Wasit Journal for Pure Science

Journal Homepage: https://wjps.uowasit.edu.iq/index.php/wjps/index
e-ISSN: 2790-5241 p-ISSN: 2790-5233

Enhancement of E-Banking System in Iraq by web application-based authentication system using face recognition

Mareim Mahmoud Jameil AL-Aadamy[1], Dr. Mohammed Khodayer Hassan AL-Dulaimi[2]

[1]First Author Affiliation,
Iraqi Commission for Computers & Informatics, Baghdad, Iraq
mareimamaar2@gmail.com

[2]Second Author Affiliation,
Department of Computer Engineering, AL-Rafidain University College, Baghdad, Iraq
mohammednofa@yahoo.com
*Corresponding Author:

DOI: https://doi.org/ 10.31185/wjps.252
Received 01 October 2023; Accepted 09 November 2023; Available online 30 December 2023

ABSTRACT: Enabling customers to access their bank accounts electronically brings many benefits, facilitating interaction between customers and banks, and saving time and effort. Customers no longer need to visit physical bank branches or exchange manual transactions. This transformation can be achieved through a strong electronic authentication system that allows customers to access their bank accounts without visiting a bank branch. The foundation of this system is a powerful and unique biometric authentication feature – facial recognition. Have developed a web application that uses real-time facial recognition for electronic banking systems. Iraqi banks previously lacked such advanced methods of electronic authentication, and research seeks to fill this gap. Implementing this system increases customer confidence regarding the security of their accounts. By using a real-time web application that processes real data, the system can accurately identify and tag individuals, and grant or deny them access as appropriate. Two web applications were created, the first using Olivette's global database for image matching and recognition. The second real-time application allows users to access their bank accounts by taking instant photos of them, and detecting, processing, and identifying the people in the photos. If an unauthorized person gains access, access will be denied. Using the Principal Component Analysis (PCA) algorithm in conjunction with the Eigenface technique and the Support Vector Machine (SVM) classifier, it is possible to achieve high accuracy in face recognition in both web programs. Specifically, able to achieve an accuracy of up to 92% and then improve it to 94%.

Keywords: E-banking system, Authentication, face recognition, web application, PCA, and SVM.

1. INTRODUCTION

The advent of Internet banking, or electronic banking, has revolutionized the management of financial resources, providing a rapid, efficient, and convenient means of handling various financial tasks. By simply sitting behind a computer, can apply for loans, settle bills, and initiate money transfers[1]. This convenience has contributed to the widespread popularity of online banking worldwide, making it an efficient and convenient method for accessing banking services [4]. This has established online banking as an exceptionally popular and popular way of conducting financial transactions among the public. Similar trends are evident around the world, and this is the model we aim to apply in Iraq. Electronic banking offers many valuable services for both financial and non-financial transactions, such as changing

 *Corresponding author: mohammednofa@yahoo.com

Automated Teller Machines (ATM PINs), obtaining summary account statements, updating personal information, and checking account balances[1].

However, online banking also comes with many inherent risks, including the potential for fraud, fraud, identity theft, and data breach. Traditional identity verification methods typically involve users memorizing passwords, PINs, or other unique identifiers, such as access cards or electronic codes[2]. These methods are vulnerable to various forms of attacks, including password theft or hacking, making them insufficient to provide robust protection. Furthermore, the challenge of remembering multiple passwords often leads to risky practices such as writing them down or reusing the same password across multiple applications, compromising security. Many everyday activities, including banking, depend on preventing identity theft. Methods based on natural biometric features provide the user with a promising solution by ensuring data security and ease of use. Although biometric technologies are becoming more attractive, they still face many challenges. [3].

A new type of banking has emerged as a result of the development of information technology. Traditional banking, which relies on a customer's physical presence, is just one type of banking activity[4]. Electronic banking has developed over the past few years, utilizing new channels of distribution like the Internet and mobile applications [5]. The primary goal was to provide businesses with the resources needed to enhance customer satisfaction, reduce transaction expenses, and deliver services to customers where and when needed. However, this convenience also exposes them to risks such as credit card fraud, phishing, and spam. Secondly, ensuring financial security is the main challenge in the field of electronic banking[6]. This study focuses on creating and implementing a web application-based authentication system based on facial recognition for an electronic banking system.

The remainder of this paper is organized as follows: In section 2, the methodologies are presented. The proposed system results and discussions are detailed in section 3. Finally, section 4 concludes the paper and presents the future direction.

Nomenclature is included if necessary
A radius of
B position of
C further nomenclature continues down the page inside the text box

1.1 Motivation

1: To address the existing security deficiencies within the Iraqi banking system.

2: Robust electronic authentication methods are a critical component of the electronic system, making it imperative to explore resolutions for this issue while considering the various aspects involved.

3: Replacing basic electronic authentication techniques such as PINs and fingerprints with a strong and distinctive approach, specifically facial recognition.

4: Develop a web application that revolves around a real-time electronic authentication methodology.

5: Implementing a secure electronic authentication system streamlines customer access to their bank accounts from anywhere. Consequently, the bank not only enhances its security but also gains the trust of customers, ultimately attracting a larger customer base, and resulting in substantial advantages.

1.2 Contributions

The main contribution of the research lies in collecting real data, emphasizing the importance of integrating electronic documentation in Iraqi banks, and advocating electronic management of customer data. Regarding data collection, the study collected images of bank customers' faces, which allowed the development of a real-time facial recognition authentication system. The dataset used by the author was obtained from a specific group of bank users in Baghdad, although the study did not reveal the name of the bank to protect privacy. The dataset consists of 20 face images.

1.3 Material and Methodologies

The proposed model for electronic authentication in Iraqi banks consists of four steps as follows: As shown in Figure 1. The first step is to define the problem and find solutions, then establish the research theories, then build a web program that performs electronic authentication using face recognition. The last step is to evaluate the performance of the model of the proposed system.

1.4 Problem definition

Iraqi banks lack electronic authentication systems based on strong biometric methods, and thus customer data may be exposed to loss, theft, or fraud. Based on these gaps, an electronic authentication system based on face recognition was proposed, trained on images of real people, and worked in real time, achieving accuracy and high performance of the system.

The work is characterized by the fact that it revolves around original images that are obtained instantly through the web application that was built, where the captured image goes through multiple stages, including detection. When the human face is identified within the image, the image is later processed by cropping the face and converting it from color to grayscale images. Then extract the features from the face. After that, the mathematical operations of the Principal Component Analysis (PCA) algorithm are performed on the face, until we reach the classification stage, which is implemented by the Support Vector Machine (SVM) classifier. Once the detection, recognition, and classification processes are completed, the results are displayed on the screen.

Below is Figure 1, which shows the research framework in all its stages, from the problem definition to the model's evaluation performance.

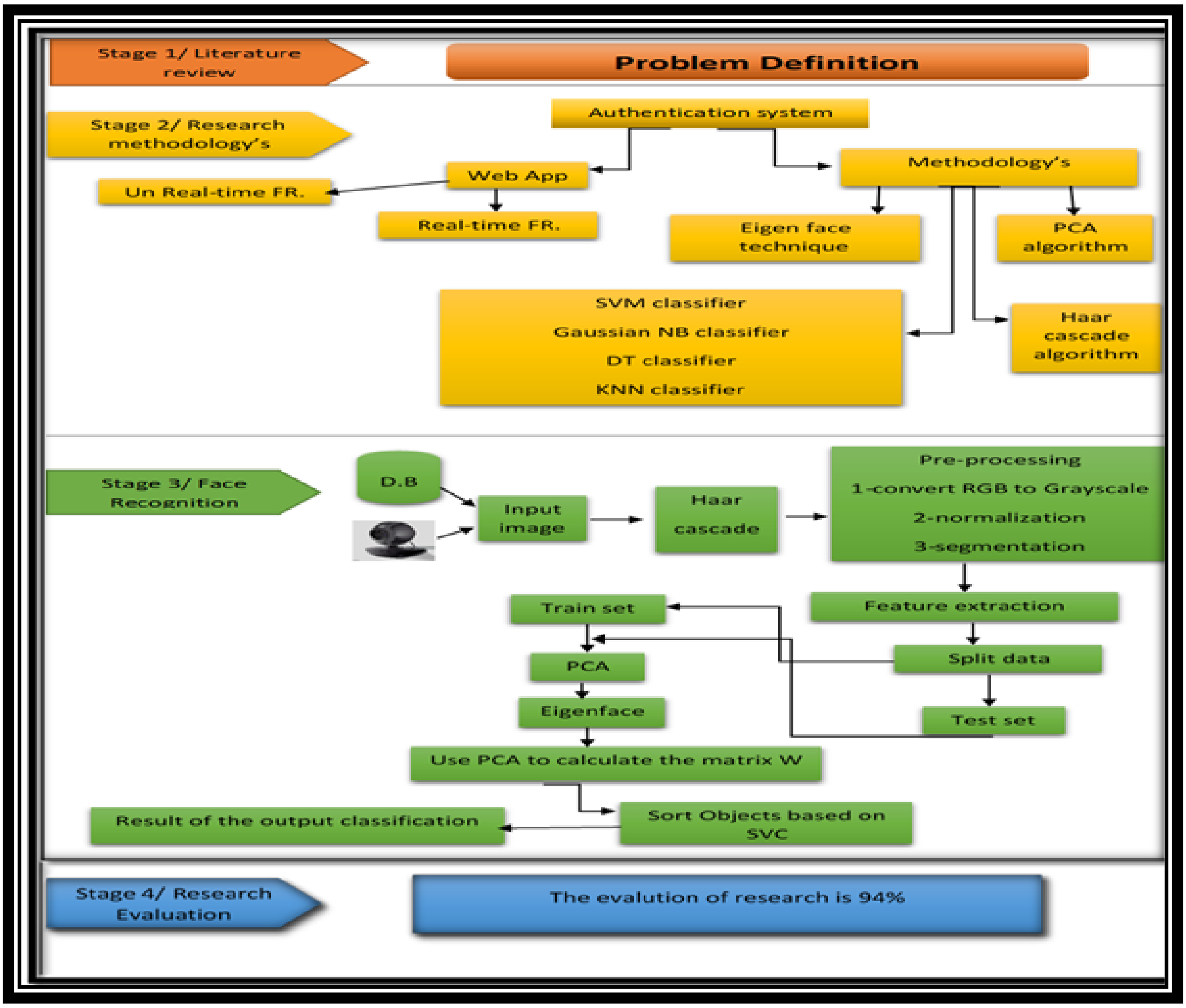


FIGURE 1. Research framework

1.5 Research methodologies

This part consists of five stages:

Face detection, image processing, training, testing, and model performance.

The first step is to apply the Haar Cascade algorithm[7], which detects faces when a command is given to enter the account through the web application so that the webcam opens at any time. After the detection process, processing operations are performed on the image, such as noise reduction, image conversion from color to grayscale, normalization, and graphic equalization. Drawing and segmentation that enhances the quality of the cropped image quickly reduces the error rate and helps in extracting facial features. Feature extraction is the most difficult and decisive. This entails identifying regional features such as the nose, eyes, mouth, and other things common to all faces. The most common feature extraction techniques, such as PCA Extract the least Dimensions[8] and Imputation of faces as Eigen using eigenvalues, which are successfully applied in the proposed system. The third step involves training the model on 70% of the data, followed by testing the model on 30% of the data and measuring the model's performance.

1.6 Face Recognition

Face recognition is a biometric identification technique based on data about facial features that provides an intuitive user interface, accurate identification, and high productivity[9]. There are several practical applications for facial recognition systems, including identity identification, access control management, and public safety[10].

Several algorithms were used in the proposed system to achieve successful and effective face recognition, which will be mentioned.

1. Principal Component Analysis (PCA)

A common name for principle component analysis (PCA), one of the key findings in real-world linear algebra. A popular mathematical method for high-dimensional data analysis is PCA, which has been utilized for dimension reduction. It is used in a wide range of analytical techniques just in the visualization and computer graphics domains. reduction in dimensions[11]., clustering[12] , face and gesture recognition[13] , motion analysis, and synthesis[14] , among many other techniques. It is a technique for identifying patterns in data and for presenting the data to highlight its similarities and differences.

The first step in PCA is to center the data by subtracting the mean (average) value of each feature (column) from the data points in that feature[15]. This process ensures that the data points are shifted around the origin (have a mean of zero) along each dimension.

$$\mu = \frac{1}{N} \sum_i N = 1^{\Gamma} \quad (1)$$

Where:

μ: *is the Mean*

N: *is the Numbers of variables.*

Γi: *is the location of the element in the array.* [16]

After centring the data, you calculate the covariance matrix. The covariance matrix describes how different features are related to each other and is used to find the principal components.

The covariance between two features, i and j, is calculated as follows:

$$\mathrm{COV} = \frac{\sum (X_i - \bar{X})(Y_j - \bar{Y})}{n} \quad \text{(For population)} \quad (2)$$

$$\mathrm{COV} = \frac{\sum (X_i - \bar{X})(Y_j - \bar{Y})}{n-1} \quad \text{(For sample)} \quad (3)$$

is a measure of the relationship between two random variables and to what extent, they change together. In other words, it defines the changes between the two variables, such that change in one variable is equal to change in another variable.

Once you have the covariance matrix, you compute its eigenvalues and eigenvectors. These eigenvalues represent the variance of the data along the corresponding eigenvector (principal component) directions.

$$\vartheta_i = \varkappa v_i \quad (4)$$

Where $\vartheta_i = EigenFace$

$\varkappa = Matrix\ of\ normalize\ images$

$v_i = EigenVector$

Calculations are shifted from the number of pixels in the images (M^2) to the number of images in the training collection (N). In practice, Face images in the training set will be relatively small (N<< M^2), and the calculations become quite manageable. The eigenvector ($\boldsymbol{\vartheta_i}$) are also called Eigenface with begin of the corresponding eigenvalue.

$\omega_i = (\Gamma_i - \mu)$

Where $\Gamma i = \mathrm{Vector}$

$\mu = Mean$ (5)

Project the normalized image open image(ω_i) into Eigenface [17]

$$w_j = \vartheta_j^T \omega_i \quad (6)$$

The weight vector is calculated as:

$$\varphi_i = [w_1^i, w_2^i, w_3^i \ldots \ldots w_k^i] \quad (7)$$

2. Support Vector Machine (SVM) classifier

An SVM classifier, or support vector machine classifier, is a machine learning technique that can be used to analyze and categorize data. Applications for classification and regression may use supervised machine-learning techniques called support vector machines[18].

1.7 Model Evaluation

An interactive visualization tool called the Performance Evolution Matrix compares performance variances to source code modifications. Information is organized according to an application's static and dynamic structures. Model classifier performance measures We describe four performance measures that are common in the fields of data analysis [19].

$$Accurecy = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

$$Sensitivity(Recall) = \frac{TP}{TP+FN} \quad (9)$$

$$Precision = \frac{TP}{TP+FP} \quad (10)$$

$$F1Score = (1+B^2)\frac{2\times precision\times Recall}{(B^2\times precision)+Recall} \quad (11)$$

Where:
TP: True Positives
FP: False Positives
FN: False Negatives

K-fold cross-validation is a valuable technique for assessing predictive models. It involves dividing the dataset into k distinct subsets or folds. The model is trained and assessed k times, with each fold serving as the validation set once. The performance metrics from these k runs are then averaged to estimate the model's generalization performance[20]. This method is instrumental in model evaluation, selection, and fine-tuning of hyperparameters, providing a robust measure of a model's effectiveness. During this process, each fold is used exactly once for training and testing. This approach helps prevent overfitting, a situation where a model performs exceptionally well on the training data but struggles with unseen data. K-fold cross-validation ensures that the model is built in a more generalized manner.

1.8 Results and discussion

The setting and framework within which the proposed system will be developed and used will have an impact on how it will be evaluated. The environment that was used to develop and implement the system is described in this section of the submitted thesis. Anaconda version 3 and Python 3.8 are the programming languages that have completed the development of planned system functions. The AI model has been implemented and the results extracted in Jupiter notebook. In addition, Microsoft Visual Studio 2022 now supports Python 9.3. The purpose of using Visual Studio is to build a web program, connect it with an AI model, and complete the entire proposed program. The device received for all of the previously described methods is an HP laptop with 16GB of RAM and an 11th Gen i7 processor. The monitor cart is an NVIDIA GTX 6G, and completing it is just as challenging. The laptop runs Windows10, 64-bit and has an SSD.

Four models have been applied and implemented for the purpose of achieving the highest possible accuracy of face recognition applied in the web application for the electronic authentication process for Iraqi banks. The highest accuracy was reached at 94% with the SVM classifier. As for the other classifiers, the accuracy of the second model with the D.T classifier reached 66%, the third model with the KNN classifier reached 72%, and the fourth and final classifier NB reached 86% accuracy. On the basis of these results, the model that achieved the highest accuracy of 92% was adopted with the web application.

Table 1. Classification accuracy results

Name	precision	recall	f1-score	support	macro average	weighted average	accuracy
SVM.	1.00	1.00	1.00	3	0.92	0.92	**0.94**
NB. Gaussian	0.89	0.67	0.75	2	0.84	0.86	**0.86**
KNN.	0.57	0.57	0.55	3	0.72	0.71	**0.72**
DT.	0.28	0.04	0.07	1.2	0.25	0.56	**0.66**

Table 2. Cross-Validation result

Model	Cross-Validation result

SVM.	0.89
NB.	0.78
KNN.	0.66
DT.	0.47

Additionally, presents the outcomes of the cross-validation process for the four models, highlighting the model with the highest percentage, indicating superior performance.

Ultimately, the SVM has demonstrated superior operational performance compared to other models by consistently achieving the highest percentage within the range of cross-validation results.

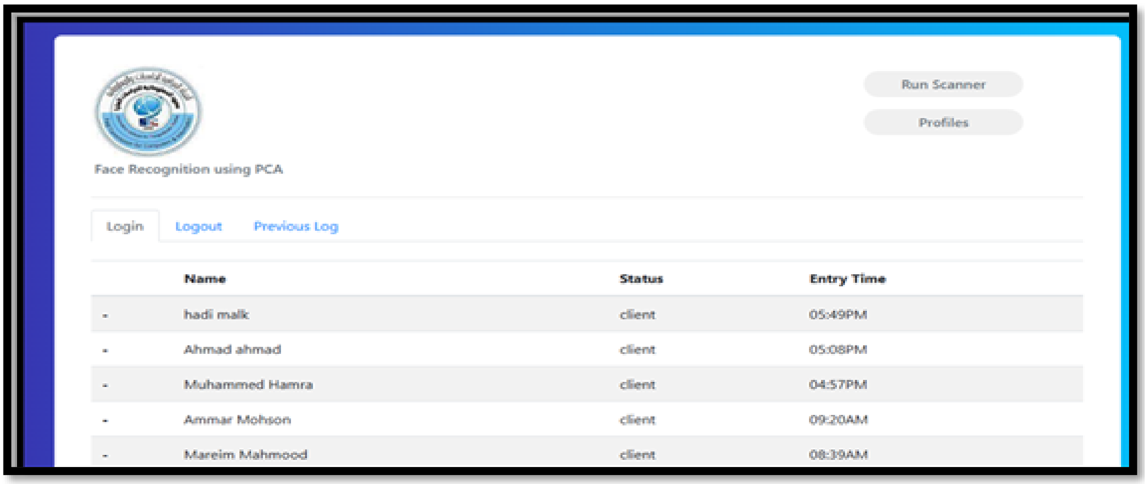
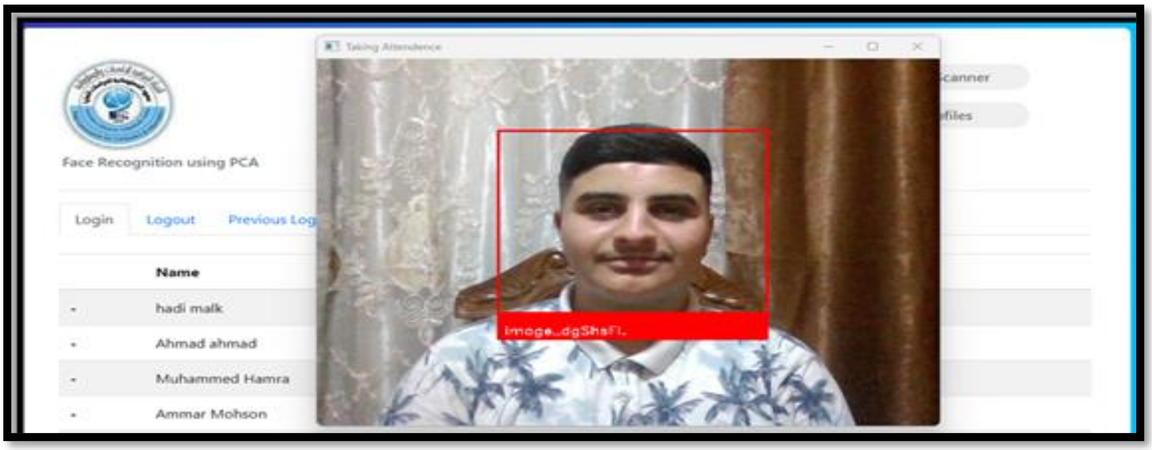


FIGURE 2. The program interface in Real-time

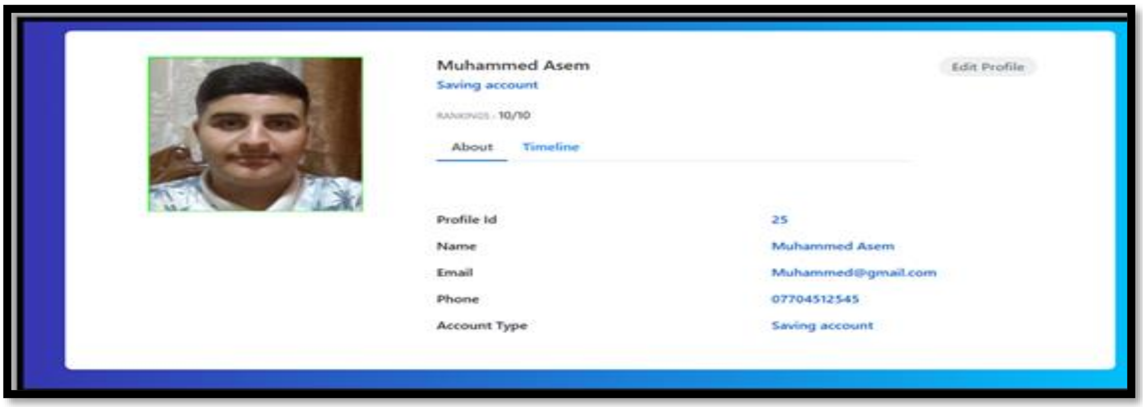
The picture in Figure (2) displays the program interface of the system proposed in the study. Within this program,



customer names are presented alongside the timestamps indicating their entry into the system in real-time.

FIGURE 3. **Real-time face detection**

The image presented serves as an illustrative example. Its primary purpose is to showcase the real-time face-detection functionality within the proposed system. The system instructs users to activate their laptop's front webcam, and it proceeds to determine whether a face is present in the camera's field of view. the bounding box around the face is colored red, as illustrated in Figure (3), it indicates that a face has been recognized in front of the camera, and this face corresponds to the individuals within the real dataset that was previously established, stored, and used for model training. Notably, the red box encompasses an image of a face assigned a name during the initial data capture, affirming the high accuracy and



reliability of the proposed system.

FIGURE 4. **Bank customer profile**

Upon successfully detecting and recognizing a face, the system permits the authorized user to access the system. Figure (4), presented above, depicts the display of a customer's profile once they have been granted login access. All of the user's personal information, which has been previously stored in the bank's database, is readily presented.

If the system fails to recognize a face, it denies entry and displays on the camera feed that the person is not identified, even though their face is detected. Additionally, the system verifies that this face does not match any existing entries in its database, ensuring it remains unclassified for an unknown individual. As shown in the figure (5):

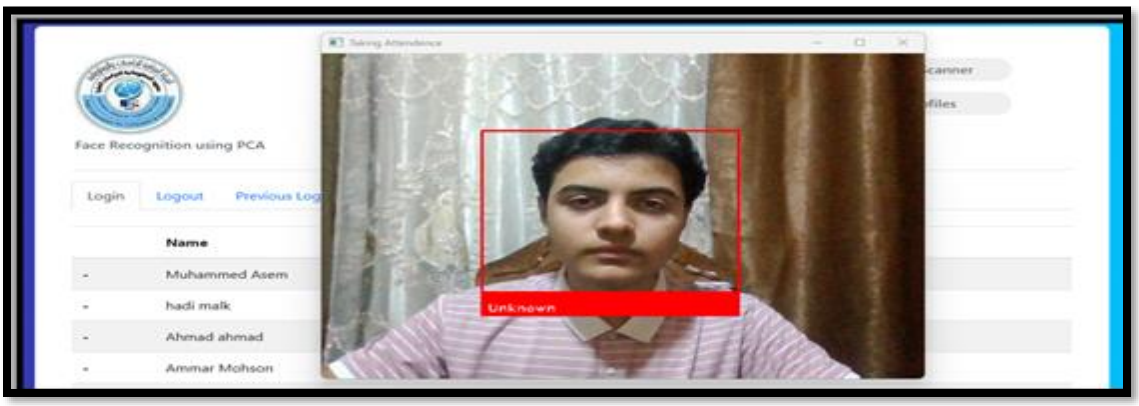


FIGURE 5. unknown individual

2. CONCLUSIONS

The proposed system introduces a web application designed for electronic authentication using biometric facial recognition technology. Its primary purpose is to facilitate user access to their bank accounts by confirming their identity through facial recognition. This is achieved by capturing real-time images of the user's face and subjecting them to a series of algorithms, particularly focusing on face detection, recognition, and classification stages. In the final step, the system grants access exclusively to authorized users with securely stored and successfully identified facial data. This rigorous verification process ensures that only authorized users can access their bank accounts, enhancing security for sensitive financial information. During the implementation of the face detection and recognition algorithms, four different classifiers were employed, resulting in four distinct models. After conducting tests, it became evident that the SVM (Support Vector Machine) classifier demonstrated superior accuracy and overall performance. Consequently, an SVM model was selected and seamlessly integrated into the web application. It's worth emphasizing that a real dataset of facial data was collected, and a web application was developed to process this dataset in real-time. The real-time web application triggers the webcam to capture, detect, and recognize images.

REFERENCES

[1] B. Chaimaa, E. Najib, and H. Rachid, 'E-banking Overview: Concepts, Challenges and Solutions', *Wirel. Pers. Commun.*, vol. 117, no. 2, pp. 1059–1078, 2021, doi: 10.1007/s11277-020-07911-0.

[2] C. U. Bah, A. H. Seyal, and U. Yahya, 'Combining PIN and Biometric Identifications as Enhancement to User Authentication in Internet Banking.', *arXiv Cryptogr. Secur.*, pp. 1–4, 2021, [Online]. Available: https://jp.arxiv.org/abs/2105.09496

[3] R. Senthilkumar and R. K. Gnanamurthy, 'A proposed method for the improvement in biometric facial image recognition using document-based classification', *J. Supercomput.*, vol. 76, no. 6, pp. 4476–4494, 2020, doi: 10.1007/s11227-018-2408-4.

[4] C. H. Tsai and P. C. Su, 'The application of multi-server authentication scheme in internet banking transaction environments', *Inf. Syst. E-bus. Manag.*, vol. 19, no. 1, pp. 77–105, 2021, doi: 10.1007/s10257-020-00481-5.

[5] 'Algorithms and Classifiers in Face Recognition for Automated Attendance', no. Icimia, pp. 195–200, 2020.

[6] A. Bani-Hani, M. Majdalweieh, and A. AlShamsi, 'Online authentication methods used in banks and attacks against these methods', *Procedia Comput. Sci.*, vol. 151, pp. 1052–1059, 2019, doi: 10.1016/j.procs.2019.04.149.

[7] A. B. Shetty, Bhoomika, Deeksha, J. Rebeiro, and Ramyashree, 'Facial recognition using Haar cascade and LBP classifiers', *Glob. Transitions Proc.*, vol. 2, no. 2, pp. 330–335, 2021, doi: 10.1016/j.gltp.2021.08.044.

[8] R. Senthilkumar and R. K. Gnanamurthy, 'A Comparative Study of 2D PCA Face Recognition Method with Other Statistically Based Face Recognition Methods', *J. Inst. Eng. Ser. B*, vol. 97, no. 3, pp. 425–430, 2016, doi: 10.1007/s40031-015-0212-6.

[9] E. I. Abbas, M. E. Safi, and K. S. Rijab, 'Face recognition rate using different classifier methods based on PCA', *Int. Conf. Curr. Res. Comput. Sci. Inf. Technol. ICCIT 2017*, no. December, pp. 37–40, 2017, doi: 10.1109/CRCSIT.2017.7965559.

[10] M. Chihaoui, A. Elkefi, W. Bellil, and C. Ben Amar, 'A survey of 2D face recognition techniques', *Computers*, vol. 5, no. 4, pp. 1–28, 2016, doi: 10.3390/computers5040021.

[11] S. Huang, M. O. Ward, and E. A. Rundensteiner, 'Exploration of dimensionality reduction for text visualization', *Proc. - Third Int. Conf. Coord. Mult. Views Explor. Vis. C. 2005*, vol. 2005, pp. 63–74, 2005, doi: 10.1109/CMV.2005.8.

[12] A. Safonova, J. K. Hodgins, and N. S. Pollard, 'Synthesizing physically realistic human motion in low-dimensional, behavior-specific spaces', *ACM SIGGRAPH 2004 Pap.*

SIGGRAPH 2004, pp. 514–521, 2004, doi: 10.1145/1186562.1015754.
[13] G. M. Zafaruddin and H. S. Fadewar, 'Face recognition using eigenfaces', *Adv. Intell. Syst. Comput.*, vol. 810, pp. 855–864, 2018, doi: 10.1007/978-981-13-1513-8_87.
[14] Y. Koren and L. Carmel, 'Visualization of labeled data using linear transformations', *Proc. - IEEE Symp. Inf. Vis. INFO VIS*, vol. 2003, pp. 121–130, 2003, doi: 10.1109/infvis.2003.1249017.
[15] V. Kumar, D. Kalitin, and P. Tiwari, 'Unsupervised learning dimensionality reduction algorithm PCA for face recognition', *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2017*, vol. 2017-Janua, no. December, pp. 32–37, 2017, doi: 10.1109/CCAA.2017.8229826.
[16] K. R. L. Reddy, G. R. Babu, and L. Kishore, 'Face recognition based on eigen features of multi scaled face components and an artificial neural network', *Procedia Comput. Sci.*, vol. 2, no. 2009, pp. 62–74, 2010, doi: 10.1016/j.procs.2010.11.009.
[17] R. Salas and S. Brahnam, 'Design of face recognition algorithm using PCA -LDA combined for hybrid data pre-processing and polynomial- based ... Related papers'.
[18] J. Hu and L. You, 'Face recognition based on cross-validation by support vector machine', *Lect. Notes Electr. Eng.*, vol. 334, pp. 1011–1018, 2015, doi: 10.1007/978-3-319-13707-0_111.
[19] G. F. Abreu, 'Feature Selection and Optimization on Naive Bayes Modeling using Genetic Algorithm Thesis to obtain the Master of Science Degree in', no. May, 2017.
[20] K. Baumann, 'Cross-validation is dead. Long live cross-validation! Model validation based on resampling', *J. Cheminform.*, vol. 2, no. S1, p. 38106, 2010, doi: 10.1186/1758-2946-2-s1-o5.