International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 1 Issue 8, October - 2012

Multilevel ATM Security Based On Two Factor Biometrics

Pooja Mali Shruti Salunke Rajashri Mane Pooja Khatavkar

Pimpri Chinchwad College of Engineering,Nigdi 44

Abstract

Security management for networks and data is an issue now-a-days. Fraudsters are increasing day by day introducing new hacking techniques. Our objective is to provide network security for real time application, ATM System. For security purpose PIN, thumb scanning and face recognition are considered. It is observed that thumb is most popular biometric among other biometrics like iris, DNA etc. When anyone wishes to use ATM system he has to follow authentication hierarchy i.e. PIN, thumb and face validation. At the time of registration only, user needs to register thumb and face pattern. These biometric patterns are stored at a server side in encrypted format. Using stegnography data like PIN, thumb pattern and face pattern is hidden at server side. Authentication is done by decrypting patterns from database, and matching with input pattern. After authentication, user will get access for ATM operations. For face recognition PCA and Eigen algorithm, for stegnogaphy LSB algorithm and for cryptography AES algorithm is used. Combining these three algorithms, a proposed system is designed.

Keywords – ATM System , Thumb Scanning, Face Recognition, Encryption, Decryption, Stegnography.

1. Introduction

Today's existing ATM system has only one security factor i.e. 4- digit PIN validation.
According to Cambridge researchers, they have documented a worrying PIN cracking technique against the hardware security modules commonly used by bank ATMs. It is possible to crack the PIN in an average of 15 guesses. According to survey the average debit card fraud amount was $2,529 in 2010.
Some of the major ATM attacks are as follows:
1) Skimming Attack:

This attack involves all the details of user using portable small card reader device known as skimming device to capture users ATM card details including PIN, card number. Skimming device can retain information from 200 ATM cards before using it.

2) Card Trapping:

Card trapping is a major attack in ATM. This attack is occur when the person insert the card in ATM, that card is physically capture by inserting a strip of metal or sleeve of metal or plastic called loop. When the card is inserted, the loop holds the card then cardholder type PIN and request for his funds.

3) PIN Cracking

ATM PIN is the primary security against ATM fraud. For cracking the PIN, the program is written in such a way that tries the PIN for particular account and this require average of 5000 transactions to discover each PIN. Also hackers have only three guesses to match against 10,000 PINS.

4) Phishing/Vishing Attack

In this technique hacker send the fraud email to the user about incompletion of bank data and request for completion of all account details by clicking on given fraud link. In such a way hacker hacks the PIN of particular account.

5) ATM Malware:

The person who is having the key of ATM, inserts the malware into system and inserts the control card into machine's card reader to trigger the malware which contains all recent transaction information from primary memory.

6) ATM hacking:

In ATM hacking hacker attacks on bank system and locate the ATM database for collecting the card information. [2]

Fraud, in these circumstances, might be still possible. The attack is simply and more powerful, optimized means of cracking PIN numbers. To overcome these types of attacks we are proposing the "Multilevel ATM Security Based on two Factor Biometrics". In this system we are using biometric features of particular user to secure ATM access. For authentication hierarchy of various biometric factors i.e. thumb and face along with 4-digit PIN is used. Also at server side for security purpose encryption of data and hiding that data stegnography is used.

2. Related Work

In iris biometric is used for network security at client side and cryptography and stegnography at server side using MD5 algorithm. But iris biometrics is more costly and only 6% people know it. [1]

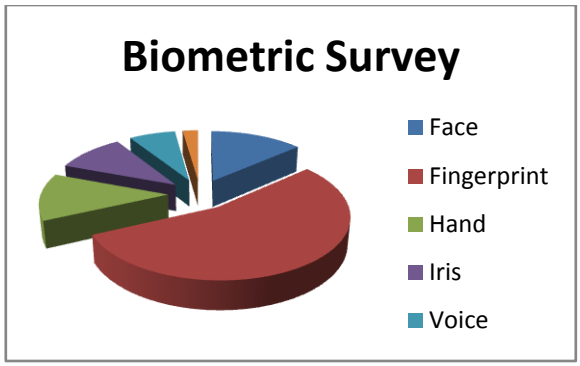


Fig1.Comparative survey of fingerprint with other biometrics

According to investigation study [3] of 2012 fingerprint biometrics is more popular than other biometrics. Fig 1. Shows the percent use of biometrics. Paper [4] uses face recognition technique for verification in ATM system. Different facial expressions and patterns can be analyzed using PCA algorithm.

In [5] the implementation of ATM security system using fingerprint and GSM model gives the advantages of stability and reliability. Global system for mobile phones provides the standard in the world but the drawback is due to insufficient range of mobile couldn't access the security code of ATM PIN.

3. Proposed System

ATM and banking security and protection of its data have been of great concern and a subject of research over the years. There are many different forms of cryptographic mechanisms like AES, Triple DES, MD5 proposed to guarantee data security. In a network, the success of the algorithm depends on the length of the key (PIN) that user uses. It is observed that due to convenience of remembering the key (PIN), user uses short keys (4 Digits). This increases the vulnerability of the data.

In this work we propose a unique authentication and encryption technique using two factor biometric pattern of a person. At the time of registration to the network, a person's face is scanned and phase features of the image are generated. Therefore a local binary code of sixty four byte is

extracted of this matrix and is transmitted to the server. Server stores this key as user's identity or password. Then the user thumb is scanned and its features are extracted and stored in server database.

At the time of transaction, user needs to swap ATM card and PIN is accepted. The accepted PIN is encrypted and sends to the server for validation purpose. At the server side encrypted PIN is decrypt and match with the server side database. If the PIN is validated then that user's face and thumb pattern is extracted and send to the client side. At client side, after matching the PIN thumb is scan and face image is capture and match with the extracted pattern by using Euclidian distance. If the face and thumb pattern matches then only user is authenticated and allow for ATM access. The success of the technique depends upon the quality of the scan and recognition rate. There is always an error margin of 5% to 10% when face code is generated which may result in an unsuccessful authentication. Therefore at the time of registration, we scan the person's face twice or thrice and generate code. Storing the rough key in the server is not safe as if the server data is hacked, then these keys can be easily tampered with. Hence rather than storing the rough keys, we embed them in random images using steganographic means and store the image binary in the server. Thus not only the data in the network, but also the server data is secured.

The main purpose of this system is to design and implement a system that read RFID Card, captures thumb and captures face images, stores, compares and authenticates over a network system.

It basically consists of 2 main components

1. The server machine:

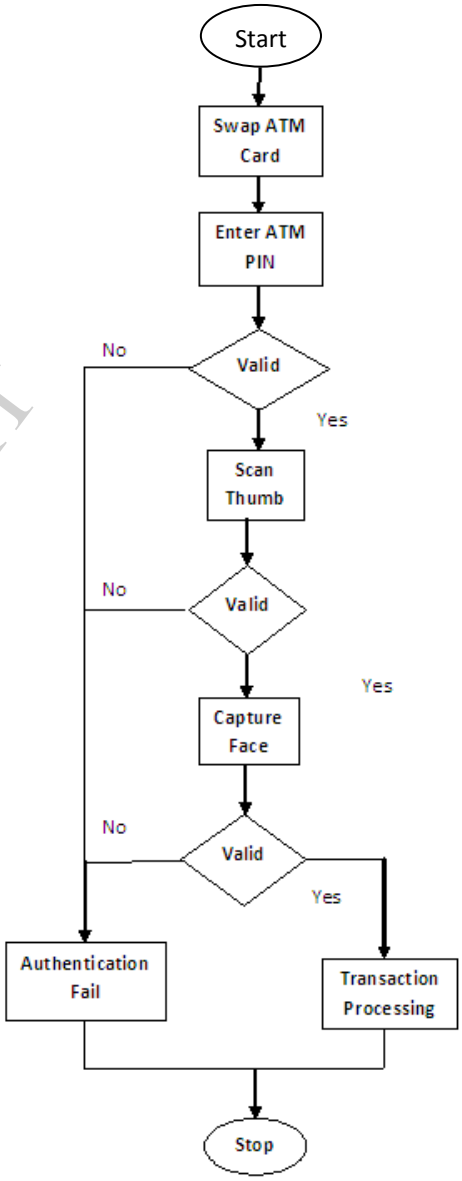
The server machine is the heart of system. All authentic and authorized users are stored on this machine. On comparison, if the user's data matches with any one of the stored data, then in that case the server returns success or else it return failure.

2. The client machine

The main job of the client machine is to read RFID, capture a thumb, capture face and send it to the server for authentication. Its main tasks are:

1)Initializing RFID Reader, scanner & camera.
2) Read RFID Card, accept the PIN
3) If the PIN is validated then scan the thumb and capture the face.
3) Checking to see if the data is valid or not.
4) If the data is valid, then sending it to the server for transaction.
5) Waiting for a response from the server.
6)Conveying the result to the user, depending on the status returned by the server.

4. System Flow Diagram



5. System Architectural Diagram

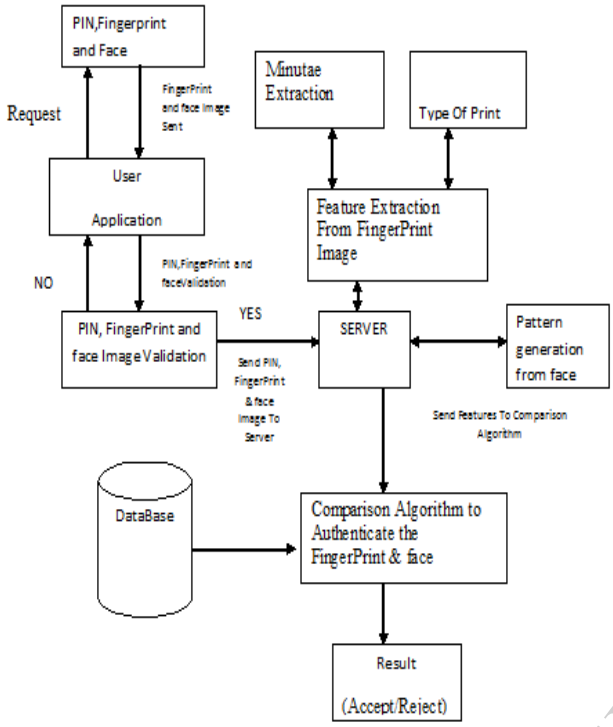


Fig 2.System Architecture

In our proposed system we are using following algorithms:

1) Face recognition :- PCA and Eigen
2) Cryptography :- AES
3) Stegnography :- LSB

5.1 Thumb recognition system is made up of:

- A sensor to record
- A computer unit to process
- An application for which authentication is necessary

5.2 LSB

LSB is a Least Significant Bit used for hiding the user information at server side for providing the more security.

Advantages of LSB:

1) High perceptual transparency.
2) Low degradation in the image quality
3) More and more commercial software available which follow this approach.

Block-diagram of a fingerprint system

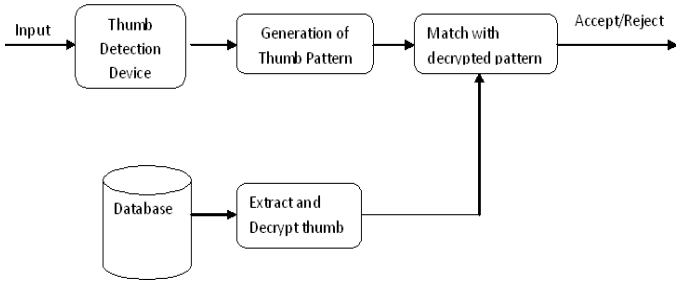


Fig 3. Block diagram of a fingerprint system

5.3 AES

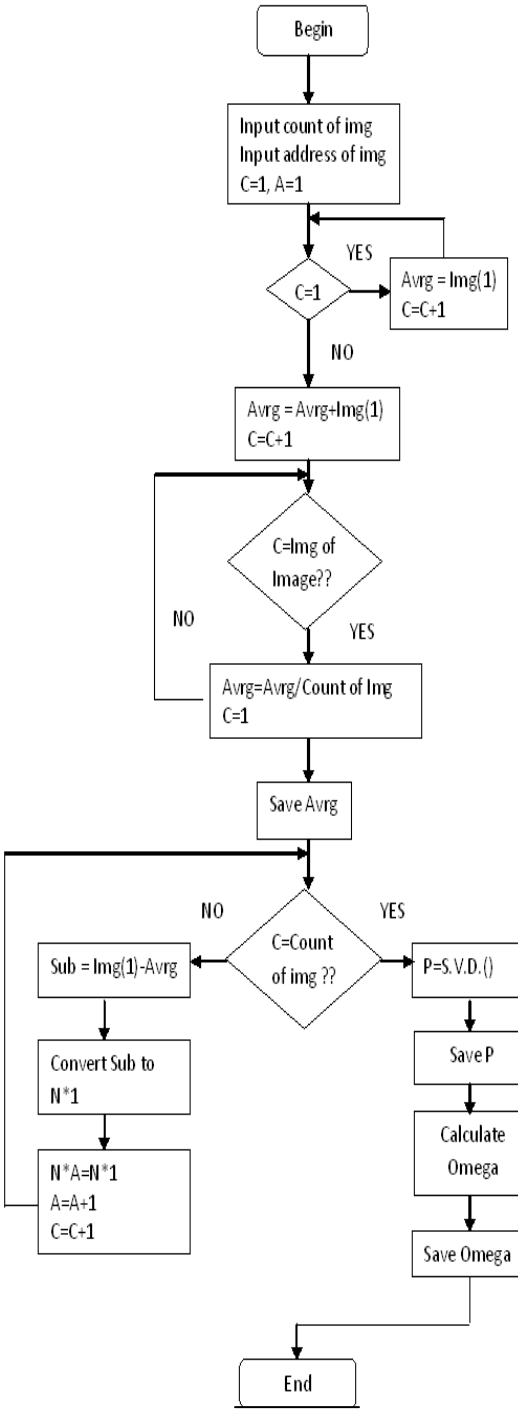
AES is an Advanced Encryption Standard used for secure transmission of data in encrypted format. In our system AES is used for sending user authentication data (PIN) in encrypted format.

Advantages of AES:

1) AES is more secure and powerful
2) It provides the key length of 256 bits.

5.4 PCA and Eigen

Fig 4.Face Recognition Flow Chart: Using Eigen Algorithm [5]



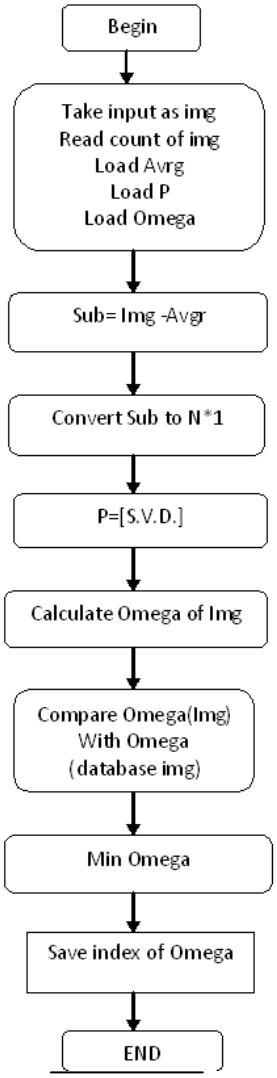


Fig 5. Face Matching Flow Chart: Using PCA Algorithm [5]

6.Advantages of proposed system

1) Multilevel security at client side using cryptography algorithm and user's biometric features.
2) Biometric features cannot be easily hack because of its unique identification.

3) At server side stegnography algorithm is used for hiding the encrypted information.

7. Applications

1) Voting system
2) Passport system
3) Data centers applications
4) E-Commerce

8. Conclusion

The network needs security against attackers and hackers. Network Security includes basic securities to protect the information from unauthorized access and loss. ATM access is not more secure using 4 digits PIN. This paper proposed the new approach for existing ATM system for providing more security using biometric features which plays an important role because these are unique and not easily hackable.

9. References

[1] V.V.Satyanrayanarayana Tallapragada, Dr. E.G.Rajan "Multilevel Network Security Based on Iris Biometric" Pentagram Research Center,Jubilee Hills, Hyderabad, India,2010

[2] Lawan Ahmed Mohammed "Use of biometrics to tackle ATM fraud" King Fahd University of Petroleum and Minerals HBCC Campus, Hafr Al Batin 31991, Saudi Arabia, vol.1 (2011)

[3] Moses Okechukwu Onyesolu "ATM Security Using Fingerprint Biometric Identifer: An Investigative Study", Vol. 3, No.4, 2012

[4] Peter, K.J.; Nagarajan, G.; Glory, G.G.S.; Devi, V.V.S.; Arguman,S.,Kannan,S."Improving ATM security via face rec ognition",2011

[5] Vinay Hiremath, Ashwini Mayakar "Face recognition using eigenface approach" malardalen university, vasteras, sweden.

[6] Vijay Kumar Sharma, Vishal Shrivastava "A steganography algorithm for hiding image in image by improved lsb substitution by minimize detection "

[7]Pennam Krishnamurthy,M.Madhusudan Reddy "Implementation of ATM security by using fingerprint recognition and GSM"