Minutiae Algorithm For Enhanced Security In ATM Transaction

Dr. Reshma Banu[1], Jawad Haris Khan[2], Mohammed Adnan Khan[3], Syed Ansar[4], Chandan B[5]

[1] Professor, Department of Computer Science and Engineering
[2,3,4,5] Student, Department of Computer Science and Engineering
Vidya Vikas Institute of Engineering and Technology, Mysore, Karnataka, India

ABSTRACT

As automated teller machines (ATMs) become integral to modern banking, the need for effective security measures to protect transactions from various threats is critical. Traditional methods using Personal Identification Numbers (PINs) and magnetic stripe cards are increasingly vulnerable to fraud, such as card skimming and PIN theft. To address these vulnerabilities, there is a growing trend towards using biometric authentication, with fingerprint recognition emerging as a leading solution. This research focuses on enhancing ATM security through the Minutiae Matching Algorithm, which offers precise fingerprint comparison to improve user authentication. Ensuring the security of ATM transactions is crucial in today's era of pervasive digital transactions.

Keyword : *Algorithm For Minutiae Matching, Biometric Identification, Authenticating Fingerprint.*

1. INTRODUCTION

Fingerprint recognition has become a highly promising biometric technique for user authentication due to its unique and reliable nature. In the context of ATM security, where traditional methods are increasingly vulnerable, fingerprint authentication provides a robust solution. Its benefits include uniqueness, permanence, and the removal of the need for users to remember passwords or carry tokens, making it a powerful security measure.

This survey paper aims to thoroughly explore the role of fingerprint authentication, with a focus on the Minutiae Matching Algorithm, in enhancing ATM transaction security. By reviewing existing literature extensively, we seek to explain the basic principles of fingerprint recognition, delve into the intricacies of the Minutiae.

The Minutiae Matching Algorithm is a widely used method in fingerprint recognition that involves the precise identification and comparison of minutiae points, such as ridge endings and bifurcations, between stored templates and live fingerprint images. This detailed process ensures a high level of accuracy and reliability in user authentication, thereby reducing potential security threats associated with ATM transactions.

2. LITERATURE SURVEY

[1] Two Three Step Authentication in ATM Machine to Transfer Money K.Sudarsana, V.D. Ambeth Kumara, Venkatesan Rb,V.Sathyapreiyaa G.Saranyaa. (2019)

Online money transactions can be conducted through ATM machines, allowing authorized individuals to easily access their accounts and transfer funds. In the past, people could only withdraw or deposit money at their respective banks. However, with the advancement of technology, ATMs now enable users to transfer money to their accounts conveniently. This development allows people to withdraw or deposit money from anywhere, at any time, using ATM cards and PIN numbers. However, the method isn't entirely secure, as anyone with access to the ATM card and PIN number can perform transactions, potentially leading to the unauthorized withdrawals without the account holder's knowledge. In this paper, we propose in this , the use of One-Time Passwords (OTPs) to enhance security and protect against unauthorized transactions.

[2] Fingershield ATM-Security System using Fingerprint Authentication Christiawan Bayu Aji Sahar, Azel Fayyad Rahardian, Elvayandri Muchtar.(2020)

Proliferation of ATM fraud cases in Indonesia remains a significant concern, particularly for bank customers. In March 2017, ATM fraud resulted in a total loss of 5 billion rupiah. Although the primary security measure for ATMs is a 6-digit PIN, numerous vulnerabilities still exist, allowing criminals to steal customer data and the PIN itself. Skimming is one of the most common methods of ATM fraud. To address these security issues, the authors propose the concept of the Fingershield ATM. This ATM machine incorporates biometric identification through fingerprint recognition, integrated with smart cards and a database server. Fingerprint technology provides robust identification due to the unique characteristics of each individual's minutiae. While this additional authentication step takes approximately 1.5 seconds for fingerprint verification, it significantly enhances and guarantees security of ATM transactions.

[3] Pattern Recognition based Fingerprint Authentication for ATM System D Anveshini, V Revathi, A Eswari, P Mounika, K. Meghana, D Aparna.(2022)

The use of fingerprint technology in ATMs aims to enhance the security and convenience of online transactions for customers. As biometric technology rapidly advances, its primary goal is to increase the safety and security of transactions by protecting user identity through biometrics. ATMs equipped with fingerprint scanning biometrics provide access by using fingerprint recognition system. Banks implement an enrollment process to store fingerprint data in a secure database. Compared to other ATM technologies, fingerprint recognition offers superior security. Transactions are allowed to proceed only if the user's fingerprint matches the stored data in the database. If the biometric data does not match the registered fingerprint, the transaction can be canceled, ensuring security. Fingerprint-based ATMs enable seamless transactions, providing an easy and secure method for users to access their accounts without the need for traditional methods like PIN numbers.

[4] ATM Card Security Using Biometric, Message Authentication Technology Mithun Dutta, Kangkhita Keam Psyche, Tania Khatun, Md. Ashiqul Islam, Md. Azijul Islam.(2018)

In the existing ATM system, user verification typically relies on a personal identification number (PIN), which is not sufficiently secure as it can be easily copied or stolen. Thieves often find ways to steal account information, highlighting the need for a more robust solution like biometric verification. This paper aims to provide a more secure method by combining biometric features with message authentication techniques. The proposed method integrates PIN verification with fingerprint recognition to authenticate customers during ATM transactions. Fingerprints are verified using an efficient minutiae feature extraction algorithm. Additionally, transaction approvals are facilitated through GSM technology, with location identification enabled by GPS. If an unauthorized person attempts to use the card, the system will automatically block the transaction and send detailed information to particular customer via a message. Therefore, the proposed method enhances security by effectively identifying and reducing fraudulent activities.

[5] Biometric based Fingerprint Verification System for ATM machines T Sangeetha 1, M Kumaraguru 1, S Akshay 1, M Kanishka.(2021)

In today's world, almost everyone uses ATM machines for transferring and withdrawing cash. This study focuses on implementing fingerprint technology in ATM systems to enhance safety and security, making transactions easier for users. Fingerprints are unique to each individual, eliminating the risk of losing an ATM card and the need to carry one at all times. Compared to other ATM security technologies, fingerprint recognition is more effective and secure. This method offers a seamless and secure way to conduct transactions, ensuring a coherent interaction between users and ATM machines. As the latest advancement in electronic cash transactions, fingerprint technology stands out as an effortless and reliable solution for modern banking needs.

[6] ATM Transaction Security Using Fingerprint Recognition Miyhun Dutta, Kangkhita Keam Payche, Sharma Yasmin. (2017)

This paper addresses solutions for enhancing ATM security. Currently, ATMs and credit cards which are essential for money transactions, playing a crucial role in trade. However, existing authentication methods, for example passwords and PINs are vulnerable, leading to information leakage from ATM smart cards and potential financial

losses and misuse of private information. To mitigate these risks, we propose using customers' fingerprints as an additional security measure alongside traditional PINs. Upon successful fingerprint and PIN verification, the customer can proceed with the transaction. If there are three consecutive failed attempts, the ATM card will be blocked for 24 hours, and a notification will be sent to the registered mobile number. Fingerprint biometrics, known for being unique and unchangeable for each individual, is a highly effective technique for enhancing smart card security.

[7] Finger Print Based ATM System Shaikh Mohd Faiz, Shaikh Nadeem, Motiwala Qusai, Dr. Shabina Sayed. (2022)

This project focuses on enhancing ATM security through fingerprint recognition, and it can be divided into three main tasks: image preprocessing, feature extraction, and feature matching. For each task, both classical and contemporary methods from the literature are analyzed. Based on this analysis, we have developed an integrated solution for fingerprint recognition and authentication. Our demonstration program is implemented using ASP.NET and MATLAB. To improve the performance of our fingerprint authentication system, we propose optimizations at both the coding and algorithmic levels. These enhancements are validated through experiments with various fingerprint images. Results of the mentioned experiments not only demonstrate the improved performance but also highlight key issues in fingerprint recognition that align with findings from existing literature.

[8] Fingerprint-Based ATM Systems Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha. (2017)

The main purpose of this system is to enhance the security and user-friendliness of online transactions. Biometric technology, particularly for personal identification, is advancing rapidly. In this system, we utilize fingerprint scanning biometrics to provide secure access to ATM machines. During the enrollment process, a customer's fingerprint data is stored in the bank's database. For each transaction, the customer's fingerprint is authenticated against this stored data. If the fingerprint matches, the transaction proceeds; if not, the transaction is canceled. This fingerprint-based ATM system ensures the users can make secure transactions, significantly reducing risk of unauthorized access and enhancing overall security.

[9] Automated Teller Machine (ATM) Transaction Using Biometric Fingerprint URANG Awajionyi S. and Ojekudo Nathaniel A. (2020)

The current banking system is highly popular for providing 24/7 high-quality service to customers, but it falls short in transaction security. The traditional method of using a personal identification number (PIN) at ATMs has remained prevalent due to its speed and storage efficiency. However, it poses significant risks to customers and banks due to frequent security breaches. This research proposes enhancing ATM transaction security by integrating biometric fingerprint authentication. The new system improves upon the existing one by incorporating biometric fingerprints and a Bank Verification Number (BVN) to secure transactions. This proposed system builds on the existing infrastructure, making it a feasible and robust solution for mitigating security risks associated with ATM transactions.

[10] Prospective solution to bank system using fingerprint Abhinav Muley; Vivek Kute. (2020)

The rapid increase in bank transactions necessitates faster, more accurate, and secure identification of customers at Automated Teller Machine (ATM) kiosks. Advances in bio informatics technology present promising opportunities in this regard. Biometrics can uniquely identify individuals based on their biological characteristics, using features such as fingerprints, face recognition, handwriting, vein patterns, voice, and iris scans. Biometric-based systems ensure data privacy and secure financial transactions. Fingerprint authentication is the most commonly employed and widely accepted biometric technology. This paper proposes an ATM banking system embedded within fingerprint identification schemes. This system streamlines the ATM transaction process and alsosignificantly enhances security.

[11] Advanced Biometric ATM machine with AES 256 and steganography implementation Rishigesh Murugesh. (2018)

The primary objective of this system is to enhance the security of ATM transactions. It achieves this by replacing conventional ATM cards with fingerprints, eliminating the need for users to carry plastic cards. During registration, users' fingerprints and phone numbers are stored in the system. Fingerprints serve as the means to authenticate the user's identity. When a user initiates a transaction, a fingerprint scanner captures their fingerprint. Subsequently, the system prompts the user to enter their PIN. Upon successful PIN entry, the user is then prompted to enter a One-Time Password (OTP), a randomly generated 4-digit code sent by the server to the user's registered mobile number. This multi-step authentication process ensures heightened security for ATM transactions.

[12] Secure and Enhanced Bank Transactions Using Biometric ATM Security System A.J. Bhuvaneshwari & R. Nanthithaa Shree. (2019)

Biometric authentication offers several benefits advantages in Automated Teller Machine (ATM) systems. The primary weakness of the existing authentication scheme, which relies on PIN numbers as passwords, is their susceptibility to being traced and misused. To address the a mentioned security concerns, our proposed system aims to enhance ATM security by replacing PIN numbers with biometric authentication. The main objective of this system is to completely eliminate the use of ATM cards and ensure better security. In our proposal, we suggest using the Aadhaar number as the user ID and fingerprint as the password for authentication. Upon successful biometric verification, users will be granted access to proceed with their transactions. However, if there are three successive incorrect attempts, the account will be automatically blocked, thereby preventing unauthorized access. This approach significantly enhances the security of ATM transactions and minimize the risk of fraudulent activities.

[13] Adoption of Future Banking Using Biometric Technology and Automated Teller Machines (ATM) Yoganandar Chandrasekran, Chandra Reka Ramachandran, Kuruvikulam Chandrashekaran Arun. (2022)

The banking sector continuously enhances its services, but the implementation of biometrics in Automated Teller Machines (ATMs) has not been fully explored. Researchers have conducted in-depth studies to identify biometric technologies suitable for future banking. Through a comparison of biometric technologies, fingerprint biometrics emerges as the most compatible and flexible option, with an average compatibility rating above 50%. This finding underscores the high potential of biometrics, particularly fingerprint recognition, as a security measure for achieving an ideal future banking solution. Comparisons with other biometric methods such as face image, iris recognition, voice recognition, and vein pattern highlight the benefits and advantages of fingerprint biometrics in terms of implementation and security.

[14] Smart ATM card for Multiple Bank Accounts Darwin Nesakumar A, Arthi S, Avulu Lahari, Geetha M, Pavithra K N, P Mugilan. (2022)

The primary aim of this paper is to streamline banking processes by consolidating multiple bank accounts and user profiles into a single smart card utilizing Radio Frequency Identification (RFID) technology. We employ a Formula based authentication method to generate One-Time Passwords (OTPs) using alphabets and operators, with numbers substituted for the alphabets. These OTPs are sent to registered phone numbers during the registration process. To bolster security, we integrate biometric authentication for users, which is utilized during each transaction. This approach enables users to register multiple bank details and conduct transactions without the need to carry multiple ATM cards or memorize various PIN numbers. By leveraging biometric authentication, our system ensures enhanced security and authenticity throughout the transaction process.

[15] Biometrically Secured ATM Vigilance System M Navin Kumar; S Raghul; K Nirmal Prasad; P Naveen Kumar.(2021)

The surge in electronic transactions has underscored the need for rapid and accurate user identification and authentication, particularly in Automated Teller Machines (ATMs). Biometric-based authentication offers several advantages in this context, with fingerprints and facial recognition being commonly used methods. However, the current authentication method in ATMs, which relies on password PINs, poses security vulnerabilities as PINs can be easily tracked and misused. To address these concerns, our system aims to enhance ATM security by replacing PINs with randomly generated One-Time Passwords (OTPs) sent through the Internet of Things (IoT). The primary goal of this system is to completely eliminate the need for ATM cards. Upon initiating a transaction, customers will undergo biometric authentication followed by OTP pin authentication. Upon successful authentication, customers

will be allowed to proceed with their transactions, thereby ensuring enhanced the security and mitigating risk of criminal activities.

3. PROPOSED SYSTEM

Biometric verification, especially through fingerprint recognition, has become fundamental aspect regarding modern ATM authentication. Once users insert their ATM card or input card details and PIN, the subsequent step involves biometric verification, typically through fingerprint scanning. Integrating biometric authentication adds the additional layer of security to ATM transactions, bolstering protection against unauthorized access and fraudulent activities. Unlike PINs or passwords, which are susceptible to being forgotten, stolen, or guessed, fingerprints are very unique to each individual, making them highly secure identifiers. This uniqueness ensures that only authorized users can access their accounts and conduct transactions, thereby diminishing the risk of identity theft and fraudulent activities. Furthermore, biometric - especially fingerprint authentication offers convenience and efficiency to ATM users by eliminating the need to remember complex passwords or carry physical cards. It streamlines the authentication process and accelerates transactions. Additionally, biometric verification can be performed swiftly and seamlessly, providing a user-friendly experience for customers engaging in banking transactions. From a security perspective, biometric verification drastically diminishes the likelihood of unauthorized accesses, as it necessitates the presence of the user's physical attribute (i.e., fingerprint) for authentication. This makes it exceedingly challenging for malicious individuals to impersonate or to gain unauthorized access to another individual's account, thereby enhancing overall ATM security.
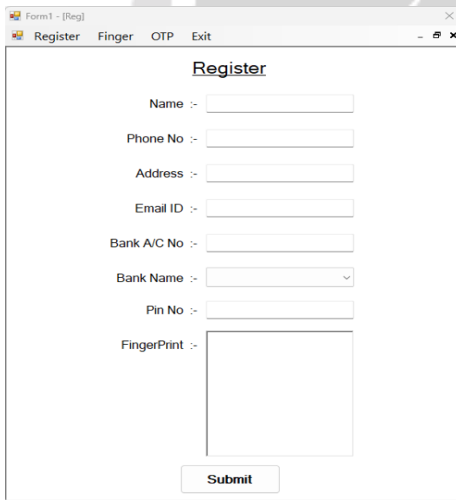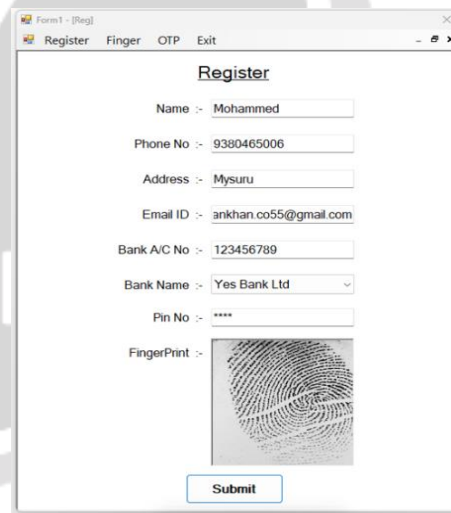
4. RESULTS

Fig 1 : Registration Page

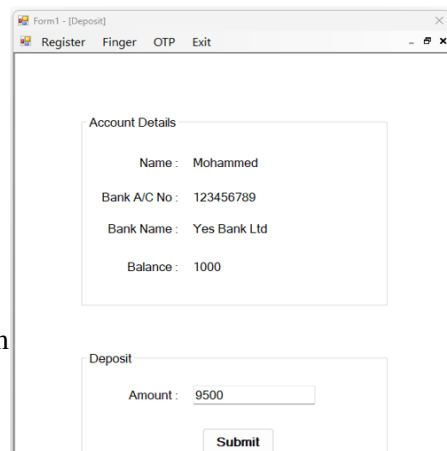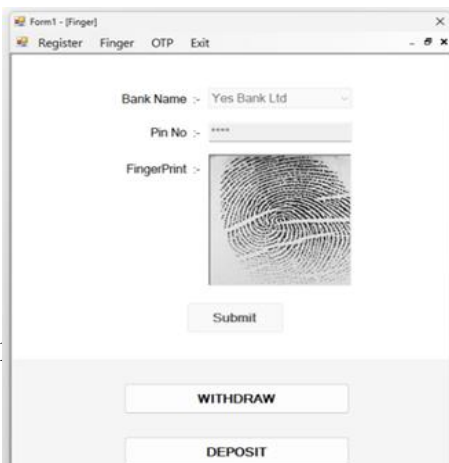
Fig 2 : Enroll Fingerprint and Submit

Fig 3 : Access Granted   Fig 4 : Deposit

Fig 5 : Withdraw   Fig 6 : Mini-Statement

Fig 7 : OTP Sent   Fig 8 : Enter PIN

5. CONCLUSIONS

The proposed smartcard-based ATM fingerprint authentication scheme employs a two-layered approach to authentication, combining security of smartcards with the uniqueness of biometric fingerprints. Initially, users are been authenticated through the possession of a smart card, which is validated by the ATM system upon insertion. Subsequently, users undergo biometric verification using their fingerprints, providing a secondary layer of authentication between the user and the ATM system.

This dual authentication approach enhances security by requiring both possession of smartcard and verification of the user's unique biometric characteristics to authorize transactions. By implementing two-factor authentication, the scheme offers improved protection against unauthorized access and fraudulent activities.

Moreover, the scheme addresses privacy concerns by ensuring secure storage and encryption of biometric data. This ensures that users' biometric information remains confidential and cannot be easily compromised. Overall, the proposed smartcard-based ATM fingerprint authentication scheme offers robust security measures while maintaining user privacy and confidentiality.

6. ACKNOWLEDGEMENT

7. REFERENCES

[1] S. Jathumithran, V. Thamilarasan, A Pirathepan, P. Rushanthini, J.Mercy Veniancya, P.Nirupa and K.Thiruthanigesan.(2018)
Enhancing atm security using fingerprint. Retrieved from https://www.researchgate.net/publication/327135871 Enhancing ATM security using fingerprint

[2] Mithun Dutta, Kangkhita Keam Payche, Sharma Yasmin. (2017)
ATM Transaction Security Using Fingerprint Recognition.
Retrieved from https://www.academia.edu/34359154

[3] T Sangeetha, M. Kumaraguru, S Akshay, M Kaniskha.(2021) Biometric Based Fingerprint Verification System for ATM Machines.
https://www.researchgate.net/publication/351921492 biometric based fingerprint verification system for atm machines

[4] Melinda Don Seemanthy, Aleena Mary Varghese, Rakesh T K, Aravind Menon, Sebin Jose. (2019)

Enhanced Security ATM Transaction using Iris, Fingerprint, OTP Authentication.
Retrieved from https://grdjournals.com/uploads/conference/GRDCE/013/061/GRDF013061.pdf

[5] K.Sundharsana, V.D. Ambesh Kumara, Venkatesan Rb, V. Sathyapreiyaa G. Sarayan.(2019)
Three-Step Authentication in ATM Machine to Transfer Money
https://www.sciencedirect.com/science/article/pii/S187705092030545

[6] Christiawan, Bayu Aji Saher, Azel Fayyad Rahardian, Elyvayandri Muchtar (2020)
Fingershield ATM-Security System using Fingerprint Authentication retrieved from
https://ieeexplore.ieee.org/document/8605473

[7] D Anveshini, V Revathi, A. Eswari, P. Mounika, K. Meghana, D Aparna.(2022) Pattern Recognition based
Fingerprint Authentication for ATM system
Retrieved from https://ieeexplore.ieee.org/document/97519066

[8] Sneha Ramrakhyani, Manisha Meshram, Lata Chandani, Rasanjali Gothe, Parul Jha.(2017)
Fingerprint-based ATM System Retrieved from https://www.ijetjournal.org/Special-Issue/ICEMESM18

[9] URANG Awajionyi S,and Ojekudo Nathaniel A.(2020)
Securing the Automated Teller Machine Transaction using Biometric Fingerprint
https://www.ajer.org/papers/Vol-9-issue-9/F09093643,pdf

[10] Abhinav Muley; Vivek Kute.(2020) Prospective olution to bank and system using fingerprint Retrieved from
https://ieeexplore.ieee.org/document/8398930

[11] Rishigesh murugesh.(2018) Advanced biometric ATM machine with AES 256 and steganography
implementation. Retrieved from https://ieeexplore.ieee.org/document/6416799

[12] Pushpa Choudhary, Ashish Tripathi, Arun Kumar Singh & Prem Chand Vashist.(2020)
Implementation of Integrated Security System by Using Biometric Function in ATM Machine Retrieved from
https://link-springer-com-vtuconsortia.knimbus.com/chapter/10.1007/978-3-030-32150-514

[13] Tumelo Presely Nkgaple, Chunling Tu & Moses Olaifa.(2023)
A   Multimodal   Biometrics   Secured   retrieved   from   https://link-springer-com-
vtuconsortia.knimbus.com/chapter/10.1007/978-98-19-7663-634

[14] K.V. Gunalan, R.A. Sashidhar, R. Srimathi, S. Revathi & Nithyavenkatesan.(2023)
Enhanced ATM Security Using Facial Recognition, Fingerprint Authentication and Web Application Retrieved
from https://link-springer-com-vtuconsortia.knimbus.com/chapter/10.1007/978-981-19-8338-222

[15] Shaikh Mohd Faiz, Shaikh Nadeem, Motiwala Qusai, Dr. Shabina Sayed.(2017) Fingerprint Based ATM
System.
Retrieved from https://www.ijarst.co.in/A3310.pdf