Design and Implementation of Secure ATM System Using Biometric and Hashing Technique

Resmi Karinattu ReghuNathan[a], and Dhanya Job[a]

[a] *MG University, Santhigiri College of Computer Sciences, Idukki, Kerala, India*

Abstract

Security is a major concern in all aspects of life, Nowadays. Automated teller machines (ATMs) are the most commonly used devices for financial transactions in which personal identification numbers (PINs) are the authentication method used by many people. For a long time, researchers have been studying how to use an individual's biometric features to enhance authentication and verification technologies beyond the existing reliance on passwords. Since the biometric features cannot be stolen, the protection of digitized biometric data becomes critical in order to prevent it from various attacks. This paper presents a method for enhancing security in ATM banking system using finger print hash code biometric authentication. The proposed system provides two levels of security between ATM machine and server by combining biometric and hashing technique.

Keywords 1

ATM, Security, Biometric, Fingerprint, Minutiae, Hash Code

1. Introduction

Many people in today's modern world depend on computers to keep track of important details. ATM is an automatic machine, and it has been in operation since 1967. John Shepphardbaren invented the ATM in the United Kingdom in June 1967. People nowadays use PINs and passwords to manage various devices such as cars, cell phones, and ATM machines; however, using PINs without security causes major problems for customers such as usability, memorability and security [1]. A customer with a bank account can obtain confidential access to their account via an ATM by obtaining a PIN or password, enabling them to conduct transactions, transfer money, and so on. PIN numbers are very critical for securing customer account information and should not be shared with others.

ATM fraud is on the rise as automated teller machines (ATMs) become more widespread. ATM fraud is a major global issue that consumers and bank operators have had to deal with on a regular basis in recent years. Traditional ATM authentication, which relies on a card and a PIN, has drawbacks. If the account holder's card is lost and the PIN is known, the account holder is vulnerable to fraud. To resolve the security issues with ATM PIN authentication, new techniques are being developed. Since biometric data cannot be duplicated or lost, biometric authentication methods may provide a solution to this issue.

Biometrics authentication ensures identification based on a physiological or behavioural characteristic. In this work, we propose a two factor authentication scheme which uses biometric fingerprint, and hashing process to provide improved security for ATM authentication. Hash values are sent across the network and stored in the central database. During verification, the new hash value is compared with the hash values stored in the database for matching.

WCNC-2021: Workshop on Computer Networks & Communications, May 01, 2021, Chennai, India.
EMAIL: resmykr@gmail.com (Resmi Karinattu ReghuNathan)
ORCID: 0000-0002-1307-8080 (Resmi Karinattu ReghuNathan)

2. Related Works

Traditional authentication are primarily based on knowledge and token. Despite the fact that the two credentials are well-known and accepted in society, they may also fail to provide true authentication. To overcome the limitations of conventional approaches, biometrics allows us to determine an individual's identity based on who they are rather than what they have or remember. Although user authentication and verification using biometrics is easy to use, it does pose concerns about the security of digitized biometric data. If an attacker gains access to this information, it can be used to perform a variety of attacks. Various security measures are used to protect the data from different attacks.

Nowadays, ATMs are widely used by the general public due to their ease of use, user-friendliness, and immediate availability of cash at any location. As the technology of ATM advances, attackers develop new techniques to bypass ATM security. Various types of fraud are common in ATM which include card theft, pin theft, card reader techniques, force withdrawals etc. As fraud approaches have become more sophisticated and occurrences have increased, financial institutions must manage the risk associated with ATM fraud by devising new security measures.

Soutar et al. [2] used an approach to fingerprint biometrics protection on images by encoding key data with a special filter in Fourier space. The decoder can retrieve the data only by showing a similar fingerprint picture. Here the matching process is based on correlation, where image translations are possible but not rotations.

In [3], ATM security is achieved by using steganography and cryptographic techniques on biometric finger vein technology. Security can be achieved by using light-weight cryptography and stegnography using variable MSB–LSB algorithm. Zhang et al. [4] also proposed the usage of finger vein technology for authentication. Alzamel et.al [5] proposed a method by fusing pin number with finger print authentication scheme. It employed POS (Point of Sale) network devices between finger print and ATM card. In [6] [7] and [8] the authors used finger print authentication method for enhancing ATM security. Onyesolu and Okpala [9], proposed a system with three levels of authentication including pin, finger print and OTP. The system provides a high level of security but the model is very complex and time consuming.

3. Proposed Method

Proposed method uses ATM authentication using hash code generated from finger print minutiae. The block diagram of the proposed method is shown in Figure 1. It consists of two stages enrolment and verification. During enrolment, finger print data is taken instead of pin and hash code is generated from fingerprint minutiae points. During verification, the hash code generated for the given input image is compared with the hash values stored in the central database. If same hash Code matching is found, the fingerprint is authenticated and integrity is checked.

3.1. Feature Extraction using Fingerprint

Fingerprint is one of the important biometric feature used in ATM for personal authentication. The unique feature called minutiae, is the most critical parameters used in fingerprint recognition systems. Based on minutiae points, ridge ending and bifurcation are the two important minutiae features used for verification or identification.

The feature extraction of minutiae from finger print images is described in this section. Many fingerprint matching models are based on minutiae. The low quality of fingerprint images is one of the issues with fingerprint recognition. The enhancement's aim is to minimize noise in the fingerprint image and improve the ridge-valley structures, allowing for more precise minutiae extraction. There are a variety of fingerprint enhancement techniques available. This paper uses Gabor filters with only four

orientations: $\theta = \{0, \pi/4, \pi/2, 3\pi/4\}$.The minutiae must be extracted after enhancement. First step is a thresholding operation that is used to binarize the enhanced image. In thresholding each gray scale pixel value is converted to a binary value. After binarization, the next step is morphological thinning operation in which the width of each ridge is reduced to a single pixel, resulting in an image skeleton. The actual minutiae detection from the skeleton image is the next step. The Bifurcation and Termination is extracted as red points and green points in minutia. The last step is the post processing operation which eliminates false minutiae if any from skeleton images and maintaining the final true minutiae points. Figure 2 shows the steps involved in minutiae extraction from input finger print image.

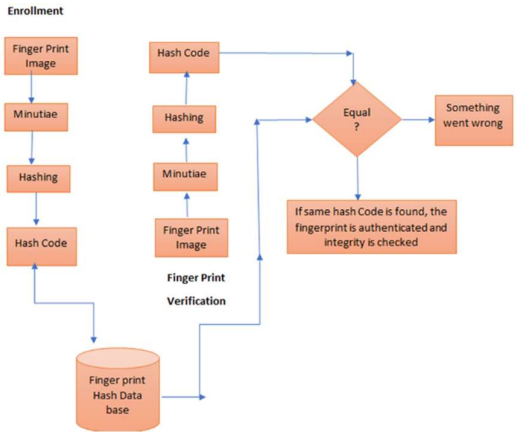

Figure 1: Proposed Authentication System in ATM

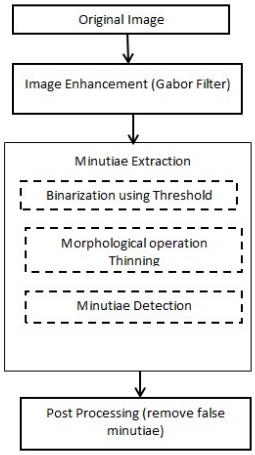

Figure 2: Steps used for Minutiae extraction

3.2. Hash code generation from finger print

Hashing is a technique by which the data is mapped to a fixed value. Authentication is the primary application of hashing. There are many hash functions available. Two popular hash functions are MD5 and SHA. The two algorithms are compared based on parameters such as running time and complexity [10].The complexity of the two algorithms are equal, but MD5 is faster than SHA. Also MD5 generate simple hash compared to SHA. Based on these properties, MD5 hashing is used in the proposed technique.

MD5 hashing algorithm is used for generating the high security 32 bit hexadecimal hash code containing text and numbers. The procedure of MD5 hash generation is summarized in Algorithm 1. This algorithm takes features extracted from minutiae as input.

Algorithm 1 The algorithm used for generating Hash Code

Input: Extracted Minutiae Features

Output: 32 bit hexadecimal Hash Code

1. Append or add extra padding bits to original image
2. Attach 64 bits at the end of step1 results.
3. Initialize four MD buffers A, B, C, D to calculate the message digest values.
   All the four buffers are 32 bit registers.
4. Process message using logical operators OR, NOR, XNOR in 16 word blocks
5. Generate output as 32 bit hash code with lower order bits A ending higher bits D

4. Experimental Results and Discussion

In this study finger print database FVC2002 [11] is used and the feature extraction and hash code generation is implemented using Matlab. The finger print images goes through various preprocessing steps before minutia extraction. The outputs generated in minutia extraction for a given input image is illustrated in Figure 3.

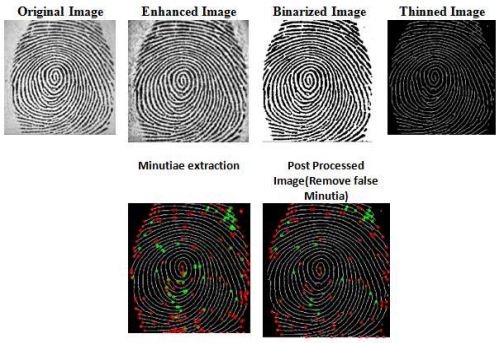

Figure 3: Extracted Minutia from the input image

After minutiae extraction, the hash code is generated from minutiae features using MD5 algorithm. Once the user enters his finger print at ATM client, hash code is generated at client side from fingerprint minutiae. The hash code is transmitted and reaches the server, the server verifies the hash code with the hash codes stored in the server database and if the verification is successful the user is authenticated. Figure 4 shows hash code generation and user authentication based on hash.

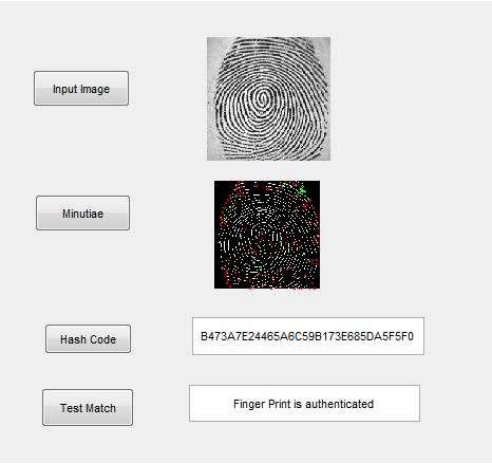

Figure 4: Hash code generation and User Authentication

60 % of images in the database is used for training, 20% for testing and 20% for validation .The performance of the proposed algorithm is measured by using the parameters false acceptance and false rejection rate.

5. Conclusion

Automatic Teller Machines are the most commonly used technology in today's world of growing financial transactions. ATM security using traditional PIN can be misused in a variety of ways. This paper presents security for ATM banking system using finger print and hashing techniques. Finger print hash code is used to uniquely identify the person. The proposed biometric and hashing techniques together for personal authentication improve the security level of ATM for efficient banking.

6. References

[1] Maltoni, D., Maio, D., Jain, A.K., Prabhakar, S.: Handbook of Fingerprint Recognition. Springer, New York, (2003).

[2] Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Kumar, V.: Biometric encryption.In Nichols, R., ed.: ICSA Guide to Cryptography. McGraw-Hill (1999)

[3] Das, I., Singh, S., Gupta, S. *et al.* Design and implementation of secure ATM system using machine learning and crypto–stego methodology. *SN Appl. Sci.* **1,** 976 (2019). https://doi.org/10.1007/s42452-019-0988-0.

[4] Zhang J, Lu Z, Li M (2018) A finger-vein extraction algorithm based on local Radon transform. In: 13th World Congress on intelligent control and automation (WCICA), July, (2018)

[5] Hussah Adnan Alzame, Muneerah Alshabanah, Mutasem K. Alsmadi, "Point of Sale (POS) Network with Embedded Fingerprint Biometric Authentication", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN: 2395-602X, Print ISSN: 2395-6011, Volume 6, Issue 5 (2019).

[6] Christiawan, B. A. Sahar, A. F. Rahardian and E. Muchtar, "Fingershield ATM – ATM Security System using Fingerprint Authentication," *2018 International Symposium on Electronics and Smart Devices (ISESD)*, Bandung, Indonesia, 2018, pp. 1-6, (2018) doi: 10.1109/ISESD.2018.8605473.

[7] Mahesh Patil and P. Sachin, "ATM Transaction Using Biometric Fingerprint Technology", *International Journal of Electronics*, vol. 2, (2012).

[8] G. R. Jebaline and S. Gomathi, "A novel method to enhance the security of ATM using biometrics," *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015]*, Nagercoil, India, 2015, pp. 1-4, (2015) doi: 10.1109/ICCPCT.2015.7159391.

[9] Onyesolu, M. O., & Okpala, A. C. (2017). Improving Security Using a Three-Tier Authentication for Automated Teller Machine (ATM), (October), 50–56 (2017). https://doi.org/10.5815/ijcnis.2017.10.06.

[10] Rachmawati, Dian & Tarigan, Jos & Ginting, A. A comparative study of Message Digest 5(MD5) and SHA256 algorithm. Journal of Physics: Conference Series. 978. 012116. (2018) 10.1088/1742-6596/978/1/012116.

[11] Fingerprint Verification Competition (FVC2002), http://bias.csr.unibo.it/fvc2002/download.asp