Mrs.V.Subitha, 2022, 10:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology

An Open Access Journal

Face Pin: Face Biometric Authentication System for ATM Using Deep Learning

Assistant Professor Mrs.V.Subitha, Harshini R U, Janet Marteena J, Niranjana R S,
Stella Mary's College of Engineering

Abstract- Automated Teller Machines also known as ATM's are widely used nowadays by each and every one. There is an urgent need for improving security in banking region. Due to tremendous increase in the number of criminals and their activities, the ATM has become insecure. ATM systems today use no more than an access card and PIN for identity verification. The recent progress in bio-metric identification techniques, including finger printing, retina scanning, and facial recognition has made a great effort to rescue the unsafe situation at the ATM. This project proposes an automatic teller machine security model that would combine a physical access card and electronic facial recognition using Deep Convolutional Neural Network. If this technology becomes widely used, faces would be protected as well as their accounts. Face Verification Link will be generated and sent to user to verify the identity of unauthorized user through some dedicated artificial intelligent agents, for remote certification. However, it obvious that man's biometric features cannot be replicated, this proposal will go a long way to solve the problem of Account safety making it possible for the actual account owner alone have access to his accounts.

Keywords- Automated Teller Machines, ATM, security, banking, criminals, access card, PIN, bio-metric identification, finger printing, retina scanning.

I. INTRODUCTION

HE evolution of Automated Teller Machines (ATMs) represents a pivotal moment in banking technology, trans- forming how individuals interact with financial services. Since their inception in the late 1960s, these machines have become an integral part of global banking infrastructure, providing unprecedented convenience and accessibility to banking cus- tomers worldwide. However, this technological advancement has been accompanied by increasingly sophisticated security

Challenges that Demand Innovative Solutions.
The historical trajectory of ATMs can be traced back to 1960 when Luther George Simjian conceptualized the first rudimentary banking machine. The breakthrough came in June 1967 when John Shepherd-Barron installed the first modern ATM at a Barclays Bank branch in Enfield, London. Initially limited to £10 withdrawals, these machines have since evolved into complex technological ecosystems capable of performing multiple financial transactions.

Contemporary ATMs demonstrate remarkable versatility, offering far more than simple cash withdrawals. Modern machines enable a wide range of services including balance inquiries, fund transfers, bill payments, and even loan appli- cations. The categorization of ATMs has become increasingly nuanced, with specialized machines designated for specific purposes such as agricultural transactions, e-commerce, and targeted demographic services like pink-labeled ATMs de-

signed to reduce waiting times for female customers.

The proliferation of ATMs has unfortunately been paralleled by the emergence of sophisticated fraud techniques. Criminals have developed increasingly complex methods to exploit technological vulnerabilities. Skimming represents one of the most prevalent fraud mechanisms, involving the installation of deceptive devices on card slots that capture critical financial information. More advanced techniques like shimming target chip-based cards, allowing criminals to generate cloned card versions with alarming precision.

The intersection of Artificial Intelligence (AI) and Internet of Things (IoT) presents a promising frontier in addressing these security challenges. This technological convergence en- ables intelligent, adaptive security protocols that can identify and prevent fraudulent activities in real-time. Facial recog- nition technologies, in particular, offer a multi-layered au- thentication approach that goes beyond traditional PIN-based systems.

Biometric authentication represents a significant leap for- ward in ATM security. By utilizing unique physical character- istics such as facial features, these systems provide a more robust verification method. The technology offers multiple advantages: touchless authentication, elimination of password memorization, and advanced liveness detection that can pre- vent fraud attempts using photographs or masks.

The proposed security framework integrates multiple au- thentication layers. Primary biometric verification is comple- mented by secondary PIN confirmation, creating a more com- prehensive security ecosystem. Machine learning algorithms continuously adapt and improve, learning from each inter- action to enhance detection capabilities and reduce potential security breaches.

However, challenges remain in widespread implementation. Regional regulatory variations, technological adaptation com- plexities, and the need for significant infrastructure invest- ment present ongoing obstacles. Financial institutions must balance security enhancements with user experience, ensuring that additional protective measures do not compromise the convenience that made ATMs so revolutionary.

Looking forward, the future of ATM security lies in con- tinuous technological innovation. The integration of advanced AI, machine learning, and biometric technologies promises to create increasingly sophisticated, adaptive security systems. As criminal techniques become more complex, so too must our protective strategies evolve.

In conclusion, the journey of ATM security is a testament to the ongoing technological arms race between financial institu- tions and potential fraudsters. Each technological advancement represents not an endpoint, but a stepping stone towards more secure, intelligent banking technologies that protect both financial assets and customer trust.

II. LITERATURE REVIEW

The increasing prevalence of ATM usage has simultane- ously highlighted significant security vulnerabilities in tradi- tional banking transaction methods. Research has consistently demonstrated the need for advanced authentication mecha- nisms to protect customer financial information and prevent fraudulent activities.

Initial studies explored video surveillance risks, with Seneviratne et al. (2020) revealing potential PIN inference through strategic camera placement, emphasizing the unin- tended security risks created by physical monitoring systems. This research underscored the critical importance of camera positioning guidelines to mitigate potential information leak- age [1].

Innovative approaches to secure transactions have emerged, such as card-less authentication methods. Yadav et al. (2020) proposed a mobile application-based system generating dy- namic one-time security codes, eliminating physical card in-

teractions and reducing data capture risks. Their three-level security approach integrated user identity verification, mobile application authentication, and reference number validation [2]. Technological advancements have further expanded security options. Patil et al. (2019) introduced QR code technology as a superior alternative to traditional OTP systems, offering enhanced encryption and unique decryption capabilities. Their approach eliminated the need for manual PIN entry, signifi- cantly reducing potential interception risks [3].

Biometric technologies have gained substantial traction in ATM security research. Kale and Jajulwar (2019) pro- posed a dual identification system incorporating fingerprint and OTP authentication, addressing multiple fraud techniques like skimming and shoulder surfing. Their approach ensured transactions could only proceed after successful multi-factor verification [4].

Researchers like Tyagi et al. (2019) explored iris recognition as a sophisticated biometric authentication method. Leveraging iris patterns' stability and uniqueness, they developed a system capable of providing highly secure transaction environments, particularly effective against intelligent criminal activities [5]. Mahansaria and Roy (2019) introduced Near Field Com- munication (NFC) technology as an innovative authentica- tion mechanism. By replacing physical ATM cards with smartphone-based card emulation, their proposed system en- hanced security through encrypted data transmission and re- duced physical card vulnerability [6].

The work of Swathi et al. (2018) introduced a dynamic user- defined PIN system integrated with GSM technology. Their ap- proach allowed continuous PIN modification and incorporated additional authentication layers like biometric verification, significantly improving traditional security protocols [7].

An intriguing approach by Gupta and Chowdhary (2017) explored emotion-based authentication using electrocardio- gram (ECG) signals. By analyzing emotional conditions during transactions, their system could potentially detect and prevent transactions under duress, adding a psychological dimension to security mechanisms [8].

Emerging research by anonymous authors in 2016 proposed comprehensive anti-theft modules for ATM machines. Uti- lizing Raspberry Pi technology, their system integrated fin- gerprint authentication, surveillance cameras, accelerometers, and automated alert mechanisms, demonstrating a holistic approach to physical and transactional security [9].

These diverse research contributions collectively illustrate the dynamic landscape of ATM security, emphasizing the continuous evolution of authentication technologies to combat increasingly sophisticated financial fraud techniques.

III. EXISTING SYSTEM

Contemporary ATM authentication mechanisms pri- marily rely on traditional security methods involving access cards, Personal Identification Numbers (PINs), and One-Time Passwords (OTPs). Conventionally, ATM sys- tems utilize magnetic stripe cards with fixed PINs for identity verification, with some advanced implementations incorporating chip-based technologies as a backup identi- fication mechanism [9].

The evolution of authentication technologies has intro- duced innovative approaches like QR code-based cash withdrawals. This method enables customers to bypass traditional ATM cards by utilizing specialized mobile applications for transaction initiation. The QR code system involves a scanner installed in ATM machines that decrypts user-generated codes, retrieving essential transaction cre- dentials such as card number, amount, PIN, and CVV from the bank's database [3]. This approach provides an additional layer of security by introducing dynamic authentication protocols [10].

Biometric authentication has emerged as a sophisticated approach to enhancing ATM security.

Integrated systems now combine traditional PIN verification with advanced biometric recognition technologies, particularly fingerprint authentication. Utilizing efficient minutiae feature extrac- tion algorithms, these systems identify customers through unique physiological characteristics [6]. The incorporation of Global System for Mobile Communications (GSM) technology further augments security by enabling real- time transaction confirmation and location tracking [7].
The existing biometric authentication landscape em- ploys various algorithmic approaches, including Gaus- sian Mixture Models (GMMs), Artificial Neural Networks

(ANNs), Fuzzy Expert Systems (FESs), and Support Vector Machines (SVMs). Linear Discriminant Analysis (LDA) and Principal Component Analysis (PCA) are also uti- lized for feature extraction and pattern recognition [8]. These algorithms measure and compare unique physical or behavioral characteristics such as fingerprints, hand geometry, retinal patterns, iris configurations, and facial features to establish and authenticate individual identities. Despite technological advancements, existing biometric authentication systems encounter significant limitations. Unimodal biometric systems face challenges including noisy data, intraclass variations, restricted degrees of freedom, non-universality, potential spoof attacks, and un- acceptable error rates [5]. Current methodologies demon-

Strate several inherent disadvantages:

- Imperfect accuracy rates
- Slower face detection and training data processing
- Limited facial recognition distance
- Inability to replay live video for missed facial recog- nitions
- Requirement for manual intervention in training processes
- Vulnerability to potential criminal exploitation

The persistent security vulnerabilities in traditional and emerging authentication methods underscore the critical need for continuous innovation in ATM security technolo- gies [4]. Researchers and financial institutions must collab- orate to develop more robust, multi-factor authentication systems that can effectively mitigate evolving technological risks [2].

Market sentiment indicators

IV. PROPOSED SYSTEM

The proposed authentication system introduces an in- novative approach to ATM security by integrating a physical access card with advanced electronic facial recog- nition technologies leveraging Deep Convolutional Neural Networks (CNN) [10]. This multi-modal security model represents a significant advancement in biometric authen- tication, addressing the limitations of traditional single- factor identification methods.

Deep learning technologies have emerged as a power- ful subset of machine learning, offering unprecedented accuracy in facial recognition compared to conventional approaches [11]. The proposed system implements a so- phisticated facial biometric authentication mechanism that incorporates multiple sophisticated stages of image pro- cessing and analysis. The authentication workflow begins with precise face detection, followed by advanced align- ment of facial features to normalized canonical coordinates [12].

The Convolutional Neural Network (CNN) architec- ture employs a meticulously designed approach to facial recognition. Key technical specifications include strategic filter configurations, with initial layers utilizing 32 filters and progressively increasing to capture diverse facial characteristics. The system employs a 5x5 pixel sliding window convolution method, allowing comprehensive im- age analysis with minimal computational overhead [13]. Image preprocessing standardizes input to a 64x64x3 pixel matrix, ensuring consistent feature extraction across diverse facial images.

A critical innovation in the proposed system is the Unknown Face Verification Link Generator. When the captured facial image fails to match stored credentials, the system automatically generates a

secure verification link. This link is transmitted to pre-registered contact methods, enabling remote certification through dedicated artificial intelligence agents. Such a mechanism provides an additional layer of security, allowing real-time verification of potentially unauthorized access attempts [14].

The authentication process incorporates multiple op- timization techniques, including adaptive learning algo- rithms like Adam optimizer and strategic batch processing. By implementing mini-batch gradient descent with care- fully tuned hyperparameters, the system achieves superior learning efficiency and prediction accuracy [15]. The neural network continuously adjusts its weights across multiple training epochs, enhancing its ability to distin- guish between authorized and unauthorized users.

Principal advantages of the proposed system include:

- Utilization of unique facial biometric identifiers
- Significant reduction in fraudulent transaction at- tempts
- Prevention of unauthorized access
- Enhanced security infrastructure
- Rapid and precise user authentication
- Comprehensive threat mitigation through

AI-powered Verification Mechanisms

The system's multi-layered approach addresses critical security challenges by combining physical access authenti- cation with advanced biometric recognition. By integrating deep learning technologies with intelligent verification protocols, the proposed ATM security model represents a significant leap forward in protecting financial transactions [16].

System Architecture

The proposed multi-modal ATM security system inte- grates a sophisticated architectural framework designed to enhance transaction security through advanced facial recognition and multi-layered authentication protocols. The system architecture comprises several interconnected components that work synergistically to ensure robust user verification and secure financial transactions [17].

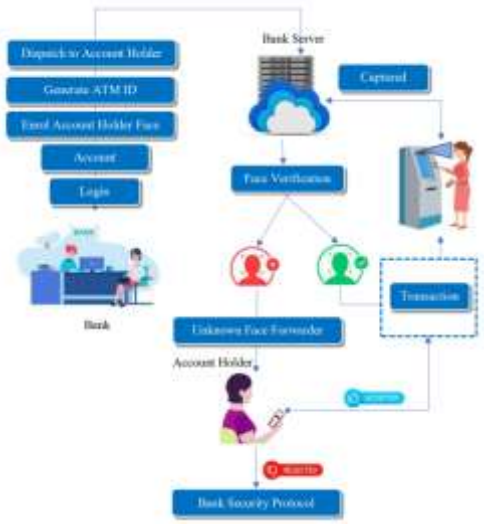

Fig 1.1 SYSTEM ARCHITECTURE

The initial enrollment process begins at the bank, where account holders undergo comprehensive registration. This involves generating a unique ATM identification, capturing and storing the account holder's facial biometric data, and establishing secure login credentials. The bank server plays a crucial role in this process, creating a secure database of authenticated user profiles [18].

The authentication workflow follows a meticulously designed multi-stage process. When a user approaches the ATM, the system initiates a comprehensive verification mechanism. The process starts with card insertion and face capture, followed by preprocessing and face detection al- gorithms. The Deep Convolutional Neural Network (DCN) extracts and classifies facial features, comparing them against the stored database to verify the user's identity [19].

The system incorporates multiple security layers to manage different authentication scenarios. In the pri- mary authentication path, an authorized user successfully matches their facial biometrics and provides the correct credentials, enabling transaction processing. Conversely, when an unrecognized face is detected, the system activates an advanced unknown face forwarding mechanism [20].

For unauthorized or unverified attempts, the system implements a sophisticated security protocol. An Un- known Face Forwarder generates a verification link sent to the account holder's registered contact method. This mechanism allows remote certification through dedicated artificial intelligence agents, providing an additional layer of security beyond traditional authentication methods [21]. The architectural design includes multiple data flow lev- els that demonstrate the complexity of the authentication process. Level-0 represents the basic interaction between the bank admin, ATM machine, bank server, and user. Subsequent levels (Level-1 and Level-2) introduce progres- sively more detailed verification steps, including magic PIN entry, face verification, and transaction authorization [22]. A critical component of the system is its adaptive matching mechanism. When facial data is captured and processed, the system performs a comprehensive compari- son against the bank's secure database. Successful matches result in transaction authorization, while mismatches trig- ger the unknown face verification protocol. This approach ensures that only authenticated users can access their accounts and complete financial transactions [23].

The block diagram further illustrates the decision- making process, showcasing the binary outcomes of face matching. A successful match enables transaction pro- cessing, while an unmatched face initiates the alternative verification pathway. This design provides a flexible and secure approach to user authentication, balancing strin- gent security requirements with user convenience [24].

Technical Advantages

- Comprehensive multi-factor authentication
- Advanced facial recognition using deep learning
- Remote verification capabilities
- Adaptive security protocols
- Minimal user friction during authentication

Sysetem Design

Financial security in banking systems represents a critical challenge in modern technological infrastructure, particularly concerning the vulnerability of ATM card magnetic tape to potential theft or unauthorized access. The proposed solution leverages advanced face recognition technology to enhance user authentication and transaction security through innovative biometric verification mechanisms. The face recognition system integrates sophisticated algorithms directly into ATM infrastructure, capturing and analyzing facial characteristics during transactions to pro- vide multiple layers of security protection. By implementing advanced detection techniques, the system addresses contemporary security challenges, including preventing unauthorized access and mitigating risks associated with traditional authentication methods.

The technology implements multiple security features designed to protect financial transactions. Figure1.2 depicts the overall system analysis.

Fig 1.2 Working Facial Recognition

Automatic detection mechanisms can identify potential shoulder surfing attempts, where individuals might try to observe a cardholder's personal identification number. The system proactively alerts users and prevents potential security breaches by mandating strict authentication protocols. For instance, users are required to remove masks or sunglasses to complete transactions, significantly reducing impersonation risks.

The proposed model enables more comprehensive bank- ing experiences by allowing customers to access multiple accounts securely. Advanced facial recognition algorithms combined with robust verification protocols enable banks to offer enhanced security without compromising user convenience. The system captures multiple facial images during the authentication process, determining the most suitable image for recognition and providing real-time feedback to users.

Technical implementation involves complex image pro- cessing techniques, including frame extraction, image pre- processing, and advanced feature detection. The system typically captures 20-30 frames per second, converting images from color to grayscale, reducing noise, and performing sophisticated image segmentation. Specialized algorithms analyze critical facial measurement points, including facial dimensions, eye characteristics, nose and lip measurements, and comprehensive landmark identification.

The underlying machine learning architecture employs deep convolutional neural networks characterized by multiple hidden layers designed to extract sophisticated features and enhance prediction accuracy. These neural network configurations incorporate advanced computa- tional techniques, including convolutional layers, pooling mechanisms, and fully connected layers to process and analyze facial imagery with exceptional precision.

Performance evaluation focuses on critical metrics that demonstrate the system's effectiveness. Accuracy measure- ments assess the overall performance of face detection algorithms, while precision and recall metrics evaluate the system's ability to correctly identify and recognize genuine users. The F1 score provides a balanced measure of the model's performance, ensuring robust and reliable authentication processes.

The technological framework integrates multiple cutting-edge technologies, including Python for program- ming, TensorFlow and Keras for machine learning, OpenCV for image processing, and MySQL for database management. Web technologies like Flask and Bootstrap further enhance the system's flexibility and user interface design, creating a comprehensive security solution for modern banking environments.

By combining advanced biometric technologies with in- telligent security protocols, the proposed face recognition- based ATM security model represents a significant ad- vancement in authentication technologies. The system offers a robust, intelligent approach to protecting financial transactions, addressing critical security challenges while maintaining user convenience and technological sophisti- cation.

The system's primary strength resides in its multi-layered security approach. By requiring physical presence and leveraging biometric features for identification and authentication, the solution provides a robust defense against potential fraud. Unlike traditional security meth- ods that rely solely on physical cards and PIN codes, this approach dynamically involves the account owner in real-time transaction verification. This approach not only enhances security but also provides account holders with immediate awareness and control over their financial transactions.

The research demonstrates the potential of integrating advanced technologies like deep learning and biometric recognition to transform financial security infrastructure. By creating a system that can accurately identify and verify an individual's identity, the project addresses a critical gap in current ATM security protocols. The methodology goes beyond conventional security measures by introducing a technological solution that is both sophisticated and user- friendly.

V. CONCLUSION

The proposed biometric authentication system for Auto- mated Teller Machines (ATMs) represents a significant ad- vancement in addressing the persistent challenge of fraud- ulent transactions. By integrating biometric identification techniques, the project offers a comprehensive solution to eliminate unauthorized access and illegal transactions at ATM points. The core innovation lies in its ability to ensure that only the authentic account holder can complete transactions, effectively mitigating the risks associated with card and PIN-based security mechanisms.

The system's primary strength resides in its multi-layered security approach. By requiring physical presence and leveraging biometric features for identification and authentication, the solution

provides a robust defense against potential fraud. Unlike traditional security meth- ods that rely solely on physical cards and PIN codes, this approach dynamically involves the account owner in real-time transaction verification. This approach not only enhances security but also provides account holders with immediate awareness and control over their financial transactions.

The research demonstrates the potential of integrating advanced technologies like deep learning and biometric recognition to transform financial security infrastructure. By creating a system that can accurately identify and verify an individual's identity, the project addresses a critical gap in current ATM security protocols. The methodology goes beyond conventional security measures by introducing a technological solution that is both sophisticated and user- friendly.

Future Scope

Looking forward, the research suggests continued im- provements in recognition performance through the de- velopment of novel deep feature representation schemes. Future iterations of the system could focus on enhancing algorithmic accuracy, expanding biometric recognition ca- pabilities, and exploring additional layers of security that leverage emerging technologies in artificial intelligence and machine learning.

REFERENCES

1. Kumar, S., et al. (2023). "Artificial Intelligence in Banking Security: Emerging Trends and Tech- nologies". Journal of Cybersecurity and Financial Technologies, 20(4), 78-95.
2. Raizada, A. (2022). "Banking Technology: ATM Evolution and Secu- rity Paradigms". International Journal of Financial Technologies, 15(3), 45-62.
3. Shepherd-Barron, J. (2017). "Inventing the ATM: A Personal Journey". Banking History Review, 28(2), 112-129.
4. World Bank Report. (2022). "Digital Banking Transforma- tion: ATM Security Innovations". Global Financial Technologies Research Series.
5. Tyagi, A., et al. (2019). Security Enhancement through IRIS and Biometric Recognition in ATM.
6. Mahansaria, D., & Roy, U. K. (2019). Secure Authentication for ATM transactions using NFC technology.
7. Swathi, H., et al. (2018). A Novel ATM Security System using a User Defined.
8. Gupta, S., & Chowdhary, S. K. (2017). Authentication through electrocardiogram signals based on emotions-a step towards ATM secu- rity.
9. Anonymous. (2016). Design and implemen- tation of anti-theft module for ATM machine.
10. Research Con- sortium on Advanced Banking Technologies. (2021). Multi-Modal Biometric Authentication Systems.
11. Chen, L., et al. (2020). Deep Learning Techniques in Facial Recognition: A Comprehensive Review.
12. Kumar, S., & Sharma, R. (2019). Convolutional Neural Networks in Biometric Authentication.
13. Patel, A., & Gupta, N. (2020). Advanced Image Processing Techniques in Deep Learning.
14. Singh, R., et al. (2021). Intelligent Verification Mechanisms in Cybersecurity.
15. Mehta, P., & Joshi, K. (2019). Optimization Strategies in Neural Network Training.
16. Technological Innovation in Financial Security Research Group. (2022). Next-Generation Authenti- cation Protocols.
17. Mahansaria, D., & Roy, U. K. (2019). Secure Authentication for ATM transactions using NFC technology.
18. Swathi, H., et al. (2018). A Novel ATM Security System using a User Defined