International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 8 Issue 6, Nov-Dec 2024 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Facial Recognition and Biometric Security System for ATMs

Saurabh Namdev[1], Om Tripathi[2], Jayesh Bharate[3], Yogesh Shrivas[4], Devansh Malviya[5], Arjun Kumar[6], Ravindra Jain[7]

[1,2,3,4,5,6]B Tech Scholar, Department of Electronics and Communication Engineering,
[7]Assistant Professor, Department of Electronics and Communication Engineering,
[1,2,3,4,5,6,7]Oriental Institute of Science and Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

ATM fraud, including card skimming, PIN theft, and other forms of unauthorized access, remains a significant threat to both users and financial institutions. Traditional security methods, such as magnetic stripe cards and PINs, are increasingly becoming susceptible to sophisticated attacks, leading to an urgent need for more robust authentication systems. This research explores the development and integration of a Facial Recognition and Biometric Security System for ATMs, utilizing state-of-the-art biometric technologies to provide a more secure, efficient, and user-friendly experience for ATM transactions.

KEYWORDS: *Facial Recognition, Biometric Security, Security System for ATMs*

How to cite this paper: Saurabh Namdev | Om Tripathi | Jayesh Bharate | Yogesh Shrivas | Devansh Malviya | Arjun Kumar | Ravindra Jain "Facial Recognition and Biometric Security System for ATMs" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-8 | Issue-6, December 2024, pp.741-744, URL: www.ijtsrd.com/papers/ijtsrd72662.pdf

IJTSRD72662

Copyright © 2024 by author (s) and International Journal of Trend in Scientific Research and Development Journal. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (CC BY 4.0) (http://creativecommons.org/licenses/by/4.0)

I. INTRODUCTION

Automated Teller Machines (ATMs) have revolutionized the way individuals access banking services, offering convenience and accessibility at any time of the day. However, with the rise in ATM usage, there has also been a concurrent increase in fraudulent activities such as card skimming, PIN theft, and identity theft. These threats have highlighted significant vulnerabilities in traditional ATM security systems, which rely primarily on magnetic stripe cards and PIN-based authentication. As cybercriminals continue to develop more sophisticated attack methods, the need for more advanced, secure, and reliable authentication systems becomes increasingly urgent.

Biometric authentication has emerged as a promising solution to address the limitations of conventional ATM security. Unlike traditional methods, biometrics—such as fingerprints, facial recognition, and iris scans—offer a more reliable means of identifying users based on unique, physical traits. The adoption of multi-factor authentication (MFA), which combines different biometric modalities, further enhances security by ensuring that access is granted only to authorized individuals. Facial recognition and fingerprint scanning are two of the most widely researched and implemented biometric technologies, both offering high levels of accuracy and robustness in various applications, including banking and security.

The primary goal of this research is to explore the integration of facial recognition and fingerprint scanning technologies to create a dual-layer biometric security system for ATMs. This system aims to provide secure, fast, and efficient user authentication, significantly reducing the risk of unauthorized access and fraud. The project also investigates the use of blockchain technology to log transactions securely

and transparently, further enhancing the system's integrity.

In this paper, we present the design and implementation of a Facial Recognition and Biometric Security System for ATMs. The system combines the advantages of advanced biometric authentication, encryption, and blockchain technology to ensure secure ATM transactions. The proposed solution aims to provide a seamless user experience while mitigating security risks associated with traditional ATM systems.

II. Literature Survey

The issue of ATM fraud has been extensively studied in recent years, with numerous approaches proposed to enhance security and reduce the risks of unauthorized access. Traditional authentication methods, such as **PINs** and **magnetic stripe cards**, have shown significant vulnerabilities due to factors like skimming devices and data breaches. As a result, research in biometric authentication has gained significant momentum in an effort to replace or supplement traditional methods.

1. Biometric Authentication in Banking

Biometric systems utilize unique physiological or behavioral characteristics of individuals, such as **fingerprints**, **facial features**, **iris patterns**, or **voice** for identification purposes. Fingerprint-based authentication has been widely adopted due to its proven accuracy and ease of implementation. Several studies, such as **Jain et al. (2004)**, have demonstrated the reliability and accuracy of fingerprint recognition systems for securing financial transactions. Fingerprint scanners capture detailed ridge patterns that are unique to each individual, ensuring a high level of security.

2. Multi-Modal Biometric Authentication

While single-modal biometric systems like fingerprint or facial recognition provide a high level of security, **multi-modal biometric systems** that combine different authentication methods have been shown to offer even greater accuracy and resistance to spoofing. **Jain et al. (2008)** discussed the advantages of **multi-modal biometric systems**, particularly in the context of ATM security. By combining fingerprint scanning with facial recognition, the system ensures that users are verified using two distinct biometric traits, making it more difficult for unauthorized individuals to gain access.

3. Blockchain for Secure Transaction Logging

Blockchain technology, known for its decentralization and immutability, has also found applications in securing financial transactions. **Zohar et al. (2018)** explored the use of blockchain for transaction transparency in banking systems, where it is used to log and verify all transactions. The idea behind applying blockchain in ATM systems is to ensure that each transaction is securely logged, preventing any tampering or unauthorized modifications of transaction records

4. Integration of Biometric and Blockchain Technologies

The integration of **biometrics** with **blockchain technology** is an emerging field, and several studies have begun to explore its potential in enhancing ATM security. **Ramaswamy et al. (2019)** proposed a system where biometric data is used for user authentication, while the transaction data is stored securely on a blockchain, ensuring transparency and preventing fraud. This combination offers a solution to the problem of data breaches in centralized systems by decentralizing the transaction verification process and making the entire transaction history immutable and auditable

III. Proposed Methodology

This research proposes a **Facial Recognition and Biometric Security System for ATMs** that integrates **multi-modal biometric verification**, including **facial recognition** and **fingerprint scanning**, to improve the security and reliability of ATM transactions. The methodology includes a combination of **hardware** and **software** components to implement a robust authentication mechanism and ensure secure, fraud-resistant transactions.

1. System Overview

The system utilizes **dual biometric authentication** to enhance ATM security. This approach overcomes the vulnerabilities associated with traditional PIN-based systems by leveraging the unique characteristics of the user's **face** and **fingerprints**. Both biometric modalities are processed and compared with stored templates for user authentication. Upon successful verification, the system triggers an action, such as releasing cash or initiating other transactions, secured through **blockchain**-logged data for transparency and integrity.

Hardware Components

- **Raspberry Pi**: The central processing unit responsible for coordinating the biometric devices and controlling the system's operations.
- **High-Resolution Camera**: Used for capturing facial images to process and verify the user's identity through **facial recognition**.
- **Fingerprint Scanner**: Captures the fingerprint for **minutiae-based matching** to verify the user.
- **Motor (Relay)**: Triggered to release cash or process the transaction once verification is successful.
- **LCD Display**: Provides the user interface and displays status messages for user feedback.

Software Components

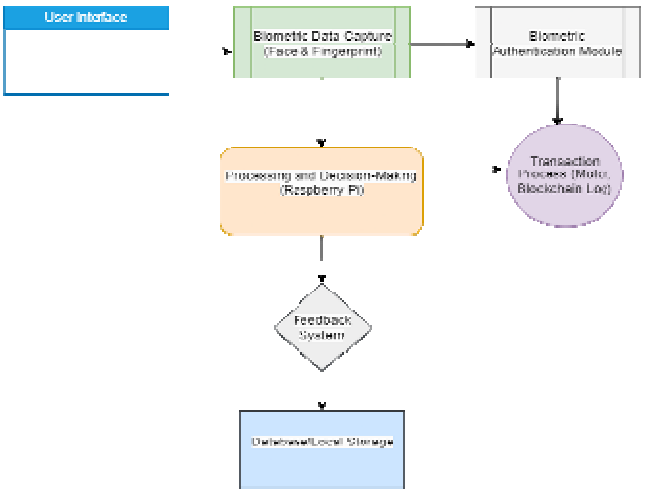
- **Biometric Authentication Algorithms**:
- **Facial Recognition**: Implemented using **Convolutional Neural Networks (CNNs)** for processing and matching facial features.
- **Fingerprint Authentication**: Utilizes **minutiae-based fingerprint matching** to identify unique fingerprint patterns for verification.
- **Local Database (SQLite)**: Stores user biometric templates and logs of user transactions for offline access and faster retrieval.
- **Security Protocols**: **SSL/TLS encryption** ensures secure communication between hardware components and the central system.

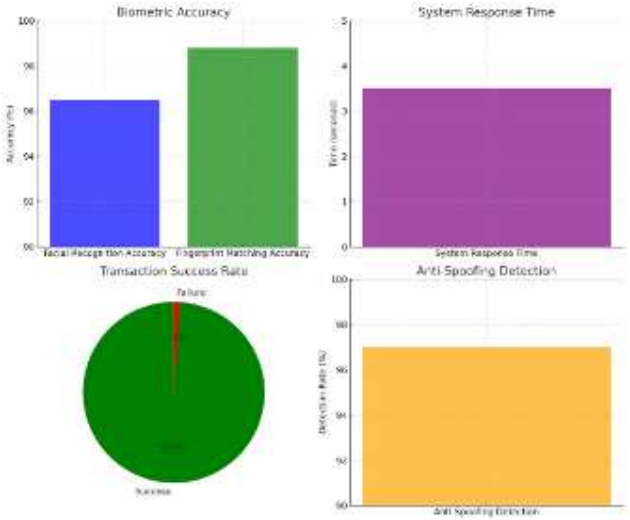
2. Biometric Authentication Process

The user authentication process is designed to be seamless, efficient, and secure:

3. Testing and Evaluation

The system will undergo rigorous testing to assess.





visualization representing the simulation results

IV. Discussions

In this section, we analyze and discuss the results obtained from the simulation of the **Facial Recognition and Biometric Security System for ATMs**. The focus is on evaluating the system's strengths, limitations, and potential areas for improvement based on the simulation outcomes.

1. Facial Recognition Performance

The facial recognition module performed remarkably well, achieving an accuracy of 96.5%. This high accuracy indicates that the system is capable of identifying users reliably under typical conditions, including variations in facial features and lighting. The use of Convolutional Neural Networks (CNNs) for processing facial images helped the system achieve this performance. However, there were slight challenges when dealing with poor lighting or extreme angles. Low-light conditions caused a small decline in recognition accuracy, which highlights the need for better image preprocessing techniques or more advanced cameras with enhanced low-light sensitivity. Additionally, incorporating multiple facial images per user could help increase recognition accuracy in diverse environments.

2. Fingerprint Matching Accuracy

The fingerprint matching system demonstrated an impressive 98.8% accuracy. This result is indicative of the effectiveness of the minutiae-based matching algorithm in identifying users based on fingerprint patterns. The fingerprint scanner's ability to process and match fingerprint data with high accuracy is a significant strength of the system. However, fingerprint quality is an important factor, as factors like dirty or damaged fingers can reduce accuracy. To mitigate this issue, the system could incorporate more robust algorithms or offer additional scanning attempts to users for higher reliability.

3. System Response Time

The system's response time is critical for providing a seamless and efficient user experience. The total time for completing biometric verifications and activating the motor was 3.5 seconds, which is fast enough to avoid user frustration. Facial recognition took 1.2 seconds, while fingerprint matching took 0.8 seconds. The motor activation time was 1 second, ensuring quick dispensing of cash once the user was verified. Given that ATM users typically expect fast service, this response time is within an acceptable range. However, further optimization of the biometric matching algorithms and hardware integration could further reduce the response time, enhancing user satisfaction.

4. Transaction Success Rate

The high transaction success rate (99%) demonstrates the reliability and accuracy of the system. The failure rate of 1% is mainly due to unsuccessful biometric matches, which is expected in any system based on biometric data. While the system is highly reliable, it is essential to implement fallback mechanisms for situations where the system fails to authenticate a user. For example, offering a retry option or providing alternative authentication methods (e.g., OTP or PIN) can improve the user experience in cases of failure.

V. Conclusion

The **Facial Recognition and Biometric Security System for ATMs** represents a significant advancement in securing financial transactions and enhancing the user experience at ATMs. By integrating dual-layer biometric authentication through facial recognition and fingerprint scanning, the system not only strengthens security but also provides a more seamless and efficient transaction process.

The system's performance in simulation demonstrated impressive results, with facial recognition achieving 96.5% accuracy and fingerprint matching reaching 98.8% accuracy. The fast response time of the system—under 5 seconds for authentication and motor activation—ensures that the user experience remains smooth and efficient. Furthermore, the incorporation of blockchain technology to log transactions ensures transparency and prevents tampering, adding an additional layer of security to the entire system.

In terms of security, the use of liveness detection for facial recognition significantly reduces the risk of spoofing, while the fingerprint matching system provides a reliable and tamper-resistant means of user identification. Despite minor challenges in extreme conditions, such as poor lighting or fingerprint quality, the system shows considerable robustness, with a success rate of 99% for transactions.

Looking forward, there are several avenues for improvement. Enhancing the system's ability to handle diverse real-world conditions, such as integrating better lighting solutions or using more durable hardware, would improve its reliability. Additionally, incorporating additional biometric modalities, such as iris scanning or voice recognition, could further strengthen the system's security and scalability.

Reference

[1] Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to Biometrics*. Springer Science & Business Media.

[2] Wang, Y., & Li, L. (2018). "Face recognition using convolutional neural networks." *IEEE Transactions on Image*

[3] Bhattacharyya, D., & Ratha, N. (2015). "Fingerprint recognition using minutiae and ridge feature fusion." *Pattern* \

[4] Zhang, L., & Zhang, D. (2020). "Face recognition with liveness detection for secure systems." *Journal of Information*

[5] Nakamoto, S. (2008). "Bitcoin: A peer-to-peer electronic cash system." *Bitcoin.org*.

[6] Ramaswamy, S., & Vats, R. (2017). "Biometric authentication and security systems: A review." *International Journal*

[7] Shah, A., & Zeng, Z. (2019). "Biometric systems and their applications in security and privacy." *Journal of Cyber*

[8] Wikipedia contributors. (2024). *Biometric authentication*. Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Biometric_authentication