International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 12 | Dec – 2025 DOI: 10.55041/ISJEM05320
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Enhancing The ATM Transaction Security Using Iris Recognition Technology

Shwetha K
AssistantProfessor,
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology
Mysore, Karnataka, India
shwetha_ece@mitmysore.in

Maheshwari D
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology
Mysore, Karnataka, India
dharaneshkumar599@gmail.com

Ananya M
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology
Mysore, Karnataka, India
ananya23suresh@gmail.com

Abhiram Bharadwaj R
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology Mysore,
Karnataka, India
abhirambharadwaj2004@gmail.com

Abhishek D
Department of Electronics and Communication Engineering,
MaharajaInstituteofTechnology
Mysore, Karnataka, India
abhishekdevaprakash@gmail.com

***Abstract*—With the increasing use of electronic banking services, protecting the confidentiality and security of transactions conducted via ATMs has become a major priority. The current security system involving cards and Personal Identification Numbers makes them prone to risks of theft, card skimming, and shoulder surfing attacks. This paper describes the development of a new and improved secure system for conducting transactions at ATMs utilizing iris scanning technology with a biometric authentication process. The proposed biometric approach involves scanning the user's iris image and identifying a match based on pre-stored templates with a Deep Learning Classifier. The uniqueness of irises makes them impervious to attacks or counterfeiting. The proposed system was tested with the IIT-Madras iris database with improved performance compared to the current security process. With its feasibility to perform transactions without requiring physical cards and memorized PIN codes, the proposed invention can be appropriately termed as next-generation ATMs.**

Keywords —ATM Security, Iris Recognition, Biometric Authentication, Deep Learning, CNN, IIT Madras Iris Dataset, Financial Transaction Security, Pattern Recognition.

I.INTRODUCTION

The rapid expansion of the Automated TellerMachine (ATM) in the current world has increased the threats of security risks, including stealing, phishing, and hacking, among others. In today's technological advancements, the main problem of using the ATM in the current world lies in the lack of security and the need for a more secure method that can't be easily accessed by thieves. The current system of using the ATM card and PIN number has posed a great problem due to the high chances of losing the cards or the PIN number being hacked by thieves.

Biometric authentication has also proven to be an innovative method of solving some of these problems by identifying a person through their physiological characteristics. Among the different biometric technologies, iris authentication has been known for its accuracy, stability, and inability to be replicated. This is due to the intricate texture that makes up the human iris, which has proven to be the most accurate biometric identifier.

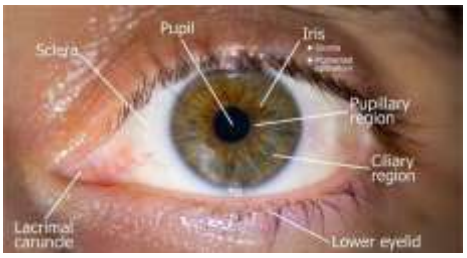


Figure 1: Labelled structure of the human eye.

In this article, an improved ATM transaction security system

based on the use of the iris recognition technique for the purpose of replacing or supplementing the standard card & PIN systems is proposed. The process entails the acquisition of the user's iris image, preprocessing, feature extraction, and finally, the authentication of the user's identity by a deep learning model. The proposed technique is trained and tested with the IIT Madras iris database.

With the incorporation of iris pattern-based biometric authentication in ATM systems, as proposed in this project, improved security, prevention of fraud cases, and provision of greater convenience to users will be achieved.

II. LITERATURE REVIEW

Ashraf [1] proposed an advanced ATM security system using iris biometric authentication to overcome the limitations of card-and-PIN methods. The system follows standard iris processing steps such as acquisition, segmentation, normalization, extraction, and matching. Experimental results show high accuracy with low false acceptance rates, effectively preventing frauds like card skimming. Compared to face and fingerprint methods, iris authentication is more stable and resistant to environmental variations, making it a reliable and convenient solution for secure ATM transactions.

Joans et al. [2] proposed an ATM security system using iris recognition for accurate, card-free authentication. The method exploits the unique, non-invasive nature of the iris and achieves high accuracy with low error rates. By reducing dependence on PINs, it prevents threats such as shoulder surfing and card loss. Experimental results confirm the feasibility of real-time ATM implementation, concluding that iris recognition significantly enhances ATM security.

Darthi Vincy & Sathana [3] proposed an iris recognition–based ATM security system to replace traditional card and PIN verification. The model includes iris capture, processing, segmentation, normalization, and encoding, using techniques such as Canny edge detection and histogram equalization. Log-Gabor filters are used for feature extraction, and matching is done using Hamming distance. The low False Acceptance and False Rejection rates demonstrate the system's reliable and authentic performance.

Rame Gowda and Vandana [4] proposed an ATM security system using both face and eye recognition to improve authentication accuracy. By combining multi-modal biometrics, the system overcomes limitations of single-mode methods and enhances anti-spoofing protection. It involves image capture, processing, and matching for both modalities, eliminating the need for cards. The authors conclude that multi-modal biometric authentication significantly strengthens ATM transaction security.

Özgür & Selçuk [5] proposed an iris-recognition–based authentication method for ATM/ITM machines to eliminate the use of cards and PINs. The system applies theDaugman method for iris segmentation, normalization, and feature extraction, leveraging the uniqueness and stability of iris features. Experimentalresults show very low False Acceptance and Rejection Rates with high accuracy.

III. METHODOLOGY

The proposed ATM security system adopts iris recognition technology for user authentication. The system eliminates the need to use cards and PINs for authentication. The process involves capturing an iris image as soon as the customer approaches the ATM. The captured iris image is then preprocessed to improve clarity and detect the iris part of the image. The iris characteristics, including rings and patterns, are extracted from the iris using feature extraction algorithms. The extracted iris characteristics are then matched with existing iris templates in the database. If there is a match, access is granted to perform transactions. However, if there is no match, access is denied as security is also alerted. The iris authentication method is more accurate due to unique iris patterns that don't change over time.

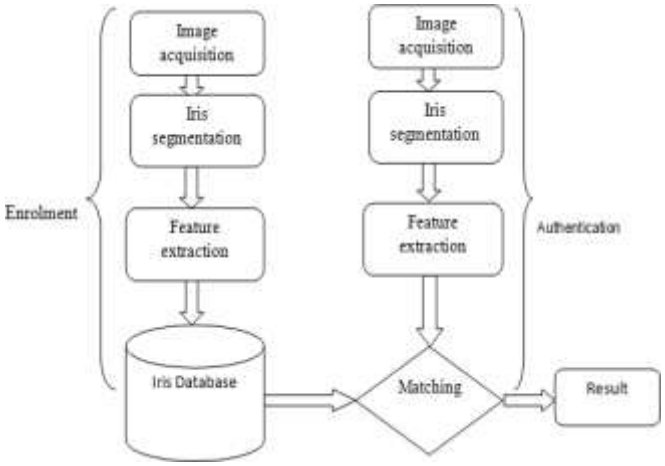


Figure 2: Architectureofirisrecognitionsystem

1. Image Acquisition: The first stage of the iris recognition system is image acquisition, which captures the user's eye image through a dedicated camera. Generally, near-infrared illumination is used to enhance iris texture visibility and minimize the impact caused by ambient lighting and reflections. Image capture has to be done of a quality nature, as poor image resolution or motion blur can seriously deteriorate system performance.

2. Iris Segmentation: Iris segmentation can be defined as the accurate isolation of the region of the iris from the captured image of the eye. This step segregates the iris from the surrounding structures such as the pupil, sclera, eyelids, and eyelashes. This may be accomplished by techniques such as edge detection, circular Hough transform, or Daugman's integrodifferential operator. Segmentation has to be performed as accurately as possible, because any inaccuracy in the segmentation may lead to a failure in feature extraction.

3. Iris Normalization: Depending on the level of pupil dilation, positioning of the eye, and distance from the camera, iris size may vary from capture to capture. Normalization of the iris converts the segmented region of the iris into a fixed-dimensional, standardized form using models such as the rubber sheet model. This provides uniformity that enables dependable matching between different iris samples.

4. Feature Extraction: During this stage, normalization of the iris image is done to extract distinctive and stable features representing the unique patterns of iris texture. These include furrows, rings, freckles, etc. Common approaches use Gabor or Log-Gabor filters that yield a binary iris template encoding the iris characteristics in an efficient way.

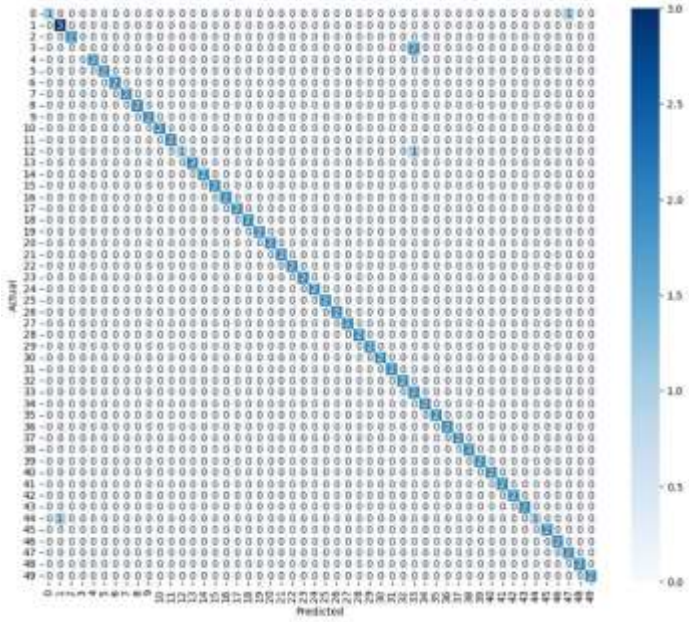
5. Enrollment: The features of irises for authorized users, after extraction, are kept in an iris database during the enrollment phase. Every iris template corresponds to a user identity. The database shall serve as the reference set from which all authentication attempts will be verified against.

6. Matching: During the authentication phase, the features extracted from the newly captured iris image are matched against those stored in the database. Most of the metrics used to quantify similarities are based on the Hamming distance between the IrisCode representations of each eye. Lower distance values reflect higher similarity in the iris patterns.

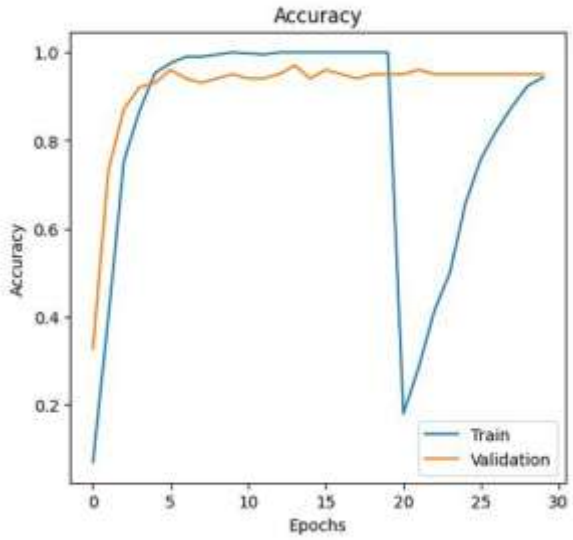
7. Decision / Result Generation A verification status is decided by the system, matching the score with a certain threshold; if the similarity score lies within an acceptable range, access is granted, otherwise, access is denied. This will establish a secure and reliable verification process.

IV. RESULTS AND DISCUSSION

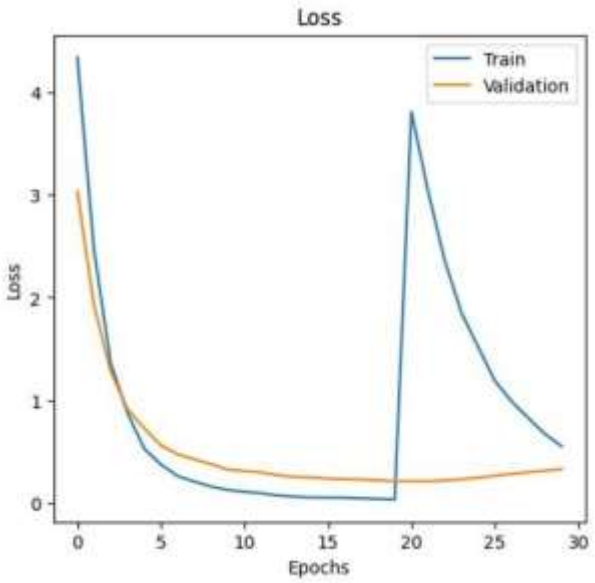
1. Confusion Matrix



2. **Accuracy Curves**



3. Loss Curves



4. Iris Recognition Testing

5. Matched Iris with Similarity Score

6. Unmatched Iris with Similarity Score

V. CONCLUSION

An iris recognition-based biometric authentication system has been proposed to improve the security of ATM transactions using deep learning with the aid of the MobileNetV2 approach. The proposed system successfully replaces the traditional card and PIN-based authentication systems using the uniqueness and steadiness of the iris patterns.

The proposed approach makes use of the preprocessing and segmentation steps for the precise extraction of the iris region and the transfer learning approach for efficient learning and classification. The experimental results with the aid of the confusion matrix validate the effectiveness and robustness of the proposed method.

The proposed system using the lightweight MobileNetV2 approach is able to be implemented in real-time at an ATM system. Future plans include real-time implementation, live iris detection, and the use of multi-biometric modalities.

VI. REFERENCES

1]. Irum Ashraf, “Enhancing ATM Security System by Using Iris (Eye) Recognition” American Journal of Geospatial Technology (AJGT) 2024.

2]. Joans R, Priyadharshini K, Iswarya A M, Shwetha R, Dr. P. Gokulakrishna, “ATM Security System with IRIS Recognition” International Research Journal of Modernization in Engineering Technology and Science 2022.

3]. A. Darthi Vincy, S. Sathana, “Recognition Technique for ATM based on IRIS Technology” International Journal of Engineering Research and Technology 2019.

4]. Rame Gowda M, Vandana R, “ATM Security Using Eye and Facial Recognition System” International Journal of Research Publication and Reviews 2024.

5]. Hafzulha Ozgur, Yunus Emre Selcuk, “Authentication in ATM / ITM Machines Using IRIS Recognition Biometrics” Department of Computer Engineering, Yıldız Technical University, Istanbul, Turkey 2023.