Inclusive Iris Recognition System For ATM

Vidya N. Waghchoure
Lecturer,*Department of* Computer Technology
K K Wagh Polytechnic Nashik
India
ajjadhav@kkwagh.edu.in

Kshitij D.Jadhav ,
Student, *Department of* Computer Technology
K K Wagh Polytechnic Nashik
India
kshitijadhav31@gmail.com

Atharva J.Morkar,
Student, *Department of* Computer Technology
K K Wagh Polytechnic Nashik
India
atharvamorkar04@gmail.com

Shreyas L.Lokhande ,
Student, *Department of* Computer Technology
K K Wagh Polytechnic Nashik
India
shreyaslokhande009@gmail.com

Tanmay S.Kolhe,
Student, Department of Computer Technology
K K Wagh Polytechnic Nashik
India
tanmaykolhe16@gmail.com

***Abstract*—With the increasing concerns over ATM fraud, traditional PIN-based authentication methods have become vulnerable to security threats such as skimming, phishing, and identity theft. This project proposes an Iris Recognition System for ATM Transactions to enhance security and provide a PIN-less, biometric-based authentication mechanism.**

Iris recognition, being one of the most reliable biometric identification techniques due to its unique and stable patterns, ensures only authorized users can access their bank accounts. The system consists of two major components: User Enrollment and Authentication. During enrollment, a user's iris is scanned and stored in a secure database using advanced image processing and machine learning techniques. During authentication, the ATM captures a live iris image and matches it with stored patterns using deep learning algorithms. If the authentication is successful, users can perform banking transactions such as cash withdrawals, deposits, and balance inquiries. The system also integrates security features like multi-factor authentication, fraud detection alerts, and AES-encrypted data transmission to prevent unauthorized access.

Keywords *— Iris Recognition, Iris Code, Iris matching, ATM Security, Customer Identity Verification, Secure Banking, Voice command.*

I. INTRODUCTION

In today's digital banking era, ATM security has become a critical concern due to increasing fraud, including PIN theft, card skimming, and identity fraud. Traditional ATM authentication methods rely on PINs and cards, which can be easily compromised. To overcome these vulnerabilities, biometric authentication, particularly iris recognition, offers a more secure, reliable, and fraud-resistant approach.

Iris recognition is considered one of the most accurate biometric authentication techniques due to the uniqueness, stability, and complexity of iris patterns. Unlike fingerprints, which can wear out or be altered, the iris remains unchanged throughout a person's lifetime, making it an ideal choice for high-security applications such as ATM transactions. The proposed system integrates iris-based authentication into ATMs, allowing users to securely access their accounts without needing a PIN or physical card.

The system operates in two phases:

- User Enrollment: The user's iris is scanned and stored securely in the system's database.
- User Authentication: During an ATM transaction, the user's iris is scanned and compared with stored biometric data. If a match is found, access is granted.

The proposed system utilizes OpenCV for image processing, TensorFlow/Keras for deep learning-based iris verification, and a secure backend with Django/Flask and MySQL/MongoDB. Additionally, security measures such as AES encryption, fraud detection alerts, and multi-factor authentication are incorporated to enhance protection.

By implementing iris recognition in ATMs, this system aims to eliminate ATM fraud, improve user convenience, and provide a highly secure banking experience. This biometric authentication method ensures that only the rightful account owner can perform transactions, making ATM systems more resilient to cyber threats and unauthorized access.

II. RELATED WORK

Several research studies and technological advancements have explored the integration of biometric authentication in banking systems, particularly iris recognition for ATM security. The effectiveness of iris biometrics has been widely recognized due to its uniqueness, stability, and resistance to forgery, making it a preferred choice over traditional authentication methods such as PINs and fingerprints.

1. Biometric Authentication in Banking Systems

Previous studies have examined various biometric techniques for ATM security, including fingerprint recognition, facial recognition, and vein pattern analysis. However, these methods have limitations. Fingerprint scanners can be affected by dirt or injuries, while facial recognition may struggle in different lighting conditions or with aging effects. Research has shown that iris recognition outperforms other biometric methods in terms of accuracy, security, and robustness, as highlighted in studies such as:

Daugman's Iris Recognition Algorithm (1993) – One of the most widely used iris recognition methods, based on Gabor wavelet transformations and Hamming distance for feature matching.

Deep Learning-Based Iris Recognition (Recent Advancements) – Machine learning and convolutional neural networks (CNNs) have significantly improved the accuracy and speed of iris recognition systems.

2. Iris Recognition in ATM Systems

Several research papers and projects have proposed ATM security enhancements using iris recognition. For example:

A Study on ATM Security using Iris Biometric Authentication (IEEE, 2020) – This study demonstrated that iris authentication significantly reduces ATM fraud and unauthorized access.

Biometric-Based ATM Security System (Elsevier, 2021) – This research highlighted the advantages of combining iris recognition with multi-factor authentication for enhanced security.

3. Challenges and Advancements in Iris Recognition

Although iris recognition is one of the most secure biometric methods, it faces challenges such as environmental lighting conditions, camera quality, and real-time processing speed. Recent improvements in deep learning-based iris recognition, edge detection algorithms, and infrared imaging have helped mitigate these challenges.

Security Method	Strength	Weakness
PIN-Based Authentication	Simple, widely used	Easily stolen, vulnerable to phishing & skimming
Iris Recognition	Highly accurate, stable, difficult to forge	Requires high-quality cameras, slightly expensive

III. IMPLEMENTATION

The implementation of the Iris Recognition System for Secure ATM Transactions involves several key components, including image acquisition, preprocessing, feature extraction, matching algorithms, and secure transaction processing. The system is designed to enhance ATM security by replacing traditional PIN-based authentication with iris biometrics.

System Architecture

The system follows a client-server architecture, where the ATM serves as the client and the bank's secure server handles authentication and transaction processing. The key modules include:

User Enrollment Module – Captures and registers a user's iris pattern.

Authentication Module – Compares the captured iris with the stored pattern.

Transaction Module – Allows users to perform banking operations.

Security & Fraud Detection Module – Monitors for unauthorized access attempts.

Technology Stack:

Component: Technology Used

Frontend (ATM UI): HTML, CSS, JavaScript (React/Angular),.net

Backend (Server & APIs): Net or Python or Node.js

Database: MySql / MySQL / MongoDB (Secure storage for iris data)

Iris Recognition: Deep Learning algorithm / Mantra IRIS MIS100V2

Security: AES Encryption, SSL/TLS for secure data transfer.

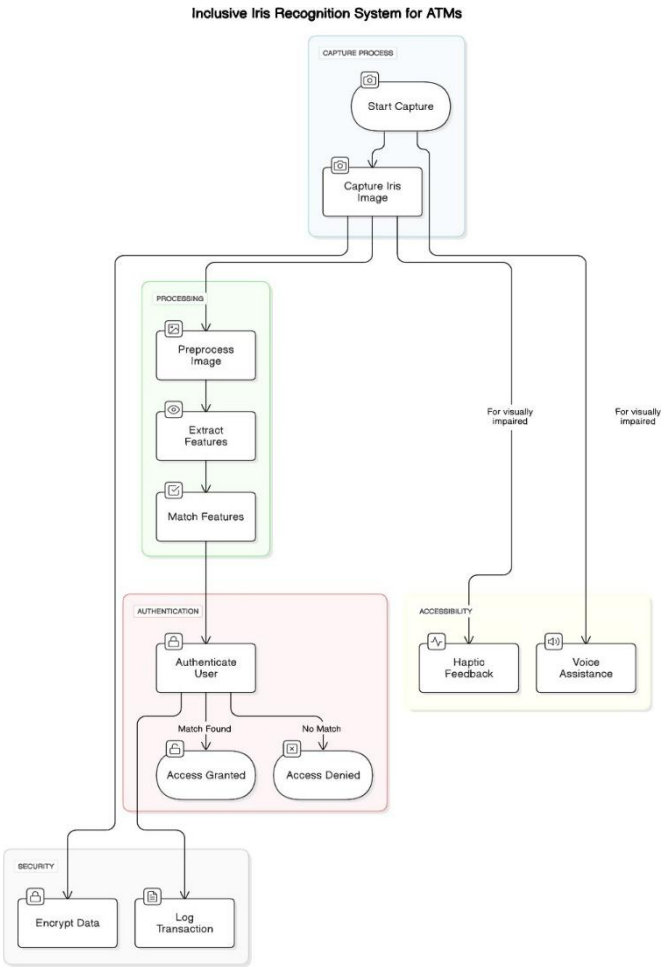

Fig. 1. System Architechure diagram for Inclusive Iris Recognition System for ATM

IV. COMPONENTS

System Components

The system consists of various hardware and software components working together to enable secure ATM transactions using iris recognition.

Hardware Components

Component & Description

ATM Machine: Standard ATM setup with a modified interface for biometric authentication.

Iris Scanner (Infrared Camera): Captures high-resolution iris images for authentication.

Processing Unit (ATM Server): Handles iris image processing, authentication, and transaction execution.

Bank Server (Centralized Database): Securely stores iris templates and transaction records.

Network Communication Module: Ensures secure data transfer between ATM and bank servers

Fig. 2. Mantra Iris MIS 100 V2

III. CONCLUSION

The implementation of an Iris Recognition System for Secure ATM Transactions provides a highly secure and efficient alternative to traditional PIN-based authentication. By leveraging biometric verification, the system eliminates risks such as card skimming, PIN theft, and identity fraud, ensuring that only the legitimate account holder can access their funds.

Through the use of advanced image processing, deep learning models, and encryption techniques, the system achieves high accuracy, fast authentication, and enhanced security. The integration of OpenCV for image preprocessing, TensorFlow/Keras for deep learning-based recognition, and AES encryption for secure data storage ensures robust performance and protection against cyber threats.

IV. REFERENCES

- Daugman, J. (1993) – "High Confidence Visual Recognition of Persons by a Test of Statistical Independence" IEEE Transactions on Pattern Analysis and Machine Intelligence, 15(11), 1148-1161.
  This paper introduced the fundamental iris recognition algorithm based on Gabor wavelets and Hamming distance.
- Wildes, R. P. (1997) – "Iris Recognition: An Emerging Biometric Technology" Proceedings of the IEEE, 85(9), 1348-1363.

Discusses different iris recognition methodologies and their applications in security systems.

- Bowyer, K. W., Hollingsworth, K., & Flynn, P. J. (2008) – "Image Understanding for Iris Biometrics: A Survey" Computer Vision and Image Understanding, 110(2), 281-307.
  A comprehensive survey on iris recognition techniques, challenges, and accuracy improvements.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004) – "An Introduction to Biometric Recognition" IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.
  Explains the role of biometrics in security systems, including fingerprint, facial, and iris recognition.
- Kumar, A., & Passi, A. (2010) – "Comparison and Combination of Iris and Fingerprint Biometrics for Identity Verification" Pattern Recognition Letters, 31(20), 1332-1339.
  Examines the accuracy and reliability of iris recognition compared to other biometrics.
- IEEE Conference Paper (2020) – "Enhancing ATM Security Using Iris Biometric Authentication" Proceedings of the IEEE International Conference on Cyber Security and Biometric Systems.