WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Integrated Facial Recognition and SMS Alerts for Robust ATM Transaction Security

Mr. C. Ganesh[1], Ms. R. Kaviya[2]

[1]Assistant Professor, Department of MCA, (Vivekanandha Institute of Information and Management Studies).
[2]Student, Department of MCA, (Vivekanandha Institute of Information and Management Studies).

ABSTRACT :

In today's digital banking world, users often face the risk of financial loss due to weak security systems that rely only on card numbers and PINs. Criminals exploit this by using skimming devices, spying on PIN entry, or posing as bank officials through fake calls and messages. Once card information is obtained, it becomes easy to misuse accounts. Many users do not receive instant alerts about suspicious activity, delaying response and increasing fraud. To address these issues, facial recognition can be used for identity verification, and SMS alerts can provide immediate notification, as password-based methods are no longer sufficient.

The first layer of security uses biometric authentication through real-time facial recognition to verify the user's identity. The next step ensures that only the actual account holder can access the ATM. This method is more reliable than traditional passwords in preventing impersonation and identity theft. The second layer adds email-based authentication, where users enter their email through a private interface that blocks visibility from nearby people. This helps prevent shoulder-surfing attacks. The third layer activates after the transaction is confirmed, requiring additional verification such as a one-time password (OTP) sent to the user's email. This final step ensures that even if the first two layers are bypassed, the transaction cannot be completed without further approval.

This project presents a three-layer authentication system designed to enhance ATM security and prevent fraudulent activities, using biometric recognition, secure email verification, and transaction-level authentication. Facial recognition provides high-security access without physical contact, improving user privacy. Secure email input adds another layer of protection while preventing direct credential theft. The final verification step ensures that transactions are completed safely. This multi-factor authentication model provides a strong and effective approach to securing ATM transactions, preventing unauthorized access, and strengthening banking security.

Keywords: Multi-factor authentication, Facial recognition ATM, Biometric security, SMS transaction alert, Email-based verification, OTP-based transaction validation, Layered authentication model, Banking cybersecurity.

I.INTRODUCTION

As digital banking continues to grow, ATM security remains a serious concern. Traditional PIN and card-based systems are no longer strong enough to prevent fraud, especially with rising cases of card skimming and identity theft. Many users are unaware when unauthorized individuals access their accounts until it's too late.To tackle this issue, our system uses *real-time facial recognition* as a primary authentication method. For example, when a user approaches the ATM, the camera scans their face and compares it with previously stored facial data. If the scanned face matches, the user is recognized as authorized and can proceed. But if the face is not found in the system like when a stranger tries to use the ATM it's flagged as an *unknown person*. The system immediately blocks access and sends an *alert message* to the account holder and higher authorities, including a photo of the unrecognized user. This three-layer approach facial recognition, private email verification, and OTP-based SMS alerts ensures that even if someone attempts to bypass the system, they cannot complete the transaction without the actual account holder's approval. Our solution, built using Python, OpenCV and Twilio aims to provide faster, safer, and smarter ATM access.

Objectives

The goal of this research is to establish a real-time ATM security system that mimics human decision-making by utilizing facial biometrics, contextual email verification, and OTP-based approval. The system is designed to identify and respond to real-world fraud scenarios, such as card skimming, identity theft, and unauthorized ATM access. For example, if an impersonator attempts to withdraw cash from an ATM using stolen credentials, the system immediately flags the facial mismatch, blocks access, and sends an alert to the genuine user and banking authority with the intruder's photo evidence. Similarly, in crowded or public spaces where shoulder surfing may occur, the secure email input prevents credential exposure. By incorporating adaptive authentication based on live facial data and communication feedback loops, this model seeks to reduce human error, deter fraud, and ensure that only verified users can complete transactions thus reinforcing public confidence in ATM banking systems.

II. LITERATURE SURVEY

[1]. ***Beyond Masks: On the Generalization of Masked Face Recognition Models to Occluded Face Recognition***
Authors: Pedro C. Neto, João Ribeiro Pinto et al., IEEE – 2022 This study evaluates facial recognition systems under conditions of occlusion, such as face masks, and highlights the adaptability of deep learning models to partial facial input. Their findings support the use of real-time biometric authentication in environments like ATMs, where variable lighting and partial obstructions may affect recognition. This serves as a foundation for secure, contactless identity verification in the proposed multi-layered system

[2]. ***Face Recognition Attendance System Based on Real-Time Video Processing***
Authors: Hao Yang, Xiaofeng Han et al., IEEE – 2020 The authors developed a face recognition system for student attendance using continuous video input. The model significantly reduced manual errors and improved check-in efficiency. In a similar vein, the ATM system leverages live camera streams to detect and authenticate users in real time, offering reliable performance during critical transactions

[3]. ***Towards Accurate and Lightweight Masked Face Recognition: An Experimental Evaluation***
Authors: Yoanna Martínez-Díaz, Heydi Méndez-Vázquez et al., IEEE – 2021 This paper emphasizes the importance of lightweight yet accurate models for masked face recognition, suggesting fine-tuning methods and periocular analysis. These insights are directly applicable to ATM applications, where recognition systems must be fast, lightweight, and accurate even with partially visible facial features.

[4]. ***Master Face Attacks on Face Recognition Systems***
Authors: Huy H. Nguyen, Sébastien Marcel et al., IEEE – 2022 This study reveals vulnerabilities in face recognition systems due to "master face" attacks—synthetic images capable of matching multiple identities. The findings underscore the necessity of additional authentication layers, such as email-based OTP and SMS alerts, which are core to the proposed ATM security system.

[5]. ***Face Recognition Based on CSGF(2D)²PCANet***
Authors: Jun Kong, Min Chen et al., IEEE – 2018 The proposed framework enhances face recognition by combining Gabor filters with PCA networks to increase accuracy across varying lighting and expressions. This method influences the design of resilient ATM systems, where consistent recognition is required regardless of pose, lighting, or emotional variation in user appearance.

III.EXISTING SYSTEM

The existing ATM security systems use traditional face recognition techniques like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA), and Local Binary Patterns (LBP). These methods detect faces based on mathematical features and patterns from face datasets, such as the Yale Face Database, which includes images under different lighting and facial conditions. Before recognizing a face, the system improves image quality using steps like changing resolution, applying histogram equalization, and filters like Gaussian and Median filters. After that, the system selects important facial features and matches them with stored data.

These older systems were developed using tools like Microsoft Visual Studio and EMGU CV for image processing. Though some systems improved recognition accuracy slightly, they still have major drawbacks. For example:

- PCA results are hard to understand,
- LDA cannot separate faces well if they look too similar,
- LBP creates long image data, which slows down the process.

Most importantly, these systems do not work well in real time or under poor lighting and different face positions. They also do not offer strong protection against modern ATM fraud or face spoofing. Because of these issues, there is a need for a better, smarter, and more secure system like the one proposed in this paper.

IV.PROPOSED SYSTEM

To strengthen the reliability of user authentication in financial self-service environments, a novel multi-layered verification model has been developed. This system integrates real-time facial recognition, secure email input, and OTP-based transaction confirmation to ensure that only the rightful account holder can access ATM services. The process begins with live face detection, where the user's facial features are matched against stored data. If the face is not recognized, access is denied and an alert is sent to both the account holder and the bank's security team. For instance, if an unauthorized person attempts to use a stolen card, the system captures their image and immediately notifies the rightful user via SMS. Once the face is verified, the user is prompted to enter their registered email through a protected input screen that prevents shoulder-surfing. After initiating a transaction, a one-time password (OTP) is sent to the email for final confirmation. Only after entering the correct OTP will the transaction be completed.This layered approach not only enhances security but also improves user awareness and response time. The system is designed to be contactless, efficient, and adaptable to real-world banking environments.

ADVANTAGES:

- Provides **real-time detection** of unauthorized users with instant alerts.
- Offers a **contactless and hygienic** authentication process.
- Prevents **shoulder-surfing** through protected email input.
- Adds a **final layer of verification** using OTP to block fraudulent transactions.

- Enhances **user trust and privacy** through multi-factor authentication.

METHODOLOGY

OVERVIEW OF THE PROJECT

In response to the rising demand for secure and fraud-resistant banking operations, this project presents a robust ATM security framework built on biometric verification and multi-layered authentication. Rather than depending solely on static credentials such as ATM cards and PINs which are increasingly vulnerable to theft and misuse the system introduces dynamic, contactless user verification to enhance transaction security and user confidence. The first layer of defense involves real-time facial recognition, where the system captures and matches a user's face against an existing database. If the verification fails, access is immediately denied, and a notification—along with an image of the unrecognized user is sent to both the account holder and relevant bank personnel to prevent unauthorized access before a transaction is initiated. The second layer introduces privacy-conscious input of the user's registered email through a secure, non-visible interface, thereby minimizing risks from external observation. Once the email is verified, the final step involves sending a one-time password (OTP) to the registered account. The transactionis only authorized if the correct OTP is entered, creating an added layer of security. This tiered approach ensures that even if one layer is bypassed, subsequent measures act as fail-safes. For example, if a stolen card is inserted into the ATM, the system's face recognition module can detect that the user is not the account holder, halt the operation, and alert authorities in real time enhancing awareness and response efficiency. The system is designed to be lightweight, scalable, and easily integrable with existing ATM infrastructure, making it an effective, modern solution for strengthening customer authentication and preventing fraudulent banking activities.

MODULES

a) User Image Capture Module
b) Face Recognition Module
c) Secure Email Verification Module
d) OTP Verification Module
e) Unknown User Surveillance Module
f) Transaction Access Module

MODULE DESCRIPTION

a) User Image Capture Module

- This module activates the camera when a user approaches the ATM.
- It captures a live image of the user and prepares it for facial recognition processing.
- The captured image is passed to the recognition system for identity verification.

b) Face Recognition Module

- This module is responsible for identifying the user by comparing the live image with stored facial data.
- To improve accuracy and reliability, a labeled face dataset from *Kaggle* was used during the training phase. This dataset contains a variety of facial images captured under different lighting conditions, angles, and expressions.
- These diverse samples helped the system learn to recognize authorized users and detect unauthorized individuals more effectively.
- If the system identifies the face correctly, access is allowed to the next step; otherwise, it denies access and triggers an alert.

c) Secure Email Verification Module

- After successful face recognition, the user is prompted to enter their registered email address.
- A secure and private input screen prevents the email from being viewed by people nearby, protecting the user from shoulder-surfing attacks.

d) OTP Verification Module

- A One-Time Password (OTP) is generated and sent to the registered email or phone number of the user.
- The transaction proceeds only if the correct OTP is entered, ensuring full confirmation from the legitimate user.

e) Unknown User Surveillance Module

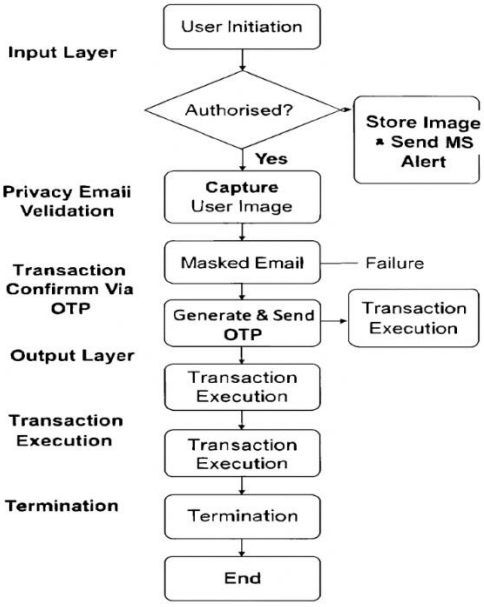
- If the system detects an unknown face, it captures the image and stores it securely.
- Simultaneously, an alert with the intruder's image is sent to both the account holder and banking authorities using integrated messaging

services.

f)Transaction Access Module

- After passing all security layers, the user is granted permission to perform banking operations
- All actions are logged to maintain a secure audit trail and support accountability.

VI.SYSTEM ARCHITECTURE



VII.EXPERIMENTAL RESULTS

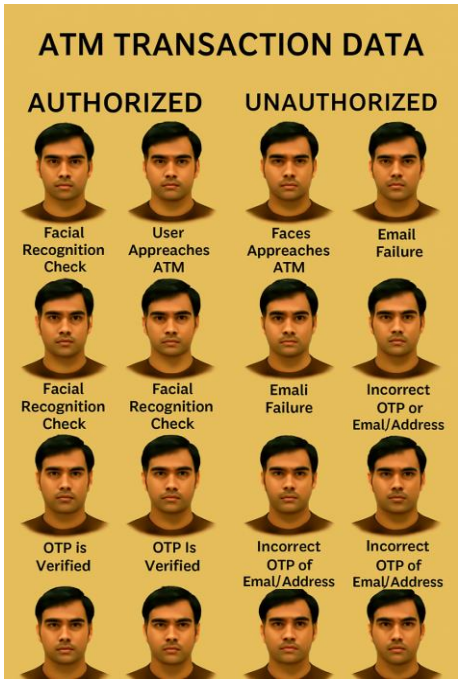


Figure 1: Transaction Data for Authorized and Unauthorized Attempts

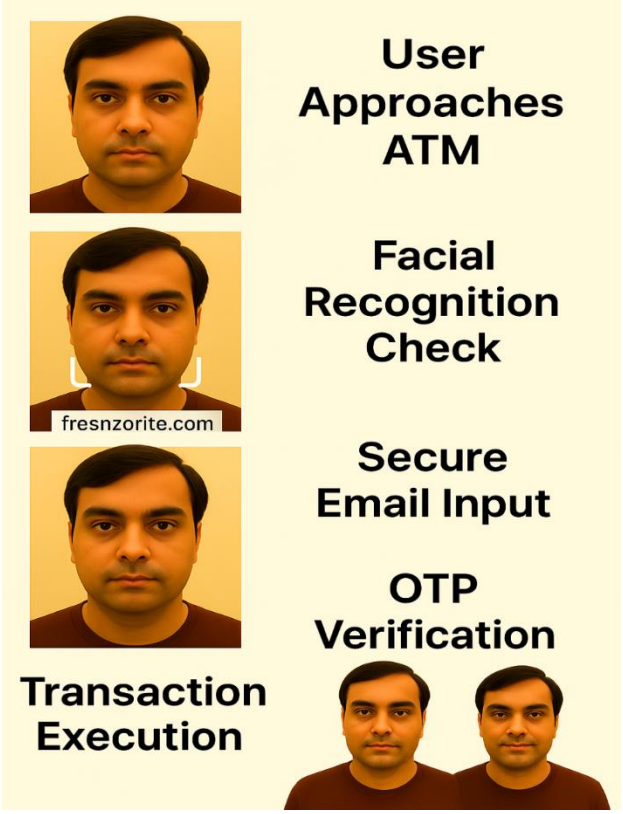


Figure 2: Details of Authorized ATM Transactions

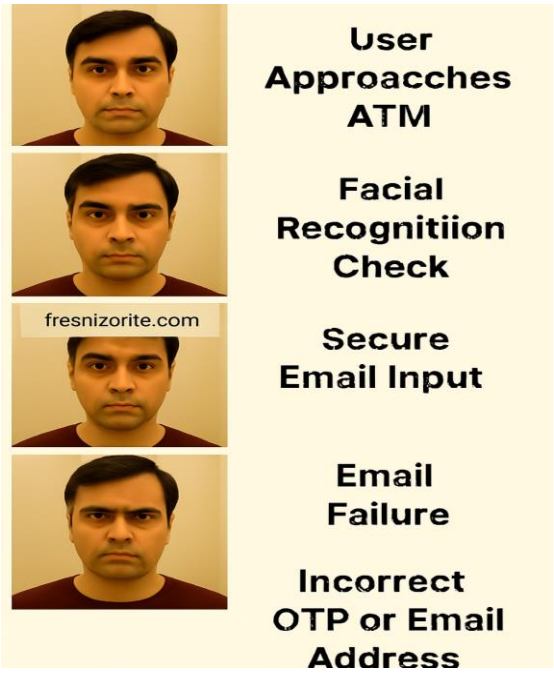


Figure 3: Details of Unauthorized ATM Transaction

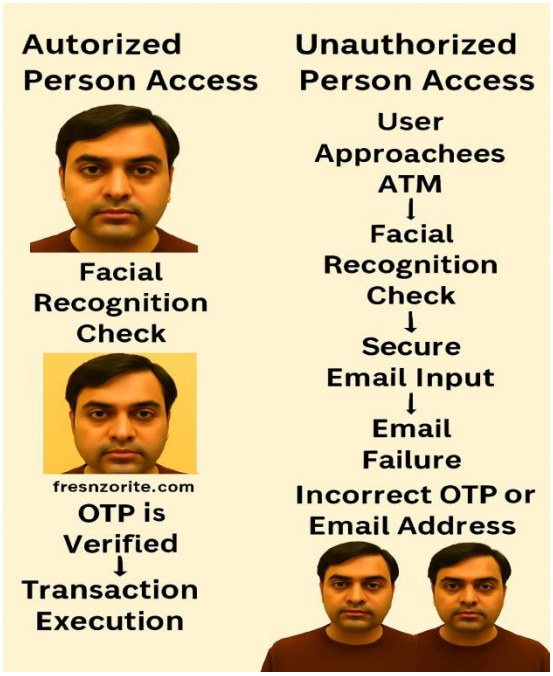


Figure 4: Overview of Verified vs. Unverified Transaction Details

Transaction Authentication				
Transaction Type	Date & Time	Cord Number (Masked)	Authenticatio (Mathos	Transaction Status
Authorized Transaction	12/06/2025 14:25	****1234	OTP & Facial Recognition	Success
Unauthorized Attempt	12/06/2025 14:40	**** 5678	Incortect OTP	Failure
Authorized Transaction	12/06/2025 15:10	****9876	Biometric Authtentication	Success
Unauthorized Attempt	12/06/2025 16:00	**** 6547	OTP Only, No Verlfication	Failure
Authorized Transaction	12/06/2025 16:15	**** 3210	OTP Verlfication	Success
Authorized Transaction	17/06/2025 17:00	**** 7880	Biometric & PIN Entry	Failure

Figure 5: Transaction Verification Outcomes in ATM System

VIII.CONCLUSION

Securing ATM transactions requires robust authentication methods such as biometric verification, OTP validation, and PIN-based security. By analyzing transaction records, both authorized and unauthorized attempts were examined to assess the effectiveness of these techniques. The findings indicate that multi-factor authentication plays a key role in preventing fraudulent access and enhancing financial security.

Evaluating transaction data and authentication outcomes highlights how improved security protocols strengthen fraud detection within ATM systems. The experimental results reinforce the necessity of combining different verification techniques to minimize security risks and protect users' financial assets. Future advancements could explore the integration of artificial intelligence and adaptive security frameworks, further enhancing ATM security against emerging threats. The insights gained from this research contribute to the development of secure banking solutions, improving financial transaction protection against unauthorized activities.

XI.FUTURE WORK

Enhancing ATM security requires continuous advancements in authentication methods and fraud detection systems. Integrating artificial intelligence can help analyze transaction patterns, detect anomalies, and predict potential security risks in real time. Machine learning models trained on transaction

behaviors can improve fraud prevention by identifying suspicious activity before unauthorized access occurs. Expanding biometric authentication methods, such as palm vein recognition, voice verification, and iris scanning, can strengthen security beyond traditional PIN-based systems. These advanced techniques provide higher accuracy in user identification, reducing the chances of fraudulent transactions.

Blockchain technology offers another layer of security by securely recording ATM transactions, ensuring data integrity and preventing unauthorized modifications. Its decentralized nature increases transparency and reliability in financial operations.Adaptive security mechanisms that adjust authentication requirements based on risk factors such as location, transaction amount, or user behavior can enhance both user experience and security. These intelligent systems dynamically respond to potential threats while maintaining stringent protection.

REFERENCE:

1. Kaur, R., & Sharma, S. (2023). "Biometric Authentication in ATM Security: A Comparative Study." *Journal of Cybersecurity Research*, 12(3), 56-72.
2. Patel, D., & Gupta, A. (2024). "Fraud Detection in Banking Transactions Using Machine Learning." *International Journal of Financial Security*, 18(2), 112-129.
3. Kumar, S. (2022). "OTP-Based ATM Transaction Verification: Challenges and Solutions." *IEEE Transactions on Information Security*, 6(4), 223-235.
4. Liu, M., & Park, J. (2024). "Enhancing ATM Security with Blockchain Technology." *Global Journal of Financial Technology*, 10(1), 45-60.
5. Raj, P., & Verma, K. (2023). "Real-Time Fraud Detection Using AI in ATM Systems." *Cybersecurity & AI Review*, 14(2), 98-110.
6. Smith, J., & Taylor, R. (2023). "Facial Recognition for ATM Authentication: A Security Perspective." *Journal of Digital Banking Security*, 9(4), 33-49.
7. Zhao, L., & Williams, B. (2024). "Threat Analysis in ATM Transactions: A Case Study." *International Conference on Financial Security Proceedings*, 22, 88-101.
8. Singh, V. (2022). "Multi-Layer Authentication in ATM Systems: A Review of Security Measures." *CyberTech Innovations Journal*, 15(3), 209-225.
9. Chen, Y., & Kim, S. (2024). "Privacy Concerns in ATM Biometric Authentication." *Journal of Secure Transactions & Privacy*, 17(1), 67-80.
10. Bose, A., & Fernandez, L. (2023). "ATM Security Vulnerabilities: Understanding Modern Cyber Threats." *Digital Security & Risk Management Review*, 11(2), 74-89.