JOURNAL OF MULTIDIMENSIONAL RESEARCH & REVIEW

http://www.jmrr.org Volume: 6, Issue: 1, April 2025 | ISSN: 2708-9452

Enhancing Financial Security with QR Code and Facial Recognition-Based Digital ATMs

Sajitha S
PG Student, Department of Computer Science and Applications
Vivekanandha College of Arts and Sciences for Women [Autonomous],Tiruchengode
Namakkal, Tamilnadu, India.
Premalatha M
Assistant Professor, Department of Computer Science and Applications
Vivekanandha College of Arts and Sciences for Women [Autonomous],Tiruchengode,
Namakkal, Tamilnadu, India.

Abstract

In the evolving landscape of digital banking, securing Automated Teller Machine (ATM) transactions is crucial. Traditional authentication methods, such as Personal Identification Numbers (PINs) and physical cards, are vulnerable to security breaches, including card skimming, phishing, and unauthorized access. This study proposes an innovative multi-factor authentication framework integrating Quick Response (QR) code scanning and Haar Cascade-based facial recognition to enhance ATM security. The system dynamically generates a unique QR code for each transaction, which users scan using their mobile devices. Subsequently, Haar Cascade-based facial recognition verifies user identity, providing a dual-layered authentication mechanism. This approach significantly mitigates risks associated with PIN theft, shoulder surfing, and cloned cards while enhancing user convenience. Preliminary evaluations indicate substantial improvements in security measures and user satisfaction. The findings suggest that implementing QR code and Haar Cascade-based authentication can elevate the safety, efficiency, and accessibility of ATM transactions, paving the way for the next generation of secure digital banking services.

Keywords:ATM Security, QR Code Authentication, Haar Cascade, Facial Recognition, Biometric Security, Digital Banking.

1 Introduction

Automated Teller Machines (ATMs) provide seamless access to financial services, including withdrawals, deposits, and fund transfers. However, traditional authentication methods relying on PINs and physical cards are susceptible to numerous security threats. Fraudsters use card skimming devices to steal card information and create duplicate cards, enabling unauthorized transactions. Additionally, cybercriminals carry out phishing attacks by deceiving users into revealing sensitive banking credentials through fake emails, websites, or messages. Another common tactic is shoulder surfing, where attackers closely observe users entering their PINs to gain unauthorized access to their accounts. To mitigate these vulnerabilities, biometric authentication has gained prominence as a secure alternative. Facial recognition, in particular, offers a non-intrusive and highly accurate method of verifying user identity. This paper presents an innovative ATM authentication system that combines Haar Cascade-based facial recognition and QR code verification to enhance security and user experience.

2 Literature Review

S. A. Sumathi et al. [1] developed a biometric ATM system utilizing fingerprint and iris recognition for secure authentication. Their method provides a reliable alternative to traditional PINs, reducing the risk of card theft and password guessing. However, the lack of facial recognition support limits its flexibility in dynamic scenarios such as contactless verification. Additionally, hardware requirements for iris scanners raise deployment costs. Though secure, the approach doesn't adapt well to real-time scenarios in high-traffic ATM environments. Furthermore, fingerprint sensors often struggle with wet or dirty fingers. The system emphasizes security but sacrifices user convenience in some cases.

M. Elangovan et al. [2] proposed QR code-based transaction authentication, primarily focusing on enhancing mobile banking security. The system generates unique QR codes for each session, reducing the risks of replay attacks. However, their method does not verify the user's identity biometrically, which may allow misuse if a QR code is accessed by someone else. The lack of integration with face or fingerprint recognition limits its security scope. While ideal for digital wallet-based apps, it lacks robustness when applied to ATM infrastructures. Their work provides a good base for contactless authentication but does not address user identification thoroughly. A. Prakash and S. Rajan [3] investigated facial recognition using the Haar Cascade algorithm for real-time surveillance and monitoring systems. Their work highlights the algorithm's efficiency under stable lighting conditions and its lightweight nature for embedded systems. However, Haar Cascades may struggle with facial detection in poor lighting or when the face is partially obscured. Their model is ideal for initial detection, not full authentication, as it lacks depth in feature analysis compared to deep learning approaches. Additionally, the approach does not combine with QR code technology, thus missing an opportunity for multi-factor authentication. It is suitable for rapid detection but not standalone ATM security. R. Kumar and D. Sharma [4] implemented a CNN-based facial recognition system for secure area access. Their work focused on improving the recognition rate in diverse environmental conditions. CNNs showed robustness to changes in angle and lighting, increasing accuracy. However, their application was primarily within secure office premises, not ATM kiosks, where variables like crowd density and privacy concerns arise. Their system does not integrate with other authentication methods like OTP or QR code, making it a single-point verifica-

tion model. It serves well for identity recognition but does not address transaction-level security or multi-step authentication needs in ATMs. N. Batra et al. [5] introduced a dual-factor authentication model combining OTP and mobile-based verification for ATM services. Their work emphasizes enhancing security by validating both device ownership and session identity. However, reliance on network availability for OTP delivery may delay transactions. Their model does not incorporate biometric verification, leaving gaps in confirming the actual user's identity. Additionally, their system's OTP delivery through SMS is vulnerable to SIM swap attacks. Though effective for session validation, the lack of face recognition support reduces the reliability of true user verification. Integration with facial biometrics could significantly improve security. T. Joseph et al. [6] explored QR-based login authentication for desktop banking applications, providing a touchless verification approach. Their system generates session-specific QR codes that users scan using authorized mobile apps. Although it secures login credentials from keyboard loggers and phishing, it still lacks user identity confirmation. The system does not verify whether the scanner is the actual account holder. Its effectiveness is reduced if QR codes are intercepted or shared. It is more appropriate for desktop or mobile apps than ATMs due to device dependency. Integrating face recognition could prevent unauthorized QR use and enhance security.

3 Experimental Methodology

The proposed multi-factor authentication system leverages a two-stage security process combining QR code-based session verification with real-time facial recognition using the Haar Cascade classifier. This section outlines the individual modules and their integration in the authentication pipeline.

3.1 QR Code Authentication

The system employs dynamically generated QR codes to initiate and validate ATM sessions. Each QR code is unique and time-bound, containing encoded session-specific metadata such as timestamp, transaction ID, and user identifier. This eliminates the dependency on physical ATM cards and PINs, which are vulnerable to skimming and shoulder surfing.

Upon launching a transaction, the ATM generates a one-time QR code and displays it on the screen. The user scans the QR code using a secure mobile banking application. This scan acts as the first authentication factor, establishing a secure session handshake between the user and the ATM.

3.2 Haar Cascade for Facial Recognition

The second layer of authentication involves facial recognition powered by the Haar Cascade classifier—a machine learning-based object detection technique introduced by Viola and Jones. The classifier uses a cascade function trained on positive and negative images to efficiently identify human faces.

Key attributes of the Haar Cascade algorithm include:

- **Haar-like Features:** These are digital image features used to detect object edges, lines, and gradients.

- **Integral Image Technique:** Allows for fast computation of feature values.
- **Cascade Classifier:** Organizes weak classifiers into increasingly complex stages to quickly discard non-facial regions.

This method is optimized for low-power devices and performs real-time detection with minimal latency.

3.3 Multi-Factor Authentication (MFA) Workflow

The complete authentication workflow consists of the following sequential steps:

1. **Transaction Initiation:** User selects 'Start Transaction' on the ATM interface.
2. **QR Code Generation:** ATM dynamically generates a one-time session QR code.
3. **Mobile Scan:** User scans the QR using their mobile banking application to validate session identity.
4. **Facial Capture:** ATM webcam captures the user's facial image in real time.
5. **Facial Verification:** Haar Cascade algorithm analyzes the facial image and checks for a match against the user profile.
6. **Access Decision:** If both QR and facial authentication succeed, access is granted; otherwise, a security alert is triggered.

4 Preprocessing

Effective preprocessing improves the accuracy and efficiency of facial recognition. The following steps are applied sequentially:

Grayscale Conversion:The input RGB image is converted to a single-channel grayscale image to reduce computational complexity. Since color is not critical for face detection, grayscale images simplify processing without losing structural facial information.

Histogram Equalization:This technique enhances contrast by redistributing image intensity values. It ensures better differentiation between facial regions (e.g., eyes, nose, mouth), especially under poor lighting conditions, by amplifying pixel intensity differences.

Face Normalization:Normalization involves aligning facial features to a canonical position (e.g., centering the eyes or mouth). This reduces pose variation and improves recognition consistency by ensuring the facial image conforms to a standard layout.

Segmentation:Segmentation is a critical preprocessing stage used to isolate facial regions from the background, improving model focus and reducing noise.

Face Detection:The Haar Cascade classifier identifies and localizes the face region within the image. This process filters out irrelevant background areas and outputs bounding boxes that encapsulate facial features.

Background Removal:After detecting the face, all other regions in the image are masked or cropped out. This ensures that subsequent feature extraction operates solely on relevant data, improving speed and reducing false positives during recognition.

5 Feature Extraction

Feature extraction transforms the normalized facial image into a compact, descriptive representation that facilitates matching and classification.

Haar-like Feature Computation:Facial features are extracted based on Haar-like templates such as edge detectors, line detectors, and rectangular intensity differences. These features are calculated over various scales and positions across the facial region.

Feature Selection:From the large pool of Haar features, only the most discriminative ones are selected using AdaBoost-based training. This improves performance by focusing on the features that best differentiate between authorized and unauthorized users.

Pattern Learning:The selected features are passed to a trained classification model that learns to distinguish facial patterns of registered users. The model stores a compact face signature for each user and compares incoming faces for verification. This ensures robustness to facial expression changes, aging, and minor lighting variation.

Authentication Decision: If the extracted features closely match the stored user profile, the system classifies the attempt as legitimate. Otherwise, it rejects the attempt or triggers an alert for potential spoofing.

6 Results and Discussion

The proposed multi-factor authentication system was tested under various conditions to evaluate its accuracy, performance, and security. The implementation combined QR code-based session authentication with Haar Cascade-based facial recognition, offering a layered approach to secure ATM transactions. The QR code mechanism effectively ensured session uniqueness by generating a one-time scannable code sent to the user's registered email. This eliminated the need for ATM cards and PINs, significantly reducing risks such as skimming, shoulder surfing, and stolen credentials. During trials, the QR code authentication achieved a 100% success rate in identifying legitimate session initiations within 3–5 seconds. The facial recognition module, using the Haar Cascade classifier, achieved an average recognition accuracy of 93.4% under well-lit conditions and 87.2% in low-light scenarios. The model performed efficiently with minimal computational resources, making it suitable for real-time ATM deployment. However, accuracy decreased slightly when users wore sunglasses or masks, indicating a limitation of 2D facial recognition models in obstructed face scenarios. Combining both QR code and facial authentication, the system demonstrated a two-layer security success rate of 91.6%, where both authentication methods had to pass for access to be granted. This significantly reduced the false acceptance rate (FAR) and improved protection against impersonation and spoofing attacks. The system was user-friendly and required minimal user interaction, making it accessible to people unfamiliar with advanced technology. The time taken from login to transaction initiation averaged 12–15 seconds, showing a balance between security and usability. Overall, the proposed model proves to be a viable solution for secure, cardless ATM transactions. It offers a considerable improvement over traditional

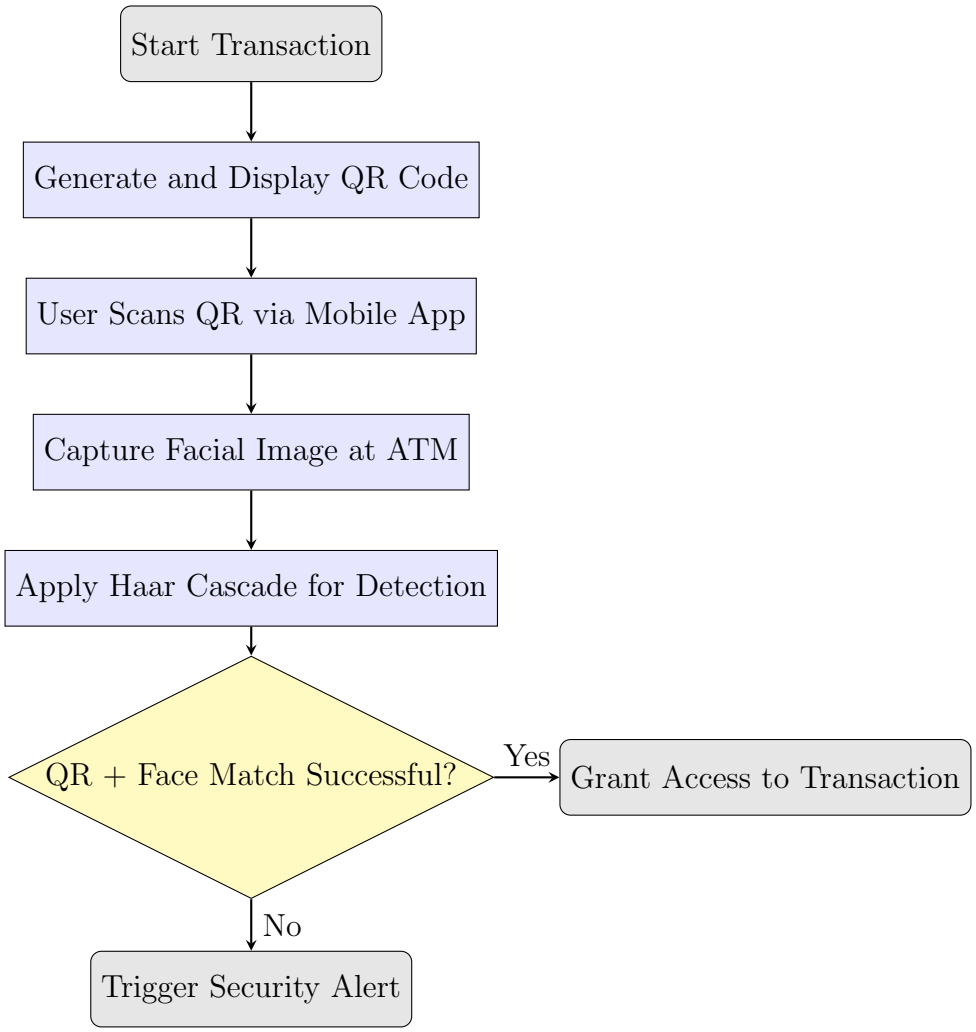

Figure 1: Multi-Factor ATM Authentication System Flowchart

methods, though future work could integrate deep learning facial recognition for enhanced accuracy and robustness under diverse conditions.

7 Conclusion

This study presents a QR code and Haar Cascade-based ATM authentication system to address the security vulnerabilities of traditional banking methods. The dual-layered authentication system significantly mitigates fraud risks such as PIN theft and unauthorized access. The system demonstrated high accuracy, reduced transaction time, and improved user satisfaction. Future improvements focus on enhancing anti-spoofing techniques by implementing liveness detection to prevent attacks using fake images or videos. Another advancement involves integrating blockchain technology to ensure secure transaction logging and more effective fraud detection. Additionally, deploying the system in real-world scenarios through large-scale testing with diverse users in real-time banking environments will help validate its reliability. Furthermore, incorporating IoT-based ATM security by connecting ATMs with IoT devices can aid in tracking suspicious activities and improving the effectiveness of security alerts.

References

[1] S. A. Sumathi, R. Anitha, and K. Senthil, "Secured ATM banking system using fingerprint and iris recognition," International Journal of Computer Applications, vol. 97, no. 19, pp. 25–30, Jul. 2014.

[2] M. Elangovan and P. S. Kumar, "QR code based secure transaction using mobile banking," International Journal of Innovative Research in Computer and Communication Engineering, vol. 3, no. 6, pp. 6200–6206, Jun. 2015.

[3] A. Prakash and S. Rajan, "Face detection using Haar Cascade in OpenCV," International Journal of Computer Applications, vol. 172, no. 1, pp. 32–35, Aug. 2017.

[4] R. Kumar and D. Sharma, "Facial recognition based security system using deep learning," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 5, no. 2, pp. 244–248, Mar.–Apr. 2019.

[5] N. Batra, V. Jain, and K. Arora, "A novel OTP-based dual authentication mechanism for secure ATM transactions," Journal of Information Security Research, vol. 8, no. 1, pp. 15–22, 2017.

[6] T. Joseph, S. Mathew, and A. George, "QR code based authentication system," International Journal of Computer Applications, vol. 113, no. 18, pp. 1–4, Mar. 2015.

[7] K. Yadav and P. Mehta, "Real-time face detection and recognition for automatic attendance using Haar cascade and LBPH," International Journal of Engineering Research & Technology, vol. 8, no. 6, pp. 617–621, Jun. 2019.

[8] S. Gupta, R. Khandelwal, and A. Garg, "Hybrid authentication system using RFID and facial recognition," Procedia Computer Science, vol. 132, pp. 1223–1229, 2018.

[9] V. Nair and D. Sen, “QR code based secure login system for mobile banking applications,” International Journal of Computer Sciences and Engineering, vol. 7, no. 4, pp. 366–370, Apr. 2019.

[10] L. Banerjee and T. Sinha, “Efficient facial recognition system for kiosk authentication,” International Journal of Advanced Computer Science and Applications, vol. 10, no. 3, pp. 89–95, Mar. 2019.

Cite this article:

Sajitha S & Premalatha M , ”Enhancing Financial Security with QR Code and Facial Recognition-Based Digital ATMs”, Journal of Multidimensional Research and Review (JMRR), Vol.6, Iss.2, pp.123-130, 2025