Computer Systems Science & Engineering
DOI:10.32604/csse.2022.020785
Article

Tech Science Press

Automated Teller Machine Authentication Using Biometric

Shumukh M. Aljuaid* **and Arshiya S. Ansari**

Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al Majma'ah 11952, Saudi Arabia
*Corresponding Author: Shumukh M. Aljuaid. Email: 411203857@s.mu.edu.sa
Received: 08 June 2021; Accepted: 21 July 2021

Abstract: This paper presents a novel method of a secured card-less Automated Teller Machine (ATM) authentication based on the three bio-metrics measures. It would help in the identification and authorization of individuals and would provide robust security enhancement. Moreover, it would assist in providing identification in ways that cannot be impersonated. To the best of our knowledge, this method of Biometric_ fusion way is the first ATM security algorithm that utilizes a fusion of three biometric features of an individual such as Fingerprint, Face, and Retina simultaneously for recognition and authentication. These biometric images have been collected as input data for each module in this system, like a fingerprint, a face, and a retina module. A database is created by converting these images to YIQ color space, which is helpful in normalizing the brightness levels of the image hence mainly (Y component's) luminance. Then, it attempt to enhance Cellular Automata Segmentation has been carried out to segment the particular regions of interest from these database images. After obtaining segmentation results, the featured extraction method is carried out from these critical segments of biometric photos. The Enhanced Discrete Wavelet Transform technique (DWT Mexican Hat Wavelet) was used to extract the features. Fusion of extracted features of all three biometrics features have been used to bring in the multimodal classification approach to get fusion vectors. Once fusion vectors ware formulated, the feature level fusion technique is incorporated based on the extracted feature vectors. These features have been applied to the machine learning algorithm to identify and authorization of multimodal biometrics for ATM security. In the proposed approach, we attempt at useing an enhanced Deep Convolutional Neural Network (DCNN). A hybrid optimization algorithm has been selected based on the effectiveness of the features. The proposed approach results were compared with existing algorithms based on the classification accuracy to prove the effectiveness of our algorithm. Moreover, comparative results of the proposed method stand as a proof of more promising outcomes by combining the three biometric features.

Keywords: ATM security; biometrics; face recognition; fingerprint; fusion technique; hybrid optimization; retina recognition; image segmentation

1 Introduction

All kinds of banking transactions are considered essential in people's lives, making banks deploy ATMs in multiple places to grant users easier access to their services. However, while using an ATM card, they may encounter many problems and difficulties. Some clients forget the PIN or card number while others forget or lose the card itself. Another problem may be frequent thefts and acts of forgery by criminals. All these problems are due to the banks' reliance on the traditional card-based system based on the Personal Identification Number (PIN). Therefore, a solution had to be made to switch to a better method for identification and authorization of ATM card transactions. However, technologies are getting more sophisticated. Also, fraud methods are increasing rapidly. A proposed solution to these problems is to use a system that relies on individual biometrics to reduce those kinds of problems, frauds, and misuse.

Furthermore, the bankers are trying to implement a high-security mechanism to ensure their customers' protection and safety of accounts information. Bankers are more interested in securing buildings, money, automated teller machines, theft, dangers, criminals, and attacks than anything else. While at the same time, criminals tend to find different and varied ways to access customer accounts to withdraw money or conduct bank transactions through hacking their accounts. ATM security presents a strong challenge to the banks, as it is a mechanism through which the customer can obtain money from any place and at any time, so many crimes are associated with it, and the methods used in fraud are various and continuously changing.

1.1 Problem Definition

The traditional ATM card and PIN-based system is a simple and uncomplicated system. But it also makes it easier for fraudulent activities to take place by either obtaining the PIN through a regular shoulder surfing attack, stealing the card, putting on a fake PIN Pad, and many other techniques. Thus, to overcome this issue, one of the most potent ways to support ATM security is the use of biometrics to identify the customer's identity.

One of the most important goals of our project is "*To verify and ensure that the person who is accessing the account is the authorized one through biometrics fusion*." Therefore, we use a biometric verification and authentication method to identify the person (User) with solid security and determine his identity to successful and safe attempt to access the desired banking service.

In this project, three biometrics (Fingerprint, Face, and Retina recognition) were collected by our team for secure ATM banking. As given in the block diagram of the basic steps of the proposed algorithm in Fig. 1, the biometrics-based ATM system scans the live biometric images of the account holder and compares them with the dataset. If the identity is matched by the triple-checking system, it is to authorize the account holder to access the system; otherwise, access would be denied.

1.2 Face Recognition ATM

The idea behind the facial recognition ATM system is to automatically identify the facial image of the individual and verify a distinct features unique to each user to verify authentication. Our proposed method extracts different features of face and relative position of elements for face recognition. The close distance, relative position, and difference between facial images would be calculated using face eigenvalues to find the differences. It depends on the face's structure and the close distance between the mouth, the eye, the nose, chin, etc. It works by drawing continuous lines to the contour of the face, where around more than 80 points can be used to identify the face. These points, which represent a map, are stored in the database.

1.3 Fingerprint Recognition ATM

Fingerprint recognition technology has been widely accepted and used in academics and industrial sectors for authentication purposes. A finger contains protrusions and depression that distinguish each

person from one another with a unique fingerprint that cannot match others. As a result, every person's fingerprint details are distinct.

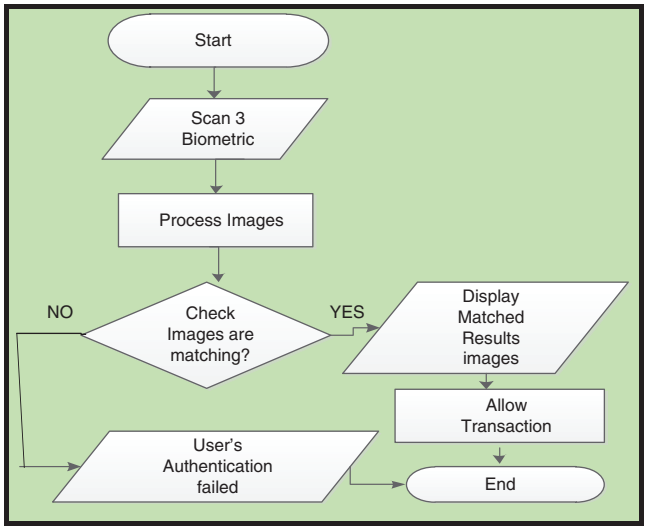

Figure 1: An illustration of Basic steps of Proposed ATM biometrics authentication checking

Here, we are using fingerprint recognition based on finger surface. The fingerprint scanner captures the finger's feeling and focuses only on the end of the bumps and dendrites. Furthermore, it separates the foreground regions from the background regions of the fingerprint image by applying the filter. Thus, it considers and works only with the foreground region to identify the fingerprints.

The proposed algorithm is set to transform the foreground region image in the ridge picture using good segmentation technique, separating the image black and white edge points, and comparing two white points. The algorithm decides matching if the calculation of matching the white points is above 90%.

$$\text{Total matched percentage} = (\text{matched data}/\text{total data}) \times 100 \quad (1)$$

The algorithm's performance can produce variations in the same person's fingerprints due to skin disease or noise while capturing his image at different times.

1.4 Retina Recognition Based ATM

Retina recognition is a biometric technique that relies mainly on the unique vascular patterns found in the retina inside the depth of the human eye. This technique helps in identifying a person's identity. Images need to be captured by a special live digital camera as well as keeping a maximum distance of 30 to 40 centimeters. Appropriate transformation is required to enhance fine vessel lines before running the comparison code. By applying a filter, the vertical edges of the blood vessels of the eye get enhance. The edge field of the retina is created for future comparison. The algorithm takes a match/mismatch decision between two images by converting the images fine vessel-lines patterns into eigenvalues in a binary form then the algorithm tries to identify the difference between two images. The percentage of difference between the two images decides the matching relevance to the person. Blinking off eyelashes can deteriorate the performance of the algorithmatic result. Retina recognition system has been proven to be a very secure biometric security system. This security measurement is used mainly when high security is needed in banking facilities, border patrols, and defense applications.

1.5 The Contribution

At this point, the following query may come up to the reader's mind: What is the benefit of having an ATM system that includes multiple biometrics? The answer to this question can be summed as follows:

- The proposed method is the first authentication and verification method that utilizes ternary biometrics features like Fingerprint, Face, and Retina together.
- Using three types of biometrics in the same algorithm provides more confidentiality and robust security to both the banking system and users' accounts.
- This paper presents a novel method for the combined use of all three biometric identification and authentication for a further secure banking experience.

2 Literature Review

Nowadays, many banks face acts of fraud in banking transactions; therefore, many researchers have worked and continue on working on ATM security measures to assist banks in establishing systems and algorithms that solve security vulnerabilities in the traditional ATM system. In addition, they are working tirelessly to increase protective methods by adding biometrics in the ATM system to identify the authorized person's identity.

In already existing biometric ATM systems, one type of features is usually neither efficient nor sufficient to predict the right individual, mainly if the gathered pictures are taken in different environmental conditions like enlightenment, darker, and impediment conditions. Therefore, most analysts focus on multimodal biometric recognition to build a recognizable proof and provide additional security. The exploration of PC-based programmed biometric recognition began during the 1960s [1]. Though face recognition is presently growing at a great pace, there are many issues to be addressed. Therefore, there is a great potential for face recognition methods to be improved. The inspiration driving biometrics research is the identification of the approved individual for security reasons using facial points, lines, regions, and textures.

Manish et al. in the paper [2], suggested the use of fingerprints and face recognition. After logging in, the verification code is later sent to the mobile phone of the bank's customer as a one-time code only. If someone enters an incorrect code, that person's face is to be saved and emailed to help identify criminals. Chowdhury et al. in paper [3] have presented the work based on multiple users' emotions. They have also used the CNN (Convolutional Neural Network) model to implement a facial recognition library and validated results based on feelings of "Happiness." However, the results were not accurate enough, and they ran into difficulties when something changed in the person's expression, and the accuracy rate is also proved to be insufficient. Kumar et al. the work in [4] has presented the Arduino ATM security system based on Haar's algorithm to recognize the face of the bank's customers. Still, they found that it needed more expansion and better implementation to produce an accurate result. Finally, Mohite et al. [5] implemented fingerprint and facial recognition ATM security using the CNN model by giving four chances to verify matching. Although the system is based on two biometrics, the person's identification was insufficient, and the results were providing little to no accuracy.

Gabotshajwe [6] suggested combining three facial recognition methods: linear discriminant analysis (LDA), principal component analysis (PCA), and local binary patterns (LBP). The three methods were applied to various factors to ensure the accuracy of the recognition. Regarding the face, it was concluded that the best of them was the local binary pattern which had poor accuracy for characterizing the user's face. Still, the accuracy result achieved by it is better than [7]. The LBP accuracy rate in facial recognition was shallow and insufficient. Ranjitham et al. in paper [8], suggested combining biometrics with a face and fingerprint for user identification and verification using a Raspberry pi micro-controller to search in the database. And they suggested integrating artificial intelligence for easier identification of

users. Jebaline et al. in paper [9], presented a biometrics ATM system named Blowfish algorithm, where it takes a photo of a fingerprint, extracts the existing features, and compares it with the database in an encrypted way before sending it to the server to ensure safety. In paper [10], Sunehra constructed a fingerprint recognition ATM system prototype, where he used a PIC16F877A micro-controller and wrote the system using C. The system enabled the identification of the user successfully. In paper [11], Murugesh proposed an ATM system based on a fingerprint, phone number, and PIN, which is stored in a database to log in to the system later. The server initiates by sending a verification code to the user's phone to verify authentication. In this system, the researcher used encryption for OTP and PIN encryption. He made use of steganography technology to send the image to the server to compare stored data in the database to obliterate any chance of cyber attacks. But, it did not solve the problem of forgetting the PIN.

Given the large number of crimes in Nigeria related to the traditional ATM system, Onyesolu et al. in the paper [12] has established a fingerprint-based system to enhance security and reduce frauds. They relied on OOADM (Object-Oriented Analysis and Design Methodology) and SSADM (Structural System Analysis and Design Methodology) to obtain results and a robust fingerprint authentication model for an ATM system. Hence, they proved that biometrics help in reducing crime. A research paper [13] suggested replacing the traditional system with a biometric system to increase ATM security and use fingerprints to identify the user in an eased process. They designed the system for fingerprint recognition and implemented it on Altera and Xilinx devices using Field Programmable Gate Array (FPGA). They compared the results with the throughput and the slices on various devices. In the paper [14], they suggested facial recognition technology with a pin, where the face was placed as a key to complete any desired operation. They have also used the Radio-Frequency Identification Tags (RFID TAG) instead of the ATM card. If they match, a pin is sent to the user to complete the process. It was concluded that PCA-based facial recognition is more robust and accurate because it takes up little storage space and little computation time. However, this system is still under development. And they did not prove the 100% accuracy of the system.

Mahendr & et al. in paper [15], have suggested Face Recognition Software (FRS) for face recognition and verification using a face detector, face ID, and Eyelashes. This data is to be preserved in the database for use upon matching. Thus, due to the increasing number of fraud and theft operations in the traditional ATM operations to enter the card and the password, banks are forced to change and develop the security methods used by introducing biometric technology. Therefore Fernandes [16] suggested a security system using the embedded system, and he concluded that the fingerprint would reduce theft and save more time than the card. Shetiya et al. [17] presented iris recognition technology for ATM security. They proposed the Hough Transform method for ATM security. The technique divides the iris of the eye features, represents the dimensions, and then searches for the features that distinguish each person from the other. The system successfully identified people with 94% accuracy. The new images were compared with the images in the database. The code was implemented using MATLAB. Joshi et al. in paper [18] have used facial recognition technology with a card to provide security to ATMs and users. The Histogram of Gradients (HOG) algorithm was used where the customer was asked to insert the card, and then the system would recognize the face, and upon matching, the process would initiate automatically. He concluded that ATMs can validate 16,000 points on a user's image, provide security to banks, and increase their status.

Similarly, the use of iris recognition technology has succeeded in many fields and sectors. Therefore, Vincy et al. in paper [19], have advised that banks to apply this technology because of its effectiveness and success in identifying the client. Researchers successfully experimented with iris recognition, using it with the 1d Log-Gabor filter. The experiment was practical as they segmented the iris and proposed to further develop it by applying a system that is also capable of detecting eyelashes and eyelids. So when connected to an ATM with iris recognition, it is more secure than a PIN and easier to use. David et al., in paper [20], presented the iris segmentation, then compared the image to the database, and then found the dimensions to obtain the identical image. The hamming separation was used to get the bits. Dogman's

algorithm succeeded in recognizing the iris of the eye, and the Chinese Academy of Sciences' Institute of Automation (CASIA) iris database also succeeded in segmentation, with a success rate of 83% for the user system, so the problem was in the upper and lower eyelids and near the eyelashes. In paper [21] Imam et al. found that the traditional ATM system had many problems in terms of security and a large number of bank accounts for a single user and his multiple PINs, so they designed a system based on a GSM fingerprint. They used an optical scanner to take an image of the fingerprint and analyze it. Upon verification, an OTP is sent to the user to log into his account and conduct banking transactions.

A few techniques and methods have been recommended in face recognition research. They can be partitioned into four approaches like local, hybrid, holistic, and deep learning based on the extraction and classification methods [22]. There is a 3D model method that offers an excellent portrayal of the face shape for a good differentiation between people; they are regularly not appropriate for constant applications since they require costly and complex computations and an explicit number of sensors. The framework presented in [23] depends on image processing techniques like filtering and histogram calculations needing less computational cost than existing frameworks. The work had a calming accuracy up to 96%. The work presented in [24] uses biometric recognition like fingerprints, face recognition to recognize the individual. At this point, Internet of Things has been utilized to upgrade the security of ATM. In [25], the PINs are supplanted by haphazardly made OTP that are sent through the IoT. The client will be permitted to proceed with the transaction after biometric and OTP pin validation. The record would be hindered in case of three back-to-back wrong endeavors. If there should be an occurrence of any dubious action is identified through the vibration sensor, it brings about the end of ATM entryways followed by delivering of the blacking out gas and cautioning the environmental factors. This will get the culprit involved with the wrongdoing and keep the extortion from occurring.

To deal with multimodal biometric feature recognition, feature_fusion has become an essential research aspect [26], because fusing different features provides complementary information. The technique introduced multimodal biometric model which incorporates the perspectives of face, ear pictures portrayal, and human grouping. Subsequently, a proficient system, in light of a crossbreed model of learning distance metric (LDM), directed acyclic graph (DAG), and support vector machine (SVM), has been proposed for multimodal biometric recognition. Distance metric learning is utilized to look for a square network from the preparing set. Plus, SVM is used to accomplish preferable speculation capacity over conventional classifiers like K-Nearest Neighbor (KNN) utilizing Euclidean distance. Broad trials have been led on the open and accessible face and ear datasets and their combinations which are built as multimodal datasets [27].

3 Proposed Method

3.1 The Block Diagram of Biometric_Fusion

The section presents the critical functionalities of the proposed method shown in Fig. 2.

3.1.1 The Proposed Biometric_Fusion Method

As shown in Fig. 2, the proposed Biometric_fusion method uses biometrics to compare two input images of the account holder to check if the camera has captured photos that match the dataset image. The proposed algorithm firstly resizes the pictures to 256 × 256 dimensions to reduce the number of iterations and ease the execution process. Then, it applies the Prewitt edge detection filter, which defines & clears the edges in the edge detection step. Prewitt filter uses a gradient-centered operative mechanism. It calculates and estimates the gradients of image intensity occupation for image edge detection. Prewitt operator works on the image pixel's normal vector or the equivalent gradient vector. After applying a filter, an enhanced Cellular Automata Segmentation procedure would be used on input filtered images to make image segments.

Here, the Cellular Automata Segmentation process aims to examine the image and reduce the color difference of pixels in a particular region of the image to generate a soft, segmented image.

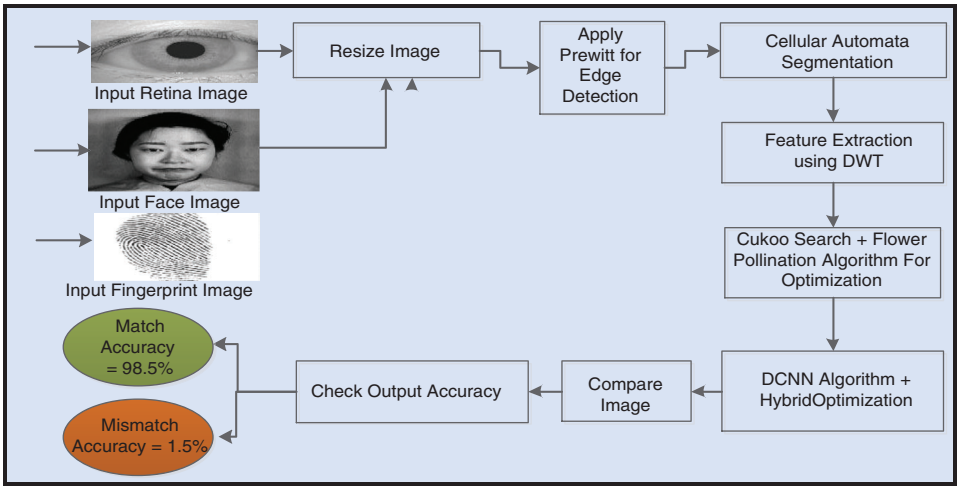

Figure 2: Block diagram of proposed method biometric _fusion

The next step is the feature extraction procedure. It is imperative in image processing to identify the uniqueness of an image. 'Mexican Hat Wavelet' has been used here to extract the unique feature vectors of images. It is a negative second derivative function of the Gaussian function. In the following step, we have applied image optimization techniques. Like Cuckoo search and Flower pollination algorithm. (*Discussed next*).

After getting optimized images from the above step, the next step is to send them to CNN to reduce the training time consumption. The results of the two images are compared to see if the images are matching or not. Deep Convolution Neural Network (DCNN) algorithm has been used to classify the image. The enhancement in DCNN will be done by integrating hybrid optimization algorithms to improve the identification of biometrics to a greater extend. (*Discussed later*). The final step compares the images and checks the accuracy to classify match or mismatch percentage based on its accuracy. The intermediate processing outputs of the proposed method are shown in Figs. 3A–3C.

3.1.2 Cuckoo Search Algorithm and Flower Pollination Algorithm

Cuckoo search has been used to increase efficiency, accuracy, convergence rate and decrease training time as it removes the redundant attributes from the given datasets.

Here are some parameters used in explaining this step. Now inputs for this step are the feature extracted images. Above is an example case. Let Out1 and Out2 are the optimized images on which the Cuckoo search algorithm with flower pollination algorithm is used to get the best-optimized picture. As the inputs applied for this step are the feature extracted images, then let it be, 'Fea_Img1' and 'Fea_Img2'respectively.

Bestnest1, Fmax1, Time1, Best1, Fmin1 are some other parameters used in the Cuckoo search algorithm. The bestnest1 is the parameter that indicates the best minimum value of the fitness function obtained from the Cuckoo search algorithm. Fmax1 is the parameter that indicates the maximum fitness value obtained from the cuckoo search. Time1 parameter is the time taken to execute the fitness value. Best1 is the parameter obtained from flower pollination to find the best lowest value using the fitness function. Fmin1 is the parameter obtained from flower pollination, which finds the lowest value from the fitness function.

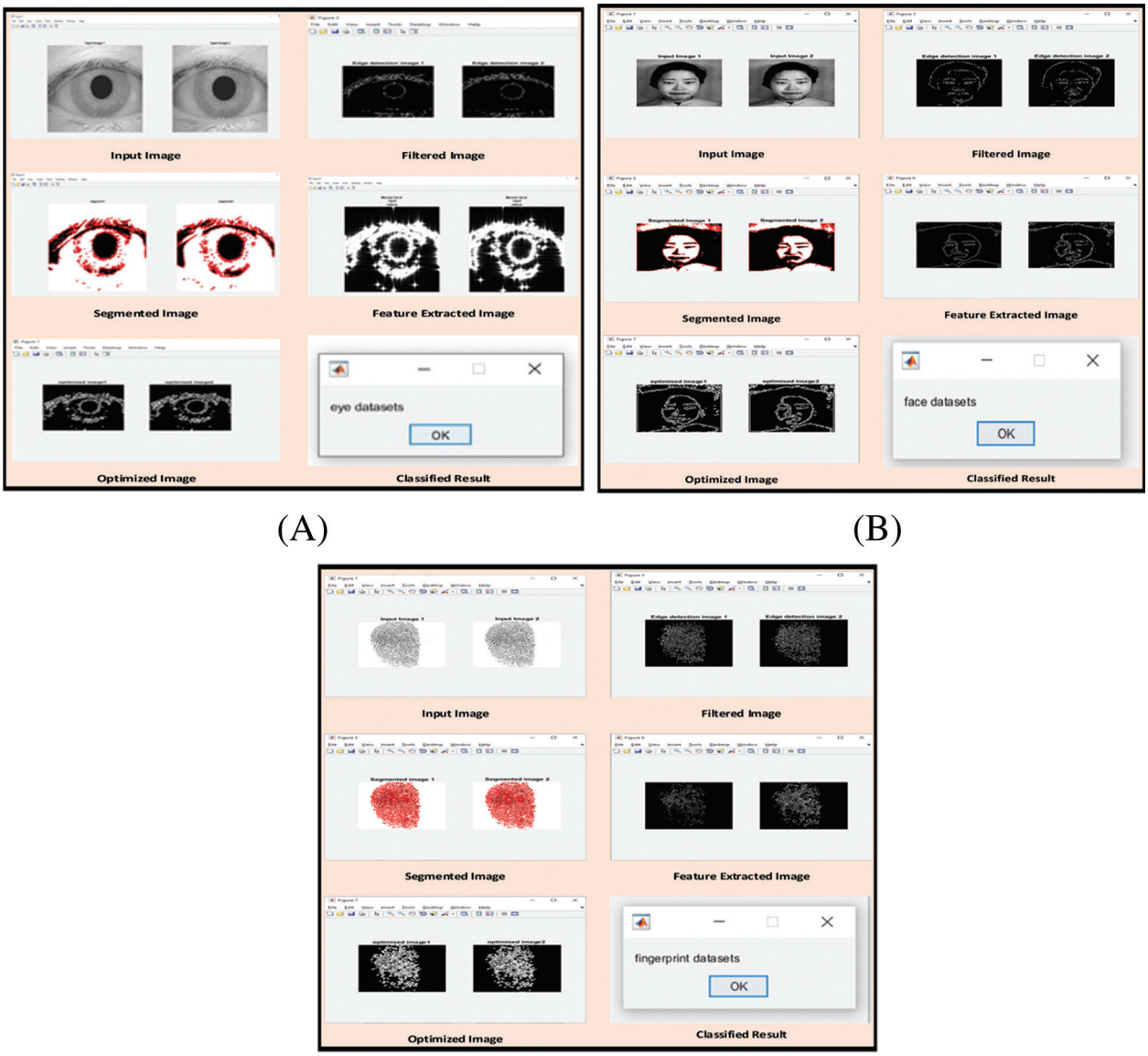

Figure 3: (A) Proposed algorithm's working steps for retina recognition (B) Proposed algorithm's working steps for face recognition (C) Proposed algorithm's working steps for fingerprint recognition

Here, the Flower pollination optimization method with Cuckoo search has been sensibly chosen because it has the capability of best optimization and convergence compared to other optimization methods. As shown in Fig. 4 the Cuckoo search algorithm and flower pollination algorithm are shown as being used in combination to get the best-optimized image.

Overall both algorithms processing are the same. The only difference is using Cuckoo search; we find the minimum fitness value. However, the flower pollination algorithm gives a maximum fitness value. Furthermore, in the Cuckoo search algorithm, time is essential, and it is an input, whereas, in the flower pollination algorithm, we give the number of iterations.

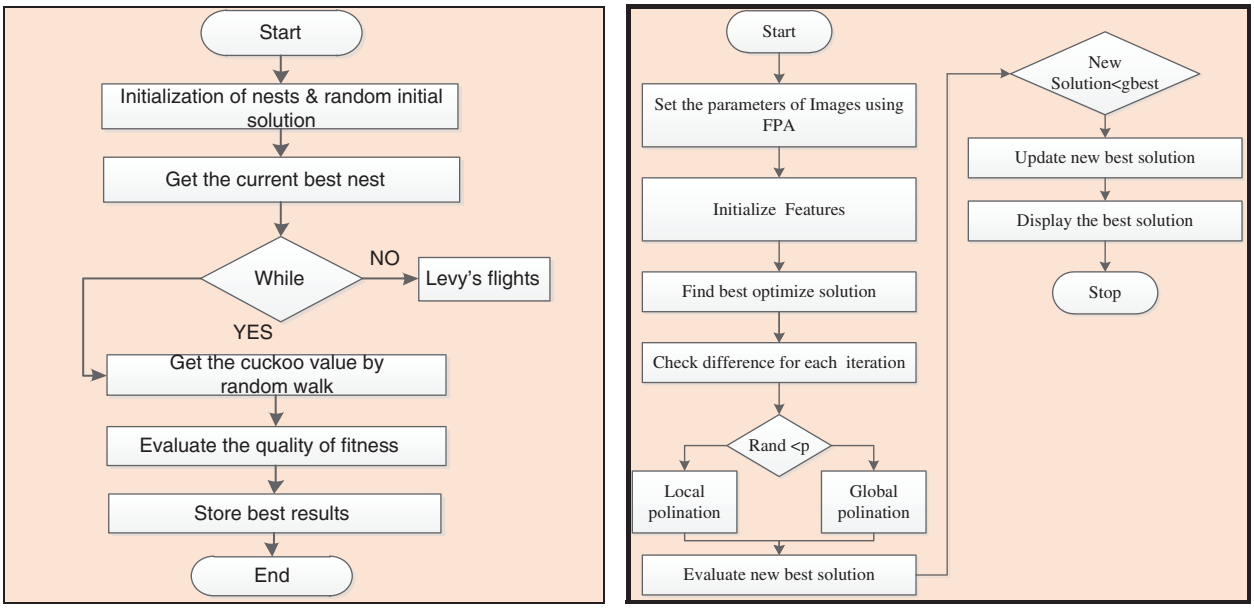

Figure 4: Flowchart of cuckoo search algorithm and flowchart for flower pollination algorithm (FPA) steps

3.1.3 CNN Classification

CNN classification divides the images into two categories 'training images' and 'testing images.' Training images contain 70% of datasets, and testing images have 30% of data sets to determine accuracy, sensitivity, and specificity. Here, using CNN for recognition, classifications, and detections to categories of the biometric imagery. CNN's first layer takes an input image and classifies it into three categories: Face, Fingerprints, and Retina images. The Face, Retina, and Fingerprints images are in the form of a pixel array. CNN convolution layer two is used to extract input image features without disturbing pixel relationships depending on the resolution. The image's pixel array matrix then feeds to the Fully Connected (FC) layer and Rectified Linear Unit (ReLU) layer; and is used to produce non-linearity in the second layer. The last layer is the Softmax layer, which is used for layer construction. Without this layer, we cannot classify the dataset. The image may contain positive or negative values from 0 to 255 or may have noise, but Softmax converts it into binaries. It converts all real values to 0 and 1.

In CNN, we divide the images into two categories training data images and testing data images. First, there is a need to train and examine all the images, including the training images folder. In the parameter called 'Data', we store testing images. 'Ext' parameter indicates what type of image format we have used. Hence, as all our images are in '.tiff' format, so we have mentioned '.tiff' in that parameter, the 'Imgs' parameter is used to store all the training images. In Layer classification, 'inputSize' is used as a parameter that indicates the 1-dimensional image of size 256×256. Since we have three different datasets (i.e., eye, face, and fingerprint), the number of classes/categories would be stored in 'NumClasses'. 'NumTrainFiles' this parameter should be equal to the number of total images in each dataset or less than that. Then the results of the two images are compared to see if the images are matching or not. 'Ypred' is the parameter where we compare testing images and training images to determine accuracy, sensitivity, specificity.

In the result analysis section, to prove the effectiveness of the proposed algorithm, the obtained image results are compared with existing algorithms based on the classification accuracy. MATLAB R2018-b with 16 GB RAM is used for the implementation of this project.

3.2 The Proposed Algorithm

Following is the pseudo proposed *Biometric_ fusion* algorithm

---

Algorithm: Biometric_ fusion

Input: Image of training data set, images of testing data set of all three biometrics.

Output: classified image with high accuracy.

Begin

Repeat for each biometric type images

Begin

1. Image1 and Image2 are the input images taken from the training and testing dataset to compare if the selected images are the same.
2. Resize input images in size 256 * 256 dimension.
3. Apply the 'Prewitt' filter.
4. Apply Cellular Automata technique for the segmentation.
5. Apply 'Mexican Hat Wavelet.'
6. Apply Cuckoo search algorithm with Flower pollination algorithm to get the best-optimized image.
7. Compare results of 2 images to check whether they match or not apply CNN classification and check accuracy.

end

End

---

4 Experiment and Result Analysis

4.1 Biometrics (Face, Fingerprint and Retina Recognition) Test Results

Here, TIFF and JPEG images in the dataset were used for experimentation. For simplicity of explanation, we take Fig. 5 to Fig. 13 sequentially to show the output results of the proposed method. All figures; Fig. 5A to Fig. 13A show selected input images from the dataset and training data set of all three biometrics. Fig. 5B to Fig. 13B show output results of the proposed method, whether the input images match with the dataset or not. All figures Fig. 5C to Fig. 13C are showing Training Progress Graphs. Validation accuracy (classification) progress starts from 0 up to 100% within 8 to 9 min. Validation accuracy at 100% means training progress is made correctly—these figures showing the time cycle are required for classification and processing. All figures Fig. 5D to Fig. 13D indicate the Likelihood Ratios LR of our method results statistics. They show the accuracy, sensitivity, specificity, and precision percentage ratio to decide match and mismatch. (*Explained soon*). Furthermore, if there is a match between the input and the already stored dataset, the specificity value reaches around 90% to 100%. If there is a mismatch between those pictures, it gets reduced. It depends on the image structure, as shown in Fig. 7D. In Fig. 8D, two same-person fingerprints match, and then the results produced are; classification accuracy at 98.522%, sensitivity at 100%, specificity at 97.08%, and precision at 97.08%.

Similarly, different person mismatch giving sharp readings reduction in sensitivity 66.66% and slightly low accuracy and specificity as per image structure. Precision matric was used to check how closely the two measure results are. Match and mismatch images comparison considered the precision value also, but the leading judgment depended mainly on sensitivity & specificity results. As shown in Fig. 8D, two same-person fingerprints pictures match, and then precision of 97.08% is received and Fig. 10D for the

mismatched picture it sharply reduced to 48.06%. Validation metrics parameters used to find the quality of a segmented image has been explained with the help of the following example. Let us assume that A and B are the binary images under consideration. They needs to be converted into Logical images if they are UNIT 8 (0,255) images. And let us assume that A is the original image, and B is the segmented image. Then by standard formula, in Matlab validation metrics parameters are given by the following,

TP = length (Find ((A + B) == 2), it will find the total number of pixels correctly segmented as Foreground.

FP = length (Find ((A – B) == −1), it will find the total number of pixels falsely segmented as Foreground.

TN = length (Find ((A + B) == 0), it will find the total number of pixels correctly segmented as Background.

FN = length (Find ((A – B) == 1), it will find the total number of pixels falsely segmented as Background.

Sensitivity gives you true-positive results, whereas specificity gives true-negative results. By combining both results, you get the accuracy results for the image. For measuring differentiation between picture match and picture mismatch basis, we would use the sensitivity & specificity measure. Accuracy is just the classification correctness. It depends on classification sensitivity and specificity results. The standard formula to get the above parameters are given below.

$$\text{Accuracy} = (\text{tp} + \text{tn})/(\text{tp} + \text{fp} + \text{tn} + \text{fn}) * 100 \quad (2)$$

$$\text{Recall/Sensitivity} = \text{tp.}/(\text{tp} + \text{fn}) * 100 \quad (3)$$

$$\text{Specificity} = \text{tn.}/(\text{tn} + \text{fp}) * 100 \quad (4)$$

$$\text{Precision} = \text{tp}/(\text{tp} + \text{fp}) * 100 \quad (5)$$

$$\text{False positive ratio (FPR)} = \text{fp.}/(\text{tn} + \text{fp}) \quad (6)$$

where,

tp = Number of true positive case result assessment (Pixel correctly segmented as Foreground)

fp = Number of false positive case result assessment (Pixel correctly segmented as Background)

tn = Number of all negative case result assessment (Pixel correctly segmented as Background)

fn = Number of false negative case result assessment (Pixel falsely segmented as background)

Here we have also used Structure Similarity Index Measure (SSIM), the latest measure to find image matched or mismatched, here it was considered for all the three categories for male and female biometrics eye, face, and fingerprints. Peak Signal to Noise Ratio (PSNR) was also utilized for processed image quality assessment calculation. It compares your main dataset image and compresses the image to check how close they are to a match and its quality. The reconstruction results are considered accurate if the resultant readings of SSIM is from 0% to 100% SSIM comparison which makes it necessary to check the quality of the resulting image if a use of any transform or compression method on images is planned. As shown in Fig. 8A and Fig. 11A PSNR value for the same person's picture is calculated as 0. In contrast, if PSNR is higher, it matches to around 12.89 with a different person's pictures. While in Fig. 6, Fig. 8, and Fig. 10, the SSIM value for the same person result is 100, and for another person, the result is in lower values 23.03,42.03 and 25.47 with different pictures as shown in Fig. 7A, Fig. 9A and Fig. 13A respectively.

4.1.1 Face Identification Testing Results

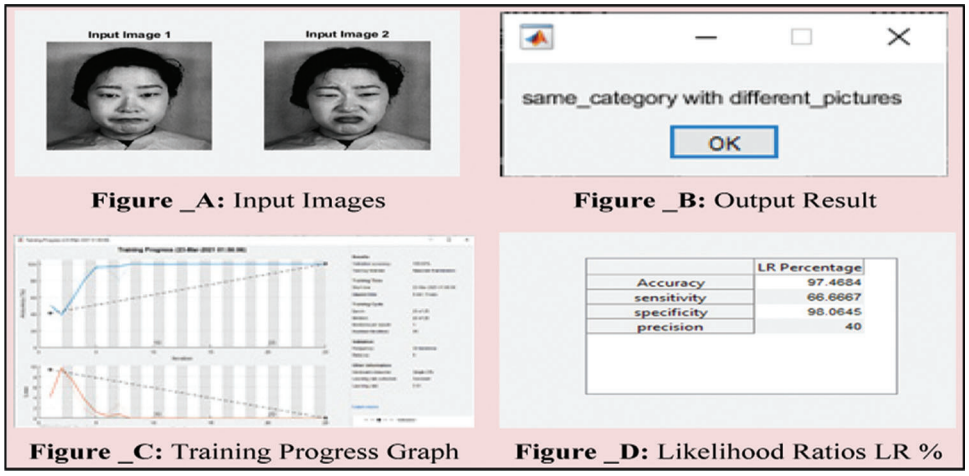

Figure 5: Case 1: Same person with a different expression, PSNR = 22.8954, SSIM = 55.3004

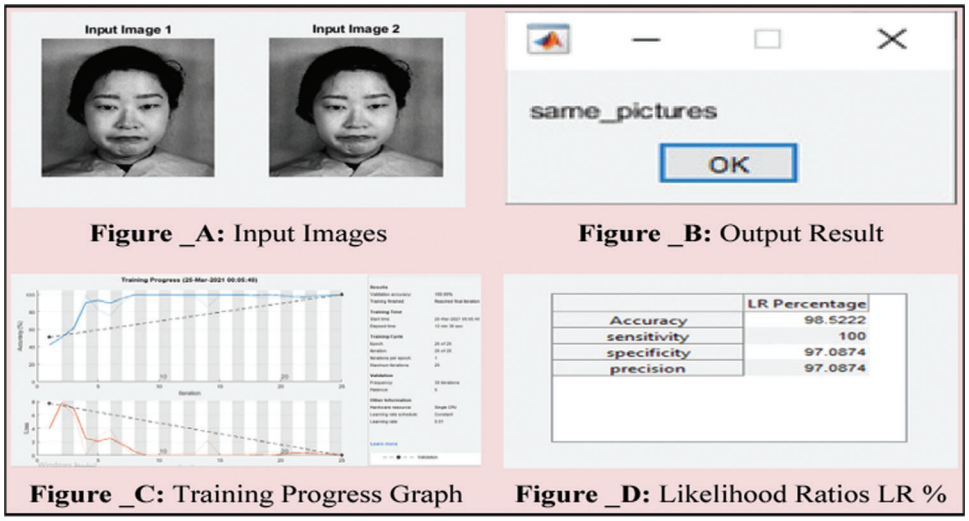

Figure 6: Case 2: Same person picture, PSNR = 0, SSIM = 100

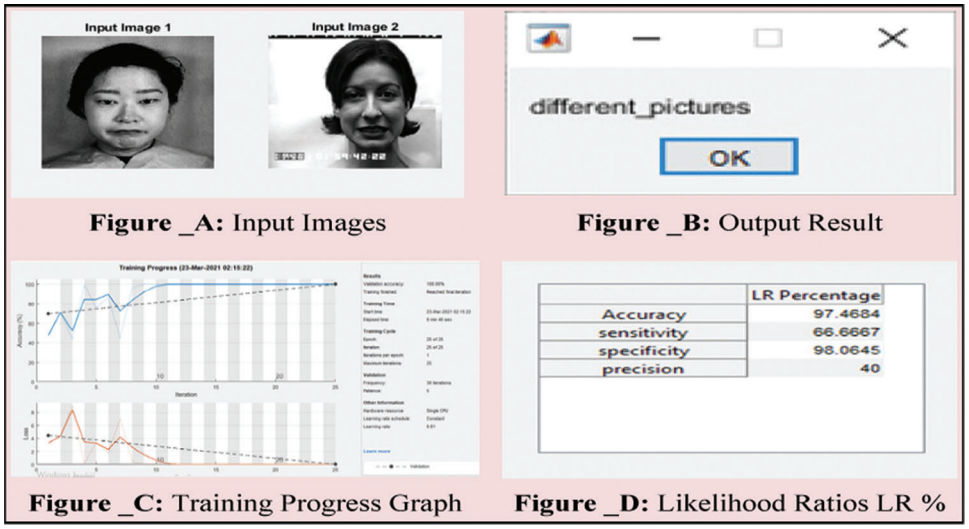

Figure 7: Case 3: Different person with a mismatch, PSNR = 12.8940, SSIM = 23.0349

4.1.2 Fingerprint Identification Testing Results

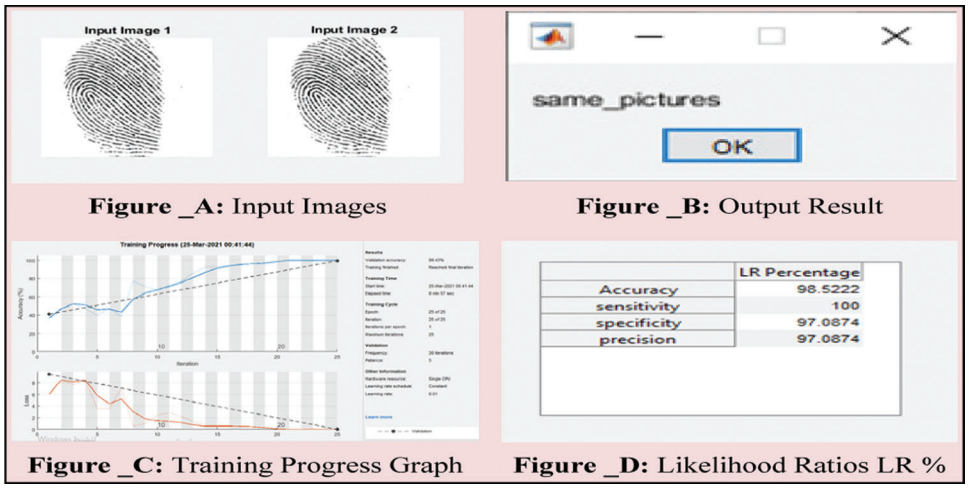

Figure 8: Case 1: Same person fingerprint with the same picture, PSNR = 0, SSIM = 100

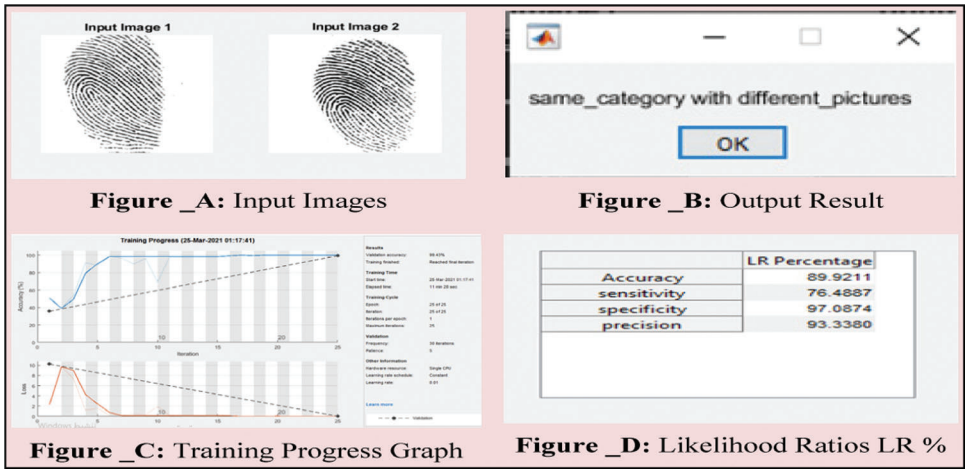

Figure 9: Case 2: Same person fingerprint with a different picture, PSNR = 12.9198, SSIM = 42.0315

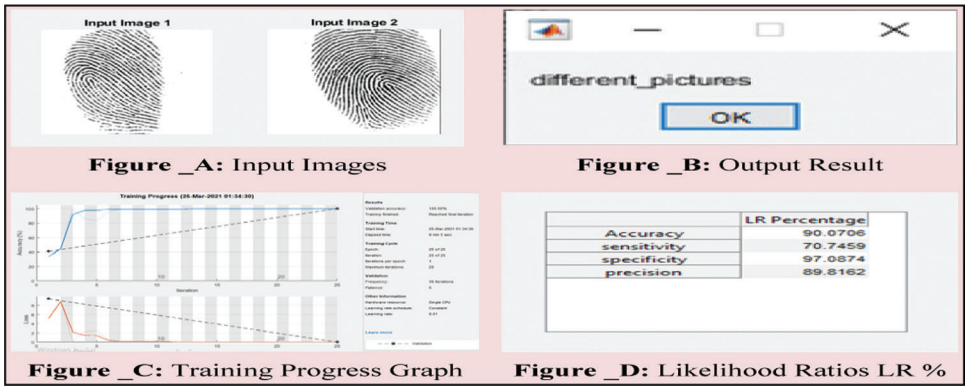

Figure 10: Case 3: Different person fingerprint with a different picture, PSNR = 10.9409, SSIM = 26.4587

4.1.3 Retina Result Testing

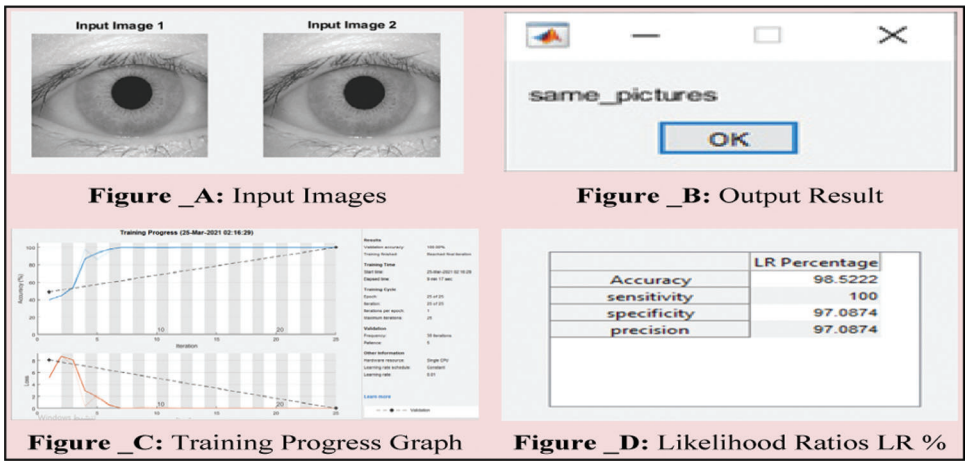

Figure 11: Case 1: Same person with the same picture, PSNR = 0, SSIM = 100

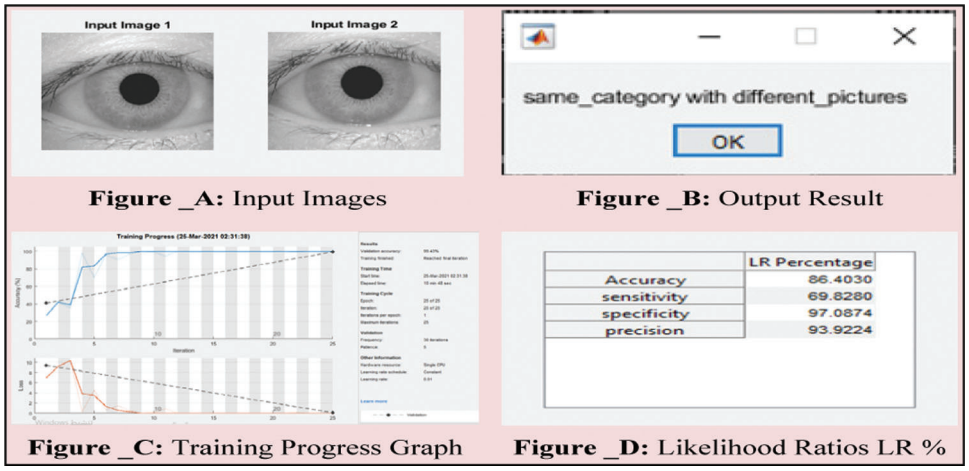

Figure 12: Case 2: Same person with a different picture, PSNR = 20.0325, SSIM = 46.3618

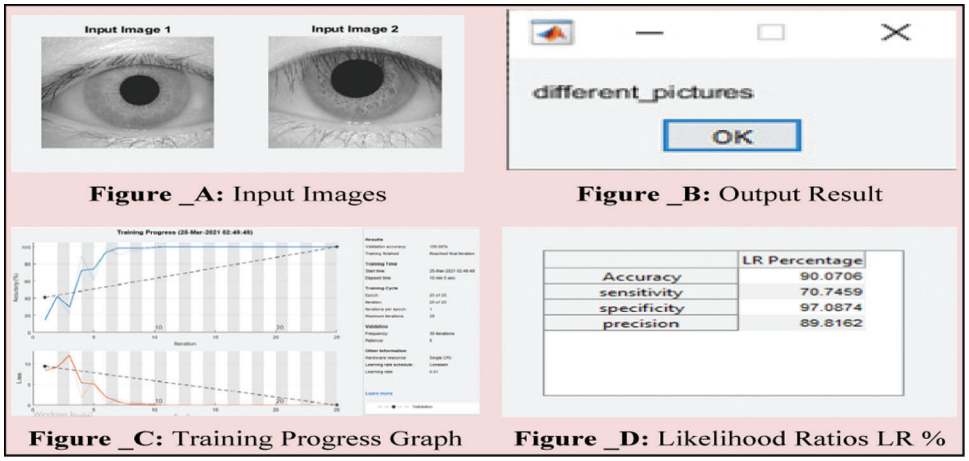

Figure 13: Case 3: Different person with a different picture, PSNR = 16.8105, SSIM = 25.4793

4.2 Accuracy Comparison of Proposed Method with Already Existing Methods

Tab. 1 shows the proposed method's promising and better results as compared to other existing ones. Other forms of reading are showing accuracy between 67% to 96%, whereas our results accuracy has increased substantially as the rate of accuracy has reached up to 98.5%, as shown in Fig. 11D.

Table 1: Accuracy results in comparison between the proposed method and existed method

Proposed method & existed method reference	Biometrics used	Evaluated results accuracy
Proposed Method	Face, Fingerprints & Retina	98.5%
Method [3]	Face only	67%
Method [4]	Face only	95%
Method [5]	Face & Fingerprints only	70%
Method [6]	Face only	76%, 96%
Method [7]	Face only	72.24%
Method [28]	Face only	96%
Method [29]	Finger only	94%

5 Conclusion

The Literature review and our survey-based study have ultimately concluded that the use of biometrics in ATM could be quite beneficial. It would make ATM banking transactions safer and faster for completing the transaction. Literature review revealed that all researchers share the same opinion about biometric ATM being very secure to reduce crimes and threats associated with ATM card. The proposed novel ternary biometrics fusion with current ATM methods proved more promising authentication results using the Prewitt filter, Cellular Automata Segmentation, and DWT Mexican Hat Wavelet transform. Our proposed system has succeeded in identifying authorized person's biometric images based on Specificity, Sensitivity Precision, Accuracy, PSNR, and SSIM observation readings, where the accuracy match reached 98.5%, which is the highest rate compared to most of the previous works [3,29].

Funding Statement: The authors may receive funding for this study after acceptance from Majma'ah University research deanship.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Z. Sun, Q. Li, Y. Liu and Y. Zhu, "Opportunities and challenges for biometrics," in *China's e-Science Blue Book 2020,* Springer, Singapore, pp. 101–125, 2021.

[2] C. M. Manish, N. Chirag, H. R. Praveen, M. J. Darshan and D. K. Vali, "Card-less ATM transaction using biometric and face recognition: A review," *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* vol. 8, no. VII, pp. 1493–1498, 2020.

[3] A. I. Chowdhury, M. M. Shahriar, A. Islam, E. Ahmed, A. Karim *et al.,* "An automated system in ATM booth using face encoding and emotion recognition process," in *Int. Conf. on Image Processing and Machine Vision (IPMV)*, New York, United States, pp. 1–10, 2020.

[4] D. A. Kumar, B. Iniyan, M. A. Askar, A. Ajay and R. Ambika, "Face recognition-based new generation ATM machine," in *Int. Conf. on Advanced Computing & Communication Systems (ICACCS)*, Coimbatore, India, pp. 938–943, 2019.

[5] A. Mohite, S. Gamare, K. More and N. Patil, "Deep learning-based card-less ATM using fingerprint and face recognition techniques," *International Research Journal of Multidisciplinary Technovation (IRJMT),* vol. 6, no. 3, pp. 3504–3509, 2019.

[6] E. Gabotshajwe, "A critical evaluation of current published face recognition systems research aimed at improving security for ATM transactions," *University of Sunderland,* vol. 8, pp. 7–11, 2019.

[7] E. Derman, Y. K. Gecici and A. A. Salah, "Short term face recognition for automatic teller machine (ATM) users," in *Int. Conf. on Electronics, Computer and Computation (ICECCO)*, Ankara, Turkey, pp. 111–114, 2013.

[8] G. Ranjitham, S. Manoharan, V. Murugesan and S. S. Ravi, "Face recognition and fingerprint-based new generation ATM," *International Journal of Innovative Science and Research Technology,* vol. 3, no. 3, pp. 749–752, 2018.

[9] G. R. Jebaline and S. Gomathi, "A novel method to enhance the security of ATM using biometrics," in *Int. Conf. on Circuits, Power and Computing Technologies (ICCPCT)*, pp. 1–4, 2015.

[10] D. Sunehra, "Fingerprint-based biometric ATM authentication system," *International Journal of Engineering Inventions,* vol. 3, no. 11, pp. 22–28, 2014.

[11] R. Murugesh, "Advanced biometric ATM machine with AES 256 and steganography implementation," in *Int. Conf. on Advanced Computing (ICoAC)*, Chennai, India, pp. 1–4, 2012.

[12] M. O. Onyesolu, M. Odoh, A. O. Akanwa and V. C. Nwasor, "Robust authentication model for ATM: A biometric strategy measure for enhancing e-banking security in Nigeria," *International Journal of Advanced Research in Computer Science,* vol. 3, no. 5, pp. 164–169, 2012.

[13] N. Ahmad, A. A. M. Rifen and M. H. Abd Wahab, "AES Card-less automatic teller machine (ATM) biometric security system design using FPGA implementation," *IOP Conference Series: Materials Science and Engineering*, Melaka, Malaysia, vol. 160, no. 1, pp. 1–10, 2016.

[14] R. Kishore, S. Suriya and K. V. Vivek, "Enhanced security for ATM machine with OTP and facial recognition features," *International Research Journal of Multidisciplinary Technovation (IRJMT)*, vol. 1, no. 2, pp. 106–110, 2019.

[15] G. Mahendar and M. Batta, "Enhanced security in ATM by iris and face recognition authentication," *International Journal of Scientific Research & Engineering Trends,* vol. 6, no. 3, pp. 1074–1076, 2020.

[16] A. Fernandes, "Biometric ATM," *International Journal for Research in Applied Science & Engineering Technology (IJRASET),* vol. 8, no. VI, pp. 2457–2459, 2020.

[17] P. Shetiya, M. Mascarenhas and M. Deshmukh, "ATM security system using iris recognition by image processing," *International Journal of Engineering Research & Technology (IJERT),* vol. 9, no. 7, pp. 999–1002, 2020.

[18] S. S. Joshi, "Face recognition system with HOG in ATMs," *International Research Journal of Multidisciplinary Technovation (IRJMT),* vol. 6, no. 6, pp. 2134–2136, 2019.

[19] A. D. Vincy and S. Sathana, "Recognition technique for ATM based on iris technology," *International Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 11, pp. 1–5, 2019.

[20] S. David, G. Sharma, A. J. Baruah and S. Sharma, "ATM using biometrics (iris)," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 8, no. 4, pp. 1754–1758, 2019.

[21] M. Y. Imam, N. Jannat and G. S. Khan, "Multi-banking automatic teller machine transaction system by utilizing GSM and biometric identification with one single touch," *International Journal of Advanced Engineering and Technology,* vol. 3, no. 3, pp. 90–94, 2019.

[22] H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong *et al.,* "Cosface: Large margin cosine loss for deep face recognition," in *Proc. IEEE*, United States, pp. 5265–5274, 2018.

[23] I. Adjabi, A. Ouahabi, A. Benzaoui and S. Jacques, "Multi-block color-binarized statistical images for single-sample face recognition," *Sensors,* vol. 21, no. 3, pp. 1–22, 2021.

[24] C. Bhuvaneswari, T. Malini, A. Giri and S. Mahato, "Biometric and IOT technology-based safety transactions in ATM," in *Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, vol. 1, pp. 949–952, 2021.

[25] M. N. Kumar, S. Raghul, K. N. Prasad and P. N. Kumar, "Biometrically secured ATM vigilance system," in *Int. Conf. on Advanced Computing and Communication Systems (ICACCS)*, Coimbatore, India, vol. 1, pp. 919–922, 2021.

[26] E. E. Hansley, M. P. Segundo and S. Sarkar, "Employing fusion of learned and handcrafted features for unconstrained ear recognition," *IET Biometrics,* vol. 7, no. 3, pp. 215–223, 2018.

[27] I. Omara, A. Hagag, S. Chaib, G. Ma, F. E. Abd El-Samie *et al.,* "a hybrid model combining learning distance metric and DAG support vector machine for multimodal biometric recognition," *IEEE Access,* vol. 9, pp. 4784–4796, 2021.

[28] K. J. Peter, G. G. S. Glory, S. Arguman, G. Nagarajan, V. S. Devi *et al.,* "Improving ATM security via face recognition," in *Int. Conf. on Electronics Computer Technology*, Kanyakumari, India, vol. 6, pp. 373–376, 2011.

[29] O. K. Afriyie and V. Arkorful, "Enhancing security of automated teller machines using biometric authentication: A case of a Sub-saharan university," *Information and Knowledge Management,* vol. 9, no. 7, pp. 7–22, 2019.