An Algorithm based on Convolutional Neural Networks to Manage Online Exams via Learning Management System Without using a Webcam

Lassaad K. SMIRANI[1]
Umm al-Qura University, Deanship of e-Learning and Distance Education KSA
InnoV'COM Lab, University of Carthage, Tunisia

Jihane A. BOULAHIA[2]
Umm al-Qura Univesity, College of Computer and Information Systems KSA
InnoV'COM Lab, University of Carthage, Tunisia

***Abstract*—Cheating attempts in educational assessments have long been observed. Because students today are characterized by their great digital intelligence, this negative conduct has intensified throughout the emergency remote teaching time. First, this article discusses the most innovative methods for combating cheating throughout the online evaluation procedure. Then, for this aim, a Convolutional Neural Networks for Cheating Detection System (CNNCDS) is presented.. The proposed solution has the advantage of not requiring the use of a camera, it recognizes and identifies IP addresses, records and analyzes exam sessions, and prevents internet browsing during exams. The K-Nearest Neighbor (K-NN) has been adopted as a classifier while the Principal Component Analysis (PCA) was used for exploratory data analysis and for making predictive models. The CNNCDS was learned, tested, and validated by using data extracted from a face-to-face exam session. its main output is a binary students' classification in real-time (normal or abnormal). The CNNCDS surpasses the fundamental classifiers Multi-class Logistic Regression (MLR), Support Vector Machine (SVM), Random Forest (RF), and Gaussian Naive Bayes (GNB) in terms of mean accuracy (98.5%). Furthermore, it accurately detected screen pictures in an acceptable processing time, with a sensitivity average of 99.8 percent and a precision average of 1.8 percent. This strategy has been shown to be successful in minimizing cheating in several colleges. This solution is useful for higher education institutions that operate entirely online and do not require the use of a webcam.**

Keywords*—Artificial intelligence; convolutional neural network; learning assessment; online cheating; online examination; higher education; emergency remote teaching

I. Introduction

Evaluation is the most important stage of the teaching process [1][2][3][4]. Indeed, assessment is at the heart of the learning service, providing faculty members with important information about what students understand, allowing them to plan and manage lessons and providing relevant feedback [5]. The evaluation stage allows students to become aware of their learning methods and use this knowledge to improve and develop their acquaintance by taking on more responsibility [6]. Additionally, data analyses as a result of the assessment allow students, faculty members, and parents, as well as the broader educational community, to be informed about the teaching outcomes achieved at a specific time to highlight success, plan interventions, and continue to foster accomplishment [7].

In the case of face-to-face or online evaluation, completing this phase is critical to the overall success of the teaching and learning procedure [8][9]. In all cases, some students try to well evaluate by their proper efforts, but some others look for violating academic integrity [10]. When students are evaluated face to face, the traditional method of cheating is for any of them to try to chat to their colleagues, pass a note around, or bring a cheat sheet. To avoid this type of cheating, a supervisor is required, and sufficient spacing between student tables is provided to make his job easier. However, there are several new techniques to cheat on online exams [11][12][13][14][15]. The access to the Internet is the most common method of cheating [16][17][18]. Cheating with Internet access provides students endless sources of information as well as the opportunity to speak with others about how to provide unlawful services to students while they are taking the exam [18][19][20]. Additionally, Internet access enables screen sharing, remote desktop access, and the ability for someone other than the candidate to access the exam via the student's computer [18].

The first solution to minimalize online cheating is using applications to block the internet navigation that can be used in combination with the Learning Management System (LMS) like Blackboard [20]. When running this special application, students will have no access to any other resource on the device. The second solution is screen recording; some applications record and store the screens of the student's device while taking the exam [20][21]. The faculty member will use these recordings to ensure that the exam ran perfectly, and that the student did not cheat [22]. The third option is to use surveillance cameras to film the students' behavior and gaze throughout the exam. However, this technique is not completely effective, particularly when the number of students is large, as it will be difficult to control their behavior [22][23]. Many faculty members claim that it is difficult to organize an electronic evaluation without the risk of cheating, but efforts are still being made to reduce the number of possible fraudulent attempts [20-26]. As a result, it is necessary to be equipped with tools to prevent cheating, as well as to properly select the test options provided by the LMS and to accurately determine the periods for online exams [27][28].

Several approaches are possible to reduce cheating during remote exams. Depending on the student's input. The problem can be divided into three sub-parts: i) video, ii) voice, and iii) handwriting/mouse clicks. As a result, deep learning methods can be efficient for completing each of these subtasks [29-35].

This paper discusses new research on smart techniques for reducing cheating on higher education online exams. This study will provide an overview of the main techniques. It investigates the impact of artificial intelligence in preventing attempted cheating during an online exam, as well as the best way to reduce the risk of cheating. The controller's task is greatly aided by the opening of the cameras during the passage of the examinations at a distance. However, the use of a webcam is not permitted in some faculties, where educators are not permitted to ask candidates to turn on the camera. In this case, it is more difficult to detect cheating. As a result, our main contribution is to present a solution without filming the candidate. Several parameters will be implemented to complete this mission, such as the identification of the IP address and the candidates' academic and personal information, as well as the capture of navigation screen images, that will be processed by Convolutional Neural Networks (CNN).

This paper is organized as follows: Section 2 presents the study background; we'll give a brief review of the most important techniques based on AI for detecting and reducing cheating behaviors in electronic online assessments. Section 3 offers solutions for managing online exams in the absence of a camera and based on LMS options. Section 4 presents the CNNCDS, its architecture, and its main components such as the K-Nearest Neighbor (K-NN): and the Principal Components Analysis (CPA). In Section 5 the experimentations and the results are offered before the conclusion section.

II. Study Background

In their evaluation methods, online education models try to emulate the traditional teaching way which remains without any doubt the most reliable method for evaluation [17][18][19], indeed the world's largest virtual universities and online training institutions always rely on presential evaluation in specially designed testing centers. Remarkably, some online evaluations do not pose any cheating problem, but for other types of evaluation, cheating is possible [17][19][20][22]. Indeed, the most important questions that arise at the beginning of this study: What types of solutions can be adopted to prevent cheating in an online exam? And, what are the means to further disseminate the notion of academic integrity?

Academic integrity is an important aspect of higher education. These values safeguard a university's reputation, as well as the scientific value and meaning of degrees, and they also provide a framework for professional and academic work. In [23], the authors attempt to answer an important question that arises when discussing online education: why does academic dishonesty occur? And, why some students are compelled to engage in these behaviors while learning online. They present the most commonly used methods for promoting academic integrity. The authors in [24] state that it is possible to uncover cases of identification of cheating behaviors through the strengthening of the faculty member-student relationship and real-time discussions between them. As a result, the proposal is to expand student-faculty member discussions similar to those that have traditionally occurred in the classroom. The authors present Intelligent Discussion Comments (IDC), using a scalable asynchronous system to engage students in real-time discussions to extract authentic student understanding. To enrich the discussion process and supporting the educational team in their supervisory, two AI services are used such as voice recognition and transcription.

Online exams have emerged on the surface on various types of academic misconduct, including plagiarism. In addition, academic misconduct and plagiarism represent a barrier to the development of students' critical thinking and analytical skills [24]. In [25] the researchers analyze various forms of academic misconduct and propose strategies applicable in higher education, nut the rapid evolution of technology has made it difficult to well detect cheating attempts, so other methods of detecting cheating must be used.

In the following section, we will first present biometric authentication, and then we discuss the most important research that dealt with smart techniques and various methods and tools for detecting and preventing cheating.

A. *Biometric Authentication*

Biometric authentication verifies an individual's identity and ensures secure access to an electronic system by utilizing an individual's unique biological characteristics. Biometric technologies are based on the notion that each individual can be uniquely identified by one or more biological characteristics such as fingerprints, hand morphology, retina and iris physiognomy, voice waves, typing dynamics, DNA, or signatures. The use of these identity proofs as part of a validation process for a user wishing to access a system is known as biometric authentication [26]. Biometric technologies are being used to secure a wide range of digital communications, whether for a business, an e-commerce site, internet payments, or simply connecting to a computer or a smartphone. Biometric authentication systems compare the provided biometric data to the confirmed authenticated data in a database. Authentication is confirmed and access is granted if the two samples match. This procedure is occasionally used as part of a multi-factor authentication system. Thus, the user of a smartphone can connect using his secret pin code and add an iris scan to it. Many types of biometric authentication technologies like the retinal scan produce an image of the arrangement of blood vessels on the photosensitive surface of a person's eye. Iris recognition identifies an individual based on the unique patterns of their iris, which is the ring of color around the pupil. Furthermore, the finger scan (a digital version of the fingerprint created with an ink pad and paper) analyzes the patterns drawn by ridges and creases on a finger image. The recognition of finger veins is based on the individual's unique pattern of finger veins. Also, facial recognition systems employ digital codes known as "faceprints" to identify 80 nodal points on the human face. Finally, rather than more variable conditions, voice identification systems rely on characteristics generated by the shape of the speaker's mouth and throat. The world has progressed from the oldest known biometric verification method, to modern biometric verification methods that are almost instantaneous. It is also becoming more precise as a result of the introduction of computerized databases, the digitization of analog data, and AI techniques. AI concerns the conception of an artificial machine capable of possessing or exhibiting the capacities and characteristics of a human brain [29][30]. It is in fact about teaching the machines to think. There are two types of approaches for AI, the first is strong, called the cognitive approach when the machine must think like a man. The second is weak, called the pragmatist approach when the machine must lead to the same solutions as humans. AI remains difficult to define because we do not know how to define the notion of Intelligence. Intelligent methods proliferate, and there is a relationship between them "Fig. 1". We are attempting to focus on those who can contribute to the administration of online exams.

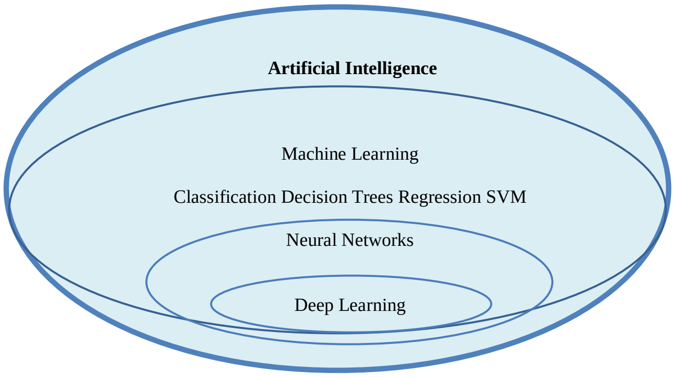


Fig. 1. The Relationship between Different Types of Machine Learning Methods.

B. *Related Work based on the Role of Intelligent System*

In the literature, several possible definitions of AI. In general, AI is a methodology that makes computers more intelligent, so they show characteristics normally associated with intelligence in human behavior, i.e. language comprehension, learning, problem-solving, and reasoning [29].

1) Natural language processing: Natural Language Processing (NLP) is a multidisciplinary field that combines linguistics, computer science, and artificial intelligence to develop natural language processing tools for a variety of applications. It should not be confused with computational linguistics, which uses computer tools to understand languages. NLP emerged from research labs to be gradually implemented in computer applications that required the incorporation of human language into the machine. As a result, NLP is also known as linguistic engineering. Some researchers have used NLP to detect cheating such as [32-34].

2) Machine learning: Machine Learning is an AI technology that gives the possibility to machines to learn without having previously been programmed. Machine Learning is explicitly linked to Big Data since to learn and grow, computers need data streams to analyze and train on [35]. The greatest advantage offered by machine learning is analyzing a very huge volume of data much more efficiently in terms of speed and precision than other traditional methodologies. Machine Learning can detect cheating in a millisecond, just by basing itself on data introduced, as well as on other historical and social information Machine Learning is the ideal science to take advantage of Big Data and its opportunities [36]. This technology can extract valuable data from immense and complex sources of information without involving humans. Entirely driven by data, Machine Learning is therefore perfectly suited to the complexity of Big Data, from which it is truly inseparable. Traditional analytical tools often come up against a maximum volume of data that can be analyzed. Machine learning reveals its full potential when data sources are growing, allowing it to learn and refine insights with precision always improved. Some researchers have used Machine Learning to find solutions against cheating in online exams [35-38]. In [37], the authors introduced a new way which consists in authenticating the student, it is a question of analyzing the answers and verifying that the student is the author of them. The researchers present FLEXauth, which is an application for discovering cheating in digital exams and based on AI techniques with the assumption that each student has an individual style to answer certain types of homework. then they made comparisons with reference material for which the author is verified. In [38], the authors present a chapter on intelligent methods of cheating detection using machine learning, and they review some scientific articles from various disciplines that address the challenges of cheating detection. They use machine learning to detect anomalies, errors, and cheatings by emphasizing numerous empirical considerations critical in developing cheating prediction models. The authors in [28] focus on the modeling of activities to prevent cheating problems, they present the RIVA method which considers the face-to-face activities undertaken at the faculty. Next, the author proposed a model for supervising an online exam that contains substantial improvements.

In [21], the authors dealt with intelligent preventive systems on neural networks and took into consideration two main modules: The Internet Protocol (IP) detector and the behavior detector. Student behavior is monitored to prevent and detect any malicious practices. They proposed an e-cheating intelligence agent that is based on the relationship model for detecting online cheating using AI technique by monitoring IP and student behavior as well as creating a new dataset for this study. The proposed method used Long Short-Term Memory (LSTM) network with a densely connected concept, namely DenseLSTM to detect online cheating. The proposed method was examined on different data groups confirming its effectiveness. The Deep Neural Network (DNN), LSTM, DenseLSTM, and Recurrent Neural Network (RNN) achieved accuracy rates of 68%, 92%, 95%, and 86%, respectively [21].

In [20], Man and Harring proposed a new method to try to prevent cheating by using an eye-tracker. The proposed method was created by integrating visual fixation and eye-tracking indication into a traditional psychometric modeling framework and investigating pattern differences in the trade-offs of visual attention. Sangalli and his colleagues in [22], suggested some measures based on co-occurring events and measures of interaction with the course to distinguish between two kinds of cheating. They used K-means clustering and Support Vector Machine (SVM). They gained good results with an accuracy of over 95%.

In [39], the authors designed a Convolutional Neural Network (CNN) model for users to enter text by looking at the on-screen keyboard and blinking. A method that divides the human gaze into nine directions. The CNN model accurately estimates how people look under different lighting conditions.

The authors in [38] used the online m-learning course sessions to design and propose a robust method of variations in pose and lighting for facial verification using a camera-based on CNN.

In [42], the authors propose students' performance evaluation examining on the computer using a new approach based on process exploration. Their approach consists of two phases: process extraction and similarity analysis. They apply a real-life application in an Enterprise Resource Planning (ERP) course to present the practicality, usefulness, and validity of the proposed approach. Fifteen student responses are evaluated by the instructor. This work proved a very good match between the automatic evaluation system and the instructor.

In the context of assessment control, the most intelligent methods used for cheating detection are based on CNN "Fig. 2". CNN are widely applied in image and video recognition, recommender systems, and natural language processing. A CNN is a type of feed-forward artificial neural network, in which the connection pattern between neurons is inspired by the visual cortex of animals [35]. The arrangement of the neurons in this region of the brain is so that they overlap when paving the visual field. Their operation is inspired by biological processes, they consist of a multilayer stack of perceptron's, the purpose of which is to preprocess small amounts of information [37]. A major advantage of convolutional networks is the use of a single weight associated with the signals entering all the neurons of the same convolutional nucleus [42]. This method reduces the memory footprint, improves performance, and allows translation processing invariance. This is the main advantage of the CNN over the multilayer perceptron, which considers each neuron independent and therefore assigns a different weight to each incoming signal [44]. When the input volume varies over time, it becomes interesting to add a parameter along the time scale in the parameterization of the neurons. In this case, we will speak of a time-delayed neural network. Compared to other image classification algorithms, convolutional neural networks use relatively little pre-processing. This means that the network is responsible for changing without supervision, which is not the case with other more traditional algorithms. The absence of initial settings and human intervention is a major advantage of CNN. A first approach would be to use a simple Machine Learning algorithm, such as logistic regression or a random forest. Although these approaches obtain relatively correct results, this type of algorithm will not be able to be generalized to images whose item ends up in a corner of the image rather than in the center of it. In other words, the spatial character of the characteristic elements of certain categories is not considered. To well achieve the goals, we need to use an algorithm capable of detecting relative shapes regardless of their position in the image: this is what CNN allow. Yann LeCun [40] was one of the first to apply this type of neural network on a large scale, to detect amounts on checks in the 1990s.

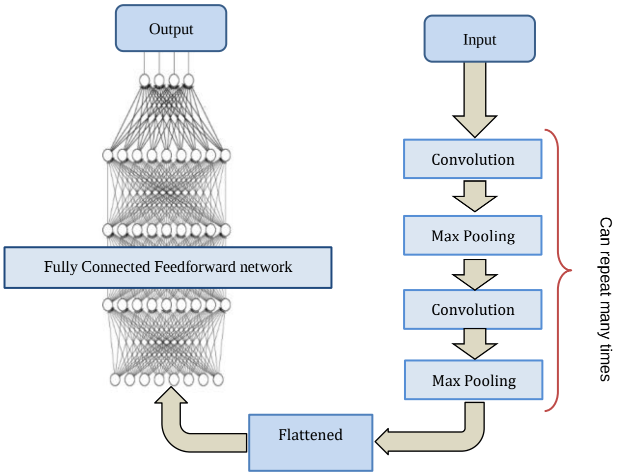


Fig. 2. Convolutional Neural Networks.

3) Using artificial neural networks for webcam analysis methods: To monitor an online exam, we only had the student's microphone, webcam, and input devices (keyboard/mouse). In this section, we will focus on video and detecting student keyboard/mouse input rather than audio. The aim of this section is to explain the method used to generate a database of synthetic student videos. When a student takes the exam online, a stream of videos is sent to the teaching team. Indeed, since the student's computer boots to a live image, it gives us greater control of their machine and allows us to gain access to the webcam, microphone, and keyboard. The aim is to give the possibility to supervise several students in parallel during the exam. The goal is therefore to annotate a video and notify the supervisor at the right time. We might think that to monitor more students, no automation is required and that it would suffice to employ more people to monitor students remotely. While this is theoretically achievable, it is not possible to scale it for a course with a larger number of students taking their exams online. This would require complex logistics. Indeed, for a small course, it is still possible for several members of the teaching team to supervise a few students at a time, but today online courses have several hundred students, it is therefore difficult to have the logistics to allow so many exams online simultaneously. These data would allow passing judgment a priori on the most diligent students, but do not help with the direct supervision of the exam. Therefore, the overall goal of the system that we wish to achieve is to flag times of suspicious activity to aid supervisors by guiding their attention helping them to supervise more students at a time. Action detection is already achievable if you have the data. This would only be based on the pre-trained actions of the network [41][42]. On the process of face images generation, the data is the basis of these types of intelligent methods. Monitoring by video is based on the notion of normality. The idea is to learn neural network normal behavior, then anything that does not fit into this normality is classified as abnormal and requires supervision by a human. This has already been done by [22] which makes it possible to obtain such a classification space. This method uses a database of videos, each with a normal or abnormal tag. More formally, it is necessary to encode the data in a vector space of greater dimension which will be used for the training. The network will then learn a decision boundary among this data, to obtain a better representation for classification. The network will therefore be able to discriminate any element belonging to this space. The boundary will classify behaviors considered normal on one side and all abnormal elements on the other. It is, therefore, necessary to provide enough normal behaviors so that the network can learn and generalize about the behavior of students during the exam period. The rest is up to human empathy to decide whether cheating is suspected. However, many researchers such as [43][44][45] had shown that we can learn and manipulate image spaces: transferring their contents and representations to others.

III. Proposed Solutions

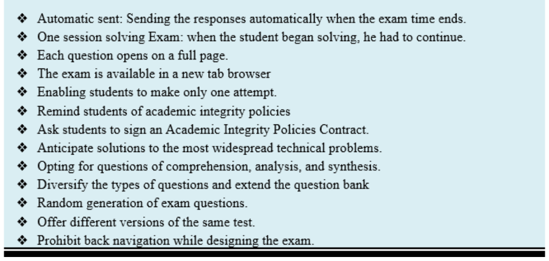
At the onset of the pandemic, and through other challenges associated with distance education, student online evaluation became the most important issue for faculty members.

The first experience of many students and faculty members with online learning was urgent and unprepared. In the spring of 2020 [13], it was discovered that the rate of cheating on online exams had increased. The peculiarity of the educational environment in some faculties is characterized by the interdiction of using the camera. Faculties cannot require students to use a camera while taking an online test, so this study considered alternatives without using a camera during the remote electronic assessment.

A. Solutions in the absence of a Camera

From a legal standpoint, the University’s policies must address the subject of digital examination monitoring, whether through biometrics and/or AI or simply recorded video surveillance (Blackboard, WebEx). This is only permissible if the students consent to it explicitly, freely, and informedly.

In the absence of a video of the student taking the exam from home, e-learning management systems like Blackboard provide a multitude of options that the faculty member should be familiar with to make the remote exam more reliable and secure “Fig. 3”.



- ❖ Automatic sent: Sending the responses automatically when the exam time ends.
- ❖ One session solving Exam: when the student began solving, he had to continue.
- ❖ Each question opens on a full page.
- ❖ The exam is available in a new tab browser
- ❖ Enabling students to make only one attempt.
- ❖ Remind students of academic integrity policies
- ❖ Ask students to sign an Academic Integrity Policies Contract.
- ❖ Anticipate solutions to the most widespread technical problems.
- ❖ Opting for questions of comprehension, analysis, and synthesis.
- ❖ Diversify the types of questions and extend the question bank
- ❖ Random generation of exam questions.
- ❖ Offer different versions of the same test.
- ❖ Prohibit back navigation while designing the exam.

Fig. 3. Tips for Secure Exams.

B. Attribute Classes

When performing online exams, the most important attribute is candidate authentication. The main attribute classes can be classified as follows:

1) Verification of normal behavior: this is a continuous verification of the candidate's normal behavior: The detection of abnormal behavior in online exams should not be done at the start of the exam only; periodic and continuous verification is needed.

2) Security: Here we are dealing with the subject of access to the exam which must be completely secure, and no foreign person can access it.

3) A rich and diversified question bank: The richer the question bank, the easier it will be to generate the exam and the more secure the evaluation.

4) LMS conviviality: The LMS should be simple and accepting.

C. Check the IP Address

Faculty members use different methods to verify the identity of students. The IP address is a way of locating the student with good precision. To ensure that they do not have students taking the exam together, the network allows each student's IP address to be communicated when connecting to the LMS. It is the main condition for sending the exam key. A trick is also to send the exam key in the video conference chat and close the exam key as soon as all students have entered. Then it is difficult for the students to pass the exam key to someone else. The exam key only controls the entrance to the exam. Students can continue to take the exam when the instructor closes the exam key.

D. Blocking the Browser

Several applications make it possible to block the browsing of students on the Internet during the examination.

E. Recording the Exam Session

All student activities while taking the exam can be recorded and saved by the instructor.

F. Use of CNN Model

CNN was the first approach suggested and used for high-dimensional image analysis. It is composed of convolutional filters that convert 2D to 3D. The major benefit of CNN over author models is that it automatically identifies important features without the need for human intervention. In our framework, we will use the CNN model for cheating detection by analyzing the stored students’ sessions. During the exam cycle, each student's computer screen is registered and processed in the database for remote proctoring. When an unexpected event occurs, the evaluation results provide alerts for exam coordinators/online surveyors. The main objective of this work is to focus on cheating and plagiarism in online exams.

IV. Convolutional Neural Network for Cheating Detection System

Many projects have investigated and detected abnormal files using smart models [30-35]. All these projects investigated the video sequences emitted by the student's webcam. Our solution treats the images from the student's navigation screens as the second stage. While the first stage focuses on the student's academic and personal information, as well as his IP address.

In the absence of a camera, our solution sought to capitalize on all data that could be recovered directly relating to the student. The data in Table I. are of three types: data provided by the student once entering the university, data provided by the administration concerning the academic results of the student, and data provided by the LMS and exactly the report established by Analytic for Learn (A4L).

TABLE I. PERSONAL AND ACADEMIC STUDENT DATA

	Var1	**Var2**	**Var3**	
1. Personal student Data	First Name	Middle Name	Last Name	
	Day of Birth	Month of Birth	Year of Birth	
	Place of Birth	City of Birth		
2. University Data	Department	Faculty	Id	
3. Student Level	Instant student level	The average level in the course	Overall average	
4. Student Location	Country	City	Street	
5. Ip address	Block One	Block Two	Block Three	Block Four
6. Student activity on LMS	Access Operations	LMS Time Spent	Degree of Student Interactions	School Assignments Submission

Before delivering the exam key to the candidate, we use personal and geographical information as the first step in our solution. This is a method of knowing the seriousness of the student by ensuring that there is only one student in a small geographical area and the other information gives an idea of the diligently and performance level of the student. In Addition to these sources of students' information, we have data provided from our proposed CNNCDS classification model which checks whether the student cheated in the exam or not. The CNNCDS requires a set of human-defined goals to forecast, make recommendations, or make decisions affecting real or virtual environments. This is accomplished using both machine and human input. CNNCDS are intended to operate with varying degrees of autonomy. The designed framework is based on specialized knowledge and data derived from the student, as well as his history in the faculty and his behavior either in person (exam session recording) or virtually via the LMS.

A. *CNNCDS' Architecture*

CNNCDS's architecture is comprised of three types of layers: Convolutional layers, grouping layers, and classification layers. Convolution is the most important operation in the formation of a convolutional network. By applying a filter to a matrix representation of an image, it generates a series of small images, which are then passed to a grouping layer. This sequence can be repeated multiple times throughout the network until the vector containing the abstract properties reaches the flattening layer and passes to the dense layer. CNN is still being used to improve computer vision in terms of precision. The common CNN architecture contains many layers for continuously extracting appropriate image characteristics and feeding them to the classification module.

The goal of designing a CNN is to analyze the images of the screenshots, received during the online blackboard exam, and predict fraud. When designing CNNCDS, three main parameters were considered: image size, number of cores, number of layers. according to the minimum learning error obtained by each neural network of a specific number of layers ranging from 1 to 5, it is observed that the network with 2 layers corresponds to the error minimum. Concerning the number of filters, we note that we did not vary the size of a filter, we took the usual sizes used (5*5) and (3*3). For picture size, choosing a large size will make it hard to learn because the CNN input layer will be so big and therefore, we will need more hidden layers which will lead to memory shortage or long calculations.

From the previous sections, we combine the best parameters to design our CNN: 4 hidden layers, 32 filters, and 256 * 256 images. A convolutional layer can be made up of several conv2d layers followed by a grouping layer and may be dropped. Consequently, we have several conv2d layers grouped into two convolution layers. Flattening layers are used to transform the output into a long vector and then process it by a classification layer.

B. *The K-Nearest Neighbor (K-NN)*

This classifier has been adopted because of its best performance compared to (Multi-class Logistic Regression (MLR), Support Vector Machine (SVM), k-Nearest Neighbor (kNN), Random Forest (RF), and Gaussian Naive Bayes (GNB)).

The kNN uses the majority rule to assign the right class of membership to each non-labeled input by considering the distance between its k-nearest neighbors nearest to the training sample. To measure the differences between examples represented as vector inputs, many kNN classifiers employ simple Euclidean metrics. The Euclidean distance is calculated by (1).

$$d(x\ ,x_T) = \sqrt{\sum_{i=1}^{n} w_i((a_i(x) - a_i(x_T))} \qquad (1)$$

N represents the dimension of the entry vector u=($a_1$1, a_2,…, a_n), the weight of each attribute is represented by w. k-nearest neighbor determines the class label by (2).

$$Y(d_i) = argmax_k \sum_{x_j \in kNN} y(x_j, c_k) \qquad (2)$$

Equation (2) means the class prediction that has the most members in the k-nearest neighbor. d_i represents the test example. In the training set, the k-nearest neighbor is represented by x_j . $y(x_j\ , c_k)$ is binary and indicates if x_j belongs to the class c_k.

C. *Principal Components Analysis (CPA)*

CPA is used in exploratory data analysis and predictive modeling. It is commonly used for dimensionality reduction by projecting each data point onto only the first few principal components to obtain lower-dimensional data while preserving as much of the data's variation as possible. The first component was calculated by (3), to maximize variance:

$$w_1 = \arg\max_{\|w\|=1} \left\{\sum_i (t_1)^2{}_{(i)}\right\} \tag{3}$$

Written in matrix form, we obtained (4).

$$w_1 = \arg\max_{\|w\|=1} \{\|Xw\|^2\} = \arg\max_{\|w\|=1} \{ W^T X^T \, Xw\} \tag{4}$$

Rayleigh’s quotient is defined as the quantity to be maximized.

The n-th component will be obtained by subtracting the first n-1 principal components from X:

$$\hat{X}_n = X - \sum_{s=1}^{n-1} X \, w_s w_s^T \tag{5}$$

Then we obtain the weight vector that extracts the maximum variance. The selection of KNN and CPA is based on the literature, these two modules have provided satisfaction in many research projects.

D. Input Data

The entries are the raw bytes of an image file to generate a matrix. The byte stream of an image will be placed in an array and then transformed into a matrix. Images are symbolized in a variety of ways, the most frequent of which is as a grid of small squares known as pixels. In a very simple image with only black and white pixels, each pixel could be represented by a 0 (black) or 1 (white).

We can represent 2^8=256 different colors or shades of gray with 8 bits per pixel. This is adequate for a black-and-white photograph but does not allow for subtle color shades in a photograph. For full-color images, 32 bits per pixel are typically used, allowing for 2^{32}=4294967296 possibilities.

E. Output Data

The network output is binary, either normal or abnormal behavior. Because any file that is not identified as an exam screen page is considered a fraudster.

F. Data Preprocessing

The CNNCDS recognizes images from a dataset placed in a folder, and a Python program using the Keras and Tensorflow libraries was invoked to use these images. There are numerous deep learning frameworks available today. Keras was chosen because it helps to lower cognitive load, it provides a unified and simple Application Programming Interface, it reduces the number of user activities needed for common use cases, and it offers clear and actionable feedback in the event of operator error. Keras is completely embedded with low-level TensorFlow functionality, facilitates the creation of highly configurable workflows with the ability to customize any piece of features.

G. The CNNCDS Learning Process

The CNNCDS learning process began with the creation of a database during the administration of electronic exams on Blackboard in a presentable manner. The exam control has been well established, ensuring that the students' monitors are not obstructed. The images of the screen captured during the examination session are the CNNCDS network entries. The output of the network is binary and represents the student's normal or abnormal state. During the training process, CNNCDS “Fig. 4” learns the values of the filters on its own. The proposed framework consists of using general and personnel student data to carry out a secure online exam on LMS.

The faculty member is called to take advantage of the options provided by Blackboard to further secure the exam by i) Establishing a bank of diversified and numerous questions and ii) Providing the exam with a password iii) Controlling Students behavior using a CNN model as described in the flowchart “Fig. 5”.

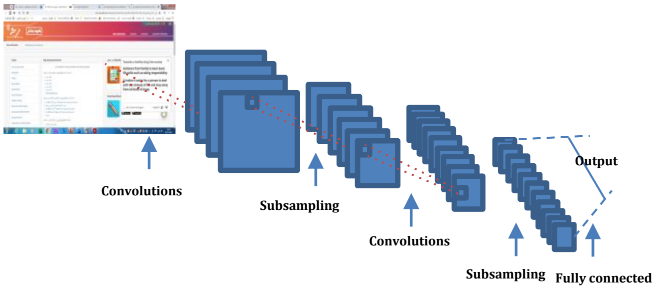


Fig. 4. The CNNCDS Structure.

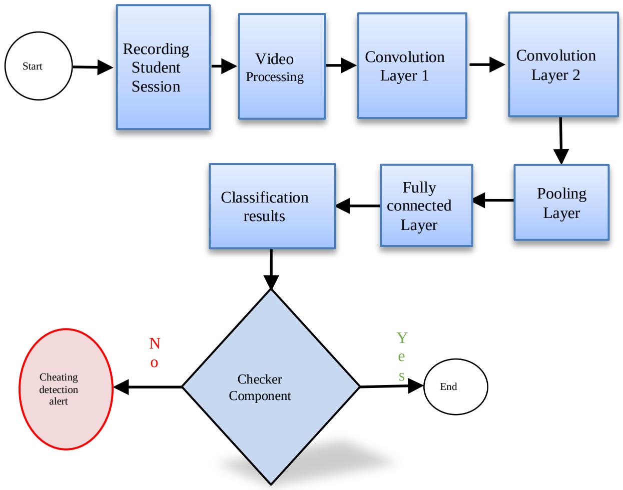


Fig. 5. Flowchart of the Proposed Video Sessions’ Management by the CNN Model.

V. Experimentations and Results

At the beginning of the academic year, an application form will be completed by the students which contains general and personal questions.

This application will be saved in the form of quizzes in the blackboard question bank tool. At any time during the exam, the faculty member can ensure the authentication of any student by launching polling from this question base. In this case, the student will have only 10 seconds to reply (Table II).

The online exam management procedure is divided into four steps: In the first step, the student had to run the program Myipaddress on his browser before connecting to Blackboard;

and he communicated it to the instructor. The instructor used a python application called IpControl to ensure that all the addresses are different and that there is only one student per address to avoid corporation between students while solving the exam. In the second step, the student launches two programs before receiving the exam key, the first to block navigation and the second to record the session. In the third step, the instructor sends the exam key to the students. The fourth step is to launch the CNNCDS program.

TABLE II. MONITORING SEQUENCE OF THE ONLINE EXAM

Students	Instructor	Time
	Preparing an application form	At the beginning of the academic year
Filling in the application form		At the beginning of the academic year
Launching My Ip Address Command		Before the beginning of the Exam
Sending Ip Address to the instructor		Before the beginning of the Exam
	Receiving Ip Addresses from all students	Before the beginning of the Exam
	Launching IpControl application	Before the beginning of the Exam
	Launching user authentication Application	Before the beginning of the Exam
	Sending confirmation to appropriate students	Before the beginning of the Exam
Blocking the navigation browser		Before the beginning of the Exam
Begin session registration		Before the beginning of the Exam
Informing the instructor		Before the beginning of the Exam
	Sending the exam key	Before the beginning of the Exam
Begin the exam		During the exam session,
	Sending a polling	During the exam session
Responding to the polling in 10 seconds		During the exam session
	Checking the results given by the CNNCDS	During the exam session
	Final classification of the student	During the exam session

To evaluate our proposed CNNCDS model at different levels, it was compared with four based classifiers. For given input data, a binary classifier generates output with two class values 1/0. The one of interest is typically represented as "positive," while the other is denoted as "negative". The observed labels for all data instances are contained in a test dataset used for performance evaluation. Having followed classification, the observed labels are compared to the predicted labels to determine performance. If a binary classifier's performance is perfect, the predicted labels will be identical, but it is relatively rare to be able to develop an ideal binary classifier that is useful in a variety of situations.

The confusion matrix is constructed from the three components of binary classification. A binary classifier predicts whether all data instances in a test dataset are positively or negatively. True positive, true negative, false positive, and false negative are the four outcomes of this classification.

- True positive (TP): correct positive prediction.
- False positive (FP): incorrect positive prediction.
- True negative (TN): correct negative prediction.
- False negative (FN): incorrect negative prediction.

Accuracy is the percentage of correct predictions that a learner has achieved. It is computed by dividing the number of correct estimates by the total number of predictions (6).

$$Accuracy = \frac{TN+TP}{TN+\ FP+FN+TP} \tag{6}$$

- Precision, also known as the positive predictive value, is the ratio of the pertinent instances to the retrieved instances (7).

$$Precision = \frac{TP}{FP+TP} \tag{7}$$

- Recall, also called sensitivity, is a fragment of the retrieved relevant instances (8).

$$Recall = \frac{TP}{FN+TP} \tag{8}$$

- The F1-score is a statistical measure that combines precision and recall with rate performance (9).

$$F1 - score = \frac{precision*recall}{precision\ +recall} \tag{9}$$

As we had mentioned above, during an electronic face-to-face exam on Blackboard, a database of examples was created in the eLearning. A list of images for normal files was created as well as a list of images for abnormal files. CNNCDS was compared to the other classifiers on two levels: the first with 70% of the base of examples reserved for learning and 30% for testing. The second test was conducted with 90% of the resources allocated to learning and 10% to testing (Table III).

TABLE III. THE PERFORMANCE OF CNNCDS

	Accuracy		**Error**		**Sensitivity**		**Pr. time**	
	70.30	90.10	70.30	90.10	70.30	90.10	70.30	90.10
Random Forest algorithm	95	96	5.0	4.0	95	96	4.0	5.0
Multi-class Logistic Regression	97	98	2.5	1.9	96	97.5	6	7
Gaussian Naïve Bayes	91	92.5	9	8	95.5	97	1	0.95
Support Vector Machine	97.1	98.0	3	2.50	96.5	97.5	10	13
CNNCDS	98.2	98.5	2	1.8	99.2	99.8	4	6

CNNCDS outperforms the basic classifiers (Multi-class Logistic Regression (MLR), Support Vector Machine (SVM), Random Forest (RF), and Gaussian Naive Bayes (GNB) in terms of mean accuracy (98.5%). Furthermore, it correctly identified screen images with an acceptable processor time, with a sensitivity average of 99.8% and a precision average of 1.8 %.

Following validation, the proposed method was tested in many sections at the first preparatory year college during the 2020-2021 academic year. The results were brilliant and provided great satisfaction except that the students found this method strange and comes to limit their activities during exams especially in the context of the covid-19 pandemic. The efficiency of the method is 100%. No fraud operation has been detected once the method is applied. The advantage of this method is the use of diverse Dataset and it does not rely on video sequences but rather on navigation sequences of students taking exams, the limitations are that the base of learning materials is specific to Umm al-Qura University.

VI. Conclusion

Dishonest students' actions reflect poorly on them and the Institute. Although copying is the most common form of dishonest, fraudulent students invent a variety of other forms of cheating. Outside the exam sessions, students should be aware that collaborative work is acceptable, but copying works against them and violates academic integrity principles.

Cheating attempts have increased, particularly with distance learning and online exams, as many faculty members seek new ways to combat the problem.

The purpose of this article is to prevent cheating and to find appropriate solutions to detect more complex types of cheating. It should also be a major concern for faculty members who want to maintain academic integrity. The document proposes new solutions to these problems to create more resilient and intelligent future systems. This work identifies intelligent methods for cheating detection in online education exams. The emphasis is placed on steps that faculty members had to undertake to secure electronic assessments. To accomplish this aim, the authors have defined the following four main objectives: i) Identify the latest technologies on cheating detection, ii) Identify the role of intelligent methods and their advantages on cheating detection and prevention, iii) Present a new model for online proctored exam process and determine its effectiveness, and iv) Apply this new model and identify the limitations of this study and recommend further work.

The most important approach is the prevention of cheating and finding appropriate solutions without using webcam. Research shows that most anti-cheating services can be hacked by various methods set up by very smart and connected students. AI techniques can help improve the performance of the detection procedure. The use of the webcam is always the most adequate solution to better overcome the problem of cheating. Not relying on the webcam made the mission difficult but possible.

The proposed method is based on i) IP address, ii) Personnel Student Data, iii) Blocking the browser, iv) Recording and analyzing the exam session. Also, when passing the exam, an authentication method is proposed to avoid cheating. Using a database specific to each student, polling questions will be sent to ensure that the student is himself and not another person who is taking the exam. A delay of 10 seconds only will be reserved for the student to respond.

The proposed method's main component is CNNCDS which classifies screenshots of students' computers while taking online exams and detects abnormal navigation. The CNNCDS was learned using a dataset created in the same environment as students took face-to-face electronic exams on Blackboard. CNNDCS was used on online electronic exams after it had been learned, tested, and validated. Its output is binary in order to alert the faculty member to unusual behavior.

In terms of mean accuracy, CNNCDS outperforms the basic classifiers (Multi-class Logistic Regression (MLR), Support Vector Machine (SVM), Random Forest (RF), and Gaussian Naive Bayes (GNB) (98.5%). Furthermore, with a sensitivity average of 99.8 % and a precision average of 1.8%, it correctly identified screen images in an acceptable processor time. This method is effective in reducing cheating in some universities where using the camera is not allowed.

Acknowledgment

The authors would like to thank the Deanship of Scientific Research at Umm al-Qura University for supporting this work by Grant Code: 19-EDU-1-03-0001.

References

[1] Crooks, T. J. (1988). The impact of classroom evaluation practices on students. Review of educational research, 58(4), 438-481.

[2] Entwistle, N., & Ramsden, P. (2015). Understanding student learning (routledge revivals). Routledge.

[3] Astin, A. W. (2012). Assessment for excellence: The philosophy and practice of assessment and evaluation in higher education. Rowman & Littlefield Publishers.

[4] Alruwais, N., Wills, G., & Wald, M. (2018). Advantages and challenges of using e-assessment. International Journal of Information and Education Technology, 8(1), 34-37.

[5] Dumford, A. D., & Miller, A. L. (2018). Online learning in higher education: exploring advantages and disadvantages for engagement. Journal of Computing in Higher Education, 30(3), 452-465.

[6] White, A. M. J. (2021). Information literacy and critical thinking in higher education: Some considerations. In Research Anthology on Developing Critical Thinking Skills in Students (pp. 111-124). IGI Global.

[7] H. M. Alakrash and N. A. Razak, "Education and the fourth industrial revolution: Lessons from COVID-19," Computers, Materials and Continua, pp. 951-962, 2021.

[8] L. W. Anderson, "Objectives, evaluation, and the improvement of education," Studies in Educational Evaluation, vol. 31, (2-3), pp. 102-113, 2005.

[9] Büchele, S. (2021). Evaluating the link between attendance and performance in higher education: the role of classroom engagement dimensions. Assessment & Evaluation in Higher Education, 46(1), 132-150.

[10] Ahsan, K., Akbar, S., & Kam, B. (2021). Contract cheating in higher education: a systematic literature review and future research agenda. Assessment & Evaluation in Higher Education, 1-17.

[11] García-Morales, V. J., Garrido-Moreno, A., & Martín-Rojas, R. (2021). The transformation of higher education after the COVID disruption: Emerging challenges in an online learning scenario. Frontiers in Psychology, 12, 196.

[12] Khenkitisack, P., & Reidt, E. The Learning Process of Students in Creating Video as an Exam Format in Higher Education–an Evaluation in an Economics Course.

[13] Bautista-Puig, N., Aleixo, A. M., Leal, S., Azeiteiro, U., & Costas, R. (2021). Unveiling the Research Landscape of Sustainable Development Goals and Their Inclusion in Higher Education Institutions and Research Centers: Major Trends in 2000–2017. Frontiers in Sustainability, 2, 12.

[14] Felix, J. J. (2021). Higher education in times of instability and disruption: Rethinking notions of values, value creation and instructional practices in Vietnam and beyond. Frontiers in Communication, 6, 22.

[15] Hamdan, K. M., Al-Bashaireh, A. M., Zahran, Z., Al-Daghestani, A., Samira, A. H., & Shaheen, A. M. (2021). University students' interaction, Internet self-efficacy, self-regulation and satisfaction with online education during pandemic crises of COVID-19 (SARS-CoV-2). International Journal of Educational Management.

[16] Almomani, E. Y., Qablan, A. M., Atrooz, F. Y., Almomany, A. M., Hajjo, R. M., & Almomani, H. Y. (2021). The Influence of Coronavirus Diseases 2019 (COVID-19) Pandemic and the Quarantine Practices on University Students' Beliefs about the Online Learning Experience in Jordan. Frontiers in Publi+c Health, 8, 997.

[17] Joseph, D., Nethsinghe, R., & Cabedo-Mas, A. (2021). Online teaching and learning during Covid-19: Flexible harmonies in higher education. In Online Teaching and Learning in Higher Education during COVID-19 (pp. 50-68). Routledge.

[18] Holden, O. L., Norris, M. E., & Kuhlmeier, V. A. (2021). Academic integrity in online assessment: a research review. In Frontiers in Education (p. 258). Frontiers.

[19] M. E. M. Amer, "Effectiveness of Using Electronic Exams in Assessment in Saudi Universities: Empirical Study," International Journal of Educational Technology and Learning, vol. 8, (2), pp. 61-69, 2020.

[20] K. Man and J. R. Harring, "Assessing preknowledge cheating via innovative measures: A multiple-group analysis of jointly modeling item responses, response times, and visual fixation counts," Educational and Psychological Measurement, vol. 81, (3), pp. 441-465, 2021.

[21] L. C. O. Tiong and H. J. Lee, "E-cheating Prevention Measures: Detection of Cheating at Online Examinations Using Deep Learning Approach--A Case Study," arXiv Preprint arXiv: 2101.09841, 2021.

[22] V. A. Sangalli, G. Martinez-Muñoz and E. P. Cañabate, "Identifying cheating users in online courses," in 2020 IEEE Global Engineering Education Conference (EDUCON), 2020, pp. 1168-1175.

[23] O. Popoola, "Marker detection of contract cheating: An investigative corpus linguistic approach," in European Conference on Academic Integrity and Plagiarism 2021, pp. 131.

[24] K. Rundle, G. J. Curtis and J. Clare, "Why students do not engage in contract cheating," Frontiers in Psychology, vol. 10, pp. 2229, 2019.

[25] M. Paechter and B. Maier, "Online or face-to-face? Students' experiences and preferences in e-learning," The Internet and Higher Education, vol. 13, (4), pp. 292-297, 2010.

[26] X. Zhu and C. Cao, "Secure Online Examination with Biometric Authentication and Blockchain-Based Framework," Mathematical Problems in Engineering, vol. 2021, 2021.

[27] H J. Bullock, A. Luccioni, K. H. Pham, C. S. N. Lam and M. Luengo-Oroz, "Mapping the landscape of artificial intelligence applications against COVID-19," Journal of Artificial Intelligence Research, vol. 69, pp. 807-845, 2020.

[28] R. Ismail, V. Osmanaj and A. Jaradat, "Moving towards E-university: Modelling the online proctored exams," AICMSE-AICSSH 2019 August (Oxford) | 12th-14th August 2019 Conference 2019.

[29] L. author, J. Boulahia and R. Bouallegue, "A semi blind channel estimation method based on hybrid neural networks for uplink LTE-A," International Journal of Wireless & Mobile Networks Vol, vol. 8, 2017.

[30] K. Muthumayil , M. Buvana, K. R. Sekar, A. E. , Amraoui, I. Nouaouri, and R. F. Mansour, "Optimized convolutional neural network for automatic detection of COVID-19," Computers, Materials and Continua, pp. 1159-1175, 2021.

[31] P. Dawson, W. Sutherland-Smith, and M. Ricksen. “Can software improve marker accuracy at detecting contract cheating? A pilot study of the Turnitin authorship investigate alpha.” Assessment & Evaluation in higher education, 45(4), 473-482.

[32] T. Lancaster, “Academic Dishonesty or Academic Integrity? Using Natural Language Processing (NLP) Techniques to Investigate Positive Integrity in Academic Integrity Research.” Journal of Academic Ethics, 1-21, 2021.

[33] S. K. Kim, and J.H. Huh, “Blockchain Agreement for Self-identification of Online Test Cheating: Improvement of Algorithm Performance,” In 2020 20th International Conference on Control, Automation and Systems (ICCAS), 2020, pp. 1124-1133.

[34] I. Đ Babić, "Machine learning methods in predicting the student academic motivation," Croatian Operational Research Review, pp. 443-461, 2017.

[35] F. Kamalov, H. Sulieman and D. Santandreu Calonge, "Machine learning based approach to exam cheating detection," Plos One, vol. 16, (8), pp. e0254340, 2021.

[36] M. Geetha, R. S. Latha, S. K. Nivetha, S. Hariprasath, S. Gowtham et al, "Design of face detection and recognition system to monitor students during online examinations using machine learning algorithms," in 2021 International Conference on Computer Communication and Informatics (ICCCI), 2021, pp. 1-4.

[37] J. Opgen-Rhein, B. Küppers and U. Schroeder, "An application to discover cheating in digital exams," in Proceedings of the 18th Koli Calling International Conference on Computing Education Research, 2018, pp. 1-5.

[38] H. S. Asep and Y. Bandung, "A design of continuous user verification for online exam proctoring on M-learning," in 2019 International Conference on Electrical Engineering and Informatics (ICEEI), 2019, pp. 284-289.

[39] J. Huang, G. Shen and X. Ren, "Connotation Analysis and Paradigm Shift of Teaching Design under Artificial Intelligence Technology." International Journal of Emerging Technologies in Learning, vol. 15, (5), 2021.

[40] Y. LeCun, Y. Bengio and G. Hinton, "Deep learning," Nature, vol. 521, (7553), pp. 436-444, 2015.

[41] T. M. Tashu, J. P. Esclamado and T. Horvath, "Intelligent on-line exam management and evaluation system," in International Conference on Intelligent Tutoring Systems, 2019, pp. 105-111.

[42] F. A. Abubakar and S. Boukari, "A Convolutional Neural Network with K-Neareast Neighbor for Image Classification,” International Journal of Advanced Research in Computer and Communication Engineering, vol. 7, pp. 1-7, 2018.

[43] C. Zhang, R. Yao and J. Cai, "Efficient eye typing with 9-direction gaze estimation," Multimedia Tools Appl, vol. 77, (15), pp. 19679-19696, 2018.

[44] S. Minaee, M. Minaei and A. Abdolrashidi, "Deep-emotion: Facial expression recognition using attentional convolutional network," Sensors, vol. 21, (9), pp. 3046, 2021.

[45] D. Canedo, A. Trifan and A. J. Neves, "Monitoring students’ attention in a classroom through computer vision," in International Conference on Practical Applications of Agents and Multi-Agent Systems, 2018, pp. 371-378.