Advanced ATM Transaction Security with OTP Verification and Face Recognition

Dhanashri Phadtare[1], Dr. Brijendra Gupta[2]

[1]Student, Information Technology, Siddhant College of Engineering
[2] Professor, Information Technology, Siddhant College of Engineering

Abstract

At the core of the current ATM security authentication mechanism is pin-based verification. Numerous elements could impact the system, such as urgency, pin memorization, interaction speed, and unintentional pin sharing. Cards with magnetic chips can be easily copied. An automated machine becomes vulnerable when its security is breached; security and vulnerability are two sides of the same coin. Automated teller machine manufacturers are constantly adding and enhancing security measures to ensure that consumers may complete banking transactions without hassle or fear of funds being deducted from their accounts. To gain access to the automated teller machine and exploit the bank accounts, the same scammers, however, work just as fast to circumvent the recently created security measures.

We want to stop ATM theft, misuse, and theft in order to assist people live safe and secure lives. An intelligence framework serves as the foundation for the proposed solution, which aims to promote worldwide digitization and guarantee that ATMs are utilized without hesitation or delay. The customer's card is inserted into the ATM, and the process begins. The idea behind the ATM security system is face verification, which was created to provide users with a true security solution. The main goal of the project is to design and construct a face verification and LRR algorithm-based ATM security system. Our proposed framework addresses inadequacies of the current system. You will be able to process any transaction using the system. The system will ask the first self-user to "Verify Face" and, if the image matches the one that banks have on file, allow the transaction to proceed.

Keywords: ATM, LRR, OTP, Fraud, Security, and Face Recognition.

1. Introduction

Science and technology are advancing so rapidly that future creations are being built with a high degree of security. But there are also dangers of compromising this degree of protection. Theft and fraud continue to occur at a number of financial institutions, including banks, and apps, such as ATMs, despite the fact that automation has typically improved things. Because fraudsters are developing new methods of attack as technology develops, security is becoming stronger. The simplest method to use is biometric technology, which can provide higher security levels in numerous areas. Biometric identifiers have several advantages over current and traditional identifying and security techniques.

The latest ATM security authentication technique is solely dependent on pin-based validation. Elements such as crises, pin reminders, interaction frequency, and accidental pin sharing have a range of effects on the system. Cards with magnetic chips are easy to claim. An automated machine is vulnerable when its security is inadequate; security and unprotected are two sides of the same coin. Automated teller machine makers keep adding security measures and improving their devices so that consumers may conduct banking transactions without worrying about money being taken out of their accounts. To gain access to the automated teller machine and exploit the accounts of account holders, the same scammers, however, work just as fast to circumvent the recently implemented security measures.

Only pin-based verification is used in the most recent ATM security authentication method. Emergency situations, pin reminders, interaction frequency, and accidental pin sharing are some of the factors that affect the system. Magnetic chip cards are easy to claim. Unprotected and secure are two sides of the same coin; an automated machine is vulnerable if its security is inadequate. Automated teller machine makers keep adding security measures and improving their devices so that consumers may conduct banking transactions without worrying about money being taken out of their accounts. To gain access to the automated teller machine, the same scammers, however, work just as fast to circumvent the recently implemented security measures.

Using facial recognition techniques: A camera positioned atop the cash machine captures a real-time image of the customer and compares it to the image of the central bank. Once the image matches, the user can be considered fully validated. After then, the client will finish the transaction. It will finish in a mere two to five seconds. The face recognition method is used to develop this system. Furthermore, some people experience alterations as a result of change. The customer's age will be important. As a result, the problem caused by duplicate card abuse can be resolved.

The OTP Method: Only one login session can be used with an OTP, which is a string of digits. Non-holders can also conduct transactions if they need to be done on behalf of the original account holder. The system provides the registered mobile phone with an OTP.

2. Exiting System and Drawbacks

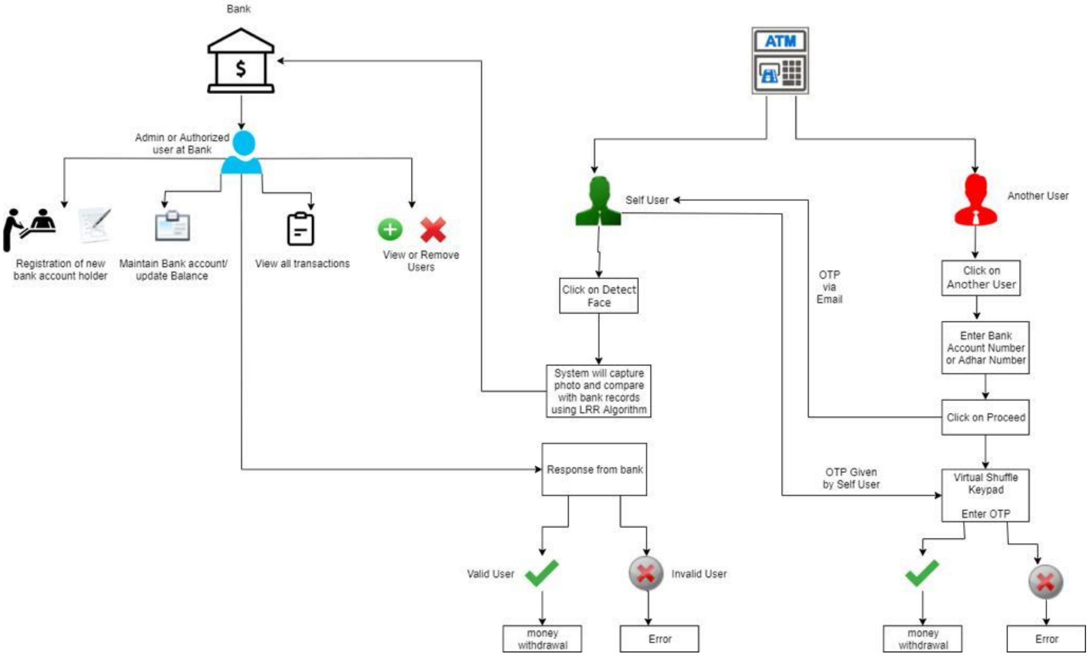
The current ATM security authentication mechanism is based on pin-based verification. Numerous elements, such as urgency, pin memorization, interaction speed, and unintentional pin sharing, affect the system. Security and vulnerability are two sides of the same coin; when an automated machine's security is breached, it becomes vulnerable. To ensure that consumers may complete banking transactions without trouble or fear of money being taken out of their accounts, automated teller machine manufacturers are constantly adding and enhancing security measures. The speed at which fraudsters create new security features, however, allows them to access the automated teller machine and exploit it.

Drawbacks:

1. Surfing on the shoulders: getting information by peering over someone else's shoulder is called "shoulder surfing." In a hectic situation, it is quite easy and effective to stand next to someone and watch how PINs are entered into the card terminal.
2. Phishing: The practice of pretending to be someone else in order to access and take advantage of their account is known as spoofing.
3. Looking through: Thieves use card skimmer devices to extract a card detail from the magnetic chip. Usually, these devices are installed inside or above an ATM card reader.
4. Phishing and Trapping Cards: Card trapping and phishing attempt to take a card when the user puts it into the ATM to finish a transaction. A device is placed inside or above the card slot to take the customer's card. These devices are designed to prevent the customer from receiving their card back after making a purchase.

3. System Implementation

To provide users with a genuine security solution, the concept of a facial detection-based ATM security system was created. The design and implementation of an ATM security system that combines facial recognition and the LRR algorithm is the primary goal of the project. The shortcomings of the existing system are addressed by our proposed approach. Users will be able to complete any transaction thanks to the technology. The user will initially be prompted by the system to "Detect Face." The system will refuse the transaction if the face does not match an image that is kept in the bank's database. The system will ask for the correct OTP that has been provided to an authorized user and allow the transaction to proceed when a guest user inputs it.



4. Module Description

The System has following Module:

- Bank Admin Module
- ATM Module

Bank Admin Module: In this module, the administrator can create an account by selecting his or her profile picture and personal details. The administrator has access to the bank's entire user base. Users are able to conduct transactions, such as making deposits and withdrawals. Additionally, users may readily view their transactions, and the administrator can remove users. Bank users can modify their existing account information, such as changing their email address, changing their pin number, or changing their old phone number. For further protection, they must update their profile photo every six months.

ATM Module: This module consists of two sub-modules:

Self-User: Only the bank's authorized users have access to Self-User. Although the self-user must be enrolled and have their account number and password, we have included features like Face Recognition to increase security and lower fraud. The Low Rank Representation Algorithm is used to take the user's photo after they click a live photo screen after entering their account number and password. The findings will now be displayed once the image has been compared to both live and database-stored photos. In the event that the user is legitimate, they will be able to withdraw their money; if they are not, an error message will appear. If the user want to, they can modify their PIN.

Guest User: This is for the individual who was sent by the self-user to withdraw money. The account number of this user is required for the guest user. The self-user's account number must be entered first when they choose another user. Upon proceeding, the self-user will receive an OTP, which must be accurately entered for the next step. The self-user will then provide the guest user with his OTP, and after the guest user has done so, the screen will display a shuffled keypad where the guest must enter the self-user's PIN in order to withdraw the money. Additionally, the virtual scrambled keypad will be locked and display an error if the OTP is incorrect. Likewise, an error message will be displayed if the PIN is entered incorrectly.

5. Methodology:

To create an automated teller machine (ATM) system that uses the LRR algorithm to recognize a user's face and verify that they are the account holder.

LRR decomposes a given data matrix X (containing face images as column vectors) into a low-rank representation and a sparse noise component:

$X=L+SX = L + SX=L+S$

Where:

- X → Input data matrix (face images as columns).
- B → Low-rank component (essential face structure).
- S → Sparse component (occlusions, noise, or variations).

The goal is to find a low-rank matrix L that captures the major facial features while eliminating noise in S.

Steps of LRR for Face Detection

1. **Prepare the Face Dataset**
   - Convert face images into grayscale and resize them.
   - Represent each image as a column vector in matrix X
2. **Apply Singular Value Decomposition (SVD)**
   - Perform SVD to extract the principal components of faces.
   - Keep only the most dominant eigenfaces.
3. **Reconstruct Faces and Detect Key Features**
   - Reconstruct denoised faces from the low-rank representation.
   - Use Eigenfaces or PCA for feature extraction.
   - Apply face detection techniques

System will also have the other option for login i.e. Guest user. For Guest user we have OTP and shuffle keypad features.

Algorithm for OTP (One-Time Password) Generation:

Input: OTP length, type (numeric/alphanumeric)

Output: A randomly generated OTP

1. Define OTP_LENGTH (e.g., 6 digits)
2. Choose the character set:

- If numeric OTP → Use digits [0-9]

- If alphanumeric OTP → Use [A-Z, a-z, 0-9]

4. Initialize an empty OTP string
5. Loop from 1 to OTP_LENGTH:

- Randomly pick a character from the chosen set
- Append it to the OTP string

6. Return the generated OTP

For shuffling keypad we have used Fisher–Yates Shuffle Algorithm

The Fisher–Yates shuffle is an algorithm used to generate a random permutation of a finite sequence (array or list). Given an ordered list of elements, it produces a completely randomized version of the list, ensuring an unbiased shuffle.

Time Complexity: O(n) in its modern implementation (Durstenfeld's version), as it swaps elements in a single pass through the array.

Space Complexity: O(1) since it performs in-place shuffling without using additional memory.

Efficiency: Highly efficient for large lists as it avoids unnecessary swaps and operations.

Commonly used in applications requiring unbiased randomness, such as card games, simulations, and randomized algorithms.

Fairness: Guarantees an equal probability for all possible permutations, making it superior to naive shuffle approaches that may introduce bias.

References

1. S. D V, A. R, E. R. K and A. S, "Enhanced Security Feature of ATM's Through Facial Recognition," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1252-1256, doi: 10.1109/ICICCS51141.2021.9432327.
2. Ashwini C, Shashank P, Shreya Mahesh Nayak, Siri Yadav S, Sumukh M, 2020, Cardless Multi-Banking ATM System Services using Biometrics and Face Recognition, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) NCCDS – 2020 (Volume 8 – Issue 1
2. 3. J. Chen and J. Yang, "Robust Subspace Segmentation Via Low-Rank Representation," in IEEE Transactions on Cybernetics, vol. 44, no. 8, pp. 1432-1445, Aug. 2020, doi: 10.1109/TCYB.2013.2286106.
3. S. Kumaresan, G. D. Kumar and S. Radhika, "Design of secured ATM by wireless password transfer and shuffling keypad," 2020 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), 2015, pp. 1-4, doi: 10.1109/ICIIECS.2015.7192993.
4. W. Park, D. Hwang and K. Kim, "A TOTP-Based Two Factor Authentication Scheme for Hyperledger Fabric Blockchain," 2020 UFN), 2018, pp. 817-819, 10.1109/ICUFN.2018.8436784.
5. The Lancet, vol. 395, no. 10223, pp. 497–506; Huang, Y. Wang, et al., "Clinical features of patients infected with 2019 novel coronavirus in Wuhan, China."
6. T. K. Hazra and S. Bhattacharyya, "Image encryption by blockwise pixel shuffling using Modified Fisher Yates shuffle and pseudorandom permutations," 2020 IEEE 7th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2017, pp. 1-6, doi: 10.1109/IEMCON.2016.7746312.