Journal of Advances in Management, Engineering and Science (JAMES), 2026; 1(2): 20-29

Research Article

Enhanced security in ATM By Face and Iris Recognition Using Improved-KF-RBF Model

Ogail Dawod, Physical Therapy Department, College of Nursing and Health Sciences, Jazan University, Jizan, Saudi Saudi Arabia ogail76@gmail.com

Received: 19th November 2025; Accepted: 12nd March 2026; Published: 1st May 2026

https://doi.org/10.65470/james.v1i02.20

Abstract –*A biometric system utilizing face recognition could enhance the security of the Automatic Teller Machine, one of the oldest and most dependable types of technology that is still in use today. A biometric system's primary use case is input authentication through database validation and identification. There are essentially five steps to the process: preprocessing, image segmentation, iris normalization, feature extraction, and training (the model). For the sake of adding complexity during preprocessing, the proposed approach used brown iris photos. Then use the ocular image to extract picture segmentation. A result of iris normalization is an iris region with consistent dimensions across all environmental and geographical contexts. To extract features, multiscale morphology is employed. Discover how to use the Improved KF-RBF model for face and iris detection in this paper's ATM section. Contrasted with RBF and KF, this method looks antiquated. Incredibly, the data reveals an improvement with a 97.23% accuracy rate.*

Keywords — *Biometrics, Facial Recognition, Radial Basis Function (RBF)*

INTRODUCTION

The bulk of bank customers now use automated teller machines (ATMs) and electronic budgeting trading platforms, thanks to the development of more advanced cash related infrastructure. The great majority of individuals who interact with finances do it through ATM. ATMs are prone to user error, as are all systems. One common issue that clients regularly have is forgetting their cash or ATM card. Increasing the level of security can address these worries. The major focus is on making an ATM camera able to detect and identify persons using a computer vision framework in order to prevent these unnecessary losses caused by CCF. In the event that the system determines that an unauthorized individual is attempting to use the card to make a transaction at the ATM, the money will be promptly deducted from the machine. Prior to matching, the photo is compared to a database gallery image under various conditions. Here, the system finds the matching image and separates it from the gallery image. Finding people in moving or still images is the main goal of applications that use facial recognition systems. Customers can find ATMs quickly because the system are now installed in many locations with frequent or substantial consumer activity. As more and more individuals use the internet, the chances of vulnerabilities increasing. Superior, multi-layered security is required to protect the approved user from theft or fraud. So, every time

someone withdraws money from an ATM, a new security measure will be put in place. This measure will include an OTP alert, a photo of the person performing the withdrawal, and a text message sent to their email address. The process begins as soon as the user inputs their PIN. The transaction is considered successful if the authorized user inserts the proper PIN. If an unauthorized user inputs the right PIN, the transaction goes through, but the registered user will get a security message via the fast2sms platform with a picture of the unauthorized user that was taken with Open CV. One further thing to think about is the user entering the wrong PIN. If the user inputs the incorrect pin, a OTP will be sent to the approved cellphone number over the platform. The approved user's mail will be sent an image with a security text after a successful transaction. The transaction will be declined if the OTP entered is wrong. Automated teller machines streamline some banking processes, including withdrawals, exchanges, account balance inquiries, and more. Customers can quickly and easily access their ledgers and conduct monetary transactions using an ATM. An individual's PIN is used by the ATM system to safeguard consumers' financial data from unauthorized access. Because it is risky to carry about and remember a lot of PINs and ATM cards, a new iris recognition mechanism has been implemented at the ATM. After the enrollment and confirmation procedures, the all of the client's records are at his fingertips, and he may go forward with any transactions. The iris recognition system provides the utmost safety and security since no one else can access it in any way. There is absolutely no possibility of fraud or theft because neither an ATM card nor a PIN code are required. After the iris scan is finished, the client's mobile phone will receive a OTP to confirm the process. An iris scan is one kind of biometric identification; it verifies a person's identity by analyzing their unique ocular characteristics. An eye's iris is the colored or pigmented ring that encircles the black pupil; it usually has a brown or blue hue. The process of an iris scan begins with a photograph. An infrared imager is used by a specialist camera, which is typically placed no more than three feet from the target, to illuminate the eye and capture shots with extremely high resolution. Mapping, recording, and saving the iris data for future matching or verification only takes a handful of seconds. The picture quality is unaffected by eyeglasses or contact lenses when using an iris-scan technology, which looks for the normal, continuous fluctuation in pupil size to determine if an eye is healthy. The inner border of the iris can be located using an iris-scan algorithm by mapping the iris' distinctive patterns and features.

RELATED WORKS

Iris recognition proposed a method for effective iris code creation. [1] Using this method, the proposed approach can demonstrate that the classic iris code, by minimizing both iris codes and feature values, is the optimal answer to an optimization problem. Better iris codes for the optimization problem can be obtained using this method, which also shows that terms in the objective function can improve efficiency. [2]proposed a method that merges two techniques to increase the code matching accuracy rate. The circular Hough transform is used to extract the iris picture. Finding the area with the zigzag collarets pattern is the next thing to do. Detection is carried out last in addition to removing the eyelashes and lids using the parabola detection method and cutting the median filters. Researchers [3] reported a method that makes use of circular Using Doug man’s rubber sheet model, the proposed approach do the difficult transform and

normalization. Fusion at the patch level is carried out. There has been a lot of study on the topic of secure ATM transactions. Many researchers in the field have made use of the many design elements that are detailed here. According to a system proposed by [4], the proposed device design can double as an RFID or NFC reader and also authenticate fingerprints. Both the input and the output of the data are customizable. Following selection, data is sent by RF signals between the device and the NFC/RFID reader, with authentication via fingerprint performed initially. Only when validation is complete is the data transfer process started. A screen, on/off button, menu keys, fingerprint scanner, and radio frequency identification reader make up the hardware of an RFID/NFC reader. [5]presented a card-less paradigm in which fingerprints are used instead of cards. As the user moves their finger across the keyboard, a proximity sensor on the terminal alters its layout in response to the movement. Alternate layouts are employed if the user's finger is detected. One approach that does not call for extra cards was proposed by [6]. Here, the data that is required is communicated with a terminal by use of the mobile device's near field communication (NFC) capabilities, which are inherent to the ATM. To get things started, the user enters their login credentials. [7]A PIN is automatically generated during the registration procedure. After the credentials submitted are validated, a One-Time Password (OTP) is generated. The authentication server verifies the username and one-time password (OTP) once the NFC reader reads them; if all is in order, the transaction can go forward. Card Emulation Mode is where the suggested idea works. The initial step in the NFC-enabled approach proposed by[8] is to swipe an ATM card. The subsequent stage is to place the NFC-enabled phone's screen on the scanner at the terminal. The vast majority of bank customers nowadays favor using ATMs for all of their financial transactions due to how convenient the system are. Unfortunately, there are security dangers associated with modern ATM technology. These hazards include the potential for card theft or misuse, loss of cards, and forgetting PINs. The paper's authors [9] proposed a facial recognition-based next-generation ATM system to solve all of these problems. Instead of using ATM cards, this approach uses RFID tags. In [10], the author describes an ATM that can identify a customer only by looking at their face. In this case, the proposed approach used One-Time Password (OTP) for secure transactions and Principal Component Analysis (PCA) for facial recognition. A face identification approach based on Eigen faces is proposed in paper [11]. This system analyses the algorithms of previous systems. Reliability, speed, and storage space requirements are all much enhanced with a PCA based method. Users' ability to alter the system through photo editing is its main drawback. The production cost of 3D face masks is too high, even if the system would represent an advancement in this technology. The research [12] suggests a vibration detector that could pick up on the vibrations of an ATM in the case of a theft. Embedded systems based on ARM controllers enable this system to process vibration sensor data in real-time. A beeping sound will be produced by the buzzer whenever it senses vibration. [13] The ATM door is closed by a DC motor. Additional measures have been implemented to guarantee security. Theft will be less common and the criminal can be caught because of this. [14] Can represent on-chip peripherals accurately using Keil Vision Debugger. Using GSM technology, this gadget can detect stolen ATMs in real-time, which helps with both speedy response and failure prevention. When it

comes to ATMs, there are essentially two main types. And can do it all from a single, simple device: check balance, make changes to PIN, get mini statements and get the latest account updates. [15] The more sophisticated devices allow to pay bills, establish a credit line, and deposit cash or cheques. Countless academics have developed and continue to develop algorithms and approaches to strengthen the security of automated teller machines (ATMs), as many financial institutions are susceptible to fraud in online banking transactions. [16] Biometrics integration into the ATM system to confirm the identification of allowed customers is one example of how the system are investing much in security measures. Using a single feature alone is usually insufficient to correctly identify the right person with contemporary biometric ATM systems. [17] Particularly in low-light, crowded, or otherwise challenging photographic conditions, this is true. The majority of studies have focused on multimodal biometric recognition since it can help build unique evidence and strengthen security. Programmable biometric recognition using personal computers was first investigated [18]. Facial recognition is now seeing explosive growth, but it still has a long way to go before it's completely bug free. As a result, face recognition techniques still have a long way to go. [19] The main motivation for biometrics research is the need to identify permitted individuals utilizing facial features, lines, areas, and textures for security reasons. In their system, [20] suggested facial and fingerprint recognition. The client receives a one-time code on their cell phone when logging in; this code can only be used once. [21] If someone inputs the erroneous code, their face will be saved and sent via email to help identify them and presented their results in paper that was based on the emotions of different consumers.

METHODOLOGY

While online banking has made life easier, it has also increased the likelihood of criminality. A great deal of money has been transferred fraudulently. Even while there are a lot of advantages to using an ATM system, there are also a lot more frauds. The proliferation of online transactions has increased the importance of robust authentication and user identification systems. When it comes to handling money, many people now rely on the Automatic Teller Machine (ATM). Figure 1 shows the process of the proposed system.

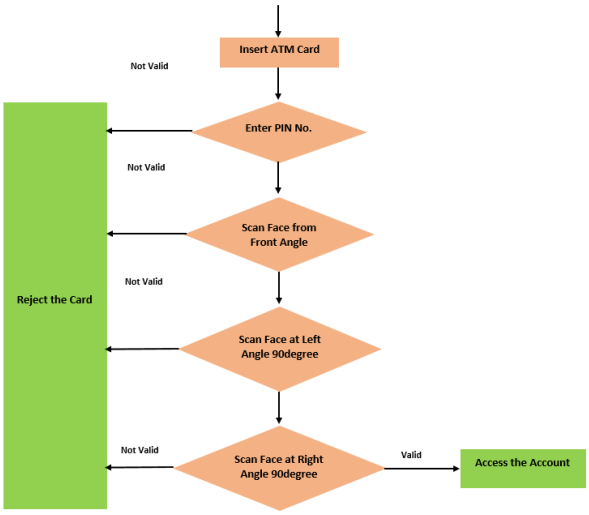

Fig. 1. Diagram of the Process Flow for Biometric ATM System

A. Preprocessing:

In order to make it harder for identification system to identify and provide better recognition accuracy, the proposed approach chose brown-colored iris photos when the proposed approach were faced with the chore of collecting these images for the neural network's training and testing. The collected irises have unique patterns and shapes up close, but the system appear very similar from a distance. The proposed approach used the iris database (Chek image

database) to acquire and undergo pre-processing 21 brown-colored photographs of distinct individuals' irises taken from the same side. Unprocessed iris pictures ranging from 300 kB to 400 kB needed pre-processing. And can see the white sclera and black pupil in every single picture. Another issue was that the binary iris picture did not include the proper content to train an artificial neural network on (irrelevant headers, etc.). The preceding three steps are data pre-processing phases; the fourth step is a BrainMaker pre-processing step. For iris extraction and picture enhancement, there are a lot of signal processing and filtering techniques described in the literature [22]. Because the proposed approach were primarily concerned with developing the Improved KF-RBF for iris identification, the proposed approach had to make some adjustments to the images by hand. It is possible to automate the first three stages of iris image processing, though. The proposed approach used open-source Java software to obtain the RGB values of each pixel and saved them in a file. The proposed approach used Photoshop to remove some unnecessary pixels from the top and bottom of each of the twenty images, and then the proposed approach saved the resulting jpg files to meet the program's specifications. Using the Java software, the contents of each pixel were converted to a 6-digit RGB value.

B. Image Segmentation:

The next step is to start eliminating the iris from the ocular image. A rectangular block with consistent size was used to standardize the derived iris region in order to address imaging discrepancies. Using the integro-differential operator, locate the round areas of the iris and pupil, the upper and lower eyelid arcs, and the eyelids themselves. A possible way to describe the integral-differential operator is

$$max_{(u,q_w,z_t)} \left| L_\tau * \frac{d}{dq} \oint (u, q_0, z_t) \frac{B(q,z)}{2\pi r} ds \right| \quad (1)$$

The eye image is represented by $B(q,z)$, the search radius is denoted by u, a Gaussian smoothing function is denoted as $L_v(u)$, and the contour of the circle given by (u, q_0, z_t) is denoted as s [23]. By adjusting the radius and center q and z positions of the circular contour, the operator finds the path where the pixel values change the most. Achieving accurate localization requires iteratively applying the operator while gradually reducing the amount of smoothing. In a similar vein, the localization of the eyelids occurs along an arc rather than a circular path of contour integration. After iris segmentation, the picture is normalized and transformed from Cartesian to polar coordinates.

C. Iris Normalization:

Converting the iris region to a 40x260 dimensional matrix for extra verification is the next step after successful iris region segmentation from one eye. The reason why eye pictures appear three-dimensional is because various levels of light cause the pupils to dilate, which in turn stretches the iris. [24] This approach generates iris regions with uniform dimensions in all settings. After selecting the desired region of the iris, a copy of Daugman's rubber sheet is made. The Daugman normalizing method is used to transform the Cartesian model of iris texture into polar coordinates. This method can remove the unwanted variations brought on by the eye's position in relation to the camera and the distance between the two. A Cartesian to polar transform is defined by us as:

$$q_w(\theta) = q_{w0}(\theta) + u_w * \cos(\theta) \quad (2)$$

$$z_w(\theta) = z_{w0}(\theta) + u_w * \sin(\theta) \quad (3)$$

$$q_b(\theta) = q_b(\theta) + u_b * \cos(\theta) \quad (4)$$

$$z_b(\theta) = z_{b0}(\theta) + u_b + \sin(\theta) \quad (5)$$

The process involves fewer angular dimensions. A linear change in texture along the radial direction is postulated by the rubber sheet concept. By employing the rubber sheet model, the iris texture is linearly mapped radially from the pupil border to the limbus border into the interval [0 1]. Simultaneously, it produces a three-dimensional transformation along the same axis.

D. Feature Extraction:

1) Multiscale Morpology:

The field of mathematical morphology provides a wealth of tools for image processing and analysis. The morphologic operators use a collection of pixels to mathematically represent an image. Consequently, the operations are defined as interactions between objects and structural elements based on set theory. Commonly used in digital image processing are flat structural elements with regular geometric shapes like disks, lines, and squares. In morphology, erosion and dilation are the backbone processes. Opening and closure are examples of additional actions that include various combinations of erosion and dilation [25]. Two instances of this are the domain of a grayscale image (m) and a flat structural member (I). The erosion of m and the dilation of m by I are defined below:

$$(m \ominus I) = min\{m(b + w, c + x)|(w, x) \in I\} \quad (6)$$

$$(m \oplus I) = max\{m(b - w, c - x)|(w, x) \in I\} \quad (7)$$

For feature or object extraction from images of a specific geometry, the size and shape of the structuring element I are crucial. The term "multiscale morphology" describes a set of morphological procedures that employs structural pieces with the same form but varied sizes. Both equations (6) and (7) define operations for opening and closing on multiple scales, with

$$(m \circ oI)(b, c) = \big((m \ominus oI) \oplus oI\big)(b, c) \quad (8)$$

$$(m \bullet oI)(b, c) = \big((m \oplus oI) \ominus oI\big)(b, c) \quad (9)$$

where the value of oI is $(o - 1)I$ multiplied by I and can be expressed as

$$oI = I \oplus I \oplus \ldots \oplus I \quad (10)$$

The same holds true for the equation $m \bullet oI = m$. It is possible to extract texture features from multiscale morphology using the top-hat transform. The underlying principle is that elements that are too bright or too dark to fit inside the structuring element are eliminated during open (or shut) operation, respectively. The bright characteristics of an image are extracted by subtracting the opened image from the original one, as open (or close) is an anti-extensive (or extensive) operation. Similarly, dark features can be created by subtracting the original image from the closed image.

E. Model Training:

1) Improved KF-RBF:

Within the context of the suggested sampling regulation mechanism, this section refines a density

function estimation technique based on KF-RBF. Using the RBF framework, then determine an estimate of the density function, which is

$$\hat{\phi}(x,q) = \delta^T(q)\hat{p} - j^T(x,W)j^{-1}(W,W)\left(\delta^T(W)\hat{p}Z(W,o)\right) \quad (11)$$

The function C(.) can be used to express the spatial and temporal correlation between any two points in the given region. As an illustration, consider the correlation between two points $j(x,W)$ and the sample positions W. The precise formulations of $j(x,W)$ and $j(W,W)$are as follows:

$$j_b = \tau_u exp\left[-\frac{(x-w_b)^2}{\tau_v^2}\right] exp\left[-\frac{(o-o_b)^2}{\tau_o^2}\right] \quad (12)$$

$$j_{bc} = \tau_u exp\left[-\frac{(w_b-w_c)^2}{\tau_v^2}\right] exp\left[-\frac{(o_b-o_c)^2}{\tau_o^2}\right] + \Psi_{bc} \quad (13)$$

It is the ith element of $j(x,W)$ and the bc th element of $j(W,W)$in the given set. The constant gain parameter is denoted by τ_u, while the values τ_s and τ_o stand for spatial and temporal sensitivity, respectively. The Kronecker Delta function, represented asΨ_{bc}, is 1 when $b = c$ and 0 otherwise. It is clear from this that K is a positive definite matrix and that the gain matrix of the Kalman filter is$D_w(o_d)$.

$$D_w(o_d) = W_d(o_{d-1})\delta^T(W)(\delta(W)W_d(o_{d-1})\delta^T(W) + U)^{-1} \quad (14)$$

In which U is the matrix of noise covariance and $W_d(o_{d-1})$ is the matrix of estimation error covariance, as demonstrated by the following.

$$W_d(o_d) = W_d(o_{d-1}) - D_w(o_d)\delta(W)W_d(o_{d-1}) \quad (15)$$

Such that, at every given point x the density function can be approximatively given by (13), and (14). The Kalman filter, used to handle sampling noise, is the source of the D_w in equation (14). Specifically, to show how the enhanced KF-RBF based estimating method works in full.

The values of τ_u, τ_s, τ_o are determined by comparing the supplied region with the density function's border. These parameters can be accurately determined through iterative calculations utilizing the MCMC method. Rasterizing the given area is the only way to get the density function's geographical distribution. A point-by-point calculation of the density function distribution across the given region can then be obtained [26]. The first term is employed to reduce density function estimation errors; the second one allows the proposed coverage control system to remove the impact of a time-varying density function; and the last one compensates for the distance between the estimated and real centroid. Along with these conditions, the suggested algorithm's estimation errors will converge to zero, guaranteeing the stability of the system.

RESULT AND DISCUSSION

Because every single individual possesses a unique combination of characteristics, a biometric system can reliably identify them. Biometric systems have been developed using a wide range of biometric data sources, such as fingerprints, voice, hand geometry, facial features, handwriting, and retina/iris scans. Nowadays, the demand for safety measures is increasing at an exponential rate. The end product is biometric recognition, a safe, reliable, and user-friendly method of identifying individuals.

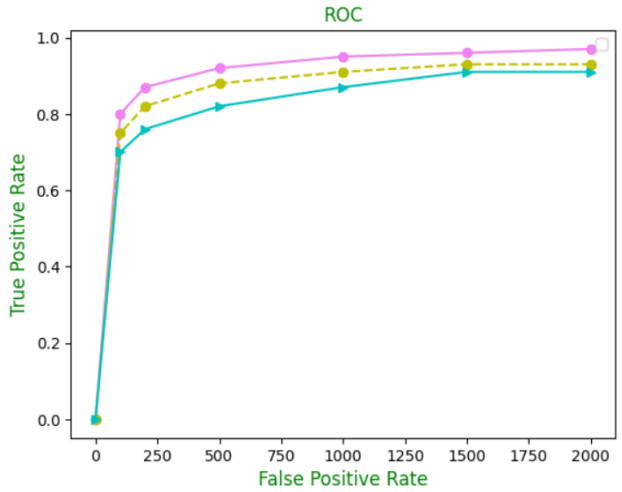

Fig. 2. ROC Curves

The roc curve for the suggested model is shown in Figure 2. To supplement the ROC curve, which does not clearly illustrate the method's advantages and disadvantages, the proposed approach turn to AUC to illustrate the method's pros and cons. There is a range of 0 to 1 for the area under the receiver operating characteristic (ROC) curve, which is represented as AUC.

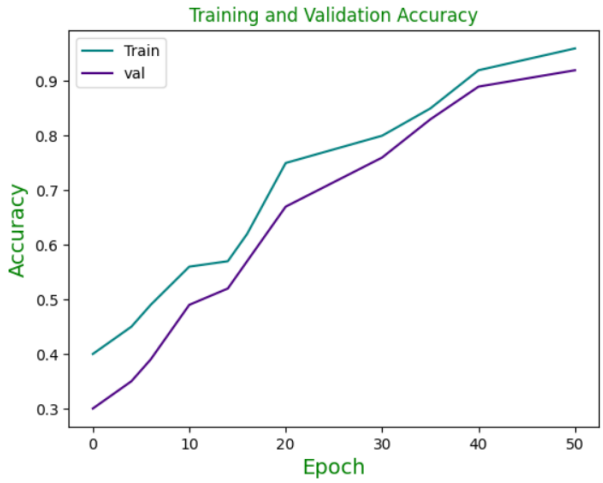

Fig. 3. Training and Validation Accuracy

Figure 3 shows the results of testing the model's accuracy over the course of 50 epochs of training. Each method's testing dataset also contained own images as well as a few randomly selected ones from the internet.

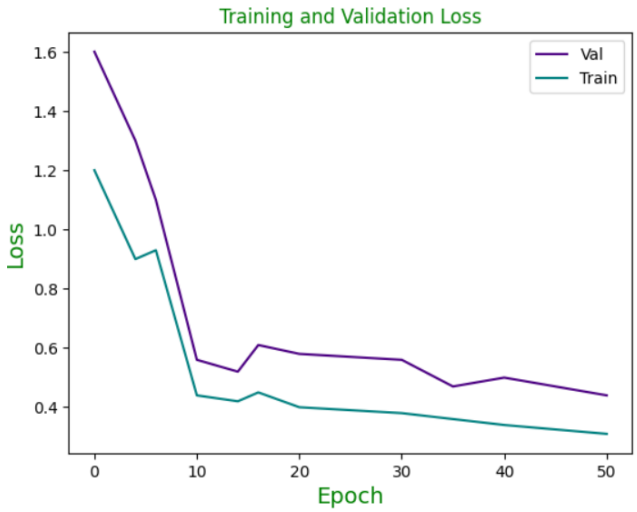

Fig. 4. Training and Validation Loss

Fifty epochs were finished during the training phase to check the model loss, as shown in Figure 4.

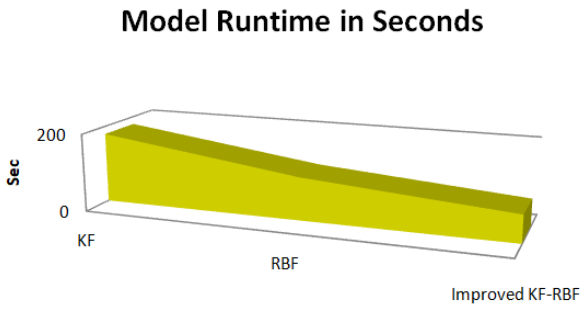

Fig. 5. Model Runtime in Seconds

Figure 5 displays a comparison of all the models using the matrices and parameters mentioned before. With the increased KF-RBF performance in real-time, the run time is comparatively quite low.

Fig. 6. Evaluation Metric Visualization

Figure 6 displays the metrics for evaluation in a visual format. The display shows a comparison of the recall, accuracy, and precision of the KF, RBF, and Improved KF-RBF models.

CONCLUSION

The Automated Teller Machine (ATM) has made it easier than ever to access one's bank account from any location and at any time. This electronic communications device lets consumers make deposits, withdrawals, and money transfers with the tap of a screen, doing away with the requirement for a human teller or cashier. A survey found that people are worried about the safety of taking money out of ATMs. The absence of suitable authentication procedures jeopardizes the security of ATM transactions. It utilized brown iris pictures to increase the level of complexity throughout the preprocessing. After that, for image segmentation, utilize the ocular image. An iris region with uniform proportions across all geographical and environmental situations is the end product of iris normalization. Features are extracted using multiscale morphology. In order to train the model, an approach known as Improved KF-RBF is employed. With an impressive accuracy level of 97.23%, the suggested technique routinely surpasses the RBF and KF models.

Acknowledgement

The author would like to appreciate the effort of the editors and reviewers.

Author Contributions

All authors are equally contributed.

Conflict of Interests

The authors declare that they have no conflicts of interest.

Ethics Approval

There are no human subjects in this article and informed consent is not applicable.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not- for-profit sectors.

REFERENCES

[1] Y. Hu, K. Sirlantzis, and G. Howells, "Optimal Generation of Iris Codes for Iris Recognition," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 1, pp. 157–171, 2017, doi: 10.1109/TIFS.2016.2606083.

[2] H. Rai and A. Yadav, "Iris recognition using combined support vector machine and Hamming distance approach," *Expert Syst. Appl.*, vol. 41, no. 2, pp. 588–593, 2014, doi: 10.1016/j.eswa.2013.07.083.

[3] W. : Www, K. Gulmire, and S. Ganorkar, "Iris Recognition Using Independent Component Analysis," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 2, no. 7, p. 433, 2012, [Online]. Available: www.ijetae.com.

[4] S. Bharadwaj, M. Vatsa, and R. Singh, "Biometric quality: a review of fingerprint, iris, and face," *Eurasip J. Image Video Process.*, vol. 2014, no. 1, pp. 1–28, 2014, doi: 10.1186/1687-5281-2014-34.

[5] S. Gokul, S. Kukan, K. Meenakshi, S. S. V. Priyan, J. R. Gini, and M. E. Harikumar, "Biometric based smart ATM using RFID," *Proc. 3rd Int. Conf. Smart Syst. Inven. Technol. ICSSIT 2020*, no. Icssit, pp. 406–411, 2020, doi: 10.1109/ICSSIT48917.2020.9214287.

[6] A. Hassan, A. George, L. Varghese, M. Antony, and S. K.K., "The Biometric Cardless Transaction with Shuffling Keypad Using Proximity Sensor," *Proc. 2nd Int. Conf. Inven. Res. Comput. Appl. ICIRCA 2020*, pp. 505–508, 2020, doi: 10.1109/ICIRCA48905.2020.9183314.

[7] 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," *Int. J. Adv. Eng. Technol.*, vol. 3, no. 3, pp. 90–94, 2020, [Online]. Available: https://lens.org/079-559-002-381-235.

[8] A. Joy, C. Babu, and A. Chandy, "A Systematic Review Comparing Different Security Measures Adopted in Automated Teller Machine," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 13, pp. 388–393, 2021.

[9] S. Sasipriya, P. Mayil Vel Kumar, and S. Shenbagadevi, "Face recognition based new generation ATM system," *Int. J. Innov. Sci. Res. Technol.*, vol. 3, no. 3, pp. 2854–2865, 2018.

[10] M. Karovaliya, S. Karedia, S. Oza, and D. R. Kalbande, "Enhanced security for ATM machine with OTP and facial recognition features,"

Procedia Comput. Sci., vol. 45, no. C, pp. 390–396, 2015, doi: 10.1016/j.procs.2015.03.166.

[11] J. J. Patoliya and M. M. Desai, "Face detection based atm security system using embedded Linux platform," *2017 2nd Int. Conf. Converg. Technol. I2CT 2017*, vol. 2017-Janua, no. April 2017, pp. 74–78, 2017, doi: 10.1109/I2CT.2017.8226097.

[12] S. S. Peter, "Face Authentication ATM using Deep Learning," *Int. J. Mech. Eng. Vol.*, vol. 7, no. 8, pp. 108–114, 2022.

[13] R. S. Ranjitha, M. S. Sheetal, S. K. Vignesh, K. A. Nitesh, and others, "Multi-Account Embedded ATM Card with Face Recognition Security System," *Int. J. Eng. Res. Technol.*, vol. 8, no. 11, pp. 16–20, 2020.

[14] H. R. Babaei, O. Molalapata, and A. A. Pandor, "Face Recognition Application for Automatic Teller Machines (ATM)," vol. 45, no. Icikm, pp. 211–216, 2012.

[15] T. Sharma and S. L. Aarthy, "An automatic attendance monitoring system using RFID and IOT using Cloud," *Proc. 2016 Online Int. Conf. Green Eng. Technol. IC-GET 2016*, pp. 1–4, 2017, doi: 10.1109/GET.2016.7916851.

[16] M. C M, "Card-Less ATM Transaction using Biometric and Face Recognition– A Review," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 8, no. 7, pp. 1493–1498, 2020, doi: 10.22214/ijraset.2020.30444.

[17] S. Eum, J. K. Suhr, and J. Kim, "Face recognizability evaluation for ATM applications with exceptional occlusion handling," *IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. Work.*, pp. 82–89, 2011, doi: 10.1109/CVPRW.2011.5981883.

[18] A. Mohite, S. Gamare, K. More, and N. Patil, "Deep Learning based Card - Less Atm using Fingerprint and Face Recognition Techniques," *Int. Res. J. Eng. Technol.*, pp. 3504–3509, 2019.

[19] 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," *Int. J. Adv. Res. Comput. Sci.*, vol. 3, no. 5, pp. 164–169, 2012, [Online]. Available: http://ezproxy.idrc.ca/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=tnh&AN=91876695&site=ehost-live.

[20] N. Ahmad, A. A. M. Rifen, and M. H. A. Wahab, "AES Cardless Automatic Teller Machine (ATM) Biometric Security System Design Using FPGA Implementation," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 160, no. 1, 2016, doi: 10.1088/1757-899X/160/1/012113.

[21] I. Omara, A. Hagag, S. Chaib, G. Ma, F. E. Abd El-Samie, and E. Song, "A Hybrid Model Combining Learning Distance Metric and DAG Support Vector Machine for Multimodal Biometric Recognition," *IEEE Access*, vol. 9, pp. 4784–4796, 2021, doi: 10.1109/ACCESS.2020.3035110.

[22] F. N. Sibai, H. I. Hosani, R. M. Naqbi, S. Dhanhani, and S. Shehhi, "Iris recognition using artificial neural networks," *Expert Syst. Appl.*, vol. 38, no. 5, pp. 5940–5946, 2011, doi: 10.1016/j.eswa.2010.11.029.

[23] A. D. Vincy and S. Sathana, "Recognition Technique for ATM based on Iris Technology," vol. 3, no. 11, pp. 1–5, 2019.

[24] D. Malviya, "Face Recognition Technique : Enhanced Safety Approach for ATM," *Int. J. Sci. Res. Publ.*, vol. 4, no. 12, pp. 1–6, 2014.

[25] S. Umer, B. C. Dhara, and B. Chanda, "Iris recognition using multiscale morphologic features," *Pattern Recognit. Lett.*, vol. 65, pp. 67–74, 2015, doi: 10.1016/j.patrec.2015.07.008.

[26] L. Zuo, M. Yan, Y. Guo, and W. Ma, "An improved KF-RBF based estimation algorithm for coverage control with unknown density function," *Complexity*, vol. 2019, 2019, doi: 10.1155/2019/6268127.