cases. In order to enhance the use of the classical approach in this field, the research develops a new classification and definition of the management problems that are probably solved by MIS, and also, some new sub approaches are developed from the classical approach in order to solve such management problems with partially use of the information system life cycle (ISLC) of the classical approach, the avoidance of the use of all stages of the ISLC will help the classical approach to save time and cost during building the MIS. And with a view to achieve a general, accurate and clear procedure that organizes the research methodologies in improving the use of classical approach in building the MIS's to solve the management problems, the research develops and implements a new integrated model which includes the developed classification of management problems and also all developed MIS sub approaches.

ACKNOWLEDGMENT

I'd like to thank Professor Cedric D. Bell, the pro vice chancellor at Limkokwing University of Creative Technology, Malaysia, for the great help, guidance and encouragements to my PhD process, and my thanks also to all Limkokwing University staff.

REFERENCES

[1] Mohammad M M Abu Omar, " *A New Approach to Increase the Efficiency of Classical Approach in Designing Management Information Systems(MIS's)*", International Journal of Research in Computer and Communication Technology-IJRCCT, November 2014, Volume 3–Issue11.

[2] Mohammed M M Abu Omar, " *Developing New Methods in Designing Management Information Systems by Using Classical Approach to Solve Management Problems*", International Journal of Computer Applications-IJCA, September 2014, Volume 101.

[3] Mathias Riechert, " *Research Information Standardization as a Wicked Problem: Possible Consequences for the Standardization*", In Proceedings of the International Conference of Current Research Information Systems, At Rome, 2014, Volume 12.

[4] Samson Yusuf Dauda, Jongsu Lee, "*Technology adoption: A conjoint analysis of consumers′ preference on future online banking services*" Elsevier Journal of Information Systems, 2015, Volume 53.

[5] Ram L Kumar, Antonis C Stylianou, " *A process model for analyzing and managing flexibility in information systems* ", European Journal of Information Systems, 2013.

[6] Abubucker Samsudeen Shaffi , Mohaned Al-Obaidy "Analysis and Comparative Study of Traditional and Web Information Systems Development Methodology (WISDM) Towards Web Development Applications" International Journal of Emerging Technology and Advanced Engineering-IJETAE, November,2013,Volume 3-Issue 11.

[7] Valdis Vizulis, Edgars Diebelis, "*Self-Testing Approach and Testing Tools*", Journal of University of Latvia, 2012, Volume 787.

[8] Lionel Briand, Yvan Labiche, "*A UML-Based Approach to System Testing* ", Journal of Carleton University, 2002, Version 4.

[9] Elizabeth Hardcastel, Business Information Systems, Ventus Publishing, 2008.

[10] Arthur M Langer, Analysis and Design of Information Systems, Springer, 3rd Edition, 2008.

[11] Laudon, Kenneth C., and Laudon, Jane P., Management Information Systems, Prentice –Hall International, 9th Edition, 2006.

[12] Laudon, Kenneth C., Essentials of Management Information Systems, Prentice –Hall International, 6th Edition, 2005.

[13] Lejk, M. and Deeks, An Introduction to Systems Analysis Techniques, 2nd Ed., Pearson Education Limited, 2002.

[14] Satzinger, J., Systems Analysis and Design, 2nd ed., Thomson Learning, 2002.

[15] Dennis, A. et al, Systems Analysis and Design: An- Object-Oriented Approach with UML, John Wiley &Sons Inc., 2002.

[16] Maciaszek, A., Requirments Analysis and System Design, Developing Information Systems with UML, Addison-Wesley, 2001.

[17] Ricky W. Griffin, Management, 7th Edition, Houghton Mifflin, 2001.

[18] A. Ziya Aktas, Structured Analysis and Design of Information Systems, Prentice- Hall, 1987.

Scrum Method Implementation in a Software Development Project Management

Putu Adi Guna Permana
STMIK STIKOM BALI
Denpasar, Bali

***Abstract*—To maximize the performance, companies conduct a variety of ways to increase the business profit. The work management between one company and the other company is different, so the differences in the management may cause the software to have a different business process. Software development can be defined as creating a new software or fixing the existing one. Technology developments led to increasing demand for software, Industrial Technology (IT) Companies should be able to project well maintenance. The methodology in software development is used in accordance with the company's needs based on the SDLC (Software Development Life Cycle). Scrum method is a part of the Agile method that is expected to increase the speed and flexibility in software development project management.**

Keywords—Metode Scrum; Agile; SDLC; Software

I. Introduction

Companies in effort to maximize its performance will try a variety of ways to increase the business profit [6]. Information technology can help the company to make a better decision, faster responses to the business, increase the communication, and make a smart investment [14]. The business development impacts on the increasing needs of software which is appropriate with the demands [4]. The needs to manage the works of one company is different between one and another, therefore the software used will be different [5]. The differences factor of the software makes the information technology companies compete in the software development business. Changes in business is a common thing in the world of business, by those changes, it may also increase the projects for software developments [1]. Software development can be defined as a process to make a new software to replace the old software or to fix the existing software [2]. To describe the solution and to develop the software faster and more precise, and to make the result to be easily developed and maintained, the development of the software needs a specific methodology [16]. Software development methodology is a process of organizing a set of method and notation convention which has been defined to develop software [8]. SDLC is a software development life cycle that consists of several key stages in building software in terms of its development. With SDLC cycle, the process of building the system is divided into several steps and on large systems, each step is done by different teams [9]. SDLC is not only important for the software production process, but also very important for the software maintenance process. Agile method is one of several methods used in software development. Agile method is a type of short-term system development that requires rapid adaptation in any form of changes [15]. In Agile Software Development, the interactions and personnel is more important than the process and the tools, a working software is more important than a complete documentation, collaboration with the clients is more important than the contract negotiation, and being responsive to changes is more important than following the plan [10]. The Scrum framework is a part of the Agile Methodology which is expected to increase the speed and flexibility in the software development project.

II. Literature Review

A. Agile

Agile Software development is one of the methodologies in the development of a software. The word Agile means to be fast, lightweight, free-moving, alert. Agile is a word used to describe a process model concept which is different from the existing process model concepts [10]. Agile software development concepts coined by Kent Beck and his 16 colleagues by stating that the Agile Software Development is a way to build software by doing it and helping others to build it all at once [3]. In Agile Software Development the interactions and personnel is more important than the process and the tools, a working software is more important than a complete documentation, collaboration with the clients is more important than the contract negotiation, and being responsive to changes is more important than following the plan. However, just as other process models, Agile Software Development has its own advantages and is not suitable for all types of projects, products, people and situations. Agile Software Development enables process model which is tolerant of the requirement changes so the response to the changes can be done faster.

B. SDLC (Software Development Life Cycle)

SDLC is the stages of work performed by system analysts and programmers in building an information system. The stages are as follows:

- Conduct a survey and assess the feasibility of information systems development project
- Study and analyze the information systems that are running
- Determine the requests of the information system users
- Select the best solution or problem solving
- Determine the hardware and software.
- Design a new information system

- Build a new information system
- Communicate and implement the new information system
- Maintain and repair / improve the new information system if necessary

System Development Life Cycle (SDLC) is a whole process in building a system through several steps [9]. There are several models of the SDLC, the model which is quite popular and widely used is the waterfall. Some other models of SDLC for example are fountain, spiral, rapid, prototyping, incremental, build and fix, and synchronize and Stabilize. With SDLC cycle, the process of building the system is divided into several steps and on large systems, each step is done by different teams.

C. Software

Software is a computer program that serves as a means of interaction between the user and the hardware. The software can also be regarded as a "translator" of commands that is run by the computer users to be forwarded or processed by the hardware [12].

D. Scrum

Scrum was developed by Jeff Sutherland in 1993 and its goal is to become a development and management methodology that follows the principles of Agile methodology [13]. Scrum is an additional responsive framework of software development for software projects and manage products or application development. The focus is on "strategy, a flexible holistic product development where the development team worked as a unit to achieve common goals" as opposed to "traditional approaches, a sequence" [5]. Scrum has a complex process in which many factors that affect the final result.

E. Role Scrum

In the Role Scrum, it is divided into 3 parts: Product Owner, Scrum Master and Team [17]. Product Owner is the person responsible for determining the specifications or the business of software applications to be built. Product Owner will register all the initial requirements to be done by the Team (known as the Product Backlog). Team is the one who runs the project, such as business analysts, system analysts, developers, testers and others. Team is the one who will be responsible for completing the Product Backlog provided by the Product Owner, Where the members of the team are responsible for each Backlog which has been divided as well as capable for knowing what to do next. Scrum Master is the one who set the scrum process during the project. Scrum Master will introduce and implement how Scrum works to the team and make sure everyone on the project implementing Scrum method.

F. Scrum Flow

A project with Scrum method begins with a depiction of the system that will be done. Then the Project Owner depicts the business process or plan into a Product Backlog [13]. Product Backlog is a list of plans that must be done by the team. There is a term in Scrum called the Sprint. Sprint is the goal to be achieved in the next scrum sprint (30 days ahead). Each Sprint starts with a Sprint Meeting Planing which is an activities to determine what kind of sprint to do next. Every day, each team gather together and discuss "What has been done since the last Daily Scrum Meeting?", "What problems are encountered during the work?", And "What will be done for the next scrum?"[5]. The meeting will be chaired by the Scrum Master and at the end of the sprint there will be a meeting for 4 hours to do a demo against everything that has been done.

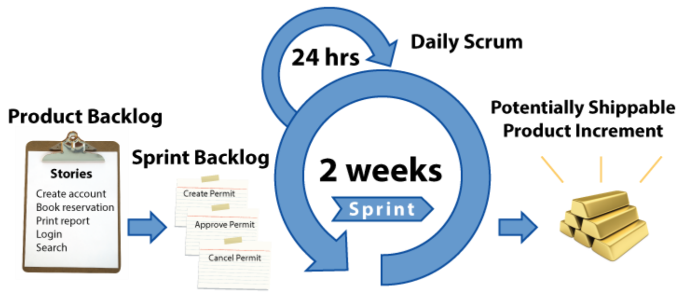


Fig. 1. Flow Scrum

III. Methodology

The research steps starts from the Development Preparation, maximize the writer/researcher study of literature for a deeper comprehension of the Scrum Method on a project. Besides the study of literature, author will also do consultations with the people who have been involved directly in Scrum to find information related to the challenges and obstacles during the process. The study also gives the knowledge about the Scrum framework and its implementation on the software development project management and manage scrum project using red mine application.

IV. Discussion and Result

A. Discussion

Writer implements the Scrum methodology on software development project using 6 personnel. The stages used will be explained in the next section.

Case Study In Arium Core Project Finance SMI:

In the process the project will be done by six personnel with the following tasks:

- *Project Manager* who is in charge to monitor, control, and responsible for the overall project
- *Business Analyst* who is in charge of analyzing the business to be developed
- *Systems Analyst* who is in charge to conduct a feasibility study, analysis and design to meet the requirements of users and applications
- *Programmers* 1who is in charge of the design process, perform coding and internal testing of the program to support the application system
- *Programmer 2* is in charge to assist Programmer 1
- *Tester* in charge of checking the program that is produced by the Programmer whether it has meet the requirements or not.

Scrum Team consists of three parts, they are:

- *Product Owner* (PO) consists of Project Manager and Business Analyst.
- *Scrum Master* (SM) consists of a Systems Analyst.
- *The team* consists of Programmer and Tester.

Fig. 2. Process Scrum

After the division of the scrum team on the Scrum process will be carried out as follows:

1) Determine The Product Backlog

Product Owner prepares the backlogs that will be the product backlog. The first step of Scrum is the determination of features based on priorities by the Scrum Master. In the case of determining the Product Backlog, the Scrum Master role is held by the Project Manager. A list of features that will be built according to priorities can be seen in Table 1.

So total there are three features that will be developed on Arium Core Project Finance SMI. The list of features is then called the *Product Backlog***.**

2) Sprint Planning

All of the scrum team conducts a meeting to make the agenda of what will be done. After determining the Product Backlog meeting held at the beginning of each Sprint to evaluate the Product Backlog, discuss the purpose and mission of each feature as desired by the Product Owner. On the Sprint Planning part the team members will determine how many hours each member will spend to carry out work on each feature. The people who choose that backlog should explain why choosing that tasks and understand what will be done. Details can be seen in Table 2.

Time for the first Sprint is determined to be 2 weeks and because the team only consisted of six people, and features that are done is still a UI (Display). After the working hours are determined, the team can start working on the first feature in the Product Backlog. The Product Backlog feature worked together in accordance with their respective roles in the team. All changes that occur during development should be postponed until the next Sprint.

3) Dialy Stand Up Meeting

As a practice to monitor the performance, there should be a meeting every day for reporting what has each member of the team done. At this stage of the Daily Stand Up Meeting not all of the team members must be present, but rather the members involved specifically on the features that are being developed (Team). At the end of each meeting, the time of completion renewed to know the rest of the work that is need to be pursued during the running Sprint. For examples of the implementation of the first to feature Sprint input commodity prices can be seen in Table 3.

TABLE I. FEATURES LIST SOFTWARE DEVELOPMENT PROJECT ARIUM CORE FINANCE SMI

No	Backlog Item	Description
1	Partial Prepayment	Partial Prepayment Module is used to make early repayment of some of the Outstanding Principal debtor
2	Top Up And Renewal	Top Up And Renewal module is a module that is used for recording on tenor extension process, the addition of ceiling, changes in interest rates on a facility that has been active
3	Early Termination	Early Termination Module is used to make early payment for all liabilities of the debtor, which includes principal, interest, late penalties and other obligations of the debtor

TABLE II. WORKING TIME PLAN

Weeks Sprint	Total Days
2Week	10Days

Role in team	Days	Hours / Days	Total Hours Sprint
Project Manager	4	4	16
Bussiness Analyst	8	4	32
System Analyst (ScrumMaster)	8	4	32
Programmer1	10	5	50
Programmer2	10	5	50
Tester	6	4	24

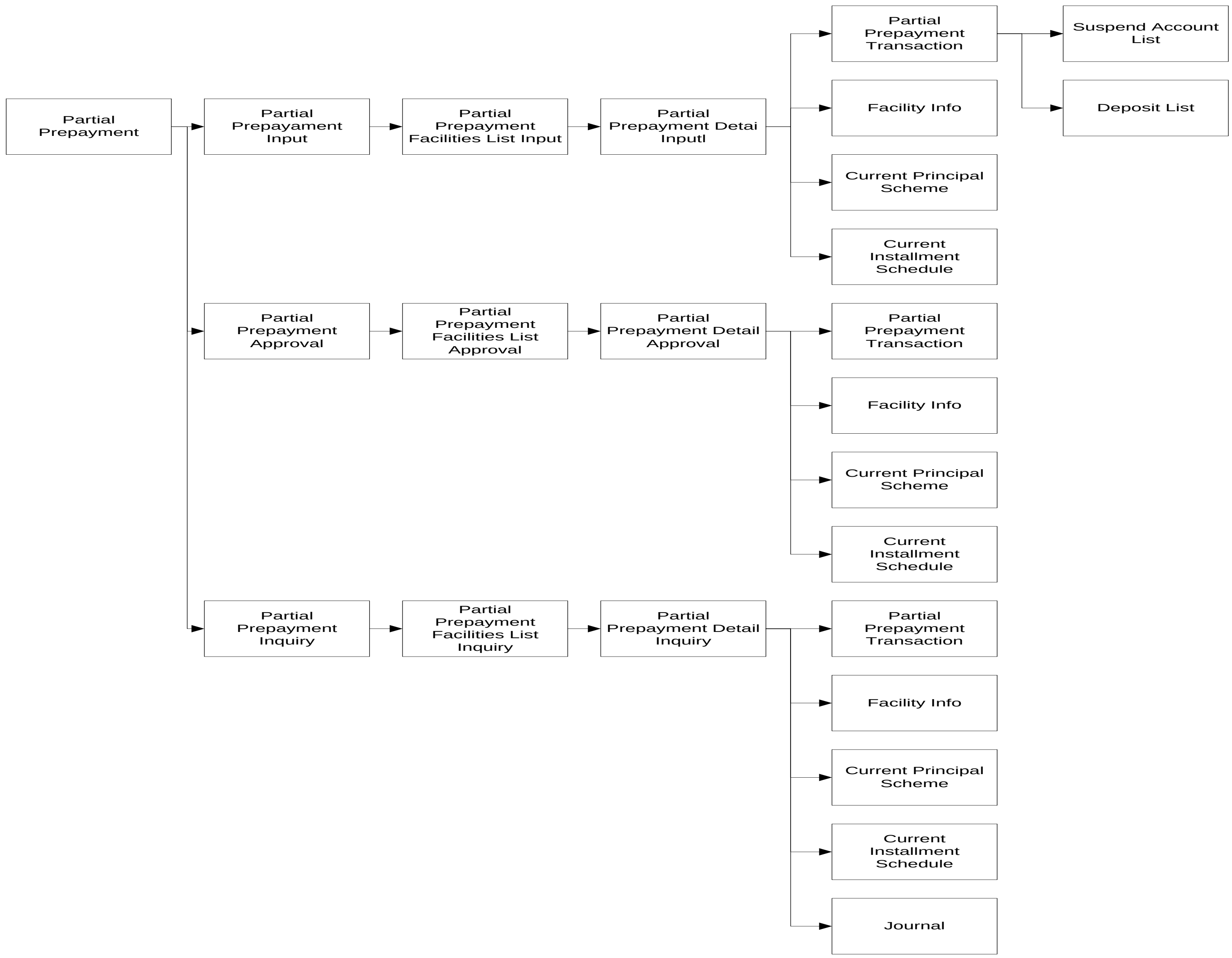


Fig. 3. Bussines Process Prepayment

TABLE III.

TABLE IV. SPRINT BACKLOG FITURE

				The number of remaining hours / day Sprint									
Fiture Backlog	**Task**	**AT**	**ET**	***H 1***	***H2***	***H3***	***H4***	***H5***	***H6***	***H7***	***H8***	***H9***	***H10***
Partial Prepayment	Business Process Design	Bussines Analyst	5	3	0	0	0	0	0	0	0	0	0
	Interface Design	System Analyst	5	5	4	2	0	0	0	0	0	0	0
	Database Design	System Analyst	5	5	5	5	3	0	0	0	0	0	0
	Coding Front End	Programmer 1	20	20	18	16	14	10	6	3	0	0	0
	Coding Back End	Programmer 2	20	20	20	18	14	12	8	4	0	0	0
	Testing	ProjectManager	2	2	2	2	2	2	2	0	0	0	0
		Tester	4	4	4	4	4	3	0	0	0	0	0

Notes:

ET = Estimated Time

As it can be seen in Table 3, the software development project starts with the first feature and system design. The system design itself is done by business analysts and system analysts covering the business processes, interfaces, and database. Once the design is completed then the task of programmers is to do the coding until it can be tested by the testers and the project managers. The process also applies for the other features in the backlog, and if it's not completed then Sprint will be continued until the products meet user needs.

Fig 4 and Fig 5 is the picture of the work process that is going on in the scrum, the real updated work based on each team tasks. In the process of work there is a story, criteria, planned, in progress, done and bugs. Story is used as columns to add cases that required by module that is worked on. Criteria is the kind of task to be done such as a partial prepayment module input. Planned is a work plan done in order to complete the task on criteria. Work still in progress will be put in *in progress* column, which has been completed will be entered into the column done, and if there are still business errors or mistakes in the module will be put into the bugs column.

Fig. 4. Monitoring (Manual Board)

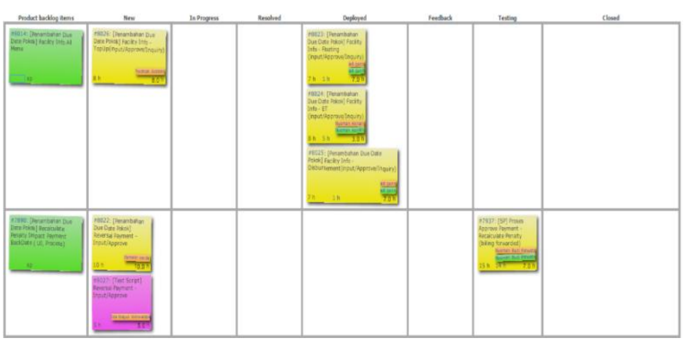


Fig. 5. Monitoring (Online Sprint Board)

Detail Monitoring (Online Sprint Board)

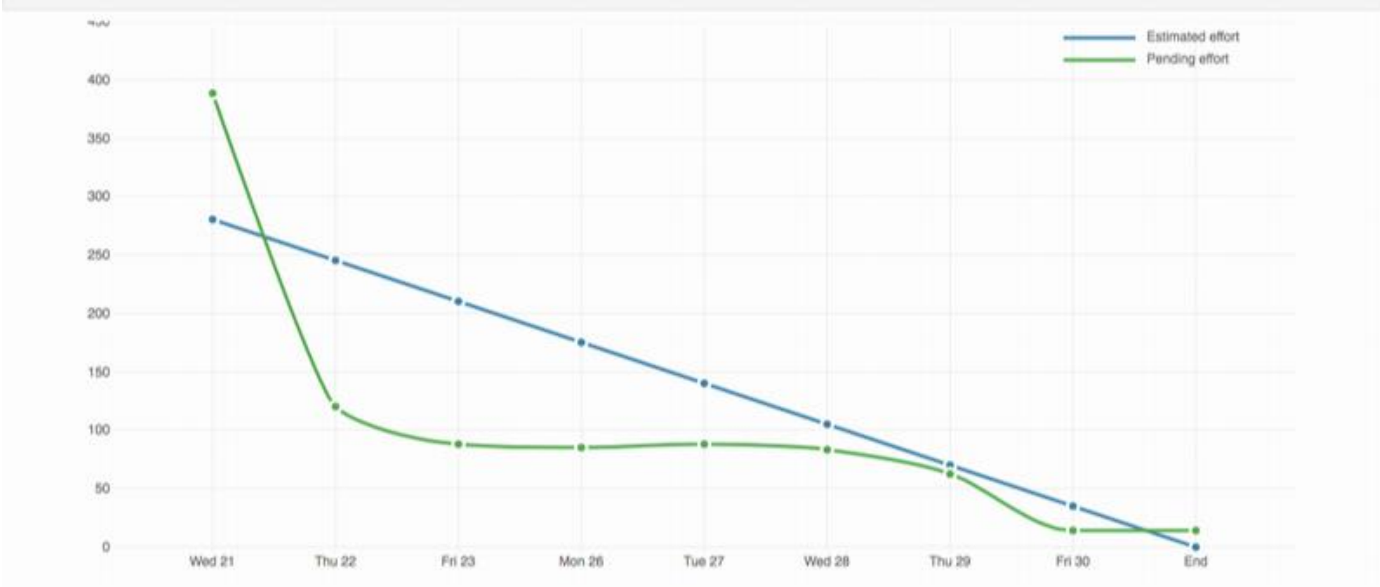


Fig. 6. Monitoring (Online Sprint Burndown Chart)

Burndown chart is a graphic that shows how much time it takes to complete the project. Burndown chart reflects the progress of the project. In Fig 6 there is a pending effort and the effort estimation, it can be seen that the average of the effort pending is below the estimated effort, which means the working progress is faster

4) Sprint Review

The people who do the task will demonstrate (running) the software feature that has been done, the demo is done by the whole team and presented without slides alternately every final sprint. Sometimes the client / customer wants to see how far is the progress of the software has been completed, therefore the product owner invited the client to come to the developer place and demonstrate the systems in front of them or through the online demo which is done at the client.

5) Sprint Retrospective

The Scrum Team discusses which task is encountering a problem, which task can be continued and that cannot be continued for the next sprint.

B. Result

Based on the discussion of the implementation process of the scrum method, then there some benefits that can be seen in Table 4.

TABLE V. BENEFITS IMPLEMENTATION OF SCRUM METHOD

Case	Description
Task Details Estimation	With the Scrum method, the details of the task has been clearly seen at the end of each sprint (2 weeks)
Quality	Sprint provides strength for team to undertake the development of software that has been determined in advance, so that the quality of the software is in accordance with the business on the sprint.
Quality Control	In terms of quality control it can be evaluated at the end of a sprint, so the quality of the application is visible in the final sprint.
Risk	With the Monitoring Board and Online Monitoring Board showed that mistakes happen all the time.
Application View	At the end of the sprint, each team demonstrates the task that has been done, therefore at the end of the sprint the display of the software being developed is visible.
Business Change	Once the software is demonstrated, if there is any business changes, it will be directly discussed in the final sprint
Customer Feedback	Customer sees the software demo and if there is any feedback it will be directly discussed in the final sprint
Project Monitoring	With the Monitoring Board and Online Monitoring Board, it provides an ease and the monitoring of the project can be done at any time.
Live (Production)	Sprint in the Scrum provides convenience in live applications, where live can be done per product backlog that has been made.

V. CONCLUSIONS

Based on the analysis that has been made and the results of the discussion in the previous section, then some conclusions can be drawn as follows:

- The quality and project risks seen more quickly.
- Business Change and Customer Feedback will be visible in the final sprint.
- Speed of visible projects in real time.
- Live Application can be done per product backlog.

In future studies a new method will be added to improve business change and customer feedback should be limited so that the project is not delayed.

REFERENCES

[1] Brunetti, G., et al, "Future business software : current trends in business software development".

[2] D'Costa, A. P., E. Sridharan. "India in the global software industry : innovation, firm strategies and development", New York, Palgrave Macmillan, 2004.

[3] Dingsøyr, T., et al, "Agile software development : current research and future directions", Berlin, Springer, 2010.

[4] Ebert, C., SpringerLink (Online service), "Best practices in software measurement how to use metrics to improve project and process performance", Berlin, Springer-Verlag,: xi, 295 p, 2005

[5] Falls, M. , Books24x7 Inc., "Inside the minds the software business : how top companies design, develop & sell successful products & applications", Inside the minds. Boston, Mass., Aspatore, 2004.

[6] Fort, T. L., "Prophets, profits, and peace : the positive role of business in promoting religious tolerance". New Haven, Yale University Press, 2008.

[7] Freeman, R. B. , K. Shaw, "International differences in the business practices and productivity of firms", Chicago ; London, University of Chicago Press, 2009.

[8] Fujita, H. , P. Johannesson, "New trends in software methodologies, tools and techniques : proceedings of Lyee W03, the second International Workshop on Lyee Methodology". Amsterdam ; Washington, DC, IOS Press, 2003.

[9] Langer, A. M., "Guide to software development designing and managing the life cycle". London ; New York, Springer,: 1 online resource (xvii, 350 p.), 2012.

[10] Martin, R. C., "Agile software development : principles, patterns, and practices",Upper Saddle River, N.J., Pearson Education, 2003

[11] Opelt, A. , Books24x7 Inc., "Agile contracts creating and managing successful projects with Scrum". Wiley series in systems engineering and management. Hoboken, N.J., Wiley, 2013.

[12] Pfleeger, S. L., J. M. Atlee, "Software engineering : theory and practice". Upper Saddle River, NJ, Pearson Prentice Hall, 2006.

[13] Pham, A., et al., "Scrum in action Agile software project management and development". Boston, Mass., Course Technology PTR, 2011.

[14] Schniederjans, M. J., et al., "Information technology investment decision-making methodology". Singapore ; Hackensack, N.J., World Scientific, 2005.

[15] Stober, T. ,U. Hansmann, "Agile software development : best practices for large software development projects". Heidelberg Germany ; New York, Springer, 2010.

[16] Venkatesh, U., "Distributed agile : dh2a: the proven agile software development methodology for geographically dispersed teams". Westfield, NJ, Technics Publications, LLC, 2011.

[17] Woodward, E., et al., A practical guide to distributed Scrum. Upper Saddle River, NJ, IBM Press, 2010.

Texture Analysis on Image Motif of Endek Bali using K-Nearest Neighbor Classification Method

I Gede Surya Rahayuda
High School of Management Information Technology and Computer
STMIK STIKOM Bali
Denpasar, Bali, Indonesia

***Abstract*—Endek fabric Bali is one form of craft woven fabric of Balinese society. Endek fabric has a variety of motifs or designs, a lot of people does not know that Endek have the type based on the design motif. In this research will be carried out an analysis texture on the Image Motif of Endek Bali and then classify them into several classes based on the type pattern motif of Endek Bali. The first step in this research is to collect some Image of Endek with different motif, then transform image into a gray level image using Edge Detection and do the extraction using GLCM, after that performed data classification using K-NN. Based on the analysis of all the grades K that have been tested, the value K with the most excellent level accuracy is on K = 15 and on Correlation component, with an accuracy percentage of 43.33%. Overall, the Cemplong motif is a motif that has recognition accuracy levels better than most other motifs, that with a percentage of 57.50%. There are quite a lot of motifs that are less precise Endek recognized at the time of classification. It's because among the Endek motifs may have the similar texture. The purpose of this study is to analyze texture and classify image motif of Endek Bali so that later can be developed into an application or program that can help to recognize the type of fabric Endek Bali. And even better if the program is implemented on the mobile phone, it can facilitate the process of image acquisition and subsequent directly extracted and classified from the mobile phone and can produce accurate classification results.**

Keywords—Analysis; Texture; Image; Endek Bali; Edge Detection; GLCM; K-NN

I. Introduction

Endek is the local word that describes the ikat process, and two types of weft ikat fabric existed. Endek fabric is one woven fabric of Balinese handicrafts. Bali is one of the several provinces in the State of Indonesia. In Indonesia there are so many types of weft ikat cloth, each province has different models for weft ikat cloth. The popular one is the model of Batik fabrics originating from Java[1-3].

Image Motif of Endek Bali has been used as a source of data that will be extracted and further classified into several classes according to the pattern of Image Motif Endek. There will declare four class where that classes was determined based on the pattern of Image Motif Endek. The type of fabric Endek distinguished based on the motif that used on woven fabrics; the pattern motif is taken from the design of Balinese Carvings. Aside from Balinese Carvings motif, design of fabrics Endek also typically taken from the motif of plant or flower. Some kind of motif that will be taken as a class is a design that has a considerable difference between the design of other Endek. To the type of pattern that is almost similar motif, it's will be not used, to facilitate future research. Some kind of motif that will be used as a Class is such as **Patlikur, Cemplong, Sekar** and **Wajik**[1]**.**

This research begins by collecting some data such as the image or a photo of each type of fabric Endek. Classification Image Motif Endek will run manually or in digital computing using digital image processing methods. Digital image classification process can be performed based on the features of each image. The best classification motif of Endek can be used for identification and could be to speed up the search process of Endek Image. Image classification process can be done by using image features such as color, shape, and texture of the image. Each image on each class is identified features that distinguishing from another class image. In this research will be used texture features for classification of Endek Image. Texture features components that will be using are Contrast, Correlation, Homogeneity, and Energy. The main objective of this study was to determine which features provide the greatest influence in the process of classification Endek Image. After obtaining the texture features of each image Endek, the next process is to perform the classification by K-NN method. K-Nearest Neighbor (K-NN) belong to a group instance – based learning. This algorithm is also one lazy learning techniques. K-NN is running by searching for objects in the group K closest training data or similar to the object on the new data or data testing. K-NN including supervised learning category, where the dataset should be trained first before the classification process itself[4-5].

The amount of the Data Set (Data Sample) used is 20 for each type of motif, so total there are 80 pieces of data set. While the amount of data (Data Training) used for this test were as many as 10 data for each type of motif Endek, so that total of 40 data.

II. Literature Review

Some words that used in this article was taken from the opinion quoted from several existing reference such as theses, dissertations, journals, and proceedings. In this literature review will be explain the meaning of each data sources and methods that used in this research.

A. Texture

Texture is a result of local variations in brightness within one small region of an image. Texture contains important information about the structural arrangement of surfaces. The textural features based on gray – tone spatial dependencies have a general applicability in image classification. Texture is an intuitive concept that describes the nature of smoothness, roughness, and regularity in the region or area. In digital image processing, texture is defined as the spatial distribution of degrees of gray in a set of neighboring pixels. In general, texture refers to the repetition of elements of a basic texture called primitive or texture element – texel. Terms formation of a texture is:

a) Primitive pattern that consists of one or more pixels. This primitive form of pattern can be a point, a straight line, curved line, area, and others which are basic elements of a texture.

b) The primitive patterns recur at intervals and specific direction so that it can be predicted or discovered repetition characteristics. An image give different interpretation of textures when viewed with different distances and angles.

Humans look at the texture based on the description that is random, such as smooth, rough, regular, irregular, and soon. This is a description of improper and non-quantitative, so it needed a quantitative description (mathematical) to facilitate analysis[6-8].

B. Texture Analysis

Texture analysis is the basis of a wide range of applications, application of texture analysis, such us: remote sensing, medical imaging, identification of quality of materials (wood, leather, textiles, etc.) and also a wide range of other applications. Texture analysis techniques can be classified into three groups:

a) Statistical Technologies: based on region histograms and their moments, they measure features such as coarseness and contrast. Examples of statistical methods are Autocorrelation Functions, Co-occurrence Matrix, Fourier Transformation, Edge Frequency.

b) Spectral Technologies: based on the autocorrelation function or power spectrum of a region, they detect texture periodicity, orientation, etc.

c) Structural Technologies: based on pattern primitives, they use placement rules to describe the texture. Examples of structural method is fractal models.

Texture analysis has also been used to evaluate ultrasound images of the prostate. Other optical imaging modalities have utilized texture analysis, such as fluorescence microscopy images of colonic tissue sections and light microscopy images of the chromatin structure in advanced prostate cancer[6].

C. Endek Bali

Weaving is one of the techniques of making fabric that has existed since centuries ago. Weaving culture grew and developed in various places along with human civilization and culture in the local area, as well as the color and decorative or pattern of woven has its own peculiarities in each region. As with other regions in Indonesia, Bali also has a traditional form of woven fabrics Endek who became the pride of the people of Bali, which gringsing Endek woven fabric produced by the people of Bali Aga Tenganan Pagringsingan, Karangasem[1].

Dynamics of weaving craft endek divided into three periods of time is that the first period in 1985 – 1995 in which development this year is very encouraging, it is due to the financial support of UNDP and state enterprises, weaving looms evolved from cag – cag become loom machines, motifs endek fabric more developed not only a motive but various motifs produced. Endek evolving fabric is not only used by the nobility, but also has been used by the upper middle class people and lower middle customized with fashion or fasion in society. Bali’s overall textile sector is now transforming endek into home goods and also into high fashion. Endek costumes are also important in rituals but this single ikat is now taking on a new life as fashion public[9-10].

The second period from 1996 to 2006 decreased developments that can be seen in terms of the production of woven fabric endek, due to competition with similar cloth factory production into the market. In addition yarn materials were hard to come by the craftsmen at that time. But it did not dampen the craftsmen to keep weave, woven fabrics and motifs Endek more developed. The third period at 2007 – 2012, the development of this year fluctuated greatly perceived decline artisans entered the year 2008 – 2010 yarn materials scarce, prices high yarn quality does not match the production standards endek cloth[10].

Fabric design motif Endek is taken from the motif of Balinese Carved, Wayang (shadow puppets), Animals, and motifs of Plants such as Leaves and Flowers. Examples of types of fabric Endek that uses design from Balinese Carved is the kind of fabrics Endek Patlikur, Cemplong, Wajik (diamond) and Patra. Then example for Endek that use motif from Wayang (shadow puppets) is Endek Wayang Kebo and Endek Wayang Putri. Example of Endek that use animals motif is Endek Ejekan Siap and for the last example for endek that use motif from Plants is Endek Sekar. In this research will be used four kinds of various types of fabrics Endek. The four types of fabrics Endek which will be used as a class is: Endek **Patlikur**, **Cemplong**, **Wajik** (diamond) and **Sekar**[1]. Here is an explanation of each type of fabric Endek:

a) Endek Patlikur

Patlikur motif is a common motif used by the craftsmen of Balinese Carving, this Patlikur motif can be met in various kinds of Balinese carving, such as on the carving of a table, chairs, figura and are also frequently used on clothing or fabrics. Motif Endek Patlikur an original motif of Tenganan Gringsing Endek[1].

b) Endek Cemplong

Cemplong Endek fabric pattern, a fabric pattern endek taken from balinese carving motifs, in contrast to Patlikur which has a large pattern, while Cemplong have a small pattern and resembles the shape of the sphere. Motif Endek Cemplong an original motif of Tenganan Gringsing Endek[1].

c) Endek Sekar

Motif Sekar is a motif Endek that takes patterns from a flowers. The shape of the circuit pattern design looks like a flower.

d) Endek Wajik

Motif Wajik (diamonds) is a very simple motif endek, Wajik are a form such as a square or a symbol looks like a diamond.

D. Edge Detection

Object selection is usually running with step Edge Detection in image processing, Edge Detection process in MATLAB using a command or function "edge" and only use images or 2D images alone. Edge Detection on an image of a process that generates the edge of the image object, the purpose is[7]:

a) To mark the passage into detail image

b) To fix the details of a blurred image, which occurs due to an error or the effect of the image acquisition process. A point (x, y) is said to be the edge of an image when the point has a height difference with its neighbors.

There are several methods in Edge Detection. Kinds of Edge Detection method for this process, among others[7][11-12]:

a) Robert Method

Robert method is another name for the differential technique developed above, that is the differential in the horizontal direction and the differential in the vertical direction, with added binary conversion process after the differential. Binary conversion technique suggested is a binary conversion to flatten the distribution of black and white. Robert method is also equated with the technique Differential Pulse Code Modulation (DPCM).

b) Prewitt Method

Prewitt method is a development method using a filter HPF robert were given a zero buffer. This method takes the principle of Laplacian function, known as HPF function to generate.

c) Sobel Method

Sobel method is a development method using a filter HPF robert were given a zero buffer. This method takes the principle of Laplacian and Gaussian functions are known as the function to generate HPF. The advantages of this Sobel method is the ability to reduce noise before performing calculations Edge Detection.

d) Canny Method

Canny Edge Detection is the optimal operator. Canny operator using Derivative Gaussian kernel to filter noise from the initial image to get a smooth edge detection results.

e) Laplacian of Gaussian Method

This method will detect the zero crossing, to define the boundary line between black and white, located on the second derivative of the image in question. Disadvantages of the application of the Laplacian operator is very sensitive to noise, however, the result of Edge Detection with this operator can be improved, by applying thresholding.

E. Gray Level Co-occurrence Matrix (GLCM)

GLCM is also called as Gray level Dependency Matrix. It is defined as a two dimensional histogram of gray levels for a pair of pixels, which are separated by a fixed spatial relationship. Matrix Co–Occurrence is one of the statistical methods that can be used for texture analysis. Co–Occurrence matrix formed from an image by looking at the pixel pairs that have a certain intensity. The use of this method is based on the hypothesis that the texture will occur in a looping configuration or pair of gray cedar[8].

F. K-Nearest Neighbor (K-NN)

K-Nearest Neighbor method is a method to classify the object, based on the data that is distance learning close to the object, according to the number or value of K-Nearest Neighbors. Near or far neighbors are usually calculated based on euclidean distance with the following **equation 1**[5][13]:

$$d(x-y) = \sqrt{\sum_{j=1}^{n}(x_j - y_j)^2} \quad (1)$$

With :

d : Distance data test to the data sample

xj : Data test j, with j = 1, 2, . . . , n

yj : Data sample j, with j = 1, 2, . . . , n

K-NN classification is done by searching k nearest neighbors of the data test and choose the class with the most members. The K-NN classification steps are as follows:

a) If a set of data sample y having N data points overall, then will do the identification of the K-Nearest Neighbors of the data test x.

b) Of a K Nearest Neighbors, data x identified in the class ωi, i = 1, 2, . . ., M. M is the number of classes.

c) Data test x included in the class with the highest number of members.

d) If there are two or more classes ω in the immediate neighborhood of the data test x, then there was a balanced condition (conflict) and use conflict resolution strategies.

e) For the class conflict, the distance d is determined between the data test x with ωi class members involved in the conflict, which amounts to E.

f) If the data sample of the class ωi involved in the conflict indicated by yim = {y1im, . . ., yNim }, then the distance between x with class ωi is at ***equation 2****:*

$$d_i = \frac{1}{E}\sum_{j=1}^{N} |(x_j - y_j^{im})| \quad (2)$$

g) Data test x put into a class with at least a small distance.

III. Research Methods

There are several methods which will be used in this research, including the method for transform image into A Gray Level Image using Edge Detection, and then for extraction Image using Gray Level Co-occurrence Matrix

(GLCM) and for the last process is perform K-NN Classification method that used to classify the results of extraction Image. In this research there are several processes are carried out from the initial data is selected, until in the end the data is classified. The process is grouped into six main processes, such us:

a) Choosing the Input Image

b) Change the Input Image into A Gray Level Image using Edge Detection Method

c) Perform Feature Extraction using GLCM Method

d) Store the Feature Extraction Results

e) Perform Data Sample and Data Training

f) Perform Image Classification process with K-NN Method

Here is a depiction or modeling flow chart of the process to be conducted in this research:

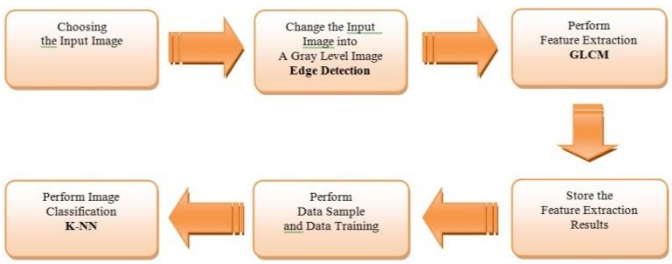


Fig. 1. Flow Process of Extraction and Classification

A. Choosing the Input Image

The process that was first performed in Texture Analysis on Image Motif of Endek Bali is to choose the input image. The input image is the image of some fabrics Endek with various types and formats supported by MATLAB. Image with other formats will not be recognized and will display an error message. In this research will be used four kind of motif fabrics Endek, such us: Endek Patlikur, Sekar, Cemplong and Wajik. The amount of the dataset (Data Sample) used is 20 for each type of motif, so the overall total there are 80 pieces of data. While the amount of data used for testing (Data Training) is as much as 10 data for each type of motif, so that a total of 40 data.

B. Change the Input Image into A Gray Level Image using Edge Detection

After selecting the input image then the next step is to convert the input image into a gray level image, the method used to change the image is to call a function that has been found in MATLAB, the name of that fungtion is edge detection function, There are several methods of edge detection is provided in MATLAB, the methods that will be used in this research is the Canny method. Canny edge detection is the optimal operator. Canny operator is using a Derivative Gaussian kernel to filter noise from the initial image to get a smooth edge detection results[7][11-12].

C. Perform Feature Extraction using Gray Level Co-occurrence Matrix (GLCM)

Texture is an important element of visual perception that can be used to separate the attractive area of an image. Texture can load important informations about the structure and its relation to the surrounding areas. The meaning of texture is the regularity of a specific patterns formed from the composition of pixels in a digital image. One important part of texture analysis is to use a matrix pair intensity Gray Level Co-occurrence Matrix (GLCM) which is a two dimensional matrix linkages. The matrix is a matrix of intensity pairs that describe the frequency of the appearance of two pairs of pixels with a certain intensity within a certain distance and direction in the image. GLCM can be calculated using the multiple spatial offset direction is 0 degrees, 45 degrees, 90 degrees, and 135 degrees. GLCM matrix obtained, characteristic texture of imagery used in this study can be measured by using the following features[14-16]:

TABLE I. SOME OF GLCM SEGMENTATION COMPONENT, DESCRIPTION AND EQUATION

Name	Description	Equation
Contrast	Contrast, is used to measure the intensity distribution fluctuation by using **equation 3**	$\sum_{i,j} \lvert i-j\rvert^2 \, p(i,j)$ (3)
Correlation	Correlation, is used to measure the correlation between a pixel to neighboring pixels of the entire image by using the **equation 4**	$\sum_{i,j} \frac{(i-\mu_i)(j-\mu_j)\,\vec{p}(i,j)}{\sigma_i \, \sigma_j}$ (4)
Homogeneity	Homogeneity, homogeneity is used to measure variations in the intensity of the image by using the **equation 5**	$\sum_{i,j} \frac{p(i,j)}{1+\lvert i-j\rvert}$ (5)
Energy	Energy, used to measure the concentration of the pair intensity on cooccurrence matrix using **equation 6**	$\sum_{i,j} p(i,j)^2$ (6)

At the MATLAB been provided all components of the GLCM segmentation, we can use the component with Graycoprops function, The following is an example of using Graycoprops function on MATLAB: GLCM = graycoprops (image, properties). GLCM is a matrix variable that will store the result of extraction using Graycoprops, Graycoprops is one function method in GLCM, image is a matrix variable of A Grey Level Image that before had been read in MATLAB and Properties is a component of GLCM that is Contrast, Correlation, Homogeneity and Energy.

D. Store the Feature Extraction Results

Characteristics obtained from the extraction image, then stored for later use in the creation of reference data. 80 data image that has been extracted and stored, to later be used as reference data or sample data. And then will be extracted 40 new data image which will be used as data training, where this 40 image extracted one by one and then each of the extracted image is also stored, and later at the K-NN Classification process will be used to compared with the data sample, and then to determine the class of the image. The data result of extraction image on MATLAB can be stored into text file (.txt) or excel file (.xls).

E. Perform Reference Data (Data Sample) and Data Test (Data Training)

The next process is carried out after storage extraction results is to perform Data Sample that have been stored before, and also a training data that recently extracted and have been stored. At MATLAB we can call the data that has been stored using the function "load" or we can also directly open the file by using the facility "open file" which has been provided in MATLAB. After being shown the file will be saved into MATLAB in the form of matrix variable, where latter the matrix variables can be used in the K-Nearest Neighbor (K-NN) classification process.

F. *Perform Image Classification using K-Nearest Neighbor (K-NN)*

After the Data Sample file and the Data Training perform and stored into a matrix variable on MATLAB, then the next process is to perform the classification process using K-Nearest Neighbor (K-NN). K-Nearest Neighbor (K-NN) process performed by comparing the data test (Data Training) with multiple data samples that have been stored before. A new data test are compared with the 80 pieces of data samples. The process performed by searching the data samples which value that is approaching the data test, if K = 5, then the system will look for 5 pieces of data samples which value approached with the data test, and so also with the others K values. This research will be performed K-Nearest Neighbor (K-NN) classification process with a value of K = 5, K = 10 and K = 15[13][17]. Examples of K-NN in MATLAB: Class = knnclassify (DataTest, Data Sample, Group, K).

IV. Implementation and Classification Result

In this research, the classification process begins with the identification database of motifs image Endek into four classes Image motifs, such as: Patlikur, Cemplong, Sekar and Wajik, as shown in Figure 2.

Endek Patlikur Endek Cemplong Endek Sekar Endek Wajik

Fig. 2. Four Class Motif of Endek Bali

The amount of data test that will be entered as the Data Training as many as 40 images from the same sources that have not been entered into the database by each class of 10 images, as shown in Figure 3.

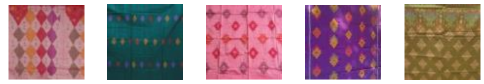


Fig. 3. Data Test (Data Training) of Endek Bali

Before the classification process performed, before had performed the Edge Detection and Gray Level Co-occurrence Matrix (GLCM) on 80 data samples, and that extraction result then stored into an text file or excel, which will be used as reference data (Data Sample) in K-Nearest Neighbor (K-NN) process. Here are some examples of data samples that have been stored.

TABLE II. Some of Reference Data (Data Sample)

Name	Contrast	Correlation	Energy	Homogeneity
SamplePatlikur1.jpg	1.33E+04	-2.96E-02	1.17E-04	4.18E-02
SampleCemplong1.jpg	6.02E+03	2.08E-02	1.34E-04	4.57E-02
SampleSekar1.jpg	3.12E+04	-6.95E-02	5.69E-05	2.27E-02
SampleWajik1.jpg	2.63E+03	-2.62E-03	4.75E-04	6.16E-02

After determining 4 class pieces and as many as 40 training data, then the next to be done is to change the image data into A Gray Level Image using the Edge Detection function and method of Canny, where function and these methods have been provided on MATLAB, The following are some examples of Edge Detection that used in this research using MATLAB:

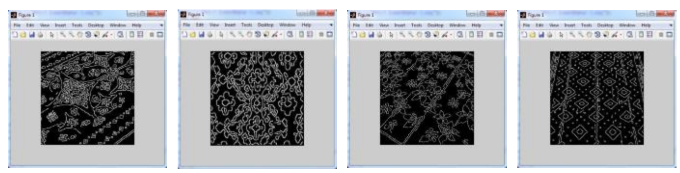


Fig. 4. Example of some Image that transform into A Grey Level Image using Edge Detection with Canny Method

Then that gray level image will be extracted using Gray Level Co-occurrence Matrix (GLCM) to obtain the characteristics of the image, then this feature will be stored into the the text or excel file and will be use as a training data that will be compared with the data sample and then to be processed on the classification process. Some examples of the extracted image using GLCM on MATLAB:

```
>> imread('Test Patlikur 1.jpg');
>> gray = rgb2gray(ans);
>> GrayImage = edge(gray,'canny');
>> GLCM = graycoprops(GrayImage);
>> GLCM

GLCM =

       Contrast: 1.0029e+04
    Correlation: -0.0466
         Energy: 9.7087e-05
    Homogeneity: 0.0385

fx >>
```

Test Patlikur 1.jpg

```
>> imread('Test Cemplong 1.jpg');
>> gray = rgb2gray(ans);
>> GrayImage = edge(gray,'canny');
>> GLCM = graycoprops(GrayImage);
>> GLCM

GLCM =

       Contrast: 5.0555e+03
    Correlation: -0.0281
         Energy: 1.6431e-04
    Homogeneity: 0.0509

fx >>
```

Test Cemplong 1.jpg

```
>> imread('Test Sekar 1.jpg');
>> gray = rgb2gray(ans);
>> GrayImage = edge(gray,'canny');
>> GLCM = graycoprops(GrayImage);
>> GLCM

GLCM =

       Contrast: 2.5066e+04
    Correlation: 0.0336
         Energy: 6.0150e-05
    Homogeneity: 0.0277

>> |
```

Test Sekar 1.jpg

```
>> imread('Test Wajik 1.jpg');
>> gray = rgb2gray(ans);
>> GrayImage = edge(gray,'canny');
>> GLCM = graycoprops(GrayImage);
>> GLCM

GLCM =

       Contrast: 1.8763e+04
    Correlation: 0.0123
         Energy: 9.2920e-05
    Homogeneity: 0.0304

>>
```

Test Wajik 1.jpg

Fig. 5. Example of some extraction results using GLCM on MATLAB

GLCM performed on some data the extraction results will be used as the data test which will be stored in file text or excel, The following are some of the data characteristics, obtained from the extraction using GLCM, There are a total of 40 data test (Data Training), the following are some examples of data test that has been extracted using GLCM methods and stored as text or excel file:

TABLE III. SOME DATA TEST (DATA TRAINING) OF EXTRACTION ON A GREY LEVEL IMAGE USING GLCM

Name	Contrast	Correlation	Energy	Homogeneity
TestPatlikur1.jpg	1.00E+04	-4.66E-02	9.71E-05	3.85E-02
TestCemplong1.jpg	5.06E+03	-2.81E-02	1.64E-04	5.09E-02
TestSekar1.jpg	2.51E+04	3.36E-02	6.02E-05	2.77E-02
TestWajik1.jpg	1.88E+04	1.23E-02	9.29E-05	3.04E-02

After performing data test extraction using GLCM then the next step is to perform an Data Sample and Data Training file using the function "load" or "open file" and then performing the K-Nearest Neighbor (K-NN) classification using the function "knnclassify", that has been provide on MATLAB. In this study taken K value, that is: 5, 10, and 15. Of each value of K will be calculated accuracy of the classification process by using the formula of accuracy as in **equation 7**[5][13].

$$\text{Accuration} = (\text{Total Corect Data Test} \div \text{Total Data Test}) \times 100\% \quad (7)$$

The process of calculating the distance between the image in the K-NN classification for texture features using the absolute value of the difference between the value of each image texture feature parameters. Endek motif classification system built using MATLAB. Almost all of the functions needed for the construction of the system has been provided by MATLAB, so it's simply call the function of the library belongs to MATLAB. K-NN classification is done by comparing the data training that will be tested with data sample that has been stored before.

```
>> uiopen('DataSample.xls',1)
>> uiopen('TestPatlikur1.xls',1)
>> class = knnclassify(TestPatlikur1, DataSample(:,1), DataSample(:,2), 5);
>>
```

Fig. 6. Example of some klasification image using K-NN function on MATLAB with K = 5

Based on the results of tests performed, obtained the results as shown in Table 4, 5, 6, 7, 8 and 9[5][7][13]. In table 4, 5, and 6 were tested by 10 data test for each motif Endek. And the data that written on the table is the number of correct data from 10 data image that has been tested on each properties of image components such as Contrast, Correlation Energy and Homogeneity. The range data will be inputed at the table is between 0 – 10, because that is 10 data test on each motif of image that will be tested at this classification prosses. And the accuracy is obtained from dividing the correct data to the total data test, then multiplied by 100%, as described in equation 5. Classification testing done 3 times for each component feature extraction, that is to the value K = 5, K = 10, and K = 15.

TABLE IV. RESULTS OF CLASSIFICATION TEST WITH K = 5

Name	KNN Classification with K = 5 and Total Data Test = 40				Total Correct Data	Accuration
	Cont	Corr	Ener	Homg		
Patlikur	2	2	2	1	7	17.50%
Cemplong	4	8	4	6	22	55.00%
Sekar	3	4	1	3	11	27.50%
Wajik	6	3	3	3	15	37.50%
Total	15	17	10	13	**55**	**34.38%**

TABLE V. RESULTS OF CLASSIFICATION TESTWITH K = 10

Name	KNN Classification with K = 10 and Total Data Test = 40				Total Correct Data	Accuration
	Cont	Corr	Ener	Homg		
Patlikur	1	2	2	0	5	12.50%
Cemplong	4	10	4	3	21	52.50%
Sekar	3	3	5	3	14	35.00%
Wajik	3	3	3	4	13	32.50%
Total	11	18	14	10	**53**	**33.13%**

TABLE VI. RESULTS OF CLASSIFICATION TEST WITH K = 15

Name	KNN Classification with K = 10 and Total Data Test = 40				Total Correct Data	Accuration
	Cont	Corr	Ener	Homg		
Patlikur	0	1	5	0	6	15.00%
Cemplong	5	10	6	5	26	65.00%
Sekar	2	2	3	4	11	27.50%
Wajik	3	4	3	3	13	32.50%
Total	10	17	17	12	**56**	**35.00%**

In Table 7[13] it can be seen that the Motifs Endek who have the highest level of accuracy is the Cemplong Motifs, which amounted to 57, 50%.

TABLE VII. RESULTS OF CLASSIFICATION TEST BASED ON IMAGE MOTIF OF ENDEK BALI WITH ALL VALUE OF K

Name	Total Data Test = 40 + 40 + 40 = 120			Total Correct Data	Accuration
	K = 5	K = 10	K = 15		
Patlikur	7	5	6	18	15.00%
Cemplong	22	21	26	69	**57.50%**
Sekar	11	14	11	36	30.00%
Wajik	15	13	13	41	34.17%
Total	55	53	56	164	34.17%

For each component influences the texture feature extraction can be seen in table 8[5][13]. On the table it can be seen that all components feature extraction (Contrast, Correlation, Homogeneity and Energy) having differences in accuracy, that is between 29.17% and 43.33%, of the highest value obtained by Correlation component with a percentage 43.33%.

TABLE VIII. RESULTS OF CLASSIFICATION TEST BASED ON COMPONENT FEATURE EXTRACTION

Name	K = 5	K = 10	K = 15	Total Correct Data	Accuration
Contrast	15	11	10	36	30.00%
Correlation	17	18	17	52	**43.33%**
Energy	10	14	17	41	34.17%
Homogeneity	13	10	12	35	29.17%

Despite having differences that are not so far, that between 33.13% - 35.00%. As for the value of K in the classification process which has the highest degree of accuracy can be seen in Table 9[5][13] that is for K = 15 with a percentage of 35.00%.

TABLE IX. RESULTS OF CLASSIFICATION TEST BASED ON VALUE OF K

Name	Total Correct Data	Accuration
K = 5	55	34.38%
K = 10	53	33.13%
K = 15	56	**35.00%**

In the classification testing that has been done, there are many motifs that are not recognized in accordance with the actual type. According to the observations, the process of classification that does not correspond to the real motifs is because among Endek motifs has the same texture pattern and Endek has a complex texture pattern. For example for Cemplong motif it is often identified as Wajik motif, as well as the motif of Wajik is often identified as Cemplong. So also with the other motives that have frequent errors on determining the classification.

V. CONCLUSION

Based on the analysis, of all grades K that have been tested, the value K with the most excellent level accuracy is K = 15. And for testing the effects of feature extraction component with the highest score obtained by the component Correlation with a percentage 43.33%. Overall, the Cemplong motif is a motif that has recognition accuracy levels better than most other motifs, that with a percentage of 57.50%. There are quite a lot of motifs that are less precise Endek recognized at the time of classification. It’s because among the Endek motifs may have similar texture and complex texture pattern. Because of that, is needs to be further investigated in to distinguish the different types of Endek Motifs that have a similar texture. The more data samples used in this study will be helpful to improve the accuracy at the time of the classification process.

REFERENCES

[1] Utami, S., Gringsing Woven Cloth: The Motif Correlation, Function, And Symbolic Meanings.Journal Universitas Negeri Yogyakarta, 2014.

[2] Coleman, H., Patterns of Culture The Textiles of Bali and Nusa Tenggara. Journal University of Leeds International Textiles Archive, 2008.

[3] Ashby, C., An, Investigation Of Ikat Weaving And Warp Printing, And Their Application To Contemporary Design, 1985, Middlesex University: London.

[4] Choudhary, D., et al., Performance Analysis of Texture Image Classification Using Wavelet Feature. International Journal of Image, Graphics and Signal Processing, 2013. 5(1): p. 58-63.

[5] D S Guru, Y.H.S., S. Manjunath, Texture Features and KNN in Classification of Flower Image. International Journal of Computer Applications, 2010.

[6] Gossage, K.W., et al., Texture analysis of optical coherence tomography images: feasibility for tissue classification. J Biomed Opt, 2003. 8(3): p. 570-5.

[7] Jitendra Malik, S.B., Thomas Leung, Jianbo Shi, Contour and Texture Analysis for Image Segmentation. International Journal of Computer Vision, 2001.

[8] Gadkari, D., Image Quality Analysis Using GLCM, in College of Arts and Sciences2004, University of Central Florida: Florida.

[9] Susan Rodgers, R.C., Encountering Asian Art through Joint Faculty - Student Field Research and Museum Curatorship: Ignatian Parallels. Jesuit Higher Education, 2012.

[10] Dewi, L.G.W.L., Perkembangan dan Sistem Pewarisan Kerajinan Tenun Ikat Endek Di Desa Sulang, Klungkung, Bali. Jurnal Widya Winayata 2013. 1(1).

[11] Li, J., Ostoja-Starzewski, M., Edges of Saturn's rings are fractal. Springerplus, 2015. 4: p. 158.

[12] Yousif Mohamed Y. Abdallah, A.H., Eltayeb Wagiallah, Automatic Enhancement of Mammography Images using Contrast Algorithm. International Journal of Science and Research, 2012.

[13] Kristian Adi Nugraha, W.H., Nugroho Agus Haryono, Analisis Tekstur Pada Citra Motif Batik Untuk Klasifikasi Menggunakan K-NN. Jurnal Informatika, 2014.

[14] Liu, C.-H., et al., Improvement of tissue analysis and classification using optical coherence tomography combined with Raman spectroscopy. Journal of Innovative Optical Health Sciences, 2014: p. 1550006.

[15] Han, D., et al., Classification of levee slides from airborne synthetic aperture radar images with efficient spatial feature extraction. Journal of Applied Remote Sensing, 2015. 9(1): p. 097294.

[16] Lu, D., et al., A survey of remote sensing-based aboveground biomass estimation methods in forest ecosystems. International Journal of Digital Earth, 2014: p. 1-43.

[17] Kiema, J.B.K., Texture analysis and data fusion in the extraction of topographic objects from satellite imagery. International Journal of Remote Sensing, 2002. 23(4): p. 767-776.

Content-Based Image Retrieval using Local Features Descriptors and Bag-of-Visual Words

Mohammed Alkhawlani
Ibb University
Ibb, Yemen

Mohammed Elmogy
Dept. of Information Technology,
Faculty of Computers and
Information, Mansoura University
Mansoura, Egypt

Hazem Elbakry
Dept. of Information Systems,
Faculty of Computers and
Information, Mansoura University
Mansoura, Egypt

***Abstract*—Image retrieval is still an active research topic in the computer vision field. There are existing several techniques to retrieve visual data from large databases. Bag-of-Visual Word (BoVW) is a visual feature descriptor that can be used successfully in Content-based Image Retrieval (CBIR) applications. In this paper, we present an image retrieval system that uses local feature descriptors and BoVW model to retrieve efficiently and accurately similar images from standard databases. The proposed system uses SIFT and SURF techniques as local descriptors to produce image signatures that are invariant to rotation and scale. As well as, it uses K-Means as a clustering algorithm to build visual vocabulary for the features descriptors that obtained of local descriptors techniques. To efficiently retrieve much more images relevant to the query, SVM algorithm is used. The performance of the proposed system is evaluated by calculating both precision and recall. The experimental results reveal that this system performs well on two different standard datasets.**

Keywords*—*Content-based Image Retrieval (CBIR); Scale Invariant Feature Transform (SIFT); Speeded Up Robust Features (SURF); K-Means Algorithm; Support Vector Machine (SVM); Bag-of-Visual Word (BoVW)

I. Introduction

Image retrieval is the field of the study that concerned with looking, browsing, and recovering digital images from an extensive database. CBIR is viewed as a dynamic and quick advancing research area in image retrieval field. It is a technique for retrieving images from a collection by similarity. The retrieval based on the features extracted automatically from the images themselves. Many of CBIR systems, which is based on features descriptors, are built and developed.

A feature is defined as capturing a certain visual property of an image. A descriptor encodes an image in a way that allows it to be compared and matched to other images. In general, image features descriptors can be either global or local. The global feature descriptors describe the visual content of the entire image, whereas local feature describes describe a patch within an image (i.e. a small group of pixels) of the image content. The superiority of the global descriptor extraction is the increased speed for both feature extraction and computing similarity. However, global features still too rigid to represent an image. Particularly, they can be oversensitive to location and consequently fail to identify important visual characteristics [1, 2].

Local feature approaches provide better retrieval effectiveness and great discriminative power in solving vision problems than global features [3]. However, the number of local features that are extracted for each image may be immense, especially in the large image dataset. Wherefore, BoVW [4, 5] is proposed as an approach to solving this problem by quantizing descriptors into "visual words."

Depending on the previous facts, the present study proposed a system for image retrieval based on local features using BoVW model. The system tries to bring more accuracy with the option to use the two main local descriptors (SIFT [6], SURF [7]).

The rest of this paper is organized as follows. Section 2 gives an overview of the BoVW model, K-Means, and SVM. Section 3 discusses two of the most commonly used local feature descriptors. Section 4 reviews some of the related work using BoVW model in image retrieval. In Section 5, the proposed architecture of our image retrieval system, which is based on local feature descriptor, is introduced. Our experimental results are manipulated in Section 6. Finally, Section 7 contains the conclusion and our future work.

II. Bag-of-Visual Word Model

The BoVW model is one of the most widely used ways that represents images as a collection of local features. For this reason, some researchers tend to name it as a bag of features. These local features are typically grouped of local descriptors. The total number of local descriptors that is extracted for each image may be colossal. In addition, searching nearest neighbors for each local descriptor in the image query consumes a long time. Therefore, BoVW was proposed as an approach to tackling this issue by quantizing descriptors into "visual words," which decreases the descriptors' sum drastically. Thus, BoVW makes the descriptor more robust to change. This model is very close to the traditional description of texts in information retrieval, but it is considered for images retrieval [5, 6]. BoVW is the de facto standard of image features for retrieval and recognition [7]. It consists of three main stages like the following in the sequent subsections:

A. Keypoint Detection

The first step of the BoVW model is to detect local interest points. For feature extraction of interest points, they are computed at predefined locations and scales [8]. Feature extraction is a separate process from feature representation in

BoVW approaches [9]. There are many keypoint detectors that were used in research, such as Harris-Laplace, Difference of Gaussian (DoG), Hessian Laplace, and Maximally Stable Extremal Regions (MSER) [10, 11].

B. Features Descriptors

The keypoints are described as multidimensional numerical vectors, according to their content [6]. In other words, features descriptors are used to determine how to represent the neighborhood of pixels near a localized keypoint [9]. The most efficient feature descriptors in the BoVW model are SIFT and SURF.

C. Building Vocabulary

In the previous stage, the total extracted feature descriptors are large. To solve this problem, the feature descriptors are clustered by applying the clustering algorithm, such as K-Means technique [12] to generate a visual vocabulary. Each cluster is treated as a distinct visual word in the vocabulary, which is represented by their respective cluster centers. The size of the vocabulary is determined using the clustering algorithm. In addition, it depends on the size and the types of the dataset [7].

The BOW model can be formulated as follows. First, BoVW is usually defining the training dataset as S including images represented by $S = s_1, s_2, \ldots, s_n$, where s is the extracted visual features. After that, used clustering algorithm like K-Means, which is based on a fixed number to visual words W represented by $W = w_1, w_2, \ldots, w_v$, where v is the cluster number. Then, the data is summarized in a V×N occurrence table of counts $N_{ij} = n(w_i, s_j)$, where $n(w_i, s_j)$ denotes how often the word w_i is occurred in an image s_j [6].

On the other hand, K-Means is one of the most unsupervised learning algorithms that take care of the well-known clustering issue. It defines the size of K clusters based on the features extracted from the images themselves [13]. It is used to calculate the nearest neighbors of the points and the cluster center. It is usually utilizing the method of computation by approximating the nearest neighbor method. This method can be scaled to similarly large vocabulary sizes by the use of approximate nearest neighbor methods [12].

SVM is supervised machine learning technique [14]. It shows the image database as two sets of vectors in a high or infinite-dimensional space. It relies on a fundamental principle, which is called a maximum margin classifier. A maximum margin classifier is a hyperplane, which separates two 'clouds' of points at equal distance. The margin between the hyperplane and the clouds is maximal. SVM built a hyperplane or set of hyperplanes that increases the margin among the images that are relevant and not relevant to the query [15]. The goal of SVM classification technique is to find an ideal hyperplane to separate the irrelevant and relevant vectors using maximizing the size of the margin between both classes [16].

An image classification is a machine learning technique. It is a step used to accelerate image retrieval in big-scale databases and is used to increase retrieval precision. Similarly, in the absence of labeled data, unsupervised clustering is found to be helpful to increase the retrieval velocity and to improve retrieval precision. Image clustering based on a similarity measure, while the image classification has been performed using different techniques that does not require the use of similarity measures [15, 17].

III. Local Feature Descriptors

In computer vision, local feature technique contains two parts [18]: feature detector and feature descriptor. Feature detector determines regions of an image that have unique content, like corners. Feature detection is used to find interest points (keypoints) in the image that remain locally invariant. Therefore, it can detect them even in the presence of scale change or rotation. Whereas, feature descriptor involves computing a local descriptor, which is usually done on regions centered on detected interest points. Local descriptors depend on image processing to transform a local pixel neighborhood into a compact vector representation [19].

On the other hand, the local descriptors are broadly used in many of computer vision research, such as robust matching, image retrieval, and object detection and classification. In addition, using local descriptors enables computer vision algorithms to deal strongly with rotation, occlusion, and scale changes.

Local feature algorithms depend on the idea of determining some interest points in the image and implementing a local analysis on them, rather than looking at the image as a whole. There are numerous algorithms for describing local image regions, such as SIFT and SURF. The SIFT and SURF descriptors depend on local gradient computations. The following subsections will discuss the SIFT and SURF algorithms briefly.

A. Scale Invariant Feature Transform (SIFT)

Lowe [3] developed SIFT as a continuation of his previous work on invariant feature detection. It has four computational phases: (a) extrema detection, (b) keypoint localization, (c) orientation assignment, and (d) keypoint description.

The first phase examines the image under different octaves and scales to isolate points of the image that are different from their surroundings. These points, which are called extrema, are potential candidates for image features. In keypoint localization phase, it selects some of extrema points to be keypoints. Candidate keypoints are refined by reject extrema points that are caused by edges and by low contrast points. In the orientation assignment phase, it represents every keypoint and neighbors as a set of vectors using the magnitude and the direction. In the last phase, it takes a collection of vectors in the neighborhood of every keypoint and combines this information with a set of eight vectors called the descriptor. The neighborhood is divided into 4×4 regions, in each region the vectors are histogrammed in eight bins. SIFT provides a 128 element of the keypoint descriptor.

B. Speeded Up Robust Features (SURF)

Bay *et al.* [4] introduced the SURF algorithm as a scale- and rotation-invariant interest point detector and the descriptor. SURF algorithm is a mixing of crudely localized information and the distribution of related gradient. SURF algorithm is similar to SIFT algorithm, but it is much more simplified and faster in computation and matching.

SURF algorithm depends on the Hessian Matrix to detect keypoints. It uses a distribution of Haar wavelet responses at the keypoint's neighborhood. The final descriptor is obtained by concatenating the feature vectors of all the sub-regions and represented with 64 elements.

The SIFT and SURF algorithms are nowadays the most widely used feature-based techniques in the computer vision community. These algorithms have proven their efficiency and robustness in the invariant feature localization (invariant to image rotation, scaling, and changes in illumination) [4, 20].

IV. RELATED WORK

The subject of image retrieval is discussed intensively in the literature. The success of using BoVW model had also contributed to increasing the number of researchers and studies. For example, Cakir *et al.* [21] studied CBIR using BoVW model. They discussed how BoVW considers an image as a document, going through using K-Means as vector quantization uses.

Zhang *et al.* [22] proposed a bag of images for CBIR schemes. They supposed that the image collection composed of image bags rather than independent individual images. They contain some relevant images that have same perceptual meaning. The image bags were built before image retrieval. In addition, a user's query is an image bag, named query image bag. In this condition, all image bags in the image collection are sorted according to their similarities to the query image bag. It hypothetically represented that the new idea can enhance the image retrieval process. However, this work needs to develop more efficient ways to measure the dissimilarity between two image bags.

Ponitz *et al.* [23] attempted to solve the problem of detecting images limitations in huge scale image databases. They decide to enhance the methodology of BoVW by improving the distance measure between image signatures to avoid the occurrence of vague features. They utilized SIFT algorithm for local visual features acquisition. Only 60% of all images were randomly chosen, and their features utilized for clustering. These features were then quantized. 100 random images are selected as input images. The images were changed with mounting distortion to test the robustness of the application. It needs more discrimination force of the actual image description.

Liu [8] reviewed BoVW model in image retrieval system. He provided details about BoVW model and explained different building strategies based on this model. First, he presented several procedures that can be taken in BoVW model. Then, he explained some popular keypoint detectors and descriptors. Finally, he looked at strategies and libraries to generating vocabulary and do the search.

Alfanindya *et al.* [24] presented a method for CBIR by using SURF with BoVW. First, they used SURF to computed interest points and descriptors. Then, they created a visual dictionary for each group in the COREL database. They concluded from their experiments that their method outperforms some other methods in terms of accuracy. The major challenge in their work was that the proposed method is highly supervised. It means that they n need to determine the number of groups before they perform classification.

The primary aim of this paper is to design a system for image retrieval based on local feature descriptors using BoVW model. Most of the previous image retrieval using BoVW systems used only one local descriptor. Whereas, our proposed system uses both SIFT and SURF descriptors. It provides a comparison of the actual performance of those local descriptors with BoVW in image retrieval field.

V. SYSTEM ARCHITECTURE

We propose a system for image retrieval based on extracting local features using BoVW model. The system uses SIFT or SURF techniques to extract keypoints and compute the descriptor for those keypoints. K-Means algorithm is used to obtain the visual vocabulary. As shown in Figure 1, the proposed system consists of two stages: a training stage and a testing stage. During the training stage, the proposed system is given below:

1) For each image in the dataset:

- Convert image to a grayscale.
- Resizing the image to (300,300 pixels) to get uniformed results.
- Image features are extracted and associated these characteristics to local descriptors.
- Cluster the set of these local descriptors for the amount of bags using a K-Means algorithm to construct a vocabulary of K clusters.

2) For each feature descriptor in the image:

- Find the nearest visual word from the vocabulary for each feature vector with L2 distance based matching.
- Compute the Bag-of-words image descriptor as is a normalized histogram of vocabulary words encountered in the image.
- Save the Bag-of-words descriptors for all image.

At the test stage, the proposed system is given below, for each input image:

- The input image is pre-processed for keypoints extraction.
- Local descriptors are computed from the pre-processed input image.
- Compute the Bag-of-Words vector with the algorithm defined above.
- In the matching step, grab the best results via SVM Classification.

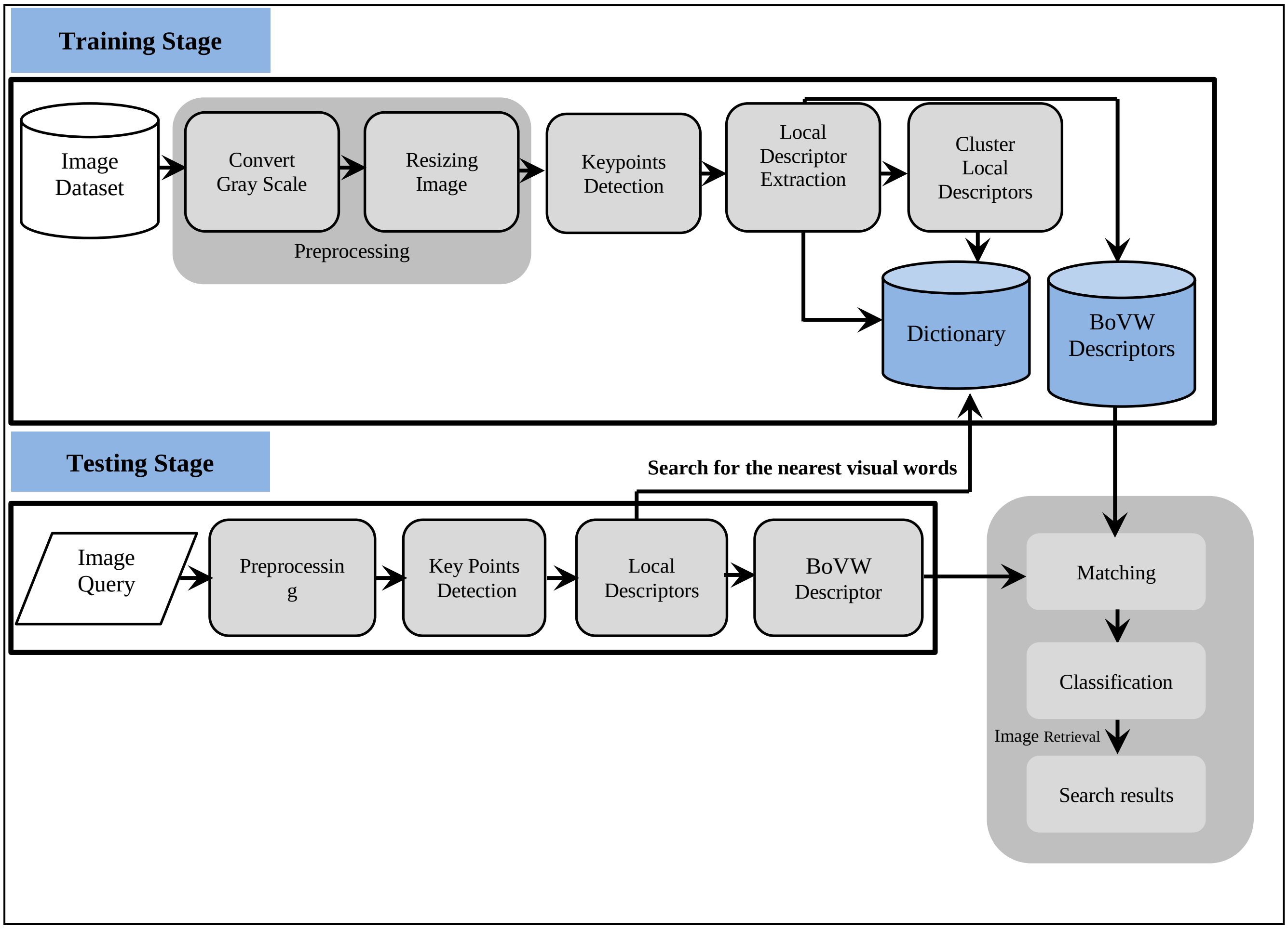


Fig. 1. The architecture of the proposed system

A. Reprocessing

The preprocessing step consists of converting the image to grayscale and resizing process. Due to the local descriptors algorithms that deal only with density information, the images are converted to the grayscale. After that, the images are resized to 300x300 pixels to normalize the results.

B. Keypoint Detection and Description

The most important step in the proposed system is to extract the local descriptors from the processed image. There are many keypoint description techniques, such as Harris, SIFT, and SURF. In this paper, SIFT and SURF description were chosen in order to test the performance of the proposed system. Once keypoints are extracted from the image, the system computes the local description of each keypoint, as shown in Figure 2.

C. BoVW Descriptor

In this step, the BoVW model is used to create the vocabulary. First, we compute the centroid of the vocabulary that is closest to the feature vector using Brute Force matcher method. Then, we calculate the difference between the centroid and the feature vector. Finally, we compute the bag-of-words image descriptor as a normalized histogram of vocabulary words.

(a) (b)

Fig. 2. The local feature extration for one of the used images, (a) The gayscale image, (b) The extracted local features

D. Matching and Classification

At this stage, the descriptor query is used to match the BoVW descriptors in the database. The nearest neighbor approach was used to retrieve similar images.

Finally, SVM classification was used to grab the best results, which has the most similarity with the image query.

VI. THE PERFORMANCE EVALUATION AND RESULTS

A. Dataset

The system was evaluated by using two different standard datasets: the Flickr Logos 27 dataset [25] and Amsterdam Library of Object Images (ALOI) dataset [26]. The Flickr Logos 27 dataset is an annotated logo dataset downloaded from Flickr, and it consists of three image collections/sets. The training set contains 810 annotated images, corresponding to 27 logo classes/brands (30 images for each class). Figure 3 shows some image samples of the training set. The query set consists of 270 images. There are five images for each of the 27 annotated classes, summing up to 135 images that contain logos. Some image samples from the queries set are presented in Figure 4.

Fig. 3. Some sample images from the Flickr Logos dataset for the training

Fig. 4. Some sample images from the Flickr Logos dataset for the queries

ALOI is a color image collection of one-thousand small objects, which is recorded for scientific purposes under various imaging circumstances (viewing angle, illumination angle, and illumination color). Over a hundred images of each object were recorded, yielding a total of 110,250 images. A large variety of object shapes, transparencies, and surface covers are considered. It makes this database quite interesting to evaluate object-based image retrieval approaches [27]. Some image samples of the training set and queries set are presented in Figures 5 and 6.

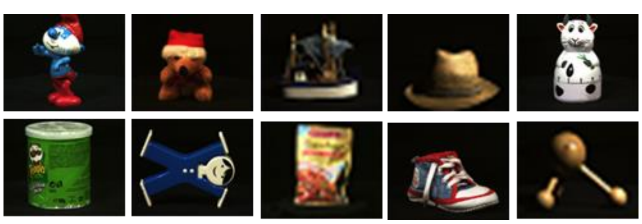


Fig. 5. Some sample images from ALOI dataset for the training

Fig. 6. Some sample images from ALOI dataset for the queries

B. Experimental Results

The performance of our system was measured using precision and recall measures. Recall measures the ability of the system to retrieve all the images that are relevant while precision measures the ability of the system to retrieve only the images that are relevant.

Eq. (1) is used to calculate the precision of the retrieval performance:

$$Precision = \frac{TruePositives}{TruePositives + FalsePositives} \qquad (1)$$

True Positives is the number of the images that are correctly retrieved from the image datasets. While, False Positives is the number of images that are incorrectly retrieved from the image datasets. In addition, the recall of the retrieval performance was calculated by Eq. (2):

$$Recall = \frac{TruePositives}{TruePositives + Missed} \qquad (2)$$

The missed parameter is the number of relevant images that is not retrieved. Additionally, Precision-Recall graphs were used to measure the accuracy of our image retrieval system. They are used to evaluate the performance of any search engine.

All tests were performed on an HP-ElitBook-2740p laptop with Intel Core i5, 2.40 GHz processor, 4GB RAM, and Windows 7 Ultimate 64-bit as an operating system. The system was implemented in Microsoft Visual Studio 2013 using OpenCV version 2.4.9 for the graphical processing functions and C Sharp for the GUI design with EmguCV as a wrapper.

In the Flickr Logos 27 dataset, ten classes randomly selected (Google, FedEx, Porsche, Red Bull, Starbucks, Intel, Sprite, DHL, Vodafone, NBC) for training stage. The total number for training stage is of 300 images and 50 images in the testing stage. In the test stage, each image has been queried twice, once using SURF and other using SIFT. Precision and recall values appear directly below the images retrieved, as shown in Figures 7, 8. Table 1, Figure 9 (Precision-Recall graphs) show the values of the average of the precision and recall of all images in the test set with 10 class (5 images for each class).

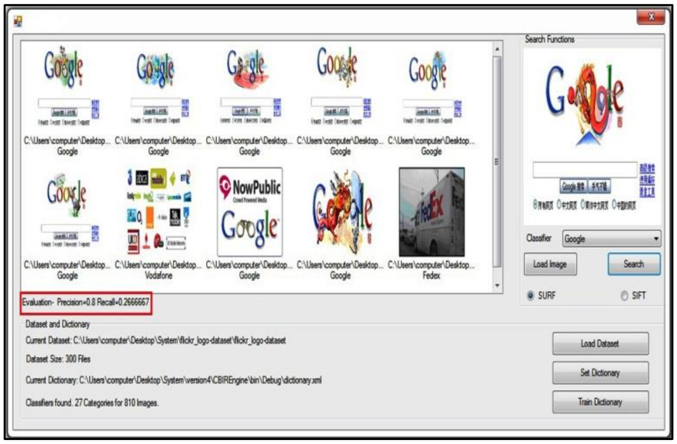


Fig. 7. A snapshot of our proposed system in Flickr dataset using SURF technique

Fig. 8. A snapshot of our proposed system in Flickr dataset using SIFT technique

TABLE I. THE AVERAGE OF THE PRECISION AND RECALL OF EACH CLASS (FLICKR LOGOS DATASET)

Class	Precision		Recall	
	SURF	SIFT	SURF	SIFT
Google	0.88	0.84	0.29	0.28
Fedex	0.84	0.78	0.28	0.26
Porsche	0.82	0.78	0.27	0.26
RedBull	0.84	0.78	0.28	0.26
Starbucks	0.82	0.96	0.27	0.32
Intel	0.82	0.78	0.27	0.26
Sprite	0.84	0.74	0.26	0.25
DHL	0.74	0.74	0.25	0.25
Vodafone	0.82	0.72	0.25	0.24
Nbc	0.76	0.68	0.25	0.22
Average	**0.82**	**0.78**	**0.27**	**0.26**

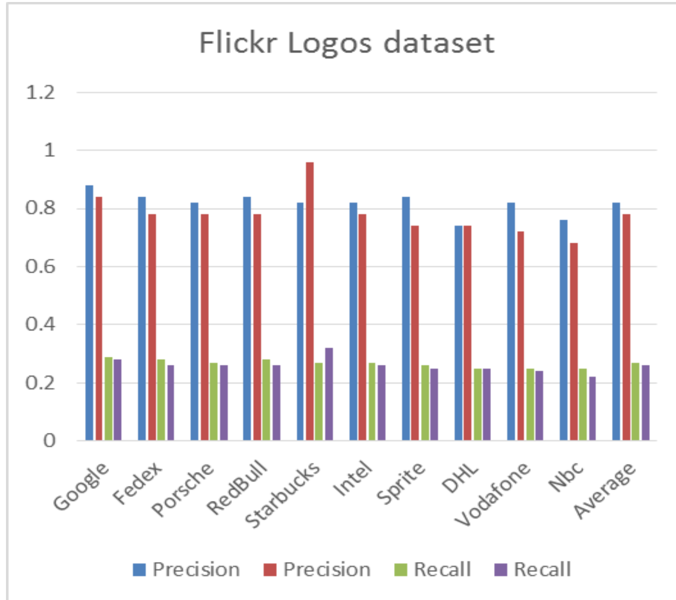


Fig. 9. The graph of the precision and Rcall of each class in Flickr Logos dataset

In ALOI dataset, the similar procedures that conducted for Flickr Logos 27 dataset were used. Accordingly, ten object images randomly selected from ALOI dataset (Big Smurf, Blue girls shoe, Boat, Christmas bear, cow kitchen clock, Green Pringles box, head, pasta and sugo, toy keys, Wooden massage) for training stage. Therefore, the total number of 300 object images for training stage and 50 object images for the testing stage. In the test set, each object has been queried twice, once using SURF and other using SIFT. Precision and recall values appear directly as shown in Figures 10, 11.

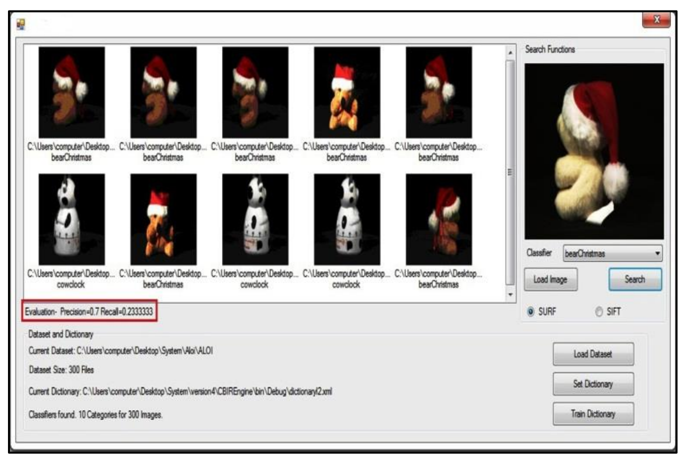


Fig. 10. A snapshot of our proposed system in ALOI dataset using SURF technique

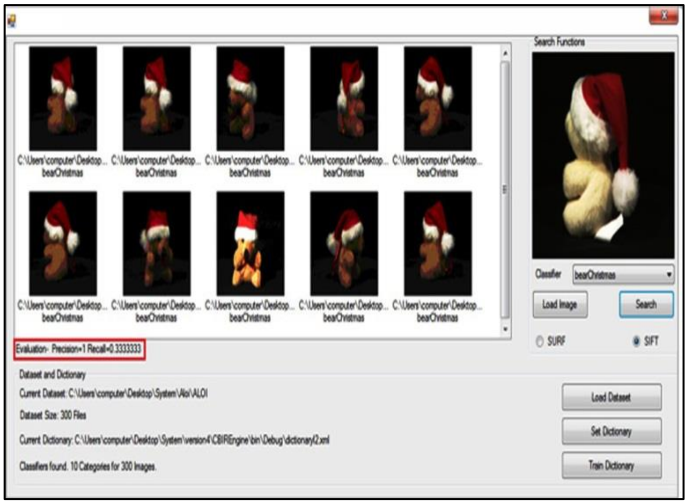


Fig. 11. A snapshot of our proposed system in ALOI dataset using SIFT technique

Table 2 and Figure 12 (Precision-Recall graphs) showing the values of the average of the precision and recall of all images in the test set with ten objects.

TABLE II. THE AVERAGE OF THE PRECISION AND RECALL OF EACH OBJECT (ALOI DATASET)

Object Name	**Precision**		**Recall**	
	SURF	**SIFT**	**SURF**	**SIFT**
Boat	0.94	0.94	0.31	0.31
Toy keys	0.84	0.76	0.28	0.25
Cow kitchen clock	0.82	0.84	0.27	0.28
Wooden massage	0.84	0.84	0.28	0.28
Big smurf	0.76	0.82	0.25	0.27
Pringles box	0.94	0.94	0.31	0.31
Pasta and sugo	0.96	0.94	0.32	0.31
Head	0.84	0.94	0.27	0.31
Blue girls shoe	0.94	0.96	0.31	0.32
Christmas bear	0.72	0.82	0.24	0.27
Average	**0.86**	**0.88**	**0.28**	**0.29**

As shown in the results of Fiker dataset, SURF algorithm was the batter than SIFT algorithm. The reason is that the SURF has good matching rate compared with SIFT. However, the results of SIFT with ALOI dataset was the better than SURF.

The reason may be due to the SIFT is more suitable for objects because it extracts more features. Also, maybe SURF are not robust enough in various imaging circumstances. However, seems both SIFT and SURF more suitable according of the type of the dataset.

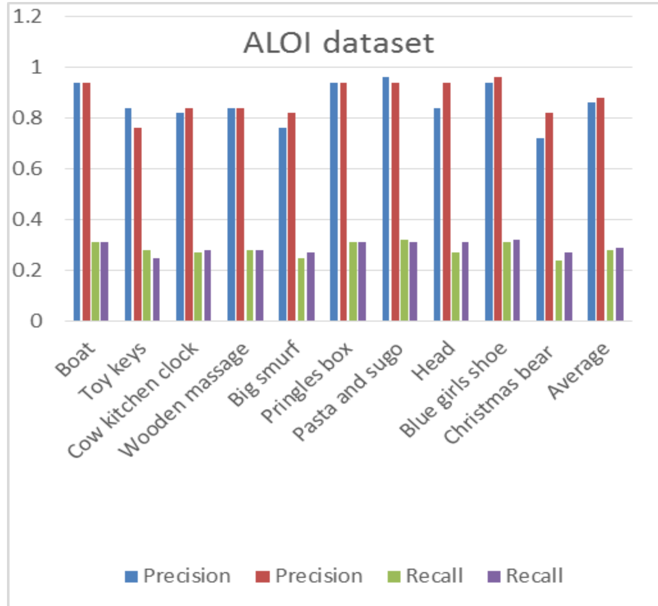


Fig. 12. The graph of the precision and Rcall of each object in ALOI dataset

VII. CONCLUSION

With advances in the multimedia technologies and the social networks, CBIR is considered an active research topic. Recent CBIR systems rely on the use of the BoVW model for being enables efficient indexing for local image features. This paper presented a system for CBIR, which uses local feature descriptors to produce image signatures that are invariant to rotation and scale. The system combines the robust techniques, such as SIFT, SURF, and BoVW, to enhance the retrieval process. In the system, we used a k-means algorithm to cluster the feature descriptors in order build a visual vocabulary. As well as, SVM is used as a classifier model to retrieve much more images relevant to the query efficiently in the features space.

We compared two different features descriptors techniques with BoVW model. Based on the experimental results, it is found that both SIFT and SURF are appropriate depending on the type of used dataset. The performance of the proposed system is evaluated by calculating the precision and recall on two different standard datasets. The experiments demonstrated the efficiency, scalability, and effectiveness of the proposed system.

In the future, we intend to study the possibility of improving the system performance using other local descriptors. We will do a comparative study between all of these descriptors according to illumination changes, scale changes, and noisy images on other types of standard datasets.

REFERENCES

[1] Datta R., Joshi D., Li J., and Wang J.Z. "Image retrieval: Ideas, influences, and trends of the new age, " ACM Computing Surveys (CSUR), vol. 40, no. 5, 2008.

[2] Halawani A., Teynor A., Setia L., Brunner G., and Burkhardt H. "Fundamentals and Applications of Image Retrieval: An Overview, " Datenbank-Spektrum, vol. 18, pp. 14–23. 2006.

[3] Aly M., Welinder P., Munich M., and Perona P. "Automatic discovery of image families: Global vs. local features, " Image Processing (ICIP), 16th IEEE Int. Conf. on, IEEE, pp. 777–780. 2009.

[4] Sivic, J., & Zisserman, A. "Video Google: A text retrieval approach to object matching in videos". In Computer Vision. Proceedings. Ninth IEEE International Conference on. pp. 1470-1477. 2003.

[5] Csurka G., Dance C., Fan L., Willamowski J., and Bray C. "Visual categorization with bags of keypoints, " Workshop on Statistical learning in compute. Vis., ECCV. Vol. 1. No. pp.1-22. 2004.

[6] Lowe D.G., "Distinctive image features from scale-invariant keypoints, " Int. journal of compute. Vis., vol. 60, pp. 91–110. 2004.

[7] Bay H., Tuytelaars T., and Van Gool L. "Surf: Speeded up robust features" Compute. Vision–ECCV, Springer, pp. 404–417. 2006.

[8] Liu, J. "Image retrieval based on bag-of-words model ". Cornell University Library:1304.5168,2013.

[9] Mikolajczyk, K., Tuytelaars, T., Schmid, C., Zisserman, A., Matas, J., Schaffalitzky, F,& Van Gool, L. "A comparison of affine region detectors". International journal of computer vision, 65(1-2), pp. 43-72.,2005.

[10] Mukherjee, J., Mukhopadhyay, J., & Mitra, P. "A survey on image retrieval performance of different bag of visual words indexing techniques" . In Students' Technology Symposium (TechSym), pp. 99-104. IEEE,2014.

[11] Tsai, C. F. "Bag-of-words representation in image annotation: A review".ISRN Artificial Intelligence, 2012.

[12] Hartigan, J. A., & Wong, M. A. "Algorithm AS 136: A k-means clustering algorithm". Applied Statistics,pp. 100-108. 1979.

[13] Chang, R. I., Lin, S. Y., Ho, J. M., Fann, C. W., & Wang, Y. C. (2012). "A novel content based image retrieval system using k-means/knn with feature extraction". Computer Science and Information Systems, 9(4), pp.1645-1661.2012.

[14] O'Hara, S., & Draper, B. A. "Introduction to the bag of features paradigm for image classification and retrieval". Cornell University Library:1101.3354.2011.

[15] Mikolajczyk, K., Leibe, B., & Schiele, B.). "Local features for the object class recognition." In Computer Vision, 2005. ICCV 2005. Tenth IEEE International Conference on (Vol. 2, pp. 1792-1799). IEEE.2005.

[16] Tuytelaars, T., & Mikolajczyk, K. "Local invariant feature detectors: a survey". Foundations and Trends® in Computer Graphics and Vision, 3(3), pp.177-280.2008.

[17] Boser, B. E., Guyon, I. M., & Vapnik, V. N. "A training algorithm for optimal margin classifiers". In Proceedings of the fifth annual workshop on Computational learning theory (pp. 144-152). ACM.1992.

[18] Li, J., & Allinson, N. M. "A comprehensive review of current local features for computer vision". Neurocomputing, 71(10), pp. 1771-1787. 2008.

[19] http://www.mathworks.com/help/vision/ug/local-feature-detection-and-extraction.html (Last accessed on 8/6/2015).

[20] Guerrero, M. "A comparative study of three image matching algorithms: SIFT, SURF, and Fast." Master Thesis (Utah State University) .2011.

[21] www.cs.bilkent.edu.tr (Last accessed on 11/6/2015).

[22] Zhang, J., & Ye, L. "Image retrieval based on a bag of images". In Image Processing (ICIP), 2009 16th IEEE International Conference on (pp. 1865-1868). IEEE.2009.

[23] Pönitz, T., Stöttinger, J., Donner, R., & Hanbury, "A. Efficient and Distinct Large Scale Bags of Words".Austrian Research Promotion Agency (FFG). 2010.

[24] Alfanindya, A., Hashim, N., & Eswaran, C. "Content-Based Image Retrieval and Classification using speeded-up robust features (SURF) and grouped bag-of-visual-words (GBoVW) ". In Technology, Informatics, Management, Engineering, and Environment (TIME-E), 2013 International Conference on (pp. 77-82). IEEE. 2013.

[25] http://image.ntua.gr/iva/datasets/flickr_logos/.(Last accessed on 17/6/2015).

[26] http://aloi.science.uva.nl/. (Last accessed on 19/6/2015).

[27] Geusebroek, J. M., Burghouts, G. J., & Smeulders, A. W. "The Amsterdam library of object images." International Journal of Computer Vision,61(1), pp.103-112. 2005.

Online Paper Review Analysis

Doaa Mohey El-Din
Information Systems Department
Faculty of Computers and Information, CU
Cairo, Egypt

Hoda M.O. Mokhtar
Information Systems Department
Faculty of Computers and Information, CU
Cairo, Egypt

Osama Ismael
Information Systems Department
Faculty of Computers and Information, CU
Cairo, Egypt

***Abstract*—Sentiment analysis or opinion mining is used to automate the detection of subjective information such as opinions, attitudes, emotions, and feelings. Hundreds of thousands care about scientific research and take a long time to select suitable papers for their research. Online reviews on papers are the essential source to help them. The reviews save reading time and save papers cost. This paper proposes a new technique to analyze online reviews. It is called sentiment analysis of online papers (SAOOP). SAOOP is a new technique used for enhancing bag-of-words model, improving the accuracy and performance. SAOOP is useful in increasing the understanding rate of review's sentences through higher language coverage cases. SAOOP introduces solutions for some sentiment analysis challenges and uses them to achieve higher accuracy. This paper also presents a measure of topic domain attributes, which provides a ranking of total judging on each text review for assessing and comparing results across different sentiment techniques for a given text review. Finally, showing the efficiency of the proposed approach by comparing the proposed technique with two sentiment analysis techniques. The comparison terms are based on measuring accuracy, performance and understanding rate of sentences.**

Keywords—Sentiment analysis; Opinion Mining; Reviews; Text analysis; Bag of words; sentiment analysis challenges

I. INTRODUCTION

World Wide Web (www) has become the most popular communication platforms to the public reviews, opinions, comments and sentiments about products, places, scientific books or papers and to daily text reviews. The number of active user bases and the size of their reviews created daily on online websites are massive. There are 2.4 billion active online users, who write and read online and Internet usage around the world [1]. Scientific research domain has a big world in journals and conferences, there are more than 4000 rated conferences and 5000 ranked journals [2]. Each one of them has thousand number of papers such as ACM, Springer and Science direct. Notably, a large fragment of WWW researchers makes their content public, allowing researchers, societies, universities, corporations to use and analyze data. According to a new survey conducted by Dimensional Research, April 2013: 90% of customer's decisions depends on Online Reviews [3]. According to 2013 Study [4]: 79% of customer's confidence is based on online personal recommendation reviews. As the result, a large number of studies and research have monitored the trending new research increasing year by year. In this work, trying to achieve trusted scientific reviews evaluation to be useful for researchers and facilitate the selection of the suitable papers.

Recently, several websites encourage researchers to express and exchange their views, suggestions and opinions related to scientific papers. Sentiment analysis [5] depends on two issues sentiment polarity and sentiment score. Sentiment polarity [6] is a binary value either positive or negative. On the other hand, sentiment score which relies on one of three models [7]. Those models are Bag-of-words model (BOW) [8], part of speech (POS) [9], and semantic relationships [10]. BOW [11] is the most popular for researchers and based on the representation of word but BOW neglects language grammar. POS [12] which is grammatically tagging especially verbs, adjectives and adverbs [13]. For example, (The research is not good.) declaring in (The/DT research/NN is/VBZ not/RB good/JJ. /.). In the example DT refers to "Determiner", NN refers to "Noun", singular or mass, VBZ refers to "Verb", RB refers to "Adverb", and JJ refers to "Adjective". But a semantic relationship method is the most complex method, which is based on the relationship between concepts or meanings for example antonym, synonym, homonym etc.

There is a research gap the sentiment analysis accuracy because of sentiment evaluation drawbacks and sentiment analysis challenges [14].The evaluation sentiment drawbacks that Reflected in language coverage. This paper focuses on understanding text reviews and introduces solutions for some sentiment challenges. The sentiment analysis challenges summarized in ten challenges [15]. They are spam and fake reviews Detection, Limitation of classification filtering, Asymmetry in availability of opinion mining software Incorporation of opinion with implicit and behavior data, Incorporation of opinion with implicit and behavior data, and Natural language processing overheads (ambiguity), Generation of highly content lexicon database, handling of bipolar sentiments, dealing with short Sentence like abbreviations, Requirement of World Knowledge, Negation. All challenges have a bad effect on the understanding of reviews.

In this paper, the research aims to fill this research gap by proposing the new technique for sentiment analysis of online scientific papers reviews (SAOOP). The technique also measures efficiency by making a comparison between SAOOP, and other two sentiment analysis techniques [16]. Namely "Natural Language Toolkit-Text processing" (NLTK) and "recursive deep models for semantic" (NLPS). The results depend on comparing accuracy, performance and rate of coverage of language through two datasets.

The rest of this paper is organized as follows: Section 2 represents related works. Section 3, the presentation of the new technique "SAOOP". In Section 4, outlines of the Experiment as well as the sample used for comparison. Section 5 highlights the comparison results. Finally, Section 6 concludes and proposes directions for future work.

II. Related Works

The purpose of this paper is sentiment evaluation which means to find the sentiment polarity (positive, negative, or neutral) of a text reviews data and evaluate the sentiment score of the text review. Generally a text review is divided into single sentences ("sentence-based") and words ("words-based") or very short texts from a single source.

A. *Sentiment Analysis: An Overview*

The author in (Sentiment analysis of document based on annotation) presented a tool which judges the quality of text based on annotations on scientific papers [17]. The authors's methodology declares in collective's sentiment of annotations in two approaches. This methodology counts all the annotation produces the documents and calculates total sentiment scores. The problem of this methodology appears in a relationship between annotations that is complex. The technique needs to have a big query knowledge base containing metadata. The notion declares in that the values are not accurate enough such as the value of "Good=0.875" has greater value than the value of "Best=0.75" although the result is wrong in logical meaning. Nevertheless, believing that collecting metadata and evaluating them could be useful to achieve higher analysis quality.

The researchers proposed a "Web Based Opinion Mining system" for hotel reviews [18]. They introduced an evaluation system for online user's reviews and comments to support quality controls into hotel management. The research is capable of detecting and retrieving reviews on the web and deals with German reviews. The multi-topic/multi-polarity is the method of this research; the system would recognize the neutral e.g., "don't know" to "classify sentiment polarity that as neutral" and the multi-topic cases identified in their corpus. The major weakness illustrates in not handling some cases in multi-topic segments. The authors [19] analyzed sentiments reviews of mobile devices products. Their Machine learning (ML) [20] system investigates the classification accuracy of Naïve Bayes algorithm. In addition to Judge the product quality and status in the market is advantageous. They use three machine learning algorithms (Naïve Base Classifier, K-nearest neighbor [21], and random forest [22] to calculate the sentiments accuracy. The random forest improves the performance of the classifier.

B. *Sentiment Analysis Techniques*

This section provides a brief description of the two sentiment analysis techniques investigated in this paper. These techniques are the most popular in the literature and they cover diverse techniques such as the use of Natural Language Processing (NLP) [23] in assigning polarity and sentiment score.

1) Natural Language Toolkit: The authors aim at an evaluation sentiment scores and polarity. They produce the Natural Language Toolkit (NLTK) [12]. NLTK is a text analysis technique that evaluates cognitive and constitutional components of a given text reviews based on using lexicon including words. They use hierarchal sentiment classification level with two levels (Neutral, Positive, and Negative). The drawback of this technique illustrated in low accuracy and some logical errors. Because the technique needs to increase handling of language coverage [24].

2) NLP Stanford sentiment (NLPS): The researchers introduce recursive neural models have in common: word vector representations and classification [25]. The authors released a tool named "NLP Stanford" NLPS [26], which develops an integration of learning techniques that produces better results and higher accuracy training model empirically. Their goal is based on Semantic word spaces have been very beneficial but NLPS cannot express the meaning of longer phrases in a primary way. So they improve this technique by detection the sentiment requires wider supervised training and evaluation resources.

III. Sentiment Analysis of Online Papers (SAOOP)

In this section, Sentiment analysis of online papers "SAOOP" will be presented. SAOOP is used in opinion mining [27] and based on a new English lexical dictionary [28]. This lexical dictionary groups adjectives, nouns, verbs, adverbs, adjectives, prefixes, suffixes and other grammatical classes into synonym. The proposed technique is an enhancement on Bag-Of-Words (BOW) model [29] in sentiment analysis to achieve high accuracy, which depends on word weight replacing term frequency of each word. The proposed technique solves two important Bag-of-words weaknesses.

The standard bag of words is not automatic in classification and creating polarity lexicons because BOW model needs to create manual lists of 'positive' and 'negative' words [30]. That means the review judgment is based on the probability of positive or negative words. The second is low accuracy because the standard BOW model neglects text grammatically. Sentiment classification levels will be divided into five classes (very positive, positive, negative, very negative and Neutral).

The proposed technique makes the sentiment classification levels are more detailed and easy by word percentage of each class. The goal of SAOOP is for inferring the polarity of common meaning and polarity concepts from natural language text at a word level, rather than at the syntactic level. SAOOP also classifies reviews into some categorizations based on papers parameters. In addition, the estimation rank of each paper based on evaluation some parameters.

A. SAOOP Overview

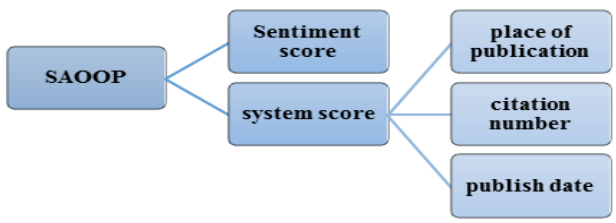


Fig. 1. SAOOP Overview

"Fig.1" shows that SAOOP model consists of two components sentiment score and system score. SAOOP can evaluate any paper based on the components. Sentiment score depends on total reviews evaluation score. And system score which depends on the sum of total scores of three parameters of paper (place of publication), citation number of paper and paper publishing date. SAOOP technique helps researchers to select the suitable paper with the total paper score.

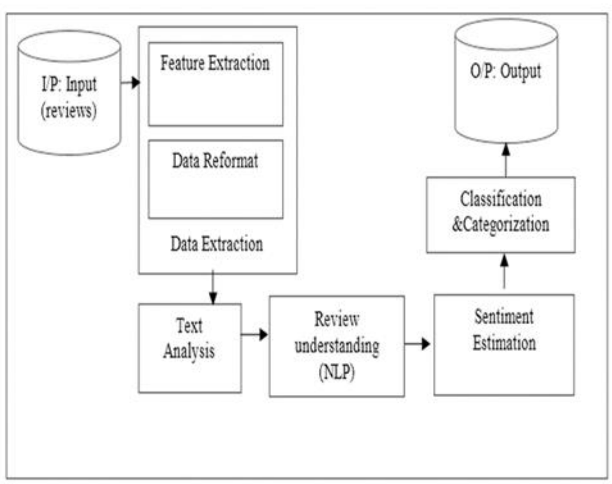


Fig. 2. SAOOP Technique overview

"Fig.2" declares SAOOP Technique overview. The input is scientific paper website link. In data extraction [31] level two parts: first, using Easy web extract tool which is web scraping tool to extract data of paper from scientific papers website online. Part two is data reformat from Excel sheet which is one output of EasWebExtract tool [32] suitable with SAOOP database format. In text analysis level, SAOOP applies some functions of text analysis on reviews of each paper. In the first, applying the splitting sentences function, tokenizing words function, and checking of stop list and removing them [33].

In review understanding (NLP) level, the proposed technique understands the sentences meaning and check words in vocabulary lexicon with similarity and differences algorithms. In estimation phase, showing the evaluation sentiment score for each word into text review and the polarity detection for each one and each sentence and calculate the total score of sentiment review score. In classification phase, that's splitting into two parts, first the reviews classification into five sentiment classification levels (very positive, positive, negative, very negative and objective (neutral), also having degrees of each sentiment level with scale from [-1, 0, 1]. There is also another classification which declares each review categorization based on five meaning classes (topic, date, author, citation, and place of publication). The benefit from the extracted data to memorize them and make relationships between evaluated papers and reviews and categorize reviews logically based on topic domain parameters. Output is the sentiment evaluation score of all reviews with all papers with caring of number of reviews parameter, and evaluation of scientific paper parameters score which is based on metadata of each paper (place of publication, publishing date, and number of citation). So the consequent result is ranking to each paper with the total score of sentiment and system scores with graphical reports of results.

B. SAOOP Methodology

SAOOP can assign polarity based on this approach, considering the words weight replacing term frequency, by assuming each word has two values and polarity with this assumption equation,

$$V(w) = \sum(W(p) + W(n)) = 1. \qquad (1)$$

V (w) is value of word, W (p) refers to positive value and W (n) refers to negative word, the selection between positive or negative polarity Influenced by the meaning of words and each other polarity. But the sentence contains negative that differs in the word value. If the word is positive, convert to negative polarity and the negative score will be as in the equation,

$$V\ (w)\ = W(p) - 0.2. \qquad (2)$$

And if the word is negative, the score will be calculated by V (w) =W(n) + 0.2. The selection of 0.2 because this disison is suitable for the five sentiment class's levels [18]. The proposed technique also creates papers ranks with calculating sentiment and measuring domain parameters. By assuming,

$$\mathrm{P(TS)} = \sum_{\mathrm{R=0}}^{\mathrm{n}} (\mathrm{T(SA)} + \mathrm{T(SS)}). \qquad (3)$$

In the equation, P (TS) refers to a total score of each paper, T (SA): is a total score of sentiment score of all reviews on each paper with caring of number of positive reviews. In the next equation,

$$(SA) = \sum_{i=1}^{n} \frac{P(SA(R))}{n}. \qquad (4)$$

The calculation of the total score of all reviews depends on the score of each review. There is a difficult problem between large number of reviews and evaluating sentiment polarity of each one, this problem is improper the most review number having assessment higher score. For example, one paper publishing in 2013 that's mean from 2 years and this paper has twenty reviews, not equal evaluation one paper publishing in 2005, that's mean from 10 years and the second paper has twenty reviews. The first one is the top rated because the evaluation number of reviews in short time. In other example, one paper publishing from 2 years and having twenty negative reviews, not equal evaluation other one publishing from 10 years and having positive twenty reviews. The second one has maximum rated because the evaluation numbers of positive reviews is larger than the one, although the second is the oldest. As mentioned before double trouble with reviews number and the relationship between date and other relation between sentiment polarity of reviews and number of reviews. That interprets difficulty of evaluation domain parameters.

The proposed technique faces these challenges and evaluates the percentage of positive reviews over total scores. But still there is a problem in relationship between date and number of reviews, for example: one paper publishing from 2 years which has twenty positive reviews, not equal evaluation other one publishing from 10 years which has positive twenty reviews. Actually that is not equal their selves because the recent has bigger reviews number. So SAOOP presents a solution for date relation with reviews number, according with two parameters number of positive reviews and the recent paper. T (SS): is a total score of system score parameters that are evaluated logically of paper parameters according to this equation,

$$V(SS) = \sum\left(\frac{S(pp)}{\lambda} + \frac{S(C)}{2\lambda} + \frac{S(D)}{2\lambda}\right). \quad (5)$$

V (SS) expresses the value of systems score. S (PP) means the score of publication place, S(C) refers to the score of paper citation number, and S (D) means the score of paper publish date. Assuming λ is a constant equal 2, dividing into λ and 2λ to determine the priority of evaluation of the parameter. The evaluation topic parameters process does not ease because of depending on the logical meaning of each one. So the research focuses on scientific papers domain to put the foundation of evaluation parameters to achieve the fact value of each paper to support researcher with sentiment analysis by ranking papers based on total score of them. There is inverse relationship between publishing date and number of citation of the paper, which declare in this equation,

$$S(C) = \frac{current\ year - publish\ date\ year}{number\ of\ Citation}. \quad (6)$$

The result is not true the highest citation number having the highest evaluation score of it. For example, one paper publishing in 2013 that's mean from 2 years which has ten citations, not equal evaluation one paper publishing in 2005, that's mean from 10 years which has ten citations. The first one is the highest score because number of citations in shortly is high, this first paper will be predicated if the paper has the same time 10 years, it mostly has 50 reviews not 10 reviews such as the second paper. In other words, the first paper has 5 papers into each year but the second has 1 into each year. To evaluate score of publishing place conference which depends on ACM conferences tiers with a sample into computer science conferences, such as "VLDB: Very Large Data Bases is in the top tier: tier 1", "ER: Intl Conf. on Conceptual Modeling (Conf. on the entity Relationship Approach)" is in next tier which is in lower tier: Tier 2, and "IDEAS: Intl Database Engineering and Application Symposium" is in a lower tier: Tier 3" [34].

C. SAOOP & Sentiment Challenges

SAOOP enables to make solutions to most significance sentiment analysis challenges [35]. The proposed technique can produce some solutions for main challenges to reach to higher accuracy. The discussion of the solutions in the following:

1) Topic domain independence

Domain-dependent [36] is a difficult challenge to recognize topic nature. There are some words have many meanings and different sentiment values relevant to the topic. There is also a problem shows in extracting keyword or features and how to evaluate words based on each topic. One feature set may give very good performance in one domain, at the same time it performs very poor in some other domain. The produced solution suitable with a small scale by applying the proposed technique on one topic domain and examine domain parameters evaluation by categorization reviews because they also give different meaning with the same word. This research presents a technique to recognize topic nature automatically. The proposed technique is based on extracting keywords and relevant features of each topic. In addition, to produce a solution for some words have many meanings and different sentiment values relevant to the topic. The proposed technique is based on Classification review of each domain features and keywords.

For example, "IEEE is [great +] publication for your paper", SAOOP can put IEEE is in a place of publication classification (based on feature name of publication) and the polarity is positive. "The publishing conference is [great+]", this review refers to the place of publication classification (based on keywords) and the polarity refers to positive. In other example, "The paper publishing date is [old-]", this reviews refers date classification (based on date attribute) and "Old" having the negative score. "The author is [old$^-$] in this field", but SAOOP can categorize the last review in author classification that is meaning the author is expert in this field so "Old" will be had positive score.

SAOOP improves the sentiment score to be more accurate and fair. By assuming some words have 0 value because of depending on classifications of each sentence of each review, there are some groups of words having a polarity and score to relate with the detected classification.

2) Negation

Negation is the biggest challenge in sentiment analysis [37]. The new technique produces a solution to improve evaluation negative with the enhanced bag of words technique. This research handles the two techniques: explicitly and implicitly negative [38]. First: explicitly is deliberately formed and are easy to self-report and by keywords. Second implicitly [5] is the unconscious level, are involuntarily formed and are typically unknown to us without any keywords of negative. In addition, the handling the negative meaning of some conjunctions such as "not only", and "But". The dual negative is the most important case which cares to achieve the total sentiment polarity. Reverses polarity of mid-level terms: great V.S not great.

A method often followed in handling negation explicitly in sentences like:

"I do [not like$^+$] $^-$ the paper", is to detect the negative polarity because the word (not) and convert the sentence operator to negative. But this does not work for "I do [not like^{+}] $^{-}$ this research but I [like^{+}] the field". But still there can be problems.

Other example, "I find the functionality of this new methodology [less $^{-}$] practical", this review refers to explicit comparative negative. "This algorithm is [not great^{+}]$^{-}$]", the proposed technique handles in this review the positive and negative evaluation which declares in [not great! = bad] but [not great = good]. Implicitly negative such as "This research is [very [complex $^{-}$] $^{-}$]" this example does not have any negative keyword, but the meaning has negative and the polarity will be negative of this sentence.

There are sentences having keywords of negation and they don't have the negative polarity such as "[Not only^{+}] I [like^{+}] this algorithm, but also [easy^{+}] to understand and apply." the polarity is not reversed after "not" due to the presence of "only". So this type of combinations of "not" with other words like "only" has to be kept in mind while designing the algorithm.

There is a difference between "not only" and not because not only strengths the meaning (more positive or less negative) based on the polarity of the sentence. In this example other case of implicit negative, I [wish $^{-}$] to work [harder $^{-}$]". In the last review, the new technique presents future words e.g. wish refers to the negative polarity but first must check the polarity of the next sentence polarity because maybe changed the polarity depends on meaning.

3) Creation lexicon

The proposed SAOOP yields an improvement over prior published bag of words built lexicons. This technique also provides an improvement in calculation technique used in reviews sentiment analysis. SAOOP technique presents a solution to take care of grammar (which is one of limitation of Bag-Of-Words) and to save time took is N-gram algorithm to create subsequences of terms. There are two phases that will be produced:

- Phase 1. Data Preparation Phase

Less number of words in vocabulary lexicon to fast search based on similarity and differences algorithms. SAOOP neglects verbs tenses or word formula (singular or plural), that's meaning neglecting English grammar and syntax because of the comparison and differentiation with the infinitive verbs, and singular words with most letters similarity.

- Phase 2. Lexicon Development Phase

Evaluation words /terms: is based on enhanced bag of words: the proposed technique doesnot depend on term frequency. This phase is based on assuming each word has two values and the total of them equal 1. Each term has 2 polarities (+/-).

Negative Algorithm

1. **For each review R in paper P sets**
2. **For each sentence Sent in Review R**
3. **Apply Pre-Processing: Remove the stop words**
4. **Convert all words to Upper case**
5. **Check on expressions have "No or Not" e.g Not Only**
6. **Check on first Negation keywords list, which effects on the polarity of the words e.g "Not" I don't like this paper.**
7. **By assuming, the negative value for positive word ,**
   $$V(w) = W(p) - 0.2$$
8. **And assume the positive value for the negative word,**
   $$V(w)=W(N) + 0.2$$
9. **Check on the next word after negative e.g "like" has positive value and polarity but here it will take negative polarity and value.**
10. **Detect the polarity and value.**
11. **Check on the second list of negation keywords, which effects on the polarity of sentence e.g. never, yet, neither.**
12. **Convert polarity of the sentence by multiplication with(-1) ,** $V(Sent) = S(Sent) * -1$
13. **Check on future words e.g "wish/hope".**
14. **Check on the next sentence polarity.**
15. **End for**
16. **Detect sentence value and polarity.**
17. **End For**
18. **calculate review value and polarity**

(Note: knowing our attention of review classification.)

4) World knowledge requirement

SAOOP technique produces a solution for Knowledge about worlds' facts, events, people are often required to correctly classify the text. Trying to achieve higher accuracy and get the evaluation for some neutral reviews. The World knowledge challenge solution is based on the hierarchical database of nouns. Semantic (hierarchal) relationships between nouns to achieve the polarity, score and meaning. Also to differ between them and keywords or features. Consider the following example, "the author is a [lion^{-}] in this field", the previous review present negative polarity because lion is a name of animal but in real evaluation in the review refers to a positive polarity. In the next review, "Bing is really [Einstein?]" evaluation sentiment analysis without world knowledge classifies above sentence as neutral, but this review is an objective sentence because Einstein is the name of the famous scientist, so it refers a positive polarity also. This review is very hard for software to understand that automatically. SAOOP creates a huge lexicon database to contain the world knowledge especially related to researchers and the most common in the reviews. The solution of world knowledge also assumes values of the words based on the most common meaning. The evaluation of these world knowledge depends on keywords and classification of reviews.

5) Spam and Fake Reviews:

The WWW contains both realistic and spam contents. For effective Sentiment classification, this spam content should be eliminated before processing.

SAOOP can be done by empty or identifying duplicates, by detecting outliers and by considering the reviewer reputation. The proposed Technique enhances reviews spam and fake. SAOOP technique can avoid and cure the most of them by:

- Remove empty reviews: To calculate the real number of reviews.
- Delete duplicate reviews by considering the same reviewer: To Calculate the real sentiment score of the paper.

For example, one paper has 10 reviews, 3 of them for the same text review and with the same user, and 2 is empty reviews , in most sentiment application, if having 10 reviews number and the same repeated reviews will calculate together, the sentiment score is not real because having fake reviews and the results became fake also. And also there are some reviews are general are not related to the paper actually. SAOOP can produce solution for the case study on citeulike.com website, through making quaternary relationship between a set of paper parameters "paper name", "author names", "review" and "Username" (who is a review writer) with taking into consideration review written time, if the review is repeated by the same review writer with ensuring if the review is fake by all parameters and time, the proposed technique will delete the spam review before calculating the sentiment analysis. SAOOP can also deal with fake reviews if it empty and deleted.

In this paper, showing the implementation of SAOOP technique using C# programming language working on Microsoft visual studio 2010 platform. The newly created lexicon is based on SQL Server Management Studio 2008.

IV. EXPERIMENT

In this section, the discussion of the comparison between the proposed technique and two sentiment analysis techniques. This comparison shows the accuracy and performance results based on two datasets. This comparison also compares with the effects and solutions of sentiment analysis challenges.

A. Datasets

The comparison uses two different datasets: 1) real data set: which splits into two data sets with training set (1000 text reviews) and test set (5000 text reviews), 2) verified data set: which is a real set with unknown evaluation around10.000 text reviews (including more than 5.000 positive words, 5.000 negative words).

1) Real dataset

The first sample set is a sample of WWW.citeulike.com papers reviews and Metadata posted by computer science papers branch [39, 34]. The comparison in real data set in computer science scope including two parts: training data and test data [40]. Training data is a set of data to evaluate sentiment around 1000 reviews, knowing the values before. The second part is a test data: which is a set of data to evaluate sentiment with hide class label around 5000 text reviews. Citeulike receives in excess of 200,000 distinct visits (defined by Google Analytics as a group of page views by a unique user with timeout after 30 minutes inactive) monthly, with each visit originating an average of 2.77 page views [41]. Of that 200,000 around distinct users who have previously visited the site on multiple occasions.

There are currently 505,402 items posted in the database (counting n people post the same article); 1,676,130 tags (counting n if there are 'n' tags applied to an article); and 130,548 distinct words used these numbers are growing exponentially. This sample set allows us to study the responses to noticeable past texts. In addition, to evaluate the improved levels of techniques, methodologies in sentiment analysis. SAOOP can handle ten cases to ease to understand text review accurately by CiteULike users they illustrated in table 1. SAOOP can care and evaluate of some English grammar to improve BOW model.

2) Verified dataset

The second dataset which is called verified data set is a real data set but they can't be known the evaluation before. The dataset has around 10.000 text reviews in this sample. This data set is splitting into two parts of verified data reviews as positive and negative. These datasets include a wide range of online papers texts reviews: general reviews. In Table 2, the sample reviews of online scientific papers. SAOOP technique can evaluate sentiment score with the relationship of reviews categorization. With applying on this human-verified sample set [29], by fitting to quantify the range with different sentiment analysis techniques can accurately evaluate polarity of text reviews.

TABLE I. TABLE ENGLISH LANAUGE COVERAGE HANDLING BY SAOOP

Cases	**Definition & Examples**
1. Expressions	Based on syntax (e.g., Not Only, No one.)
2.Topic objects[3]	Features (e.g., lot of contributions)
3.Negation	Implicit (e.g., Independent)) and explicit (e.g. not bad, does not very good)meaning
4.Suffixes &prefixes	The beginning or end letters of word to have different meaning (e.g., dislike, opposed to, useless)
5.Verbs	Converting verbs tenses into infinitive
6.Adjective& Adverb	e.g., Well, improved, highly
7.Nouns	e.g., algorithms, improving, enhancing
8.Comparative [4] comparisons	e.g., easier convert to➔ easy. ("More"; "higher") and ("most", "highest").
9. Phrases	e.g., very good, the professional work
10. Some special (Need, Wish)	(e.g., hope, wish): in the most times, they have negative polarity.

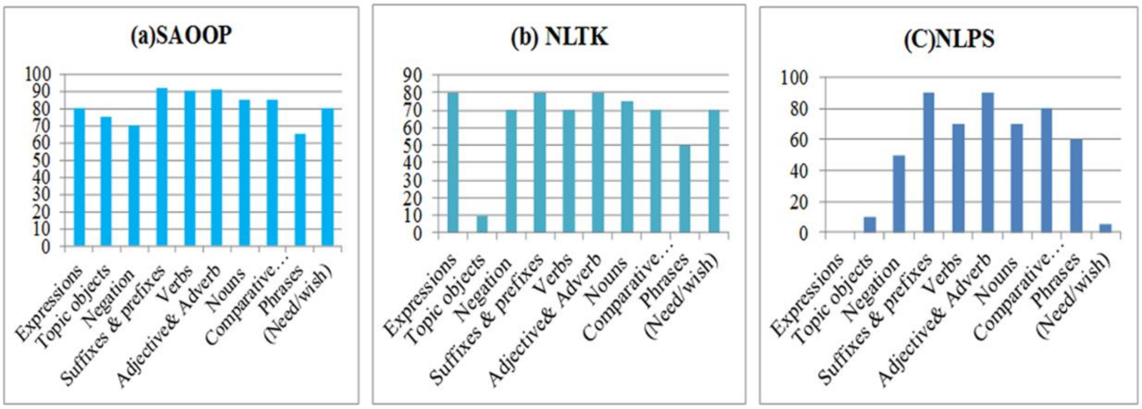


Fig. 3. Coverage Rate of ten cases understanding cases with the three techniques

TABLE II. SAMPLE OF REVIEWS

Sample of reviews
This paper is very well.
It's not great
The best web point
I am interesting in this field
Extremely good
It's not only hot research area but also having new scientific contributions.
This point research is more affected in web mining than using in neural network.
high accuracy
It's not have good value enough
Citation is valuable

B. Comparsion Measures

In order to define the evaluation of accuracy and performance of the three techniques, which will consider in the following table.3:

TABLE III. MEASUREMENT TABLE

		Actual observation Positive	Negative
Predicted	Positive	x	y
expectation	Negative	z	w

Let present True positive (x) was defined when a text was correctly classified as positive, False Positive (y) is a negative text which was classified as positive, False Negative (z) is a positive text but was classified as negative, and the last one True Negative (w) is a correctly classified as negative [42]. In order to compare and evaluate the techniques, by considering the following metrics, commonly used in information retrieval: true positive rate or recall: $R = x/(x + z)$, false positive rate or precision: $P = x/(x + y)$, accuracy: $A = (x + w)/(x + y + z + w)$, and F-measure (performance): $F = 2 \cdot (P \cdot R)/(P + R)$. In many cases simply use the F-measure, as it is a measure of a test's accuracy and relies on both the precision and recall [10]. By reporting, all the measurement mentioned above by practical interpretation. The true positive rate or recall can be understood as the rate at which positive reviews are predicted to be positive (R), whereas the true negative rate is the rate at which negative reviews are predicted to be negative.

The accuracy represents the rate at which the method predicts results correctly (A). The precision also called the positive predictive rate, calculates how close the measured values are to each other (P). The comparison also provides the F-measure results, since it is a standard way of summarizing precision and recall (F). Ideally, a polarity identification method reaches the maximum value of the F- measure, which is 1, meaning that its polarity classification is perfect. The y-axis is a percentage of the understanding sentence rate.

V. COMPARISON RESULTS

In order to facilitate understanding the advantages, disadvantages, and limitations of the various sentiment analysis techniques [43]. This section also presents the comparison results among them.

Understanding of word coverage: in the beginning, the comparison of the coverage of English grammar cases across the representative scientific reviews from CiteULike website. Then examination the intersection of the covered reviews cases across the techniques were in table 1. "Fig. 3 (a)" shows the result for the proposed technique SAOOP, which explain in section 4. "Fig. 3 (b)" declares the NLTK technique. NLTK which is a teaching tool works in, computational linguistics using Python [44]. And "Fig.3 (c)" shows NLP technique. NLPS technique which is predicting the sentiment of reviews based on a recursive model.

As shown in the figure, SAOOP has the highest understanding sentence coverage with 82.5 % with two data sets with three data sets samples, respectively, followed by NLPS which can't evaluate the total sentiment score but with detecting word by word polarity its percentage is 72%.

NLTK can interpret less than 10% of all relevant reviews. In addition, we compare with the percentage of handling sentiment analysis challenges to high accuracy and performance of sentiment analysis of the three techniques of the text reviews depicted in "Fig. 3".

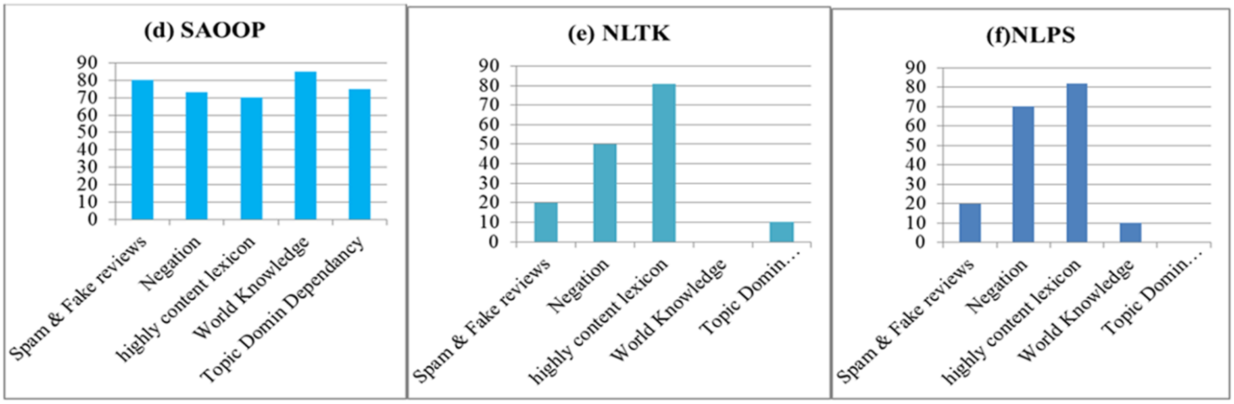


Fig. 4. Perecentage of handling sentiment analysis with the three techniques

According to “Fig.4 (d)” in fact, SAOOP had a new solution for some sentiment challenges but NLPS and NLTK, they and can’t produce methodology to solve them expect some cases in negation but they have many logical errors, that shown by “Fig.4 (E) and (F)”. The analysis results in table 3, refers to the: Percentage of accuracies between techniques based on different data set size. Also we examine the average result analysis of the two big data set that spirited into three data sets, that illustrate the highest average results with sentiment score of the proposed SAOOP technique then NLPS and the lowest one is a NLTK Technique. Finally, the summarization the results with the average of the three data sets (real and verified sets), we find the average of sentiment score of the proposed technique improve the results. Because of working binary analysis solutions of some important challenges and evaluate some technical cases in the text which have a problem in evaluation to be more accurate. In next section, we discuss the accuracy results of the comparison.

a) Accuracy: With the examination of the percentage degree of different techniques accuracy on text reviews content. In order to compute the accuracy of each technique, by calculating the intersections of the positive or negative proportion given by each technique. Table.4 presents the percentage of accuracy for the three compared techniques. For each technique in the first column, showing the estimation from the two data sets of reviews. Finding that some techniques have a high coefficient as in the case of SAOOP (82.5%), while others have least overlap such as NLTK (62%) and NLPS (70.2%).

The last “column” of the table shows on average to what extent each technique agrees with the other two samples. The last “row” quantifies how other methods agree with a certain technique, on average.

With the results of table 4, they illustrate differences between accuracy and performance of the three techniques. Table 4 shows techniques recall, precision, accuracy and performance.

“Fig.5” is shown the accuracy results of them. In a summary, the result indicates that existing tools vary widely in terms of accuracy about sentiment score, with scores ranging from 60% to 80%.

TABLE IV. AVERAGE RESULTS FOR ALL DATASETS

Metric	SAOOP	NLTK	NLPS
Recall	0.856	0.571	0.253
Precision	0.867	0.845	0.846
Accuracy	0.817	0.629	0.715
F-measure	0.846	0.665	0.729

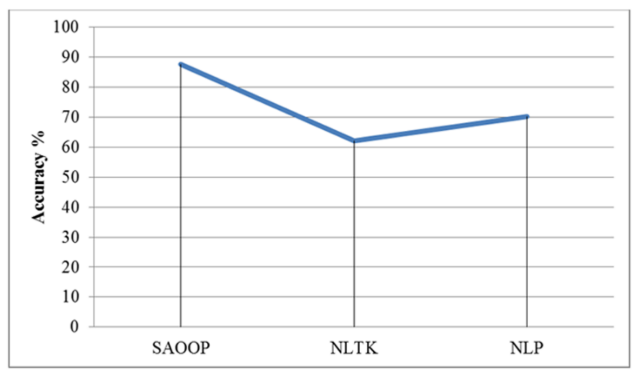


Fig. 5. Differences between Accuracies of three techniques

TABLE V. PRECENTAGE OF ACCURACY BETWEEN TECHNIQUES

Dataset	SAOOP	NLTK	NLPS	Average
Training set 1.000	83.5%	62%	72%	72%
Test set 5.000	81.99%	61%	70%	70.99%
Teal set 10.000	82.5%	60%	71.56%	71.186%
Average	82.5%	61.514%	71.604%	-

b) Perfromance: In this section, showing an evaluation of the performance of the three compared techniques. For comparing the performance results, Table.5 which gives the average of the results obtained for all datasets. For the F-measure, a score of 1 is ideal and 0 is the worst possible.The technique with the highest F-measure was faced sentiment analysis challenges and cover ten cases of each text review (0.846), which had the highest sentiment accurate and understanding text coverage. The second rated technique in the understanding of F-measure is NLPS, which obtained a much higher coverage than understanding and challenges. It is important to note this problem that it can't be interpreted into of total score of the text review. For observation better performance on data sets that contain more expressed sentiment, such as text reviews (e.g., papers online) and the lowest performance is NLTK technique.

VI. Conclusion

Sentiment analysis is the most important source in decision making. Almost people becomes depends on it to achieve the efficient product. Thousands of researchers rapidly year by year that focuses on scientific online reviews for papers to help them. So the researchers introduce a new sentiment technique. In this paper, the researchers create a new technique is called sentiment analysis of online papers "SAOOP". The proposed technique will be a suitable and efficient solution to analyze online reviews. The target of technique to improve accuracy and achieve to accurate review meaning. The proposed SAOOP approach is based on two methods: evaluation and analysis reviews (sentiment analysis) and solve some sentiment analysis challenges. In order to serve researchers in selecting efficient papers. In addition, it evaluates topic domain parameters of scientific papers (place of publication, publishing date, and a number of citation paper) to evaluate the total score of papers. To evaluate SAOOP efficiency, making a comparison between it and two famous techniques. The results have a comparison between the accuracy and performance between the three techniques when the researchers apply the techniques on three data sets (training, test and verified). The comparison results illustrate how proposed technique can increase accuracy and performance with facing many language coverage cases and solving some sentiment analysis challenges. The accuracy results show in NLTK (62%) and NLPS (70%) to 82% (SAOOP) with the proposed technique.

References

[1] Suman, D.R, Wenjun, Z., Social Multimedia Signals: A Signal Processing Approach to Social Network Phenonmena, ISBN-13: 978-3319091167, Springer International Publishing Switzerland, 2015.

[2] Larsen, Peder Olesen, and Markus von Ins. "The Rate of Growth in Scientific Publication and the Decline in Coverage Provided by Science Citation Index."Scientometrics 84.3 (2010): 575–603. PMC. Web. 25 Sept. 2015.

[3] Peng, L., Cui, G., Zhuang, M., & Li, C. (2014). What do seller manipulations of online product reviews mean to consumers? (HKIBS Working Paper Series 070-1314). Hong Kong: Hong Kong Institute of Business Studies, Lingnan University.

[4] Thomas, B., Keep Social Honest , "What Consumers Think about brands on social media, and what bunesses need to do about it" Report, 2013.

[5] Namita, M., Basant, A., Garvit, C., Nitin, B., & Prateek, P., "Sentiment analysis of Hindi Review based on Negation and Discourse Relation", International Joint Conference on Natural Language Processing, Nagoya, Japan, 2013.

[6] Theresa,W. ,Janyce, W. ,& Paul, H., "Recognizing Contextual Polarity in Phrase-Level Sentiment Analysis", proceeding HLT'05 proceedings of the conference of Human Language Technology and Empirical Methods in Natural Language Processing, 2006.

[7] Ian, H.W., Eibe, F., & Mark A. H., Data Mining: Practical machine learning tools and techniques. The Morgan Kaufmann series in data management systems, 3rd Edition, Morgan Kaufmann Publishers is an imprint of Elsevier, 2011.

[8] Yin, Z., Rong, J., & Zhi-Hua, Z., "Understanding Bag-of-Words Model: A Statistical Framework", International Journal of Machine Learning and Cybernetics, 2010.

[9] Diana, M., & John.C.,"Disambiguating Nouns, verbs, and adjectives using automatically acquired Selectional preferences", Association for Computational Linguistics , Vol. 29, 2003.

[10] Presutti, V., Stankovic, M., Cambria, E., Cantador, I., Di Iorio, A., Di Noia, T., Lange, C., Reforgiato Recupero, D., Tordai, A., "Semantic web evaluation challenge. 1st Edition, Series title: Communications in Computer and Information Science, Springer International Publishing, 2014.

[11] Bing, L., "Sentiment Analysis and Subjectivity". In Nitin, I. & Fred, J. (eds). Handbook of Natural Language Processing. 2nd Ed, Machine Learning & pattern recognition series, Chapman& Hall/CRC, 2010.

[12] Samih,Y., Erdogan,Y.,& Halife, K., "Tagging Accuracy Analysis on Part-of-Speech Taggers", Journal of Computer and Communications, 2014.

[13] Mitchell, P.M., Mary A.M., and Beatrice, S., "Building a Large Annotated Corpus of English: The Penn Treebank", Computational Linguistics Journal , Voul. 19, Number 21993.

[14] Saifee, V., & Jay, T., "Applications and Challenges for Sentiment Analysis: A Survey", International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue2, 2013.

[15] Hassena, R.P., "Opinion Mining and Sentiment Analysis Challenges and Applications", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 5, 2014.

[16] Bing, L., Sentiment Analysis and Opinion Mining. Morgan & Claypool Publishers, 2012.

[17] Archana, S., "Sentiment analysis of document based on annotation", CORR Journal, Vol. abs/1111.1648, 2011.

[18] Walter, K., & Mihaela, V., "Sentiment analysis for hotel reviews", proceedings of the computational linguistics-applications, Jacharanka Conference, 2011.

[19] A.Tamilsevi, & M.Parveen, T., "Sentiment analysis of micro blogs using opinion mining classification algorithm", International Journal of Science and Research (IJSR), Vol. 2 Issue 10, 2013.

[20] Nisha.J, & Dr.E. Kirubakaran, "M-Learning sentiment analysis with Data Mining Techniques", International Journal of Computer Science and Telecommunications, Volume 3, Issue 8, 2012.

[21] G¨unes, E., Ahamed, H., Qian, D., & Dragomir, R., "Improved Nearest Neighbor Methods for Text", Technical Report CSE-TR-576-11, University of Michigan, Department of Electrical Engineering and Computer Science, 2011.

[22] Frederick, L., "Implementation of Breiman's Random Forest Machine Learning Algorithm", ECE591Q Machine Learning Journal Paper, 2005.

[23] Christof, M., "Machine learning for query formulation in question and answering", Natural Language Engineering, Cambridge University, 2011.

[24] Steven, B., Ewan, K., and Edward, L., Natural Language Processing with Python, 1st Edition, O'Reilly Media publisher, 2009.

[25] Richard, S., Alex, P., Jean, Y.W., Jason, C., Christopher, D.M., Andrew, Y.N. & Christopher, P., "Recursive Deep Models for Semantic Compositionality Over a Sentiment Treebank", Conference on Empirical Methods in Natural Language Processing, 2013.

[26] I. Hemalatha , Dr. G. P Saradhi V., & Dr. A. Govardhan, "Preprocessing the Informal Text for efficient Sentiment Analysis" , International Journal of Emerging Trends & Technology in Computer Science (IJETTCS),Volume 1, Issue 2, 2012.

[27] Dushyant, B.R., & Samrat, K., "A Review on Emerging Trends of Web Mining and IT's Application", International Journal of Engineering Development and Research | IJEDR, 2013.

[28] Bo, P., & Lillian, L., "Opinion mining and sentiment analysis", Journal Foundations and Trends in Information Retrieval, Vol. 2, 2008.

[29] Bing, L., "Sentiment Analysis: A Multi-Faceted Problem", IEEE Intelligent Systems, 2010.

[30] Hang, C., Vibhu, M., & Mayur, D., “Comparative experiments on sentiment classification for online product reviews”, American Association for Artificial Intelligence (AAAI Conference), 2006.

[31] Mr. Akshay, A. Adsod, & Prof. Nitin R.C., “A review on web mining”, International Journal of Engineering Trends and Technology (IJETT)”, Volume 10 Number 3, 2014.

[32] Alberto, H.F.L., Berthier, A.R-N, Altigran, S. d. S., and Juliana, S. T., “A brief survey of web data extraction tools”, ACM SIGMOD, Vol.31, Issue 2,, New York , USA, June 2002

[33] Farah, B., Carmine, C., & Diego.R., “Sentiment analysis: Adjectives and Adverbs are better than Adjectives Alone”, International Conference on Weblogs and Social Media -ICWSM , Boulder, CO USA, 2007.

[34] Utkarsh, G., Clemente, I., and Mike P. W.,Understanding Factors Inuencing the Citation Count of Networking Conference Papers, in proc. CHI 09 proceedings of the SIGCHI Conference on human factors in computing systems, 2009.

[35] Sujata, R. & Patreek, K., “Challenges of Sentiment Analysis and Existing State of Art”, International Journal of Innovation and Research in Computer Science (IJIRCS), 2014.

[36] Chenghua, L., and Yulan, H., “Joint Sentiment/Topic Model for Sentiment Analysis”, CIKM '09 Proceedings of the 18th ACM conference on Information and knowledge management, Hong Kong, China, ACM 978-1-60558-512-3/09/11, 2009.

[37] Andreas, H., Gerhard, P., and Andreas, N., “A Brief Survey of Text Mining”, LDV Forum - GLDV Journal for Computational Linguistics and Language Technology, 2005.

[38] Bas, H., Paul, v.I., Alexander, H., Flavius, F., & Uzay, K., “Accounting for Negation in sentiment analysis”, DIR, Amsterdam, the Netherlands, 2011.

[39] John, M. B., “Counting publications - Journals vs. Conferences in Computer Science”, in NIK-2013 conference, 2013.

[40] Quoc, L., & Tomas, M., “Distributed Representations of Sentences and Documents”, Proceedings of the 31 st International Conference on Machine Learning, Beijing, China. JMLR: W&CP volume 32, 2014.

[41] Umer, F.,Yang, S., John, M. C., and Lee, G.,“Social Bookmarking for Scholarly Digital Libraries”, Published by the IEEE Computer Society, *Pennsylvania State University,* December 2007.

[42] Pollyanna, G., Matheus, A., Fabrico, B., & Meeyoung, C.,“Comparing and Combining Sentiment Analysis Methods”, ACM Association for Computing Machinery, 2013.

[43] Mark, C., Oliver, D., & Fatih, U., “Potential and Limitations of Commercial Sentiment Detection Tools”, Emotion and Sentiment in Social and Expressive Media-ESSEM, 2013.

[44] Steven, B., Ewan, K., Edward, L., & Jason, B., “Multidisciplinary Instruction with the Natural Language Toolkit”, Proceedings of the Third Workshop on Issues in Teaching Computational Linguistics (TeachCL-08), Columbus, Ohio, USA, 2008.

Towards Agile Implementation of Test Maturity Model Integration (TMMI) Level 2 using Scrum Practices

Ahmed B. Farid
Information Systems Dept, Faculty of Computers and Information, Helwan University, Cairo, Egypt

Enas M. Fathy
Information Systems Dept, Faculty of Computers and Information, Helwan University, Cairo, Egypt

Mahmoud Abd Ellatif
Information Systems Dept, Faculty of Computers and Information, Helwan University, Cairo, Egypt

***Abstract*—The software industry has invested the substantial effort to improve the quality of its products like ISO, CMMI and TMMI. Although applying of TMMI maturity criteria has a positive impact on product quality, test engineering productivity, and cycle-time effort. But it requires heavy software development processes and large investments in terms of cost and time that medium/small companies do not deal with it. At the same time, agile methods deal with changing requirements and continuous delivery of valuable software by short time iterations. So that the aim of this paper is to improve the testing process by applying a detailed mapping between TMMI and Scrum practices and verifying this mapping with a study providing empirical evidence of the obtained results. The research has been evaluated on a sample of 2 large-sized TMMI certified companies. In conclusion, the experimental results show the effectiveness of using this integrated approach compared to other existing approaches.**

Keywords—Agile software development; Scrum; TMMI; Software Testing; CMMI

I. Introduction

As the software industry is evolving rapidly but it still far away from zero defects software, so the software industry focused on developing the development process [1].

“Despite the fact that testing often accounts for at least 30-40% of the total project costs” [1], most of the widely used software industry standards like Capability Maturity Model Integration (CMMI) only give limited attention to the testing process improvement, so that the testing community created a TMMI [1].

“The TMMI is a detailed model for test process improvement and is positioned as being complementary to the CMMI.” [1].

TMMI aims to help software organization to improve the software quality by preventing defects and save time and cost [2].

more and more software organizations moving from the waterfall model to more agile models like Scrum, as the benefits of agility including faster delivery to customer, flexibility with requirement changes and higher software quality [3].

The paper is organized as follows: Section 2 presents the background and related research of agile software development and TMMI. Section 3 describes the research problem. Section 4 and 5 describe the research goals, approach, and assumptions. Section 6 shows the theoretical mapping of the two approaches. Section 7 shows overall results of the theoretical mapping. Section 8 describes the background of the analyzed study. Section 9 summarizes the assessment results from the study. Section 10 the results of this study are discussed. The last section concludes the paper with the key findings, research limitations and future work related to the TMMI and agile integration.

II. Overview

A. TMMI

Capability Maturity Model Integration (CMMI) includes few testing process areas like verification and validation with lack of details so Test Maturity Model Integration (TMMI) has been created to cover most of testing processes [4].

TMMI includes best practices of testing that helps in process improvement and assessment [5].

There are five levels in the TMMI, each level contains a number of process areas, to move to the higher level it should complete all process areas in the lower level [6].

“At TMMI level 2, testing becomes a managed process and is clearly separated from debugging. The main objective of testing in a TMMI level 2 organization is to verify that the product satisfies the specified requirements” [1].

B. Scrum

Scrum is not a defined process or standard it is a framework that enables the organizations to set their own customized processes and techniques for their software development projects [7].

“The main aim of using Scrum is to enable a project team to react quickly, simply and appropriately instead of wasting time and energy creating, implementing and updating outdated plans” [8].

"The Scrum team consists of a Product Owner, Scrum Master, and a Development Team. Scrum teams are self-organizing and cross-functional, they are not directed by others outside the team and have all the competencies to accomplish their work" [9].

There are 3 roles in Scrum process: Scrum Master who audits and monitors the scrum process, Product owner who responsible for product requirements and the team who develop the products [10].

Scrum begins with creating the product backlog that contains customer requirements. Then the team prioritizes the requirements. The iteration is a Sprint that consists of a period of one month's duration. Every sprint starts with sprint planning meeting that clarify the details of tasks and they discuss the tasks and the progress in daily scrum meeting and at the end of each sprint, sprint review meeting is held to evaluate the sprint and check the current status against the sprint goals determined in sprint planning meeting [11].

C. Related work

There have been a number of publications focusing on the relationship between CMMI project management process areas and Scrum practices, showing the gaps and strengths between them [12, 13] but unfortunately their studies did not include an empirical evidences and Others analyze the feasibility of the CMMI process improvement in combination with the agile software development and project management area [14] however this study provide only a theoretical survey at the project management level . Neil Potter and Mary Sakry [15] listed only the main practices of CMMI that map cleanly to Scrum process steps. Few publications intend to increase the understanding of the relationship between Scrum and CMMI reporting empirical results that confirm theoretical comparisons between Scrum practices and CMMI level 2 [16]. Unlike these researches, As known software does not work correctly can lead to many problems, including loss of money, time or business reputation, and could even cause injury or death so this study is concentrated on testing process and presents the details of the mapping between Scrum practices and TMMI, and illustrates this mapping with a study providing empirical evidences of the obtained results which will increase the understanding of the mapping in theoretical and practical study. This research covers Level 2 process areas in TMMI.

III. PROBLEM DEFINITION

Organizations seek to improve testing process by applying new methodologies and models. When talking about TMMI**,** it requires a considerable amount of time and effort for implementation, it may require additional resources and knowledge required in smaller organizations and also requires a major shift in organizational culture and attitude so the number of TMMI certified companies is limited to 23 only all over the world. Trying to merge TMMI with another methodology will be a good choice to avoid those disadvantages. So it is needed to know if using TMMI will be compatible with the Agility concept or not. And if the two approaches are compatible the next step is to identify how the integration will be analyzed between them and how the organizations will apply this mapping perfectly.

IV. RESEARCH APPROACH

The goal of this research was to study how TMMI model could be used in assessing Scrum practices and to help TMMI certified companies to shift toward agility. The approach was developed in Three-phase model. The first phase was to discover an appropriate possible theoretical mapping between TMMI and Scrum practices. The second phase was to verify the applicability of this mapping. An empirical study has been conducted, the mapping was applied to a sample of TMMI certified companies to make sure that merging TMMI, and Scrum processes within those organizations is possible. The Third phase has been conducted in order to measure the effect of this merge.

V. RESEARCH ASSUMPTIONS

- Using TMMI and Scrum practices together will be useful for the organizations to achieve better team productivity.
- TMMI needs a heavy documentation in contradiction with agile software development which focuses on small projects so organizations can reduce this problem and improve their test process areas by applying both of them together.

VI. STUDY PHASE 1: DESIGNING A MAPPING MATRIX BETWEEN TMMI AND SCRUM PRACTICES

After a deep study of TMMI Practices, and scrum recommended practices. A Mapping matrix has been produced to show how scrum practices could be mapped to the TMMI practices.

The tables below show several TMMI practices (using TMMI text taken from the model definition) and how Scrum can implement each practice. To appraise Level 2, it is assumed that the Scrum implementation is robust and shows evidence of the TMMI practice being performed.

For each process area, a mapping between its specific practices and the Scrum practices was carried out. Several considerations were identified in order to establish this mapping, identifying gaps and strengths. After that, a coverage rating for each practice was established considering the following criteria in table I. The data is filled based on conducting interviews, questionnaires and practical work with experts in testing field working in Vodafone Group, ITWORX, HP Enterprise Services and MCS and the results are combined in "Rating" column as Covered, Uncovered or Partially Covered.

TABLE I. CRITERIA FOR SCRUM PRACTICES RATING

Rating		**Criteria**
U	Uncovered	The practice is not covered by Scrum.
P	Partially Covered	The practice is partially covered by Scrum.
C	Covered	The practice is fully covered.

PA 2.1 Test Policy and Strategy

"The purpose of the Test Policy and Strategy (TPS) is to develop and establish a test policy, and an organization-wide or program-wide test strategy in which the test levels are unambiguously defined. To measure test performance, test performance indicators are introduced [1]". The mapping of TPS process area and its related scrum practices is shown in table II.

TABLE II. MAPPING BETWEEN TPS SPECIFIC PRACTICES AND SCRUM PRACTICES

TPS	TMMI Practice	Scrum Practice	Rating
SP 1.1	Define test goals	• Specify the test goals based on business needs, this occurs in release planning meeting and sprint planning meeting.	C
SP 1.2	Define the test policy	• Define test policy in release planning meeting.	C
SP 1.3	Distribute the test policy to stakeholders	• Share the test policy with involved stakeholders in release planning meeting.	C
SP 2.1	Perform a generic product risk assessment	• Create Generic Risk Profiler which highlight commonly identified risks and how to reduce them, this occurs in release planning meeting and sprint planning meeting.	C
SP 2.2	Define test strategy	• Define the test strategy in release planning meeting.	C
SP 2.3	Distribute the test strategy to the stakeholders	• Share the test strategy with involved stakeholders in release planning meeting.	C
SP 3.1	Define test performance indicators	• Define sprint metrics to enhance the predictability for examples: o Measuring progress ▪ Burn down charts. o Defect metrics ▪ Root cause analysis. ▪ Results from defect tracking system. o Traceability metrics ▪ Test coverage (story vs. test cases). ▪ Code coverage.	C
SP 3.2	Deploy test performance indicators	• Discuss the results with involved stakeholders in daily Scrum meeting.	C

PA 2.2 Test Planning

"The purpose of Test Planning (TP) is to define a test approach based on the identified risks and the defined test strategy, and to establish and maintain well-founded plans for performing and managing the testing activities [1]".

The mapping of TP process area and its related scrum practices is shown in table III.

TABLE III. MAPPING BETWEEN TP SPECIFIC PRACTICES AND SCRUM PRACTICES

TP	TMMI Practice	Scrum Practice	Rating
SP 1.1	Define product risk categories and parameters	• Create Product Risk Profiler which addresses the functional and non-functional risks that most concern the involved stakeholders.	C
SP 1.2	Identify product risks	• Identify product risks, assess the associated level of risk, estimate the effort required to reduce those risks sufficiently, and then mitigate those risks through test design, implementation, and execution.	C
SP 1.3	Analyze product risks	• In Release planning: business representatives who know the features in the release provide a high-level overview of the risks, and the whole team, including the tester(s), may assist in the risk identification and assessment. • In Sprint planning: the whole team identifies and assesses the quality risks.	C
SP 2.1	Identify items and features to be tested	• Select, allocate, and prioritize test conditions to maximize effectiveness and efficiency according to product (Quality) risk analysis, this occurs in release planning meeting and sprint planning meeting.	C
SP 2.2	Define the test approach	• Identify the relevant test design techniques, this occurs in release planning meeting and sprint planning meeting.	C
SP 2.3	Define entry criteria	• Identify sprint entry criteria in sprint planning meeting.	C
SP 2.4	Define exit criteria	• Identify sprint exit criteria in sprint planning meeting.	C
SP 2.5	Define suspension and resumption criteria	• Specify suspension and resumption criteria in sprint planning meeting.	C
SP 3.1	Establish a top-level work breakdown structure	• Identify user stories and write them down on the cards at the prepared Sprint Task board.	C
SP 3.2	Define test lifecycle	• Specify test phases in sprint planning meeting.	C

SP 3.3	Determine estimates for test effort and cost	• tester detect how many hours should have to complete testing for each of selected user stories In sprint planning meeting for examples: ○ Using PERT technique. ○ Using User Story points (USP) technique.	C
SP 4.1	Establish the test schedule	• Specify the testing effort based on the user stories sizes in sprint planning meeting. • Specify the testing phases in the sprint planning meeting.	C
SP 4.2	Plan for test staffing	• In sprint planning meeting, the testing team clarifies open questions and for each item the team discusses if they have enough capacity, the required know-how and if everything else needed is available.	C
SP 4.3	Plan stakeholder involvement	• In sprint planning meeting, the testing team discusses if they have the required resources based on the sprint backlog.	C
SP 4.4	Identify test project risks	• In Release planning: business representatives who know the features in the release provide a high-level overview of the risks, and the whole team, including the tester(s), may assist in the risk identification and assessment.	C
SP 4.5	Establish the test plan	• Create test plan by the team based on the sprint planning meeting.	C
SP 5.1	Review test plan	• Review test plan in daily Scrum meeting.	C
SP 5.2	Reconcile work and resource levels	• Review resources allocation in daily Scrum meeting.	C
SP 5.3	Obtain test plan commitments	• After the sprint planning meeting the Scrum master of the team - calls the team to define the details of how the committed items are going to be implemented.	C

PA 2.3 Test Monitoring and Control

"The purpose of Test Monitoring and Control (TMC) is to provide an understanding of test progress and product quality so that appropriate corrective actions can be taken when test progress deviates significantly from plan or product quality deviates significantly from expectations [1]". The mapping of TMC process area and its related scrum practices is shown in table IV.

TABLE IV. MAPPING BETWEEN TMC SPECIFIC PRACTICES AND SCRUM PRACTICES

TMC	TMMI Practice	Scrum Practice	Rating
SP 1.1	Monitor test planning parameters	• Monitor the progress by using specific tools for examples: ○ Sprint Burn down chart. ○ Sprint Task board ○ Progress chart. ○ Release Burn down chart.	C
SP 1.2	Monitor test environment resources provided and used	• This is Scrum master responsibility.	C
SP 1.3	Monitor test commitments	• Monitor the team commitments in Daily Scrum meeting and Sprint review meeting. • Sprint burn down chart that tracks effort remaining. • Release burn down chart that tracks story points that have been completed.	C
SP 1.4	Monitor test project risks	• This is Scrum master responsibility.	C
SP 1.5	Monitor stakeholder involvement	• Monitor stakeholder involvement in: ○ Daily Scrum meeting. ○ Sprint review meeting.	C
SP 1.6	Conduct test progress reviews	• Review the progress in: ○ Daily Scrum meeting. ○ Sprint review meeting.	C
SP 1.7	Conduct test progress milestone reviews	• This occurs in sprint review meeting.	C
SP 2.1	Check against entry criteria	• This occurs in daily Scrum meeting.	C
SP 2.2	Monitor defects	• Discuss defects in daily Scrum meeting. • Defects per iteration metric: ○ This metric is calculated either as a simple count or count weighted by the severity of defects that was introduced during a Sprint.	C
SP 2.3	Monitor product risks	• This occurs in daily Scrum meeting.	C
SP 2.4	Monitor exit criteria	• This occurs in daily Scrum meeting.	C
SP 2.5	Monitor suspension and resumption criteria	• This occurs in daily Scrum meeting.	C

SP 2.6	Conduct product quality reviews	• This occurs in daily Scrum meeting.	C
SP 2.7	Conduct product quality milestone reviews	• This occurs in sprint review meeting.	C
SP 3.1	Analyze issues	• Discuss the defects in daily Scrum meeting • Analyze the appeared defects in the shared test management tool.	C
SP 3.2	Take corrective action	• This occurs in: o Daily Scrum meeting. o Sprint review meeting.	C
SP 3.3	Manage corrective action	• This is Scrum master responsibility.	C

PA 2.4 Test Design and Execution

"The purpose of Test Design and Execution (TDE) is to improve the test process capability during test design and execution by establishing test design specifications, using test design techniques, performing a structured test execution process and managing test incidents to closure [1]". The mapping of TDE process area and its related scrum practices is shown in table V.

TABLE V. MAPPING BETWEEN TDE SPECIFIC PRACTICES AND SCRUM PRACTICES

TDE	TMMI Practice	Scrum Practice	Rating
SP 1.1	Identify and prioritize test conditions.	• Create test conditions and scenarios based on the selected user stories. • Prioritize the test conditions according to the size given to each user story.	C
SP 1.2	Identify and prioritize test cases	• Write the required test cases which needed for each user story. • Sort the test cases according to the importance of each one of them.	C
SP 1.3	Identify necessary specific test data	• Prepare the test data required to fulfill the test cases.	C
SP 1.4	Maintain horizontal traceability with requirements	• Use Traceability metrics to measure test coverage (story vs. test cases).	C
SP 2.1	Develop and prioritize test procedures	• Develop the test procedures and determine if test scripts will be executed automatically or manually.	C
SP 2.2	Create specific test data	• Create the required test data as identified in SP 1.3.	C
SP 2.3	Specify intake test procedure	• Specify the main areas needed to be tested. • Detect the positive paths to decide the start of testing.	C
SP 2.4	Develop test execution schedule	• This occurs in sprint planning meeting.	C
SP 3.1	Perform intake test	• Execute the smoke test to decide if the current build will be tested or rejected.	C
SP 3.2	Execute test cases	• Execute test cases manually or by using automatic test scripts.	C
SP 3.3	Report test incidents	• Record the appeared defects in the shared test management tool. • Discuss the defects in daily Scrum meeting.	C
SP 3.4	Write test log	• Track the test execution in: o Sprint Task board. o Daily Scrum meeting.	C
SP 4.1	Decide disposition of incidents in configuration control board	• This occurs in daily Scrum meeting.	C
SP 4.2	Perform appropriate action to fix the test incidents	• This occurs in daily Scrum meeting.	C
SP 4.3	Track the status of test incidents	• Review the issues in the shared test management tool. • Discuss the issues status in daily Scrum meeting.	C

PA 2.5 Test Environment

"The purpose of Test Environment (TE) is to establish and maintain an adequate environment, including test data, in which it is possible to execute the tests in a manageable and repeatable way [1]".The mapping of TE process area and its related scrum practices is shown in table VI.

TABLE VI. MAPPING BETWEEN TE SPECIFIC PRACTICES AND SCRUM PRACTICES

TE	TMMI Practice	Scrum Practice	Rating
SP 1.1	Elicit test environment needs	• Define requirements for test environment in sprint backlog. • This occurs in sprint planning meeting.	C
SP 1.2	Develop the test environment requirements	• Set requirements for test environment in sprint backlog. • This occurs in sprint planning meeting.	C
SP 1.3	Analyze the test environment requirements	• This occurs in sprint planning meeting.	C

SP 2.1	Implement the test environment	• Implement the test environment as specified and according to the sprint backlog.	C
SP 2.2	Create generic test data	• Create the required test data.	C
SP 2.3	Specify test environment intake test procedure	• Specify environment sanity check to decide if the environment is implemented correctly.	C
SP 2.4	Perform test environment intake test	• Run the environment sanity check.	C
SP 3.1	Perform systems management	• This is operation (support) resources responsibility according to the SLA (service level agreement) identified in the sprint planning meeting.	C
SP 3.2	Perform test data management	• This is the responsibility of the tester with the operation (support) resources identified in sprint planning meeting.	C
SP 3.3	Coordinate the availability and usage of the test environments	• This occurs in sprint planning meeting.	C
SP 3.4	Report and manage test environment incidents.	• Report environment incidents in: ○ Daily Scrum meeting. ○ The shared test management tool.	C

PA 2.6 Configuration Management

"The purpose of Configuration Management (CM) is to establish and maintain the integrity of work products using configuration identification, configuration control, configuration status accounting, and configuration audits [18]". "CM is not specifically called out in Scrum. However, in an agile environment it is pretty easy to add a layer of CM to protect your work. Even for groups that like to use white boards, you can be creative and at least establish some basic protection by labeling items (e.g. "V1.1," or "Story dated 1/2/YY") and taking a photo [15]".

The changes in requirements are managed implicitly in product backlog and sprint backlog [17]. This practice is classified partially covered.

PA 2.7 Process and Product Quality Assurance

"The purpose of Process and Product Quality Assurance (PPQA) is to provide staff and management with objective insight into processes and associated work products [18]". The mapping of PPQA process area and its related scrum practices is shown in table VII.

TABLE VII. MAPPING BETWEEN PPQA SPECIFIC PRACTICES AND SCRUM PRACTICES

PPQA	TMMI Practice	Scrum Practice	Rating
SP 1.1	Objectively Evaluate Processes	• Scrum master periodically checks that the scrum process is being followed. • Evaluate the scrum process in retrospective meeting.	C
SP 1.2	Objectively Evaluate Work Products and Services	• Scrum master periodically checks that the scrum process is being followed. • Evaluate the scrum process in retrospective meeting.	C
SP 2.1	Communicate and Ensure Resolution of Noncompliance Issues	• This is Scrum master responsibility.	C
SP 2.2	Establish Records	• This is Scrum master responsibility.	C

VII. OVERALL RESULTS OF THE MAPPING

General results of the mapping are shown in the *Fig. 1*, a consolidated view of the coverage of TMMI Level 2 Process areas by Scrum practices.

This result shows that most of specific practices of TMMI Level 2 Process areas are Covered and 90% of Configuration management process area is Uncovered. This means that TMMI Level 2 process areas are mostly satisfied for the organizations that need to improve their test processes by applying TMMI within Scrum.

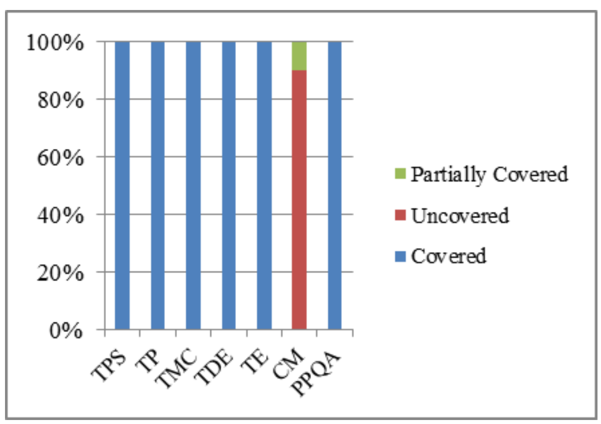


Fig. 1. TMMI Level 2 Process areas covered by Scrum

VIII. Study Phase 2: Empirical Study

Once theoretical comparison between TMMI and Scrum were established, a sample of the certified companies was selected to apply the approach and find the strengths and weakness in using the provided study.

A. *Study description*

The number of TMMI certified companies from level 2 to level 5 is 23 all over the world like Vodafone UK, Tech Mahindra Global Test Factory, Wipro Limited, Virgin Media, etc. A sample of 2 large companies was taken which is 8.7% from the certified companies. Working on 4 projects; the average of testing team members in each project was 6 members. The process used in all the projects was Agile/Scrum. This study was limited to TMMI Level 2 and all the involved teams were less than 10 members.

IX. Study Phase 3: Verifying Applicability of Research Work

The objective of the study was to discuss the effects of testing projects before and after using Agile/Scrum practices inside the TMMI process and to show an empirical evidence of understanding the mapping between TMMI and Scrum practices. Scrum practices widely used as they enhance the testing process in specific KPIs that mentioned in this study. The study was applied on a telecom projects which using Scrum process and the projects' data is extracted from HP ALM test management tool (represented in table VIII). In this project the KPIs are calculated based on the following equations and (P) stands for defect priority and the result is shown in table IX:

Test Case Effectiveness = Number of valid defects mapped to test cases / Total number of valid defects.

Defect Quality = Total number of valid defects / Total number of defects.

Defect Density = Number of valid defects / Total number of executed test cases.

Defect Removal Efficiency = Valid defects / (Valid defects + Valid Production defects).

Total Number of defects = Number of defects created (P1+P2+P3+P4).

Total number of valid defects mapped to test cases = Number of defects created (P1+P2+P3+P4) Mapped to test cases.

Total Number of cancelled defects= Number of defects cancelled (P1+P2+P3+P4).

Total Number of valid defects = Total Number of defects - Total Number of cancelled defects.

TABLE VIII. Calculated Test Execution Factors before and after using Scrum

Test execution factor	Before Scrum	After Scrum				
		Iteration 1	*Iteration 2*	*Iteration 3*	*Iteration 4*	*Iteration Average*
Number of test cases executed	200	100	120	120	100	110
Number of priority 1 defects created (P1)	8	5	7	6	4	5.5
Number of priority 2 defects created (P2)	20	10	12	9	5	9
Number of priority 3 defects created (P3)	25	15	12	10	6	10.75
Number of priority 4 defects created (P4)	19	20	15	17	12	16
Number of defects created P1 Mapped to test cases	3	4	6	5	4	4.75
Number of defects created P2 Mapped to test cases	11	8	10	8	3	7.25
Number of defects created P3 Mapped to test cases	13	12	11	7	6	9
Number of defects created P4 Mapped to test cases	10	16	12	15	11	13.5
Number of defects cancelled P1	3	1	1	2	1	1.25
Number of defects cancelled P2	8	2	1	2	0	1.25
Number of defects cancelled P3	7	3	2	1	0	1.5
Number of defects cancelled P4	4	1	0	1	1	0.75
Valid Production defects	19	5	7	5	4	5.25
Total Number of defects	72	50	46	42	27	41.25
Total Number of valid defects	50	43	42	36	25	36.5
Total number of valid defects mapped to test cases	37	40	39	35	24	34.5
Total Number of cancelled defects	22	7	4	6	2	4.75

TABLE IX. CALCULATED KPIS BEFORE AND AFTER USING SCRUM

KPIs Values	Before Scrum	Iteration 1	Iteration 2	Iteration 3	Iteration 4	Iteration Average
Test Cases effectiveness	51%	80%	85%	83%	89%	84%
Defect Quality	69%	86%	91%	86%	93%	89%
Defect Density	25%	43%	35%	30%	25%	33%
Defect Removal Efficiency	72%	90%	86%	88%	86%	87%

The following figure (*Fig. 2*) displays the percentages of test cases effectiveness before and after using Scrum and it illustrates that the study helped in enhancing this KPI by [100*(84-51)] /51= 64.71%.

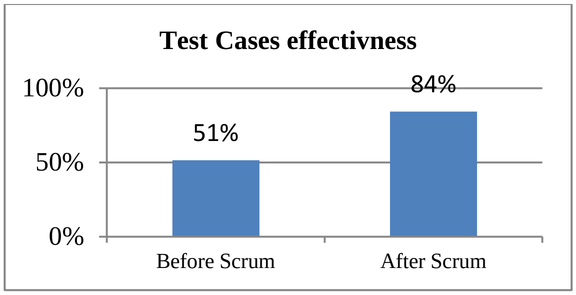


Fig. 2. A summary of test Case effectiveness after using Scrum

The following figure (*Fig.3*) displays the percentages of defect quality before and after using Scrum and it illustrates that the study helped in enhancing this KPI by [100*(89-69)] /69= 28.99%.

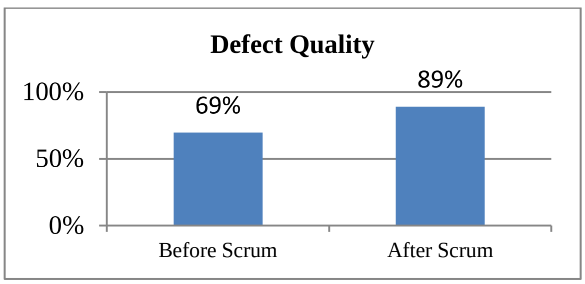


Fig. 3. A summary of Defect Quality after using Scrum

The following figure (*Fig. 4*) displays the percentages of defect density before and after using Scrum and it illustrates that the study helped in enhancing this KPI by [100*(33-25)] /25= 32%.

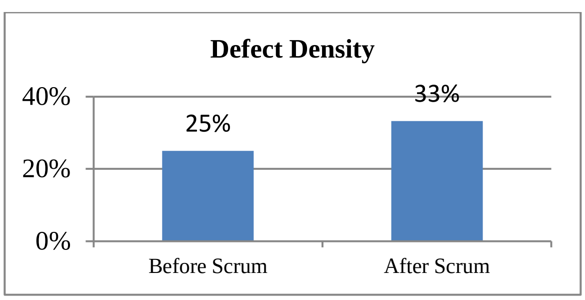


Fig. 4. A summary of Defect Density after using Scrum

The following figure (*Fig. 5*) displays the percentages of defect removal efficiency before and after using Scrum and it illustrates that the study helped in enhancing this KPI by [100*(87-72)] /72= 20.83%.

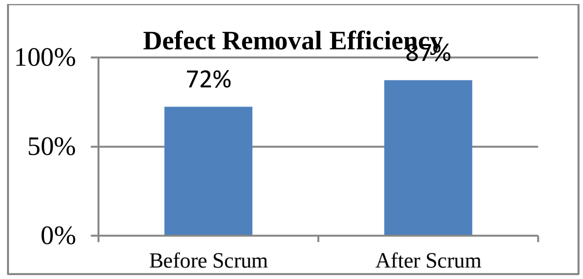


Fig. 5. A summary of Defect Removal Efficiency after using Scrum

The following questionnaire is distributed among testing experts to display their opinions about how was the communication between involved stakeholders in the projects using legacy and others using Scrum practices. The result of this survey is shown in table x and the summary is represented in *Fig. 6*.

TABLE X. TESTING KPIS BEFORE / AFTER USING SCRUM

KPI	Before Scrum	After Scrum
Quality Delivered to Customers (k1)	75%	95%
Team Enthusiasm (k2)	70%	80%
Retrospective Process Improvement (k3)	40%	80%
Communication among stakeholders (k4)	50%	90%
Customer Satisfaction (k5)	60%	85%
Employee Satisfaction (k6)	70%	80%
Meet the project deadlines (k7)	70%	95%

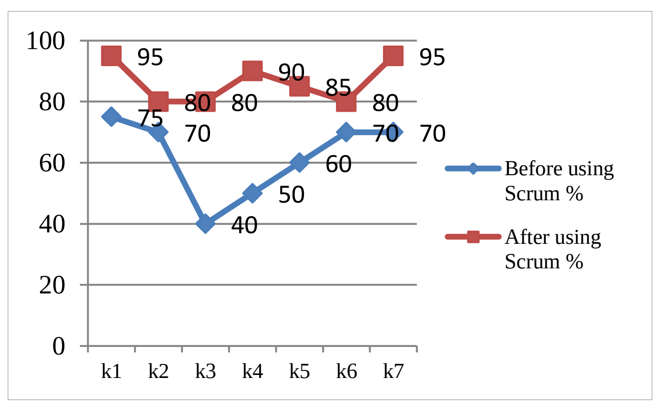


Fig. 6. A summary of testing KPIs before / after using Scrum

X. DISCUSSION

From the previous study the results show that using the mapping helped in enhancing and improving test cases effectiveness to reach 89% in some iteration and also defects quality was increased to reach 93% in some iteration.

The research helped the companies to make improvements in the quality delivered to the customers as project requirements were discussed and refined during sprint planning and daily scrum meetings. It helped in increasing the customer and employee satisfaction. Also applying the research helped the companies in the following achievements:

- Business assurance - consistent delivery adherence and test effectiveness exceeding customer targets and improved business assurance.
- Step change in cost - significant reduction in test costs given to the client.
- Tester error is reduced from iteration to iteration based on root cause analysis of defects.
- Small iterations helped in identifying issues early and made it easier to respond to change.

XI. Conclusion and Future Work

The goal of this paper was to improve testing process by comparing Scrum practices with TMMI Level 2 process areas, showing the major strengths and gaps between them and identifying how organization are adopting complementary practices in their projects to make these two approaches more compliant.

The study results showed that most of the specific practices of TMMI Level 2 Process areas are covered and 90% of configuration management process area is uncovered and also the organizations that their process based on TMMI model can be improved by adding some Scrum practices.

In the light of that, it is suggested as future works: The field of software engineering is changing very quickly so more studies will help the companies to find a detailed reference containing the best practices regarding TMMI maturity levels and another point to map the TMMI with other agile methods for example XP, FDD, and DSDM.

Refrences

[1] Erik van Veenendaal, “Test Maturity Model Integration (TMMI)”, release 0.1, pages [1- 219], 2012

[2] David Consulting Group, “What is TMMi® – and Why Should You Care?” , pages [1- 2], May 2013

[3] Dean Leffingwell, “Scaling Software Agility: Best Practices for Large Enterprises”, pages [5- 15], 2007

[4] Erik van Veenendaal, Richard Grooff and Rob Hendriks,”Test Process Improvement using TMM(i)”, STAR Tester, Issue 19, pages [1- 7], October 2007

[5] David Consulting Group, “How does TMMI work and what does it contain”, pages [1- 5], June 2013

[6] Cognizant 20-20 insights, “Adopting the Right Software Test Maturity Assessment Model”, pages [1- 5], June 2014

[7] Ken Schwaber and Jeff Sutherland, “The Definitive Guide to Scrum: The Rules of the Game”, pages [1- 16], July 2013

[8] Linz, Tilo,” Testing in Scrum: A Guide for Software Quality Assurance in the Agile World”, pages [11-32], March 2014

[9] Sander Bannink, “Challenges in the Transition from Waterfall to Scrum – a Casestudy at Portbase, Twente Student Conference on IT”, pages [1-10], January 2014

[10] Deepa Vijay and Gopinath Ganapathy, “GUIDELINES TO MINIMIZE THE COST OF SOFTWARE QUALITY IN AGILE Scrum PROCESS, IJSEA, Vol.5, No.3”, pages [61- 69], May 2014

[11] Ahsan Nawaz & Kashif Masood Malik, “SOFTWARE TESTING PROCESS IN AGILE DEVELOPMENT”, pages [3-9], June 2008

[12] Ana Sofia C. Marçal, Felipe S. Furtado Soares, Teresa M. Maciel, “Blending Scrum practices and CMMI project management process areas”, pages [17-29], January 2008

[13] Ana Sofia C. Marçal, Bruno Celso C. de Freitas, Felipe S. Furtado Soares, Arnaldo D. Belchior, “Mapping CMMI Project Management Process Areas to SCRUM Practices”, pages [1- 9], 2007

[14] Armin Preis, “Integration Evaluation of Scrum and CMMI - Theoretical Survey at the Project-Management Level”, pages [1- 28], January 2012

[15] Neil Potter and Mary Sakry, “IMPLEMENTING SCRUM (AGILE) AND CMMI® TOGETHER”, pages [1- 6], March 2009

[16] Jessica Diaz, Juan Garbajosa, and Jose A. Calvo-Manzano,” Mapping CMMI Level 2 to Scrum Practices: An Experience Report”, pages [93-104], 2009

[17] Juha Koskela, “Software configuration management in agile methods”, pages [33- 54], ESPOO 2003

[18] CMMI Product Team, “CMMI® for Development”, Version 1.2, pages [114- 130, 353- 363], August 2006

Ontology-Based Textual Emotion Detection

Mohamed Haggag
Computer Science Department
Faculty of Computers and information
Cairo, Egypt

Samar Fathy, Nahla Elhaggar
Information Technology Department
Faculty of Computers and Information, Helwan University
Cairo, Egypt

***Abstract*—Emotion Detection from text is a very important area of natural language processing. This paper shows a new method for emotion detection from text which depends on ontology. This method is depending on ontology extraction from the input sentence by using a triplet extraction algorithm by the OpenNLP parser, then make an ontology matching with the ontology base that we created by similarity and word sense disambiguation. This ontology base consists of ontologies and the emotion label related to each one. We choose the emotion label of the sentence with the highest score of matching. If the extracted ontology doesn't match any ontology from the ontology base we use the keyword-based approach. This method doesn't depend only on keywords like previous approaches; it depends on the meaning of sentence words and the syntax and semantic analysis of the context.**

Keywords—emotion detection; ontology; ontology matching; natural language processing

I. Introduction

Textual analysis has many areas that have established standard methods and are also beneficial to emotion detection studies. Emotion detection is considered a newer area of textual analysis and therefore, has weaker standard methods.

Emotion detection of the text plays a key role in the human-computer interaction. People may express emotions by speech, facial and text emotion detection. There are a sufficient amount of work that has been done regarding facial and speech emotion detection, but text-based emotion detection system still needs attraction of researchers. In computational linguistics, the detection of human emotions in the text is becoming increasingly important from an applicative point of view. Automatic detection and classification of emotions has several potential areas of application such as sentiment analysis or opinion mining, market analysis, monitoring newsgroups and forums, affective computing, and natural language interfaces such as e-learning environments or educational/edutainment games.

Three approaches currently dominate the emotion detection task that will be discussed in the next section; Keyword based approach, Learning based approach, and Hybrid approach.

This paper is structured as follows. The second section is related work that covers emotion theories; emotion labeled datasets, emotional lexicon, computational approaches of emotion detection and their limitations. The third section presents our proposed method. The fourth section is a case study. The fifth section discusses our results. The sixth section is a conclusion.

II. Related Work

A. Emotion Theories

Ekman, Izard, and Pultchick lists which are shown in table 1 are the most common lists of emotions used in emotion detection methods. Also there is a model which called OCC (Ortony/Clore/Collins) model. The OCC model presents emotions generally expressed by an agent. The OCC model includes 22 emotion categories [15] designed to model humans in general. It is based on the premise that emotions "are not themselves linguistic things, but the most readily available non phenomenal access we have to them is through language [15].

TABLE I. COMMON LISTS OF EMOTIONS USED IN EMOTION DETECTION METHODS [11, 19, AND 20]

Lists of Basic Emotions	
Ekman	anger, disgust, fear, joy, sadness, and surprise
Izard	anger, Contempt, disgust, distress, fear, guilt, interest, joy, shame, and surprise
Pultchick	anger, anticipation, disgust, fear, joy, sadness, surprise, and trust

B. Emotion Labeled Datasets

Emotion labeled datasets are blocks of text that have been collected and annotated with emotion tags. It is very expensive and time consuming to annotate datasets manually. However, because the most stabilized method of checking the accuracy of an algorithm is comparing results to annotated text, annotated datasets have been established and consistently used throughout emotion detection studies. The most common annotated datasets are:

SemEval 2007-Task [4]

It is a common dataset used in many emotion detection studies for training or testing. It is an affective text that consists of newspaper headlines. This dataset multiple emotion tags for one sentence [11]. The annotations are labeled with Ekman's six basic emotions (anger, disgust, fear, joy, sadness, and surprise) along with a neutral category. The dataset is composed of 1,250 annotated news titles, extracted from news web sites (such as Google news, CNN) and/or newspapers that is split between a training set of 250 headlines and a test set of 1,000 news headlines.

International Survey on Emotion Antecedents and Reactions (ISEAR)

It is an annotated dataset which is composed of 7.666 sentences provided by 1,096 participants with different cultures and from different countries and fields. They were questioned about experiences and reactions that related to emotions of anger, disgust, fear, joy, sadness, and guilt.

Fairy Tales

Fairy tales is an emotion labeled dataset which is compiled of stories by the authors B. Potter, H. C. Anderson, & the Brothers Grimm. The stories are annotated at the sentence-level.

A larger set of specific emotions is provided by varying annotation processes which have conducted by Alm. In 2005, a dataset labelled with Izard's set of ten basic emotions which consists of 1580 sentences is compiled. In 2009, a dataset labelled with five emotion classes: angry-disgusted, fearful, happy, sad, and surprised is complied.

C. Emotional Lexicon

In the previous approaches of emotion detection discovering keywords or phrases that associated with emotions is the first step. These keywords and phrases are very important for training. Emotional lexicon is a list of emotions and words that express each emotion [20]. The first step to make this lists is to identify the words that highly associate with one emotion, and expand by using synonyms. There are a few lexicons that generated a sufficient start. The most popular lexicons are:

ANEW Word List (Affective Norms for English Words) [3]

The ANEW list consists of a list of words scored within three emotional dimensions: pleasure, arousal and dominance, according to the SAM standard.

DAL Dictionary (Whissell's Dictionary of Affect Language) [23]

The DAL list contains 8742 words rated by people for their *activation*, *evaluation* and *imagery*.

LIWC Dictionary *(Linguistic Inquiry and Word Count Dictionary)* [17]

The LIWC dictionary provides a set of 2290 words and stems, classified in one or more categories, such as sadness, negative emotion or overall affect.

The use of words or stems, instead of concepts, as the primitive units, without recognizing the context in which the words are used is the main limitation of these lexicons. The lexicon which is on the contrary is:

WordNet Affect database [22]

The WordNet Affect Lexicon consists of 911 WordNet synsets labeled with a hierarchical set of emotional categories. It is a manually created collection of words. Each word is annotated with the emotion they evoke. The creation process involved annotating a few seed words or words that highly associate with one emotion with Ekman's six basic emotions then expanding the collection by using the WordNet synonyms of each word with the same emotion. The full list reached 1456 words.

Even though emotion lexicons is very important and growing it would be beneficial in detecting emotion, an annotated collection of words and phrases would only increase detection accuracy to a certain extent. In fact, most of the time emotion is not expressed through the use of words in emotion [1]. The majority of words, or the synonyms of a word, fall under more than one emotional classifier [20]. These words have unclear emotional meaning making the emotion label change by context or by the words surrounding it.

D. Computational Approaches for Emotion Detection

Currently there are three approaches dominating the emotion detection task; keyword based, learning based and hybrid based approach. In this section, the authors will provide a brief description of each of these approaches with particular emphasis on the pros and cons as presented in [7, 8].

Keyword based approach

This approach depends on the presence of keywords and involves pre-processing with a parser and emotion dictionary. It is easy to implement and straight forward since it involves identifying words to search for in text.

This approach has been applied in chat systems by:

- M. Chunling, H. Prendinger, and M. Ishizuka in [15]. This chat system displays emotion using an avatar.
- J. T. Hancock, C. Landrigan, and C. Silver in [14]. They introduce a laboratory controlled online chat experiment to enact sadness and happiness and reporting strategies that people employ to express emotions in text.
- H. Li, N. Pang, and S. Guo in [12]. They introduce the emotion detection incorporating personality factor in chatting system to improve accuracy.

Learning Based Approach

This approach uses a trained classifier for emotion detection task by using keywords as features. It can quickly learn new features from corpora by supplying a large training set to a machine learning algorithm for building a classification model; so it is easily and faster.

This approach has been applied by:

- C. Yang, K. H.-Y. Lin, and H.-H. Chen in [16]. They introduced an emotion classification method from training at sentence level and applying at document level with sentence level contextual meaning.
- Z. Teng, F. Ren, and S. Kuroiwa in [25]. They presented a recognition of Emotion method with SVMs (support vector machine).

Hybrid Approach

The hybrid approach is a combination of the keyword based implementation and learning based implementation. This approach can yield higher accuracy results from training a combination of classifiers and adding knowledge-rich linguistic information from dictionaries and thesauri.

This approach has been applied by:

- S. Aman and S. Szpakowicz in [18]. They introduced an Emotion annotation task by category, intensity and word/phrase.
- E. C.-C. Kao, L. Chun-Chieh, Y. Ting-Hao, H. Chang-Tai, & S. Von-Wun in [9]. They introduced a survey on detection methods and possible improvements.
- Haji Binali, Chen Wu, and Vidyasagar Potdar in [13]. They presented a hybrid based architecture comprising of keyword based component and learning system component.
- C.-H. Wu, Z.-J. Chuang, and Y.-C. Lin in [6].They utilize a rule-based approach to extract semantics related to specific emotions, and Chinese lexicon ontology to extract attributes. These semantics and attributes are then associated with emotions in the form of emotion association rules.

Limitations in Current Approaches

From the above discussion there are few limitations:

Ambiguity in Keyword Definitions

Using emotion keywords isn't the best way to detect associated emotions, every keyword could change its meaning according to different usages and contexts. The meanings of keywords could be multiple and vague, as most words could change their meanings according to different usages and contexts.

Incapability of Recognizing Sentences without Keywords

Keyword-based approach is totally based on emotion lexicons, so the emotion of sentences which doesn't contain any emotion keyword can't be detected. For example, "I passed my exam" and "Hooray! I passed my exam" should imply the same emotion (joy), but actually the emotion of the first simple can't be detected by using the keyword-based approach because it doesn't contain any emotion keyword like "hooray".

Lack of Linguistic Information

Syntax structures and semantics also affects the expressed emotions. For example, "I laughed at John" and "John laughed at me" would suggest different emotions from the first person's perspective. As a result, the keyword-based approach has a problem because of ignoring the linguistic information.

Difficulties in Determining Emotion Indicators [21]

Although learning-based methods can automatically determine the probabilities between features and emotions, it still need keywords as features, so this approach have the same problems of the keyword-based approach.

Over-simplified Emotion Categories

Nevertheless, the problems caused by using keywords as features, most learning-based methods classifies sentences into positive and negative categories only.

III. PROPOSED ARCHITECTURE

The main idea of our method is to extract ontology from input sentences and match it with our ontology base. This ontology base consists of the ontology relation between classes or objects (simple ontology) and its related emotion.

We make some pre-processing tasks on the input text and get the ontology relation(s) from the sentence, and then we make ontology matching between sentence relation(s) and our ontology base to get the emotion of the sentence. So by this method we put the sentence in a form which can be compared with others to get the similarity between sentences not based only on keywords but also its meaning of the words and the syntax and semantic analysis of the sentence.

You can find our proposed architecture at Fig.1. If the new sentence ontology doesn't match with any relation of our ontology base we use the keyword based approach. For the keyword based approach we use the WordNet affect database.

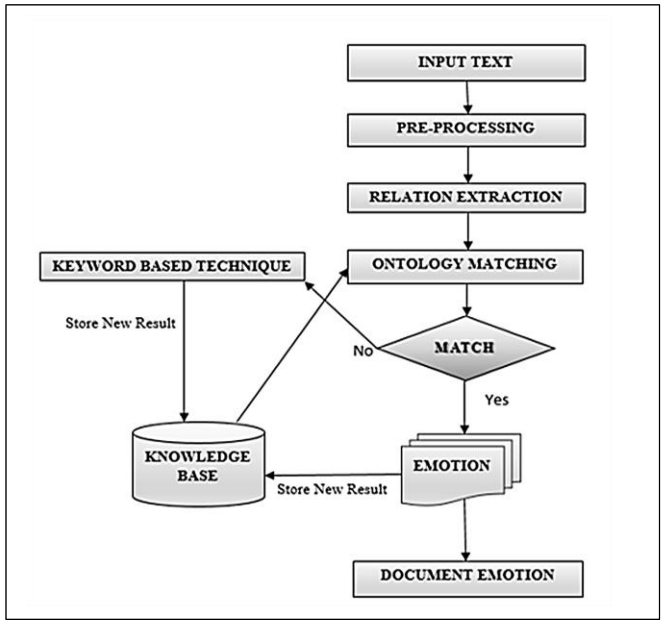


Fig. 1. Proposed Architecture

A. Pre-processing

There are some steps must be done to the input text to extract the ontology from sentences. These steps are:

Sentence detecting: Is to convert our input text into sentences.

Parsing: To break a sentence down into its component parts of speech with an explanation of the form, function, and syntactical relationship of each part.

Sentence splitting: Is the process of converting the compound and complex sentence into simple sentences.

Example for sentence splitting:

John plays football, but Jack plays basketball.

The result will be two separated simple sentence:

Sentence 1 = John plays football.

And

Sentence 2 = Jack plays basketball.

B. Ontology Extraction

Sentence Triplet Extraction

Our method for extracting ontology relations or simple ontologies from sentence is based on ***sentence triplet extraction*** (subject, predicate, and object). Which means that the subject will be the first class or individual, the object will be the second one and the predicate will be the relation between them. Delia Rusu*, Lorand Dali*, Blaž Fortuna°, Marko Grobelnik°, & Dunja Mladenić, 2007 presented in [8] four different well known syntactical parsers for English for generating parse trees from the sentences, followed by extracting the triplets from the parse trees. They are the Stanford parser, OpenNLP parser, Link parser, and MINIPAR parsers. They made a comparison between them and proved that the OpenNLP parser is the best. So authors use the OpenNLP parser; In OpenNLP parser a sentence (S) is represented by the parser as a tree; each tree having three children: a noun phrase (NP), a verbal phrase (VP) and the full stop (.). The root of the tree will be S.

Firstly, the subject can be found by performing breadth first search and selecting the first descendent of the NP subtree that is a noun. Secondly, for determining the predicate of the sentence and checking for negation, for searching for the predicate and negation check a search will be performed in the VP subtree. The verb can be found by finding the deepest verb descendent of the verb phrase. Thirdly, objects can be found in three different subtrees, all siblings of the VP subtree containing the predicate. They are: (prepositional phrase), NP and ADJP (adjective phrase). In NP and PP the object can be found by searching for the first noun, while in the ADJP by searching for the first adjective. After that we get the attributes of each element of the triplet using the algorithm in Fig. 2 which is mentioned in [8].

You can find OpenNLP Part-of-Speech (POS) Tags in table 2.

Named Entity Recognition (NER)

After ontology extraction using triplet extraction we make the Named entity recognition subtask for each element in our ontology which seeks to locate and classify elements in text into pre-defined categories such as the names of persons, organizations, locations, expressions of times, quantities, monetary values, percentages, etc.

Stop Words Handling

It is the process of removing the stop words from the ontology elements to decrease the execution time for the next steps.

```
function EXTRACT-ATTRIBUTES(word) returns a solution, or
failure
        // search among the word's siblings
        if adjective(word)
                result ← all RB siblings
        else
                if noun(word)
                        result ← all DT, PRP$, POS, JJ,
                        CD, ADJP, QP, NP siblings
                else
                        if verb(word)
                                result ← all ADVP
                                siblings
        // search among the word's uncles
        if noun(word) or adjective(word)
                if uncle = PP
                        result ← uncle subtree
        else
                if verb(word) and (uncle = verb)
                        result ← uncle subtree
        if result ≠ failure then return result
        else return failure
```

Fig. 2. The algorithm for extracting the attributes of the triplet in treebank output

C. Ontology Matching

Ontology matching is the process of finding the similarity between the first classes of the two simple ontologies, the two relations of the two ontologies, and the second classed of them, then we get the score of the ontology matching between the two ontologies. For calculating the similarity we use the Wu & Palmer measure. wup finds the depth of the LCA depth of the concepts, and then scales that by the sum of the depths of the individual concepts. We use the WordNet 2.1 to get it. Before we get the similarity between any pair of them we get the meaning (sense) of each word by using the Lesk algorithm to get more accurate similarity. We make ontology matching with all ontologies in the ontology base, and we get the emotion of the one with the best score of similarity.

Example of ontology matching shown in Fig. 3.

This figure shows two simple ontologies .To make ontology matching between them we get the semantic similarity between “author” and “illustrator”, ”write” and “compose”, and “story” and “report”.

D. Keyword Based Approach

In our keyword based approach we use WordNet affect database. Firstly we make tokenization, POS tagging, stop words handling, and then get the similarity of each token with keywords in the WordNet affect database instead of depending on the appearance of the keywords.

TABLE II. OPENNLP POS TAGS

Number	Tag	Description
1.	CC	Coordinating conjunction
2.	CD	Cardinal number
3.	DT	Determiner
4.	EX	Existential *there*
5.	FW	Foreign word
6.	IN	Preposition or subordinating conjunction
7.	JJ	Adjective
8.	JJR	Adjective, comparative
9.	JJS	Adjective, superlative
10.	LS	List item marker
11.	MD	Modal
12.	NN	Noun, singular or mass
13.	NNS	Noun, plural
14.	NNP	Proper noun, singular
15.	NNPS	Proper noun, plural
16.	PDT	Predeterminer
17.	POS	Possessive ending
18.	PRP	Personal pronoun
19.	PRP$	Possessive pronoun
20.	RB	Adverb
21.	RBR	Adverb, comparative
22.	RBS	Adverb, superlative
23.	RP	Particle
24.	SYM	Symbol
25.	TO	*to*
26.	UH	Interjection
27.	VB	Verb, base form
28.	VBD	Verb, past tense
29.	VBG	Verb, gerund or present participle
30.	VBN	Verb, past participle
31.	VBP	Verb, non-3rd person singular present
32.	VBZ	Verb, 3rd person singular present
33.	WDT	Wh-determiner
34.	WP	Wh-pronoun
35.	WP$	Possessive wh-pronoun
36.	WRB	Wh-adverb

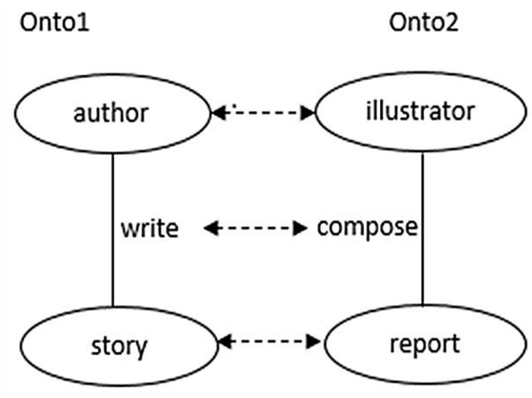


Fig. 3. Example of ontology matching

IV. CASE STUDY

If our ontology base is as shown in Table 3

TABLE III. EXAMPLE OF SIMPLE ONTOLOGY BASE

Ontology Base					
Sentence_id	***Class1***	***Relation***	***Calss2***	***negation***	***emotion***
1	Mortar assaults	leaves	dead	No	sadness
2	Bombers	kill	shoppers	No	fear
3	Havana	deal	good experiment	No	joy
4	person	marrying	Doherty	No	joy
5	Women in 60	are	perfectly good mothers	No	sadness

And the sentence to test is:

John shoot the customers.

Steps will be as follow:

A. Pre-processing

- *Sentence splitting*: John shoot the customers.
- *Parsing*: The result shown in fig. 4

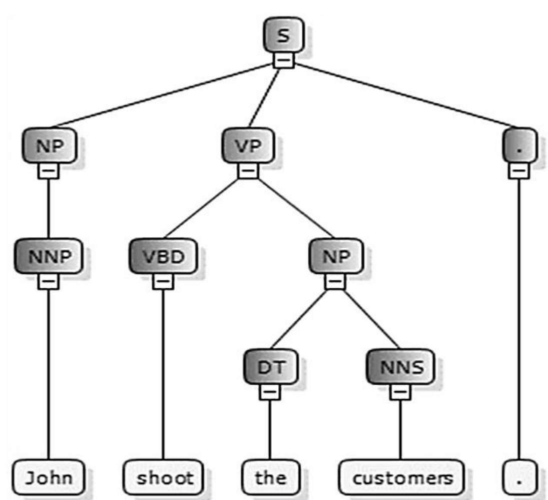


Fig. 4. The result of parsing

B. Ontology Extraction

The result of ontology extraction from sentence shown in Table 4.

TABLE IV. ONTOLOGY EXTRACTION RESULT FROM SENTENCE

Class1	Relation	Calss2	negation
person	shoot	customers	no

C. Ontology Matching

This step is shown below in Table 5

TABLE V. ONTOLOGY MATCHING

Sentence_id	Class 1 similarity	Relation Similarity	Class 2 similarity	Score
1	(Person, Mortar Assaults) = 0.35	(Shoot, Leaves) = 0.78	(Customers, dead) = 0.15	0.4
2	(Person, Bombers) = 0.89	**(Shoot, Kill) = 0.61**	**(customers, Shoppers) = 0.93**	0.81
3	(Person, Havana)= 0.35	(Shoot ,deal) = 0.6	(customers, good experiment) = 0.17	0.37
4	(person, Person)= 1	(Shoot, marrying)=0	(customers, Doherty)= 0	0.33
5	(Person, Women in 60)= 0.58	(Shoot, are)=0	(customers, perfectly good mothers) = 0.3	0.29

We choose the highest score and at the same time the similarity with each ontology element isn't less than 0.5.

In this case the best score is 0.81 which is for sentence 2, so the emotion of the sentence will be (***Fear***), and then add this new relation in our ontology base. But if there is no matching then we apply our keyword based approach.

V. EXPERIMENTAL RESULTS

Our testing will be at the sentence level. For training we create a data set of 511 sentences which are similar in meaning of 511 newspapers headlines of the SemEval dataset which are complete sentences with the help of online dictionaries, and make our training on these new headline to create our ontology base. This ontology base contains 31 ontologies which have 'anger' emotion, 14 have 'disgust' emotion, 75 have 'fear' emotion, 120 have 'sadness' emotion, 83 have 'surprise' emotion, 188 have joy emotion.

We made our testing on the SemEval dataset. Like most emotional detection approaches, results are presented with the common measures of precision, recall, and f-score. Precision is the number of relevant instances retrieved by the given algorithm over the total number of instances retrieved by the algorithm. In this case, precision is the number of correctly labeled sentences retrieved by the algorithm divided by all the sentences retrieved by the algorithm. Recall is the number of relevant instances retrieved by the given algorithm over the total number that should have been returned. In this study, recall is the number of correctly labeled sentences retrieved by the algorithm divided by all the sentences annotated as correct. After precision and recall are calculated, we multiply them by 100 then the values are used to calculate the f-score, or the harmonic mean of precision and recall that functions as a weighted average equation. You can find the f-score equation in (1):

$$f\text{-}score = 2 \times \frac{Precision \times Recall}{Precision + Recall} \quad (1)$$

In all measures, 100.0 is the highest value and 0.0 the lowest.

For example, When a search engine returns 30 pages only 20 of which were relevant while failing to return 40 additional relevant pages, its precision is (20/30)*100= 66.67 while its recall is (20/60) * 100 = 33.33

Results are shown in Table 8.

TABLE VI. OUR RESULTS

Precision	Recall	F1
Anger		
70.49	66.15	68.25
Disgust		
77.27	77.27	77.2
Fear		
95.33	62.58	75.55
Joy		
89.5	66.02	76.2
Sadness		
93.2	73.66	82.28
Surprise		
90.15	64.67	75.38

We compare our results with those obtained in [7] which have implemented five different systems for emotion analysis:

WN-Affect Presence, which is used as a baseline system, and which annotates the emotions in a text simply based on the appearance of words from the Word-Net Affect lexicon.

LSA Single Word, which calculates the latent semantic analysis similarity between the given text and each emotion, each emotion is represented as the vector of the specific word denoting the emotion (e.g., anger).

LSA Emotion Synset, which calculates the latent semantic analysis similarity between the given text and each emotion synset, where in addition to the word denoting an emotion, its synonyms from the WordNet synset are also used.

LSA all Emotion Words, which increases the previous set by adding the words in all the synsets labeled with a given emotion, as found in WordNet Affect.

NB Trained on Blogs, which uses a Naive Bayes classifier trained on the blog data annotated for emotions.

Table 7 show their results.

TABLE VII. RESULTS OF THE FIVE SYSTEMS

	Precision	Recall	F1
Anger			
WN-affect presence	**33.33**	3.33	6.06
LSA single word	6.28	63.33	11.43
LSA emotion synset	7.29	86.67	13.45
LSA all emotion words	6.20	**88.33**	11.58
NB trained on blogs	13.68	21.67	**16.77**
Disgust			
WN-affect presence	0	0	-
LSA single word	2.41	70.59	**4.68**
LSA emotion synset	1.53	64.71	3.00
LSA all emotion words	1.98	**94.12**	3.87
NB trained on blogs	0	0	-
Fear			
WN-affect presence	**100.00**	1.69	3.33
LSA single word	12.93	**96.61**	**22.80**
LSA emotion synset	12.44	94.92	22.00
LSA all emotion words	12.55	86.44	21.91
NB trained on blogs	16.67	3.39	5.63
Joy			
WN-affect presence	**50.00**	0.56	1.10
LSA single word	17.81	47.22	25.88
LSA emotion synset	19.37	72.22	30.55
LSA all emotion words	18.60	**90.00**	**30.83**
Sadness			
WN-affect presence	**33.33**	3.67	6.61
LSA single word	13.13	55.05	21.20
LSA emotion synset	14.35	58.71	**23.06**
LSA all emotion words	11.69	**87.16**	20.61
NB trained on blogs	20.87	22.02	21.43
Surprise			
WN-affect presence	**13.04**	4.68	6.90
LSA single word	6.73	67.19	12.23
LSA emotion synset	7.23	89.06	13.38
LSA all emotion words	7.62	**95.31**	**14.10**
NB trained on blogs	8.33	1.56	2.63

That paper also compare their results with those obtained by three systems participating in the Semeval emotion annotation task: SWAT, UPAR7 and UA. The authors briefly describe below each of the three systems:

UPAR [10]: It is a rule-based system. Uncapitalizes common words in the news titles is the first pass through the data. The system then identifies what is being said about the main subject by exploiting the dependency graph of the modified title obtained from the Stanford syntactic parser. The system then rate each word separately for each emotion and then the main subject rating is boosted. The system uses a combination of WordNet Affect and SentiWordNet [2], which were semi-automatically enriched on the basis of the original trial data provided during the Semeval task.

UA [24]: This system determines the kind and the amount of emotion in each headline by using statistics gathered from three search engines. The emotion scores are obtained through Pointwise Mutual Information (PMI). First, the number of documents obtained from the three web search engines by using a query that contains all the words of the headline and an emotion (the words occur in an independent proximity across the Web documents) is divided by the number of documents containing only an emotion and the number of documents containing all the headline words. Second, the system estimates an associative score between each content word and an emotion and then uses it to weight the final PMI score. Then normalizes the final results to the 0-100 range.

SWAT [5]: This system is a supervised system which annotates emotional content by using a unigram model, then performs synonym expansion on the emotion label words, using the Roget Thesaurus.

The SWAT team annotated an additional set of 1000 headlines, in addition to the development data provided by the task organizers. They used these 1000 sentences for training.

The results of the three systems shown in Table 8.

TABLE VIII. RESULTS OF THE SYSTEMS PARTICIPATING IN THE SEMEVAL TASK - EMOTION ANNOTATIONS

	Precision	Recall	F1
Anger			
SWAT	12.00	5.00	7.06
UA	12.74	**21.6**	**16.03**
UPAR7	**16.67**	1.66	3.02
Disgust			
SWAT	0	0	-
UA	0	0	-
UPAR7	0	0	-
Fear			
SWAT	25.00	14.40	18.27
UA	16.23	**26.27**	**20.06**
UPAR7	**33.33**	2.54	4.72
Joy			
SWAT	35.41	**9.44**	**14.91**
UA	40.00	2.22	4.21
UPAR7	**54.54**	6.66	11.87
Sadness			
SWAT	32.50	11.92	17.44
UA	25.00	0.91	1.76
UPAR7	**48.97**	**22.02**	**30.38**
Surprise			
SWAT	11.86	10.93	11.78
UA	**13.70**	**16.56**	**15.00**
UPAR7	12.12	1.25	2.27

+The overall average results obtained by our system and all the other systems shown in Table 9.

TABLE IX. OVERALL AVERAGE RESULTS

	Precision	Recall	F1
Our system	**85.99**	68.39	**75.8**
WN-affect presence	38.28	1.54	4.00
LSA single word	9.88	66.72	16.37
LSA emotion synset	9.20	77.71	13.38
LSA all emotion words	9.77	**90.2**	17.57
NB trained on blogs	12.04	18.01	13.22
SWAT	19.46	8.61	11.57
UA	17.94	11.26	9.51
UPAR7	27.60	5.68	8.71

Best results shown in bold. We show that our system has the best results in precision, and F-score. LSA all emotion words has the best result in recall.

Our results in recall can be better if the number of ontologies extracted from sentences that matches our ontology base increased. That can be achieved by making an ontology base for each domain separately e.g. medical, sport, tourism, and so on.

VI. CONCLUSION

Emotion detection has a promising future. Although not enough time has passed to have established standards in the field, there is some consistency between the approaches, and the algorithms are continuing to increase in accuracy. This paper describes a new method for emotion detection from the text by ontology extraction from sentences, ontology matching with our ontology base that consists of ontologies and the related emotion for each one. This method provides syntax and semantic analysis of the context and provides the meaning of words. We show our results of testing on the SemEval dataset, and compare our results with different results that were implemented by Carlo Strapparava and Rada Mihalcea in 2008. We show that our system has the best results in precision and F-score.

REFERENCES

[1] A. Balahur, J. M. Hermida, and A. Montoyo. Detecting implicit expressions of sentiment in text based on commonsense knowledge. In Proceedings of the 2nd Workshop on Computational Approaches to Subjectivity and Sentiment Analysis, WASSA '11, pages 53{60, Stroudsburg, PA, USA, 2011. Association for Computational Linguistics.

[2] A. Esuli and F. Sebastiani. SentiWordNet: A publicly available lexical resource for opinion mining. In Proceedings of the 5th Conference on Language Resources and Evaluation, Genova, IT, 2006.

[3] Bradley, M.M., Lang, and P.J.: Affective norms for English words (ANEW): Instruction manual and affective ratings. Technical Report C-1, the Center for Research in Psychophysiology, University of Florida (1999).

[4] C. Strapparava and R. Mihalcea, SemEval-2007 task 14: Affective Text. In Proceedings of SemEval-2007, Prague, Czech Republic, June 2007.

[5] C. Yang, K. H.-Y. Lin and H.-H. Chen, "Emotion classification using web blog corpora," Proc. IEEE/WIC/ACM International Conference on Web Intelligence. IEEE Computer Society, Nov. 2007, pp. 275-278, doi: 10.1109/WI.2007.50.

[6] C.-H. Wu, Z.-J. Chuang, and Y.-C. Lin, "Emotion Recognition from Text Using Semantic Labels and Separable Mixture Models," ACM Transactions on Asian Language Information Processing (TALIP), vol. 5, issue 2, Jun. 2006, pp. 165-183, doi:10.1145/1165255.1165259.

[7] Carlo Strapparava and Rada Mihalcea, Learning to Identify Emotions in Text. Proceedings of the 2008 ACM symposium on Applied computing, 1556-1560.

[8] Delia Rusu*, Lorand Dali*, Blaž Fortuna°, Marko Grobelnik°, and Dunja Mladenić. "Triplet Extraction from Sentences", Technical University of Cluj-Napoca, Faculty of Automation and Computer Science G. Bariţiu 26-28, 400027 Cluj-Napoca, Romania. Department of Knowledge Technologies, Jožef Stefan Institute.Jamova 39, 1000 Ljubljana, Slovenia, 2007.

[9] E. C.-C. Kao, L. Chun-Chieh, Y. Ting-Hao, H. Chang-Tai, and S. Von-Wun, "Towards Text-based Emotion Detection," in International Conference on Information Management and Engineering, 2009, pp. 70-74.

[10] F. Chaumartin. Upar7: A knowledge-based system for headline sentiment tagging. In Proceedings of SemEval-2007, Prague, Czech Republic, June 2007.

[11] F. Keshtkar and D. Inkpen. A corpus-based method for extracting paraphrases of emotion terms. In Proceedings of the NAACL HLT 2010 Workshop on Computational Approaches to Analysis and Generation of Emotion in Text, CAAGET '10, pages 35{44, Stroudsburg, PA, USA, 2010. Association for Computational Linguistics.

[12] H. Li, N. Pang, and S. Guo, "Research on Textual Emotion Recognition Incorporating Personality Factor," in International conference on Robotics and Biomimetics, Sanya, China, 2007.

[13] Haji Binali, Chen Wu, and Vidyasagar Potdar, "Computational Approaches for Emotion Detection in Text", Digital Ecosystems Business Intelligence Institute Curtin University of Technology Perth, Australia, 4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010).

[14] J. T. Hancock, C. Landrigan, and C. Silver, "Expressing emotion in text-based communication," in Proceedings of the SIGCHI conference on Human factors in computing systems, 2007, pp. 929 – 932.

[15] M. Chunling, H. Prendinger, and M. Ishizuka, "Emotion Estimation and Reasoning Based on Affective Textual Interaction" in Affective Computing and Intelligent Interaction. vol. 3784/2005: Springer Berlin / Heidelberg, 2005, pp. 622-628.

[16] P. Katz, M. Singleton, and R. Wicentowski, Swat-mp:the semeval-2007 systems for task 5 and task 14. In Proceedings of SemEval-2007, Prague, Czech Republic, June, 2007.

[17] Pennebaker, J.W., Francis, M.E., Booth, and R.J.: Linguistic Inquiry and Word Count (LIWC): LIWC2001. Erlbaum Publishers, Mahwah, NJ (2001)

[18] S. Aman and S. Szpakowicz, "Identifying Expressions of Emotion in Text " in V. Matousek, P. Mautner (eds.): Proc 10th International Conf. on Text, Speech and Dialogue TSD 2007, Plzeň, Czech Republic.

[19] S. M. Kim, A. Valitutti, and R. A. Calvo. Evaluation of unsupervised emotion models to textual affect recognition. In Proceedings of the NAACL HLT 2010 Workshop on Computational Approaches to Analysis and Generation of Emotion in Text, CAAGET '10, pages 62{70, Stroudsburg, PA, USA, 2010. Association for Computational Linguistics.

[20] S. M. Mohammad and P. D. Turney. Emotions evoked by common words and phrases: using mechanical turk to create an emotion lexicon. In Proceedings of the NAACL HLT 2010 Workshop on Computational Approaches to Analysis and Generation of Emotion in Text, CAAGET '10, pages 26{34, Stroudsburg, PA, USA, 2010. Association for Computational Linguistics.

[21] S. Mohammad. From once upon a time to happily ever after: tracking emotions in novels and fairy tales. In Proceedings of the 5th ACL-HLT Workshop on Language Technology for Cultural Heritage, Social Sciences, and Humanities, LaTeCH '11, pages 105{114, Stroudsburg, PA, USA, 2011. Association for Computational Linguistics.

[22] Strapparava, C., Valitutti, and A.: Wordnet-affect: an affective extension of WordNet. In: Proceedings of the 4th International Conference on Language Resources and Evaluation, pp. 108--1086. Lisbon, Portugal (2004)

[23] Whissell, C.M.: The dictionary of affect in language. In: Robert Plutchik and Henry Kellerman (Ed.), Emotion: Theory, Research, and Experience, pp. 113--131 (1989).

[24] Z. Kozareva, B. Navarro, S. Vazquez, and A. Montoyo. Ua-zbsa: A headline emotion classification through web information. In Proceedings of SemEval-2007, Prague, Czech Republic, June 2007.

[25] Z. Teng, F. Ren, and S. Kuroiwa, "Recognition of Emotion with SVMs," in Lecture Notes of Artificial Intelligence 4114, D.-S. Huang, K. Li, and G. W. Irwin, Eds. Springer, Berlin Heidelberg, 2006, pp. 701-710, doi: 10.1007/11816171_87.

Osteoporosis Detection using Important Shape-Based Features of the Porous Trabecular Bone on the Dental X-Ray Images

Enny Itje Sela
Department of Informatics
STMIK AKAKOM
Yogyakarta, Indonesia

Rini Widyaningrum
Department of Dentomaxillofacial Radiology
Faculty of Dentistry
Universitas Gadjah Mada
Yogyakarta, Indonesia

***Abstract*—Osteoporosis screening using dental X-Ray images has been growing an interesting research. Existing methods for osteoporosis screening have been performed using the dental periapical or panoramic in X-Ray images. There was limited research using both the periapical and panoramic due to the expensive cost of obtaining data. This paper presents a combination of the periapical and panoramic images for osteoporosis detection. The image processing was performed to obtain the shape-based features of the porous trabecular bone on both the dental radiograph images. The important features were selected from the extracted features. These selected features were chosen for osteoporosis detection using the decision tree. The quantitative evaluation used confusion matrix. It was found accuracy rate to be 73.33%, sensitivity rate to be 72.23, and specificity rate to be 72.23% for data testing.**

Keywords*—dental X-Ray; feature selection; osteoporosis Detection; porous trabecular bone

I. INTRODUCTION

Dentists often use radiographs images to support their diagnosis [1][2][3]. The panoramic and the periapical radiograph is kind of extra oral and intraoral assessment which is very widely used by dentists because it is fast, easy to operate, and its cost is relatively inexpensive. Changes in trabecular and cortical mandible radiographically appearing on the images are the first sign of osteoporosis which can be found by dentists [4].

Low bone density is one indicator of the occurrence of osteoporotic fracture. The screening of bone mass density (BMD) is an ideal method for early detection of osteoporosis [5][6][7]. Screening BMD using dual technique X-ray absorptiometry (DXA) is the gold standard for osteoporosis diagnosis [3]. Using a densitometer for osteoporosis diagnosis can be performed on the arms, spine, and thigh [20]. One of the results of measurements of bone density using DXA is a T-Score. Based on WHO criteria, the T-score can be interpreted in 3 categories, which are normal bone density, low bone density (osteopenia), and osteoporosis (brittle bones) [8]. However, screening of osteoporosis using DXA is relatively expensive for Indonesian, and not all hospitals in Indonesia have this tool. Also, DXA still has a limitation because it cannot describe the bone microarchitecture. Bone microarchitecture is quite parameter in the assessment of bone quality [9]. Several studies have been done related to the osteoporosis screening using the periapical radiograph images [10][11][12] as well as the panoramic radiograph images [7][13][14]. However, studies using these images for Indonesian are still limited. Also, detection using both images had not performed yet due to the lack of data. The selection of features is one of the important stages before detection of osteoporosis. One of the feature selection methods used by [11][13][14] is a decision tree. Then, the selected features can be used to detect osteoporosis. Previous studies in [15] had performed porous features selection but they used only the periapical images for osteoporosis screening. This study proposes a model for detection of osteoporosis through the panoramic and periapical radiograph images using the selected shape-based porous trabecular bone features. These features were performed by [13][15]. Using both images will be expected increase the performances of detection. The model is expected as an alternative for DXA.

II. RELATED WORKS

A. Panoramic

In study [5], panoramic radiographs of 100 postmenopausal women who had had BMD assessments of the lumbar spine and the femoral neck were used osteoporosis detection. Experienced oral radiologist determined the position of the mental foramen on 100 digitized dental panoramic radiographs. After determination of the mental foramen, mandibular cortical width below the mental foramen was measured automatically with a computer-aided system by identifying the area of interest, enhancing the original image, determining inner and outer margins of the cortex, and selecting an appropriate point. There were statistically significant correlation between cortical width measured by the computer-aided system and spinal BMD and femoral neck BMD. These correlations were similar with those between cortical width by manual measurement and skeletal BMD. Sensitivity and specificity for identifying postmenopausal women with low spinal BMD by the computer-aided system were about 88.0% and about 58.7%, respectively. Those for identifying postmenopausal women with low femoral neck BMD by this system were about 87.5% and about 56.3%, respectively. Cortical width measured by this system was compared with BMD of the lumbar spine and the femoral neck.

In this paper [17], an extraction method of trabecular structures from dental panoramic radiographs using mathematical morphological operations is proposed. It can extract trabeculae excluding roots of teeth and enables the assessment of tooth extraction for trabecular pattern. A measurement method of the lengths and directions of trabecular segments is also proposed in this paper. It is suggested that the measurements of healthy and osteoporotic examples support our hypothesis that the trabeculae parallel to the roots are reduced more than those perpendicular to the roots by osteoporosis.

In this paper [18] proposed a new method for detecting osteoporosis using Weighted Fuzzy ARTMAP from the features measured in dental panoramic radiographs. The method developed an activation match function by integrating Simplified fuzzy ARTMAP and symmetric Fuzzy ART. Fourier method and segmentation processing were applied for obtaining features of a radiograph in frequency and spatial domain. The experimental results for osteoporosis detection show that the new method achieved accuracy of 87.88%, sensitivity of 93.33%, and specificity of 83.33%.

B. Periapical

This study [15] aims to select the important features from the combination of porous trabecular pattern with anthropometric features for osteoporosis screening. The study sample has their bone mineral density (BMD) measured at the proximal femur/lumbar spine using dual-energy X-ray absorptiometry (DXA). Morphological porous features such as porosity, the size of porous, and the orientation of porous are obtained from each dental radiograph using digital image processing. The anthropometric features considered are age, height, weight, and body mass index (BMI). Decision tree (J.48 method) is used to evaluate the accuracy of morphological porous and anthropometric features for selection data. The study shows that the most important feature is age and the considered features for osteoporosis screening are porosity, vertical pore, and oblique pore. The decision tree has considerably high accuracy, sensitivity, and specificity.

Reference [19] used the dental periapical radiograph images for extracting porous trabecular features. Then, the decision tree with C4.5 method was performed to obtain selected porous features. The usage of confusion matrix to evaluation performance neural network classification had the accuracy, sensitivity, specificity to be 85.71%, 86.90 %, and 85.84%, respectively. Calculating the area under the ROC curve (AUC) results 0.8171 or 81.71%.

III. MATERIALS

A. Subjects

Ethical clearance for this study was obtained from the unit and advocacy ethics of Dentistry Faculty, Universitas Gadjah Mada, Yogyakarta, Indonesia. The research sample obtained from a previous study [10][13] [15] on Javanese Indonesian women who have undergone menopause. The inputs of model were 69 images of the panoramic and periapical radiograph.

B. Dental X-Ray

All periapical X-Ray images were collected from the Department of Radiology of Prof. Soedomo Dental Hospital, Faculty of Dentistry Universitas Gadjah Mada, as in [10][15]. Panoramic radiograph performed using Panora deluxe dental X-ray unit with the voltage setting, currents, strong, and successive exposure time, were 70-80 kVp, 12mA, and 12 s. The panoramic radiography processing is done digitally using DBSWin 4.5, Durr Dental. In [16] also used these images for obtaining the correlation between the trabecular texture features and BMD. Fig.1 shows the periapical and the panoramic images.

A. B.

Fig. 1. Dental Periapical X-Ray Image, B. Dental Panoramic X-Ray

C. BMD

Assessment of BMD on femoral neck and lumbar spine carried out from the Department of Radiology Dr. Sardjito Hospital using densitometer DXA. The specifications of DXA are 76kV, 1.5mA, during 1 min 14s (femoral), and 1 min 27s (spine). We classified subjects into one of three groups according to the WHO classification. These BMD were also used in [10][13][14][15]. But, in this study, we used only classification which was normal (N) and osteoporosis (OP).

IV. METHODOLOGY AND DESIGN

A. Methodology

On Fig. 2 shows research methodology. The first step is selection ROIs from the panoramic and the periapical images. Each image of panoramic was selected 3 ROI from anterior, right posterior, and left posterior. For each periapical image was selected 1 ROI. So, we had 4 ROI for a subject. The mandibular trabecular bone images obtained from each ROI subsequently processed using digital image method as in [10][13][15]. The second step is images processing on all ROI which are segmentation and porous feature extraction. After segmentation, we extracted the shape-based features of the porous trabecular images. The third step is feature selection. For obtaining the potential features as the predictor of osteoporosis, we selected these features using the decision tree method. The class targets were normal (N) and osteoporosis (OP). Finally, the selected features were used as input for detection. The last steps are detection and evaluation. On detection process, 15 data were tested using decision tree by tracing from root to the node of the tree, on selected features. The performance of detection was shown using confusion matrix.

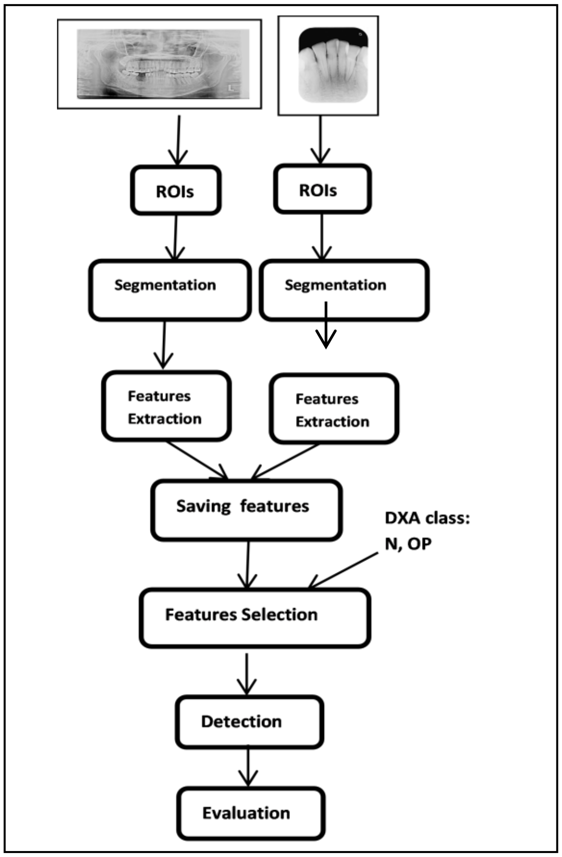


Fig. 2. Research Methodology

V. RESULT

Fig. 3 shows the examples of the selection of ROI anterior 100x100 pixels, the right posterior ROI 92x85 pixels, and the left posterior ROI 92x85 pixels, using methods that have been implemented in previous studies [10][15].

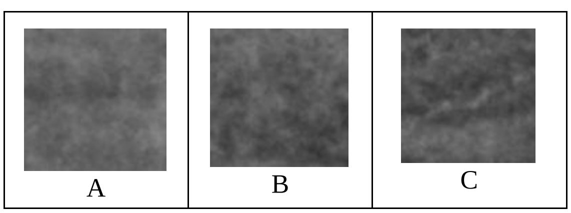


Fig. 3. Result of the panoramic ROIs: A. anterior, B. right posterior, C. left posterior

The example of the segmentation on ROI images is a binary image as shown in Fig. 4. Also, it was used a software as in [10][13][14].

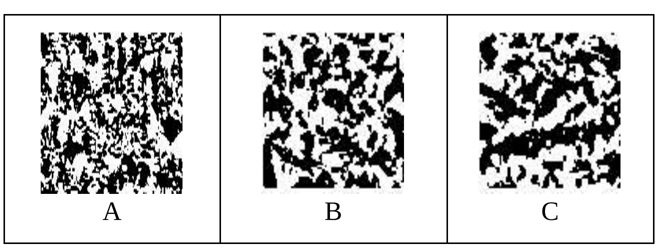


Fig. 4. Segmented the panoramic images A. anterior, B. right posterior, C. left posterior

Then, shape-based porous trabecular features were extracted from binary images. This process obtained 6 features on each ROI, so there were totally 24 features on a subject. The name of the features was based on the main characteristics of the porous i.e the porosity, the size of pore, and orientation of the pore [10][13][15]. Furthermore, these features are named according to the ROI location and characteristics. A total of 24 features were obtained : `OAnPor (porosity anterior), OAnJK (small pore anterior), OAnJB (large pore anterior), OAnV (vertical pore anterior), OAnH (horizontal pore anterior), OAnM (pore anterior oblique), OKaPor (right posterior porosity), OKaJK (small pore posterior right), OKaJB (large pore posterior right), OKaV (right posterior vertical pore), OKaH (right posterior horizontal pore), OKaM (pore sloping right posterior), OKiPor (left posterior porosity), OKiJK (small pore posterior left), OKiJB (large pore posterior left), OKiV (left posterior vertical pore), OKiH (left posterior horizontal pore), and OKiM (left posterior oblique pore)`. The features were extracted from the periapical images: `Por (porosity), JK (small pore), JB (large pore), V (pore oblique), H (pore horizaontal)`, and `M (pore oblique)`. The result of selection features using decision tree was the major features as the predictor of osteoporosis (Fig. 5).

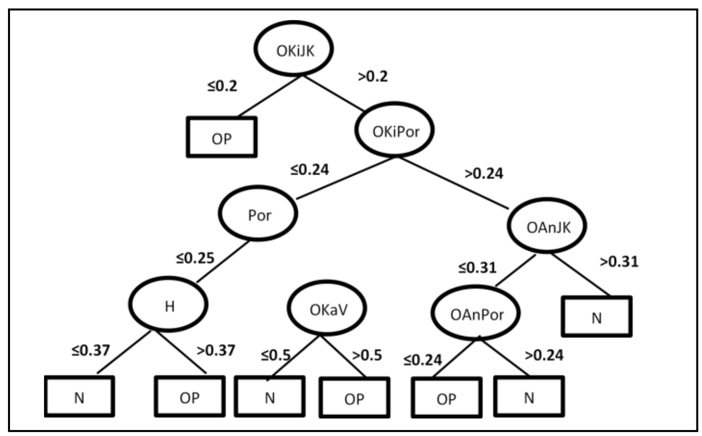


Fig. 5. ROI of trabecular bone from digitized X-Ray

Of the 24 features, there are 7 features that play a role in the detection of osteoporosis: `OKiJK, OkiPor, Por, OanJK, H, OkaV`, and `OanPor`. Table 1 shows the result of evaluation of training on 54 data. From 54 data, 49 data can be detected correctly. It consists of 30 as normal class and 19 as osteoporosis class. Thus the average value of sensitivity was 90.69%, and the average value of specificity was 90 055%. Furthermore, the selected features were used for testing on 15 data. Table 1 shows the confusion matrix as the results of testing process.

TABLE I. CONFUSION MATRIX

	Normal (N)	Osteoporosis (OP)	Total
Normal (N)	7	2	9
Osteoporosis (OP)	2	4	6
Total	9	6	15

The selection of features was used in training phase. This method had been performed in previous studies [10] [11] [15] but these studies used mandibular trabecular ROI on periapical and panoramic radiographs separately. In this study, an important feature on the detection of osteoporosis using panoramic and periapical radiograph images is porosity. It is represented at the left anterior, the right anterior, and the periapical. Moreover, small pore at the left posterior and anterior, horizontal pore on the periapical, vertical pores in the left posterior also contribute for osteoporosis screening. These results are similar to previous studies [15] which state that the most important feature on the detection of osteoporosis using periapical radiograph image is the porosity. The most important features found in this research that features small pore on the part of the left posterior (`OkiJK`) is similar to the study [13], but it did not make the process of detection of osteoporosis. Accuracy value of this research is using the panoramic and periapical images which is still not as good as the accuracy of the value of research [5][17][18][19]. The difference of value occurs because (1) the type of image that is used in all four studies did not use the panoramic and the periapical images, (2) the difference in the number of images, (3) extracted features method, and (4) methods of identification. This study is one of the first steps to build an intelligent system of detection of osteoporosis using either dental panoramic and periapical radiograph images. The idea of drafting an intelligent system of detection of osteoporosis using dental panoramic radiographs and periapical has been delivered approximately one decade ago [3] [5] [11] [20]. The utilization of dental radiographs to build an intelligent system requires a multidisciplinary collaboration involving dentists and developers of computer systems. Dentists play a role as experts who can interpret radiographs, as well as a user of the intelligent system that will be built. Several studies are still being developed, but studies using both the panoramic and the periapical radiographic images for Indonesian are still very limited.

VI. Conclusion

Based on the research that has been done, there can be drawn some conclusion as follows:

1) The proposed model could performed for osteoporosis detection using the selected porous trabecular bone features

2) Using the decision tree, the selected features for the detection of osteoporosis on panoramic and periapical images are `OKiJK`, `OkiPor`, `Por`, `OanJK`, `H`, `OkaV`, *and* `OanPor`

3) The results of performance detection obtained accuracy, sensitivity, specificity are 73.33%, 72.23%, and 72.23%, respectively.

For further study, there needs to be plan to carry out detection of osteoporosis using supervised learning methods. The class is a class that used normal, osteopenia, and osteoporosis.

References

[1] H.I. Othman, and S.A. Ouda, Mandibular radiomorphometric measurements as indicators of possible osteoporosis in celiac patients. JKAU: Med. Sci., vol.17, no.2, pp.21-35, DOI: 10.4197/Med. 17-23, 2010.

[2] M. Primiarti, B. Kiswanjaya, and H.B. Iskandar, Radiographic evaluation of osteopororsis through detection of jaw bone changes: a simplified early osteoporosis detection effort, Makara Kesehatan, vol.14, no.2, pp.51-56, 2010.

[3] S.C. White, Oral radiographic predictor of osteoporosis, Dentomaxillofac. Radiol, vol.31, pp. 84-92, 2001.

[4] P.C.A. Watanabe, A. Farmer, M.G.C. Watanabe, and J.P.M Issa, 2008, Radiographic signal detection of systemic disease: Orthopantomographic radiography, Int. J. Morphol., vol.26, no.4, pp.915-926, 2009.

[5] A.Z. Arifin, A. Asano, A. Taguchi, T. Nakamoto, M. Ohtsuka, and K. Tanimoto, Computer-aided system for measuring the mandibular cortical width on panoramic radiographs in osteoporosis diagnosis, Proceeding of the SPIE Medical Imaging, vol. 5747, pp.813-821, 2005.

[6] G.M. Blake, and I. Fogelman, The role of DXA bone density scans in the diagnosis and treatment of osteoporosis, Postgrad Med J., vol.83, pp.509-517, 2007.

[7] T. Nakamoto, A. Taguchi, M. Ohtsuka, Y. Suei, M. Fujita, M. Tsuda, M. Sanada, Y. Kudo, A. Asano, and K. Tanimoto, A computer-aided diagnosis system to screen for osteoporosis using dental panoramic radiographs, Dentomaxillofac. Radiol, vol.37, pp. 274-281, 2008.

[8] A. Gulsahi, S. Ozden, A.I. Cebeci, N.O. Kucuk, C.S. Paksoy, and Y. Genc, The relationship between panoramic radiomorfometric indices and the femoral bone mineral density of edentulous patients, Oral Radiol, vol.25, pp.47-52, 2009.

[9] M.L. Brandi, Microarchitechture: the key to bone quality. Rheumatology, vol.48, pp.iv3-iv8, 2008.

[10] E.I Sela, S. Hartati, A. Harjoko, R. Wardoyo, and Munakhir MS, Segmentation on the dental periapical X-Ray images for osteoporosis screening, IJACSA, vol.4, no.7,pp. 147-151, DOI: 10. 14569/IJACSA.2013.040720, July 2013.

[11] R. Licks, V. Licks, F. Ouriqe, H.R. Bittencourt, and V. Fontanella, Development of a prediction tool for low bone mass based on clinical data and periapikal radiography, Dentomaxillofac. Radiol., vol.39, pp. 224-230, 2010.

[12] BD. Lee, and S.C. White., Age and trabecular features of alveolar bone associated with osteoporosis, Oral Surg Oral Pathol Oral Radiol Endod, Elsevier Inc., 2005.

[13] E.I. Sela, and R. Widyaningrum, Pemilihan fitur bentuk porus tulang trabekula mandibula pada radiograf panoramik untuk deteksi osteoporosis, Proceeding Forsila II ISBN: 9786021145135, Unisula Press, Semarang, 2005.

[14] R. Widyaningrum, and S. Lestari, The correlation between mandible trabecular texture parameter on panoramic radiograph with bone mass density, Proceeding of The International Symphosium of Advanced Clinical Approach for The Prevention of Dental Caries and Implicated Diseases, Yogyakarta, Indonesia, pp. 206-214, 2013

[15] E.I Sela, S. Hartati, A. Harjoko, R. Wardoyo, and Munakhir MS, Feature selection of the combination of porous trabecular with anthropometric features for osteoporosis screening, IJECE, vol.5, no.1, pp 78-83, ISSN: 2088-8708, DOI: 10. 11591/ijece v5i1. 6922, 2015.

[16] W.G.M. Geraets, J.G.C. Verheij, P.F. van der Stelt, K. Horner, C. Lindh, K. Nicopoulou-Karayianni., R. Jacobs, E.J. Marjonovic, J.E. Adams, and H. Devlin, Selecting Regions of Interest on Intraoral radiographs for Predictions of Bone Mineral Density, Dentomaxillofac Radiol, vol. 37, pp. 375-379, 2008.

[17] A. Asano, T. Tambe, A.Taguchi, C.M. Asano, 2006, Extraction of trabecular structures of mandible excluding tooth roots on dental panoramic radiographs using mathematical morphology, vol.3, 2006.

[18] D. Herumurti , A.Z Arifin, R. Sulaeman, A. Asano, A Taguchi, T. Nakamoto , K. Uchimura, Weighted Fuzzy ARTMAP for Osteoporosis Detection, 16th Korea-Japan Joint Workshop on Frontiers of Computer Vision, 2008.

[19] E.I. Sela, S. Hartati, A, Harjoko, R. Wardoyo, M. Mudjosemedi, Dissertation: Shape-based features extraction model of the porous trabecular bone on the dental periapical radiograph images for osteoporosis screening, Universitas Gadjah Mada, Yogyakarta, 2014.

[20] Kemenkes RI. Keputusan Menteri Kesehatan Republik Indonesia No. 1142/Menkes/SK/XII/2008 tentang Pedoman Pengendalian Osteoporosis.

AATCT: Anonymously Authenticated Transmission on the Cloud with Traceability

Maged Hamada Ibrahim
Department of Electronics, Communications and Computers Engineering
Faculty of Engineering, Helwan University
1, Sherif St., Helwan, P.O. Box 11792, Cairo, Egypt

***Abstract*—In Cloud computing, anonymous authentication is an important service that must be available to users in the Cloud. Users have the right to remain anonymous as long as they behave honestly. However, in case a malicious behavior is detected, the system – under court order – must be able to trace the user to his clear identity. Most of the proposed authentication schemes for the Cloud are either password-based authentication schemes that are vulnerable to offline dictionary attacks, or biometric-based authentication schemes that take a long time of execution specially in case of high security requirements. In this paper, we propose an efficient and secure scheme to non-interactively authenticate the users on the Cloud to the remote servers while preserving their anonymity. In case of accusations, the registration authority is able to trace any user to his clear identity. We avoid using low entropy passwords or biometric mechanisms, instead, we employ pseudonym systems in our design. The computation complexity and storage requirements are efficient and suitable to be implemented on smart cards/devices. Our proposed scheme withstands challenging adversarial attacks such as, stolen databases attacks, databases insertion attacks, impersonation attacks, replay attacks and malicious users/servers collaboration attacks.**

Keywords*—*Cloud computing; anonymous transmission; pseudonym systems; smart cards; mobile devices; authentication; IT security

I. INTRODUCTION

Cloud computing paradigm is becoming an interesting new technology in the recent years with companies of all sizes accessing the Cloud. As cost efficiency, unlimited storage, backup and recovery, automatic software integration, easy access to information stand out as advantages, security services still need attention. Efficient security services for the Cloud is a major demand for all organizations. The Cloud has many security issues as it coordinates many technologies such as networking, virtualization, memory and database management. In Cloud security, authentication is the most important factor with the need for well-defined authentication strategies. One of the first steps toward securing an IT system is to verify the authentic identity of its users [1]. Authentication is generally referred to as a mechanism that establishes the validity of the claimed identity of the individual. There are basically four approaches to achieve authentication services: *Something known* (e.g. cryptographic keys, passwords, PINs, etc.), *Something possessed* (e.g. tokens, devices or cards, etc.), *Something an individual is* (e.g. fingerprints or voice patterns, face, eye retina, etc.), *Something an individual does* (e.g. history of Internet usage). On the other hand, users' identity privacy is also expected in Cloud services. If the access to a Cloud discloses a user's real identity, the user could still be unwilling to accept this issue. Thus, the user authentication without identifying the real identity, also called anonymous authentication [2], [3] is required.

In order to preserve users privacy and allow anonymous authentication/access in a Cloud, users can anonymously authenticate themselves as part of authorized users/groups to the Cloud provider (remote server). Users can anonymously access and modify resources. The encrypted data stored by a user can be decrypted by other members of the same group. Anonymous authentication can also be used in other scenarios such as E-DRM, E-commerce, E-voting, E-library, E-cash, E-auctions as well as some medical applications, and mobile agent applications [4], [5], [6], [3], [7], [8].

The end users do not want to be classified in any manner. In these examples, people may prefer to register only once (e.g. after some payment or being a member) and would like to keep their anonymity and privacy when they use these applications. Therefore, Anonymity is one of the important services that must be available to users in the digital world as long as they behave honestly. Users communication must be kept authentic and anonymous unless malicious behaviors are detected. In this case the accused user's clear identity must be traced and revealed by the system to solve accusations. In the Cloud, anonymity and traceability are two important services, yet, achieving a satisfactory security level for both of them with acceptable complexity is not an easy task due to the contradicting requirements: anonymous transmission must not be traceable by any individual while if a transmission is traceable, then anonymity is threatened.

Many of the previous contributions in the area of authenticating remote users to remote servers in the Cloud are *password-based authentication* protocols which incorporates a user's password (text, graph or picture) in the online authentication process for login and establishing a session key for authenticated transmission between the remote user and the remote server. Such protocols are always vulnerable to offline dictionary attacks whatever the strength of the incorporated passwords since by nature, passwords have to be memorable and hence have very low entropy. On the other hand, many of them do not consider anonymity and traceability of malicious users. Moreover, none of these protocols consider the non-repudiation service where a malicious user and/or server brought to the court cannot deny the transmission. Conventional digital signature schemes with certified public/private key pairs indeed realize the non-repudiation service, yet the transmission is not anonymous because the certificates of the public verification key incorporates the clear identity of the user. Servers and authorities have to store the users' public keys side by side with their clear identities. Many other schemes are biometric-based schemes. Biometric-based authentication requires long execution time and their security level is always constrained by time complexity. Also, the security proofs for such schemes are heuristic. Most of the previously proposed schemes are password-based, biometric based or hybrid of both. These protocols do not preserve anonymity and do not guarantee that a user (in case of a raised dispute) will not be able to deny the transmission. Conventional digital signatures will not help in this case since they are not anonymous.

When anonymous and authenticated transmission is considered, Group signatures (GS) come to play [9], [10], [11], [12]. This cryptographic tool originally introduced in [13] allows members belonging to a group to sign messages on behalf of the group such that, the signature verifier (whether a group member or a non-member) is able to check that the signature is a valid group signature but cannot trace the identity of the signer. In case of a dispute, the trusted authority (group manager) can trace the identity of the signer.

Ring signatures introduced in [14] and further studied in [15] and [16] do not require any group manager to form a group. For signature generation, every user builds a set of public keys that includes his public key and the public keys of other users. A generated signature does not reveal the public key of the signer, but a set of public keys of all possible signers. Therefore, ring signatures cannot be used for a direct communication between a verifier and a signer. Additionally, ring signatures provide unconditional anonymity, i.e., no party can reveal the signers identity. Although ring signatures have many cryptographic applications, they are not suitable for our system since traceability is impossible.

Pseudonym systems were introduced in [17] as a way of allowing a user to work effectively but anonymously with multiple organizations. The author suggests that each organization may know a user by a different pseudonym. These are unlinkable such that two organizations cannot combine their databases to build up a dossier on the user. Nonetheless a user can obtain a credential from one organization using one of his pseudonyms and demonstrate possession of the credential to another organization without revealing his pseudonym to the second organization [18]. One may view pseudonyms as a blinded version of the users clear identities.

In our construction in this paper, we use ideas from [19], [20], [21], [22], [17], [18] and proofs of knowledge primitives from [23], [24] to devise an efficient and secure message authentication scheme to allow users to communicate anonymously with the remote servers on the Cloud in an authenticated way while in case of a dispute, the user can be traced to his clear identity to solve accusations. Our scheme is of low complexity so that it is suitable to be implemented on devices with limited resources. The authentication phase in our scheme is non-interactive, i.e. in one-move, a user is able to establish a session key with the remote server.

Paper organization: This paper is organized as follows: In section II, a study of previous and related work in the field is presented. Section III describes the motivations behind the work in this paper and also our contribution. In section IV, we describe the cryptographic tools used to construct our scheme. Our assumptions and network model are given in section V. The concrete description of our AATCT scheme is presented in section VI. The security of the proposed AATCT scheme is analyzed in section VII. The efficiency of the scheme is evaluated in section VIII. Discussions and suggested improvements are given in section IX. Finally, the conclusions of our work are given in section X.

II. Related Work

Password Authentication System (PAS) [25] for Cloud Environment uses graphical passwords. Graphical-based password techniques are developed as a potential alternative to text-based techniques, supported partially by the fact that humans can remember images better than text. Psychologists have confirmed that images are more memorable and usable than text. However, graphical passwords still hard to manage and store, still of low entropy and for high security levels requires a long time for execution and a huge amount of storage. Thus, they are also constrained by time and storage complexities. Yet, graphical passwords could be fine for securing personal devices.

Multi-dimensional password generation technique for the purpose of accessing Cloud services [26] considers multiple input parameters of Cloud paradigm referred to as multidimensional passwords. The multidimensional password is generated by considering the parameters of Cloud paradigm such as: vendor details, consumer details, services, privileges and confidential inputs such as logos, images, textual information and signatures. All these dimensions combined together produce a multidimensional password. By doing so, the probability of brute force attack for breaking the password can be reduced to a large extent. It was shown that the reduction in the probability of successful hacking improves drastically with the increase in the dimension of the input. However, based on the required level of security, one can decide the dimensions for the input. Major concerns are that the processing time increases with the increase in the dimensions of input parameters.

In textual based password authentication [2] users do not need to register their passwords to a service provider. The Users are supplied with the necessary credential information from the data owner. Furthermore, to enable the service provider to know the authorized users, data owner provides the service provider with some secret identity information that is derived from the pair (username/password) of each user. The protocol consists of three stages; setup, registration, and authentication. Setup and registration stages are executed only once, and the authentication stage is executed whenever a user wishes to login. In the setup and registration stages, the user registers her/his identity (username and password) with Data Owner. Data Owner then provides public system parameters to the service provider and each user on a secure channel.

Identity-based hierarchical model (IBHM) [27] for Cloud computing is composed mainly of three levels: The top level (level- 0) represent the root private key generator (PKG). The level-1 is sub-PKGs. Each node in level-1 corresponds to a data-center (such as a Cloud Storage Service Provider) in the

Cloud computing. The bottom level (level-2) are users in the Cloud computing. In identity based hierarchal model of Cloud computing (IBHMCC), each node has a unique name, the name is the node's registered distinguished name (DN) when the node joins the Cloud storage service. The identity of a node is the DN string from the root node to the current node itself. The deployment of IBHMCC needs two modules, namely, root PKG setup and lower level setup which provides secret keys to all nodes. The IBHM does not provide anonymity service to the users.

A biometric authentication as a service on Cloud [28] uses Single Sign On/Off (SSO) property for authentication. SSO is a property of access control of multiple related, but independent software systems. The blind protocol technique reveals only the user's identity. As the protocol is based on asymmetric encryption of the biometric data, it captures the advantages of biometric authentication as well as the security of public key cryptography. During the registration process, the user enrolls with the biometric system which is provided by a Cloud, once the identity is registered his/her biometric authentication details are stored in a Cloud service provider database. The authorization details are also entered at the registration time which is then stored in encrypted format. Once authenticated, the user is redirected to the actual Cloud service for which he is authorized to use.

A 3-D password authentication system [29] combines Recognition, Recall, Tokens and Biometrics in one authentication system. The 3-D password is a multi-factor authentication scheme. It can combine all existing authentication schemes into a single 3-D virtual environment. This 3-D virtual environment contains several objects or items with which the user can interact. The type of interaction varies from one item to another. The 3-D password is constructed by observing the actions and interactions of the user and by observing the sequences of such actions. The user has the flexibility of selecting the type of authentication techniques that will be the part of their 3-D password. This is achieved through interacting with the objects that acquire information that the user is comfortable in providing and ignoring the objects that request information that the user prefers not to provide. Other schemes that are based on biometrics in establishing the authentication service are found in [30], [31], [32]. The authors in [32] proposed an authentication scheme known as Cloud cognitive authenticator (CCA). It applies one round zero knowledge protocol for authentication. CCA is an API designed for Cloud environment that integrates bio-signals, knowledge proof and Rijndaels algorithm. CCA improves security in a public Cloud by providing bi-level authentication. It also provides encryption and decryption of user identities. Electro dermal responses are used for first level authentication. The main advantage of CCA compared to other existing models is that it provides two levels of authentication combined with the encryption algorithm.

The problem with biometric-based authentication schemes is that they take a long time for execution, thus, their security level is constrained by time complexity. Also, the security level achieved by such schemes is heuristic. Finally, we recommend the reader to refer to [33] for a survey and a demonstration on the weaknesses associated with password-based authentication and why it is considered a weak link in Cloud computing technologies in general.

III. Motivations and Contribution

A. Motivations

The work in this paper is motivated by the observation that most of the previously proposed schemes for the purpose of achieving anonymous and authenticated transmission on the Cloud are password-based schemes whether these passwords are memorized or extracted from biometric patterns. Their purpose is to authenticate the users and the servers in the Cloud and establish a session key (extracted from the password) to secure the session. Passwords in general suffer from their low entropy and when they are incorporated in the communication on the link for authentication, they are always vulnerable to password guessing attacks, specially offline dictionary attacks [33]. Also there is no clear strategy how the user is traced to his clear identity in case of a dispute. Biometric-based authentication schemes require long execution time and their security level is always constrained by time complexity. Also, the security proofs for such schemes are heuristic. Most of these protocols do not preserve anonymity and do not guarantee that a user (in case of a raised accusation) will not be able to deny the session. Conventional digital signatures will not help in this case since they are not anonymous.

B. Our contribution

In this paper we devise a message authentication scheme suitable for authenticated communication on the Cloud. Our scheme avoids using passwords and biometrics in the authentication process and does not require any interaction between a user and the remote server by any means prior to the establishment of the session. The users and the remote servers interact only with the registration authority. While the communication of the user and the server is anonymous, in case of a dispute, the registration authority is able to trace the user to his clear identity and prove the transmission. In this case, a traced user cannot deny the transmission. Our scheme's computation and storage complexities are suitable for implementation on the user's smart device with limited resources and also for smart card implementation. In our scheme, the user is able to setup a session key with the remote server in a one move non-interactive way. The computations required by the user can be performed offline. Our scheme withstands challenging adversarial attacks such as, stolen databases attacks, databases insertion attacks, impersonation attacks, replay attacks and malicious users/servers collaboration attacks.

IV. Cryptographic Primitives

In this section we describe the cryptographic primitives used in building our AATCT scheme.

A. Diffie-Hellman problem (DHP)

Let p and q be two large primes such that $q|p-1$ that is there is an integer k satisfying $p = kq + 1$. Pick $a \in_R Z_p^*$ and compute $g = a^k \mod p$. If $g \neq 1$ then g is a generator of order q in Z_p. Now pick $x \in_R Z_q^*$ where $|x| = |q|$ and compute $y = g^x \mod p$. Given (q, p, g, y) it is computationally infeasible to compute $x = \log_g y$.

B. Computational Diffie-Helman problem (CDHP)

Let (p, q, g) be as above. Pick two large integers $a, b \in_R Z_q^*$ and compute $A = g^a \mod p$ and $B = g^b \mod p$. Now given (q, p, g, A, B), it is computationally intractable to compute $g^{ab} \mod p$ without knowing a and b.

C. Decisional Diffie-Helman problem (DDHP)

Let (p, q, g) be as above. Pick three large integers $a, b, r \in_R Z_q^*$ and compute $A = g^a \mod p$ and $B = g^b \mod p$. Now given (q, p, g, A, B), it is computationally intractable to distinguish $g^{ab} \mod p$ from $g^r \mod p$ without knowing a, b and r.

D. Proof of equality of two discrete logarithms

We review the protocol of [23], [24] and also in [22] that is believed to be a zero knowledge proof of equality of two discrete logarithms. In this protocol, the public parameters are two large primes p and q such that $q|p-1$, two elements $\alpha, \beta \in Z_p^*$ and the two quantities $G_1, G_2 \in Z_p^*$. The prover ($\mathcal{P}$) proves to a verifier ($\mathcal{V}$) that he knows $x \in Z_q^*$ such that $G_1 = \alpha^x$ mod$p$ and $G_2 = \beta^x \mod p$. The protocol is as follows:

- $\mathcal{P} \rightarrow \mathcal{V}$: Choose $r \in_R Z_q^*$ and send ($A = \alpha^r$ mod$p$, $B = \beta^r$ mod$p$).
- $\mathcal{V} \rightarrow \mathcal{P}$: Choose $c \in_R Z_q^*$ and send c.
- $\mathcal{P} \rightarrow \mathcal{V}$: Compute and send $y = r + cx$ mod$q$.
- $\mathcal{V}$: Check that $\alpha^y = AG_1^c$ mod$p$ and $\beta^y = BG_2^c$ mod$p$.

The above protocol can be made non-interactive (we denote it, $\Pi_{LogEq} \leftarrow P_{LogEq}(\alpha, \beta, G_1, G_2, x)$) using a sufficiently strong hash function $\mathcal{H}$ and setting $c = \mathcal{H}(A, B)$. The NIZK proof of knowledge protocol Π_{LogEq} becomes as follows:

- $\mathcal{P} \rightarrow \mathcal{V}$: Choose $r \in_R Z_q^*$ and send ($A = \alpha^r$ mod$p$, $B = \beta^r$ mod$p$, $c = \mathcal{H}(A, B)$ and $y = r + cx$ mod$q$.
- $\mathcal{V}$: Check that $\alpha^y = AG_1^c$ mod$p$ and $\beta^y = BG_2^c$ mod$p$.

V. Assumptions and Model

The main entities in our protocol, as illustrated in Figure 1, are: The registration authority (RA), the remote server (RS) and the Cloud user U_i. The RA is assumed fully trust to manage all secret parameters in the system while the RS as well as U_i could behave maliciously and could collaborate trying to disclose the privacy of other users in the system. We assume the existence of a PKI, such that RA and each remote server RS has its own certified public/private key pair to realize authenticated and private channels among all entities. We emphasize that the users in our scheme may use the servers' certified public keys but they are not related to this PKI.

Our scheme does not incorporate any users' passwords in the authentication process. Yet, personal PIN may be used by the user to secure his own smart card. Our scheme allows any user to anonymously establish a session secret key using the remote server's public key. The users do not interact with each other or the remote server RS, they interact only with the RA for registration and setup. Then after the registration phase is completed, any registered user can communicate anonymously with any remote server in the Cloud. Finally, in the description of our protocol we focus on the anonymity of the user. Later we show how mutual anonymity is achieved.

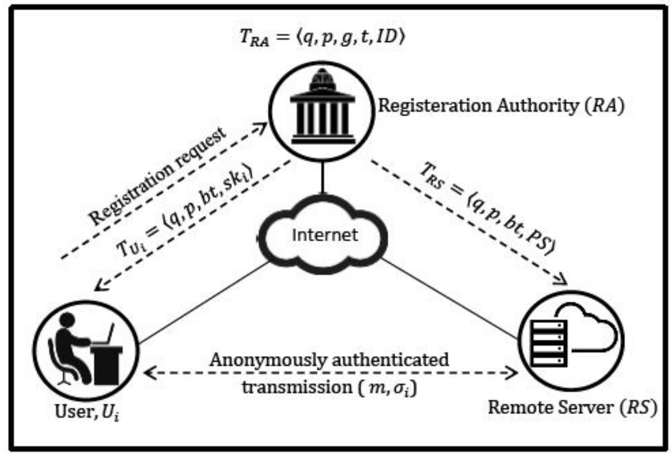


Fig. 1. Our AATCT scheme and architecture

VI. Concrete Description of our AATCT Scheme

In this section we give a detailed description of our AATCT. There is a registration authority RA and a remote Cloud server RS. There is a remote user U among the set of Cloud users. The RA and each remote server RS has his own certified public/private key pair to allow regular authenticated and confidential communications. The phases of our scheme are described next.

A. Initialization phase by the RA

The RA initializes the system parameters as follows:

- Picks two large primes p and q where $q|(p-1)$ and a generator g of order q in Z_p^*.
- Picks a secret tracing trapdoor parameter $t \in_R Z_q^*$ and computes its blinded version $bt = g^t \mod p$.

B. Registration phase

The RA registers a user U_i as follows:

- Picks $x_i \in_R Z_q^*$ as U_i's private key and computes $id_i = g^{x_i} \mod p$ as U_i's public identity.
- Computes U_i's pseudonym as $ps_i = (id_i)^t \mod p$.
- Parses U_i's secret key $sk_i = (x_i, ps_i)$.
- On U_i's smart card, RA installs the tuple,
$$T_{U_i} = \langle q, p, bt, sk_i \rangle$$

Let $\mathcal{ID} = \{id_1, ..., id_n\}$ be the set of the users' clear identities while $\mathcal{PS} = \{ps_1, ..., ps_n\}$ be the set of the users' pseudonyms. The RA signs and publishes to each remote server RS the tuple,

$$T_{RS} = \langle q, p, bt, \mathcal{PS} \rangle$$

The RA finalizes the registration phase by storing the tuple,

$$T_{RA} = \langle q, p, g, t, \mathcal{ID} \rangle$$

and erasing all other parameters.

Remark. In the registration phase we assumed that RA generates the private key x_i and computes the identity id_i for U_i. It is possible that U_i by himself generates his own private key, computes and sends his identity to RA. He can also compute his pseudonym $ps_i = (bt)^{x_i}$. However, in this case, U_i must provide a proof of knowledge of x_i. Notice that in this case, RA does not know the private key x_i which avoids the key escrow problem. The choice is left to the organization.

C. Authentication phase

User U_i anonymously signs a message m using his private key sk_i as follows:

- Picks a random integer r, hashes m as $H = \mathcal{H}(m, r)$ and computes $z = H^{x_i}$ mod$p$.
- Generates a NIZK proof of knowledge, $\Pi_{LogEq} \leftarrow P_{LogEq}(H, bt, z, ps_i, x_i)$, which proves that $\log_H(z) = \log_{bt}(ps_i) = x_i$.
- Parses σ_i as $(r, z, ps_i, \Pi_{LogEq})$. σ_i is U_i's anonymous signature on m.

On the reception of a signature σ_i on m, RS verifies as follows:

- Parses σ_i as $(r, z, ps_i, \Pi_{LogEq})$.
- Ensures that $ps_i \in \mathcal{PS}$.
- Runs the verification algorithm, $V_{LogEq}(H, bt, z, ps_i, \Pi_{LogEq})$, if the verification failed, then reject m and abort. Else, accept σ_i as a valid signature on m.

Notice that, a remote server is able to reply by a message dedicated to a particular user U_i by simply including his pseudonym ps_i in the replied message. Moreover, ps_i is indeed a the public key of U_i that could be used to encrypt messages to U_i as will be discussed later.

D. Tracing an accused user

In case of a dispute and under court order, given a pseudonym ps_i, RA is able to trace the identity of U_i by simply computing $(ps_i)^{1/t} = id_i$ where t^{-1} is computed modulo q.

E. Establishing a session key

A user U_i anonymously establishes an authenticated session key K in a one move non-interactive way by simply setting $m = E_{pk_{RS}}(K)$ where $E_{pk_{RS}(.)}$ is an encryption using RS's public key pk_{RS}.

VII. Security Analysis

The secrecy of the tracing trapdoor parameter t is very important for retaining the anonymity service of our scheme, since it is the only parameter that can trace any pseudonym ps_i to its clear identity id_i. From the Diffie-Hellman problem (DHP), no information is revealed to a computationally bounded adversary about t from its blinded version $bt = g^t \mod p$. The same infeasibility follows for the user's private key x_i and his clear identity $id_i = g^{x_i} \mod p$. The remote server RS is delivered the set of pseudonyms $\mathcal{PS}$ with no information revealed about t or any of the x_i's. From the Decisional Diffie-Hellman problem (DDHP), even if a randomly permuted version of the sets $\mathcal{ID}$ and $\mathcal{PS}$ are known to an adversary, she cannot trace any $ps_i = (id_i)^t \mod p$ to its clear identity id_i since she cannot distinguish $g^{x_i t}$ from g^r for a random r. We want to emphasize that neither $\mathcal{ID}$ nor $\mathcal{PS}$ are necessarily kept secret, only the correspondence is secret.

In the authentication phase, U_i computes $z = H^{x_i} \mod p$ as his signature on a message m and parses this signature with his ps_i, notice that RS knows the set $\mathcal{PS}$ and hence it is easy to check whether $ps_i \in \mathcal{PS}$. Now U_i must prove to RS that his secret key x_i used to compute z is the same value in the exponent of bt to compute the ps_i and consequently U_i parses the signature with the NIZK proof of equality of discrete-log, $\Pi_{LogEq} \leftarrow P_{LogEq}(H, bt, z, ps_i, x_i)$ to prove that $\log_H(z) = \log_{bt}(ps_i) = x_i$. This proves to RS that the anonymous signer is indeed a registered user.

Since Π_{LogEq} is a zero knowledge proof of knowledge, a verifier that receives a signed message with a certain pseudonym ps_i is faced with the DHP problem to compute x_i given bt and $(bt)^{x_i}$. Given the set of identities $\mathcal{ID}$ and pseudonyms $\mathcal{PS}$ the DDHP preserves the anonymity of the signer.

From the discussion above, in case of a dispute and under court order, only RA, the holder of the tracing trapdoor parameter t, can disclose the clear identity id_i from a given pseudonym ps_i by computing $(ps_i)^{t^{-1}} = id_i$, where t^{-1} is computed modulo q.

Mutual authentication is achieved since U_i encrypts the session key K using RS's public key. Only RS with the corresponding private key is able to decrypt for K. Both entities can test the validity of K at the beginning of the session.

In the following we discuss possible adversarial attacks, the countermeasures to be taken against these attacks and how our scheme withstands them.

A. RS compromise

An adversarial compromise of RS does not threaten the security and anonymity of any user. Actually, one may have noticed that none of the parameters delivered to RS is secret.

B. RA database compromise

Beyond the tracing trapdoor parameter t, compromising the database of RA and stealing $\mathcal{ID}$ does not threaten the anonymity of any of the users without the knowledge of t.

C. Stolen RS and RA databases

Beyond the tracing trapdoor parameter t, if all other parameters are stolen by an adversary, i.e., if the adversary steals the set $\mathcal{ID}$ and the set $\mathcal{PS}$ from RA and RS, she cannot map any pseudonym ps_i to any clear identity id_j without knowing the tracing trapdoor parameter t. Given a stolen id_i and ps_i, an adversary cannot create a valid authenticated message without the knowledge of x_i.

D. Impersonation/emulation/masquerade attacks

An adversary trying to impersonate a legal user u_i by using his pseudonym ps_i will not succeed in creating the NIZK proof of knowledge without knowing his private key x_i.

E. Databases Insertion attacks

An adversary that is able to gain access to RA and RS databases is able to insert a valid pair (id_A, ps_A) as to become registered in the system. There are variety of countermeasures to withstand such attack. One solution is that, the RA signs all entries in her database using her own digital signature key. Also, each remote server RS signs each entry in the $\mathcal{PS}$ database using his own digital signature key. In this case, the adversary's insertions in the databases become invalid as these entries are not digitally signed. Another more efficient solution is to hash each entry in the database using a keyed hash (e.g. message authentication code (MAC)) and append this hash with the corresponding entry in the database. In this case an adversary – without knowing the secret key – will not be able to append a correct hash to the pair (id_A, ps_A), and hence the entry in the database is invalid.

F. Replay attacks

Like any other digital signature scheme, replay attacks are avoided by a simple association of a time-stamp mechanism. Also, one may consider random nonce and sequence numbers.

G. User compromise

The private key x_i of the user U_i is stored on his smart card which is a tamper proof device and hence an adversary will not be able to reach x_i. Any other parameter on the user's side other than x_i, if known to an adversary, does not threaten the security of this user. If a certain x_i of a user U_i is revealed to an adversary, this does not threaten other users in the system. However, for this particular user, if his x_i is revealed, he must re-register for a new private key.

H. Users-servers collaboration attacks

It is possible that several malicious minority of the users are willing to collaborate with the remote servers in order to disclose privacy of other users. Malicious users are willing to reveal their private keys x_i's, their identities $id_i = g^{x_i}$ and their pseudonyms $ps_i = g^{x_i t}$. In our scheme each user private parameters are completely independent of any other user in the system. From the CDHP/DDHP, the revealed information does not allow the collaborated entities to reveal any information about the tracing trapdoor parameter t and hence, the security of the rest of the users is preserved.

VIII. Efficiency Evaluation

To evaluate the efficiency of our scheme, we assume the standard number theoretic settings on the size of the big prime p and the small prime q where $|p|$=1024 bits = 128 bytes while $|q|$=160 bits = 20 bytes. Also, roughly we have, $|g| = |bt| = |ps_i| = |id_i| = |p|$ while $|x_i| = |t| = |q|$.

A. Complexity evaluation

A concrete evaluation of the computations and storage complexities for each party in our system is shown next. Let n be the number of registered users in the system.

1) Complexity of the RA: The RA stores the tuple, $T_{RA} = \langle q, p, g, t, \mathcal{ID} \rangle$ requiring a storage of $2|q| + 2|p| + n|p|$ which totals $(296+128n)$ bytes. On the other hand, in the registration phase, the RA computes for each user his identity id_i and his pseudonym ps_i each of which is a one modular exponentiation. In the tracing algorithm the RA performs only on modular exponentiation to reveal id_i.

2) Complexity of the RS: The RS receives the tuple $T_{RS} = \langle q, p, bt, \mathcal{PS} \rangle$ which requires a storage of $|q| + 2|p| + n|p|$ totaling $(276 + 128n)$ bytes. On the reception of a signed message from the user, the RS runs the verification algorithm by computing $V_{LogEq}(H, bt, z, ps_i, \Pi_{LogEq})$. This algorithm requires the computation of four modular exponentiations and two modular multiplications.

3) Complexity of the user: The user U_i receives and stores the tuple $T_{U_i} = \langle q, p, bt, sk_i \rangle$ where $sk_i = (x_i, ps_i)$. This tuple requires $2|q| + 3|p|$ of storage which totals 424 bytes of memory. In computing a signature $\sigma_i = (r, z, ps_i, \Pi_{LogEq})$, we ignore the hashing since it is cheap. U_i performs one modular exponentiation to compute z, two modular exponentiations, one modular multiplication and one modular addition to compute Π_{LogEq}. The storage requirements and computation complexity of our system are summarized in Table I.

4) Communication complexity: The user U_i transmission is a message m concatenated with a fixed length anonymous signature $\sigma_i = (r, z, ps_i, \Pi_{LogEq})$. We have $|\Pi_{LogEq}| = 2|p| + |q|$ in addition to $2|p|$ for z and ps_i. This totals 532 bytes of communications overheads in addition to a few bytes for r. The communication complexity of our system is summarized in Table II.

TABLE I. *Storage requirements and computations*

	Storage (in bytes)	Modulo computations		
		Exponentiations	Multiplications	Additions
RA	296+128n	3 per user	-	-
RS	276+128n	4	2	-
User	424	3	1	1

TABLE II. *Communication complexity*

	Communications (in bytes)
RA→RS	276+128n
RA→User	424
User→RS	$\|m\|$+532

B. Computation time and energy consumption

In the following, the time required by the user to prepare his authentication message is evaluated on smart cards and mobile devices. An estimation of the energy consumed by our scheme on mobile devices is also given. These are summarized in Table III and described next.

1) Computation time on smart cards: The basic method (binary method) for computing modular exponentiations is through the square-and-multiply strategy. For an k-bit exponent, this method requires $k-1$ squarings and on the average of $1.5(k-1)$ multiplications. From Table I, the user requires three modular exponentiations, one modular multiplication and one modular addition. Benchmarks on Smart-card devices [34] shows that on an Oberthur ld-one v7.0-a, one modular exponentiation of 160 bits exponent and 1024 bits modulus takes 190 ms, one modular multiplication on two 1024 bits numbers and 1024 bits modulus takes 200 ms. The modular addition and hash invocations are a negligible fraction of milliseconds. Hence, it takes the user 3(190)+200 plus few fractions of milliseconds resulting in about 800 ms to generate an authentication message. Computation time on other smart cards could be deduced from [34]. We remind the reader that these computations could be performed offline.

2) Computation time on mobile devices: An implementation of modular arithmetic on an ASUS-TF300T tablet shows that a modular exponentiation of 160 bits exponent and 1024 bits modulus takes 4 ms, one modular multiplication on two 1024 bits numbers and 1024 bits modulus takes 0.1 ms. Hence, it takes only about 13 milliseconds to generate an authentication message on a mobile device. The computation time of modular arithmetic operations on other smart phones could be found in [34].

3) Energy consumption: In this part, the energy consumed by cryptographic operations is used to evaluate the schemes. This time, we use a low-processor and 64 MB memory running Windows Mobile 5.0 for pocket pc[1]. According to PXA270, the typical power consumption of PXA270 in active is 500 mW. Therefore, using the computation time in the previous calculations, we can calculate the corresponding energy consumption. For example, if it takes 13 ms to generate the authentication message, the energy consumption is approximately 13(500/1000) = 6.5 mJ.

TABLE III. *Computation time and energy consumption*

Device	Computation time	Energy Consumption
Oberthur ld-one v7.0-a smartcard	800 ms	
ASUS-TF300T tablet	13 ms	
Pocket PC with Intel PXA270		6.5 mJ

C. Simple key management

In the proposed scheme, the key management is very simple since only the tracing trapdoor parameter t is required to be kept secret by RA. On the user's side, only his private key x_i is required to be kept secret. On the server's side, no parameter is required to be kept secret. The private keys for the PKI are already there and are not due to our scheme. Notice that, the users are not part of this PKI.

[1]http://pdf.dzsc.com/cxx/nhpxa270cxxx.pdf

IX. Discussions and Improvements

A. Users join and leave

The RA easily manage the joining of a new user to the system by running the setup phase for him, adding his new identity to the set $\mathcal{ID}$ and notify the RS with the new pseudonym. Also leaving the group (revoking a user) is as simple as erasing the user from $\mathcal{ID}$ and $\mathcal{PS}$.

B. User's embedded El-gamal public/private key pair

Recall that $bt = g^t \mod p$, where g is a generator of order q on the form $g = a^k \mod p$ for $a \in_R Z_q^*$ and $k = (p-1)/q$. We have $bt = (a^t)^k \mod p$ and hence, bt is indeed a generator of order q. Thus, the pair (x_i, ps_i) where $ps_i = (bt)^{x_i}$ could be used as the user's U_i El-gamal public/private key pair for an El-gamal cryptosystem [35]. A remote server RS may encrypt a message m for U_i as follows: Picks $\mu \in_R Z_q^*$, computes the El-gamal ciphertext $C = (A, B)$ where $A = (bt)^\mu \mod p$ and $B = m(ps_i)^\mu \mod p$. Only U_i, the holder of the corresponding private key x_i, is able to decrypt C for m where $m = B/A^{x_i} \mod p$.

C. Mutual anonymity

We focused in our AATCT scheme on the anonymity of the user since it is the most important. Although servers' anonymity to the users is much less important (sometimes is undesired), it could be achieved by treating the servers in the Cloud as a group in the same way the users were treated and assign an identity and a pseudonym sets for them. However, the storage requirements on the user's side will grow linearly with the number of communicating servers in the Cloud.

D. Further Improvements

The cryptographic number theoretic tools used in devising our scheme could be replaced with Elliptic Curve (EC) tools where in this case the storage and computation time are improved by more than 20% [36]. The security of the tracing trapdoor parameter t could be further improved by applying threshold cryptographic techniques [37], [38], [39] to distribute the trust among several entities. Although in our AATCT, the user U_i stores a tuple $T_{U_i} = \langle q, p, bt, sk_i \rangle$ where $sk_i = (x_i, ps_i)$, the user may not store ps_i preserving 128 bytes of storage. However, this requires the user to compute ps_i each time a signature is performed. On the other hand, the RA may store the set of secret keys $\{x_1, ..., x_n\}$ instead of the set of identities $\mathcal{ID}$ preserving a significant amount of space ($20n$ bytes instead of $128n$ bytes). However, although it allows key recovery, this requires countermeasures for managing the privacy of the secret keys.

E. Future work

1) Deniable transmission: Another important service that must be available to users on the Cloud is deniable transmission, which allows a user on the Cloud to escape a coercion attempted by a coercive adversary. Such an adversary approaches the coerced user after transmission forcing him to reveal all his random inputs used during encryption or decryption. Since traditional encryption schemes commits the user to his random inputs, the user is forced to reveal the true values of all his random inputs (including the encrypted/decrypted messages and the encryption/decryption keys) which are verifiable by this coercer using the intercepted ciphertext. In this scenario, a coercer may force the user to perform actions against his own beliefs. For more information about this notion, please refer to [40], [41], [42]. A deniable encryption helps to protect the users in many applications such as E-voting, E-elections and E-auctions where coercive actions come to play as a potential threat.

2) Forward security: It would be nice if one is able to efficiently realize forward security in our scheme where the blinded identity and the user's private key is updated at regular intervals so as to provide a forward security property: compromise of the current private key does not enable an adversary to forge signatures pertaining to the past. This can be useful to mitigate the damage caused by key exposure.

3) Reducing transmission overheads and complexity: One may also work on a way to reduce the bit-length of the user's signature to reduce transmission overheads. For example, finding a way to minimize the burden of the proofs of knowledge and the modular exponentiations. Working on elliptic curves would greatly improves the bit-length of all parameters as well as the computation time.

X. Conclusions

In this paper, we proposed an efficient scheme to realize anonymous authentication for Cloud computing networks based on pseudonym systems which allows a user to non-interactively establish an authenticated channel with the remote server while a registration authority is always able to trace the user to his clear identity in case of a dispute. We avoided using passwords and biometrics in the design of our scheme. Our scheme could be regarded as an anonymous signature scheme for the Cloud where a user cannot later repudiate the transmission. We designed our system in a way that the storage requirements and computation complexity for the user is suitable for mobile devices and also for smart card implementation. A complete security analysis and efficiency evaluation was presented. Our scheme requires few milliseconds to prepare the authentication message on mobile devices and few hundred milliseconds to prepare the authentication message on a smart card. Moreover, since the scheme is non-interactive, the user can prepare this message offline. Our scheme allows a user to non-interactively establish a session key with any of the remote servers in a fully private, authenticated and anonymous way. Our scheme withstands challenging attacks such as, stolen databases attacks, databases insertion attacks, impersonation attacks, replay attacks, and malicious users/servers collaboration attacks. Finally, we discussed further possible improvements to the scheme and suggested several future work for other researchers in the field to add other services and improve the proposed scheme.

Acknowledgment

The author of this paper would like to thank the anonymous reviewers of the IJACSA for their valuable and helpful comments.

References

[1] B. Guttman and E. A. Roback, *An introduction to computer security: the NIST handbook*. DIANE Publishing, 1995.

[2] A. A. Yassin, H. Jin, A. Ibrahim, W. Qiang, and D. Zou, "Efficient password-based two factors authentication in cloud computing," *International Journal of Security and Its Applications*, vol. 6, no. 2, pp. 143–148, 2012.

[3] M. H. Ibrahim, "Noninteractive, anonymously authenticated, and traceable message transmission for vanets," *International Journal of Vehicular Technology*, vol. 2009, 2010.

[4] M. H. Ibrahim, "Secure and robust enterprise digital rights management protocol with efficient storage," *International journal on information (information-Tokyo)*, vol. 18, no. 2, pp. 625–640, 2015.

[5] M. H. Ibrahim, "Efficient robust and secure E-DRM with encrypted content search," *International journal on information (information-Tokyo)*, vol. 18, no. 6(A), pp. 2531–2546, 2015.

[6] M. H. Ibrahim, "A novel approach to fully private and secure auction: A sealed-bid knapsack auction," *International Journal of Research and Reviews in Applied Science (IJRRAS)*, vol. 9, no. 2, 2011.

[7] A. H. Soliman, M. H. Ibrahim, and A. E. El-Hennawy, "Improving security and efficiency of enterprise digital rights management," in *proceedings of the 6th IEEE International Conference on Computing, Communications and Networking Technologies (ICCCNT 2015)*. IEEE, July 2015.

[8] M. H. Ibrahim, "Secure anonymously authenticated and traceable enterprise DRM system," *International Journal of Computer Applications*, vol. 126, no. 3, pp. 1–9, September 2015.

[9] A. Kiayias and M. Yung, "Group signatures with efficient concurrent join," *Advances in Cryptology–EUROCRYPT 2005*, pp. 198–214, 2005.

[10] M. Bellare, H. Shi, and C. Zhang, "Foundations of group signatures: The case of dynamic groups," *Topics in Cryptology–CT-RSA 2005*, pp. 136–153, 2005.

[11] J. Camenisch and J. Groth, "Group signatures: Better efficiency and new theoretical aspects," *Security in Communication Networks*, pp. 120–133, 2005.

[12] M. Bellare, D. Micciancio, and B. Warinschi, "Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions," *Advances in Cryptology–Eurocrypt 2003*, pp. 614–629, 2003.

[13] D. Chaum and E. Van Heyst, "Group signatures," in *Advances in Cryptology–EUROCRYPT'91*. Springer, 1991, pp. 257–265.

[14] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in *Advances in CryptologyASIACRYPT 2001*. Springer, 2001, pp. 552–565.

[15] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy*. Springer, 2004, pp. 325–335.

[16] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," in *Theory of Cryptography*. Springer, 2006, pp. 60–79.

[17] D. Chaum, "Security without identification: Transaction systems to make big brother obsolete," *Communications of the ACM*, vol. 28, no. 10, pp. 1030–1044, 1985.

[18] A. Lysyanskaya, R. L. Rivest, A. Sahai, and S. Wolf, "Pseudonym systems," in *Selected Areas in Cryptography*. Springer, 2000, pp. 184–199.

[19] M. Manulis, A. R. Sadeghi, and J. Schwenk, "Linkable democratic group signatures," *Information Security Practice and Experience*, pp. 187–201, 2006.

[20] M. Manulis, "Democratic group signatures: on an example of joint ventures," in *Proceedings of the 2006 ACM Symposium on Information, computer and communications security*. ACM, 2006, pp. 365–365.

[21] J. K. Liu, V. K. Wei, and D. S. Wong, "Linkable spontaneous anonymous group signature for ad hoc groups," in *Information Security and Privacy*. Springer, 2004, pp. 325–335.

[22] M. H. Ibrahim, "Resisting traitors in linkable democratic group signatures." *IJ Network Security*, vol. 9, no. 1, pp. 51–60, 2009.

[23] C.-P. Schnorr, "Efficient signature generation by smart cards," *Journal of cryptology*, vol. 4, no. 3, pp. 161–174, 1991.

[24] D. Chaum and T. P. Pedersen, "Wallet databases with observers," *Advances in Cryptology–CRYPTO92*, pp. 89–105, 1993.

[25] A. Bhavana, V. Alekhya, K. Deepak, and V. Sreenivas, "Password authentication system (PAS) for cloud environment," *International Journal of Advanced Computer Science and Information Technology*, vol. 2, no. 1, p. 29, 2013.

[26] V. Agrawa *et al.*, "Multi-dimensional password generation technique for accessing cloud services," *arXiv preprint arXiv:1207.3636*, 2012.

[27] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *Cloud computing*. Springer, 2009, pp. 157–166.

[28] H. Vallabhu and R. Satyanarayana, "Biometric authentication as a service on cloud: Novel solution," *International Journal of Soft Computing and Engineering*, vol. 2, no. 4, p. 163, 2012.

[29] D. Pooja, G. Shilpi, S. Sujata, and G. Vinita, "Secured authentication: 3d password," *International Journal of Engineering and Management Sciences*, vol. 3, no. 2, pp. 242–245, 2012.

[30] A. A. Pawle and V. P. Pawar, "Face recognition system (FRS) on cloud computing for user authentication," *International Journal of Soft Computing and Engineering (IJSCE)*, vol. 3, 2013.

[31] P. Wang, C.-C. Ku, and T. C. Wang, "A new fingerprint authentication scheme based on secret-splitting for enhanced cloud security," 2011.

[32] L. Jivanadham, Y. Katayama, S. Komaki, S. Baharun *et al.*, "Cloud cognitive authenticator (cca): A public cloud computing authentication mechanism," in *Informatics, Electronics & Vision (ICIEV), 2013 International Conference on*. IEEE, 2013, pp. 1–6.

[33] W. Page, "http://searchcloudsecurity.techtarget.com/tip/password-based-authentication-a-weak-link-in-cloud-authentication."

[34] J. Hajny, L. Malina, Z. Martinasek, and O. Tethal, "Performance evaluation of primitives for privacy-enhancing cryptography on current smart-cards and smart-phones," in *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2014, pp. 17–33.

[35] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469–472, 1985.

[36] D. Hankerson and A. Menezes, "Nist elliptic curves," in *Encyclopedia of Cryptography and Security*. Springer, 2011, pp. 843–844.

[37] M. H. Ibrahim, "Eliminating quadratic slowdown in two-prime RSA function sharing," *I. J. Network Security*, vol. 7, no. 1, pp. 106–113, 2008.

[38] M. H. Ibrahim, I. I. Ibrahim, and A. H. El-Sawy, "Fast three-party shared generation of rsa keys without distributed primality tests," in *in Proceedings of the Information Systems: New Generations (ISNG'04)*, 2004.

[39] M. H. Ibrahim, I. A. Ali, I. I. Ibrahim, and A. El-sawi, "A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme," in *Circuits and Systems, 2003 IEEE 46th Midwest Symposium on*, vol. 1. IEEE, 2003, pp. 276–280.

[40] M. H. Ibrahim, "Efficient coercion resistant public key encryption," *International Journal of Computer Science and Security (IJCSS)*, vol. 8, no. 1, pp. 1–24, 2014.

[41] M. H. Ibrahim, "Realizing sender's deniability in public key encryption via random coins isolation," *European Journal of Scientific Research*, vol. 119, no. 2, pp. 177–187, 2014.

[42] B. Meng, "A critical review of receipt-freeness and coercion-resistance," *Information Technology Journal*, vol. 8, no. 7, pp. 934–964, 2009.

Resistance to Statistical Attacks of Parastrophic Quasigroup Transformation

Verica Bakeva, Aleksandra Popovska-Mitrovikj and Vesna Dimitrova
University "Ss Cyril and Methodius" - Skopje,
Faculty of Computer Science and Engineering,
P.O. Box 393 1000 Skopje,
Republic of Macedonia

***Abstract*—The resistance to statistical kind of attacks of encrypted messages is a very important property for designing cryptographic primitives. In this paper, the parastrophic quasigroup PE-transformation, proposed elsewhere, is considered and the proof that it has this cryptographic property is given. Namely, it is proven that if PE-transformation is used for design of an encryption function then after n applications of it on arbitrary message the distribution of m-tuples ($m = 1, 2, \dots, n$) is uniform. These uniform distributions imply the resistance to statistical attack of the encrypted messages. For illustration of theoretical results, some experimental results are presented as well.**

***Keywords*—uniform distribution; cryptographic properties; statistical attack; encrypted message; quasigroup; parastrophic quasigroup transformation**

I. Introduction

Quasigroups and quasigroup transformations are very useful for construction of cryptographic primitives, error detecting and error correcting codes. The reasons for that are the structure of quasigroups, their large number, the properties of quasigroup transformations and so on. The quasigroup string transformations E and their properties were considered in several papers.

A quasigroup $(Q, *)$ is a groupoid (i.e. algebra with one binary operation $*$ on the finite set Q) satisfying the law:

$$(\forall u, v \in Q)(\exists! x, y \in Q) \quad (x * u = v \ \& \ u * y = v) \tag{1}$$

In fact, (1) says that a groupoid $(Q, *)$ is a quasigroup if and only if the equations $x * u = v$ and $u * y = v$ have unique solutions x and y for each given $u, v \in Q$.

In the sequel, let $A = \{1, \dots, a\}$ be an alphabet of integers ($a \geq 2$) and denote by $A^+ = \{x_1 \dots x_k | \ \ x_i \in A, \ k \geq 1\}$ the set of all finite strings over A. Note that $A^+ = \bigcup_{k \geq 1} A^k$, where $A^k = \{x_1 \dots x_k | \ x_i \in A\}$. Assuming that $(A, *)$ is a given quasigroup, for any letter $l \in A$ (called leader), Markovski and al. (see [5]) defined the transformation $E = E_l^{(1)} : A^+ \to A^+$ by

$$E(x_1 \dots x_k) = y_1 \dots y_k \Leftrightarrow \left\{ \begin{array}{lcl} y_1 & = & l * x_1, \\ y_i & = & y_{i-1} * x_i, \quad i = 2, \dots, k \end{array} \right. \tag{2}$$

where $x_i, y_i \in A$. Then, for given quasigroup operations $*_1, *_2, \dots, *_n$ on the set A, we can define mappings $E_1, E_2, \dots, E_n$, in the same manner as previous by choosing fixed elements $l_1, l_2, \dots, l_n \in A$ (such that E_i is corresponding to $*_i$ and l_i). Let

$$E^{(n)} = E^{(n)}_{l_n, \dots, l_1} = E_n \circ E_{n-1} \circ \dots \circ E_1,$$

where $\circ$ is the usual composition of mappings ($n \geq 1$). It is easy to check that the mappings E is a bijection. In the same paper, authors proposed a transformation $E^{(n)}$ as an encryption function and proved the following theorem.

Theorem 1. *Let $\alpha \in A^+$ be an arbitrary string and $\beta = E^{(n)}(\alpha)$. Then m-tuples in β are uniformly distributed for $m \leq n$.*

Also, in Theorem 2 in [1], Bakeva and Dimitrova proved that the probabilities of $(n+1)$-tuples in $\beta = E^{(n)}(\alpha)$ are divided in a classes where $a = |A|$, if $(p_1, p_2, \dots, p_a)$ is the distribution of letters in an input string and $p_1, p_2, \dots, p_a$ are distinct probabilities, i.e., $p_i \neq p_j$ for $i \neq j$. Each class contains a^n elements with the same probabilities and the probability of each $(n+1)$-tuple in i-th class is $\dfrac{1}{a^n} p_i$, for $i = 1, 2, \dots, a$. If $p_{i_1} = p_{i_2} = \dots = p_{i_\nu}$ for some $1 \leq i_1 < \dots < i_\nu \leq a$, then the classes with probabilities $\dfrac{1}{a^n} p_{i_1} = \dfrac{1}{a^n} p_{i_2} = \dots = \dfrac{1}{a^n} p_{i_\nu}$ will be merged in one class with νa^n elements. Using these results, the authors proposed an algorithm for cryptanalysis.

In paper [4], Krapez gave an idea for a new quasigroup string transformation based on parastrophes of quasigroups. A modification of this quasigroup transformation is defined in [2]. In [3], authors showed that the parastrophic quasigroup transformation has good properties for application in cryptography. Namely, using that transformation the number of quasigroups of order 4 useful in cryptography is increased. To complete the proof of goodness of parastrophic quasigroup transformation for cryptography, it is needed to prove that Theorem 1 holds for that transformation, too. It will guarantee that message encrypted by the parastrophic quasigroup transformation will be resistant to a statistical kind of attacks.

In Section II, we briefly repeat the construction of parastrophic quasigroup transformation given in [2]. In Section III, we give the theoretical proofs that PE-transformation guaranties a resistance to statistical kind of attacks. Some experimental results (in order to illustrate the theoretical results) are presented in Section IV. In Section V, we make some conclusions about the goodness of PE-transformation for application in cryptography.

II. Parastrophic transformation

Recall that every quasigroup $(Q, *)$ has a set of five quasigroups, called parastrophes denoted with $/, \backslash, \cdot, //, \backslash\backslash$ which are defined in Table 1.

TABLE I: Parastrophes of quasigroup operations $*$

Parastrophe operations				
$x\backslash y = z$	$\iff$	$x * z = y$		
$x/y = z$	$\iff$	$z * y = x$		
$x \cdot y = z$	$\iff$	$y * x = z$		
$x//y = z$	$\iff$	$y/x = z$	$\iff$	$z * x = y$
$x\backslash\backslash y = z$	$\iff$	$y\backslash x = z$	$\iff$	$y * z = x$

In this paper the following notations for parastrophe operations is used:

$$f_1(x, y) = x * y, \quad f_2(x, y) = x\backslash y, \quad f_3(x, y) = x/y,$$
$$f_4(x, y) = x \cdot y, \quad f_5(x, y) = x//y, \quad f_6(x, y) = x\backslash\backslash y.$$

Let $M = x_1 x_2 \dots x_k$ be an input message. Let d_1 be an random integer such that $(2 \le d_1 < k)$ and l be random chosen element (leader) from A. Also, let $(A, *)$ be a quasigroup and $f_1, \dots, f_6$ be its parastrophe operations.

Using previous transformation E, for chosen l, d_1 and quasigroup $(A, *)$ we define a parastrophic transformation $PE = PE_{l,d_1} : A^+ \to A^+$ as follows.

At first, let $q_1 = d_1$ be the length of the first block, i.e., $M_1 = x_1 x_2 \dots x_{q_1}$. Let $s_1 = (d_1 \bmod 6) + 1$. Applying the transformation E on the block M_1 with leader l and quasigroup operation f_{s_1}, the following encrypted block is obtained.

$$C_1 = y_1 y_2 \dots y_{q_1 - 1} y_{q_1} = E_{f_{s_1}, l}(x_1 x_2 \dots x_{q_1 - 1} x_{q_1}).$$

Further on, using last two symbols in C_1 we calculate the number $d_2 = 4y_{q_1 - 1} + y_{q_1}$ which determines the length of the next block. Let $q_2 = q_1 + d_2$, $s_2 = (d_2 \bmod 6) + 1$ and $M_2 = x_{q_1+1} \dots x_{q_2 - 1} x_{q_2}$. After applying $E_{f_{s_2}, y_{q_1}}$, the encrypted block C_2 is

$$C_2 = y_{q_1+1} \dots y_{q_2 - 1} y_{q_2} = E_{f_{s_2}, y_{q_1}}(x_{q_1+1} \dots x_{q_2 - 1} x_{q_2}).$$

In general case, for given i, let the encrypted blocks $C_1, \dots, C_{i-1}$ be obtained and d_i be calculated using the last two symbols in C_{i-1}, i.e., $d_i = 4y_{q_{i-1}-1} + y_{q_{i-1}}$. Let $q_i = q_{i-1} + d_i$, $s_i = (d_i \bmod 6) + 1$ and $M_i = x_{q_{i-1}+1} \dots x_{q_i - 1} x_{q_i}$. Applying the transformation $E_{f_{s_i}, y_{q_{i-1}}}$ on the block M_i the obtained encrypted block is

$$C_i = E_{f_{s_i}, y_{q_{i-1}}}(x_{q_{i-1}+1} \dots x_{q_i}).$$

Now, the parastrophic transformation is defined as

$$PE_{l,d_1}(M) = PE_{l,d_1}(x_1 x_2 \dots x_n) = C_1 || C_2 || \dots || C_r, \quad (3)$$

where $||$ is a concatenation of blocks. Note that the length of the last block M_r may be shorter than d_r (depends on the number of letters in the input message). The transformation PE is schematically presented in Figure 1.

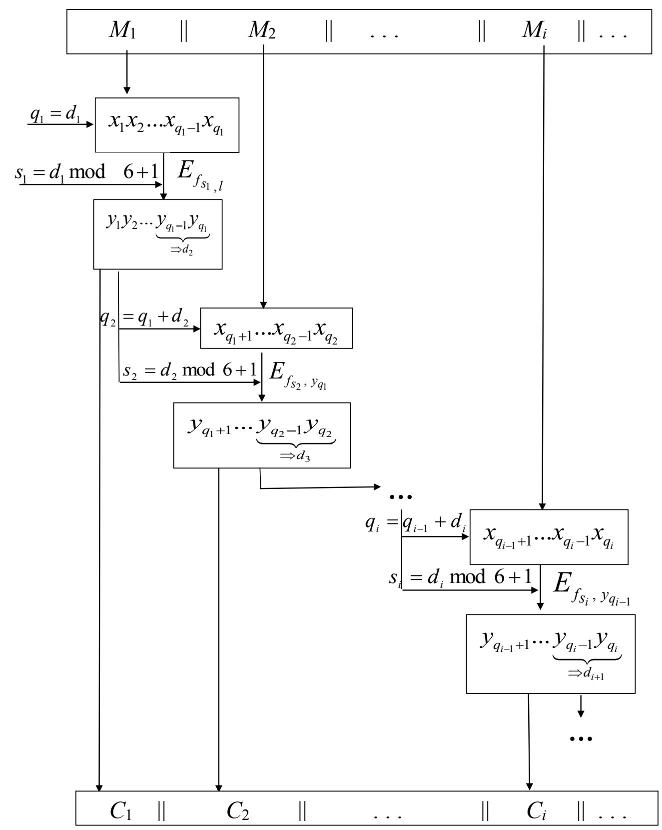


Fig. 1: Parastrophic transformation PE

For arbitrary quasigroup on a set A, random leaders $l_1, \dots l_n$ and random lengths $d_1^{(1)}, \dots, d_1^{(n)}$, we define mappings PE_1, PE_2, $\dots$, PE_n as in (3) such that PE_i is corresponding to $d_1^{(i)}$ and l_i. Using them, we define the transformation $PE^{(n)}$ as follows:

$$PE^{(n)} = PE^{(n)}_{(l_n, d_1^{(n)}), \dots, (l_1, d_1^{(1)})} = PE_n \circ PE_{n-1} \circ \dots \circ PE_1,$$

where $\circ$ is the usual composition of mappings.

III. Theoretical proof for resistance to statistical kind of attacks

Let the alphabet A be as above. A randomly chosen element of the set A^k can be considered as a random vector $(X_1, X_2, \dots, X_k)$, where A is the range of X_i, $i = 1, \dots, k$. Let consider these vectors as input messages. The transformation $PE = PE_{l,d_1} : A^+ \to A^+$ can be defined as:

$$PE_{l,d_1}(X_1,\dots,X_k) = (Y_1,\dots,Y_k) \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} Y_1 = f_{s_1}(l, X_1), \\ Y_j = f_{s_1}(Y_{j-1}, X_j),\ j = 2,\dots,d_1, \\ \\ Y_{q_i+j} = f_{s_{i+1}}(Y_{q_i+j-1}, X_{q_i+j}),\ \begin{matrix} i = 1,\dots,r-1, \\ j = 1,\dots,d_{i+1} \end{matrix} \end{cases} \tag{4}$$

Let $(p_1, p_2, ..., p_a)$ be the probability distribution of the letters $1, ..., a$ in an input message. That implies $p_i > 0$ for each $i = 1, 2, ..., a$ and $\sum_{i=1}^{a} p_i = 1$.

An important property of one transformation for application in cryptography is the uniform distribution of the substrings in the output message $(Y_1,\dots,Y_k)$. This property guarantee the resistance to statistical attack. Therefore, we investigate the distribution of substrings in the output message obtained using PE-transformation. At first we will prove that after applying the transformation $PE^{(1)}$ on an input message α, the letters in transformed message are uniformly distributed.

Theorem 2. *The letter Y_t has uniform distribution on the set $A = \{1,\dots,a\}$, i.e., $Y_t \sim U(\{1,\dots,a\})$ for each t ($t = 1,2,\dots,k$).*

Proof. In this proof we use the same notations as in construction of parastrophic quasigroup transformation given in the previous section.

At first, note that the leader l can be consider as uniformly distributed random variables on the set A since it is randomly chosen from the set A. Therefore, $l \sim U(\{1,\dots,a\})$, i.e.,

$$P\{l = i\} = \frac{1}{a}, \qquad \text{for each } i \in A.$$

Also, leader l is independent of each letter X_i in the input message.

Let $t = 1$. Using the equation (4) and total probability theorem, for distribution of Y_1, we obtain

$$\begin{aligned} P\{Y_1 = j\} &= P\{f_{s_1}(l, X_1) = j\} \\ &= \sum_{i=1}^{a} P\{l = i\} P\{f_{s_1}(l, X_1) = j | l = i\} \\ &= \sum_{i=1}^{a} \frac{1}{a} P\{f_{s_1}(l, X_1) = j | l = i\} \\ &= \sum_{i=1}^{a} \frac{1}{a} P\{f_{s_1}(i, X_1) = j\} \\ &= \frac{1}{a} \sum_{i=1}^{a} P\{X_1 = f'_{s_1}(i, j)\} \end{aligned}$$

Here, f'_{s_1} is the inverse quasigroup transformation of f_{s_1}, i.e., if $f_{s_1}(u, x) = v$, then $f'_{s_1}(u, v) = x$. Note that if i runs over all values of A then for fixed j, the expression $X_1 = f'_{s_1}(i, j)$ runs over all values of A, too. Therefore,

$$P\{Y_1 = j\} = \frac{1}{a} \sum_{i=1}^{a} P\{X_1 = f'_{s_1}(i, j)\} = \frac{1}{a} \sum_{i=1}^{a} p_i = \frac{1}{a},$$

i.e., $Y_1 \sim U(\{1,\dots,a\})$.

The proof is proceed by induction. Let suppose that $Y_r \sim U(\{1,2,\dots,a\})$. Similarly as previous, using that $f_{s_{r+1}}$ is the parastrophe operation applied in $(r+1)^{th}$ step we compute the distribution of Y_{r+1} as follows.

$$\begin{aligned} P\{Y_{r+1} = j\} &= P\{f_{s_{r+1}}(Y_r, X_{r+1}) = j\} \\ &= \sum_{i=1}^{a} P\{Y_r = i\} P\{f_{s_{r+1}}(Y_r, X_{r+1}) = j | Y_r = i\} \\ &= \sum_{i=1}^{a} \frac{1}{a} P\{f_{s_{r+1}}(i, X_{r+1}) = j | Y_r = i\} \end{aligned}$$

According to definition of parastrophic operation given with (4), one can conclude that the random variables X_{r+1} and Y_r are independent. Applying that in previous equation, we obtain

$$\begin{aligned} P\{Y_{r+1} = j\} &= \sum_{i=1}^{a} \frac{1}{a} P\{f_{s_{r+1}}(i, X_{r+1}) = j\} \\ &= \frac{1}{a} \sum_{i=1}^{a} P\{X_{r+1} = f'_{s_{r+1}}(i, j)\} \\ &= \frac{1}{a}. \end{aligned}$$

As previous, $f'_{s_{r+1}}$ is the inverse quasigroup transformation of $f_{s_{r+1}}$. In the last equation, we use that $X_{r+1} = f'_{s_{r+1}}(i, j)$ runs over all values of A when j is fixed and i runs over all values of A, i.e.

$$\sum_{i=1}^{a} P\{X_{r+1} = f'_{s_{r+1}}(i, j)\} = \sum_{i=1}^{a} p_i = 1.$$

On this way, we proved that Y_t has uniform distribution on the set A, for each $t \geq 1$.

From the Theorem 2 the following can be concluded. If $M \in A^k$ and $C = PE_{l,d_1}(M)$ then the letters in the message C are uniformly distributed, i.e., the probability of the appearance of a letter i at the arbitrary place of the string C is $\frac{1}{a}$, for each $i \in A$.

Theorem 3. *Let $M \in A^+$ be an arbitrary string and $C = PE^{(n)}(M)$. Then the m-tuples in C are uniformly distributed for $m \leq n$.*

Proof. Let $(Y_1^{(n)}, Y_2^{(n)}, \dots, Y_k^{(n)}) = PE^{(n)}(X_1, X_2, \dots, X_k)$. This theorem will be proved by induction. For $n = 1$, the statement is satisfied according to Theorem 2. Let suppose that the statement is satisfied for $n = r$, i.e., $(Y_{t+1}^{(r)}, Y_{t+2}^{(r)} \dots Y_{t+m}^{(r)}) \sim U(\{1,2,\dots,a\}^m)$ for each $1 \leq m \leq r$ and each $t \geq 0$. Now, let $n = r+1$. We consider the distribution of $(Y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} \dots Y_{t+m}^{(r+1)})$ for each $1 \leq m \leq r+1$ and arbitrary t.

$$P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} = y_{t+2}^{(r+1)}, \dots, Y_{t+m}^{(r+1)} = y_{t+m}^{(r+1)}\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, f_{s_{t+2}}(Y_{t+1}^{(r+1)}, Y_{t+2}^{(r)}) = y_{t+2}^{(r+1)}, \dots$$

$$\dots, f_{s_{t+m}}(Y_{t+m-1}^{(r+1)}, Y_{t+m}^{(r)}) = y_{t+m}^{(r+1)}\},$$

where f_{s_j} is the parastrophe operation applied in the step j and f'_{s_j} is its inverse transformation, $j = t+2, \dots, t+m$. Now,

$$P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} = y_{t+2}^{(r+1)}, \dots, Y_{t+m}^{(r+1)} = y_{t+m}^{(r+1)}\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, f_{s_{t+2}}(y_{t+1}^{(r+1)}, Y_{t+2}^{(r)}) = y_{t+2}^{(r+1)}, \dots \\ \dots, f_{s_{t+m}}(y_{t+m-1}^{(r+1)}, Y_{t+m}^{(r)}) = y_{t+m}^{(r+1)}\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r)} = f'_{s_{t+2}}(y_{t+1}^{(r+1)}, y_{t+2}^{(r+1)}), \dots \\ \dots, Y_{t+m}^{(r)} = f'_{s_{t+m}}(y_{t+m-1}^{(r+1)}, y_{t+m}^{(r+1)})\}$$

$$= P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}\} P\{Y_{t+2}^{(r)} = f'_{s_{t+2}}(y_{t+1}^{(r+1)}, y_{t+2}^{(r+1)}), \dots \\ \dots, Y_{t+m}^{(r)} = f'_{s_{t+m}}(y_{t+m-1}^{(r+1)}, y_{t+m}^{(r+1)})\}.$$

The last equality is obtained by using the fact that $Y_{t+1}^{(r+1)}$ is independent of the vector $(Y_{t+2}^{(r)}, \dots, Y_{t+m}^{(r)})$, since $Y_{t+2}^{(r)}, \dots, Y_{t+m}^{(r)}$ are not used for obtaining $Y_{t+1}^{(r+1)}$.

Using the inductive hypothesis $(Y_{t+2}^{(r)}, \dots, Y_{t+m}^{(r)}) \sim U(\{1,2,\dots,a\}^{m-1})$, $Y_{t+1}^{(r+1)} \sim U(\{1,2,\dots,a\})$ and from previous expression we obtain that

$$P\{Y_{t+1}^{(r+1)} = y_{t+1}^{(r+1)}, Y_{t+2}^{(r+1)} = y_{t+2}^{(r+1)}, \dots, Y_{t+m}^{(r+1)} = y_{t+m}^{(r+1)}\}$$

$$= \frac{1}{a} \cdot \frac{1}{a^{m-1}} = \frac{1}{a^m}.$$

So, we have proved that $(Y_{t+1}^{(n)}, Y_{t+2}^{(n)} \dots Y_{t+m}^{(n)}) \sim U(\{1,2,\dots,a\}^m)$ for each $m \leq n$ and each $t \geq 0$.

IV. Experimental results

We made many experiments in order to illustrate our theoretical results. Here an example is given. We have randomly chosen a message M with 1,000,000 letters of the alphabet $A = \{1,2,3,4\}$ with the distribution of letters given in the Table II .

TABLE II: The distribution of the letters in the input message

1	2	3	4
0.70	0.15	0.10	0.05

The quasigroup (5) and its parastrophes are used.

$*$	1	2	3	4
1	1	2	4	3
2	3	4	2	1
3	4	3	1	2
4	2	1	3	4

(5)

After applying $PE^{(3)}$ on M, the encrypted message $C = PE^{(3)}(M)$ is obtained. In each PE-transformation, we chose the length of the first block $d_1 = 3$ and the initial leader $l_1 = 4$.

The distribution of letters in the output C is given in the Table III.

TABLE III: The distribution of the letters in the output message

1	2	3	4
0.2501	0.2393	0.2576	0.2530

It is obvious that the distribution of letters in the output message C is uniform.

The distribution of pairs, triplets and 4-tuples of letters in C are given on the Figure 2, Figure 3 and Figure 4. On the Figure 2, the pairs are presented on the x-axis in the lexicographic order ($'11' \to 1$, $'12' \to 2$, ..., $'44' \to 16$). On the similar way, the triplets and 4-tuples are presented on Figure 3 and Figure 4.

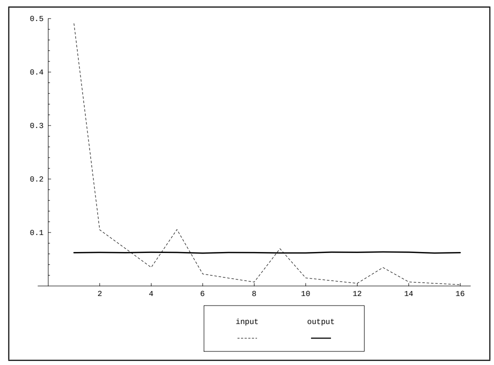


Fig. 2: The distribution of the pairs in the input message and the output message

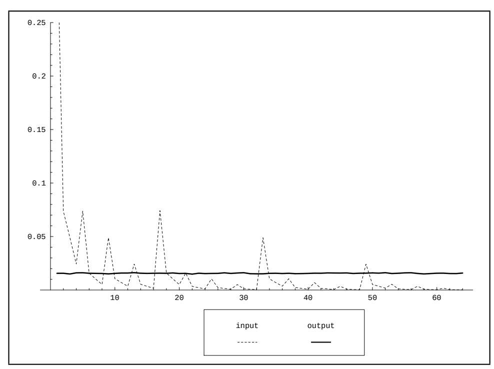


Fig. 3: The distribution of the triplets in the input message and the output message

One can see on Figure 2 and Figure 3 that after three applications of PE-transformations, the pairs and triplets are also uniformly distributed as we proved in Theorem 3. Also, the distribution of the 4-tuples in C is not uniform, but that distribution is closer to the uniform distribution than the distribution of 4-tuples in the input message (see Figure 4).

Next, we check whether Theorem 2 in [1] is satisfied when PE-transformation is applied. The distribution of pairs after one application of PE-transformation is presented on Figure 5. On Figure 6, the distribution of pairs after one application of

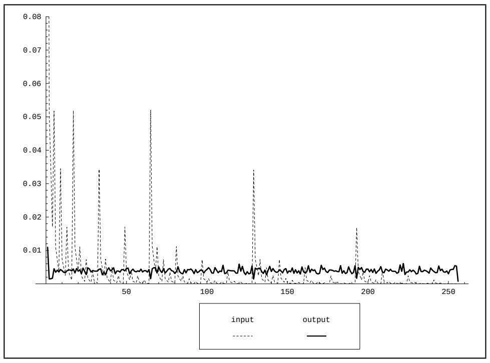


Fig. 4: The distribution of the 4-tuples in the input message and the output message

E-transformation is given. From Figure 6 it can be noticed that probabilities of pairs are divided in 4 classes, as the Theorem 2 in [1] claims. But we cannot distinguish any classes for probabilities on Figure 5. This means that the algorithm for cryptanalysis proposed in [1] cannot be applied when an input message is encrypted by PE-transformation. Therefore encryption by PE-transformation is more resistant to statistical kind of attacks.

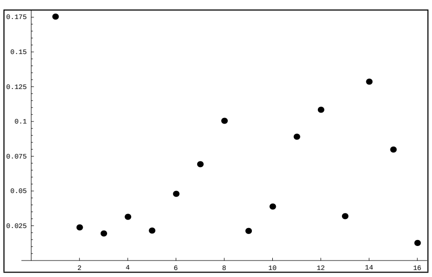


Fig. 5: The distributions of the pairs in output messages obtained by PE-transformation

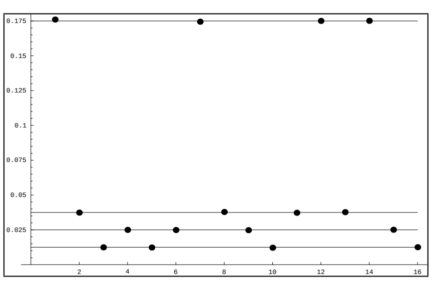


Fig. 6: The distributions of the pairs in output messages obtained by E-transformation

Note that for relevant statistical analyses, it is important to have enough large input message. Namely, in experiments, the probabilities of n-tuples are computed as relative frequencies. So, a relative frequency of an event tends to probability only if we have enough large sample. The relevant statistical analyses cannot be done for shorter message. Therefore, statistical kind of attack is impossible on not enough large input message. Note that if an intruder catches and concatenates a lot of short messages encrypted by the same $PE^{(n)}$-transformation, it will obtain a long message and it can apply a statistical attack. But, the attack will be impossible if quasigroups used in encryption $PE^{(n)}$-transformation is changed more often.

V. Conclusion

In this paper we proved that after n applications of PE-transformation on an arbitrary message the distribution of m-tuples ($m = 1, \ldots, n$) is uniform and we cannot distinguish classes of probabilities in the distribution of $(n+1)$-tuples. This means that if PE-transformation is used as encryption function the obtained cipher messages are resistant to statistical kind of attacks when the number n of applications of PE-transformation is enough large.

In [5], the authors concluded that E-transformation can be applied in cryptography as encryption function since the number of quasigroups is huge one (there are more than 10^{58000} quasigroups when $|A| = 256$) and the brute force attack is not reasonable.

If PE-transformation is used in encryption algorithm then the secret key will be a triplet $(*, l, d_1)$. In that case, the brute force attack also is not possible since except the quasigroup operation $*$ and leader l, the key contains the length of the first block d_1 which has influence of the dynamic of changing of parastrophes.

At the end, in [3] authors proved that PE-transformation has better cryptographic properties than E-transformation for quasigroups of order 4. Namely, some of fractal quasigroups of order 4 become parastrophic non-fractal and they can be used for designing of cryptographic primitives. An investigation for quasigroups of larger order cannot be done in real time since their number is very large.

Finally, from all results we can conclude that PE-transformation is better for design of an encryption function than E-transformation.

Acknowledgment

This research was partially supported by Faculty of Computer Science and Engineering at the University "Ss Cyril and Methodius" in Skopje.

References

[1] V. Bakeva, V. Dimitrova, Some Probabilistic Properties of Quasigroup Processed Strings useful in Cryptanalysis, In: M. Gusev, P. Mitrevski (Eds.) ICT-Innovations 2010, Springer, 2010, pp. 61-70.

[2] V. Bakeva, V. Dimitrova, A.Popovska-Mitrovikj, Parastrophic Quasigrouop String Processing, Proceedings of the 8^{th} Conference on Informatics and Information Technology with International Participants, Macedonia, 2011, pp. 19-21.

[3] V. Dimitrova, V. Bakeva, A.Popovska-Mitrovikj, A.Krapež, Cryptographic Properties of Parastrophic Quasigroup Transformation, In: S. Markovski, M. Gusev (Eds.) ICT-Innovations 2012, Springer, 2012, pp. 221-230.

[4] A. Krapež, An Application Of Quasigroups in Cryptology, Mathematica Macedonica **8**, 2010, pp. 47-52.

[5] S. Markovski, D. Gligoroski, V. Bakeva, Quasigrouop string processing: Part 1, Contributions, Sec. Math. Tech. Sci., MANU, **XX 1-2**, 1999, pp. 13-28.

Fuzzy Based Evaluation of Software Quality Using Quality Models and Goal Models

Arfan Mansoor
Software Architectures and
Product Line Group
Ilmenau University of Technology
Ilmenau, 98693, Germany

Detlef Streitferdt
Software Architectures and
Product Line Group
Ilmenau University of Technology
Ilmenau, 98693, Germany

Franz-Felix Füßl
Software Architectures and
Product Line Group
Ilmenau University of Technology
Ilmenau, 98693, Germany

***Abstract*—Software quality requirements are essential part for the success of software development. Defined and guaranteed quality in software development requires identifying, refining, and predicting quality properties by appropriate means. Goal models of goal oriented requirements engineering (GORE) and quality models are useful for modelling of functional goals as well as for quality goals. Once the goal models are obtained representing the functional requirements and integrated quality goals, there is need to evaluate each functional requirement arising from functional goals and quality requirement arising from quality goals. The process consist of two main parts. In first part, the goal models are used to evaluate functional goals. The leaf level goals are used to establish the evaluation criteria. Stakeholders are also involved to contribute their opinions about the importance of each goal (functional and/or quality goal). Stakeholder opinions are then converted into quantifiable numbers using triangle fuzzy numbers (TFN). After applying the defuzzification process on TFN, the scores (weights) are obtained for each goal. In second part specific quality goals are identified, refined/tailored based on existing quality models and their evaluation is performed similarly using TFN and by applying defuzzification process. The two step process helps to evaluate each goal based on stakeholder opinions and to evaluate the impact of quality requirements. It also helps to evaluate the relationships among functional goals and quality goals. The process is described and applied on 'cyclecomputer' case study.**

***Keywords*—Decision making; Goal Models; Quality Models; NFR; Fuzzy numbers**

I. Introduction

The distinct purpose of software development is to satisfy various stakeholders needs [1]. There are multiple stakeholders involved in the system development and these stakeholders might have different concerns/opinions about the goals to be achieved by the system. Requirements engineering must provide a way to understand stakeholders needs so that high quality software systems are developed. Although stakeholders needs are placed at the most important place, their classification is regarded as the most difficult task. Each stakeholder might have different requirements and sometimes these requirements are of contradicting nature. Therefore, satisfying these requirements is a challenging task [2]. The goal models of goal oriented requirements engineering(GORE) are used to identify and refine the high level goals. Finding the criteria based on GORE require high level goals to be analysed till leaf goals are achieved, that is, until operational requirements are achieved. These leaf level goals are used as criteria for the established high level goals.

There are multiple criteria in one goal model and each criterion may have different importance for various perspective stakeholders, that is, some criteria are more important than others [3]. Stakeholders opinions and preferences should be involved in the process to find the relative importance of each criterion. Normally, there is uncertainty and vagueness about selected criteria because of contradicting stakeholder interests and to find relative importance of criteria according to different stakeholders, one need to perform multi-criteria analysis (MCA). These kind of problems are known as Multi-criteria problems and in general fuzzy set theory is adequate to deal with these problems [4].

Goal Oriented Requirements Engineering (GORE) considers requirements as goals that stakeholders want to be fulfilled. In GORE, goals are refined through AND/OR refinement [5]. By these refinements and by applying heuristics, the functional goals and quality goals are obtained. Functional goals are achieved by operationalization of them either by the system or by external actor while quality goals capture system qualities. The non-functional requirements framework (NFR) [6] deals with the modelling of quality requirements using GORE concepts.

In the context of this paper, GORE is used for identifying and managing the criteria for higher level goals. The leaf level goals help us in establishing the criteria which are used to accumulate stakeholder opinions. These criteria based on stakeholders needs and preferences help to identify the importance of requirements by using qualitative and quantitative reasoning techniques. After the relative importance of each leaf level functional goal, the quality models are used to identify quality goals related to accepted functional goals. Then the impact of quality goals among each other and among functional goals is determined.

The general procedure consists of the following steps:

1) Establishing leaf level functional goals for higher level goals
2) Involving stakeholders opinions
3) Finding scores of each leaf level functional goal
4) Identify quality goals related to functional goals

5) Establish links (contributions) among functional goals and quality goals
6) Measure the impact of quality goals and functional goals
7) Ranking quality goals

GORE is used to explore and establish the leaf level functional goals. These leaf level functional goals are then prioritized based on the stakeholders interests, for determining which of them are more important than others. It serves two purposes:

1) Involving the stakeholders opinions
2) Finding the relative importance

The output of this step is a prioritized list of functional goals. This list is then used to find the impact of quality goals which helps in the evaluation of quality goals among each other and on functional goal.

The remainder of this paper is organized in the following sections: next section gives the literature review on topics used in our approach. Section 3 describes the proposed methodology. Section 4 introduces the 'cyclecomputer' project and gives details of implementing proposed methodology for mentioned project. Section 5 focuses on related work on prioritization and contributions of quality goals on functional goals and vice versa. Finally, last section concludes this paper.

II. Literature Review

A. GORE and Quality Goals

Goal oriented requirements engineering refers to the use of high level goals for requirements elicitation, elaboration, organization, specification, analysis, negotiation, documentation and evolution [5]. One essential output of GORE is goal models. Goal model is a set of goal graphs representing the goals in a top-down or bottom-up hierarchy. Goals are refined into subgoals by using the AND/OR relations. In [5] a catalogue of refinement patterns is proposed. Subgoals describe how the overall goal is achieved. Refinement of a subgoal ends when that subgoal may be associated with a single agent. Most important GORE work includes Non-Functional Requirements framework(NFR) [6], i* framework [7], Goal Oriented Requirements Language (GRL) [8] and Knowledge Acquisitions in automated Specification or Keep All Objects Satisfied (KAOS) [9].

GORE frameworks used the concept of softgoals for quality requirements. Softgoals are goals which can not be fulfilled in their true scene. These are the goals without a clear definition and definite criteria for their fulfilment. Because of their interdependencies and positive/negative influences on each other they are used for handling conflicts and for making trade-offs. Dependencies among the softgoals and their contribution links are useful for the determination of quality goals impact on functional goals [6].

Non-functional requirements are considered from two perspectives [10]:

1) As requirements that describe the properties, characteristics or constraints of the system
2) As requirements that describe the quality attributes the system must have

First type consist of business rules, external interfaces, development constraints and any other requirements that do not describe the functionality of the system. Quality attributes are properties of functional requirements that describe characteristic other than its functionality. An important part of quality attributes is that they should be measurable i.e., one or more metrics can be attached to the quality attribute e.g., response time, throughput time etc. Quality aspects represent the properties of the system that concern stakeholders and these properties affect the degree of satisfaction of the system while constraints unlike qualities are not subject to negotiation, they are off-limits during design trade-offs. [11], [12] argue that quality requirements serve as basis for non-functional requirements in quality models. Quality models used for specifying non-functional requirements provide a hierarchical list of quality attributes also called quality aspects or quality factors. Number of quality models are available in literature. Most of the quality models consist of layers. The number of layers are two (characteristics, sub-characteristics) or three; third layers usually consisting of metrics.

Although these quality model give a systematic structure to quality requirements, they are not consistent with each other [20], for example, understandability is a sub-quality of usability in IS0 9126 [19], but is a sub-class of maintainability in Bohem's model [13]. A comparison of quality models [13], [14], [15], [16], [17], [18], [19] is presented in figure I.

B. Fuzzy Numbers

The functional goals and quality goals help to identify the criteria for the acceptance of target system. There are requirements derived from goal models and quality models which are imprecise in nature. In literature, fuzzy numbers are very popular in engineering disciplines for their ability to represent imprecise and vague information. By using fuzzy sets, requirements are described using linguistic terms. These linguistic terms are then converted into formal representation by using membership functions described for fuzzy numbers [21]. Membership function is the set of real numbers (R) whose range is the span of positive numbers in the closed interval [0,1], where '0' represents the smallest possible value of the membership function, while '1' is the largest possible value [22].

Fuzzy numbers depict the physical world more realistically than single-valued numbers. Among the fuzzy number Triangular Fuzzy Number (TFN) is capable of aggregating the subjective opinions [23]. A triangular fuzzy number (TFN) is described by a triplet (L, M, H), where M is the modal value, L and H are the left (minimum value) and right (maximum value) boundary respectively. TFN is used to represent stakeholder opinions for functional goals and quality goals which are established through goal models and quality models. Fuzziness of TFN is (L, M, H) is defined by the equation 1:

$$TFN(L, M, H) = \frac{H - L}{2M} \quad (1)$$

The membership function $\mu(x)$ for TFN is defined by the

TABLE I: Quality Models Comparison

Factors/Attributes/ Characteristics	Boehm's Model	McCall's Model	Romann Model	Sommerville Model	Dromey's Model	FURPS/ FURPS+	ISO9126 Model
Maintainability	*	*	*		*		*
Flexibility	*	*	*				
Testability	*	*		*			maintainability
Correctness	*	*	*				maintainability
Efficiency	*	*	*	*	*		*
Reliability	*	*	*	*	*	*	*
Integrity	*	*	*		*	*	*
Usability	*	*	*	*		*	
Portability	*	*	*	*	*		*
Reusability	*	*	*		*		
Interoperability		*	*	*		*	
Human Engineering	*		*	*		*	
Understandability	*						
Modifiability	*						maintainability
Functionality			*	*	*	*	*
Performance			*	*		*	
Supportability			*			*	
Clarity	*						
Documentation	*		*	*		*	
Resilience	*						
Validity	*						maintainability
Generality	*		*	*		*	
Economy	*		*				

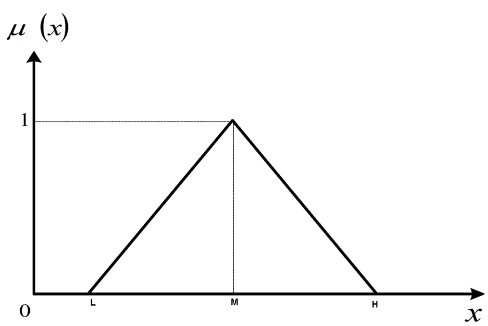


Fig. 1: TFN membership function

equation 2 and is shown in the figure 1 [4] .

$$\mu(x) = \begin{cases} 0, & x < L \\ \frac{x-L}{M-L}, & L \leq x \leq M \\ \frac{H-x}{H-M}, & M \leq x \leq H \\ 0, & x > M \end{cases} \tag{2}$$

III. The Proposed Method

In this section, the approach is described on how to use fuzzy number for functional goals and to find out among different functional goals, the ones which lead to better stakeholder satisfaction. After that the impact of quality goals to those functional goals is determined. First of all, higher level goals are modelled and for that, GORE is used to get goal models as a result of it. AND/OR diagrams which are essential output artefact of these goal models are used in the exploration phase of alternatives. The leaf nodes of goal models are used as criteria for functional goals. These criteria are compared based on the weighted scores. The criteria are weighted using fuzzy numbers and stakeholders opinions are taken as input. By using the fuzzy numbers, TFN, we can convert the qualitative information of stakeholders into quantitative one. The proposed methodology consist of following steps and is represented in the figure 2:

1) Establish high level goal(s), refine them using GORE and identify functional goals.
2) Functional goals are refined till we reach on leaf level goals. The leaf level goals are identified as goals directly assignable to agents: either humans or system agents. These are used as establishing criteria for functional goals.
3) Identify relevant stakeholders and take their opinions for above established functional goals as inputs. The input is taken in linguistic terms to ease the stakeholder.
4) Calculate relative importance of each criterion by using fuzzy numbers. TFN are used for aggregating stakeholder opinions.
5) Apply defuzzification process.

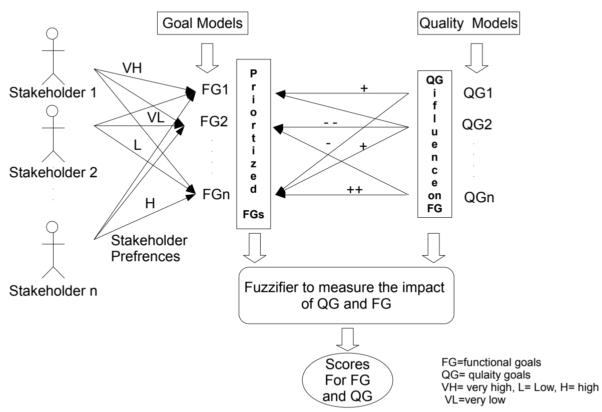


Fig. 2: Proposed methodology

6) Normalize the scores.
7) Identifying quality goals. Use quality models to refine these quality goals.
8) Find the impact of quality goals and functional goals using TFN and defuzzification process.

IV. Case Study

The 'cyclecomputer' system is used as case study for our work which is developed in our research group. The aim of 'cyclecomputer' project is to develop a flexible and modular bicycle computer which is adaptable to the needs of the driver. A driver will be supported while riding the bike, for maintenance issues, for tour preparations, or to enhance the safety using the bike e.g., besides the normal cycling activities one could use the 'cyclecomputer' as a medical device which will support people having of health problems. It can be used for professional cyclist or just for entertainment purposes. A variety of sensors in 'cyclecomputer' provide a comprehensive view of bike, driver/rider and route. In addition to speed, temperature, altitude, geographic location, heart rate; measurements like oil quality and pressure in the damper elements, brake wear or brake fluid quality are relevant to our project. Measurement of the quality framework on strain gauges is also an important requirement. This system will be attached to a bicycle, will process data from various sensors. All data is processed in the 'cyclecomputer' itself or it will communicate with a standard PC in the aftermath of a tour. One of the results of the requirements engineering phase is a goal model [24].

A. Establishing High level Goals

Though there are many goals related to 'cyclecomputer' but for space and simplicity considerations we take following identified high level goal Achieve[TourPlaningServiceSatisfied].

B. Refine Goals to Leaf Levels (establish functional goals)

The above mentioned goal is refined using GORE until they are assignable to agents i.e., human agents or software agents. These leaf levels goals are used as criteria for functional goals. Quality goals which include non-functional

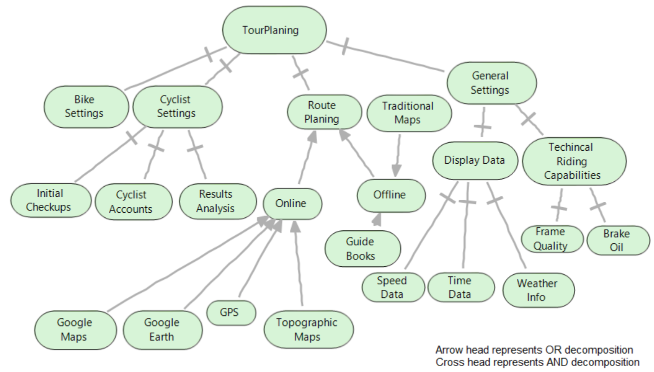


Fig. 3: Partial goal model

requirements and often serve selection criteria are also refined based on quality models. The goals along with their subgoals and short description are presented in table II, while figure 3 shows partial goal model for high level goal Achieve[TourPlaningServiceSatisfied].

C. Stakeholders and Their Opinions

1) Identifying Stakeholders: Though there are number of stakeholders in 'cyclecomputer' but following are the relevant stakeholders for goal Achieve[TourPlaningServiceSatisfied]:

1) Medical Cyclist: People who need a defined training / exercise due to any disease e.g., a heart disease. Medical cyclist can use pulse measurement, blood pressure, calory consumption by 'cyclecomputer' device.
2) Doctor (medical): The doctor will cooperate with a patient to set-up the correct tour plans.
3) Touring Cyclist: People who like to ride the bicycle for long trips (>100km) and they need specific services for their tours. The trips might take more than one day.
4) Analyst: analyse the touring details, analyse the cyclist.

2) Stakeholders Opinions Accumulation: For case study three stakeholders are selected and these stakeholders are asked to give their judgements against functional goals described in table II. Their judgements are used to elicit the importance degree of each functional goal. To enhance the user-friendliness for interacting with stakeholders linguistic terms are used. Linguistic terms are used to describe complex and ill-defined situations which are difficult to be described in quantitative measure. These linguistic terms are represented using TFN. The TFN values for these linguistics terms are derived from [4]. Table III shows the linguistic terms and their representative TFN values. Table IV shows stakeholders judgements against functional goals in table II.

D. Aggregating the Importance Using TFN

The different importance degrees of each functional goal assigned by stakeholders is calculated using TFN. TFN is used to aggregate the subjective opinions of stakeholder using fuzzy set theory. Many methods based on mean, median, min, max,

TABLE II: Partial Goal subgoal description

High level goal	Sub-goals till functional goals	Description
TourPlanningServiceSatisfied	Route planning	The cycle computer should offer route planning
		Routing should consider the current weather forecast
	Initial checkups	The cycle computer should offer an initial check-up to assess the drivers capabilities.
	Technical riding capabilities	Frame quality level should be analyzable and visible i.e., show the condition of the frame, interpret the frame condition by a coloured icon.
		The quality level should be visualized by the time until the frame might break.
		The cyclist should see the current speed of the cycle.
		The cyclist should be informed when the oil in the shocks should be changed.
	Weather info	The cyclist should see the current environmental temperature.
		The temperature of the last 5 days should be analyzable.
	Transferable to web	Track data should be transferred to a Web-portal to enable online competition / comparison.
	Tour details	The cycle computer should provide complete details of the tours.
		The cyclist should be informed about the current height (above sea level). A cumulative value should be shown by ascended and descended meters.
	Navigation	The cyclist should be able to navigate to a given location. The location could be a point of interest, e. g., a hotel.
		The cyclist should be informed about his global position on a map.
	Trip suggestions	The cycle computer should offer trip tips for professional sports cyclists e.g., gear change tips, speed tips based on the (known) route.

TABLE IV: Stakeholder judgements

High level goal	Sub-goals till functional goals	Linguistic terms		
		SH1	SH2	SH3
TourPlanningServiceSatisfied	Route planning	VH	H	VH
	Initial check-ups	M	H	H
	Technical riding capabilities	H	M	H
	Weather info	L	H	M
	Transferable to web	L	L	M
	Tour details	H	VH	H
	Navigation	VH	H	VH
	Trip suggestions	M	M	M

TABLE III: Linguistic terms and their TFN values

Linguistic terms	Representative TFN
Very High	(0.9, 1.0, 1.0)
High	(0.7, 0.9, 1.0)
Medium	(0.3, 0.5, 0.7)
Low	(0, 0.1, 0.3)
Very Low	(0, 0, 0.1)

etc.; are available to aggregate the opinions. Among them average operation is most commonly used aggregation method [3]. Here, the avergae operator is used as an aggregation methods to accumulate stakeholder opinions. Let's say there are 'k' number of stakeholders who assign linguistic term values according to table III to 'n' number of functional goals. The aggregated weight (importance) of each functional goal is calculated as [3]:

$$r_f = \frac{1}{k}\left\{L_f, M_f, H_f\right\} \tag{3}$$

where 'f' represents functional goals from 1...n

$$L_f = \sum_{j=1}^{k} L_{fj}, \quad M_f = \sum_{j=1}^{k} M_{fj}, \quad H_f = \sum_{j=1}^{k} H_{fj} \tag{4}$$

where 'j' represents number of stakeholders from 1...k

E. Apply Defuzzification Process on TFN

After calculating TFN for each functional goal the defuzzification process is applied. Defzzuification process is used to convert calculated TFN values into quantifiable values. Defuzzificatio process is represented by the equation 5 which is derived from [22]:

$$D^{\alpha}\left(x_i\right) = \alpha f_R\left(x_i\right) + \left(1-\alpha\right) f_L\left(x_i\right) \tag{5}$$

where $x_i = TFN_i$ representing triangular fuzzy number. The developer is also involved in the process by representing his preference. α in the above equation represents the preference value of developer and it's value is in the range [0,1].

When $\alpha = 1$ it shows the optimistic view of developer resulting in the equation 6:

$$D^{1}\left(x_i\right) = f_R\left(x_i\right) \tag{6}$$

When $\alpha = 0$ it shows the pessimistic view of developer resulting in the equation 7:

$$D^{0}\left(x_i\right) = f_L\left(x_i\right) \tag{7}$$

Where $f_L\left(x_i\right)$ represents the left end value of TFN_i i.e., pessimistic value. While $f_R\left(x_i\right)$ represents the right end value of TFN_i i.e., optimistic value. These values are represented by the equations 8, 9 respectively:

$$f_L\left(x_i\right) = L_i + \left(M_i - L_i\right)\beta \tag{8}$$

Equation 8 represents left end boundary value.

$$f_R\left(x_i\right) = H_i + \left(M_i - H_i\right)\beta \tag{9}$$

Equation 9 represents right end boundary value.

β in the above equations represents the risks tolerance for particular functional goal and it's value is in the range [0,1]. To keeps things simple we have chosen value 0.5 of preference and risk tolerance against each calculated TFN.

If the only preference value are considered and risk tolerance value is ignored, defuzzification value can be calculated using the equation 10 or 11:

$$D^{\alpha}\left(x_i\right) = \frac{1}{2}\alpha\left(M_i + H_i\right) + \frac{1}{2}\left(1-\alpha\right)\left(L_i + M_i\right) \tag{10}$$

$$D^{\alpha}\left(x_i\right) = \frac{1}{2}\left[\alpha H_i + M_i + \left(1-\alpha\right)L_i\right] \tag{11}$$

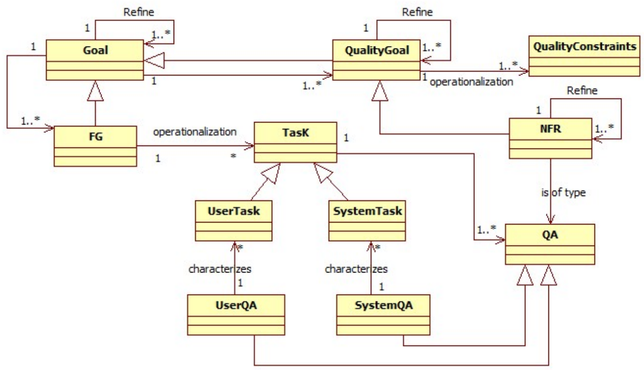


Fig. 4: Conceptual model of functional goal and quality goal integration

F. Normalizing Values Obtained by Defuzzification Process

Although in this paper all the fuzzy numbers are in interval [0,1] and therefore the calculation of normalization is not required, still the scores after the defuzzification process can be normalized by using the equation 12:

$$ND_i = D_i / \sum_{i=1}^{m} D_i \tag{12}$$

where 'm' represents number of functional goals.

Table V represents TFN, defuzzification and final normalized defuzzification values that give the importance of degrees of each functional goal. The defuzzification normalized values give the prioritized list of functional goals.

G. Functional and Quality Goal Impact Measurement

This process consist of three steps:

1) Determining project specific quality goals
2) Determining and evaluating the dependency among quality goals
3) Determining and evaluating the impact of quality goals and functional goals

1) Determining Project Specific Quality Goals: Quality models and NFR framework are useful for determining project based quality goals, that is, the quality goals related to high level system goals. Figure I provides widely used quality attributes in these models. The advantage of using these models is that they provide clear, detail definitions of quality attributes. The universality of these models, because of their acceptance all around the software community. The quality goals are then integrated to functional goal model. Figure 4 represents the conceptual model of quality goals integration to functional goal. This conceptual model is developed by using StarUML.

Figure 5 shows two quality goals 'Safety' and 'Availability' for 'cyclecomputer' functional goal 'RoutePlanning'. These quality goals are represented as softgoals using openOME tool.

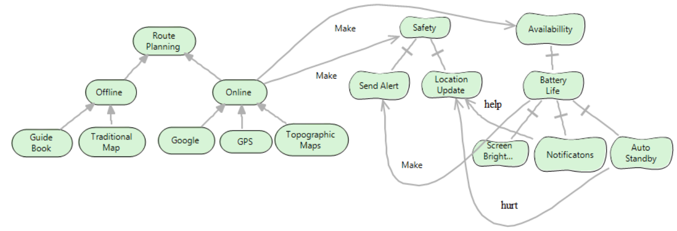


Fig. 5: Quality goals and functional goals

TABLE VI: Linguistic terms and their values for quality goals

Linguistic terms	Numerical Scale
Make	(0.4, 0.5, 0.5)
Help	(0.2, 0.4, 0.5)
Neutral	(-0.2, 0, 0.2)
Hurt	(-0.5, -0.4, -0.2)
Break	(-0.5, -0.5, -0.4)

2) Determining and Evaluating the Dependency between Quality Goals: Quality goals are refined same as functional goals are refined in goal models. These lower level quality goals may influence other quality goals positively or negatively, for example, the fulfilment of one quality goal may hurt or help in the fulfilment of another quality goal. In this step, the importance of each individual quality goal identified in previous step (IV-G1) using TFN (IV-E) is measured and crisp values are obtained by applying the defuzzification process (IV-F). This helps to measure the strength of relationships between quality goals. The linguistic terms and their numerical values used to get crisp values and to measure the relationship strengths are shown in figure VI. The real number interval which represents the direction and strength of relationships among quality goals is set [-0.5,0.5]. The range from negative number is chosen because the contribution 'hurt' or 'break' will have negative impact on other quality goals. These linguistic terms (make, help, hurt, break) are very common in GORE for their use as softgoals contribution. The same linguistic terms are used and numerical values in the range [-0.5,0.5] are defined for these terms.

Let's say there are two quality goals (QG1, QG2) and each goal is refined to four leaf level goals. Now leaf level goals of QG1 are influencing QG2 in positive and/or negative way. Table VII shows their contributions, measurements and final column representing the priority of each leaf level goal of QG1.

The strength of relationships between two quality goals is measured by equation 13. The relationship strength values for goals in table VII are given in table VIII, for example, relationship (LQG1, LQG2, 1.0) gives relationship value (1.0) between leaf level QG1 and leaf level QG2. Here first element LQG1 is impacting or contributing to second element LGQ2 (impacted by LGQ1). These are one-way relationships, the values for (LQG2, LQG1) may be different from (LQG1, LQG2).

$$RS_i = H_i + (M_i - H_i) + L_i + (M_i - L_i) \tag{13}$$

TABLE V: TFN, Defuzzification and Normalized Scores

Functional goals	Linguistic terms	TFN	Defuzzification	Normalized Values		
	SH1	SH2	SH3			
Route planning	VH (0.9, 1.0, 1.0)	H (0.7, 0.9, 1.0)	VH (0.9, 1.0, 1.0)	(0.83, 0.96, 1.0) 0.93	0.17	
Initial checkups	M (0.3, 0.5, 0.7)	H (0.7, 0.9, 1.0)	H (0.7, 0.9, 1.0)	(0.56, 0.76, 0.9)	0.74	0.13
Technical riding capabilities	H (0.7, 0.9, 1.0)	M (0.3, 0.5, 0.7)	H (0.7, 0.9, 1.0)	(0.56, 0.76, 0.9)	0.74	0.13
Weather info	L (0, 0.1, 0.3)	H (0.7, 0.9, 1.0)	M (0.3, 0.5, 0.7)	(0.33, 0.5, 0.66)	0.49	0.08
Transferable to web	L (0, 0.1, 0.3)	L (0, 0.1, 0.3)	M (0.3, 0.5, 0.7)	(0.1, 0.23, 0.43) 0.24	0.04	
Tour details	H (0.7, 0.9, 1.0)	VH (0.9, 1.0, 1.0)	H (0.7, 0.9, 1.0)	(0.76, 0.93, 1.0)	0.9	0.16
Navigation	VH (0.9, 1.0, 1.0)	H (0.7, 0.9, 1.0)	VH (0.9, 1.0, 1.0)	(0.83, 0.96, 1.0)	0.93	0.17
Trip suggestions	M (0.3, 0.5, 0.7)	M (0.3, 0.5, 0.7)	M (0.3, 0.5, 0.7)	(0.3, 0.5, 0.7)	0.5	0.09

TABLE VII: Quality Goals Impact and Measurement

	LQG21	LQG22	LQG23	LQG24	TFN	DFN	Nomalized Score
LQG11	-	Make (0.4, 0.5, 0.5)	Help (0.2, 0.4, 0.5)	Hurt (-0.5, -0.4, -0.2)	(0.03, 0.16, 0.3)	0.15	0.18
LQG12	Make (0.4, 0.5, 0.5)	-	Help (0.2, 0.4, 0.5)	Make (0.4, 0.5, 0.5)	(0.33, 0.46, 0.5)	0.43	0.51
LQG13	Hurt (-0.5, -0.4, -0.2)	Help (0.2, 0.4, 0.5)	-	Help (0.2, 0.4, 0.5)	(-0.03, 0.13, 0.26)	0.11	0.13
LQG14	Make (0.4, 0.5, 0.5)	Help (0.2, 0.4, 0.5)	Hurt (-0.5, -0.4, -0.2)	-	(0.03, 0.16, 0.3)	0.14	0.16

TABLE VIII: Relationship Strength Values

	LQG21	LQG22	LQG23	LQG24
LQG11	-	1	0.8	-0.8
LQG12	1	-	0.8	1
LQG13	-0.8	0.8	-	0.8
LQG14	1	0.8	0.8	-

3) Determining and Evaluating the Impact of Quality goals and Functional goals: In last part of this step, the impact of quality goals and functional goals is determined. Table VI is used to assign the values, impacting goals are arranged vertically and impacted goals are arranged horizontally. Same steps as in IV-G2 are repeated to measure the contributions and relationship strengths.

V. Discussion and Related Work

Success of the software system depends on its capability to satisfy both functional and non-functional requirements. Traditionally, the functional requirements are given high priority while dealing with requirements at abstract level. Goal oriented requirements engineering has been used in representing the requirements at higher level. Goal models combined with quality models can represent both functional and non-functional requirements adequately. However, the impact measurement of contributions among quality goals and also between functional and quality goals is rarely addressed. Because of imprecise nature of the requirements, fuzzy number combined with goal models and quality models can sufficiently represent the requirements impact among each other by quantitative means.

To measure the importance degree of each requirement many requirements prioritizations methods are present in literature. Analytic Hierarchy Process (AHP) is one popular method for prioritization, it involves pair-wise comparison [25]. All pair of requirements are compared to determine the priority level of one requirement over another requirement. Requirements are arranged in matrix form, that is, rows and columns. Then priority is specified to each pair of requirements by assigning a preference value between 1 and 9, where 1 expresses equal value while 9 indicates extreme value. AHP involves stakeholders opinions but pairwise comparison of all requirements make it cumbersome and difficult to use. Proposed methodology in this paper also involves stakeholders opinions and take into consideration both functional and non-functional requirements. Comparisons are made only between the impacting requirements. Importance of both functional and quality goals is obtained using linguistic terms which are easy to deal from stakeholders point of view. These stakeholder opinions are then evaluated using fuzzy set concepts, weight for each functional goals and contribution/impact values are calculated.

In [5] [26] qualitative approaches are used for measuring the contributions. These methods mainly focus on choosing the best alternative. They use temporal logic and label propagation algorithm. We used quantitative approach for measuring the strength of relationships. In [23] prioritizing process for software requirements is highlighted. It considers prioritization of both functional and non-functional requirements at the same level and as a result produces two separate prioritized lists: one of functional requirements and second for non-functional requirements. Like the approach in this paper, their work also used the concepts from [22] but their work is only used for prioritization of functional and non-functional requirement while our work gives an integration model for functional and quality goals and it uses the prioritized requirements to measure their impact on each other.

Wiegers [27] method is semi-quatitative method which focused on customer involvement. Requirements are prioritized based on four criteria defined as benefit, penalty, cost, and risk. The attributes (criteria) are assessed on a scale from 1 (minimum) to 9 (maximum). The customer determines the benefit and penalty values whereas the developers provides the cost and risk values associated with each requirement. Then, by using a formula, the relative importance value of each requirement is calculated by dividing the value of a requirement by the sum of the costs and technical risks associated with its implementation.

The work in [28] focused on modelling the impact of non-functional requirements on functional requirements. For that matter, they investigate the relationships between functional and non-functional requirements. They advocate to define non-functional requirements at the highest level of abstraction like functional requirements. Their proposed approach uses and modifies the NFR framework concepts of contribution but there is nothing mentioned about how to measure the relationships (contributions, impacts) quantitatively.

The work of [21] was the initial attempt to use fuzzy concepts in requirements engineering. Their method deal with conflicting requirements and focus of their work is on prioritizing the conflicting requirements by finding some trade-off between these requirements. The conflicting requirements were represented using fuzzy logic and then they use reasoning scheme to infer the relationship between these conflicting requirements. Ito [2] discussed the uncertainty of design decisions. This work suggests to use AHP and Quality Function Deployment (QFD) for prioritizations and for conflict resolution. In [20] the distinction is made between functional goals and quality goals. They presented non-functional requirements as requirements over qualities i.e., non-functional requirements are modelled as quality goals. For quality goals they use ISO/IEC 25010 standard as reference. They distinguished between domain and co-domain of quality goals. The problem with their model is that functional goal(s) can not be refined into quality goal(s) and vice versa but in GORE we face situations where we encounter these refinements i.e., functional goal refinement results into quality goal and vice versa.

In [29] proposed the guidelines for the elicitation of trustworthy requirements. These guidelines are helpful in selection of project specific quality goals from goal models. Their model consist of three parts: decomposition tree, correlation matrix (CM) and priority vector. Their CM is also base based on fuzzy set theory but it is restricted to elicitation of trustworthy requirements.

In this paper the Fuzzy set concepts are used to evaluate the importance of leaf level functional goal. Weight for each functional goal is calculated based on stakeholders opinions. These weights display stakeholders priorities for all functional requirements. The interaction of stakeholders at early phase of requirements engineering helps to capture the rational (by documenting the preferences) of each requirement and also helps to identify inconsistencies at the early phase of requirements engineering. Using the same method importance weight of quality goals is calculated. Quality goals are tailored using quality models and dependencies among quality goals and functional goals are modelled and measured using fuzzy concepts. The method gives a systematic structure to calculate the fuzzy weight of functional and quality goals. The subjective weights assigned by stakeholders are normalized into a comparable scale. The contributions and strength values are also determined and the strength of the relationships is measured using TFN and defuzzification process.

VI. Conclusion

In this paper an approach is presented to use the goal model of goal-oriented requirements engineering to establish the functional goals as criteria. These leaf levels functional goals are prioritized according to stakeholders preferences. Triangular fuzzy numbers and defuzzification process is used for prioritization, the developers input and risk tolerance is dealt by defuzzification of TFN. After that, the process is used for specified quality goals which are tailored using quality models. In the final step, dependencies among quality goals and between functional goals are evaluated. Therefore, the proposed methodology was used to measure the strength of relationships.

The methodology was explained by 'cyclecomputer' case study where 8 functional goals were established and stakeholders opinions were collected for these functional goals. After calculating the importance value of each functional goal, we integrated quality goals and prioritized them according to their dependencies. This approach is promising for ranking of both functional and quality goals because of stakeholders and developers involvement in the process. The formalization of the approach, goal models and complete quality models integration, implementing it for complete set of non-functional requirements (derived from quality models) and the validation by additional examples are future research topics.

VII. Acknowledgement

We acknowledge support for the Article Processing Charge by the German Research Foundation and the Open Access Publication Fund of the Technische Universit Ilmenau.

References

[1] J. Karlsson and K. Ryan, "A cost-value approach for prioritizing requirements," *Software, IEEE*, vol. 14, no. 5, pp. 67–74, Sep 1997.

[2] T. Ito, "Dealing with uncertainty in design and decision support applications," *International Journal of Soft Computing Applications*, vol. Vol.1, no. No.1, pp. pp.5–16,, 2007.

[3] r. Erturul and N. Karakaolu, "Comparison of fuzzy ahp and fuzzy topsis methods for facility location selection," *The International Journal of Advanced Manufacturing Technology*, vol. 39, no. 7-8, pp. 783–795, 2008. [Online]. Available: http://dx.doi.org/10.1007/s00170-007-1249-8

[4] C.-T. Chen, "Extensions of the topsis for group decision-making under fuzzy environment," *Fuzzy Sets Syst.*, vol. 114, no. 1, pp. 1–9, Aug. 2000. [Online]. Available: http://dx.doi.org/10.1016/S0165-0114(97)00377-1

[5] A. van Lamsweerde, "Requirements engineering in the year 00: a research perspective," in *ICSE*, 2000, pp. 5–19.

[6] L. Chung, J. Cesar, and S. P. Leite, "Non-functional requirements in software engineering," 1999.

[7] E. S.-K. Yu, "Modelling strategic relationships for process reengineering," Ph.D. dissertation, Toronto, Ont., Canada, Canada, 1996, uMI Order No. GAXNN-02887 (Canadian dissertation).

[8] GRL. (2008) Goal-oriented requirement language.

[9] A. Dardenne, A. van Lamsweerde, and S. Fickas, "Goal-directed requirements acquisition," in *Selected Papers of the Sixth International Workshop on Software Specification and Design*, ser. 6IWSSD. Amsterdam, The Netherlands, The Netherlands: Elsevier Science Publishers B. V., 1993, pp. 3–50. [Online]. Available: http://dl.acm.org/citation.cfm?id=171349.156032

[10] A. I. Anton, "Goal-based requirements analysis," in *Proceedings of the 2Nd International Conference on Requirements Engineering (ICRE '96)*, ser. ICRE '96. Washington, DC, USA: IEEE Computer Society, 1996, pp. 136–. [Online]. Available: http://dl.acm.org/citation.cfm?id=850944.853130

[11] X. Franch and J. Carvallo, "Using quality models in software package selection," *Software, IEEE*, vol. 20, no. 1, pp. 34–41, Jan 2003.

[12] X. Franch, "Systematic formulation of non-functional characteristics of software," in *Proceedings of the 3rd International Conference on Requirements Engineering: Putting Requirements Engineering to Practice*, ser. ICRE '98. Washington, DC, USA: IEEE Computer Society, 1998, pp. 174–181. [Online]. Available: http://dl.acm.org/citation.cfm?id=645536.657176

[13] B. W. Boehm, "Software engineering," *IEEE Trans. Comput.*, vol. 25, no. 12, pp. 1226–1241, Dec. 1976. [Online]. Available: http://dx.doi.org/10.1109/TC.1976.1674590

[14] D. T. Ross and K. E. Schoman, Jr., "Classics in software engineering," E. N. Yourdon, Ed. Upper Saddle River, NJ, USA: Yourdon Press, 1979, ch. Structured Analysis for Requirements Definition, pp. 363–386. [Online]. Available: http://dl.acm.org/citation.cfm?id=1241515.1241537

[15] G. C. Roman, "A taxonomy of current issues in requirements engineering," *Computer*, vol. 18, no. 4, pp. 14–23, Apr. 1985. [Online]. Available: http://dx.doi.org/10.1109/MC.1985.1662861

[16] I. Sommerville, *Software Engineering (5th Ed.)*. Redwood City, CA, USA: Addison Wesley Longman Publishing Co., Inc., 1995.

[17] R. G. Dromey, "A model for software product quality," *IEEE Trans. Softw. Eng.*, vol. 21, no. 2, pp. 146–162, Feb. 1995. [Online]. Available: http://dx.doi.org/10.1109/32.345830

[18] R. B. Grady, *Practical Software Metrics for Project Management and Process Improvement*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1992.

[19] I. O. for Standardization, *ISO/IEC TR 9126-4: Software engineering - product quality - Part 4 : Quality in use metrics*. ISO, 2004. [Online]. Available: http://books.google.de/books?id=LM5xkQEACAAJ

[20] F.-L. Li, J. Horkoff, J. Mylopoulos, R. Guizzardi, G. Guizzardi, A. Borgida, and L. Liu, "Non-functional requirements as qualities, with a spice of ontology," in *Requirements Engineering Conference (RE), 2014 IEEE 22nd International*, Aug 2014, pp. 293–302.

[21] J. Yen and W. A. Tiao, "A systematic tradeoff analysis for conflicting imprecise requirements," in *Proceedings of the 3rd IEEE International Symposium on Requirements Engineering*, ser. RE '97. Washington, DC, USA: IEEE Computer Society, 1997, pp. 87–. [Online]. Available: http://dl.acm.org/citation.cfm?id=827255.827815

[22] T.-S. Liou and M.-J. J. Wang, "Ranking fuzzy numbers with integral value," *Fuzzy Sets Syst.*, vol. 50, no. 3, pp. 247–255, Sep. 1992. [Online]. Available: http://dx.doi.org/10.1016/0165-0114(92)90223-Q

[23] S. P. L. Mohammad Dabbagh, "An approach for integrating the prioritization of functional and nonfunctional requirements," *The Scientific World Journal*, vol. Volume 2014 (2014), no. Article ID 737626, p. 13 pages, 2014.

[24] A. Mansoor and D. Streitferdt, "On the impact of goals on long-living systems," in *Software Engineering (Workshops)*, 2011, pp. 133–138.

[25] T. L. Saaty, "Decision making with the analytic hierarchy process," *Int. J. of Services Sciences,*, vol. Vol.1,, no. No.1, pp. pp.83 – 98, 2008.

[26] J. Castro, M. Kolp, and J. Mylopoulos, "Towards requirements-driven information systems engineering: The tropos project," *Inf. Syst.*, vol. 27, no. 6, pp. 365–389, Sep. 2002. [Online]. Available: http://dx.doi.org/10.1016/S0306-4379(02)00012-1

[27] K. Wiegers, "First Things First: Prioritizing Requirements," *Software Development Online*, vol. 7, pp. 48–53, Sep. 1999.

[28] C. Gnaho, F. Semmak, and R. Laleau, "Modeling the impact of non-functional requirements on functional requirements," in *Advances in Conceptual Modeling*, ser. Lecture Notes in Computer Science, J. Parsons and D. Chiu, Eds. Springer International Publishing, 2014, vol. 8697, pp. 59–67. [Online]. Available: http://dx.doi.org/10.1007/978-3-319-14139-88

[29] F. Shao, R. Peng, D. Sun, H. Lai, and Y.-S. Liu, "An attribute-driven model for trustworthy requirements elicitation," *International Journal of Digital Content Technology and its Applications*, vol. 6, no. 23, pp. 531–540, 2012.

Skill Evaluation for Newly Graduated Students Via Online Test

Mahdi Mohammed Younis
University of Sulaimani
Sulaimani, KRG-IRAQ

Miran Hikmat Mohammed Baban
University of Sulaimani
Sulaimani, KRG-IRAQ

***Abstract*—Every year in each university many students are graduated holding a first university degree. For example Bachelor degree in Computer Science. Most of those students have a motivation to continue with further studies to get higher education level degree in universities. However, some other students may have enthusiasm towards working based on their skills that they got during their life of studies in university. In both cases, it is required that applicant must pass a test that comprise the entire subject that they learned before. For this reasons, this research is proposing a new technique to evaluate graduate students skills.**

Keywords—LAN-Network; Database; Online Test; Skills evaluation; feedback

I. Introduction

Today's, there are lots of demand for getting a job in either government organization or public companies. Moreover, these requirements are usually asked by the people who finished a higher education degree. Also, these degrees include Diploma, Bachelor, Masters, and Doctoral. Also, It is evident that university degree makes the opportunity for getting a job much easier. However, every level needs to have one previous level. For example, it will not be possible to get matters unless they hold a bachelor degree and same for the other qualifications.

People when they get that grade, it means that they graduated from university or institution. Means completed the organizations studies successfully. After that, most of those graduated people trying to get a job or studying for a higher level of study. Furthermore, to get that opportunity most of the universities and other private organizations put a standard of restriction to make a competition between the applicants. This level of competition is testing skills through all courses that they studied during their years in universities or institutions.

Also, the most of the test that will be held in the organization and during the amount of time that will conduct to the test difficulties.

The test will comprise many subjects in the area of study and work that the applicant will apply. Thus, every graduated person will do the test in the fields they studied in their levels of educations.

On the other hand, the level of difficulties will be the same for all the testers without making different between them. However, there may be some other ways may do that, but still do the same. For example, some people may apply for networking job or some others apply for database job, in this case, there may be the various level of questions will be held.

All the test will hold on the computer in laboratory specified for the test, which provided by the specific organization. Also, all the testers must be on their computers named with their name. In the last step, the final result of the test will be shown on the screen, this means each tester will see their result with acceptance in the organization or rejected.

The question that provided are multi-choices or filling in black, but as it can notice most of these jobs in companies doing muti-choices which based on a general understanding of the working area. Furthermore, It usually starts with a simple question and level up to harder with every answer and number of question. Also, with each answer, there are points on it, for instance, the truth answer of the harder question is much more than a simple one. These points will indicate with some percentages data.

In contrast to job application process, in higher level study application process, there are lots of things to do. Moreover, one of the most important points is to take the test in many subjects. However, these subjects will be chosen by the university or the institution for instance Multimedia, Database, Networking and Artificial Intelligence.

Unlike the job application test, in this trial the form will be vary among different kinds of questions. Filling in the blank, multi-choices, writing the answers. They arranged from easier to harder. Moreover, every question has their mark, and the marks will be vary from one to another. Nevertheless, the mark will not be shown directly, and the test will hold on the paper. Later on, the exam community will check the paper exams. This one level of completion and there are lots of other comparison points to accept in the higher study.

In fact, this research will talk about how the skills can test and how to arrange the test. Also, in this propped research the following subject has mentioned:

- In the first section, a short introduction to the work and proposed idea has been written.
- General literature review and background research about the work.
- Researching some other works that have similarities with this research.
- Also, it mentioned how the work will implement and how to design the system.
- It shows how the result will show, and what the output is.

- It gives a conclusion and future work.

II. Literature Review

A. Online testing system

These days, in many universities there are lots of tastings will be held online and in different areas of study and subjects. Also, most of these tests are a multi-choices test. However, there are lots of test forms, and these forms will be vary depending on the subject and the area of study. Furthermore, some private sectors who test the applicants prefer mostly multi-choice questions. Usually, online tests are done with using computers in the laboratory that specified for the tests [1].

The online term means using internet access to do the test process, in contradiction with the idea of online. Thus, It is not mean doing the test from home, but the checking questions will through online with World Wide Web. On the other hand, the higher education test will be done on paper exam [2].

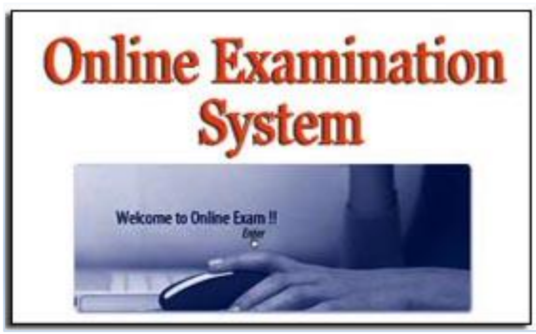


Fig. 1. Online examination web pages

B. E- learning online system

The term of e-learning refer to electronic learning, and the most part mean learning through online methods. Such as using the internet for learning in a different level of education (schools, colleges, Institutions, and Universities). Also, there some devices these days that will put the idea on E-Learning, and those devices called Smartphones (IPad, IPod, IPhone and Galaxy et.al.) [3].

With these online study, their tests and courses available online from the much educational organization, and the mostly from universities. Moreover, those universities specify the online courses for studies called distance learning for pursuing a higher level of educational. These kinds of study will be mostly from countries who host students from other countries [4].

C. Login System Design

This system is the most popular system among people who work or studies in different places and organizations. In fact, it is the easy way to keep member account and their secret data in safe. By using this idea, the data will not be visible to others [5]. Also, in the meaning of testing, everyone must have their page or account to conduct the test online. With doing online test the person who took the exam can see the result once finished. The next step is to close the account. From this way, no one can steal the certificate or outcome from another one [6].

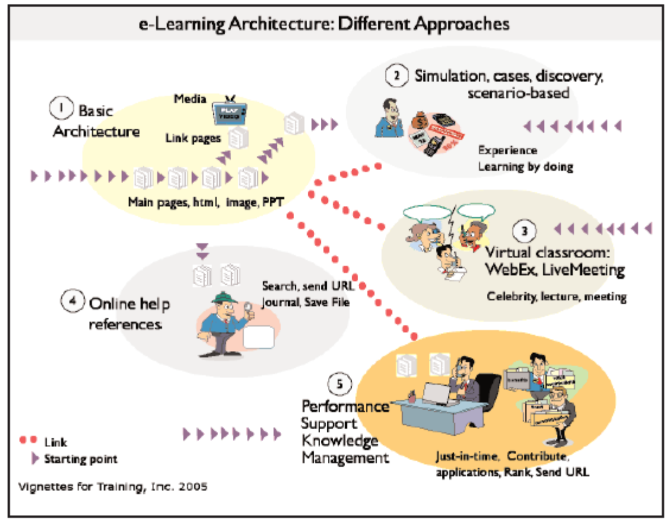


Fig. 2. E- Learning Architecture

Fig. 3. Online Login System

D. Test Storage place

The online test means doing the test online and not in the papers. This idea means there must be a place that test came from, and this place is called database storage place. From the database, the data will be loaded which means the test will be called randomly to be shown by the user end [7].

Also, when the user finished the test in specific time, all data that that related to testing such as the name of the person, answer time, Date of Birth and Address. Also, the number of correct and wrong answers will be shown as well as. Also, this storage may contain database servers or Cloud computing. Also, there are other stages such Drop Box, Sky Drive, and Google Drive [8].

Fig. 4. Cloud Computing

Fig. 5. Online Storage Webs

E. Skills and job opportunities

Nowadays, in many companies whenever a person who wants to apply for getting a job. Also, he/she will be asked to hand in lots of documents and some personal information. However, the process will not stop at this stage, but they will need to know and assess the person's skills [9]. From this way, the companies can be assured of the performance of the applicants and put in the desired position. Thus, the company will save their reputation from accepting people with lack of information and making the company going with low trends [10].

Fig. 6. Job opportunity

F. Higher Education study

In most of the countries, there are some obstacles for the students to study further degrees. This kind of difficulties happened due to the rules of the government of the countries. For example, in some countries the students before they accepted to study at the universities must get a high level of degree to go to the colleges. However, some colleges accept students with excellent grades such as the 90s, or 80s [11] [12].

In addition to the grade, some colleges provide obligation test to every person before acceptance in the colleges. Moreover, these test maybe on some basic subjects related to the previous skills. However, this skill test may go further hardness, especially English Academicals Qualification, academicals tests, and from this way the colleges will pick up the most suitable person who can study further [13].

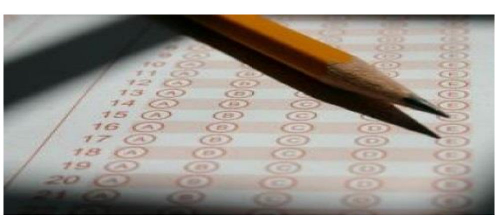


Fig. 7. Higher Education Study

G. Exams and Time

With every test either online or on papers, it is required to answer the question in the amount of time. Although there is time for each exam, there should be some desired calculation to each question. This idea means, there must be equality with giving time to each question [14].

However, there are differences between online test and the paper exams. Also, one of these differences is time-consuming on the test. In an online test, there is automatic decreasing clock starting from test time and begin to decrease second. Usually, the online test has less amount of time comparing to the paper tests [15].

Fig. 8. Examination time and test coverage

H. LAN Network (Local Area Network)

This kind of networking designed for making a small communication among many different devices ranging from mobiles smartphones and IPad to computer machines and servers. Through this networking scheme, users of organization can communicate and send –receive data from each other (see figure 9).

Even through some organizations, which conducts tests either for academicals test or applicants jobs. These companies, provide a secure LAN Networking system for people who take the test, which they use login system to using the network.

Furthermore, these devices that specified for online assessments are connected to the main server that contain databases. So, they receive the question from the server, when they finished they submit the answer to the server and calculated there [16][17].

Fig. 9. LAN Networking System

I. Database Security Issue

It is important to provide a secure level of safety to protect database server in every organization. In some databases, there are a lot of sensitive data that related to people, either bank account, personal details or examination information tests.

In case of testing centers, those people who are working there as a staff member of the organization, they should work on protecting all the servers and databases from attackers. It happens because of some intruders may try to extract information from the server such as questions and their answers as well. This kind of fraud will leave a bad effect on the organizations and the people who do the test. In other meanings, that kind of organizations will lose their name of famousness. Moreover, people may don't get their correct grade even they do their best in the test because hackers change all the information on the server. Also, they may lose their truth opportunity to lose their job that they desire [18][19].

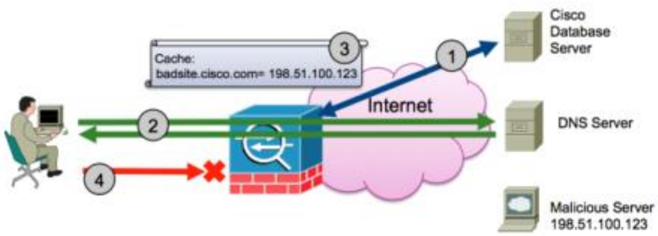


Fig. 10. Hacking Database server

J. Online test types

Usually, their many kinds of test can be seen on online and on papers. Questions such as multi-choices, filling in the blank, writing a brief desorption. With all of these kinds of tests, multi-choices are the most usable these days [20].

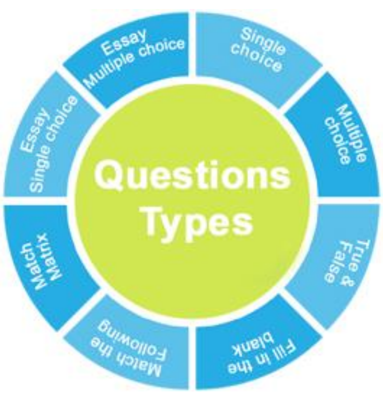


Fig. 11. Different form of questions

III. Related Work

While researching and reading some papers, it has found out some works have done in the same area, which the have little similarity with our research. However, those works used techniques different from our techniques.

A. Related work - 1

According to Randy Elliot, it shows how the online test work on human knowledge either it gives the advantages or drawbacks. Also, it shows the issues that face the testers during the test time.

Also, he displays the impact of online assessment in a different range of study and educational organization from elementary to university degrees.

Also, he shows that the environment of the test must be compatible in many cases. For example:

- The test should time correctly and should not exceed the number of question, which mean that the time should limit to the questions.
- The hardness and difficulties of the test should have the same range whether done online or on the paper.
- The test must not affect the sight of the testers, this means that people who do the test on computers must be able to see the texts of test clearly on small and large screen.
- The score on the test must divide equally for online and on paper.
- The most of the assessment should give enough information to the testers rather just do the normal test.

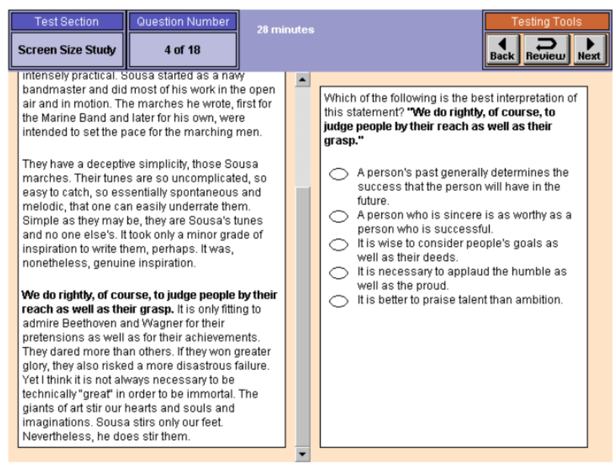


Fig. 12. Test style multi-choices

Also, it has been mentioned in his research, the most important point of the online trials:

- The correctness of the academically, which means the question must truly knowledge and not fraud data.
- The tests should be correct in grammars and spells.
- The test must have answers, and they should not vague.
- All text must be readable and not blur or hidden texts. If the texts are unclear, it will affect the user answers.

Also, in the new proposed system for the online test, it has put those point as the first important point for preparing the test for online assessment [21].

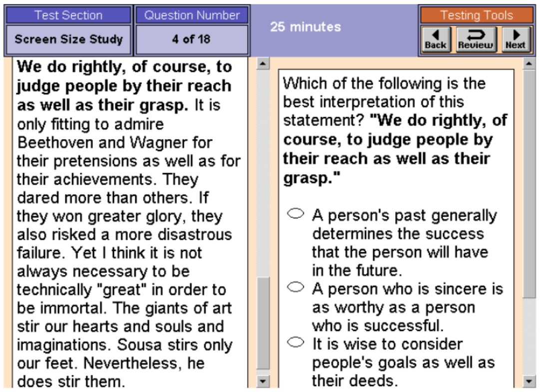


Fig. 13. Clarity of texts of the questions

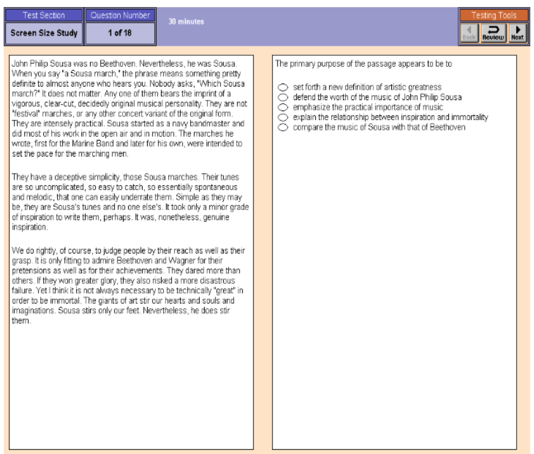


Fig. 14. Unreadable texts of the questions

B. Related Work – 2

According to Shachar M,& Neumann, Y., (2010). They showed that the online test had more ability to examine the capabilities of students in many different areas of studies. For example, Natural Sciences, health sciences, technologies and other studies.

- This case happens due to of the capabilities of online to test general skills in their subject area. Moreover, the question usually is multi-choices and rarely contain fill-in blanks.
- Also, those multi-choice contain four possible answers.
- Users chose only one answer between them, only one answer is possible.

Based on this research paper, it shows the effectiveness of online assessments and online materials for the students either they are graduated or still looking for further studies.

In the table below, it can be noticed that the number of people who are demanding the online sources will increase dramatically. Also, it shows the rate in percentages and starting the statistics from the year 1991 to the latest one that is 2009. Also, shows different area and level of studies. Also, in the sixth column is specified for the graduated student from universities and institutions.

Moreover, the given data encompass other levels, such as FTF Students, DE Students, Graduates, Undergraduate and another level of studies. In each level shows how many rates have got in each year as the demands for the online materials.

On the other hand, the study shows that some tests that are an available online website may name under biased test. This idea means that the test are not trusted by any academical organizations and private sectors [22].

TABLE I. TABLE DEMAND SOURCES FOR ONLINE TEST

Period	K	ES Pos n (%)	FTF Student n(%)	DE Student n (%)	Graduate k (%)	Under Grad. + College k (%)	Other k (%)
1991 – 1998	38	24 (63%)	4,392 (50%)	4,454 (50%)	7 (18%)	21 (55%)	10 (26%)
1999 – 2000	33	22 (67%)	1,924 (58%)	1,393 (42%)	10 (30%)	20 (61%)	3 (9%)
2001 – 2002	29	20 (69%)	3,802 (64%)	2,102 (36%)	0 (0%)	27 (93%)	2 (7%)
2003 – 2009	25	21 (84%)	1,380 (51%)	1,337 (49%)	7 (28%)	11 (44%)	7 (28%)
1991 - 2009	125	87 (70%)	11,498 (55%)	9,286 (45%)	24 (19%)	79 (63%)	22 (18%)

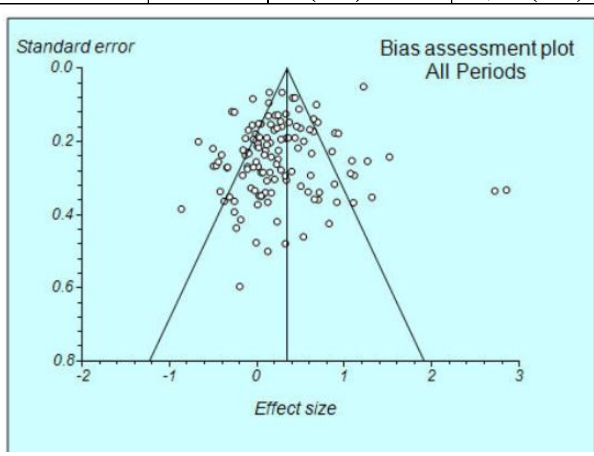


Fig. 15. The Bias with online tests

IV. IMPLEMENTATION AND DESIGN

In our research, we have planned to propose a new systematic online test for getting applicant skills. This test consists of 50 questions in the subject area that related to the general applicant qualification. Giving examples, someone has finished bachelor degree in Computer Science; the questions will comprise general computers subjects, such as database, programming, and networking.

The form test is multi-choice with the single correct answer; this means that the tester must choose one single answer between four given answers. Thus, this kind of test mostly checks the user understanding of the subjects. However, the arrangements of the questions are not ordered according to the subjects.

The amount of the time that has been given to the test divided into the number of issues. The total time is 60 minutes; however each question must take at most 72 seconds. The graduate student should finish the test with answering all the questions in 60 minutes. After that the system will stop, there will not be any possibility to make changes to answer. Furthermore, the instructor or the lab investigator will inform the attendance to stop using a computer. Furthermore, the test will be stopped when the time reached it is final destination automatically.

At the end of the test, each person who took the test after submitted the answers they will get a page that contain the information about his/her given answers. Also, they get the final result of the test on the computer. The requirements that have been used to build this online testing system are PHP and MySQL, LAN, and wide area networking. Also, the design of the system has constructed in cooperation with the eFront learning management system.

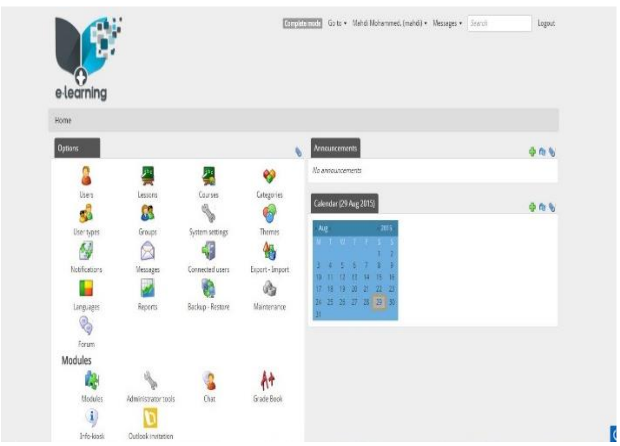


Fig. 16. System administrator panel

The same person who manage the tests and the databases who insert the questions and answers is the same employee who serves the website.

Fig. 17. Web administrator panel

In the following sections, it has been shown how the system was designed and implemented:

A. System administrator

The system controlled by an administrator, who control and monitor the whole system. Also, control the system database and their contents of data. Thus, all questions and answers will be entered by the admin, and the certificate will be printed out by him/her. Also, in this stage admin can add and remove users from the system.

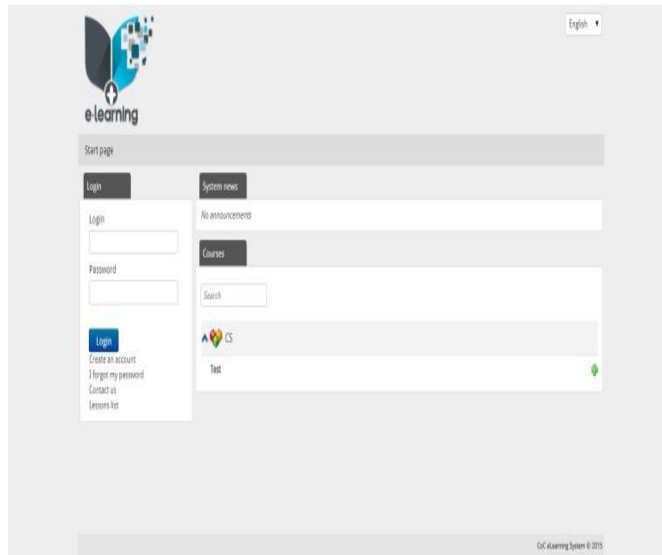


Fig. 18. Admin Login

B. User account creation

The graduate student will get an account to login to the system as a first stage. The reason for this security level is to protect user account from hackers. Therefore, username and password will be given them before the test.

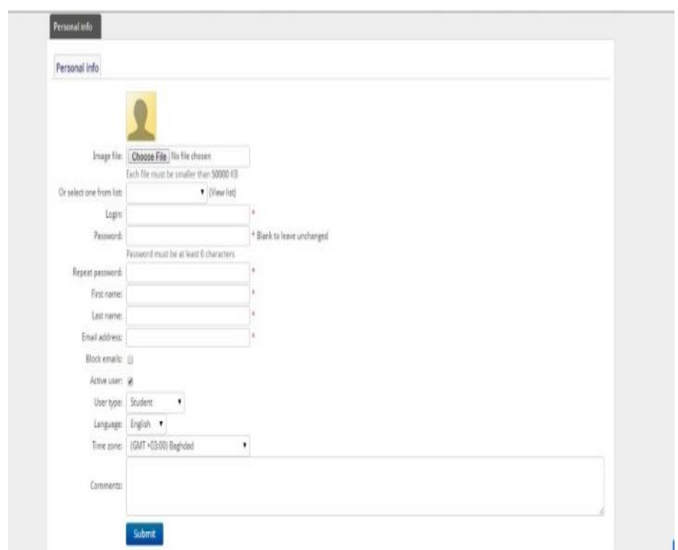


Fig. 19. User creating page

C. Questions and answer insertion

In this stage, admin can insert the question and responses to Mysql database using insertion that specified for that matter. Also, the question can be modifying later.

Fig. 20. Writing questions and answer

D. User login system

On the user part, users get a web page on their computer screen; these will be asked to enter their username and password, which they got it before the test. In the case of entering wrong username or password, they will be notified with error message tells the users that they have entered wrong username or password. However, in the case of entering correct username and password they welcomed and routed them to test page with multi-choice questions.

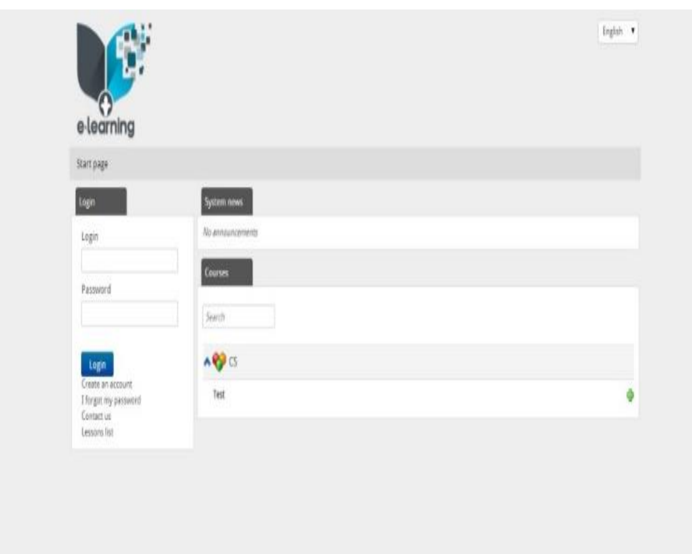


Fig. 21. User login page

E. Test Information Page

On this page users, will get information about the test, and this information is about the time, name of the subject, start and end time and number of questions. Users that do the test is very useful to have a general idea of it; this will help them to feel more comfortable while conducting the test.

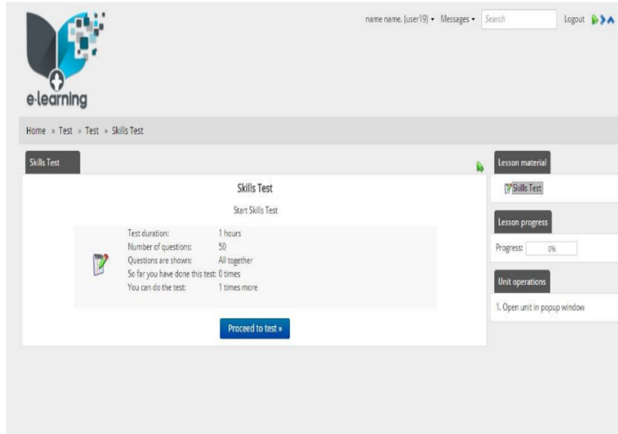


Fig. 22. Exams information page

F. List of questions page

In this page, the registered users will get the list of multi-choice questions that consist of 50 questions from different area subjects. Also in this page it can be noticed a time specified for answering the questions, which, in fact, each question has a specific amount of time (72) seconds.

Also, the weight of score for each question is equal to 2%, and this data has been found by using the following formula:

Score of the question * weight of score = real score

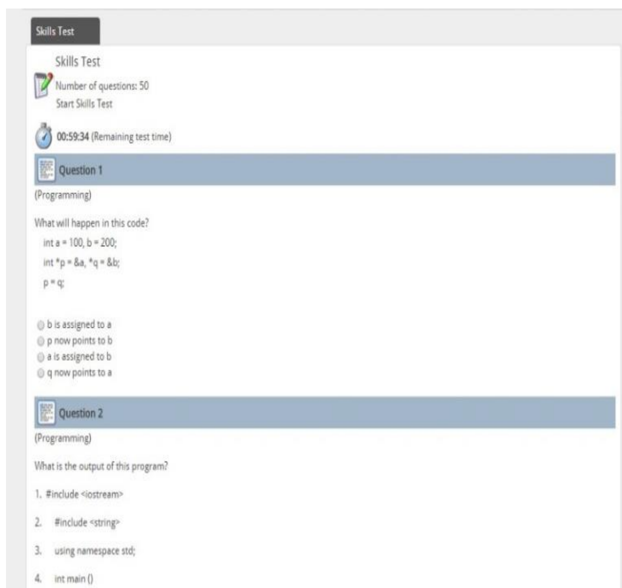


Fig. 23. First part of the question

Fig. 24. Last part of the question

G. Final Result and Feedback

At the last stage of the system, the users will get the outcome of the test at the time of submitting the answers. In this page, users can see the final score and can check their responses to know the false answers that they did in the test.

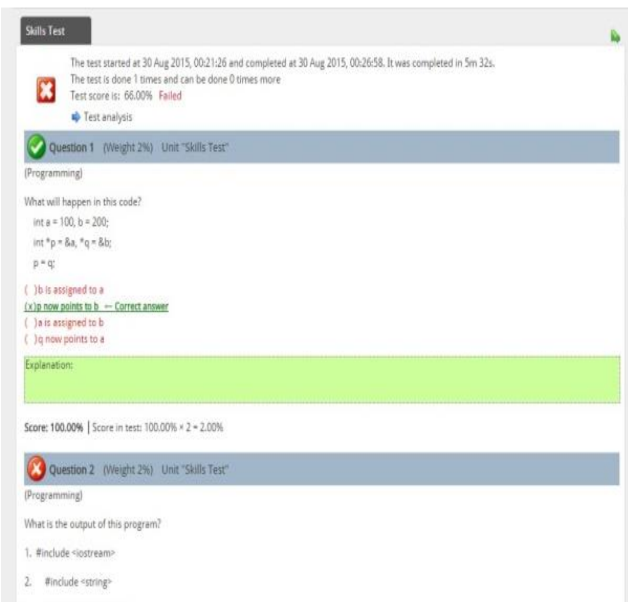


Fig. 25. Users answers feedback

H. Online System database

All of these data, including questions, answers and user account information, are stored in a place on the server that is a database server. Also, in this database that specified for online testing systems, there are many tables. In this chart is the main place that hold all the required data about the test.

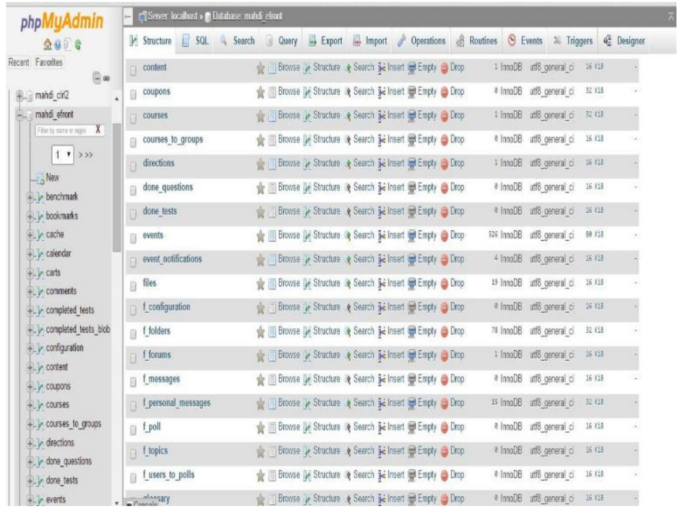


Fig. 26. Database of the system

I. Design process flowchart

Due to the fact, students of graduating universities must do some steps to complete the system, that all these process of d The main process of our system is showing in the following flowchart:

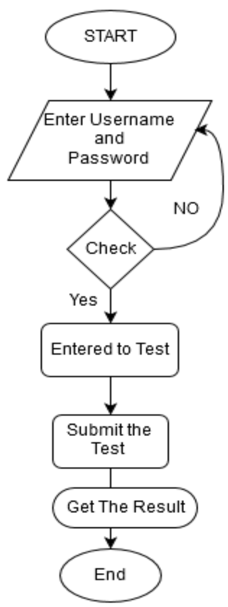


Fig. 27. Flowchart design

Users start with opening the web pages or the system. Then entering their username or password, if the username or password are correct, then they can enter the online test system successfully, if not they must re-enter the username and password correctly. After the finishing this step, user start to answer the questions and then submit the answer to the server and then they get the final result.

V. Result and Discussion

As a consequence of our system, each user of the system will have their account, and can use it to track their data. Also, the user will be given a username and password before the test, to login to the test web pages. As well as the username and password, users will get a private link that is the web pages that will load from the server, and displayed on the client screen. These web pages are contained questions that considered as online tests. However, these tests are tested on both wireless and wired networks, between 10 computers. Also, we used a server as the main machine to provide the web pages and data. In fact, all these computers and even smartphones are connected to a private network. However, in our system we made the test on private and wider network. So, we had done a test for ten persons who were graduated universities in a different range of subject areas.

Each of these 10 people answered all questions, and he or she tested the system on both sides, on private and on public as well. The way that they did on the public means they went on online web pages that we put our website on that host. So, they can access the test in the lab. Also, they got their grade at the time that they submitted the test. Through the given table and statistic chart, it shows the various range of data and grades from high to low grades. Also, the charts are given, shows that how each user was doing in each particular part of the question. This shows how a particular person did on specific professional skills. For example, a user may do a test in computer science skills knowledge. Also, this test comprises lots area of computer subject such as programming, database, and networking. Also, the result and chart shows that how each person even in each section.

It is clear from the table below that their nine columns contain the name of the subjects or section for each question meaning the categorized of the question into which area is related to each question. This shows that the overall score for each person that took the test and the test score which is out of 100%. Also, the total number of the questions are 50 questions. So, from column 3 to column 7 it shows how each user did in the subcategory questions. For instance, Aram Kamal got 12 correct in programming, Networking, Database, Security and 14 IT. Also, Aram Kamal got 58.37% as an Overall grade in the test. There is the amount of time at the last column that shows when each user finished the test. In other meaning how many minutes, it took to finish the test.

If we take Aram Kamal as an example again, it finished at 58.37 minutes.

According to the following statistic bar charts (see fig 28), it is the statistical data for the online test. This test has done for the one graduated students who finished university degrees bachelor and masters in computer sciences. In this test, we have planned to evaluate the knowledge skills in different computer science subject area. We include in our test subjects, Programming, Networking, Database, Security and IT. Moreover, those ten graduate students are asked to take the evaluation test to answer 50 questions in 60 minutes.

In bar charts, we can see, different statistics values and these values divided into subject categories, and the main one is the overall score for each one. As it is clear the user named Bilal was the candidate, who got the higher score among the rest of the other students.

On the other hand, and the lowest grade that has been recorded by students named Snwr and Huner, which they got just below 50%.

Also, the person who got the average result among the other participates was named Havar, who got exactly 50%. However, the person of the test got the same result that is 70% and this grade taken by the two graduated participants named Hazhar and Haidar.

Moreover, there is another point that can which is understandable from the bar chart that is the chart for each subject. Also, everyone who has placed in the statistic bar got their rate in each area of studies. So, the subject area that recorded the highest score by the students was IT Technologies that scored about 20%. Furthermore, in the second level database, was the subject that was recorded just about to 15%.

In addition to the grade evaluations, there is another important aspect, and this aspect is the amount of time for the test and the time that used by each student. In the image, there is a different range of finishing time for the online tests. Moreover, the fastest one who finished and submitted the test was in 11 minutes and 21 seconds, this was done by a participant named Bilal. Consequently, the slowest one was Aram, who finished the test in 58 minutes and 37 seconds. Furthermore, after all of these calculation and skills evaluation we came into account that each person has an excellent skill in a range of area subjects, and lack of skills in some others.

TABLE II. Online Test Result

First Name	Last Name	ProgramScore	Network Score	Data base Score	Security Score	IT Score	Final Score	Time
Aram	Kamal	12	12	12	12	14	62	58.37 Sec
Havar	Bakhtyar	12	6	14	10	12	54	31.49 Sec
Bilal	Najmaddin	14	14	18	16	20	82	11.21 Sec
Haidar	Abdulrahman	16	16	14	12	16	74	46.22 Sec
Hazhar	Najat	10	14	18	14	18	74	38.11 Sec
Snwr	Jamal	4	8	4	6	10	32	30.07 Sec
Bestan	Bahaddin	16	8	14	12	18	68	24.03 Sec
Nyaz	Ali	10	12	10	10	16	58	41.13 Sec
Rebwar	Rashid	12	6	8	6	18	50	47.22 Sec
Huner	Hiwa	8	6	8	8	10	40	30.39 Sec
Aram	Kamal	12	12	12	12	14	62	58.37 Sec
Havar	Bakhtyar	12	6	14	10	12	54	31.49 Sec

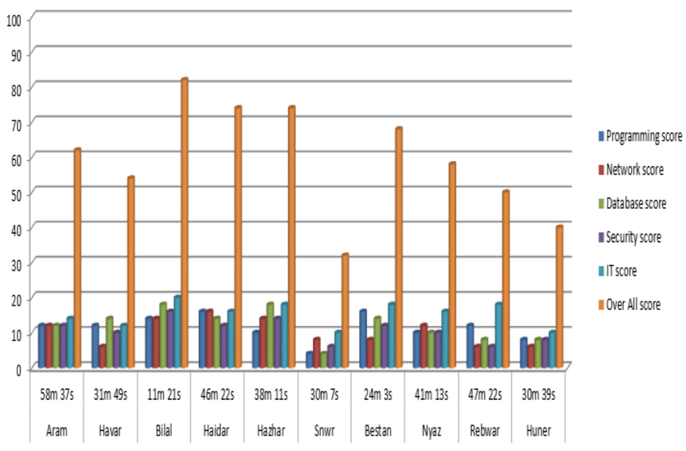


Fig. 28. User statistic results

In the table below, it shows the best skills and the worst one for each person who participated in the test. However, in some cases it can be seen that some of the test takers have more than one subject either as best skills or the worst one. Also in some other rows it says, "the rest of topics," means one of them are higher than another one. For example, the student named Aram Kamal got excellent skills in IT and the all the other area are considered as poor compare to IT subjects.

Another fact that has marked in the table is that most of the testers have got excellent skills in IT. This idea is obvious because most of the graduate students from computer sciences who want to work in company mostly adored the IT section.

In contrast to the best skill, in the poor skills column most of the applicant are suffering from lack of competencies in networking and programming as the top one, and security second one.

TABLE III. USER'S SKILLS

Student Name	Best Skills	Poor Skills
Aram Kamal	IT	The rest of subjects
Bestan Bahaddin	IT	Networking
Bilal Najmaddin	IT	Programming and Networking
Haidar Abdulrahman	The rest of subjects	Security
Havar Bakhtyar	Database	Networking
Hazhar Najat	Database and IT	Programming
Huner Hiwa	IT	Networking
Nyaz Ali	IT	The rest of subjects
Rebwar Rashid	IT	Networking and Security
Snwr Jamal	IT	Database and Programming
Aram Kamal	IT	The rest of subjects
Bestan Bahaddin	IT	Networking
Bilal Najmaddin	IT	Programming and Networking

VI. CONCLUSION

In the final part of this research, it has concluded that there are lots of demands to get a job by the graduated student from the universities and institutions. Also, they try to get jobs according to their skills with that they got from the organization that they studied.

Also, it is quite obvious from this research that most of the companies accept their employees according to the some rules. Also, one of them is testing skills, cause they afraid of unskillful people to be a member staff of the company, by doing a specific test related to their area of study.

However, it may make difficulties for some applicants to apply, because most of them are afraid to do the test because they do not want to fail in the exam, to protect their personality. Thus, the company does not wish to accept these people with low skills.

Moreover, using test during job application will make a competent between applicants rush to get a higher score. Thus, the company by this way can choose the best one with full of knowledge in the field that they work.

Also, those companies who offer that kind of job applications, provide a security environment between their appliers and employees. So, their account information and their exam results will be safe, so it provides a good way to interest people to apply.

The university policies have the same rules for their students who apply for higher education levels. They put an exam as one of their conditions to apply. Also, this condition is the most important one because each applicant must pass the exam even they got a higher score in the other part of the rules of applying for the higher education in the universities policies.

VII. FUTURE WORK

In the future research, there is a plan for doing this research to comprise wider area of studies:

- Getting result by SMS and E-mail
- There is a plan in the future to provide tests with a different form of testing including (filling-blank and writing description).
- Migrating to Linux server to store all the information, and to provide an area of security.
- Conducting tests on the Mobile Devices Smart Phone.

ACKNOWLEDGMENT

At the end of this research, we would like to thank University of sulaimaniyah for giving lots of facilities with computers and laboratories for doing our research. Also, we would like to send our thankful to all of our colleagues who helped us with completing this research.

REFERENCES

[1] L. Min, 'Design and Application of Online Testing System Based on Fuzzy Mathematics', AMM, vol. 182-183, pp. 1079-1083, 2012.

[2] X. Fu and S. Fu, 'Algorithm Analysis and Achievement for Function Module of Online Testing System Based on Web', AMR, vol. 850-851, pp. 714-719, 2013.

[3] D. Barton and D. Potts, 'Language Learning Online as a Social Practice', TESOL Q, vol. 47, no. 4, pp. 815-820, 2013.

[4] Kurniali, 'AN APPROACH TO ONLINE LEARNING USING LEARNING MANAGEMENT SYSTEM IN HIGHER EDUCATION INSTITUTION', Journal of Computer Science, vol. 10, no. 8, pp. 1517-1521, 2014.

[5] Y. Yang, 'The Design of Unified Identity Authentication and Single Point Login System', AMM, vol. 155-156, pp. 391-395, 2012.

[6] N. Raajan, G. Shiva, P. Vijayabhas, P. Mithun and J. Raj, 'Secured Login System', Research J. of Information Technology, vol. 5, no. 3, pp. 462-467, 2013.

[7] S. Aydoğdu and F. Başçiftçi, 'Methods Used in Computer-Assisted Bone Age Assessment of Children', JACN, vol. 2, no. 1, pp. 14-17, 2014.

[8] C. PEREZ-LEGUIZAMO and K. MORI, 'Timeliness Multi-Agent Coordination Technology in Autonomous Decentralized Database Systems', IEICE Transactions on Information and Systems, vol. 94-, no. 1, pp. 27-34, 2011.

[9] M. Chang and C. Cheng, 'How balance theory explains high-tech professionals' solutions of enhancing job satisfaction', Journal of Business Research, vol. 67, no. 9, pp. 2008-2018, 2014.

[10] 'The Job guarantee: toward true full employment', Choice Reviews Online, vol. 51, no. 01, pp. 51-0391-51-0391, 2013.

[11] 'Simple test confirms correct catheter placement', Springer Healthcare News, vol. 1, no. 1, 2012.

[12] A. Hershkovitz and R. Nachmias, 'Online persistence in higher education web-supported courses',The Internet and Higher Education, vol. 14, no. 2, pp. 98-106, 2011.

[13] R. Romsdahl and M. Hill, 'Applying the learning community model to graduate education: linking research and teaching between core courses', Teaching in Higher Education, vol. 17, no. 6, pp. 722-734, 2012.

[14] S. Orlando Gibelli, P. e Melo and S. Bogado Leite, 'Risk-Based Allowed Outage Time and Surveillance Test Interval Extensions for Angra 1', International Journal of Quality, Statistics, and Reliability, vol. 2012, pp. 1-13, 2012.

[15] E. Harris, 'Exam Q&A: time prioritizing', InnovAiT, vol. 5, no. 2, pp. 126-126, 2012.

[16] M. Tekkalmaz and I. Korpeoglu, 'Distributed power-source-aware routing in wireless sensor networks', Wireless Netw, 2015.

[17] M. Nada, M. Nakamura and H. Matsuzaki, '25-Gbit/s burst-mode optical receiver using high-speed avalanche photodiode for 100-Gbit/s optical packet switching', Opt. Express, vol. 22, no. 1, p. 443, 2014.

[18] W. Kim, 'On U.S. Homeland Security and Database Technology', Journal of Database Management, vol. 16, no. 1, pp. 1-17, 2005.

[19] 'How Portable Is Level-0 Behavior? A Test of Level-k Theory in Games With Non-Neutral Frames', Econometrica, vol. 82, no. 3, pp. 1133-1151, 2014.

[20] H. Khiat, 'An analysis of the relationship between learning satisfaction and academic achievement of non-traditional learners in Singapore', IJRSE, vol. 3, no. 1, 2014.

[21] D. Seo and G. De Jong, 'Comparability of Online- and Paper-Based Tests in a Statewide Assessment Program: Using Propensity Score Matching', Journal of Educational Computing Research, vol. 52, no. 1, pp. 88-113, 2015.

[22] J. Yang, 'Design on Online Examination System for College Chinese', AMM, vol. 687-691, pp. 2331-2334, 2014.

Secure Clustering in Vehicular Ad Hoc Networks

Zainab Nayyar
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad Pakistan

Dr. Nazar Abass Saqib
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad Pakistan

Dr. Muazzam Ali Khan Khattak
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad Pakistan

Nazish Rafique
Department of Computer Software Engineering, College of Electrical and Mechanical Engineering NUST, Islamabad Pakistan

***Abstract*—A vehicular Ad-hoc network is composed of moving cars as nodes without any infrastructure. Nodes self-organize to form a network over radio links. Security issues are commonly observed in vehicular ad hoc networks; like authentication and authorization issues. Secure Clustering plays a significant role in VANETs. In recent years, various secure clustering techniques with distinguishing feature have been newly proposed. In order to provide a comprehensive understanding of these techniques are designed for VANETs and pave the way for the further research, a survey of the secure clustering techniques is discussed in detail in this paper. Qualitatively, as a result of highlighting various techniques of secure clustering certain conclusions are drawn which will enhance the availability and security of vehicular ad hoc networks. Nodes present in the clusters will work more efficiently and the message passing within the nodes will also get more authenticated from the cluster heads.**

Keywords*—Vehicular ad hoc networks; secure clustering; wireless technologies; certification authority; cluster heads

I. INTRODUCTION

With The growth of wireless communication technology, two elementary wireless network models have been established for the wireless communication system [1] [2]. The fixed infrastructure wireless model consists of a large number of Mobile Nodes and relatively fewer, but more powerful, fixed nodes. The communication between a fixed node and a MN within its range occurs via the wireless medium. However, this requires a fixed infrastructure. Another system model, an Ad-hoc Network, it is a self-organizing collection of Mobile Nodes that form an infrastructure less wireless network on a shared wireless channel. Nodes which lie in the range of each other can easily communicate, while those which are far apart from each other communicate over the routers. Their deploying cost is relatively low as compared to other wireless networks because there is no necessity of a proper fixed infrastructure. Security is an important issue which is faced while deploying the ad hoc networks; the security issues under consideration are availability, confidentiality, integrity, authentication and non-repudiation [3] [4]. Availability refers that the system must survive in critical conditions such as denial of service and worm attacks. The attackers also try to create hindrance in the communication between the nodes and also try to interrupt the routing protocols. Confidentiality is the secret information requires safety so it cannot be disclosed to the unauthorized users. Integrity is that data should not be corrupted and the original information should remain original. Authentication is achieved by not to permitting those entities within the network which can harm the network and only register the trusted entities. In non-repudiation the source of the data should be safe and secure [6]. The concept of Vehicular Ad Hoc networks is derived from mobile ad hoc networks. The reason for deploying vehicular ad hoc networks was that over the years many motor accidents were observed leading to critical injuries, fatalities, and excessive cost on vehicle repairs. Since a proper solution was not efficiently worked out, therefore just like Mobile Ad Hoc Networks (MANETS); Vehicular Ad Hoc Networks (VANETS) were introduced in the cars for the sake of additional safety and comfort for vehicle drivers [2].

A VANET turns every participating car into a wireless router or node, allowin**g cars approximately 100 to 300** meters of each other to connect and, in turn, crea**te a network with a wide range** [5]. There are two main types of communications discussed under the section of VANETs: Vehicle to Vehicle communication (V2V) and Vehicle to Infrastructure communication (V2I). The former protocol is necessary to be applied on the vehicles for proper communication, Road safety and collision avoidance which are necessary for avoiding accidents. The later includes the provisioning of safety related, real time, local and situation based services such as speed limit information, safe distance and warning, lane keeping support, intersection safety, traffic jam warning and accident warning. All accidents are aimed to be saved by providing timely information related to the safety of cars and drivers [9].

Clustering means that different nodes in the system act as a whole system, securing a cluster means that to apply such protocols and actions on the clusters that it is not exposed to any attacker, malware etc. Securing actually belongs to the robustness of the system to certain attacks. The other issue due to which secure clustering is necessary is when there is a time of collecting and aggregating data from the nodes. At that time there are more chances of attacks for accessing the data by the attackers. Due to this reason secure clustering protocols are used for preventing and securing the clusters from various attacks [10].

In secure clustering there are symmetric as well as asymmetric algorithms used. In a symmetric algorithm there is often a shared key whereas in an asymmetric algorithm there is a requirement of secure mapping of public keys with the user's identities using public key infrastructure. PKI is often used in certification authority where a digitally signed certificate is issued to every registered user so that they can get their public key [11].

This paper gives the state-of-the-art review of typical secure clustering techniques for vehicular ad hoc networks. It is impossible to say which technique is better for a given condition. Hence, the motivation is to compare these strategies this paper includes new technical trends such as public key infrastructure, Shamir secret key algorithm, dynamic demilitarized zone etc. The rest of the paper comprises of II literature review, III comparative analysis, IV conclusion and future work and V references.

II. Literature Review

A. Key Management in Ad hoc Networks

In [5] key management in ad hoc networks was addressed, where in ad hoc networks the old methods to achieve security were not adaptable. Due to these factors key management was very difficult in ad hoc networks. In key management technique the public key infrastructure used a centralized approach in similar clusters and a distributed key was used between the cluster heads. It resulted in suitable, economical, scalable and autonomous key management.

B. Shamir's Secret Scheme

It is observed in [6] that in ad hoc networks it was easy to launch worm, man in the middle, denial of service attacks and to inoculate a malicious node, this was all done due to the lack of data integrity. The Shamir's secret scheme along with data redundancy mechanism of certificate revocation and renewal was applied. It was a hop by hop protocol. On every hop the data got authentication from certificate authority. Each node had the authority of checking the behavior of its previous node and on the basis of that behavior it could declare that node as malicious or trustworthy. The detection of malicious node became easy. During packet delivery less overhead and delay occurred.

C. Threshold Cryptography

In the [11] architecture was proposed for securing the clusters in ad hoc networks. A network was divided into clusters and a decentralized certification of authority was implemented. Decentralization was achieved using threshold cryptography and a network secret. The reason for deploying decentralized approach of distributing a certification authority on the nodes was that the ad hoc entities were vulnerable to several attacks and their reachability was not possible for all the nodes of the network. In the intra cluster security asymmetric key distribution was used. These keys used to protect all the traffic nodes. The attackers could not break the secrets even if they got some data it was of no use to them. Scalability and availability was achieved by dividing the network into small clusters. Availability was enhanced because certificates can be issued even if some nodes were out of reach. The asymmetric key distribution was useful in a way that there were no other means needed to secure the communication.

D. Trust Based Physical Logical Domains

The aim of [12] was to achieve trust on the basis of keys in mobile ad hoc networks. The trust based physical logical domains was introduced for grouping nodes and getting distributed control over the network.

E. Secure Message Aggregation & Onion Signature

In [13] two methods were introduced – first was the approach of secure message aggregation, and second was onion signature which was declared as a part of onion routing. The highlighted problem was that asymmetric solutions were resource hungry in the case of communication and computation. The accuracy in aggregation of vehicles depends upon the density of vehicles, the higher the density the greater the accurate aggregation. The grouping of vehicles was set geographically normally the range set is 300m. When the vehicle (leader) moves out of range, the election procedure takes place and the vehicle having lowest ID is declared as a leader. For security purposes the IDs which vehicles generate were not their actual IDs instead they were pseudonyms. Grouping of several messages provide the receiver with more information regarding the specified event. Simplicity and robustness was achieved by dividing the roads into cells. Using PKI and digital signatures authentication was achieved. Reduction in the network traffic due to aggregation of messages and achieved availability. Efficiency and routing benefits are achieved due to election of leaders. Data verification is escaped due to the aggregation of messages. The division of roads into cells can cause an overhead and thus this aspect needs to be improved. Due to aggregation false data can be inserted by the attackers into the network that is why only honest nodes could apply this algorithm. Combining signatures could create security overhead and delay.

F. Secure Clustering Algorithm

Mobile ad hoc networks are increasing in size day by day so in [14] a problem aroused in which due to the growth of nodes in number it became difficult to handle them. So a secure method was to divide the nodes in an hierarchal way which was known as secure clustering algorithm that provided more effectiveness, protection and trust in increasing the size of the cluster. It also defined how much a node could be trusted and by allocating certificates protecting the nodes from certain attacks. The algorithms which were previously defined for managing clusters were not helpful for managing big clusters. Secure clustering algorithms proposed a weight based algorithm which includes the certain parameters for electing the algorithm.

G. Position Based Prioritized Clustering

In [15] due to rapid change in the positions of cars during long journeys, change of direction and network topologies some information may be lost. So for solving that issue, position based prioritized clustering was implemented and for that CORSIM and NS-2 simulators were used. The radius regarding each cluster was taken under consideration as any node could be a part of the cluster until it gets out of the range of radio frequency. So if the radius of any node considers being the greater than the specified radius than that vehicle was no more than the part of that cluster. If the threshold between two clusters was less than that which was set, then the cluster with lesser nodes became a part of another cluster. The MDS election algorithm is followed in which the election of cluster heads is defined; this algorithm was the solution of the problem which was created due to the presence of many cluster heads formation which was caused due to other cluster head election algorithms. Using MDS technique stability in the performance of cluster heads was increased. Position based prioritized clustering was helpful in decreasing the cluster overheads.

H. Fully Distributed Trust Based Model

In [16] the problem identified was the creation of the trusted environment by applying the techniques applied on fixed networks security and trust could not be achieved therefore a fully distributed trust based model was proposed in which ad hoc networks generate and distribute a public key without any fixed mode of transmission. A threshold was also included in the public model so that the malicious nodes cannot get the authorized key from the certification authority.

I. Dynamic Demilitarized Zone Technique

In [17] the problem identified was that many anonymous nodes sometimes become successful in getting signed certificates, so the dynamic demilitarized zone technique was introduced in which the unknown nodes were not authorized to communicate with the certificate authority nodes. All the nodes have to pass through the dynamic demilitarized zone to request the certificate from the certificate authority node. There were multiple certificate authorities involved in that algorithm each of which was responsible for its own geographical area. The road side units were also combined with the central certificate authorities who worked as an intermediate between the central certificate authorities and dynamic certification authorities on the road. Along with dynamic certification registration authorities and sub cluster heads were also involved in this mechanism. Reference [21] was the extension of [17] as in [17] the issue was detected during the election of certification authorities in which denial of service was occurring. The issue was solved in [21] using VANET dynamic demilitarized zone that would handle the certificate request from the unknown vehicles and prohibit malicious communication between certification authority and nodes. Its additional feature was that each vehicle which was at 1-hop from other vehicles sent hello messages, as result the nodes which received that message saved the each and every record of the vehicle and thus response with a joint message to that node. Detection of malicious nodes became more efficient. Confidentiality increased, overhead decreased. Shifting from one cluster to another enhanced due to the presence of sub cluster heads. It removed the issues of denial of services.

J. Distributed Algorithm:

In the [18] the distributed algorithm was used in the protocol for the security and formation of the cluster, the system also checked that if the claimed data was reliable and authentic. The cost delivery protocol, cluster head designation protocol and cluster management protocol are used for cluster formation. It provided the reliability and authenticity of data. The biggest risk of deploying this technique is that according to the supposition all the data is considered to be correct and authenticated.

K. Vehicular Clustering Based On Weighted Clustering Technique:

In [19] three suitable scenarios that are mainly for highway traffic were discussed. The first was that was used for choosing the cluster heads giving different parameters which could improve stability, connectivity and security of VANETS. The second technique was the Adapter allocation of transmission range which used hello messages and ensured connectivity among the vehicles. The third scenario was Monitoring of malicious vehicles to detect abnormal vehicles in the system. The re-affiliation issue in which the swapping of clusters occurred caused the great overhead, so this problem was also resolved by reducing the swapping of clusters. In [22] secure and stable vehicular clustering based on weighted clustering algorithm was proposed in which secure and stable cluster formation along with malicious node detection was done. The issue which was resolved due to its deployment was that if a cluster was very large then the Cluster head could not deliver the messages efficiently and if it was very small then the clusters may not be stable and thus re-affiliation took place. Secure and stable vehicular clustering based on weighted clustering algorithm worked on cluster creation and cluster maintenance. Communication cost for joining the cluster increased. It provided better ways of creating and maintaining clusters.

L. Virtual Forces Virtual Clustering:

The algorithm which was mentioned in [20] was virtual forces virtual clustering which was used to create stable clusters in an urban environment. Virtual clustering virtual forces not only took care of current positions but future positions also and their relative velocities also but only for those vehicles which keep their lane.

III. COMPARATIVE ANALYSIS

In [5] clustering consisted of grouping of nodes whereas every cluster had a cluster head. The proposed solution i.e key management in ad hoc networks split the nodes into groups known as clusters. It used a threshold scheme to distribute the key in the cluster to achieve security of the cluster, and protection of the key against denial of service attacks. By applying this technique not only the certificates for the cluster heads are generated but also the nodes can join the new cluster heads by getting certificates from them. Inter and intra cluster authentication, integrity, confidentiality and non repudiation were achieved.

The aim of [6] was to achieve data integrity using three components which were monitoring routing cum forwarding, certificate renewal and certificate revocation. The routing cum forwarding scheme detected the problems with the routing protocols and data; whereas, certificate renewal method by sending more than one shared key to the node guarantees the presence of original nodes in the network. Certificate revocation assured the removal of malicious nodes from the network. The certificate authority while approving certificates to the nodes mentions the node ID, initiation time and expiry time. These approaches altogether deployed in Shamir's Secret Sharing Model. Thus the integrity of data is achieved.

The problem highlighted in [11] due to the usage of centralized certification authority was solved by using decentralized scheme and thus a secret sharing scheme known as proactive secret sharing is used in ad hoc networks. In this technique secret keys changed periodically without changing the secrets, so it is difficult for the attacker to break the secret keys. A clustering technique was also mentioned in which all the nodes (cars) were divided into small clusters there were cluster heads and gateways. Gateways were also cluster heads but they were helpful in communicating between different clusters, whereas cluster heads were only responsible of maintaining communication among the nodes of the cluster. Cluster Heads had information regarding the different nodes and their actions within the clusters whereas Gateways also had information of other clusters too. To make clustering secure a private key was distributed among all the cluster heads by the certification authority and from cluster heads a public key was distributed among the nodes of the cluster. If a node found no cluster to be attached with it, it declares itself as a cluster. There was an inter network communication which is between different clusters and intra network communication which was among the network. In an intra network, an asymmetric communication is observed at cluster heads level but symmetric level communication was held between nodes of a cluster for making communication smoother and better. Apart from these the ways of merging the clusters, logging on of the nodes and routing strategies are also discussed. The advantages which were observed in this method were that the merging techniques of clusters were elaborated in a cost effective way. Secondly availability was enhanced because certificates could be issued even if some nodes were out of reach. The security infrastructure was more resistant to the intruders so integrity was achieved.

In [12] the author derived the trust formalization from watch dog and path rater used for grouping the nodes in ad hoc networks. In the evaluation of trust model the approaches used were namely, optimistic or greedy approach, simple average weighted products, weighted average and double weighted approach.

In [13] the resource hungry solutions of cryptography were eliminated by introducing the concept of secure message aggregation and onion signature. The technique for the symmetric group key distribution was secure VANETs Group Protocol. In this technique roads were divided into cells having a leader which distributes a public key to the nodes. The basic advantage of this was simplicity and robustness but the overhead that was produced left the large space for improvement. The grouping of vehicles was set geographically normally the range set was 300m when the vehicle (leader) moved out of the range, the election took place in the vehicle having lowest ID was declared as a leader, for the security purposes the IDs which vehicles generate were not their actual IDs instead they were pseudonyms. In the secure message aggregation technique several sort of signature methodologies were observed which includes combine signatures, concatenate signatures, onion signatures and hybrid signatures. In combine signatures to save time of data verification and cheated messages, the entire distributed signature from the group were combined to check the validity of the message and then sent to the group so that the combining of signatures was evidence that the message was verified and correct. In concatenated signatures a vehicle that received a correct message appended its signature with the already existing signatures and rebroadcasted the message. The message was then distributed over the group with the appended new signature with the already existing signature of each node that also eliminated data verification but could cause overhead. Another difficulty was to reduce the size of signature as the signature size was considered as constant. Therefore, the Onion signature strategy was deployed in which the vehicle only kept the signature of the last one which sent a message and on the next hop sent the message with its signature so the new vehicle which would receive its message would overwrite the message signature with its own and the process continued.

In [14] the basic parameters which were derived for deploying secure clustering algorithm were max value, min value, d-hop clusters, identity ID and weight these parameters were also involved in the election criteria. To elect the cluster heads several criteria were defined in secure clustering algorithm such as trust value in which it was analyzed how much any node could be trusted by its neighbors. Degree was another criteria which was defined in terms of specified radius, it was checked that whether a node with in a given radius servers maximum nodes or not. In battery power it was observed that for how much time a node could serve and the max value determined the cluster head which could handle more neighbors. Stability was decided on the basis of distance and average distance, distance between the two nodes tell the hops between the nodes and average distance checked the mean distance so by checking these parameters the most stable node as cluster head could be decided. Clusters heads regularly sent beacons to the nodes where the structure of beacon composed of cluster head certificate and the command which was assigned to the node by the cluster head. The election algorithm invoked when the nodes of a cluster needed to maintain their architecture so it required several stages such as discovery stage for selecting a node to participate in the election algorithm and the computed weight on the basis of which the node could be selected as a cluster head.

In the position based prioritized scheme [15], each node and cluster head was assigned a unique ID, node geographical location, and the ID of next node to whom it would communicate and the priority number of the node. So in that way a stable cluster structure came to its existence. If a cluster got out of the radio frequency area, it could join the new cluster on the basis of the attributes given to it. A special cluster head election algorithm was designed which told about the selection of new cluster heads under different situations. In MDS clustering algorithm the node which had a longer trip or remained in travel longer could be declared as the cluster heads and that vehicle assigned the higher priority. To avoid the cluster heads loosing connectivity the cluster head had the authority to work as the cluster head until its velocity remained within the average speed otherwise the cluster would again calculate the priorities and chose a new cluster head.

In [16] a fully distributed public secret sharing key trusted model was applied which aimed to maintain a trust relationship in mobile ad hoc networks and prevented the network from the authorization of a malicious nodes without the involvement of any third party. For achieving the objective threshold cryptography was also included in the network. This technique generally included four basic operations namely initialization phase, joining the system, partial certificates creation and exchange and public key authentication. In the initialization phase the nodes get initialized with the inclusion of threshold cryptography. In the joining phase each node could enter or leave the system without any restriction. In the certification creation and exchange a private and public key was issued to the user if the public key belonged to the user, the user signed a certificate. In the public key authentication phase when the nodes needed to authenticate a public key of another node they merged their partial trust graphs according to the trust model.

In [17] dynamic demilitarized zone technique was a one hop from the certificate authority. Its goal was to register only known and trusted nodes whereas all the other nodes which were unknown and untrusted nodes would not be registered. So all the nodes which wanted to get registered would pass from dynamic demilitarized zone. All the trusted nodes would maintain a trust table in which the record of each trusted node would be maintained along with its public key. There were multiple certificate authorities involved in this algorithm each of which was responsible for its own geographical area. The road side units were also combined with the central certification authorities that worked as an intermediate between the central certification authorities and dynamic certification authority on the road. There was a trust matrix defined in which for untrusted node the value of Tm=0.1 and for trusted node = 1. Registration Authority was responsible to act as a Dynamic demilitarized zone as it checked the level of trust of each node and then moved that node to get signed certificate. A Sub cluster head was responsible to create communication between many clusters. If a node left a cluster, the Sub cluster head was responsible for adding that node into another cluster on the basis of its trust level. In [21] a concept of dynamic key distribution was observed in which there were multiple central certificate authorities present at their respective geographical areas and an asymmetric key distribution algorithm was used. All the vehicles had to pass from VANET dynamic demilitarized zone to request a certificate from a certificate authority. Its additional feature was that each vehicle which was at 1-hop from other vehicles sent hello messages as result the nodes which received this message saved each and every record of the vehicle and thus respond with a joint message to that node. Hello messages were also used during election algorithm.

In [18] there was a global Certificate authority and a local Certificate authority. The global Certificate authority was responsible for issuing certificates if different clusters wanted to communicate with each other whereas local Certificate authority was responsible for issuing certificates with in the cluster for proper communication. They used symmetric key distribution algorithm along with many protocols such as cluster management protocol, cluster head designation protocol and cost delivery protocol. However, the biggest risk of deploying this technique was that according to this supposition all the data was considered to be correct and authenticated.

In [19] three algorithms were introduced; the first one was the vehicular clustering based on weighted clustering. Some parameters were needed to be set while deploying this technique. T_d was set as distrust value and sigma was the threshold. Two lists were maintained by the vehicles if the T_d value of the vehicles was less than the threshold then they were maintained in the white list and if T_d value was greater than they were sent in black list. The copy of black list was sent to all the nodes and clusters that came under the area of particular Certificate authority. For each vehicle setting itself as a cluster head sent its user name and ID to all the nodes. On the basis of certain criteria the node could declare itself as a Cluster head. The criteria could be decided by performing five steps mentioned in [19]. Another algorithm was the adaptive allocation of transmission range algorithm which catered to the problem where sometimes messages cannot transfer to their neighbors on time due to topology changes or variable frequency. Thus through the application of this algorithm, the vehicles could find their neighbors dynamically. This algorithm also involved three steps mentioned in [22]. The third and last algorithm was monitoring of malicious vehicles. This algorithm would simply monitor the abnormal vehicle and cater out its abnormality factor. The algorithm mentioned in [22] named as Secure and stable vehicular clustering based on weighted clustering algorithm was similar to that mentioned in [19]. But the issue which was resolved due to its deployment was that if a cluster is very large then the Cluster head could not deliver the messages efficiently and if it was very small then the clusters might not be stable and thus re-affiliation took place. Secure and stable vehicular clustering based on weighted clustering algorithm worked on cluster creation and cluster maintenance.

The Virtual clustering vehicle forces [20] applied Coulomb's law to assign the virtual forces to the network; vehicles were considered as charged particles, and force was applied on the vehicles which needed to be communicating on the basis of relative velocity and distances. When vehicles moved away from each other, they gave negative force and vice versa. "$\mathbf{F_{rel}=k\ q_iq_j/r^2_{ij}}$", the charge of every vehicle was proportional to many parameters of that vehicle. 'r' was the distance, q_i q_j are the vehicles at certain directions and k depends on the factors present in the equation.

Table 1 mentioned below shows the brief comparison of the related works and comparative analysis.

TABLE I. COMPARATIVE ANALYSIS OF VANET TECHNIQUES

R. No	Technique	Availability	Confidentiality	Integrity	Non repudiation	Authentication
[7]	Public key Infrastructure & threshold cryptography	Decrease	Increase	Increase	Increase	Increase
[8]	Shamir's secret scheme	Increase	Medium	Increase	Increase	Increase
[13]	Proactive Secret sharing	Increase	Increase	Increase	Medium	Increase
[14]	Trust based model	Decrease	Medium	Medium	Increase	Increase
[15]	Secure VANET group protocol	Decrease	Medium	Increase	Increase	Increase
[16]	Secure clustering algorithm	Increase	Medium	Medium	Increase	Medium
[17]	Position based prioritized clustering, MDS	Increase	Decrease	Decrease	Decrease	Decrease
[18]	Fully distributed trust based model	Decrease	Medium	Medium	Increase	Increase
[19]	Dynamic demilitarized zone	Decrease	Medium	Medium	Increase	Increase
[20]	Distribution algorithm	Decrease	Medium	Increase	Medium	Increase
[21]	Vehicular clustering based on weighted clustering	Increase	Increase	Decrease	Increase	Increase
[22]	Coulomb's Law	Increase	Decrease	Decrease	Decrease	Decrease
[23]	VANET dynamic demilitarized zone	Increase	Increase	Medium	Medium	Increase
[24]	Secure and stable vehicular clustering based on weighted clustering algorithm	Increase	Medium	Medium	Medium	Increase

IV. CONCLUSION & FUTURE WORK

A. Conclusion

In summary, secure clustering can efficiently support a wide variety of applications that are characterized by a close degree of collaboration, typical for many VANETs. And the design of the secure clustering algorithms are driven by specific goals and requirements based on respective assumptions about the network properties or application areas.

This paper presents a comprehensive survey of the secure clustering techniques for VANETs. The purpose of this paper is to survey the secure clustering techniques and study their primary principles. It discuss the characteristics, security properties of each of these clusters selected from the class of similar approaches, which can reflect the state of- the-art research work on secure clustering techniques. The classifications of the primary secure clustering principles can simplify the task of a network designer in deciding the clustering strategies to be adopted at a given condition.

Then, it is believed that this survey will be very useful to the research community and also serve as a great introductory material for someone embarking on VANETs.

B. Future Proposition

As mentioned earlier, research in the area of secure clustering algorithms over VANETs is far from comprehensive. Much of the effort so far has been on devising secure clustering techniques to support effective and efficient communication between nodes that are part of a same group. However, there are still many topics that deserve related to security while clustering the VANETs.

REFERENCES

[1] Christian Lochert, Hannes Hartenstein, Jing Tian, Holger Füßler, Dagmar Hermann and Martin Mauve: A Routing Strategy for Vehicular Ad Hoc Networks in City Environments Traffic Assistance Systems, Intelligent Vehicles Symposium, 2003, Proceedings. IEEE, pages 156 – 161, 2003

[2] Syed R. Rizvi, Stephan Olariu, Cristina M. Pinotti, Shaharuddin Salleh, Mona E. Rizvi and Zainab Zaidi: Vehicular Ad Hoc Networks,

International Journal of Vehicular Technology, Volume 2011, 2 pages, 2011

[4] Drs. Baruch Awerbuch and Amitabh Mishra: Introduction to Ad hoc Networks, CS-647: Advanced Topics in Wireless Networks, 2008

[5] Mohamed Elhoucine Elhdhili, Lamia Ben Azzouz and Farouk Kamoun: A Totally Distributed Cluster Based Key Management Model for Ad hoc Networks

[6] Rajaram Ayyasamy and Palaniswami Subramani: An Enhanced Distributed Certificate Authority Scheme for Authentication in Mobile Ad-hoc Networks, The International Arab Journal of Information Technology, Volume 9, pages 291-298, 2012

[7] Xue Yang, Jie Liu, Feng Zhao and Nitin H. Vaidya: A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning. Mobile and Ubiquitous Systems: Networking and Services, 2004, MOBIQUITOUS 2004, The First Annual International Conference, pages 114 – 123, 2004

[8] Marc Torrent-Moreno, Jens Mittag, Paolo Santi, and Hannes Hartenstein: Vehicle-to-Vehicle Communication FairTransmit Power Control, Vehicular Technology, IEEE Transactions, Volume:58, pages 3684 – 3703, 2009

[9] Pavle Belanovi´c, Danilo Valerio, Alexander Paier, Thomas Zemen, , Fabio Ricciato and Christoph Mecklenbr¨auker: On Wireless Links for Vehicle-to-Infrastructure Communications, Vehicular Technology, IEEE Transactions, Volume 59, pages 269 – 282, 2010

[10] Sanaz Sadeghi and Behrouz Sadeghi: Designing Secure Clustering Protocol With The Approach Of Reducing Energy Consumption In Wireless Sensor Networks, The International Journal of Computer Networks & Communications (IJCNC), Volume 5, 2013

[11] M. Bechler, H.-J. Hofi, D. Kraftt, E Pmket and L. Wolf: A Cluster-Based Security Architecture for Ad Hoc Networks, Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, Volume 4, pages 2393 – 2403, 2004

[12] Mohit Virendra, Murtuza Jadliwala, Madhusudhanan Chandrasekaran and Shambhu Upadhyaya: Quantifying Trust in Mobile Ad-Hoc Networks, Integration of Knowledge Intensive Multi-Agent Systems, 2005, International Conference, pages 65-70, 2005

[3] Lidong Zhou, Zygmunt J. Haas and Cornell: Securing Ad Hoc Networks, Network, IEEE, Volume 13, pages 24 – 30, 1999

[13] Maxim Raya, Adel Aziz and Jean-Pierre: Efficient Secure Aggregation in VANETs, Proceedings of the 3rd international workshop on Vehicular ad hoc networks, Pages 67-75, 2006

[14] B. Kadri, A. M'hamed, M. Feham: Secured Clustering Algorithm for Mobile Ad Hoc Networks, IJCSNS International Journal of Computer Science and Network Security, volume 7, pages 27-34, 2007

[15] Zhigang Wang, Lichuan Liu, MengChu Zhou and Nirwan Ansari: A Position-Based Clustering Technique for Ad Hoc Intervehicle Communication, Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions, Volume 38, pages 201 – 208, 2008

[16] Mawloud Omar, Yacine Challal, and Abdelmadjid Bouabdallah: Fully Distributed Trust Model based on Trust Graph for Mobile Ad hoc Networks, Published in Computers & Security, 2009

[17] Tahani Gazdar, Abdelfettah Belghith and Abderrahim Benslimane: A cluster based secure architecture for vehicular ad hoc networks, Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference, pages 1 – 8, 2010

[18] Helena Rifà-Pous, Jordi Herrera-Joancomartí: A Fair and Secure Cluster Formation Process for Ad Hoc Networks, Journal Wireless Personal Communications, volume 56, pages 625-636, 2011

[19] Ameneh Daeinabi, Akbar Ghaffar Pour Rahbar and Ahmad Khademzadeh: VWCA: An efficient clustering algorithm in vehicular ad hoc networks, Journal of Network and Computer Applications, Volume 34, Pages 207–222, 2011

[20] Leandros A. Maglaras: Clustering in Urban environments, Virtual forces applied to vehicles. Communications Workshops (ICC), 2013 IEEE International Conference, pages 484 – 488, 2013

[21] Tahani Gazdar, Abderrahim Benslimane, Abdelfettah Belghith and Abderrezak Rachedi: A secure cluster-based architecture for certificates management in vehicular networks, 2013.

[22] Ankit Temurnikar, Dr.Sanjeev Sharma and RGPV Bhopal: Secure and Stable VANET Architecture, Journal IJCSN publisher, volume 2, pages 37-43, 2013.

An Analysis of Encryption and Decryption Application by using One Time Pad Algorithm

Zaeniah
Academy of Computer Information Management Mataram
AMIKOM Mataram
Mataram, Indonesian

Bambang Eka Purnama
School of Information Management and Computer
"Nusa Mandiri", STMIK Nusa Mandiri
Jakarta, Indonesian

***Abstract*—Security of data in a computer is needed to protect critical data and information from other parties. One way to protect data is to apply the science of cryptography to perform data encryption. There are wide variety of algorithms used for encryption of data, this study used a one-time pad algorithm for encrypting data. Algorithm One Time Pad uses the same key in the encryption process and a decryption of the data. An encrypted data will be transformed into cipher text so that the only person who has the key can open that data. Therefore, analysis will be done for an application that implements a one-time pad algorithm for encrypting data. The application that implements the one time pad algorithm can help users to store data securely.**

Keywords—cryptography; algorithms One Time pad; encryption; Decryption

I. Introduction

Security of data in a computer is very important to protect the data from other parties that do not have the authority to determine the content of the data [1]. If the data has a very high value that has been stored in the computer and then opened by another party then it would be very detrimental.

One way to protect data is to password protect the data. But now to unlock the data that is already widely available password receipts of software that we can use. Another way that is used for encoding is to use the science of cryptography is to encrypt the data so that the data can not be read, deleted and changed by others[4].

Science of cryptography has been applied since ancient times to the present in accordance with technological developments. Various kinds of complex algorithm created as a tool to encrypt data one of which is the algorithm One Time Pad. The advantage of the one-time pad algorithm is to perform the encryption process and a decryption of each character plaintextnya use each character in the key. One Time Pad This algorithm uses the same key to encrypt and a decryption of the data. [1]

There are many algorithms are created to make applications in addition to data encryption algorithms One Time Pad one of which is the DES algorithm (Data Encryption Standard). DES is an algorithm that has the Feistel structure so that the structure of the encryption and the same decryption. But the DES key possessed only 56 bits that are considered unsafe[5]. Therefore, it will be created an application for data encryption as well as a decryption applying modern algorithm is an algorithm one time pad. One time pad algorithm is only used one time for one key encryption key then it will be destroyed and not used again to encrypt other data. In this study will be discussed regarding the encryption process and the decryption of data using one-time pad algorithm. This research is expected to be useful to be able to protect the data of those who do not have the authority to fill in the data so that data confidentiality is maintained properly.

II. Review of Related Literature

Cryptography is derived from the Greek, crypto and Graphia. Crypto means confidential while Graphia means writing. In the term of the terminology, cryptography is the science and art that is used when a message is sent from one place to another to maintain the security of the message. Engineering data encryption (cryptography) is applied to the data and information, performed by encoding or hiding the original data. In cryptography, a message which will be kept secret called the plaintext and encrypted messages that have been called cipher text. In 1960s, the development of computers and communication systems has an impact on the demand of the parties - certain parties to provide various security services and protect information in digital form.

One-time pad (OTP) is a stream cipher encryption and decryption of one character each time. This algorithm was found in 1917 by Major Joseph Mauborgne as the improvement of the Vernam cipher to produce the perfect security. Mauborgne proposes the use of one-time pad (pad = paper notebooks) which contains the generation of random sequences of characters - a key character. To encrypt a message pad, it is simply used once (one-time), afterwards to encrypt messages, the pad that has been used cab be destroyed in order that no one can used it[12].

III. Research Method

The techniques of OTP algorithm uses a stream cipher manner in which the proceeds of the XOR cipher between plaintext bit and bit key encryption and XOR the hash value of the password.

For examples:

Samples are taken from a sentence "The World is wonderful" if it is represented into byte it would be "87 111 114 108 100 32 105 115 32 119 111 110 100 101 114 102 117 108 108 "(19 Byte without the quotes).

While each byte of data is read randomly generated bytes are used as keys, for example: "234 119 208 217 14 109 212 144 71 40 150 242 27 135 180 125 223 120 73 "(19 bytes without the quotes).

Taken a password for example: "ZAENIAH" after the one-way hash function obtained hash value is "3100" (4 bytes without the quotes).

The results of encryption are:

```
        87  111 114 108  100 32  105  115  32 119 111 110
                 100 101 114  102  117 108 108
XOR     234 119 208 217 14 109 212 144 71  40 150 242 27
                 135 180 125 223 120 73
        ______________________________________________
        189 24 162 181 106 77  189 227 103 95 249 156 127
                 226 198 27 178 20 37
XOR     3100
        ______________________________________________
        3233 3076 3262 3241 3190   3153 3233 3327 3195
         3139 3301 3200 3171 3326 3079 3246 3080 3129
                          (19 byte)
```

The results of encryption is "3233 3076 3262 3241 3190 3153 3233 3327 3195 3139 3301 3200 3171 3326 3079 3246 3080 3129" (19 bytes without the quotes).

The results of byte values obtained through XOR encryption between each plaintext byte and byte key value and the password hash value, then the creation of the software, which need to be considered in data decryption by using OTP algorithm that is a random number generator and key word.

For the random number generator, or in this case to obtain the encryption key, the process by means of a generator or random number generator (RNG) that generate a key from the keyboard and mouse input values and random noise. As for the management of this key, involved sub of the hash function is a one way hash operation performed in addition to the key XOR and AND already in the random pool.

Generally, the form of the algorithm or techniques of data encryption algorithm method One Time Pad (OTP) are as follows:

a) Open the application program encryption and decryption of data.

b) Enter the password program, then check it in the register. Whether the password is entered or entered in accordance with the password stored in the register.

- If the *passwords* do not match those stored in *registers* or no, the program will provide comments that *the password is* incorrect and automatically program cannot be used until a password is entered in accordance with the in- *registers.*
- If the *password* is entered or entered in accordance with the password that is stored in a register, then will be displayed program or *form* for the encryption and decryption of data.

c) In the Form encryption and decryption of data, Read Data / plaintext (data size, location of the data, the name data)

d) Create Key or key by using random (random noise and the input from the keyboard and mouse)

- Create output *key* (key) in the size of *the input* (data size / *plaintext)*
- Fill each *byte* with a random value (the value of which has been obtained through the hash between *random noise* and the *keyboard and mouse)*
- The key test, good or not
- Compress the key *(key)*, the key here will be compressed, if the key size after compression> = the original data, the key is feasible to be used, otherwise if the key size after being compressed <of the original data, the key is not feasible to be used. As for some of the methods used to compress or calculate *the frequency of* occurrence of a character such method *Huffman, RLE, chi-square* etc.

e) Read per byte of data / plaintext and Key is already in Hash

f) Perform XOR operation on the data / plaintext with the key (key) which has been obtained and in XOR again with the hash key.

g) Finish (data encrypted / ciphertext).

While the algorithm to decrypt the encrypted data / ciphertext it is, basically the same as the encryption process, the general form of the algorithm is:

a) Open application program encryption and decryption of data.

b) Enter the password program, then check it in the register. Whether the password is entered or entered in accordance with the password stored in the register.

- If the *passwords* do not match those stored in *registers* or no, the program will provide comments that *the password is* incorrect and automatically program can not be used until *a password* is entered in accordance with the in- *registers.*
- If the password is entered or entered in accordance with the password that is stored in a *register*, then will be displayed program or *form* for the encryption and decryption of data.

c) In Form encryption and decryption of data, Read or download the encrypted data (ciphertext)

d) Take Key / key (key = key encryption)

e) Read per byte of data between the ciphertext with the key / lock

f) Perform XOR operation between the ciphertext with a hash key (hash value of the password) and XOR again with data key (encryption key).

g) Finish (data decrypted or original data / plaintext)

IV. Result and Discussion

The results of this study after testing the application that implements the one-time pad algorithm, we discussed password making when the application was first used until the encryption process and a decryption of the data and results. For the first time use, it will displayed following message like figure 1.

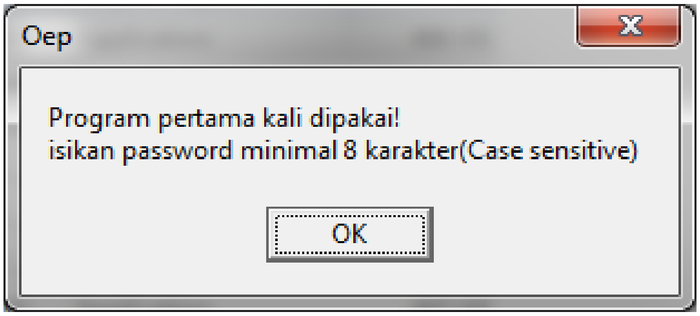


Fig. 1. Messages when the application is first used

To create a password, fill in the spaces at least 8 characters that consist of numbers and letters. Enter the password and then click the button confirm the entered password is stored into the register. If the password entered is correct, then the password is already registered in the register. If the password is wrong, it must be registered on the registration. The first Password is made is the first security level of the application as shown in Figure 2.

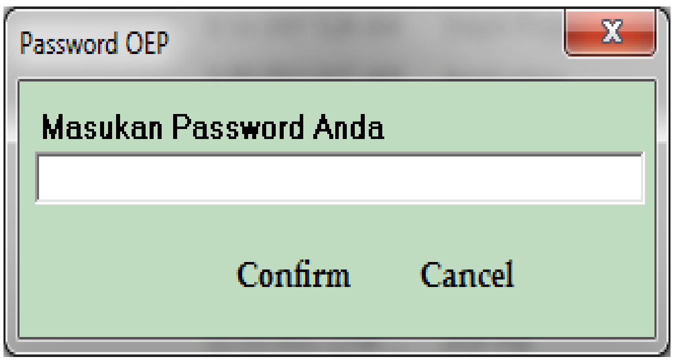


Fig. 2. The form of charging password

Data encryption process is done by taking a file that will then enter the password encryption to secure the data that has been encrypted files. Meanwhile, to make the decryption of the data is done by taking the files that have been encrypted using OTP app, enter the password that was used to encrypt the data, then grab the key that has been made time encryption key using the pick button then described.

A. A Test result on document formats doc

The encryption process is carried out in doc format documents with long file size of 835KB with the encryption process 31 milliseconds and the speed of the process is 27 581 bytes / mDtk as shown in Figure 3.

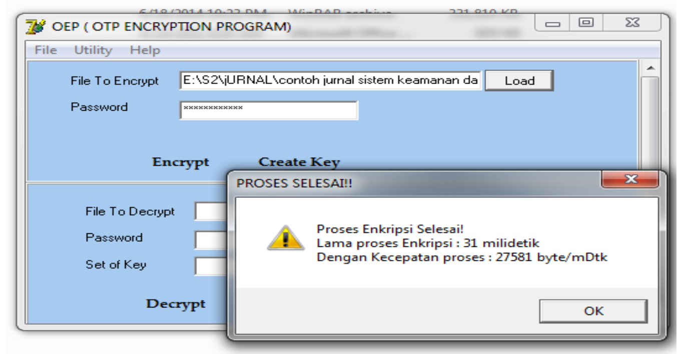


Fig. 3. Encryption processes with the doc format

After performing the encryption process, the application will change the original file of the document. Results encryption of documents with the doc format can be seen in Figure 4.

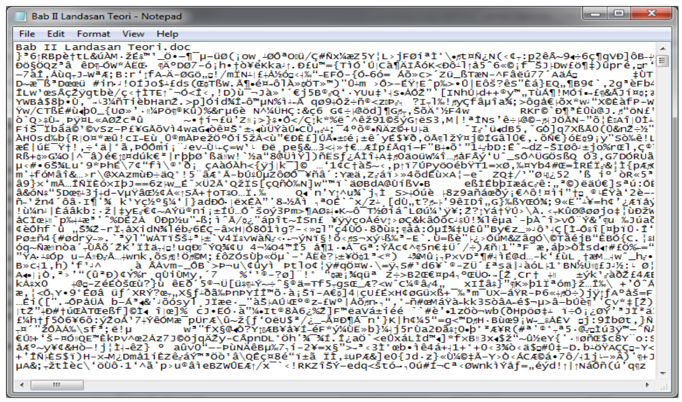


Fig. 4. Encrypted files with .doc format

To open a document that has been encrypted is then encrypted file must first be described in advanced. The process of Decryption file to doc format can be seen in Figure.5. The decryption of the process is done with a long process that is 16 milliseconds to speed the process 53 456 bytes / mDtk with 835KB file size.

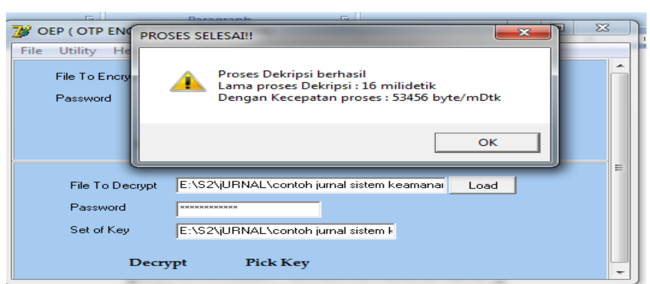


Fig. 5. Process decryption file to doc format

The decryption of the file to doc format can be seen in Figure 6.

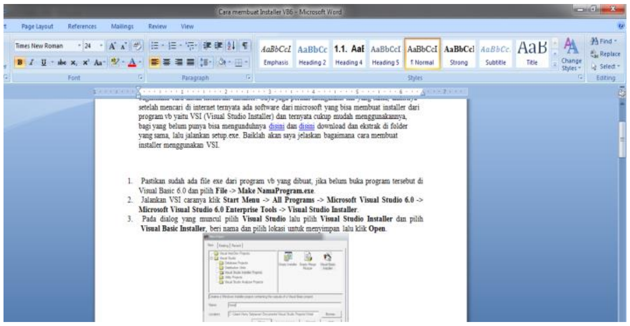


Fig. 6. The decryption of the file format doc

B. Excel file encryption process

The encryption process is carried out in a excel file with a file size of 256 KB to 16 milliseconds longer the encryption process and speed of 16352 bytes / mDtk as terliahat in Figure 7

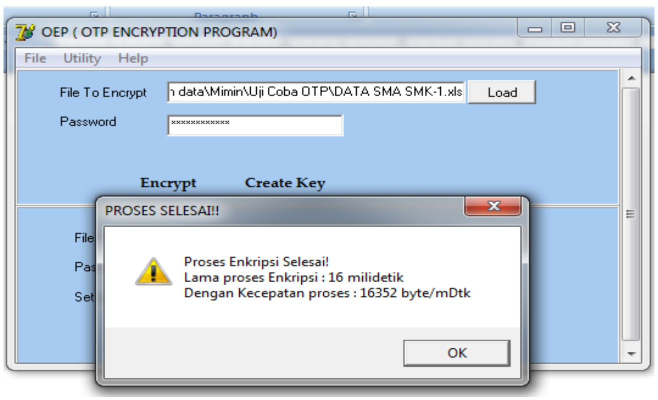


Fig. 7. Excel file encryption process

The Result of excel files stored encryption can be seen in Figure 8

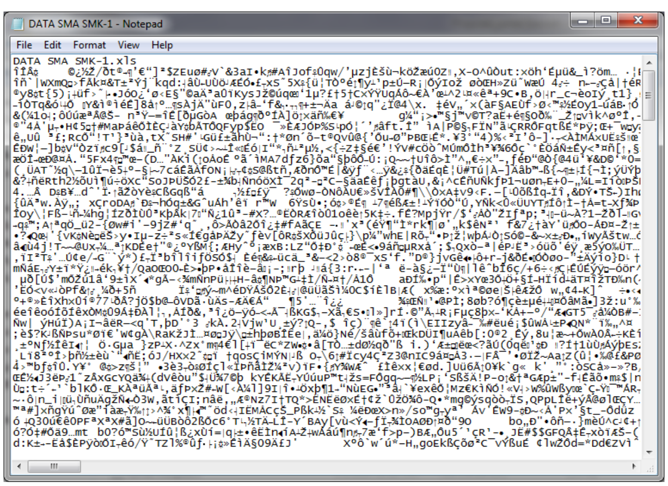


Fig. 8. Results excel file encryption

Process file decryption is conducted by the time the process is 16 milliseconds and the speed of the process is 16 368 bytes / mDtk with a 256 KB big file as shown in Figure 9.

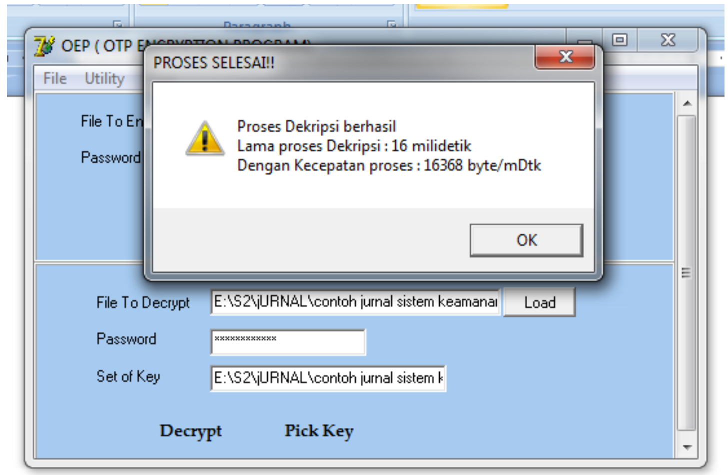


Fig. 9. Process decryptions excel file

The Result of excel file decryption can be seen in Figure 10

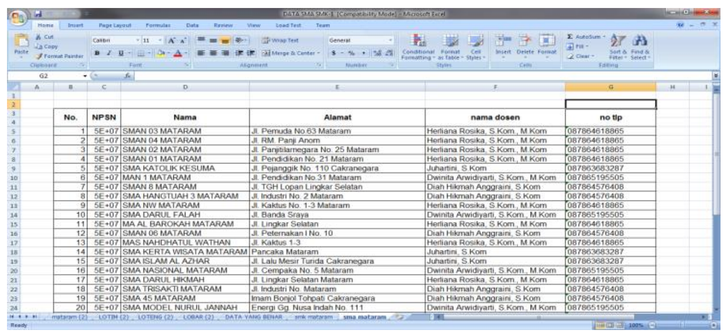


Fig. 10. Results excel file decryption

C. A Test on an image file

Encryption process of image files with file size 6715 KB, 125 milliseconds longer the encryption process with process speed 55 002 bytes / mDtk can be seen in Figure 11.

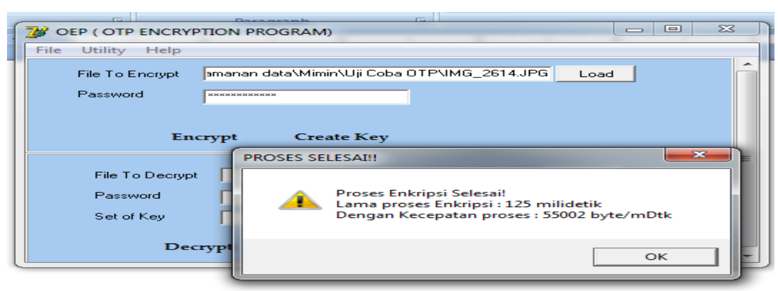


Fig. 11. Image file encryption process

Encryption results of image files can be seen in Figure 12

Fig. 12. Result image file encryption

Decryption process of image files can be seen in Figure 13 with 125 milliseconds long process decryption as well as the speed of 55 004 bytes / mDtk

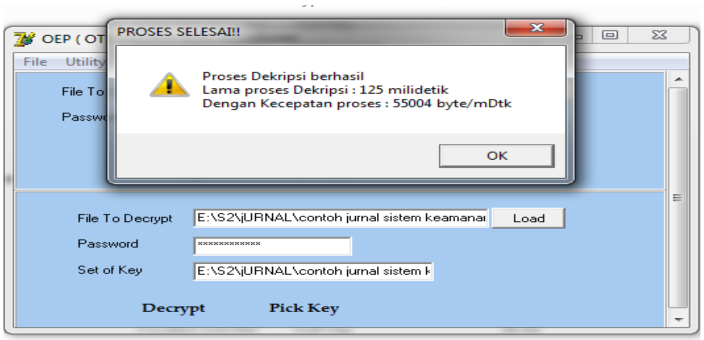


Fig. 13. The process decryption file image

The Results of Decryption on image files can be seen in Figure 14

Fig. 14. The decryption of the image file

D. A Test on a PDF file

The encryption process is performed on a file with a size of 1786 KB with the old encryption process 62 milliseconds to speed the process 29 489 bytes / mDtk as shown in figure 4.14.

Fig. 15. Pdf file encryption process

Encrypted file after the encryption process is shown in Figure 16

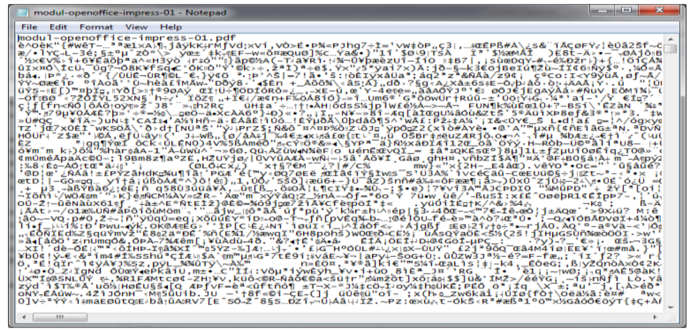


Fig. 16. The results of pdf file encryption

Decryption process lasted 62 milliseconds and with speed process 29 493 bytes / mDtk as shown in figure 17.

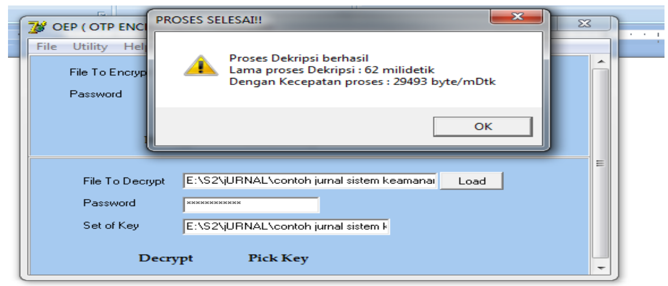


Fig. 17. Process decryption pdf file

The result decryption that is stored can be seen in Figure 18

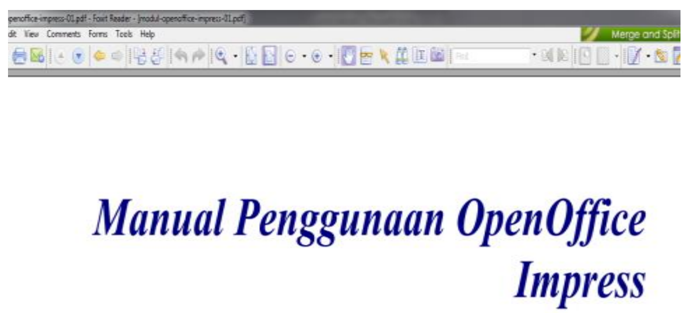


Fig. 18. Results of pdf file decryption

Experiment has been conducted on various types of file formats such as doc, pdf, ppt, and image file formats. Tests were also conducted on various types of file size.

TABLE I. File Size and Time Process

File Size	Time Process
1 KB	16 Milidetik
835 KB	31 Milidetik
1599KB	62 Milidetik
6715 KB	125Milidetik

From Table 1, we can see some test results influence the file size of the processing time required, the time required performing the encryption or decryption process also depends on the speed of the computer used. Meanwhile, to make the process of file encryption and file decryption does not change the size of the file.

From the test results that have been done, it can be seen the advantages of using the application of algorithm on One Time Pad

- It helps the users to store data securely because the password used to encrypt the file must be the same as the password used to decrypt the file so that the right to open the files you have encrypted the only person who has the right to open it.
- Data security when it is encrypted is quite reliable because it uses the algorithm is the result of one-time pad encryption in the fox into cipher text that is very different from the original file.
- By using this application, it can encrypt and describe the various types of file formats such as doc, pdf, ppt and image files.

While the limitations of the application that implements the algorithm one time pad is between the length of a key must be equal to the length of plaintext (original message). This thing can cause the application to run less efficiently because of a long encryption on a long message.

V. Conclusions and Suggestions

From various experiments performed on One time pad algorithm implementation, it can be concluded that this application can protect data properly. Applications that implement the one time pad algorithm can help the users to save data and information from those who do not have the authority. This application can encrypt and decrypt the data in various file formats and file size does not change when performing the encryption process and a decryption of the document.

Developing of this application can increase the security level of the encrypted document and create more interesting design.

References

[1] S. P. Agustanti, "Pengamanan Kunci Enkripsi One-Time Pad (Otp) Menggunakan Enkripsi Rsa", Vol. 7, No. 1, pp. 95-100, 2010.

[2] I. R. Widiasari, "Combining Advanced Encryption Standard (AES) and One Time Pad (OTP) Encryption for Data Security", Vol. 57, No. 20, pp. 1-8, 2012.

[3] M. A. Muda, M, Komarudin and Y. Susanty, "Rancang Bangun Sistem Enkripsi Sebagai Security Komunikasi Handie-Talkie Menggunakan Mikrokontroler Avr Seri", Vol. 1, No. 1, pp. 25-37, 2007.

[4] R. Primartha, "Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)", Vol. 3, No. 2, 2011.

[5] Y. Kurniawan, A. S. Ahmad, M. S. Mardiyanto, I. Supriana dan S. Sutikno, "Analisis Sandi Diferensial terhadap AES, DES dan AE1", Vol. 38 A, No. 1, pp. 73-88. 2006.

[6] E. Sitohang, "Perangkat Aplikasi Keamanan Data Text Menggunakan Electronic Codebook dengan Algoritma DES", Vol. 5, No. 3, 2013.

[7] M. Sholeh dan J. V. Hamokwarong, "Aplikasi Kriptografi dengan Metode Vernam Cipher dan Metode Permutasi Biner", Vol. 7, No. 2, pp. 8-13, 2011.

[8] D. Wirdasari, "Prinsip Kerja Kriptografi Dalam Mengamankan Informasi", Vol. 5, No. 2, 2008.

[9] M. Fairuzabadi, "Implementasi Kriptografi Klasik Menggunakan Borland Delphi", Vol. 4, No. 2, pp. 65-78, 2010.

[10] Inayatullah, "Analisis Penerapan Algoritma MD 5 Untuk Pengamanan Password", Vol. 3, No. 3, 2007.

[11] F. W. Nurwiyati dan I. Yatini B., "Enkripsi Dekripsi Data Menggunakan Metode Stream dan Vigenere Cipher", Vol. 3, No. 23, 2013.

[12] R. Munir, "Algoritma Enkripsi Citra dengan Pseudo One-Time Pad yang Menggunakan Sistem Chaos", 2011.

Competence Making on Computer Engineering Program by Using Analytical Hierarchy Process (AHP)

Ahmad Yani
Academy of Information Management and Computer
AMIKOM Mataram
Mataram, Indonesia

Lalu Darmawan Bakti
Academy of Information Management and Computer
AMIKOM Mataram
Mataram, Indonesia

***Abstract*—This paper shows competence election for the students of the Academy of Information Management and Computer (AIMC) Mataram on computer engineering courses who completed the study in semester 1, 2 and 3 and choose lesson competence. The competence election on computer engineering courses is intended to make students get easier in choosing the appropriate competence and professional expertise of students in an effort to steer students to the ability and the students' academic achievement. It is an uneasy thing for the students. Limited information make the students find it difficult to choose the competence of determining the best based on the academic achievement and interest. To solve the problems, standard decision support system is required to help and provide a solution or an alternative based on the accurate data by using Analytical Hierarchy Process (AHP) that is computerized.**

Keywords—Decision Support System; AHP; Competence; Criteria

I. Introduction

Everyone is often faced with a situation that is very frustrating and confusing, so everyone find it difficult to determine the choice of several options. A problem can be resolved in various ways, solutions or alternatives in problem-solving [8].

Academy of Information Management and Computer students at engineering study program who complete his or her study in semester 1, 2 and 3 choose the competence. It is intended to make students more easily in determining the appropriate competence and professional expertise of students to steer students to the ability and the students' academic achievement. It is uneasy to choose the competence because of the limited information. So, it is hard for them to choose it based on his or her interest.

Competence election is usually determined by three factors. The first is based on the parents. The second is based on the tradition. The third factor is the academic achievement of the students. Competence determination by these three factors will certainly make regret for the students concerned because they do not correspond to their talents, interests, and their profession[4].

To solve the problems, it is needed a standard decision support system that can help and provide a solution or the best alternative to solve problems effectively and efficiently based on factual data. Therefore, this study only focuses on the competence election on system engineering informatics courses using Analytical Hierarchy Process (AHP)[5].

II. Review of Related Literature

A. Decision Support System

Decision support system is an interactive information system that provides information, modeling, and manipulation of data. It was first introduced in the early 1970s by Michael S. Scott Morton with the terms Decision Management System. The concept of decision support is characterized by a computer-based interactive system that helps decision-making, utilize data and models to solve problems that are not structured [5].

B. Hierarchy Analytical Process (AHP)

Hierarchy Analytical Process (AHP) is a functional hierarchy that helps to be better in making the decision on issues that have a lot of objectives. Another goal of the AHP approach is to equip a framework and techniques rank viable alternatives based on decision making [1].

AHP is a decision support models developed by Thomas L. Saaty. It will outline the multi-factor problem or a complex multi-criterion into a hierarchy. According to Saaty, hierarchy is a representative of a complex problem in a multi-level structure and it is the first multi -level goal. It also followed the level of factors, criteria, sub-criteria, and the last of alternatives level. By using the hierarchy, a complex problem can be described in their groups were then organized into a hierarchical form so that the problem would appear more structured and systematic. AHP is often used as a method of solving the problem compared to other methods because of the following reasons[8]:

- The hierarchical structure as a consequence of the criteria chosen to the deepest sub-criteria.
- Taking into account validation until the limit of tolerance inconsistencies various criteria and alternatives are selected by decision makers.
- Taking into account the durability of the sensitivity analysis output decision.

AHP was designed to reflect the way people think. This method enables the quantitative and qualitative aspects of the decision that will be taken into consideration. AHP reduces complex decisions into a series of one -on-one comparison that then gives accurate results. It also uses a scale to weight ratio and scoring criteria alternative that adds to the measurement precision [5].

C. Phase AHP Method

This study was done by using Process Analytical Hierarchy in making the decision. The stages in the method of AHP were as follows [11][9][8]:

1) Define the problem and determine the desired solution. In this phase, the problems that faced is choosing the best competence based on the academic achievement of certain courses, ability test competence, and students' interests to get the right decision.

2) Make a hierarchical structure that begins with the main goal. The main destination is located on the top level, followed by the level of hierarchy and alternative.

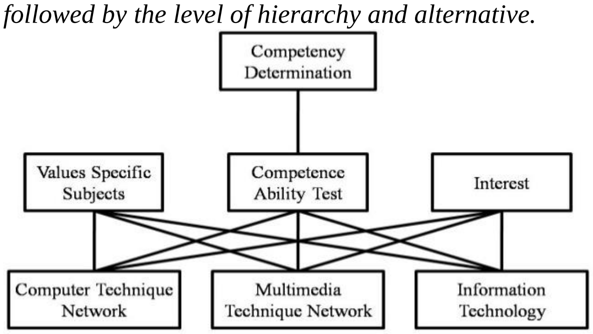


Fig. 1. Structure AHP

3) Make the pairwise comparison matrix that describes the contribution of a relative or influence each element of the destination or the equivalent criteria above. Comparisons are made based on judgment of decision makers to judge the importance of an element. Whereas the importance of the elements of the other elements are as follows:

a) Subjects specific criteria Value 4 times more important than interest, and three times more important than competence Ability Test.

b) Competence Ability Test Criteria 2 times more important than interest.

TABLE I. PAIRWISE COMPARISON

Criteria •	**Values Specific Subjects**	**Competence Ability Test**	**Interest** •
Values Specific Subjects	• 1	• 3	• 4
Competence Ability Test	• 1/3	• 1	• 2
Interest	• ¼	• ½	• 1

4) Performing pairwise comparisons in order to obtain the number of votes as much entirely nx [(n - 1) / 2]. Where n is the number of elements relevant to the comparison. The comparison of each element will be a number from 1 to 9 which shows a comparison of interests of an element.

TABLE II. BASIC SCALE PAIRWISE COMPARISON

Values	**Definition**	**Details**
1	Equally Important	Both elements have the same effect
3	Slightly More mportant	Experience and judgment so favoring one element compared to her partner
5	More Important	One element is preferred and practically very real domination, compared with elements of partner.
7	Very Important	One element proved to be well-liked and very real practical domination, compared with elements of partner.
9	Absolutely More Important	One element of absolute proven preferable to his partner, the highest confidence.
2,4,6,8	Median	Given if there is any doubt in the ratings between the two levels of interest nearby
Reverse	If activity i got a figure compared to activity j , then j has the opposite value compared with i	

5) Calculate the eigen values and test consistency. If not consistent then the decision may be repeated.

6) Repeat steps 3, 4 and 5 for all levels of hierarchy .

7) Calculating the eigenvectors of each pairwise comparison matrix that is the weight of each element for the determination of priority elements at the lowest level of the hierarchy until it reaches the destination.

8) Check the consistency of the hierarchy. As measured in Hierarchy Analytical Process is the ratio of consistency with seeing the consistency index. Consistency is expected that close to perfect in order to produce a valid decision approached. Consistency ratio expected to be less than 10%.

9) Berordo consistency index of the matrix n can be obtained by the following formula:

$$CI = \frac{\varphi\ maksimum - n}{n - 1}$$

The formula in determining the consistency ratio (CR)

$$CR = \frac{CR}{RI}$$

TABLE III. VALUE INDEX RANDOM CONSISTENCY FOR COMPARISON N CATEGORY

N	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.9	1.12	1.24	1,32	1.41	1.45

D. Competence

Competence is the skill or expertise that is owned by someone in the running or doing some field work according to their talents and interests. To achieve a certain competence, one needs to have a number of capabilities. Capability is usually a combination of a personal nature dimensions, skills and knowledge. There are five types of basic characteristics on competence, namely [4]:

- Motif is something which continually thought or wanted by someone who causes the action.
- Nature is a physical characteristics and consistent response to the situation and information.
- The concept of personal (Self Concept), namely behavioral values and personal impressions of a person.
- Knowledge is information regarding a person who has a certain substance field.
- Skill is the ability to perform certain physical and mental tasks.

III. Research Method

A. Types of Research

This study belongs to a qualitative research, because it tests the hypotheses by using statistical techniques. The statistical data obtained from the weighted value of certain subjects obtained by students in semester 1, 2 and 3, tests the ability of competence and interests of students using Hierarchy Process Analytical method and then tested with the Expert Choise 11 software [5].

B. Data Collecting Techniques

Data collecting techniques was conducted by collecting the students' paper score of the and performing weighting on three courses the student competence by giving the value of the sub criteria of competence (Very Good for grades 3-4, Good for the value of 2- Quite to the value of 2.9 and 1-1.9) and the value for each weighting is 1 to Very Good, 2 and 3 for Good Enough.

We gave a test with 10 questions that consisted of three for network computer technique, three for network multimedia technique, and three for Information technology and one for general question.

The data was collected after the students conducted the test. The scores were grouped based on the competence problems that exist with the sub-criteria assessment of the results obtained by the students (Very Good for grades 3-4, Good for the value of 2-2.9 and 1-1.9 Enough to value) and value for each weighting is 1 to Very Good, 2 for Good and 3 for Undecided.

Giving questionnaire based on the students' interest by circling the numbers which indicated on each competency with the provisions of sub-criteria (1 to choice Interests First, 2 For option Interest Second, and Third Interests 3 for selection).

Collecting questionnaires that were filled by the students and categorized it into some category options 1, 2 and 3.

IV. Finding And Discussion

A. Design System

Decision-making system design using Hierarchy Process Analytical method shown in Figure 2

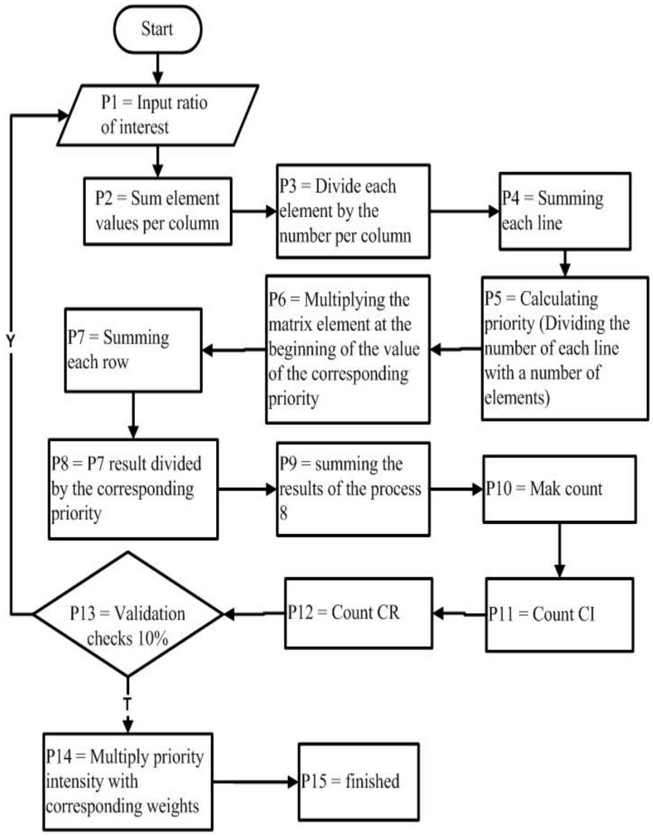


Fig. 2. Flowchart AHP

B. Discussion

1) Changing the comparison matrix in table 1 into decimal and elements scores.

TABLE IV. Comparison Matrix Form Decimal

Criteria	Values Specific Subjects	Competence Ability Test	Interest
Values Specific Subjects	1,000	3,000	4,000
Competence Ability Test	0,333	1,000	2,000
Interest	0,250	0,500	1,000
Sum	1,583	4,500	7,000

2) Dividing each element of the column with the number of the column in question.

TABLE V. DISTRIBUTION OF ELEMENTS EACH COLUMN

Criteria	Values Specific Subjects	Competence Ability Test	Interest
Values Specific Subjects	0.632	0,667	0,571
Competence Ability Test	0,210	0,222	0,286
Interest	0,158	0,111	0,143

TABLE VI. CALCULATION TECHNIQUE DIVISION OF ELEMENTS

= 1,000/1.583 = 0,632	= 3,000/4,500 = 0,667	= 4,000/7000 = 0,571
= 0,333/1.583 = 0,210	= 1,000/4,500 = 0,222	= 2,000/7000 = 0,286
= 0,250/1.583 = 0,158	= 0,500/4,500 = 0,111	= 1,000/7000 = 0,143

3) Calculating Egien Vector normalization by adding each line is then divided by the number of criteria in this case is the number of criteria 3.

TABLE VII. EIGEN VECTOR NORMALIZATION

Criteria	Values Specific Subjects	Competence Ability Test	Interest	Number of Rows	Eigen Vector Normalization
Values Specific Subjects	0.632	0,667	0,571	1,870	0,623
Competence Ability Test	0,210	0,222	0,286	0,718	0,239
Interest	0,158	0,111	0,143	0,412	0,137

4) Calculating the ratio of consistency to determine whether comparative assessment is consistent with the way:

a) Calculating Eigen values Maximum (α mak). αmak = (1,583 x 0,623) + (4,500 x 0,239) + (7,000 x 0,137) = 3,021

b) Calculating Consistency Index (CI) .

CI = (3,021-3)/3-1 = 0,011

c) Calculating Consistency Ratio (CR) .

CR= 0,011/0,58 = 0,019

Because CR < 0.100 means the weighting preferences are inconsistent or invalid.

5) Determine the comparison matrix for sub-criteria; in this case the same value will be used mainly by the matrix comparison criteria.

a) Sub Criteria Values Specific Subjects.

TABLE VIII. COMPARISON MATRIX SUB CRITERIA VALUE SPECIFIC SUBJECTS

Criteria	Very Good	Good	Undecided	Number of Rows	Eigen Vector Normalization
Very Good	0.632	0,667	0,571	1,870	0,623
Good	0,210	0,222	0,286	0,718	0,239
Undecided	0,158	0,111	0,143	0,412	0,137

b) Sub Criteria Competence Ability Test

TABLE IX. COMPARISON OF SUB CRITERIA MATRIX COMPETENCE ABILITY TEST

Criteria	Very Good	Good	Undecided	Number of Rows	Eigen Vector Normalization
Very Good	0.632	0,667	0,571	1,870	0,623
Good	0,210	0,222	0,286	0,718	0,239
Undecided	0,158	0,111	0,143	0,412	0,137

c) Sub Criteria Interests

TABLE X. COMPARISON OF SUB-CRITERIA MATRIX INTEREST

Criteria	Very Good	Good	Undecided	Number of Rows	Eigen Vector Normalization
Very Good	0.632	0,667	0,571	1,870	0,623
Good	0,210	0,222	0,286	0,718	0,239
Undecided	0,158	0,111	0,143	0,412	0,137

6) Determine the ranking of alternatives by calculating eigen vectors for each criteria and sub-criteria.

TABLE XI. DETERMINATION OF ALTERNATIVE RANKING

Criteria	Values Specific Subjects	Competence Ability Test	Interest	Result
Computer Technique Network	2	1	1	0,383
Multimedia Technique Network	3	2	3	0,161
Information Technology	1	2	2	0,478

In this case, the student will be taken one person that will be made sample of the research in computer engineering courses Amikom Mataram on behalf of students Didik Saputra with the students' number: 13.TK.198.

The data obtained from the weighting was as follows:

a) Subjects specific value for Competence Computer Technique Network = 2 (Good), Value Competence Multimedia Technique Network = 1.6 (Undecided) , and Information Technology = 3 (Very Good).

b) Competence Ability Test for competence Computer Technique Network = 1 (Very Good) , Multimedia Technique Network = 2 (Good) and Information Technology = 2 (Good).

c) Interest for competence Computer Technique Network = 1 (Very Good), Multimedia Technique Network = 3 (undecided) and Information Technology = 2 (Good).

To fill in the results in Table 11, multiplication was made between vector invitation criterion vector value sub-criteria, and adding each of the multiplication results.

- Computer Technique Network = (0,623 x 0,239)+(0,239 x 0,623)+(0,137 x 0,623) = 0,149 + 0,149 + 0,085 = 0,383
- Multimedia technique Network = (0,623 x 0,137)+(0,239 x 0,239)+(0,137 x 0,137) = 0,085 + 0,057 + 0,019 = 0,161
- Information Technology = (0,623 x 0,623)+(0,239 x 0,239)+(0,137 x 0,239) = 0,388 + 0,057 + 0,033 = 0,478

C. Results

The result of the study by using Analytical Hierarchy Process (AHP) was implemented into Expert Choice 11 software to determine the level of accuracy in decision making. The results obtained from Expert Choice 11 software as in figure below:

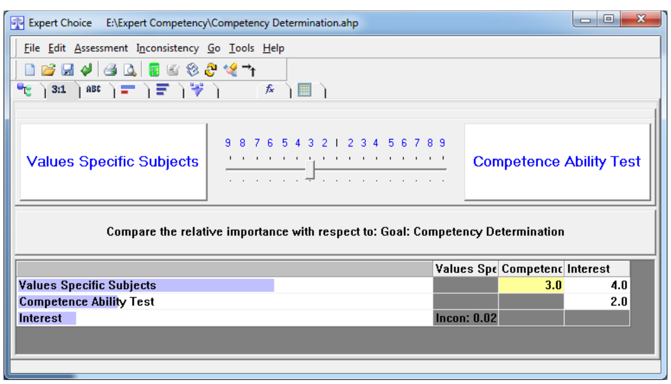


Fig. 3. Pair-wise Comparison

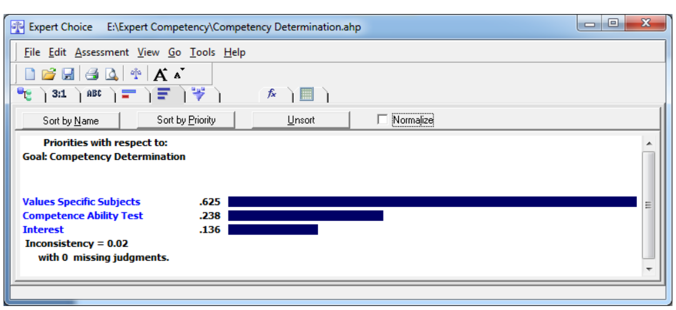


Fig. 4. Comparison Priority Competence

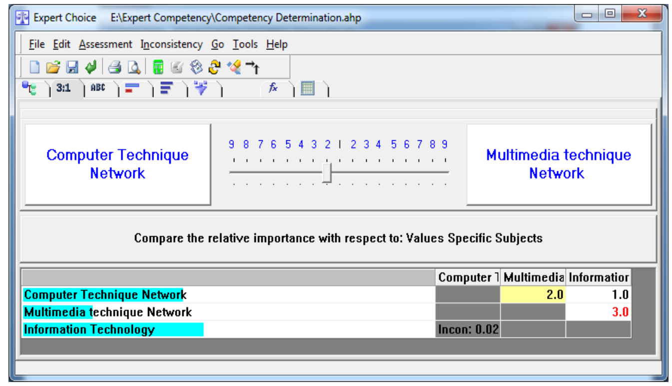


Fig. 5. Based on the Pair-wise Comparison Value Specific Subjects

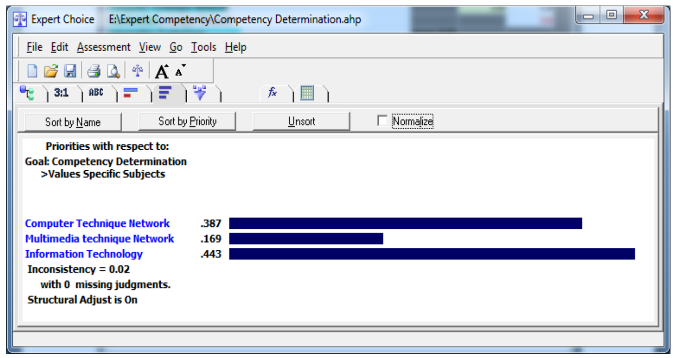


Fig. 6. Priority Pair-wise Comparison Based Value Specific Subjects

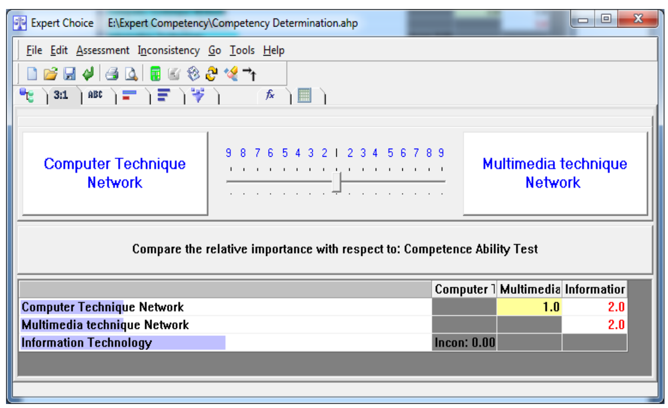


Fig. 7. Based on the Pair-wise Comparison Competence Ability Test

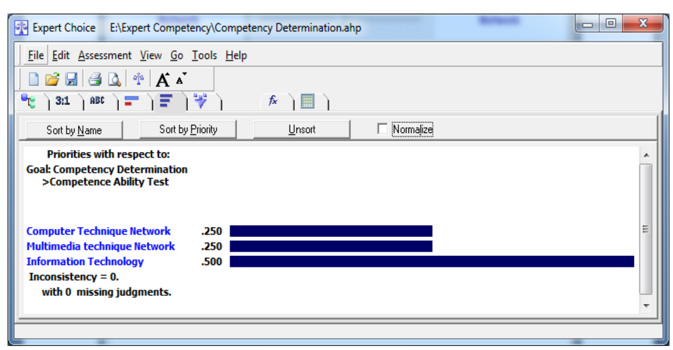


Fig. 8. Priority Pair-wise Comparison Based on Competence Ability Test

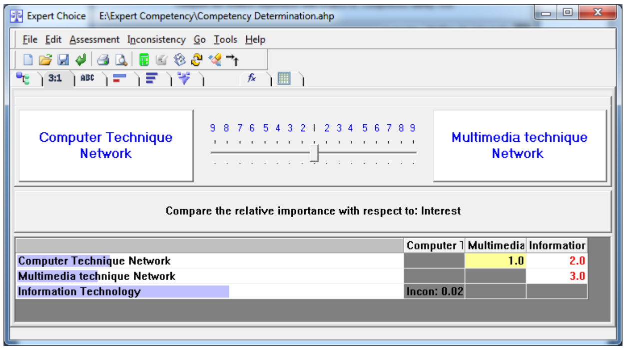


Fig. 9. Pairwise Comparison By Interest

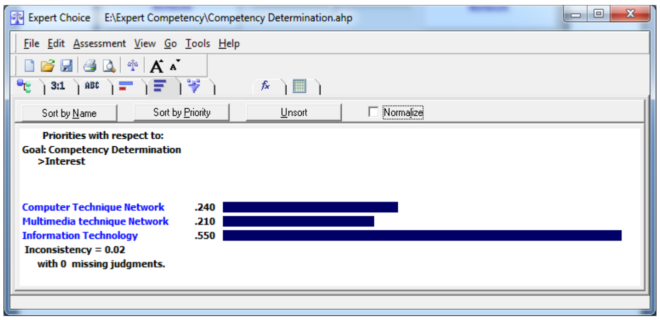


Fig. 10. Based on the Pair-wise Comparison Priority Interest

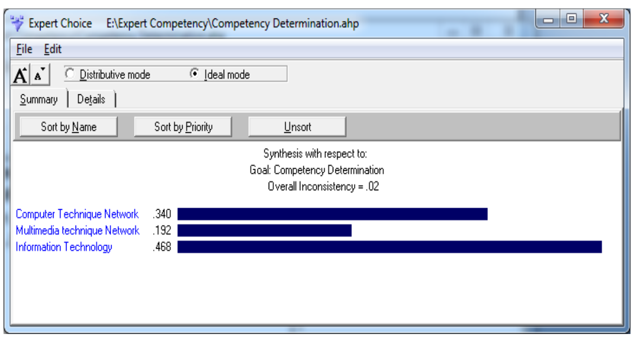


Fig. 11. Comparison of Competence Final Results

V. Conclusion

Based on the competence election on computer engineering, courses at the Academy of Information Management and Computer Mataram used Hierarchy Process Analytical methods, Expert Choice and 11 software with the value of certain courses, competence test ability, and students' interests. It can be concluded that the students do not find it difficult to choose his or her major.

References

[1] Industri, J. T., Teknik, F., & Andalas, U. (2015). ANALISIS PEMILIHAN PEMASOK DENGAN METODE ANALYTICAL HIERARCHY PROCESS, *14*(1), 50–65.

[2] Lemantara, J., Setiawan, N.A. & Aji, M.N., 2013. Rancang Bangun Sistem Pendukung Keputusan Pemilihan Mahasiswa Berprestasi Menggunakan Metode AHP dan Promethee. , 2(4), pp.20–28

[3] Metode, M., & Ahp, F. (2011). Sistem Pendukung Keputusan (Spk) Pemilihan Karyawan Terbaik Menggunakan Metode Fuzzy Ahp (F-Ahp), *2011*(Snati), 17–18.

[4] Nurmianto, E., Siswanto, N., & Sapuwan, S. (2006). PERANCANGAN PENILAIAN KINERJA KARYAWAN DENGAN METODE ANALYTICAL HIERARCHY PROCESS (Studi Kasus di Sub Dinas Pengairan, Dinas Pekerjaan Umum, Kota Probolinggo). *Jurnal Teknik Industri*, *8*(1), 40–53..

[5] Pangkalpinang, L., & Magdalena, H. (2012). Sistem Pendukung Keputusan Untuk Menentukan Mahasiswa Lulusan Terbaik Di Perguruan Tinggi (Studi Kasus Stmik Atma, *2012*(Sentika).

[6] Process, A.H. & Alam, W., 2014. Aplikasi pendukung keputusan dalam penentuan objek wisata alam menggunakan metode ahp berbasis android. , 1(1).

[7] Putra, D.S. et al., Dan Sig Dalam Menentukan Lokasi Pembangunan Cabang (Decision Support System Using Ahp and Gis in Determining the. , pp.1–6.

[8] Saragih, S. H. (2013). PENERAPAN METODE ANALITYCAL HIERARCHY PROCESS (AHP) PADA SISTEM PENDUKUNG KEPUTUSAN PEMILIHAN LAPTOP, 82–88.

[9] Sukoharjo, P. R. (2012). Sistem pendukung keputusan dengan metode, 2(1), 1–15.

[10] Supriyono, Arya Wardhana Wisnu, S. (2007). sistem pemilihan pejabat struktural Dengan Metode AHP. Seminar Nasional III SDM Teknologi Nuklir Yogyakarta, 21-22 November 2007 ISSN 1978-0176, (November), 21–22.

[11] Suryadi, Kadarsyah dan Ramdhani, M. Ali (1998), Sistem Pendukung Keputusan Suatu Wacana Struktural Idealisasi & Implementasi Konsep Pengambil an Keput usan, Remaja Rosdakarya, Bandung.

A Survey on Smart use of BBM and its Influence on Academic Achievement in SMK Health PGRI Denpasar

I Wayan Gede Narayana
STMIK STIKOM Bali
Denpasar, Indonesia

***Abstract*—Black Berry Messenger chat facility is very popular in the process of communicating through text messages, pictures and videos, so that the process of communication in the interaction between users can be carried out actively in virtual world. In this study, it will be examined as to whether the Black Berry Messenger has a significant influence on academic achievement in SMK Health PGRI Denpasar. This study will show the effect of the BBM in the improvement of academic achievement, using quantitative methods by distributing questionnaires from a random sample of the student population of SMK health PGRI Denpasar. The correlation analysis uses the correlation coefficient Kendall's tau which managed to deliver the results that the BBM is very influential with the increase of academic achievement.**

Keywords—Black Berry Messenger; Academic Achievement; Correlation; Simple Random Sampling; Kendall's Tau

I. INTRODUCTION

BBM is a very popular chat facility [7] in the process of communicating through text messages, pictures and videos so that the process of communication in the interaction between users can be carried out actively in virtual world. One technology that is used is the chat facility available on smart phones such as BBM. BBM Chat is utilized very effectively by the students especially for the learning process in the exchange of information both material and knowledge sharing.

In entire, the student's personality [6] can be seen from the way they communicate, as a way to exchange information with other friends. Previously, the information exchange process between students used SMS, which has some limitation in sending picture or video. Now, many students use BBM in the learning process or sharing knowledge. In the study the effect of the BBM on academic achievement, the effect of BBM is examined significantly to know the improvement of academic achievement [9] In the SMK Health PGRI Denpasar. Community students [10] can get more information through BBM .This Research is about the influence of BBM on academic achievement, using quantitative methods by distributing questionnaires from a random sample of the student population SMK health PGRI Denpasar. Quantitative research method can be interpreted as a research method based on positive philosophy, used to examine the population or a particular sample, sampling technique is generally done at random, using a data collection [3] instrument of research, analysis of quantitative data in order to test the hypothesis that is set.

This research studies the effect of BBM with academic achievement, to determine the positive and negative influences of BBM (Blackberry Messenger), and learning to use the BBM and increase academic achievement using BBM.

In order to gain insight into the effect of BBM to increase academic achievement in this paper, the following structure is organized. In the second part some background information about the main concept paper will be provided. A more detailed description of the research method used is presented in section 3. Furthermore, the result of research conducted is presented in Section 4. In section 5 the conclusions are drawn.

II. BACKGROUND

In this section, every concept and its relationship with the problem at hand are explained.

A. Role of Information Technology

The role of information [1] technology becomes a key is capable of an information technology provides an exceptional influence in the field of improvement of students everyday learning course where the relationship between education and technology into an extraordinary relevance in the development of future learning.

B. Black Berry Messenger

BlackBerry Messenger, abbreviated as BBM, is instant messenger application available to BlackBerry device users. This application [7] features the ability to adopt a popular activity among users of mobile devices.

C. Benefit of Learning Media

In a learning process, two very important [12]elements are the method of teaching and teaching media, in which these two aspects are interrelated. Selection of one particular teaching method of teaching will affect the type of media used, although there are other aspects that must be considered in choosing the media, among others, the purpose of teaching, types of tasks and a response is expected to take place controlled by the students after teaching and learning context includes the characteristics students. Nevertheless, it can be said that one of the main functions of teaching media is as a teaching aid that also affect the conditions, and the learning environment organized and created by teachers.

D. Productivity

Productivity is the relationship between [2] the amount of output and input quantity for expected output result, it is essentially a measure of the effectiveness and efficiency of the organization in generating output based on those resources available. Productivity is very important for the long-term and profitability, capable to increase if managed hilistikly and systematicly. Identification and measurement of productivity is estimated in accordance with output and input. In productivity output may be expressed in physical quantities, the output can be expressed in physical units, while the input is an act that consists of resources used to produce output, a very common form of input, for example can, be seen from the workforce.

E. Correlation

Correlation between variables [5]in the mentioned research methodology, is divided into three types, namely the is symmetrical relationship, asymmetrical relationship and reciprocal relationship. Correlation is one of the statistical analysis used to find the relationship between two quantitative variables. Correlation analysis is the study of the discussion about the degree of relationship or the degree of association between two variables, such as variables X and Y.

III. Research Method

The research is conducted at SMK Health PGRI Denpasar for 3 months from March - May 2015.

A. Place dan Time Research

The research is conducted at SMK PGRI Denpasar Health for 3 months from March - May 2015

B. Systematics Research

Stages of systematic research as follows:

1) The first stage is the process of identifying things that become factor in the using system of BBM (BlackBerry Messenger) in the field. This process is carried out by performing understanding in the field, literature studies, and previous research studies. Results of the identification process are the analysis of field conditions regarding the use of BBM (Black Berry Messenger).

2) The next step is the establishment of the conceptual model and research plan. In the second stage where the process is carried out is variable identification, the relations among the constructs, as well as the preparation of the research hypothesis. Results of the second stage are a list and description of the variables as well as research instruments. Research instruments adapted to the description of the variables.

3) The next step is data collection, hypothesis testing, and the interpretation of test results. Results of testing the hypothesis that the hypothesis is accepted or rejected.

4) The last process is making a conclusion.

Systematic research can be show by Figure 1.

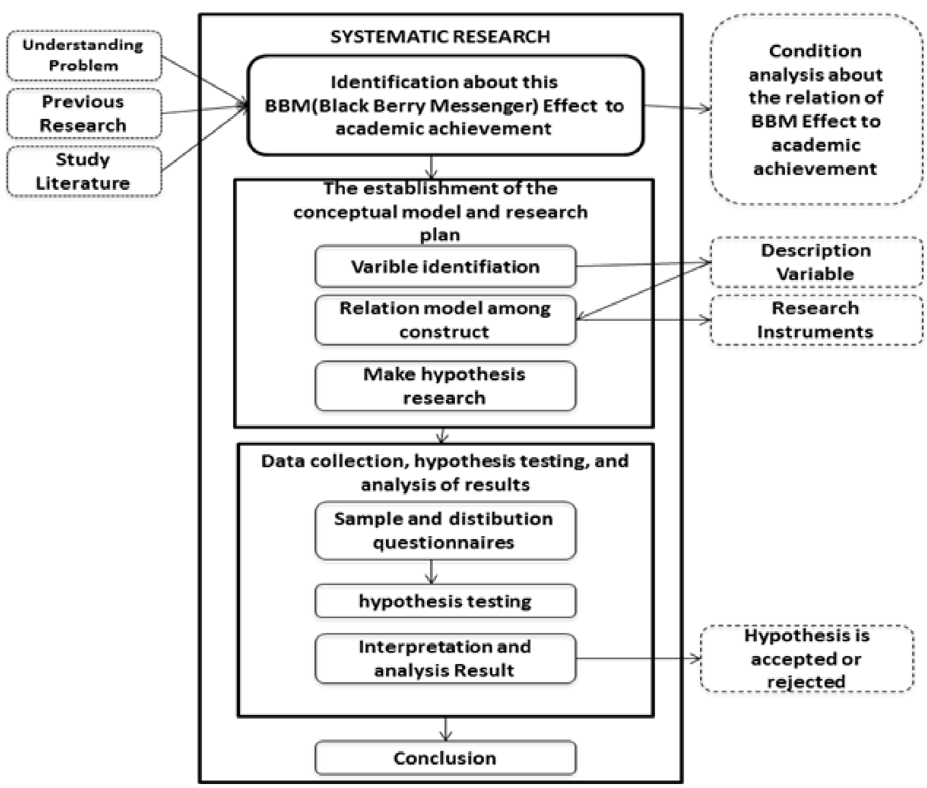


Fig. 1. Systematics Research

C. Data Collection Technique

Data was collected by distributing questionnaires to users of BBM (Black Berry Messenger). Samples taken from the Student of SMK Health PGRI Denpasar sampling technique is simple random sampling. This technique is used [8]when the population has members / elements that are not homogeneous and stratified proportional.

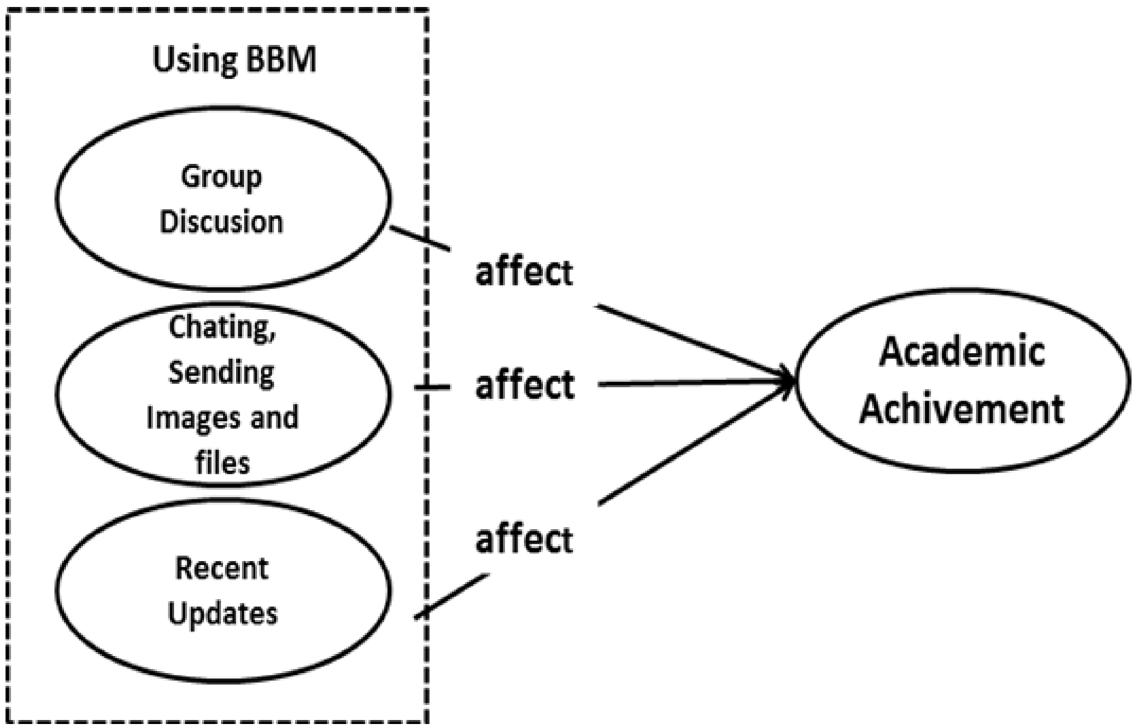


Fig. 2. Relation Model Variable

Definitions of these variables can be explained as follows:

1) Group Discussion

Group discussion is a feature owned by BBM in a group chat where there are some members who have similarity aim to be able to communicate simultaneously to chat, sharing video and image.

2) Chat, Sending Images and files

Chat, sending images and files are features that are used in personal chat, in this case between two or more personals can communicate and chat to discuss the topic.

3) Recent Updates

Recent Updates is facility that is most often used, in which the member who is in a particular BBM will be seen doing activity of making Personal Message Display Picture or change will be seen in the recent updates

4) Academic Achievement

The student academic activity using communication technology is one of the key to improve academic achievement, such as in increasing the learning liveliness value.

D. Variable Research

There are two variables in this study, the use of BlackBerry Messenger and Achievement. The relationship of the four variables is as shown in Figure 2.

E. Hypothesis Research

Based on the hypothesis, the variables will be demonstrated in this study are as follows:

H0:The use of BBM (Black Berry Messenger) and significant positive effect on students Academic Achievement in SMK Health PGRI Denpasar

H1: The use of BBM (Black Berry Messenger) had no effect on students academic achievement in SMK Health PGRI Denpasar

F. Analysis Technic and Hypothesis Test

The analysis technique used is the technique of Kendall's Tau correlation analysis. Kendal Tau correlation is used to locate and test the hypothesis relationship between two or more variables if the data in the form ordinal or ranking. In this study, the data form is in scale used is Likert ordinal measurement. Tools used to calculate the correlation coefficient Kendal Tau is SPSS 20.

Reliability test data used[11] by Cronbach Alpha. Cronbach's alpha was developed by Lee in 1951 to provide a measure of internal consistency test or scale. The value of Cronbach Aplha expresses as a number between 0 and 1.

According to [4] the value of alpha can be interpreted as follows. Table I shows this.

TABLE I. ALPHA VALUES AND INTERNAL CONSISTENCY

Cronbach's alpha	*Internal consistency*
$\alpha \geq 0.9$	*Excellent (High-Stakes testing)*
$0.7 \leq \alpha < 0.9$	*Good (Low-Stakes testing)*
$0.6 \leq \alpha < 0.7$	*Acceptable*
$0.5 \leq \alpha < 0.6$	*Poor*
$\alpha < 0.5$	*Unacceptable*

IV. RESULT

Data collection is done in SMK PGRI Denpasar Health during dated April 5 to 30 2015.From 100 questionnaires were distributed, only 61 questionnaires were returned and all questions were answered. Based on these data 61 then, data analysis can be done as follows:

A. Profil Respondents Research

Discussion identity of respondents is based on by gender and by grade

1) Respondents by gender

Based on the data collected, the number of respondents by gender is shown in Table II below.

TABLE II. RESPONDENT BY GENDER

Respondents by gender	
Men	8 %
Women	92 %

To make it easier to observe the number, then the data is visualized in the form of pie charts, as shown in Figure 2.Based on these data, it is known that the data analyzed in this study largely derived from female respondents. Not yet known about the effect of gender imbalance respondents to the results of the analysis. In the next study to do research on the influence of gender on using BBM.

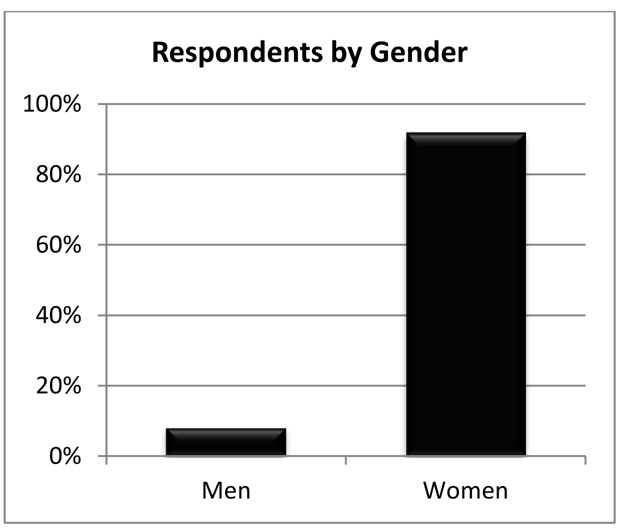


Fig. 3. Visulation Respondens by Gender

2) Respondents by grade

There are 3 grade, but currently only taken two grades of classes XI and XII in SMK Health PGRI Denpasar. Recapitulation of respondents by grade is shown in Table III below.

TABLE III. RESPONDENT BY GRADE

Respondents by grade	
Grade XI	33%
Grade XII	67%

Based on data from Table III, it is known that the majority of respondents were from Grade XII as much as 67% and as much as 33% Grade XI. If the data is visualized in a bar chart, the obtained Figure 4 below.

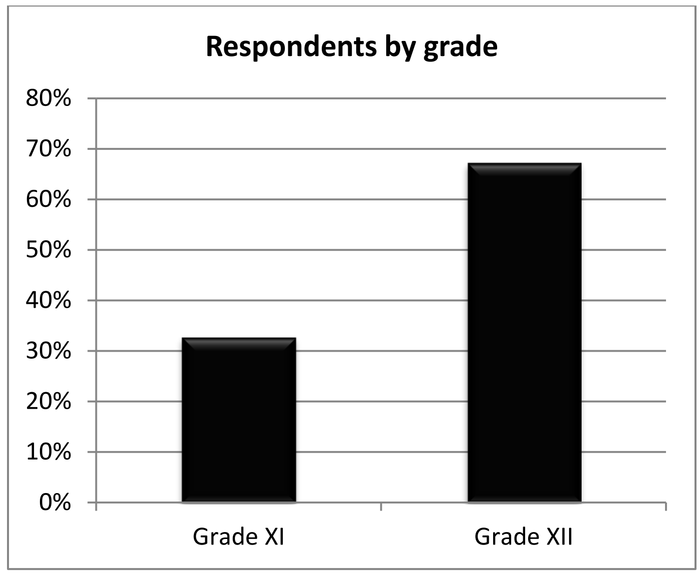


Fig. 4. Visualization Respondents by Grade

B. Result of Realibility test and Validity Data

1) Realibility Statistics

Based on the results of reliability test, the obtained results that the Cronbach's Alpha value of the data is equal 0.838.Number can be interpreted that the data obtained are good and can be used. the obtained Figure 5 below.

Reliability Statistics

Cronbach's Alpha	N of Items
.949	13

Fig. 5. Result of Reliability Test using SPSS 20

The interpretation of the results is referring to the standard interpretation of internal consistency [4].

2) Result Correlations Test

Testing Results correlation using techniques Kendal Tau with SPSS 20, obtained the results as figure 6.

Correlations

			Group_Discusion	Chat_sending_files_and_images	Recent_updates	academic_achievement
Kendall's tau_b	Group_Discusion	Correlation Coefficient	1.000	.302**	.564**	.356**
		Sig. (2-tailed)	.	.008	.000	.001
		N	61	61	61	61
	Chat_sending_files_and_images	Correlation Coefficient	.302**	1.000	.284*	.311**
		Sig. (2-tailed)	.008	.	.015	.003
		N	61	61	61	61
	Recent_updates	Correlation Coefficient	.564**	.284*	1.000	.386**
		Sig. (2-tailed)	.000	.015	.	.000
		N	61	61	61	61
	academic_achievement	Correlation Coefficient	.356**	.311**	.386**	1.000
		Sig. (2-tailed)	.001	.003	.000	.
		N	61	61	61	61

**. Correlation is significant at the 0.01 level (2-tailed).
*. Correlation is significant at the 0.05 level (2-tailed).

Fig. 6. Result of Correlation Test

Based on the above results, it can be interpreteds as table IV:

TABLE IV. RESULT OF CORRELATION TEST

No	Relations Variable	Coefficeint Relation	Conclusion
1	Group_discusion with academic_achievement	0.356	Positive
2	Chat_sending_files_and_images with academic_achievement	0.311	Positive
3	Recent_updates with academic_achievement	0.386	Positive

Based on the above results, it can be interpreted that there is a positive relationship between the variables group_discusion with academic_achievement with large coefficient is equal to 0.356. Chat_sending_files_and_images variables also have a positive relationship with academic_achievement, with a coefficient of 0.311 and a variable Recent_updates with academic_achievement positive relationship with koefisienn relation of 0386. Z value of the third relationship is less than 0.05, suggesting that the relationship between these variables is significant. If the described relationship of these variables on figure 7:

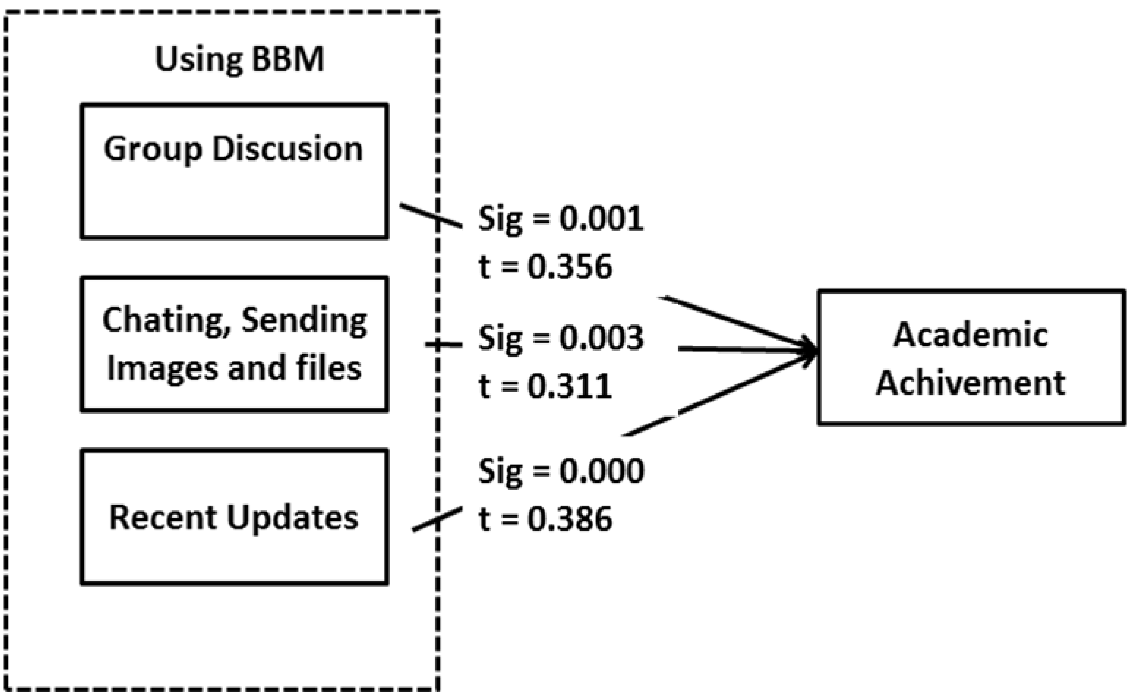


Fig. 7. Relation Result of Effect BBM to Academic Achievement

With the above test results, it can be concluded that the H0 is rejected and H1 accepted, namely the use of BlackBerry Messenger in a positive and significant effect on achievement. This shows that the learning media BBM (Black Berry Messenger) is best used to increase academic achievement.

V. CONCLUSION AND RECOMENDATION

A. Conclusion

Conclusion of the implementation of the study and research "Effect of BBM (Black Berry Messenger for Improving Academic Achievement in Health SMK PGRI Denpasar" as follows:

1) From the observations, it showed that BBM technology when using Group Discussion to increase academic achievement is very influential, result is the error rate of 0.001, below 0.005

2) From the observations, it showed that BBM technology when used in chatting, sending images and files increase the academic achievement of the results,it is very influential and is valued below the error rate is 0.003, below 0.005

3) From the observations, it indicates that the current BBM technologies of recent updates to increase the academic achievement of the results is very influential it is valued below the error rate is 0.000, below 0.005

B. Recommendation

The advice can be given with respect to future research are as follows:

1) On further research would be better if you use more variable as a moderator variable, intervening variable and control variable as a guide as a tool of analysis used together to analyze the data to obtain an appropriate decision.

2) On Further research may also use techniques other than Kendall Tau correlation analysis such as ratio, Spearman Rank, Biseral, Point biserial, Phi and Partial correlation as a guide and measuring devices that can be used to perform the analysis so that the results of such research to be better again.

References

[1] Abreu, F. B. e., "Quantitative Approaches In Object-Oriented Software Engineering" London: Sterling, VA, Kogan Page Science, 2003.

[2] Asio, V. "Research Productivity In Soil Science In The Philippines." Scientometrics 100(1): 261-272, 2014

[3] Bernard, H. R,"Research Methods In Anthropology : Qualitative And Quantitative Approaches", Lanham, Md., AltaMira Press, 2011

[4] Cortina, J.M. ,"What Is Coefficient Alpha? An Examination Of Theory And Applications" Journal of Applied Psychology 78, 98–104,1993

[5] Godinjak, A., et al., "Insulin Resistance And Lipid Accumulation Product In Corelation To Body Mass Index In Women With Polycystic Ovary Syndrome." Med Arch 66(6): 409-411, 2012

[6] Hoyle, R. H, "Handbook Of Personality And Self-Regulation", Chichester, U.K. : Malden, MA, Wiley-Blackwell, 2010

[7] Ifenyi-obi C.C, Olatunji S.O and Enyindah, F.,"Effect Of Blackberry Messenger Usage On The Academic Activities Of Agriculture Students In University Of Portharcourt", USA, PP 07-11, 2014

[8] Onyeka,A.C., Nlebedim, V.U. & Izunobi,C.H., "Estimation Of Population Ratio In Simple Random Sampling Using Variable Transformation", USA, 2013

[9] Orelus, P. W, "Academic Achievers : Whose Definition? : An Ethnographic Study Examining The Literacy (Under) Development Of English Language Learners In The Era Of High-Stakes Tests. Rotterdam": Boston, Sense, 2010

[10] Smith, G. A. And D. Sobel, "Place- And Community-Based Education In Schools" New York, NY, Routledge, 2010

[11] Tavakol, M., Dennick, R. (2011), "Making Sense of Cronbach's alpha", International Journal of Medical Education. Pp. 53-55, 2011

[12] Tohwidi, Afsaneh, "Distance Education Technologies And Media Utiliation In Higher Education", Iran, 2010

The Use of Programming Languages on the Final Project Report by Using Analytical Hierarchy Process (AHP)

(Case Study on the Student of Information Management Amikom Mataram)

Juhartini
Academy Of Information Management and Computer
AMIKOM Mataram
Mataram, Indonesia

Muhammad Suyanto
School Of Information Management and Computer
AMIKOM, STMIK AMIKOM Yogyakarta
Yogyakarta, Indonesia

***Abstract*—The development in information technology provides a lot of convenience for everyone. Academy of Information Management and Computer (AIMC) students of the fourth semester, implementing the Job Training must specify the type of programming that will be used as a Final Project Report. The study assessed five types of programming language by using the approach of Analytical Hierarchy Process (AHP) to obtain information on the programming language that has the quality or better rating than 5 programming languages is based on the parameters. Analytical Hierarchy Process (AHP) is one way in determining or making a decision that are multi-criteria or multi-objective such as choosing the programming language for the Student Information Management at the Academy of Information Management and Computer (AIMC). Programming language based on five criteria consisting of Clarity, Simplicity, and unity; Orthogonality; Fairness for Applications; Supports Abstraction; Environment Program; and Portability Program.**

***Keywords*—programming language; parameters; AHP**

I. Introduction

The developments in information technology provide a lot of convenience for everyone. One type of technological development is an information system that is a means of information spread that highly efficient and easy to use to assist people in an institution [1]

The fourth Semester of Academy of Management Information and Computer Mataram (AIMC) that implemented the Job Training should specify the type of programming that will be used as a Final Project Report. The selected program influence the students' success, especially for students who have limited control of languages program [2]

To help the students in determining the programming language to be used required a lot of technical focus. This study will only focused on five types of programming languages by using Hierarchy Analytical Process (AHP) to obtain the information of programming language that has a quality or better rating than five programming languages based on the parameters. Programming Language concerned with those programs in the preparation of Final Project Report i.e. Programming Delphi, Visual Basic, Java, PHP and C / C ++. [3]

The study is aimed to choose programming Language by using Analytical Hierarchy Process (AHP) to obtain appropriate programming language based on Information Management Program or good rating of specified parameters. It is useful to improve the capabilities in information technology, especially in the use of programming languages that relevant to the program used on Final Project Report. Also an encouragement to further improve the control of the relevant programming language to be used in making the program. [4]

II. Relevant Study

Marsani Asfi and Ratna Purnama Sari conducted a study entitles the Decision Support Systems Achievement Student Selection Method Using AHP (Case Study: CIC STMIK Cirebon). Another study conducted by Dyno Syah Putra and Sulfikar Sallu entitles the Decision Support System Using AHP And Sig In Determining Location New Branch development Enterprises Culinary. Similarly, Adelia conducted a research entitles Decision Support System Teacher Achievement Selection method Using Analytical Hierarchy Process in State Vocational School of Semarang 9.

Those studies above applied AHP approach to determine the decisions to be taken of several alternatives by established criteria. In this study, we will only use Super Decision aids in the process of calculation and decision eigenvector to find a solution to get priorities.

The similarity of the three approaches used in this study is using the same approach to the assessment of the AHP and the resemblance of a language program by students of a reference or review in completing this study. It determined which of the language program will be used when drafting program Final Project Reports.

A. The Type of Hierarchy Analytical Process (AHP)

One of the analysis or synthesis methods used by the decision maker to make decisions is by using AHP; it can give a clear picture to the rational decision maker of the resulting decisions. [5]

As for the types AHP are:

1) Single-criteria

In this type, decision-making is done by involving one / more alternatives with one criterion.

2) Multi-criteria

In this type, decision-making is done by involving one / more alternatives with more than one criterion.

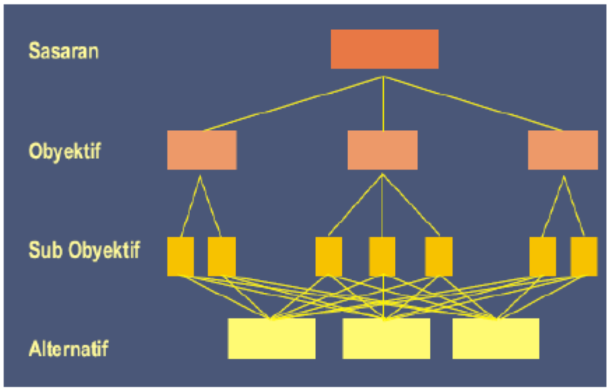


Fig. 1. Structure Chart AHP

The Figure above showed that each element in a level in the AHP will affect the elements at a higher level [6]

In determining priority values often AHP using standard preference table. Table preference these standards have been determined by the researcher's experience AHP that have considerable basis in comparing two or more alternatives on the following forms:

TABLE I. THE TABLE OF PREFERENCES STANDARDS

the level of interest	Definition	explanation
1	The second equally important criteria	The second criterion has the same value
3	criteria which one is more important	slightly more votes in favor of one of the criteria than one partner
5	criteria that one is much more important than others	assessment is very in favor of one of the criteria than one partner
7	one criterion is clearly more important than others	one of the criteria is very influential and dominance seemed very real
9	one absolute criterion much more important than others	evidence that one very important criterion than his partner is very clear
2,4,6,8	the midpoint between two adjacent consideration	This value is given if there is any doubt between the two adjacent assessment
reverse	if the value of x has one value when compared with the above criteria, the criteria y y has a value opposite when compared to criteria x	

B. The basic principles of Analytical Hierarchy Process (AHP)

In the process, AHP is not only used to determine the priority choices with a lot of criteria, but its application has been extended as an alternative model to solve a variety of problems. AHP offers problem-solving decisions involving all sources of complexity.

According to [7] in solving the problems with AHP, we need principles that must be understood such as decomposition, comparative judgment, synthesis of priority, and logical consistency.

1) Decomposition

once the problem is defined, it is necessary to break down the decomposition that whole issue into its elements. If you want to get accurate results, the solution is also made to the elements until no further possible solution, so we get some level of problems faced. There are two types of hierarchy, namely the complete and incomplete. In the complete hierarchy, all elements on a level have all the elements that exist on the next level. Otherwise called incomplete hierarchy

2) Comparative Judgment

This principle means making judgments about the relative interests of the two elements at a certain level in relation to the previous one. This assessment is at the core of AHP, since it will affect the priority elements. The results of this assessment will look better when presented in the form of a matrix called pair wise comparison matrix

3) Synthesis of priority

In each pair wise comparison matrices then the eigencator will be sought to get local priority. Because there is a pair wise comparison matrix at any level, then the global priority to get to do the synthesis between local priorities. The procedure of doing synthesizing is different according to the form of the hierarchy. Ordering the elements according to the interests relative through procedure synthesis of so-called priority setting

4) Logical consistency

Consistency has two meanings, the first is that similar objects can be grouped according to the uniformity and relevance, for example: wine and marbles can be grouped in a set of uniform if the round is the criterion but cannot be grouped if the taste as the criterion, the second is related to the degree of relationship among the objects that are based on certain criteria, for example: if the criteria and honey sweet is rated 5 times sweeter than sugar, and sugar 2 times sweeter than syrup, then it should be a sweet honey rated 10 times sweeter than syrup. If honey is only rated 4 times sweeter than syrup, the valuation was consistent and the process must be repeated if you want to obtain a more precise assessment.

C. Consistency Testing Techniques

In making a decision using AHP approach, Satty defines that a consistency ratio (CR) to provide a consistent matrix tolerance criterion. A matrix is considered consistent if the value of CR <0.1 or inconsistencies that allowed only 10%. To calculate inconsistent limit a matrix, Consistency Ratio can be calculated using the following formula:

$$CR = \frac{CI}{RI} \quad (1)$$

Ratio Index (RI) is a random index that differs according to the size of his order. Saaty determine a matrix **berordo** random index n according to the table below:

N	1	2	3	4	5	6	7	8	9	10
RI	0	0	0,58	0,9	1,12	1,24	1,32	1,41	1.45	1,49

For **berordo** n matrix, then the consistency index is:

$$CI = \frac{\lambda \max - n}{n-1}$$

Where:

CI = consistency index

λmax = the largest of eigen values of matrix berordo n, obtained by summing the product of the number of columns each criterion with the main eigenvector value, according the following equation:

$$\lambda \max = \sum_{i=1}^{n} Ki.Ni$$

Where:

Ki = the sum of all the criteria in the column of the matrix K (matrix results criteria weighting)
Ni = the value eigenvector of the matrix of criteria in line to i.

$$K = \begin{bmatrix} 1.000 & 1.049 & 0.955 & 1.107 & 0.875 \\ 0.953 & 1.000 & 0.911 & 1.055 & 0.834 \\ 1.047 & 1.098 & 1.000 & 1.159 & 0.915 \\ 0.903 & 0.948 & 0.863 & 1.000 & 0.790 \\ 1.143 & 1.199 & 1.411 & 1.266 & 1.000 \end{bmatrix} \qquad N = \begin{bmatrix} 0.1974 \\ 0.1882 \\ 0.2066 \\ 0.1690 \\ 0.2387 \end{bmatrix}$$

Total 5.047 5.294 5.140 5.587 4.414

So that

λ max = (5,047 x 0,1974) + (5,294x0,1882) + (5,140x0,2066) + (5,587 x 0,1690) + (4,414 x 0,2387)
= 5,050

then the value of CI is

$$CI = \frac{5{,}050 - 5}{5 - 1}$$
= 0,0132

If the CI is zero, then the matrix perfect consistency. Because CI is not zero, then it should be counted for consistency ratio (CR), namely:

$$CR = \frac{0{,}0132}{1{,}12}$$
= 0,0118

Because the index is still below the 0.0118 consistency ratio of 0.1, the assessment done is still considered to be consistent.

1) Rationale Decision

According to Simon (1977), a decision support system is a process of selecting action (among the various alternatives) to achieve a goal or several goals. The decision making process is basically a screening of some alternative good decisions agreed that the final decision was an optimal alternative chosen by the particular mechanism.

Methods of decision-making process introduced by Simon, HA (1977) consists of four main phases, namely:

a) Intelligence Phase

Decision-making process begins in this phase where the investigation and identify the scope of the problems were collected in this phase.

b) Design Phase

This stage is the process construction to make estimates is likely to occur from each of the variables and relationships between variables. This stage includes the process to develop and analyze alternative actions that can be performed.

c) Selection Phase

After analyzing alternatives action on this phase, the selection process is done between to run. It includes finding, evaluating and recommending appropriate solutions of the model. Solution of a model is a unity of decision variable values in the selected alternatives.

d) Implementation Phase

At this stage the solution has been agreed upon is started.

2) Basic Decision Making Model

Decision-making in an organization is held or controlled by the employer, because the decision is more to the point the organization. In making a decision grouped into three main components:

a) Objective, an objective that will be achieved

b) Constraints, looking below the limit values of the layer objective

c) Alternatively, the option will be taken from the multi choice.

This method can be applied to the criteria of little or a lot of the criteria of (multi criteria of).

D. Stages of Decision Making

In one organization, a managerial decision-making technique is known as decisions makers, who have a very strong power to accept or reject a proposed solution by the engineering level.

At the engineering level, multi-criteria decision-making process of defining and seek all possible alternatives desired or by ignoring out of the consideration of alternative options as a basis of a multi-criteria analysis methods. [8] At this level are capable of running a multi criteria classification of multi-alternative. The steps in multi criteria decision making are as follows:

1) Determine system evaluation criteria relating to the capabilities of the goal.

2) Establish or create an alternative system for the achievement of the purpose (generating alternatives)

3) Evaluation of alternatives and functions criteria (the value of the function criteria)

4) Run or using normative criteria analysis method

5) The acceptance of a multi alternative that shows the optimal value (preferred), *6) When the relevant decision is not acceptable, then gather new information and return to the next iteration of the multi-criteria optimization of data.*

1) Framework of the Study

The framework of the study is to determine the language program by using AHP method is started from analyzing problems and choosing the topic, and then defining the criteria of alternative language program support using AHP to produce a language program that can be used as a guide on writing the Report Task. [9]

The following diagram illustrated the framework of this study.

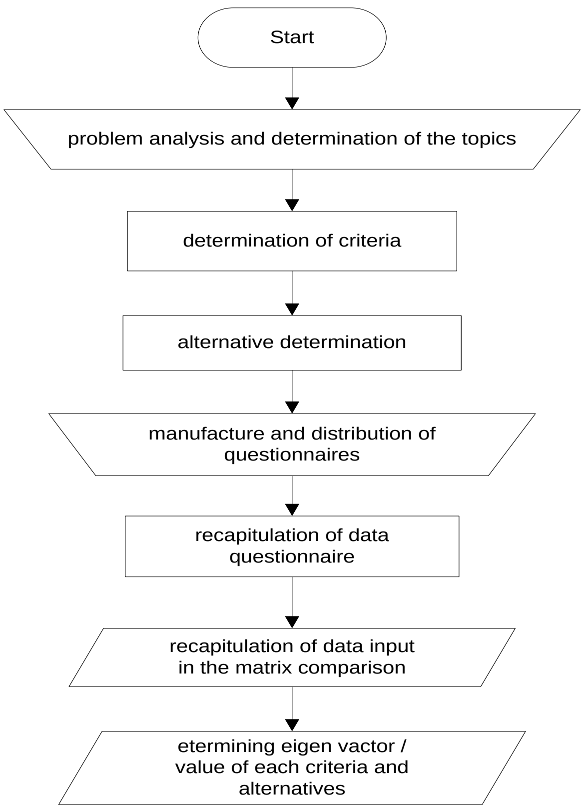


Fig. 2. Flowchart Framework

From the diagram above, it can be explained that when choosing a language program in the preparation of Final Report of work by using AHP, it is began with analyzing the problems and choosing the topic, and then determining the criteria of which will be used as a reference in assessing an alternate assessment that is determined. After determining the criteria of and alternatives, then design the questionnaire and then distributed to the respondents. Questionnaires were distributed to respondents subsequently recapitulated then fed into the matrix comparisons / pair. The next step is to determine the eigen vector / eigen value of each of the criteria of and alternatives that have been determined and the last is the determination of priorities and criteria of each alternative. It means that the criteria of which is the most important of the criteria and which alternative is better or has best quality of some of the alternatives that have been determined.

III. Needs Analysis and Process Analysis

A. Needs Analysis

1) Determination of AHP

Analytical method Hierarchy Process (AHP) is one way in determining or making a decision that are multi-criteria or multi-objective such as determining the programming language for the Student of Information Management of the Academy of Information Management and Computer (AIMC). [10]

The determination of the assessment or evaluation of programming languages based on criteria or parameters. These criteria are as follows:

a) Clarity, simplicity, and unity

Programming language should be able to help programmers to create a design program long before programmers coding. Ease, simplicity, and unity is a combination that helps programmers develops algorithms so that the resulting algorithm has a low complexity.

b) Orthogonality

Orthogonality is an attribute that can be combined with a variety of programming language features so that each combination has a meaning and can be used. For example, a programming language supports an expression that can produce a value, and the programming language also supports the statement that evaluates the condition of an expression to get the value of true or false. Two features of the programming language, the expressions and statements conditions, are orthogonal if any expression can be used and evaluated in the condition statement. When programming language features are orthogonal, then the programming language that will be easily understood and easy to learn and program will be written because there are few exceptions and a case that should be remembered.

c) Reasonableness to Application

Programming languages require proper syntax and matching that used in the program structure to reflect the logical structure that underlies an algorithm. Programming language must have a data structure, operations, control structures, and natural syntax appropriate / suitable to suss out a problem. A programming language designed specifically for particular needs, for example Prologue is used for the purposes of deduction or C ++ object-oriented programming.

d) Supports Abstraction

Abstraction is a substantial thing for the programmer to make a solution of the problems faced. Then these abstractions can be easily implemented using existing features in a programming language.

e) Programming Environment

The programming language has a good environment and a complete programming will make it easier for programmers to implement abstraction that was drawn up. Programming environment here can mean the editor used, good Documentation of programming languages, debugging facilities, a good user interface, or other tools that can be used *f) Portability Program*

One of the important criteria for a programming project is the ease of ready-made programs to be transferred from the computer used to create and develop to another computer that will use it. It will facilitate the work of programmers.

2) Determination of AHP Alternatives

Alternative selection is based on observation and experience of researchers who often see and ask the students and lecturers of the programming language commonly used in the preparation of the Final Project Report [11] .The process of comparison to some alternative programming language by using AHP, namely:

a) Programming languages Borland Delphi

b) Visual Basic Programming Language

c) Java Programming Language

d) PHP Programming Language

e) Programming languages C / C ++

B. Analysis Process

1) Architectural Model AHP

Decisions or priority setting that is both complex (multi-criteria or multi-objective) can be done by using AHP. In AHP, criteria and alternatives are two very important components; it is known that the AHP is used to determine the priority of multiple criteria / alternatives by analyzing paired comparisons (pair wise comparison) of each criterion / alternatives. [12]

2) Questionnaire Model

The making of questionnaire model, it is based on the needs to be processed using AHP, the processing results of the questionnaire will be performed using software Super Decision.

The form of a questionnaire which is designed in this study is as follows:

Name : ....
Completion date : ....
Signature : ....
Instructions on filling : ....

Give the cross mark (X) on the selected value, where:

Value 4 = very important / very good

Value 3 = critical value / good

Value 2 = fairly important / fairly good

Value 1 = less important / less good

Value 0 = not important / not good

Examples:

In assessing a programming language, how important the following criteria!

TABLE II. EXAMPLES CHARGING QUESTIONNAIRE

Criteria	**Value / Score**				
	4	*3*	*2*	*1*	*0*
Clarity, Simplicity dan unity	X				
Orthogonality		X			
Reasonableness to Application		X			
Supports Abstraction		X			
Programming Environment			X		
Portability Program			X		

TABLE III. ALTERNATIVE QUESTIONNAIRE BASED ON THE LEVEL OF CLARITY, SIMPLICITY, AND UNITY

Criteria	**Value / Score**				
	4	*3*	*2*	*1*	*0*
Borlan Delphi		X			
Visual Basic		X			
Java				X	
PHP	X				
C/C++			X		

3) Respondents

This research was conducted at the Academy of Information Management Computer (AMIKOM). The respondents are the fourth semester of the Student of Information Management. Random technique was used in choosing the participant with the following formula:

Slovin formula $n = \frac{N}{N.d^2 + 1}$ ----------------------- (1)

Where:
n = sample size
N = population size
d = error estimation

The numbers of participants are 102 people, if the number of participants was 102 people, with an error level / error is estimated at 10%, then the total number of respondents is (102) / (102. (10% ^ 2) +1) = 50

IV. SYSTEM DESIGN

A. Data Recapitulation Techniques

Before making decision by using AHP, at first the data was recapitulated from the questionnaire that was distributed to the respondents. Summary data of the questionnaire in this study consisted of data recapitulation questionnaire: [13]

1) Criteria

Data on each of these criteria can be gained by taking every value which is filled and / or provided by the respondent on each of criteria to form a recapitulation as follows:

TABLE IV. RECAPITULATION DATA QUESTIONNAIRE

No	Respondents	Criteria				
		Criterion 1	*Criterion 2*	*Criterion 3*	… …	*Criterion n*
1	Respondent 1	X1.1	X1.2	X1.3	…	X1.n
2	Respondent 2	X2.1	X2.2	X2.3	…	X2.n
3	Respondent 3	X3.1	X3.2	X3.3	…	X3.n
…	……..	……..	……..	……..	…	……..
n	Respondent n	Xn.1	Xn.2	Xn.3	…	Xn.n
Average		$Y1=\frac{\Sigma Xn.1}{n}$	$Y2=\frac{\Sigma Xn.2}{n}$	$Y3=\frac{\Sigma Xn.3}{n}$	… ….	$Yn=\frac{\Sigma Xn.n}{n}$

2) Elements Matrix Pair

After the recapitulation of the questionnaire data according to the table above, then insert each element into a matrix of pair wise form the average value of each of the criteria of the concept based on AHP with matrix form pairs as follows:

TABLE V. AHP PAIR WISE MATRIX

Criteria	Criteria				
	Criterion 1	*Criterion 2*	*Criterion 3*	……	*Criterion n*
Criterion 1	Y1/Y1	Y1/Y2	Y1/Y3	……	Y1/Yn
Criterion 2	Y2/Y1	Y2/Y2	Y2/Y3	……	Y2/Yn
……..	……..	……..	……..	……	……..
Criterion n	Yn/Y1	Yn/Y2	Yn/Y3	……	Yn/Yn

3) Consistency Testing Techniques

To obtain a good decision or solution, it takes consistency in charging or weighting criteria. In making a decision using AHP approach, Satty defines a consistency ratio (CR) to provide a consistent matrix tolerance criterion.

A matrix is considered consistent if the value of CR <0.1 or inconsistencies that allowed only 10%.

To calculate the value of the consistency of each matrix pairs have been described in previous chapters (can be seen in chapter II).

B. Summary of Data

1) Summary of questionnaire data criteria

Based on the questionnaire that was distributed to the respondents obtained the following data:

TABLE VI. RECAPITULATION QUESTIONNAIRE RESULTS CRITERIA

No	Criteria	Average
1	Clarity, Simplicity and unity	**3.52**
2	Orthogonality	**2.80**
3	Reasonableness to Application	**3.22**
4	Supports Abstraction	**2.20**
5	Programming Environment	**3.04**
6	Portability Program	**2.36**

Recapitulation alternative questionnaire data based on the level of clarity, simplicity and unity, orthogonality, Fairness for Applications, Supports Abstraction, and Portability Programming Environment Program Based on the questionnaire that was distributed to the respondents obtained the following data:

TABLE VII. SUMMARY DATA OF ALTERNATIVES BASED ON THE LEVEL OF CLARITY, SIMPLICITY AND UNITY, ORTHOGONALITY, FAIRNESS FOR APPLICATIONS, SUPPORTS ABSTRACTION, AND PORTABILITY PROGRAMMING ENVIRONMENT PROGRAM

No	Alternative	Criteria					
		Clarity, Simplicity and unity	*Orthogonality*	*Fairness for Applications*	*Supports Abstraction*	*Programming Environment*	*Portability Program*
1	Borland Delphi	**3.08**	**3.12**	**2.88**	**3.02**	**3.36**	**3.18**
2	PHP	**3.38**	**3.32**	**3.60**	**3.50**	**3.66**	**3.34**
3	Java	**2.18**	**1.78**	**1.58**	**2.60**	**2.68**	**2.86**
4	Visual Basic	**2.66**	**2.04**	**1.64**	**2.80**	**3.16**	**2.98**
5	C/C++	**1.80**	**2.24**	**1.86**	**1.78**	**2.92**	**2.70**

C. Pair wise Comparison Matrix

After getting the data from the recapitulation of the questionnaire, then enter the value of each criterion and an alternative to the matrix of pair wise comparisons using Super Decisions software.

1) Matrix of pair wise comparisons for all the criteria of from the recapitulation of the questionnaire data collected from respondents, the data obtained as in table 4.3. The data is then inserted into the matrix of pair wise using software Super Decisions as follows:

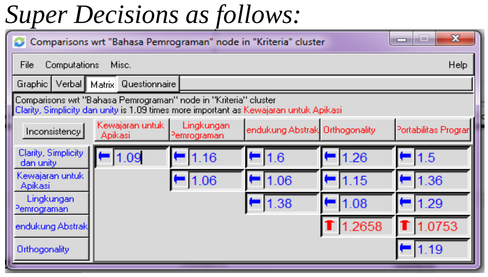


Fig. 3. Pair wise comparison matrix for the criteria

2) Matrix pair wise comparisons for all the alternatives based on the criteria of Clarity, Simplicity and unity

From the recapitulation of the questionnaire data collected from respondents, the data obtained as in table 4.4. The data is then inserted into the matrix of pair wise using software Super Decisions as follows:

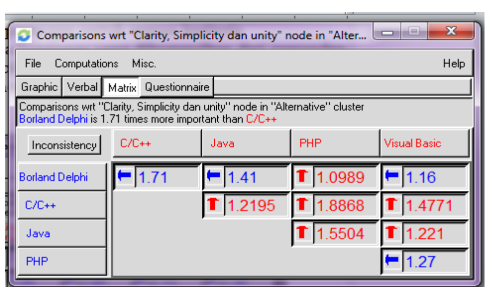


Fig. 4. Matrix of pair wise comparisons of alternatives to the criteria Clarity, Simplicity and unity

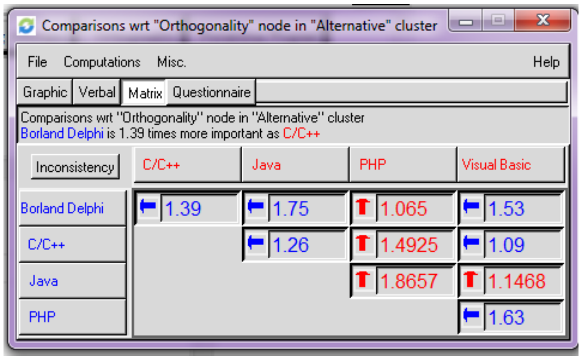


Fig. 5. Matrix of pair wise comparisons of alternatives to the criteria Orthogonality

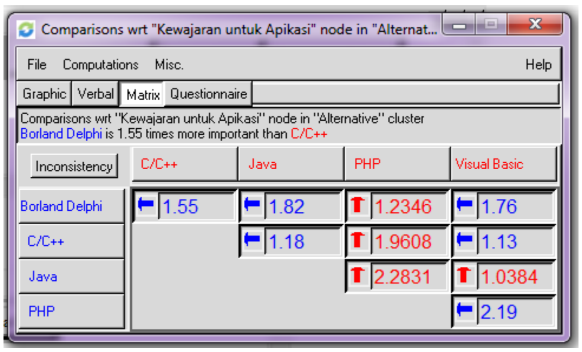


Fig. 6. Matrix of pair wise comparisons of alternatives to the criteria Fairness For Applications

D. Consistency Value

Measurement error rate in determining the numbers pair wise comparisons of each criterion and each alternative based on a criterion can be done by looking at the value of consistency. If the value of consistency is equal to zero, it is considered perfect (no error in charging or weighting matrix), but if the consistency is greater than 0.1 it is considered inconsistent. Measurement error tolerance value against the value of consistency is 10%. So, if the value is smaller than 0.1 then it is considered to be consistent. From the processing of data obtained through the questionnaire is entered into the matrix of pair wise using Super Decisions software to determine the programming language to some alternatives based on several criteria described above, the value of inconsistencies (Table VIII) as follows: [14]

E. The Results of Synthesis Super matrix with Super decision

After processing by using software Super Decisions concerning the determination of the language program synthesis of the results obtained as follows:

1) Synthesis results Criteria

Of the five criteria were used as the standard programming language assessment couple of (alternative) namely; Clarity, Simplicity and unity, Orthogonality, Fairness for Applications, Supports Abstract, Environmental Programs and Portability Program priorities solution obtained by eigen values / eigen vector of each of the following criteria: [15]

TABLE VIII. THE SYNTHESIS OF CRITERIA

No	Criteria	*Eigen Value/Eigen Vector*
1	Clarity, Simplicity and unity	0.20600
2	Orthogonality	0.17900
3	Reasonableness to Application	0.17700
4	Supports Abstraction	0.13600
5	Programming Environment	0.16400
6	Portability Program	0.13800

2) Alternative syntheses results

Based on 5 criteria to assess six reference sources (website) learning programming synthesizing the results obtained in order to determine priorities website (alternatives) based on the following criteria:

TABLE IX. PRIORITY / RANKING OF PROGRAMMING LANGUAGES BASED ON ALL CRITERIA

Programming Language	*Eigen Value / Eigenvector*					
	Clarity Simplicity and unity	*Orthogonality*	*Reasonableness to Application*	*Supports Abstraction*	*Programming Environment*	*Portability Program*
Borland Delphi	0.234981	0.249371	0.249775	0.220091	0.216743	0.211150
C/C++	0.127097	0.178789	0.160366	0.129103	0.188088	0.178807
Java	0.166667	0.142370	0.136552	0.189907	0.172839	0.189275
PHP	0.258271	0.266088	0.311358	0.256302	0.217387	0.222598
Visual Basic	0.202984	0.163382	0.141949	0.204598	0.204942	0.198170

From table IX data was obtained from the results of the determination of the overall synthesis programming language using AHP with the following priority

TABLE X. PRIORITY PROGRAMMING LANGUAGE BASED ON THE RESULTS OF THE SYNTHESIS

No	Information	Normal value	percentage
1.	Borland Delphi	0.231447	23 %
2.	C/C++	0.161794	16 %
3.	Java	0.164665	16 %
4.	PHP	0.256628	26 %
5.	Visual Basic	0.185466	19 %

These results were obtained after performing data processing using software Super Decision with the following results:

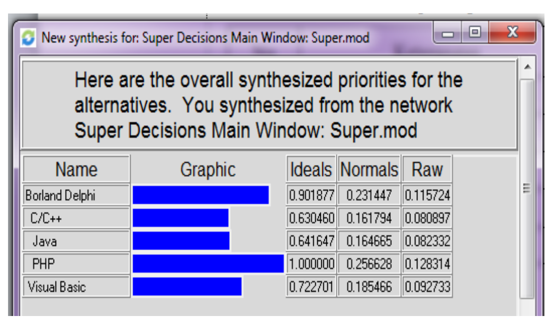


Fig. 7. Synthesis results Super matrix with Super Decision

V. Conclusion and Suggestions

A. Conclusion

The conclusions of the study,

1) Programming Language based on five criteria that are Clarity, Simplicity and unity; Orthogonality; Fairness for Applications; Supports Abstraction; Environment program; and Portability Program resulting percentage Borland Delphi is 23%, C / C ++ 16%, Java is 16%, PHP is 26% and Visual Basic is 19%.

2) Questionnaire to obtain the above results, 50 questionnaires from the total students of Information Management in the sixth Semester is 102 people with a level of error / error is estimated at 10%.

B. Suggestions

In this study, there are many shortcomings. Therefore the suggestions are:

1) To obtain more accurate results, it is advisable to use a rating scale questionnaire better and distributing questionnaires to the respondents were properly addressed.

2) Choosing programming languages using AHP method can be prepared or implemented into an application program such as online applications.

References

[1] Uhtadan, M. et al., 2008. Application Development To Repair Image Digital Film Radiography. , Pp.25-26.

[2] Rahmana, A., 2009. Role of Information Technology in Improving.

[3] Seminar 2009 (SNATI), pp.B11-B15. Available at:

[4] Son, D.S. et al., and Sig In Determining the Location of Development Branch (Decision Support System Using AHP and Gis in Determining the., pp.1-6.

[5] Process, A.H. & Nature, W., 2014. The decision support applications in the determination of the natural attractions using AHP based on Android. , 1 (1).

[6] Lemantara, Julianto, Noor Akhmad Setiawan, and Marcus Nurtiantara Aji. 2013. "Design of Decision Support System Outstanding Student Selection Method Using AHP and Promethee." 2 (4): 20-28.

[7] Respati, Good (2006), Decision Support System with Expert Choice.

[8] Diktat unpublished. Yogyakarta: Gadjah Mada University.

[9] Saaty, Thomas L. (1990), Decision Making For Leaders: The Analytical Hierarcy For Decision Process in a Complex World. Pittsburgh: Univesity of Pittsburgh

[10] Armadyah Amborowati, Housing Selection Decision Support System by using Expert Choice AHP method.

[11] Setiawan N. (2007), sample size determination using the formula Slovin and tables krejcie- morgan: Assessing Concepts And Applications.

[12] Sinaga J. (2009), Application of Analytical Hierarchy Process (AHP) in the selection of Company's state-owned enterprises (SOEs) as a university student workplaces North Sumatra (USU).

[13] Turban, Efraim; Aronson, Jay; Liang Peng Ting (2005), Decision Support Systems and Intellegent Systems. New Jersey : Pearson Education, Inc

[14] Utari L. (2011), Implementation of Analytic Hierarchy Process (AHP) For Budget Plan In AMIK Bogor.

[15] Wahyuddin (2010), Determination Networking Promotional Media New Student Using Analytical Hierarchy Process.

[16] Yohana, et al. Applications SPK Tender Winners Contractor Selection With AHP method

[17] Zain, Ruri Hartika, S Kom, and M Kom. 2012. "Design and Implementation RC4 Cryptography Method On the File Document Type Language Programming Using Visual Basic 6. 0. "12 (1): 71-81.