A Smart Framework for Enhancing Automated Teller Machines (ATMs) Fraud Prevention

Mohamed Abdelsalam Ahmed[1], Nada Tarek Abbas Haleem[2], Amira M. Idrees[3]
Information Systems Department-Faculty of Commerce & Business Administration, Helwan University, Cairo, Egypt[1]
Business Information Systems Department-Faculty of Commerce & Business Administration, Helwan University, Cairo, Egypt[2]
Faculty of Computers and Information Technology, Future University in Egypt, Cairo, Egypt[3]

***Abstract*—Over the past years, clients have largely depended on and trusted Automated Teller Machines (ATMs) to fulfill their banking needs and control their accounts easily and quickly. Despite the significant advantages of ATMs, fraud has become a very high risk and danger. As it leads to controlling all clients' accounts. In this paper, the proposed framework is using the iris recognition technology combined with the one-time password (OTP) to detect and prevent the known as well as the unknown attacks on ATMs and provide a table of the attackers and the suspected attackers with a counter to take a preventive action with them. Our proposed preventive actions are: card withdrawal, flagging the identified iris as an attacker in the database, notifying the card owner with this suspicious behavior, reporting to the Central Bank of Egypt (CBE), and calling the police when an attacker's iris counts three capturing times, even if for a different card. Two case studies were attempted to achieve the highest accuracy, the first case was using the Chinese Academy of Sciences' Institute of Automation V1.0 (CASIA-IrisV1) dataset using the Cosine Distance. The second one was using the Indian Institute of Technology Delhi (IITD) dataset using k-Nearest Neighbors (KNN) and Histogram of Oriented Gradient (HOG) techniques together reaching 100% accuracy.**

Keywords—Automated Teller Machines (ATMs); digital banking; image processing; iris recognition; One Time Password (OTP); machine learning; fraud detection; fraud prevention; biometrics; security; banking

I. Introduction

Automatic Teller Machines (ATMs) provide a non-stopping banking services without any time or place limitations [1, 2], which gives it this huge importance worldwide. It allows cash withdrawal, cash deposits, checking the account balance, paying bills and many other banking services over 24 hours / 7 days.

Despite all these advantages, ATMs are a very risky banking channels if they are not provided with the right security methods [3]. The current ATM framework was designed to avoid this risk, the current framework is that ATMs are designed with the Personal Identification Number (PIN) as the main authentication factor and some monitoring cameras to record all the daily interactions.

However, this design does not provide the required protection as the PIN has not become a very safe authentication technique [4], as when ATM cards are lost or stolen, an unauthorized user can get and enter the correct PIN and access all the clients' accounts and money [5]. In addition, this monitoring tool is insufficient because of the lack of security guards and because the human factor is the only monitoring factor, this security design is not helpful for detecting or preventing ATM fraud. This can be helpful after a fraud occurs.

The current – after fraud - scenario is that the client receives an SMS from the bank saying that he made a withdrawal with a specific amount, then the client begins to realize that he is a fraud victim and starts to report this fraud and asks for this video to check who is the criminal. In most of these cases, clients cannot get their money back or find the criminal. As the number of ATM users is growing daily because of the digital transformation awareness and the high increase in the number of deployments of new ATMs in addition to the increasing economic impact of the banking services [6]. So, detecting the fraud or the criminal is not enough as a preventive action all the time. As the same criminal can do this fraud in many other places with many different clients easily without detecting that he is a recorded criminal.

In this paper, a framework is proposed by using the iris recognition for the authentication of ATMs which can automatically detect and prevent the known as well as the unknown attacks on ATMs. Iris recognition is an advanced biometric technology that is used for detecting and identifying human iris from an image or video. It has many benefits that make it a perfect solution for the ATMs authentication. One of these benefits is that they are stable and unique over the whole life.

The biometric authentication became an important concern for many researchers because of the huge continuous wave of ATMs attacks worldwide. It is the process of identifying whether a specific person is the authorized person or not using a unique biological characteristic such as the fingerprint, face recognition, Iris recognition, voice recognition, behavior authentication and many other types [7, 8]. It works by comparing the enrolled biometric in the database with the person's captured biometric to authenticate. That is what makes it very helpful in the fast transactions-based authentications, as it is fast, accurate and not forgettable.

Iris recognition is an advanced biometric technology that is used for detecting and identifying human iris from an image or video. It has many benefits that make it a perfect solution for the ATMs authentication. One of these benefits is that it is stable and unique over the whole life [9]. The biometric authentication has been a very important concern for many researchers due to the huge continuous wave of attacks all over the world [10]. Biometric authentication is the process of identifying whether a specific person is the authorized person or not using a unique biological characteristic such as the fingerprint, face recognition, Iris recognition, voice recognition, behavior authentication and many other types [11]. It works by comparing the enrolled biometric in the database with the person's captured biometric to authenticate. That is what makes it very helpful in the fast transactions-based authentications, as it is fast, accurate and not forgettable [12].

Our paper is organized as the following: Section I which is an introduction of our paper including all the related topics of our framework. Followed by Section II, which gives a background about fraud and some biometric technologies with a comparison of how much they are effectively works to prevent any fraud. Then Section III, which includes a sample of other similar researches that were taken as a reference while our study. Then Section IV, which proposes our framework with two case studies to achieve the highest accuracy, followed by Section V which presents the structure of the database of our proposed framework. Then Section VI provides our experimental setup showing how our framework was implemented to get the case studies' results. Then Section VII, which presents the research contribution showing how our workflow overcomes the limitations of the other proposed solutions. Then in Section VIII we will present our results. And finally, Section IX concludes the paper.

II. Background

Fraud has many increasing techniques when it is related to the banking sector. It may be direct to the banking channels by stealing the card itself, the client's credentials, and many other direct ways. Or through any other way like the social media for example, which has been increasing and by sequence affects the banking sector which makes it a must to consider the information credibility as a very high concern to be considered at any fraud detection and prevention solution including all its perspectives [13]. It had been noticed also that the gap that allows the fraud to increase is the spread of using the technology by all its applicable tools without giving an attention to the relation between the more advanced the current technologies are and the greater the risk of the leakage of our data security and privacy [14].

For the example of social media, we are currently facing a very increasing phenomenon of customizing fraud campaigns over the social media and SMSs using some fake information and news to be able to steal the clients' banking data, which leads to being able to attack their banking channels and take their money [15, 16].

Noting that the fraud process is not necessary to start from the attacker's side, as sometimes the user is the initiator of this fraud, by listening to the spreading social media fake news (specially the Facebook as it is the most influencing social media application) and aim to gain more money and benefits then enters his banking or financial data to an untrusted source [17, 18].

There are various techniques that can be used to authenticate using biometrics. Below is a comparison in Table I:

TABLE I. Comparison of the Biometric Technologies

Biometrics	Cost	Accuracy	Performance	Flaws	Stability
Iris	High	High	High	Lighting	High
Retina	High	High	High	Glasses	High
Face	Medium	Medium	Medium	Beard, Glasses, Age	Medium
Fingerprint	Low	Medium	Medium	Dirt, Dryness	High

III. Literature Review

In this section we will provide a view of the historical researches about the iris authentication and how researchers used it to detect the ATM fraud actions and enhance the ATM security.

After reviewing several studies, we found that some researchers used only the iris recognition as a single authentication technique, while some of them used it in cooperation with other techniques also.

Some researchers used the multi-factor authentication approach, Akinola Kayode E. and his colleagues, (2019) proposed in their paper they used the iris recognition with the PIN to obtain the benefit of both the accuracy, the low cost (compared to the other approaches), the small size of its tool, the easiness of its programming language, and to avoid the risk of using only the PIN. The results of their paper were that the Fake Acceptance Rate (FAR) was 0% while Fake Rejection Rate (FRR) was found to be 99.94% which means that it was not possible for any fraudster to match the identity of another user in the database. There was 1.6% of the authentic users got denied access, which is small amount. ATM users should be security focusing while withdrawing money to prevent forced withdrawals. However, using the PIN with the iris is useless as a security with, it is just making the ATM journey timing longer which is against the purpose of the ATMs [19].

Other research such as Joyce Soares and A.N.Gaikwad, (2016) didn't only decide to replace the current ATM system with another biometric system using the iris recognition and the fingerprint to authenticate. But also protected the ATMs terminals from the thieving attacks and from the fire danger by making provisions of the pump motor and a direct current (DC) motor for rolling the shutter. Their system uses two techniques each for each recognition type. The Circular Hough Transform for iris recognition and the minutiae matching algorithm for fingerprint recognition. From the technical perspective, they used the ARM7 (a processor) based LPC2148 (a microcontroller) controlling to make the accessing process easy and smart. Their system's results provide the average accuracy of the overall system is 91.6% and the of these biometric technologies: average equal error rate is 0.076 in addition to securing from the fire and thief attacks. It also shows that the taken time for whole the ATM transaction is less than 10 seconds per user. After analysis, they mentioned that the accuracy and the security of this system is maximum and reaches up to 95%. However, they lost the main purpose of the

ATMs, which is the fast timing of making financial banking interactions. Also, if the user used the choice of the fingerprint, he/she will face a hygienic risk [20, 21].

Mohamed A. Kassem and his colleagues, (2014) noticed the high risk of attacks on the ATMs. So, they decided to make a framework that is secured an also fast using the multimodal biometrics. But to choose the right biometrics to be used they followed some criteria like the universality, uniqueness, permanence, measurability, performance, acceptability, and the circumvention. The main purpose of this proposed system is to reach a higher performance than using only a single biometric system. After passing the above-mentioned criteria to choose the right biometrics, they decided to use the fingerprint and the iris together as they are having the most acceptance of people than face recognition for example and based on the availability of their integration devices. However, they lost the main purpose of the ATMs, which is the fast timing of making financial banking interactions. In addition, if the user used the choice of the fingerprint, he/she will face a hygienic risk [22].

N.Geethanjali and K.Thamaraiselvi, (2013) proposed a system that is not only based on the multimodal biometrics, but also on the two levels of authentication in the ATMs. The system provides three choices of the multimodal biometrics during the authentication: Fingerprint and Iris, Iris and Face, Face and Fingerprint. The user can choose any system of them based on the biometrics that he wants to enroll for the verification to be authenticated. If the user failed to authenticate because of any reason, the user will be directed to a second choice of verification using another two biometrics. This will make the false acceptance rate (FAR) and the false reject rate (FRR) decrease and ensure a high level of security. However, they lost the main purpose of the ATMs, which is the fast timing of making financial banking interactions. Also, if the user used the choice of the fingerprint, he/she will face a hygienic risk [23].

Other research used only the iris recognition technology, like Pratiksha, and her colleagues, (2020), they used the iris recognition as it offers a new solution for identifying, authenticating and securing the user by analyzing the random pattern of the iris. Their iris system works by recognizing the person from an eye image and comparing it to the human iris pattern that is already stored at the template database. They used CASIA database at their paper and applied their project using MATLAB. Their results after using 20 images for training, 10 images for testing to calculate some features such as the contrast, the energy and the homogeneity were that their proposed system ad recognition rate of 94.6 % using the probabilistic neural network (PNN) [9].

Abiodun Esther Omolara and his colleagues, (2019) proposed a system that solves the ATMs fraud problem using the FingerEye. Their proposed system passes with three phases. The FingerEye is a strong system that is integrated with the iris scanning authentication. They register the users' iris at the profile creation stage and analyze it then convert it into a binary code then store it at the bank database. Their target was not only to prevent the ATM fraud, but also to design a new solution that helps the clients with disabilities as the blind clients to use ATMs' services. The results were saying that the proposed solution has a competitive advantage than the other proposed solutions as it does not only mitigate the Shoulder-surfing attacks, but prevents all the possibilities of shoulder-surfing, eavesdropping, and man-in-the-middle attacks. They also found that they improved the efficiency of the system by making the average authentication time to be 1.4 seconds instead of the current timing which is 6.5 seconds (using the bin or the password). They were unable to test this solution on a blind client, but they concluded that the authentication will be also secured and faster. However, the proposed module is really a difficult & complicated workflow, as they are depending on many processes and tools to implement the framework. So, it loses the main purpose of the ATMs, which is the fast timing of making financial banking interactions [24].

Komal Marathe and Hemant Mande, (2019) decided to develop a system to protect the ATMs' consumers from any fraud. They proposed an application called "Face Recognition System" (FRS), which can identify the client from a captured digital image or even from a video. The normal technique of this system is to match the captures photo's facial features with the stored one at the database. But that is not everything, if they availed a strong lighting and learning, the future authentication trials and transactions will have a wide base with boarders to compare with in case of failing at the original account image comparing. In their system, when the face image gets captured, the face gets located, then the iris gets detected and scanned then compared with the captured image at the database. At the end, they found that using a 2D and 3D technology had protected the authentication security level of the ATM strongly [25].

S. Koteswari and his colleagues, (2012) applied the concept of visual cryptography (VC) in the iris recognition by implementing the cryptographic software using Matlab 7.9.A modified version which is a method of maintaining the security of the captured images. That happens by dividing the image into a random share with encrypting it using a key. And it will be decrypted also using the same key. Their proposed method focuses on protecting the iris templates that are saved at the database. They divided their proposal into two phases. The enrolment phase and the authentication phase. As a result of their proposed system, this identification system is quite simple requiring few components and is effective enough to be integrated within security systems that require an identity check. The errors that occurred can be easily overcome by the use of stable equipment. Judging by the clear distinctiveness of the iris patterns we can expect iris recognition systems to become the leading technology in identity verification in ATM banking [26].

IV. The Proposed Framework

After passing with all the previous papers, we can start with our proposed framework. In this paper we are proposing a multi-authentication framework that detects and prevents the fraud actions on the ATMs, that will be applied through using the iris recognition biometric technology at the authentication phase at the ATM with the One Time Password (OTP) as a second step authentication to allow the client to access his/her accounts. The following figure represents the proposed framework (see Fig. 1):

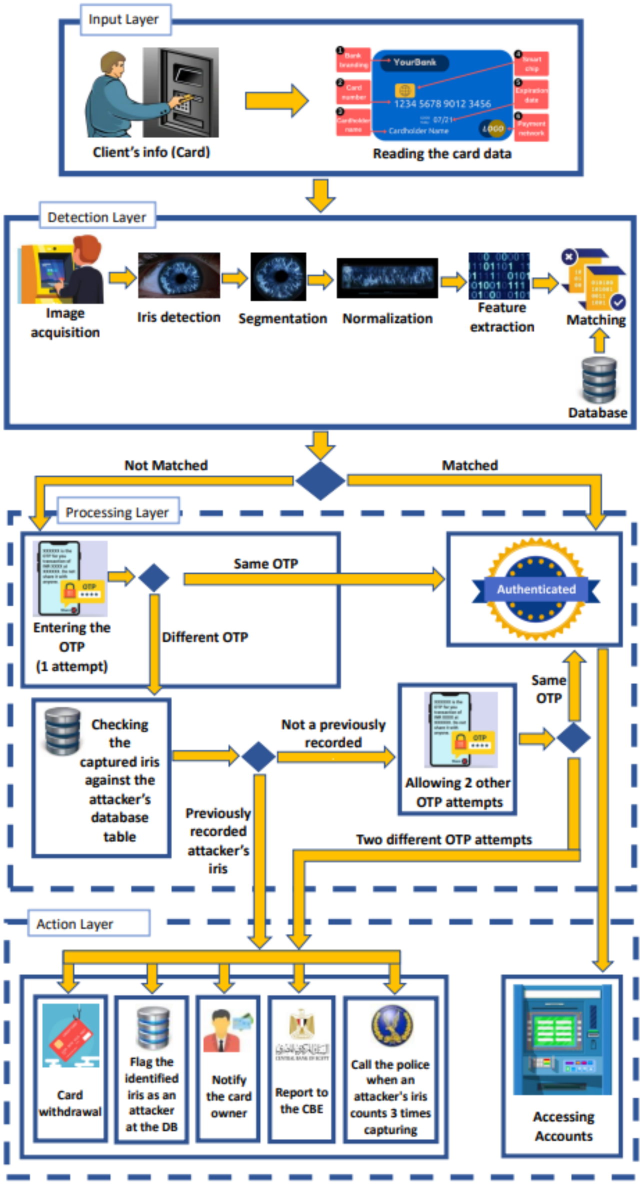


Fig. 1. The proposed framework.

In order to achieve the goal of our framework, we have gone through two case studies with two different techniques and datasets which gives us the ability to discover the most efficient and effective technique to achieve our main goal with this framework.

1) Case study (1): Our framework contains four layers (see Fig. 5), the input layer (see Fig. 2), the detection layer, the processing layer, and the action layer. It starts with the input layer, in which the client enters his card into the ATM, then the ATM starts reading the card data which includes the bank branding, the card number, the cardholder's name, a smart chip, an expiration date, and the payment network.

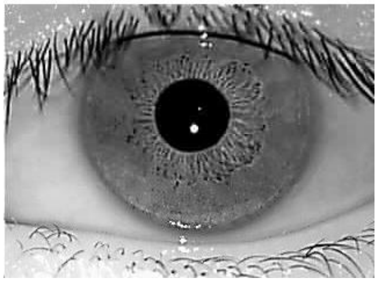


Fig. 2. The input layer.

Then it moves to the second layer, which is the detection layer, it includes the iris recognition cycle which starts with the user's image acquisition, and then it automatically detects the user's iris. After detecting the iris, this detected iris goes through another three steps before being matched with the database:

- Segmentation: In which the iris region gets isolated from the whole eye (see Fig. 3).

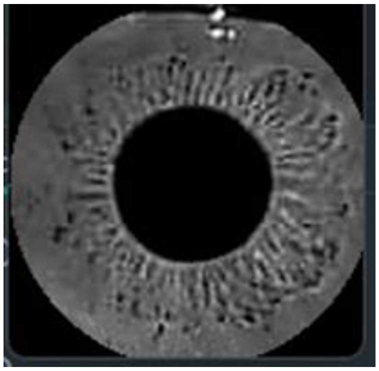


Fig. 3. The segmentation layer.

- Normalization: In which the segmented iris image gets transformed into a fixed size and dimensions to be ready for the next step (see Fig. 4) which is the feature extraction step. The below formula [27] is the normalization formula which was used at our framework:

$$\begin{gathered} I_n(X,Y) = I_o(x,y) \\ x = x_p(\theta) + \left(x_i(\theta) - x_p(\theta)\right)\frac{Y}{M} \\ y = y_p(\theta) + \left(y_i(\theta) - y_p(\theta)\right)\frac{Y}{M} \\ \theta = 2\pi X/N \end{gathered} \tag{1}$$

where, I_n is a $M \times\ N$ (64× 512 in our experiments) normalized image, $x_p(\theta)$, $y_p(\theta)$, and $\left(x_i(\theta) - y_p(\theta)\right)$ are the coordinates of the inner and outer boundary points in the direction θ in the original image I_0 [27].

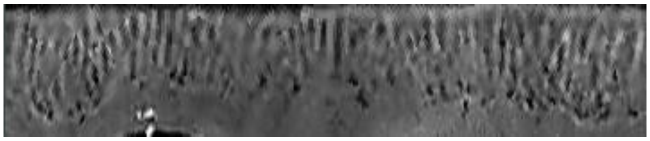


Fig. 4. The normalization layer.

- Feature Extraction: In this step, the normalized iris image gets converted to a set of parameters (mathematical parameters) to be ready to be easily matched with the database at the next step. The below formulas [27] are the feature extraction formulas which were used at our framework:

$$G(x,y,f) = \frac{1}{2\pi\delta_x\delta_y} exp\left[-\frac{1}{2}\left(\frac{x^2}{\delta_x^2}+\frac{y^2}{\delta_y^2}\right)\right] M_i(x,y,f),$$
$$i = 1,2.$$
$$M_1(x,y,f) = \ cos\left[2\pi f\left(\sqrt{x^2+y^2}\right)\right] \qquad (2)$$
$$M_2(x,y,f) = \ cos[2\pi f(xcos\theta + ysin\theta)]$$

where, $M_1(x,y,f)$ denotes the modulating function, M_1 and in M_2 are the modulating function of the defined filter and Gabor filter, respectively, f is the frequency of the sinusoidal function, δ_x and δ_y are the y axis, respectively, the θ denotes the orientation of Gabor filter [27].

$$m = \frac{1}{n}\sum_{\omega}|F_i(x,y)|\,, \quad \sigma = \frac{1}{n}\sum_{\omega}\big||F_i(x,y)| - m\big| \qquad (3)$$

where, w is an 8 × 8 block in the filtered image, n is the number of pixels in the block w, and m is the mean of the block ω [27].

$$F_i(x,y) = \iint I(x_1,y_1)\, G_i(x-x_1, y-y_1\ )dx_1dy_1;$$
$$i = 1,2 \qquad (4)$$

where, G_i is the ith channel of the spatial filters, $I(x,y)$ denotes the ROI, and $F_i(x,y)$ is the filtered image [27].

The last step at the iris recognition cycle and the detection layer is the matching step, in which the extracted feature gets compared to the stored one at the database during the enrolment phase to see if it is the cardholder or not. The following formula [27] is the matching formula which was used in our framework:

$$d_3(f,f_i) = 1 - \frac{f^T \quad f_i}{\|f\| \ \|f_i\|} \qquad (5)$$

where, f and f_i are the feature vector of an unknown sample and the i th class, $d_n(f,f_i)$ denotes the similarity measure, d_3 is the L1 distance measure, L2 distance measure (i.e., Euclidean distance) and cosine similarity measure, respectively. The feature vector f is classified into the mth class, which is the closest mean, using the similarity measure $d_n(f,f_i)$ [27].

It leads us to the next layer, which is the processing layer, in this layer; we will have two possible options: the first one is that the captured iris and the stored iris at the database are matched, and the second option is that they are not matched.

1) *If* matched, the user will authenticate normally and will be able to move to the action layer to access his/her accounts.

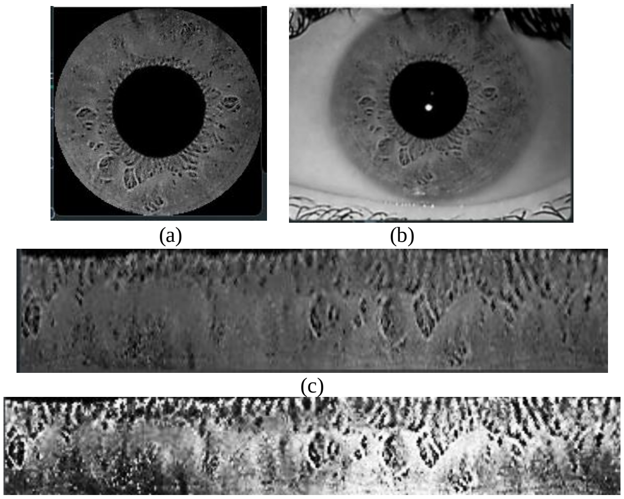
2) *If* not matched, the user will receive an SMS with an OTP on his/her mobile and will be asked to enter it into the ATM for a just one attempt. If it was the same OTP, then he/she will authenticate normally and will be able to move to the action layer to access his/her accounts. But if it is not the same OTP, then the system will start checking the captured iris against the attackers database table to check if it is a previously recorded attacker's iris or not.

If his/her iris got matched with any attacker's iris, then the system will move to the action- layer to take the below actions on the user as he/she will be detected as an attacker:

1) *Card* withdrawal.
2) *Flag* the identified iris as an attacker at the DB.
3) *Notify* the card owner.
4) *Report* to the CBE.
5) *Call* the police when an attacker's iris counts three times capturing, even if for a different card.

If not matched, then the user will receive another SMS with an OTP and will be asked to enter this OTP with only two attempts. If he/she entered the same OTP, then he/she will authenticate normally and will be able to move to the action layer to access his/her accounts. But if he/she entered a wrong OTP at the two attempts, then the system will move to the action layer to take the below actions on user as he/she will be detected as an attacker:

1) *Card* withdrawal.
2) *Flag* the identified iris as an attacker at the DB.
3) *Notify* the card owner.
4) *Report* to the CBE.
5) *Call* the police when an attacker's iris counts three times capturing, even if for a different card.


(a) (b)

(c)

(d)

Fig. 5. Image pre-processing (a) The original image (b) The segmented / localized image (c) The normalized image (d) The normalized image after enhancement.

2) *Case study (2):* Our framework at this case contains a pre-processing stage, which is the Image Pre-processing stage, as we are using here Indian Institute of Technology Delhi (IITD) dataset, which contains eyelashes and eyelids and are in many different sizes which affects the results efficiency. So, we will go through the Image Resizing to unify the iris images and make sure these are all with the same dimensions and suitable for the framework's best results by allowing it to get the same number of features from all the dataset's iris.

Considering also that there is a relation between decreasing the image’s size and the processing time [28] so, the images sizes became (200×200 pixels) after this stage.

The second stage is the Segmentation stage, at this stage the mission is to remove the non-useful surrounding regions of the iris by detecting the boundaries of both the iris and the pupil automatically which ease the feature extraction process of these images. As an output of this stage, we should have a ready image for the next stage which is the Feature Extraction stage. In this case study, we are using the Daugman‘s Integro-Differential operator technique for the iris segmentation which works by dividing the eye into two circles, the pupil and the iris, then detecting the center and radius of the pupil and the iris. The circle on the pupil explains the distance between the pupil and the iris then the circle on the iris shows the distance between the iris and the other parts of the eye. The third stage is the Feature Extraction, which is the most important stage and in which the needed and important features get extracted from the image and un-needed features are excluded. In our framework we will use Histogram of Oriented Gradients (HOG) for the feature extraction stage. In which the image gets divided into some cells, and each cell into some pixels. Now, we have arrived to the last stage at our framework which is the Classification stage, at this stage we have user K-Nearest Neighbor (k-NN) algorithm to be able to obtain the highest accuracy which works by finding the nearest neighbor object at the extracted feature space then gives an output that the entered iris belongs to which group of features.

V. Structure of Database

Fig. 6 shows the Entity Relation Diagram (ERD) that represents our proposed framework, it contains all the related parties of our framework and explains the relation between them. The “Attackers History” table includes all the history of any detected attacker, which has a many-to-one relation with the “Attackers” table, which counts the iris’s capturing time as an attacker. It also has all the required tables with all the data that helps at the fraud detection, prevention, reporting to the central bank of Egypt (CBE), and taking the right legal action.

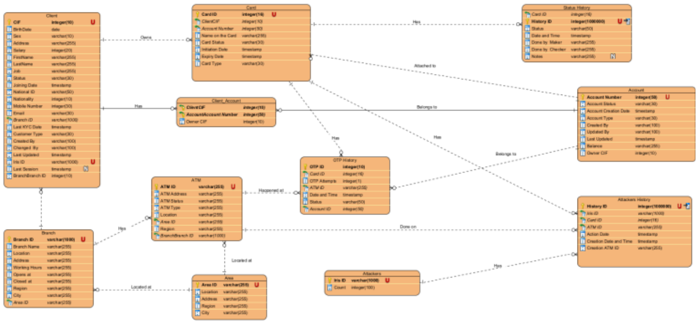


Fig. 6. Database Entity Relation Diagram (ERD).

VI. Experimental Setup

Due to the difficulty of implementing the proposed model at this stage in the real life because of its very high-cost hardware requirements, we decided to simulate the ATM device currently by a Graphical User Interface (GUI) that describes the customer interactions with the ATM into our framework. Below we will attach some highlights of our framework:

1) The main step that appears to the customer to enter his Card ID and the ID of the ATM he is acting with is a simulation to the physical card entering to the ATM and to upload his Iris as a simulation to the live scanning of his iris, then the client clicks on “Enter” (see Fig. 7):

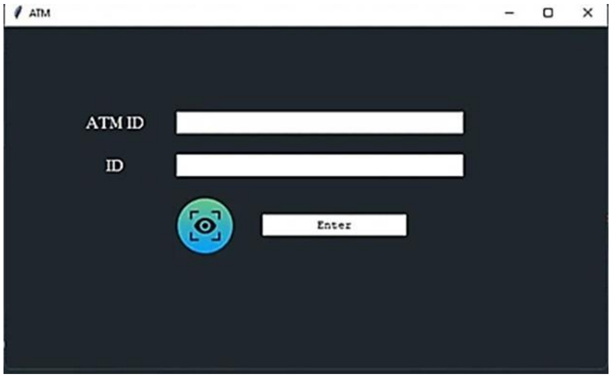
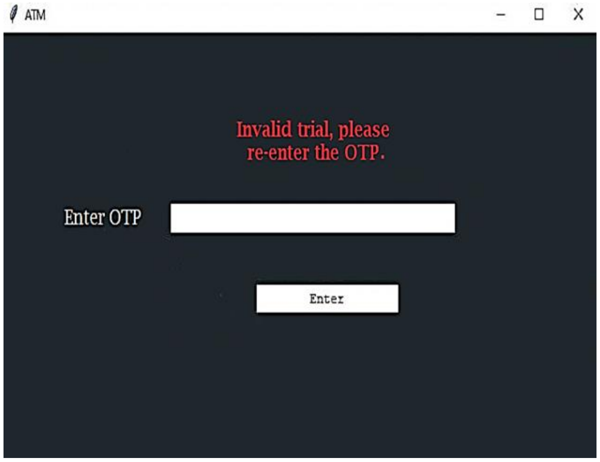


Fig. 7. The first step at our proposed system.

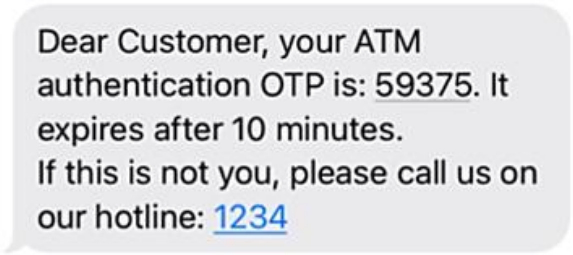
2) In case if the captured Iris was a wrong iris (not the iris of this card), then the client will be asked to enter the OTP the was sent to the mobile number of his card. So, the below screen simulates this step to allow the client to enter his OTP (see Fig. 8):



Invalid trial, please
re-enter the OTP.

Fig. 8. Case of capturing a wrong iris.

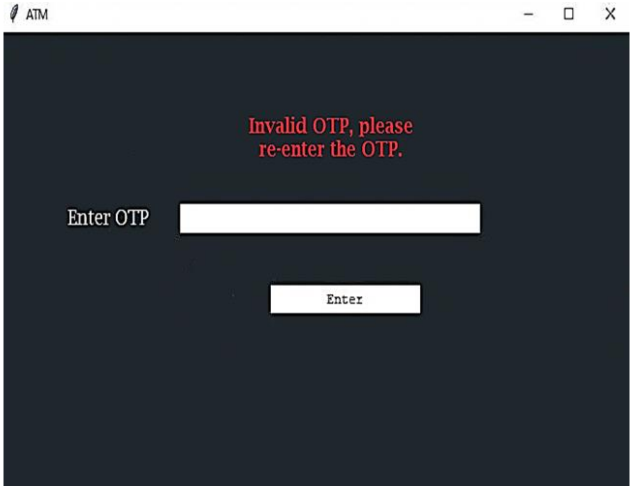
3) The OTP SMS that will be delivered to him from the SMS gateway with a random OTP (see Fig. 9):



Dear Customer, your ATM authentication OTP is: 59375. It expires after 10 minutes.
If this is not you, please call us on our hotline: 1234

Fig. 9. First OTP SMS

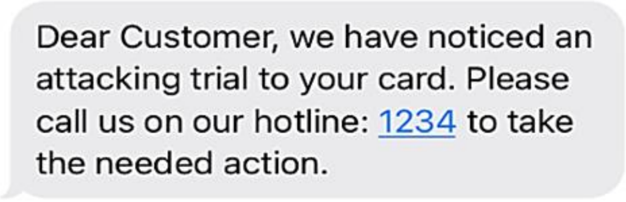
4) In case of entering a wrong OTP, the system will verify the captured iris against the attackers table first, then if it does not match with any attacker's iris, another OTP attempts will be allowed to him with two different SMSs (The third SMS will be sent to him only in case of entering a wrong OTP for the second time). The below screen shows the screen that asks the client to re-enter the OTP (see Fig. 10):



Invalid OTP, please re-enter the OTP.

Fig. 10. Case of entering a wrong OTP.

5) In case of entering a wrong OTP for three times (even if in a different periods or ATMs), the card will be withdrawn, and the customer will receive the below SMS at the mobile number of his card (see Fig. 11):



Dear Customer, we have noticed an attacking trial to your card. Please call us on our hotline: 1234 to take the needed action.

Fig. 11. Case of entering a wrong OTP for three times.

VII. Research Contribution

Our workflow overcomes the limitations of the other proposed solutions as shown in the below Fig. 12, at this part we will explain all our contribution points in details:

1) Suitable to all cultures, as it does not need a specific level of knowledge, age, education or a specific culture to be used, it is just following the signs on the ground of the ATM to be able to allow the iris to be captured.

2) Achieves the main purpose of ATMs, which is making some banking transactions in a short time: as this framework balances between the high security and the effectiveness at the same time, as it is not complicated and does not take much time to authenticate with.

3) Prevents ATMs fraud, not just detects it: as the main idea of our framework is to prevent the attacker from making any fraud on the card without limiting the client's needs from the service. So, in case of noticing any abnormal behavior, the card will be withdrawn, and a legal action will be taken with the attacker and his data.

4) Hygienic way to authenticate: as it is touchless, so, no way to transfer any virus or disease while authenticating.

5) Ensures a high level of security: as it uses the two factors authentication technique to make sure that if the iris recognition failed according to any surrounding reason, the OTP will pass.

6) In case of detecting a fraud action, the card will be withdrawn: to ensure the safety of clients' data and money, our framework will prevent the attacker from keeping the client's card with him, to avoid being used at any suspicious website that does not require an OTP.

7) Using the iris recognition to authenticate: as this technique is highly secured, unique, and can't be affected by age or illness. It avoids the weakness of the PIN and face recognition, avoids the complication of the other high-level biometric security techniques like the retina, and avoids the high hygienic risk of the fingerprint.

8) Uses the two factors authentication in case of failing at the iris recognition: this point achieves the required balance between making the business process runs smoothly and normally and ensuring a high level of security. As we always give the client another chance to validate that he is the card owner, not an attacker.

9) Reporting the attackers' details to the CBE: as this step ensures having a centralized database between all the banks and the governmental institutions with the attackers' data, which accelerates and facilitates avoiding any upcoming attacks and taking the right legal action in case of facing any attack.

10) Building a database table of the detected attackers with a counter: this step facilitates taking the right preventive action with the captured attackers and prevents the fraud from happening next time.

11) Calling the police when the attacker's iris counts three times capturing; this step will be an instant action to prevent the attacker if it was faster than the attackers' trials.

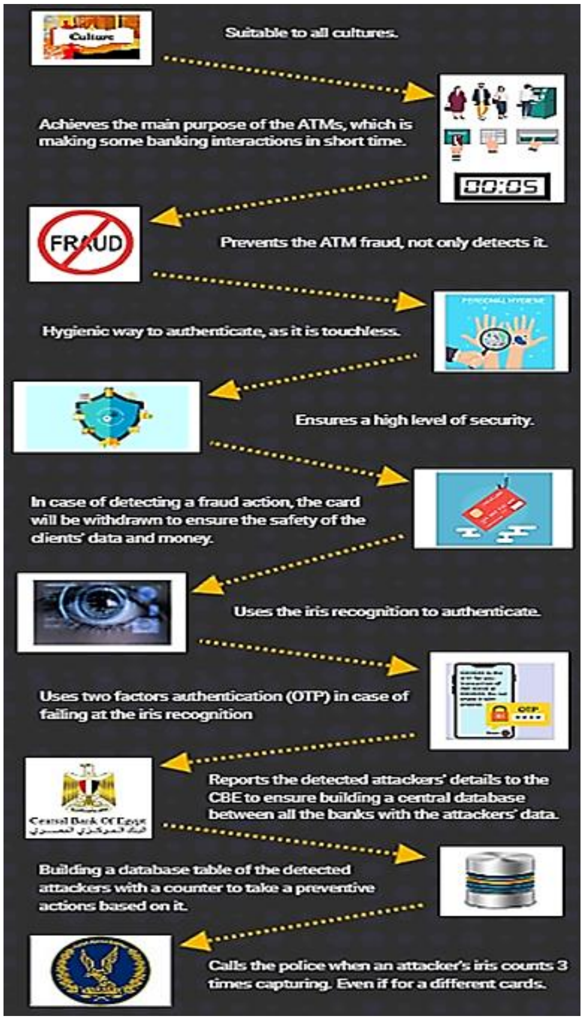

Culture
Suitable to all cultures.
Achieves the main purpose of the ATMs, which is making some banking interactions in short time.
00:05
FRAUD
Prevents the ATM fraud, not only detects it.
PERSONAL HYGIENE
Hygienic way to authenticate, as it is touchless.
Ensures a high level of security.
In case of detecting a fraud action, the card will be withdrawn to ensure the safety of the clients' data and money.
Uses the iris recognition to authenticate.
Uses two factors authentication (OTP) in case of failing at the iris recognition
OTP
Reports the detected attackers' details to the CBE to ensure building a central database between all the banks with the attackers' data.
Central Bank Of Egypt
Building a database table of the detected attackers with a counter to take a preventive actions based on it.
Calls the police when an attacker's iris counts 3 times capturing. Even if for a different cards.

Fig. 12. Workflow overcomes the other solutions' limitations.

VIII. Results

For the case study (1), we selected to use the Chinese Academy of Sciences' Institute of Automation V1.0 (CASIA-IrisV1) [29] dataset currently at our module. It consists of 756 iris images from 108 eyes. For each eye, there are seven images captured in two sessions and stored in bitmap (BMP) format with a resolution of 320*280 pixels.

These 756 irises are specified as two main groups, the first group is for the iris that was captured at the first session, they are three images and used as a training dataset. While the second group is for the iris that was captured at the second session, they are 4 images and used for testing.

Using CASIA-IrisV1 dataset, we applied our framework on two different cases and ways.

1) The first one is using the original CASIA-IrisV1 dataset normally, where each folder contains the training and testing iris for the same person. In this case, the recognition results using Different Similarity Measures are as provided in Table II:

TABLE II. The Recognition Results Using the Original Dataset

Similarity Measures		Correct Recognition Rate (CRR) %	
		Original Feature Set	Reduced Feature Set (107)
1	**L1**	60.87963	66.203704
2	**L2**	54.398148	73.611111
3	**Cosine Distance**	54.398148	75.925926

We decided to work with the Cosine Distance as it provides the highest accuracy as shown above 75.925926%.

Which means that out of 107 irises, there are around 81 irises got matched successfully. However, there are 26 irises didn't get matched successfully due to many environmental factors.

Noting that reducing the feature set to "107" resulted into a higher accuracy and a lower computational power, as this reduction had reduced the confusion of comparing across many features.

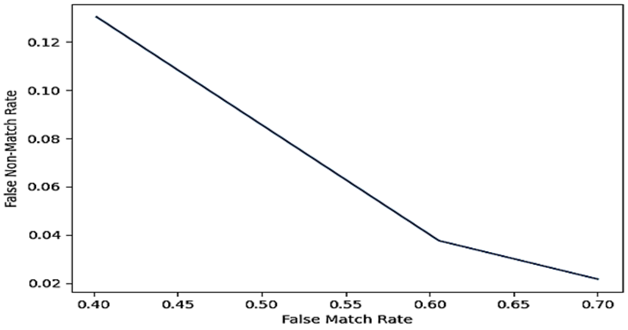


Fig. 13. Recognition results using cosine distance.

This graph in Fig. 13 describes the relation between the false non-match rate (FNMR) and the false match rate (FMR), the FNMR is when we compare the iris of someone to his other iris during the testing phase, and the results became another one's iris. So, it is a false non-match result. During the FMR is when we compare two different iris of two different people at the testing phase, and it results as the same iris. So, it is a false matching result. So, it is an inversely proportional relation between them as shown at the graph. The relation of coaptation (ROC) is calculated as: FMR/1-FNMR. At this case, the FMR and the FNMR are the percentage of the non-accurate results of the framework, this percentage of non-accuracy can be treated by the data augmentation. By increasing the training dataset, the module will be more trained and will have the ability to reach more accuracy and avoid any FMR or FNMR.

At each iris, we can extract many features to be used at detecting the iris owner, which takes a very high computational power. So, we reduced the taken features to be just 107 features. This graph in Fig. 14 shows that when we reacted 40 features extracted, we got the highest accuracy we need. So, at this point, we can close the program and get enough results. However, if we completed 107 features, we would reach highest accuracy that we can get using the extracted features, which is: 75.925926%.

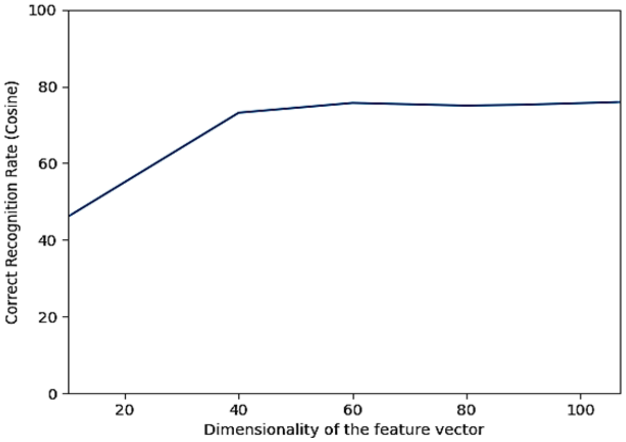


Fig. 14. Receiver Operating Characteristic Curve (ROC).

2) The second one is using CASIA-IrisV1 dataset but with applying some changes on it, by replacing the testing iris of each folder with another person's iris to check if it will be matched normally or not. In this case, the recognition results using Different Similarity Measures are as provided in Table III:

TABLE III. THE RECOGNITION RESULTS USING THE NEGATIVE DATASET

Similarity Measures		Correct Recognition Rate (CRR) %	
		Original Feature Set	**Reduced Feature Set (107)**
1	**L1**	1.388889	0.462963
2	**L2**	1.388889	0.462963
3	**Cosine Distance**	1.388889	0.462963

As shown at the above table, the resulted CRR is 0.46%, this very low accuracy rate is due to some human errors during capturing the iris dataset, which led to a FMR and FNMR by this percentage. So, we do recommend availing this framework at a very suitable environment by applying the ATMs shields as what is already happening at most of the banks, that will lead to getting the highest results and accuracy from the module.

For the case study (2), we have decided to use IITD (IIT Delhi [30] dataset using k-Nearest Neighbors (KNN) and Histogram of Oriented Gradient (HOG) techniques. We have selected to use the Indian Institute of Technology Delhi (IITD) database, this database is a bitmap format image database which was collected from the students and the staff of the Indian Institute of Technology Delhi (IITD) at July 2007 using JIRIS, JPC1000, and digital CMOS camera which consists of 2240 images from 224 different groups of users who are between 14-55 years (176 males and 48 females) 10 images gets registered for each user in an indoor environment. The resolution of each image is 320 x 240 pixels. The results of this combination were great! as it reached 100% accuracy with seven images for training and 3 images for testing as in Table IV:

TABLE IV. TESTING RESULTS OF USING (HOG) + (KNN)

Images Numbers Per Person	Training: 7 images Testing: 3 images	Training: 3 images Testing: 2 images	Training: 2 images Testing: 3 images	Training: 1 image Testing: 4 images
Accuracy %	100%	99.33%	98.21%	96.31%

IX. CONCLUSION

The technique of using the iris recognition combined with the OTP as a second step authentication is a reliable technique to secure the ATMs, as it provides a highly secured system with a fast timing to complete any financial transaction. In addition to our proposed model, which does not only succeed in achieving this security at a fast time, but also enhanced its prevention by providing a table of the attackers and the suspected attackers with a counter and a preventive action (notifying the user, notifying the bank, reporting to the CBE to centralize & share these data with the other banks, and reporting to the police). We also recommend by the end of our paper to use k-Nearest Neighbors (KNN) and Histogram of Oriented Gradient (HOG) techniques together to reach the highest accuracy (100%).

In the future, it is noted that the larger the dataset size we use, the better the accuracy we get. So, we are planning to use the other mentioned sources of data in our module to achieve the needed level of accuracy and to use the deep learning technology: Convolutional Neural Network (CNN). It is necessary to plan to enhance this model by cancelling the use of any cards to authenticate and by providing a suitable system for the users with disabilities to be able to do all their financial actions through the ATM normally.

REFERENCES

[1] O. H. Embarak, “A two-steps prevention model of ATM frauds communications,” 2018 Fifth HCT Information Technology Trends (ITT), Nov. 2018, doi: https://doi.org/10.1109/ctit.2018.8649551.

[2] M. C M, “Card-Less ATM Transaction using Biometric and Face Recognition– A Review,” International Journal for Research in Applied Science and Engineering Technology, vol. 8, no. 7, pp. 1493–1498, Jul. 2020, doi: https://doi.org/10.22214/ijraset.2020.30444.

[3] M. Sharaf, S. M. Ouf, and A. M. Idrees, “Risk Assessment Approaches in Banking Sector-A Survey,” Future Computing and Informatics Journal, vol. 8, no. 1, 2023, doi: http://Doi.org/10.54623/fue.fcij.8.1.3.

[4] M.-B. B.L, A. M.E, G. Ganiyu, and S. O. S.O, “An Enhanced ATM Security System using Second-Level Authentication,” International Journal of Computer Applications, vol. 111, no. 5, pp. 8–15, Feb. 2015, doi: https://doi.org/10.5120/19533-1181.

[5] N. S. Elhusseny, S. M. Ouf, and A. M. Idrees, “Credit Card Fraud Detection Using Machine Techniques ,” Future Computing and Informatics Journal, vol. 7, no. 1, 2022, doi: https://doi.org/10.54623/fue.fcij.7.1.2.

[6] A. M. Idrees and A. E. Khedr, “A Collaborative Mining-Based Decision Support Model for Granting Personal Loans in the Banking Sector,” International Journal of E-Services and Mobile Applications, vol. 14, no. 1, pp. 1–23, Jan. 2022, doi: https://doi.org/10.4018/ijesma.296573.

[7] A. T. Siddiqui, "Biometrics to Control ATM scams: A study," 2014 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2014], Nagercoil, India, 2014, pp. 1598-1602, doi: https://doi.org/10.1109/iccpct.2014.7054755.

[8] S. Oko and J. Oruh, “ ENHANCED ATM SECURITY SYSTEM USING BIOMETRICS ,” IJCSI International Journal of Computer Science, vol. 9, no. 5, 2012.

[9] Meryl Mascarenhas, “ATM Security System using Iris Recognition by Image Processing,” International Journal of Engineering Research and, vol. V9, no. 07, Jul. 2020, doi: https://doi.org/10.17577/ijertv9is070414.

[10] A. T. Siddiqui and Mohd. Muntjir, “A Study of Possible Biometric Solution to Curb Frauds in ATM Transaction,” IJASCSE, vol. 2, no. 3, 2013.

[11] S. Phadke, “The Importance of a Biometric Authentication System,” The SIJ Transactions on Computer Science Engineering & its Applications (CSEA), vol. 01, no. 04, pp. 18–22, Oct. 2013, doi: https://doi.org/10.9756/sijcsea/v1i4/0104550402.

[12] S. T. Bhosale and B. S. Sawant, “SECURITY IN E-BANKING VIA CARD LESS BIOMETRIC ATMS,” International Journal of Advanced Technology & Engineering Research (IJATER), vol. 2, no. 4, 2012.

[13] A. M. Idrees, Y. Helmy, and A. E. Khedr, “Credibility aspects’ perceptions of social networks, a survey,” Social Network Analysis and Mining, vol. 12, no. 98, 2022, doi: https://doi.org/10.1007/s13278-022-00924-6.

[14] F. Yasser, S. AbdelGaber AbdelMawgoud, and A. M. Idrees, “Mining Perspectives for News Credibility: The Road to Trust Social Networks,” Handbook of Research on Technologies and Systems for E-Collaboration During Global Crises, 2022, doi: https://doi.org/10.4018/978-1-7998-9640-1.ch017.

[15] F. Yasser, S. AbdelGaber AbdelMawgoud, and A. M. Idrees, “News’ Credibility Detection on Social Media Using Machine Learning Algorithms,” Future Computing & Informatics Journal, vol. 8, no. 1, 2023, doi: https://doi.org/10.54623/fue.fcij.8.1.2.

[16] F. Yasser, S. AbdelGaber AbdelMawgoud, and A. M. Idrees, “A Survey for News Credibility in Social Networks,” International Journal of e-Collaboration (IJeC), vol. 18, no. 1, 2022, doi: https://doi.org/10.4018/IJeC.304378.

[17] A. M. Idrees, F. K. Alsheref, and A. I. B. Elseddawy, “A Proposed Model for Detecting Facebook News’ Credibility,” International Journal of Advanced Computer Science and Applications, 2019, doi: http://doi.org/10.14569/ijacsa.2019.0100743.

[18] A. M. Idrees, M. H. Ibrahim, and N. Y. Hegazy, “A proposed model for predicting stock market behavior based on detecting fake news,” Empowering Science and Mathematics for Global Competitiveness, 2019.

[19] A. Kayode, A. Y., A. A., and O. S., “Multi-Factor Authentication Model for Integrating Iris Recognition into an Automated Teller Machine,” International Journal of Computer Applications, vol. 181, no. 45, pp. 1–8, Mar. 2019, doi: https://doi.org/10.5120/ijca2019918530.

[20] J. Soares and A. N. Gaikwad, "Fingerprint and iris biometric controlled smart banking machine embedded with GSM technology for OTP," 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), Pune, India, 2016, pp. 409-414, doi: https://doi.org/10.1109/ICACDOT.2016.7877618.

[21] J. Soares and A. N. Gaikwad, "A self banking biometric machine with fake detection applied to fingerprint and iris along with GSM technology for OTP," 2016 International Conference on Communication and Signal Processing (ICCSP), Melmaruvathur, India, 2016, pp. 0508-0512, doi: https://doi.org/10.1109/ICCSP.2016.7754189.

[22] M. A. Kassem, N. E. Mekky, and R. M. EL-Awady, “An Enhanced ATM Security System Using Multimodal Biometric Strategy,” International Journal of Electrical & Computer Sciences, vol. 14, no. 04, 2014.

[23] N. Geethanjali and K. Thamaraiselvi, “Feature Level Fusion of Multimodal Biometrics and Two Tier Security in ATM System,” International Journal of Computer Applications, vol. 70, no. 14, pp. 17–23, May 2013, doi: https://doi.org/10.5120/12030-8041.

[24] A. E. Omolara, A. Jantan, O. I. Abiodun, H. Arshad, and N. A. Mohamed, “Fingereye: improvising security and optimizing ATM transaction time based on iris-scan authentication,” International Journal of Electrical and Computer Engineering (IJECE), vol. 9, no. 3, p. 1879, Jun. 2019, doi: https://doi.org/10.11591/ijece.v9i3.pp1879-1886.

[25] K. Marathe and H. Mande, “ATM Security Using Eye and Facial Recognisation,” International Journal of Research in Engineering, IT and Social Sciences, vol. 9, no. Special Issue, 2019.

[26] S. Koteswari, P. John Paul, and S. Indrani, “VC of IRIS Images for ATM Banking,” International Journal of Computer Applications, vol. 48, no. 18, pp. 1–5, Jun. 2012, doi: https://doi.org/10.5120/7445-0198.

[27] Li Ma, Tieniu Tan, Yunhong Wang, and Dexin Zhang, “Personal identification based on iris texture analysis,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 12, pp. 1519–1533, Dec. 2003, doi: https://doi.org/10.1109/tpami.2003.1251145.

[28] M. A. A. Alhamrouni, Iiris recognition by using image processing techniques,” atilim university, 2017.

[29] Chinese Academy of Sciences' Institute of Automation (CASIA) (n.d.). CASIA-IrisV1 (no date) Bit. Available at: http://biometrics.idealtest.org/login.do (Accessed: March 25, 2023).

[30] IIT Delhi Iris Database version 1.0, http://web.iitd.ac.in/~biometrics/Database_Iris.htm.