Encrypted Biometric Authenticated ATM System – An Overview

Mannat Doultani, Riddhi Khole, Nidhi Rohra, Muheet Rashid, Nachiket Joag

Vivekanand Education Society's Institute of Technology, Mumbai, India

Corresponding author: Riddhi Khole, Email: 2018.riddhi.khole@ves.ac.in

Choosing a biometric framework helps provide Identity for a person based upon various anomalous characteristics and specialties. For various purposes, we use various methods of biometric identification. Fingerprint and Iris scanning are some of the challenging and prominent methods which provide challenging patterns. Taking the challenges to security into consideration, we choose to take our system ahead with the help of Fingerprint and Iris scanning. Inexpensive and easily available apparatus provides another opportunity to test the datasets more clearly and precisely with proper scanning. Using these frameworks can help provide various benefits for the ATM (Automated Teller Machine) systems. The current ATM card PINs are easily traceable and can be misused. To overcome this weakness in current ATM systems, along with the ATM card PINs the security can be much enhanced by combining the PIN, Fingerprint scanning, and Iris Scanning altogether. Every individual's Biometric details would be updated by the bank and linked to the bank account.

Keywords: Iris Scan, Fingerprint Scan, ATM, Biometric, Image Processing.

2021. In Rahul Srivastava & Aditya Kumar Singh Pundir (eds.), *New Frontiers in Communication and Intelligent Systems*, 605–614. Computing & Intelligent Systems, SCRS, India. https://doi.org/10.52458/978-81-95502-00-4-62

1 Introduction

Taking a look into the past several years, we see that people have become more conscious about their privacy and security. Moreover, the cases of theft and robbery have also increased in which a huge number of cases involve ATM robbery. Usually, Banks issue an ATM card along with a PIN to customers, which they use to withdraw cash, make online payments, etc. But these PINs can be easily noted down by someone or can be easily hacked. This means that in this modern world, going only with a PIN is not enough, the system needs to be more secure.

Biometric authentication can help improve this system and serve as a solution to this problem. Because of their uniqueness and permanence, bringing the Fingerprint and Iris scanning into this field can help to a much greater extent. Among all the people on this planet, nobody's fingerprint or iris scan is found to match with someone else. So, this can serve as an efficient way to go with. The biometric system includes two major phases, the first phase is the Enrollment phase and the second is the recognition phase. Usually, the Enrollment phase includes capturing the biometric data and generation of the digital image. Then pre-processing and post-processing are applied to clear unwanted data and storing the data into the database respectively. Verification or matching is done, in which a person's Biometric details are verified with the database.

2 Related Work

Throws light on the recent studies on the fingerprint recognition system and explains its conceptual as well as structural details including the four stages of fingerprint recognition process and the summaries of fingerprint databases along with their characteristics [1].

Narayan et al. [2] attempts to provide a comprehensive scoping of the fingerprint recognition process issues, address its major design and implementation problems, and provide an insight into its prospects.

Malathi et al. [3] proposes a method for an efficient and secured biometric-based user identification system based on minutiae mapping in order to extract the finger, iris and palm print and also discusses RC4, DWT algorithm for encrypting and hiding the information.

Ali et al. [4] discusses the four stages of fingerprint recognition but the main crux is upon the last stage of this process which is the matching (identification & verification) stage used to match two minutiae points by using the minutiae matcher method which uses the similarity and distance measures. It also calculates the accuracy of the system on the basis of FAR and FRR scores.

Patel et al. [5] focuses on the most important post-processing stage of fingerprint authentication process, viz. minutiae matching which is used to distinguish uniquely between various fingerprint patterns. An algorithm for minutiae score matching has also been discussed. The research work has been done using C# using a custom database of 100 fingerprint images from 25 different persons. Four different fingerprint images of the same finger have been used for the biometric fingerprint matching experiment. The enrolment of 25 fingerprint images has been done, and other fingerprint images of users have been matched with already enrolled fingerprint images. Finally, a similarity score has been calculated for differentiating between the original fingerprint image and the enrolled fingerprint image.

Bhuvaneshwari [6] aims to eliminate the use of ATM cards completely and to ensure better security. In the proposed system, the idea of using Aadhar number as user ID and fingerprint as password instead of the PIN number is discussed. After biometric verification, the user will be allowed to proceed with the transaction of their choice. In case of three successive wrong attempts, the account will be blocked.

The main motive is to replace the traditional insecure ATM transaction scheme using PIN which can be misused easily with a modern and a more secure biometric authentication scheme.

Gizuir et al. [7] presents the alternative to existing traditional cryptographic approaches that ensure the data integrity without the need to use the public key infrastructure and time-consuming process of encrypting and decrypting data. The solution proposed here uses the blockchain concept named Light Blockchain Communication Protocol (LBCP). This paper also compares the performance of classic encryption and proposed protocol.

Sevugan et al. [8] surveys the image quality of images acquired from a standard camera and recognizes the most imperative issues in this regard. The purpose of this project is to study the unique pattern of the iris in the human eye and measure the performance on the basis of various factors which introduce errors and influence the execution and accuracy of this idea like different types of noises and reflections from light sources.

Nithaya et al. [9] provides a timeline review of various iris recognition techniques, developed since 1993. It also talks about the iris recognition framework and iris databases.

Nanayakkara et al. [10] presents a literature survey related to the iris recognition system. The aim of this paper is to explore recent developments in iris recognition systems, the process flow and algorithms used in various stages of the iris recognition system.

Nawaz et al. [11] throws light on an ATM banking system with the help of an optimized and secured AES algorithm. To achieve an ATM system with less power consumption, the AES algorithm has been proposed in this paper using a combination of biometric and cryptography-based techniques. The paper also analyzes the speed metric of the processor and also compares it with other studies in ASIC technology to prove its efficiency.

Muley et al. [12] proposes an ATM banking system embedded with a fingerprint identification scheme to fasten the transaction process while escalating the security level.

Richard et al. [13] provides a summary of major iris recognition studies. It also discusses the most famous algorithms used in different stages of iris recognition.

Sangeetha et al. [14] talks about the fingerprint recognition stages and its application idea in ATM systems to make effortless and yet secure transactions.

Darlow et al. [15] proposes a deep neural network for minutiae extraction for formulating a post-processing procedure to determine precise minutiae locations. It also compares its performance with other minutiae extractors.

Ravi et al. [16] discusses the fingerprint recognition methodology using minutiae score matching algorithm (FRMSM) and also the block filter method for fingerprint thinning.

3 Proposed system

3.1 Fingerprint Authentication

Fingerprints have one of the finest degrees of accuracy among all biometric attributes and have been extensively employed by forensic professionals in criminal investigations. The flow of ridge patterns within the tip of the finger is referred to as a fingerprint. The ridge flow demonstrates anomalies in local regions of the fingertip, and the position and orientation of these anomalies are utilized to depict and match fingerprints. Human fingerprints are abundant with features called minutiae, which can be utilized as identity markings for fingerprint verification. We can have two key modules in fingerprint Authentication: Enrolment and encryption Module and Identification and Verification Module.

For this module, we will be extracting and matching minutiae using various algorithms. Pre-processing using the image enhancement and binarization techniques is done onto the fingerprints before they are inspected in order to ensure effective minutiae extraction from fingerprints of different quality.

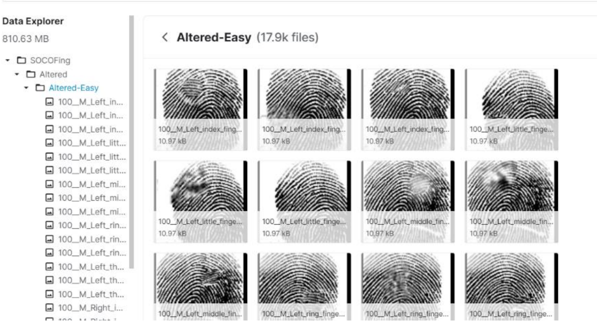

Fig. 1. Fingerprint Dataset

MINUTIA EXTRACTOR: This module consists of Pre-processing of minutia, Minutia extraction and Minutia Post-processing. Let us study each stage in detail.

Pre-processing*:* The pre-processing of fingerprint images is developed to increase the clarity of ridge structure. There are several phases to this procedure:

- **Image enhancement**: Enhancement of pictures is highly beneficial for retaining a greater accuracy in fingerprint recognition by boosting the contrast between ridges and valleys and connecting the false breakpoints of ridges. Histogram equalization and the Fourier transform are the two methods used to accomplish image enhancement. The goal of histogram equalization is to enhance perceptual information by expanding the pixel value distribution of an image.
- **Image binarization**: Since the fingerprints are obtained as grayscale photos, the ridges nevertheless fluctuate in intensity, despite the fact that they are indeed ridges. Binarization converts a 256-level image into a binary-level image that has the same information. A value of "1" is typically assigned to an object pixel, whereas a value of "0" is assigned to a background pixel. Finally, based on the label of each pixel, a binary picture is formed by colouring each pixel white or black (black for 0, white for 1). The fingerprint image is binarized using a locally adaptive binarization approach. This approach divides the image into 16x16 blocks, calculates the mean intensity value for each block, and then turns each pixel into 1 if its intensity value is greater than the mean intensity value of the current block to which the pixel belongs.
- **Image segmentation**: Only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check, while the second is done using some Morphological methods.

Minutiae extraction: The purpose of a fingerprint feature extraction program is to find, measure, and encode ridge ends and bifurcations. The features of a fingerprint picture can be extracted using a variety of ways.

- **Thinning**: Ridge Thinning is the process of removing unnecessary pixels from ridges until they are only one pixel wide. The algorithm adopted is an iterative parallel thinning approach. This technique notes down redundant pixels in each small picture window (3x3) after each scan of the whole fingerprint image and then removes all those marked pixels after numerous scans.
- **Minutia Detection (marking)**: It's fairly easy to designate minutiae spots after the fingerprint ridge has been thinned. For extracting minutiae, the idea of Crossing Number (CN) is commonly employed. In general, if the center pixel in a 3x3 window is 1 and has exactly 3 one-value neighbors, that pixel represents a ridge branch [Figure 4.2.1]. If the center pixel is 1 and has only one one-value neighbor, it is a ridge ending; that is, given a pixel P, if Cn(P) = 1 it is a ridge end, and if Cn(P) = 3 it is a ridge bifurcation point.

Minutia Post-processing: False minutiae Removal: All of the preceding stages of pre-processing minutia can sometimes introduce artifacts that lead to false minutia. If these fake minutiae are simply accepted as genuine, they will have a major impact on matching accuracy. To keep the fingerprint verification system successful, some strategies for deleting erroneous minutiae are required.

MINUTIA MATCHER: The minutiae matcher's function is to compare the acquired feature to the database template. In other words, the matching step calculates the degree of similarity between an input test image (for the user to establish his or her identity) and a database training image (the template which was created at the time of enrolment).

An alignment-based match algorithm is employed which comprises of two successive stages: one is the alignment stage and the second is match stage.

- **Alignment stage**: Choose any minutia from each of the two fingerprint images to be matched; calculate the similarity of the two ridges associated with the two referred minutiae spots. Transform each set of minutiae into a new coordination system whose origin is at the reference point and whose x-axis is coincident with the direction of the referred point if the similarity is greater than a threshold.
- **Match stage**: We use the elastic match technique to count the matched minutia pairs when we have two sets of altered minutiae points. We assume two minutiae with approximately the same position and directions are identical.

3.2 Iris Authentication

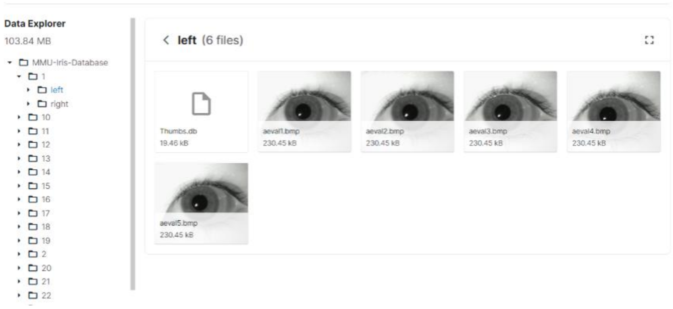

Fig. 2. Iris Dataset

For iris scanning, visible and near-infrared light scanners are used to take a high contrast image of the user's iris. These scanners detect and capture the iris. The scanning camera can be mounted near the ATM machine. After the image is captured, the following methods are processed:

1. **Segmentation:** In segmentation a digital image is partitioned into multiple segments. Here, the actual iris region is isolated from eyelids and eyelashes. This helps in extracting the required features of the iris. For this, we propose two methods for segmentation:

- Hough transform (time efficient but less accuracy):
  In image processing, the commonly used algorithm to detect geometry of objects is Hough Transform. Circular Hough transform is used to detect radius and centre coordinates of pupil and iris region and parabolic Hough transform is used to deduce eyelids.

- Daugman Integro-differential operator(time consuming but more accurate)
  It locates the iris and pupil region along with the border of iris. This method gives better segmentation results.

2. **Normalisation:** After the iris region is segmented successfully from the eye, normalization is performed. It produces the iris region by nullifying the effects of dimensional inconsistencies. It transforms a segmented image into a fixed dimensional rectangular box and polar conversion of the iris image is done. The following equation is used to convert cartesian coordinates to polar coordinates.

$$x1 = x + r * \cos(\mathrm{F})$$
$$y1 = y + r * \sin(\mathrm{F})$$

Fig. 3. Daugman rubber sheet model

3. **Feature extraction:** The next stage is feature extraction where significant information is extracted from the iris pattern. The extracted features are encoded to generate unique mathematical templates for the iris. Gabor filters are widely used for feature extraction. This filter is sensitive to textures with specific orientation and wavelength. Based on feature extraction, unique iris templates are generated.

These steps will be performed at the bank when a customer opens an account at the bank; complete details of the customer are stored at the banking terminal and at the ATM when the biometric authentication block is initialised. Then the image captured at the ATM is sent to the bank when matching takes place.

4. **Matching:** At the matching stage, both the iris templates: iris template received from ATM and template stored at the Bank's database, are compared to check similarity and dissimilarity. Bitwise comparison is performed using the Hamming distance metric. The other proposed equations are Weighted Euclidean distance and Canberra distance metric.

3.3 Encryption

The proposed system aims to improvise the existing systems by introducing new technologies. It ensures ease of access to the customers and a multi-layer secured system for transactions.

Furthermore, we plan to ensure a more secure system by incorporating the concept of blockchain in the solution. Blockchain technology uses strong encryption algorithms to keep the data secure in decentralized ledgers that can only be accessed by those by the one in authority, or if the authoritative figures have granted others access.

Fingerprint image and image of eye acquired from the ATM is enhanced, features are extracted and then encrypted using 128-bit private key algorithm. This encrypted data along with user's details and transaction details is added to a block in the chain and transmitted to the central banking server via a secured channel. At the bank, the encrypted record of biometric data of customers is stored in the system using a fingerprint scanning device and iris infrared scanner. For authentication the data is decrypted and matching is done. If the matching score is above the threshold value, User is authenticated and the transaction is successful. If the matching score is below threshold value, the user is invalid and the transaction is denied.

4 Modular Diagram

The system consists of two main segments, one is the Customer segment (ATM interaction Module) and the second is the Banking segment. Each segment consists of several modules to deal with.

The first segment consists of:

1. Swipe Card Module: The user needs to swipe the card in the machine and all the required details such as Card number, CVV, etc will be fetched.
2. Enter PIN Module: The user will be asked to enter the PIN to get further access to the account.
3. Perform Transaction Module: This module consists of several operations that a user may want to perform. Such operations include Cash-Withdrawal, Balance Enquiry, PIN change, etc.
4. Biometric Authorization Module: The user will be asked to provide his Bio-metric details such as Fingerprint Scan and Iris Scan through physical fingerprint and eye scanning respectively.
5. Transaction Denied and Confirm Transaction Module: These modules are Confirmation modules that confirm the status of a transaction.

The second segment consists of:

1. Register User Module: This module provides a method for the Registration of new users. Whenever a case of New User registration would arise, this module would be used to add the user details such as Name, Address, Mobile, Biometric Data, etc.
2. Edit User Module: To edit or make some changes in the existing users' data, this module is created. Changes may be in the Name, Address, Mobile number, e-mail.
3. Delete User Module: To remove a customer's account or to delete any customers' account permanently this module would be used.
4. Store in Database Module: Saving or storing the newly added user data or modified user data into the database would be carried out by this module.
5. Biometric Authentication Module: Matching the current Biometric data of a customer (provided via ATM), to the saved customer's Biometric data in the database would be carried by this module. This is the Verification Module.

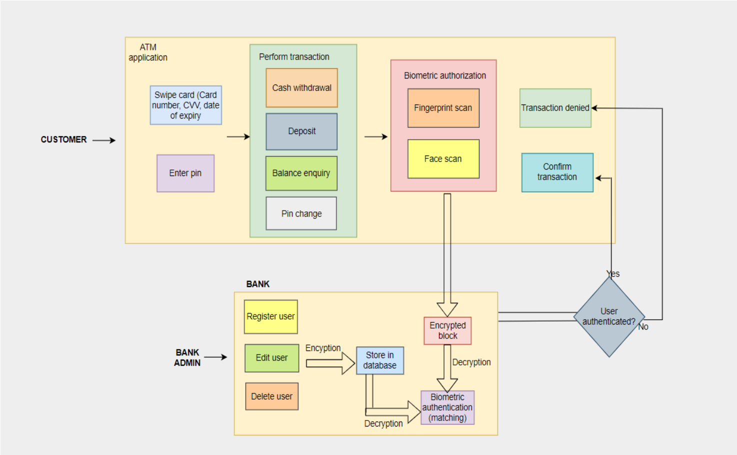

Fig. 4. Modular diagram of the system

5 Block Diagram

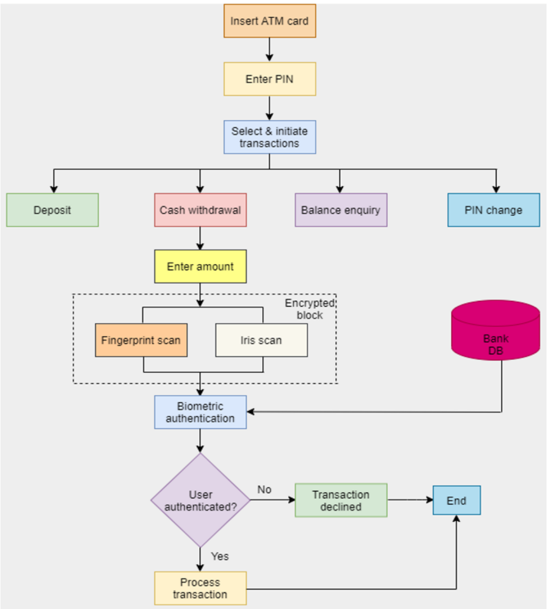

Fig. 5. Block diagram of the Querencia system

The functioning will start from swiping the ATM card and end with a message whether the Transaction was successful or not.

The user needs to enter the ATM card into the swipe folder of the machine, followed by Entering the card PIN provided by the bank or set by the user. A series of options will be provided on the screen of the ATM system after the user has entered the card PIN, the user will choose a single option according to his need/requirement.

If the user goes with the Cash-Withdrawal option, then he needs to enter the amount that he/she wants to withdraw.

Now, the user will be asked to prove his/her identity, by authorizing their Biometric data i.e., by scanning Fingerprint and Iris. Scanning will then lead to feature extraction and matching of the extracted data with the bank Database.

If the data matches with the bank Database, the Transaction status will be shown as Successful otherwise the transaction would be declined.

6 Limitations

1. Some people (majorly senior citizens and illiterate people) may not feel comfortable to use the technology-packed system due to digital illiteracy and/or less technological acquaintance and hence may hesitate to use it.
2. Not suitable for people with eye problems (e.g. cataract surgeries which can alter the iris patterns in the eye leading to errors in biometric verification and hence would lead to a failure during user authentication)
3. Not suitable for totally blind people.

7 Conclusion

1. Although the biometric authentication system has been employed today in mobile phones and laptops heavily and for recording attendance in many schools and colleges, it has not been implemented in any other domain so extensively, especially in the banking sector. Our solution could serve as a good attempt to utilize the biometric system in banking effectively as it is a blend of biometric and cryptography techniques.
2. When implemented using Blockchain technology, it is extremely difficult or rather almost impossible for the attackers to tamper with the system and bypass the 3-layer authentication procedure illegally. Thus, our proposed system guarantees a great level of security altogether.
3. Such systems when deployed at banks would be preferred by the customers which will indirectly have a positive impact on the business of banks.
4. The biometric system is revolutionizing globally and many industries are innovating its usage across their products for the convenience and safety of their customers.

8 Future scope

1. Introducing the concept of nominees for user authentication: In cases of emergency such as an accident or death of an account holder, his/her biometric patterns cannot be used for authentication. In such scenarios, his/her closest relative/s should be allowed to access the account. Hence, their

fingerprint and iris patterns have to be stored in the database right at the time of the biometric registration of the account holder while opening a new bank account.

2. Detection of fingerprint forgery: Detecting attempts of identity theft and violation and bypassing of the fingerprint authentication mechanism by using machine learning algorithms, raising a red flag immediately and reporting such cases to concerned authorities.
3. Mobile app: A mobile app (for the respective bank) may be developed to authenticate the users directly via app (for those with mobile phones having a built-in fingerprint scanner and a camera) to further escalate their user experience.

References

[1] Ali, M. et al. (2016). Overview of Fingerprint Recognition System. In *International Conference on Electrical, Electronics, and Optimization Techniques*, 1-5.

[2] Narayan, L. K. et al. (2020). Fingerprint and its Advanced Features. *International Journal of Engineering Research & Technology*, 9(4).

[3] Malathi, R. and Jeberson, R. R. R. (2016). An Integrated Approach of Physical Biometric Authentication System. *Procedia Computer Science*, 85: 820-826.

[4] Ali, M. M. H. et al. (2016). Fingerprint Recognition for Person Identification and Verification Based on Minutiae Matching. In *IEEE 6th International Conference on Advanced Computing (IACC)*, 332-339.

[5] Patel, R. B., Hiran, D. and Patel, J. (2021) Biometric Fingerprint Recognition Using Minutiae Score Matching. In *Kotecha K., Piuri V., Shah H., Patel R. (eds) Data Science and Intelligent Applications. Lecture Notes on Data Engineering and Communications Technologies*, 52. Springer, Singapore.

[6] Bhuvaneshwari, J. (2019). *SECURE & ENHANCED ATM WITH BIOMETRIC AUTHENTICATION.*

[7] Guziur, J. et l. (2018). Light Blockchain Communication Protocol for Secure Data Transfer Integrity. In *Castiglione A., Pop F., Ficco M., Palmieri F. (eds) Cyberspace Safety and Security. CSS 2018. Lecture Notes in Computer Science*, 11161. Springer, Cham.

[8] Sevugan, P. et al. (2017). IRIS RECOGNITION SYSTEM. *International Research Journal of Engineering and Technology*, 4(12): 864-868.

[9] Nithya, A. and Lakshmi, C. (2015). Iris recognition techniques: A Literature Survey. *International Journal of Applied Engineering Research*, 10(12): 32525-32546

[10] Nanayakkara, S. and Meegama, R. (2020). A Review of Literature on Iris Recognition. *International Journal of Research*, 1-10.

[11] Ali, N. et al. (2013). Biometric Authentication Scheme for ATM Banking System Using Energy Efficient AES Processor. *Electrical Engineering Research*, 1(2): 1-5.

[12] Muley, A. and Kute, V. (2018). Prospective solution to bank card system using fingerprint. In *2nd International Conference on Inventive System and Control*, 898-902.

[13] Ng, R. et al. (2008). A review of iris recognition algorithms. In *Proceedings of International Symposium on Information Technology*, 1-7.

[14] Sangeetha, T. et al. (2021). Biometric based fingerprint verification system for ATM machines. *Journal of Physics: Conference Series, Volume 1916, 2021 International Conference on Computing, Communication, Electrical and Biomedical Systems (ICCCEBS), 25-26.*

[15] Darlow, L. N. and Rosman, B. (2017). Fingerprint minutiae extraction using deep learning. In *IEEE International Joint Conference on Biometrics (IJCB)*, 22-30.

[16] Ravi, J., Raja, K. B. and Venugopal, K. R. (2010). Fingerprint Recognition Using Minutia Score Matching. *IJEST*, 1(2): 35-42.