Fingerprint based ATM System

ANKIT SINGH

Abstract

Biometric system is a pattern identification system that recognizes an individual by determining the originality of the physical features and behavioral characteristic of that person. Of all the recently used biometric techniques, fingerprint identification systems have gained the most popularity because of the prolonged existence of fingerprints and its extensive use. Fingerprint is dependable biometric trait as it is an idiosyncratic and dedicated. It is a technology that is increasingly used in various fields like forensics and security purpose. The vital objective of our system is to make ATM transaction more secure and user friendly. This system replaces traditional ATM cards with fingerprint. Therefore, there is no need to carry ATM cards to perform transactions. The money transaction can be made more secure without worrying about the card to be lost. In our system we are using embedded system with biometrics i.e r305 sensor and UART microcontroller. The Fingerprint and the user_id of all users are stored in the database. Fingerprints are used to identify whether the Person is genuine. A Fingerprint scanner is used to acquire the fingerprint of the individual, after which the system requests for the PIN (Personal Identification Number). The user gets three chances to get him authenticated. If the fingerprints do not match further authentication will be needed. After the verification with the data stored in the system database, the user is allowed to make transactions.

Keywords: ATM, PIN, r305, UART, Embedded System, Biometrics, Fingerprint Verification, Recognition, ATM (Automatic Teller Machine) Terminal, Features Extraction

I. INTRODUCTION

Of all the biometrics, fingerprint recognition is one of the most dependable and promising personal identification technology. Fingerprints play an important role in biometric system. In biometrics technology, fingerprint authentication has been in use for the longest time and bears more advantages than any other biometric technologies. Fingerprints are the most widely used biometric feature for an individual identification and verification. We have proposed fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its characteristics like availability, reliability and high accuracy. The fingerprint based biometric system can be implemented easily to secure the ATM machine. In this system the working of these ATM machine is when the customer places his finger on the fingerprint module when he needs to access the ATM to withdraw the cash then the machine processes the fingerprint of the user. With the help of biometrics, it verifies and identifies the fingerprint and gives accurate result that if it is valid or not. In this way we can try to control the criminal activity of ATM and secure it.

The present scenario to operate an ATM is with digital locks that have keys. Individually biometrics lags behind in providing hundred percent protections. To provide perfect security and to make our work easy we are using two different technologies i.e. Biometrics with Embedded system.

First of all we are gathering the information related to Fingerprint enrollment phase. This module is interfaced with the PC via Visual Basic front end page so that user should store the images when accessing the ATM and when accessing the ATM if the images match only then the transaction can proceed further.

To initiate the application, the fingerprint of the person is entered and it is stored into database as a template. To login into application user has to scan his/her fingerprint, if it matches with the pre-stored images then the person has to enter the unique id which is given to him to access his ATM. An unauthorized person tries to login then the user will be alarmed with the help of a buzzer which is linked with the controller. An authorized user is given 3 chances to re-enter the id if he/she forgets.

In order to avoid criminal activities like man-in-the-middle attacks, biometric authentication system is implemented. Fingerprint based ATM system is one of the secure system. In this system, we are implementing ATM system based fingerprint authentication. System keeps certain space within Flash for fingerprint template storage, i.e fingerprint collections. Capacity of the library changes according to the capacity of Flash memory, system recognizes the latter automatically. Fingerprint template's storage in Flash is

in systematic order. Let us consider the fingerprint storage capacity N, then the serial number of template in library is 0, 1, 2, 3 ... N. User can only access library by its template number, so we are storing image as a template in database and then matching the saved image with the input image and if the image does not match further authentication is done to proceed with the transaction.

A fingerprint recognition system can be used for both verification and identification to make the system more secure. In verification, the system compares an input fingerprint to the fingerprint stored in the database of a specific user to determine if they are from the same finger (1:1 match). In identification, the system compares an input fingerprint with the prints of all registered users in the database to determine if the person is already known under a replica or false identity (1: N match).

Fingerprint has distinct feature that do not change for whole life and they are easy to use, cheap and the most suitable miniaturization. So, fingerprint verification is an efficient and secured method that has been the most widely used in comparison with other biometric information.

II. LITERATURE SURVEY

Euclidean distance and principal lined mechanism use unimodal system to multimodal system conversion. The conversion is carried out since unimodal system is very sensitive to noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. The proposal includes an extraction algorithm to acquire features from given fingerprint and a palm print feature extraction algorithm to acquire palm print features. Then an integration of these two algorithms to perform a multibiometric authentication was done. Matchers inappropriately handle the distortion and noise, despite huge computational cost [1].

Image is preprocessed using a new hybrid Modified Gabor Filter-Hierarchal Structure Check (MGF-HSC) system model based on an MGF integrated with an HSC. To ameliorate the accuracy of financial infrastructure, face biometrics are introduced using a fast principal component analysis algorithm, in which different face conditions such as lighting, soften, pose, head orientation and other conditions are addressed. The fingerprint characteristics are captured with the help of fingerprint scanner and the captured fingerprint produces a stream of distortions and misalignments [2].

The concepts of Cryptography and Steganography are known to us. In fingerprint based ATM system, they intend to use the finger print image captured by the fingerprint scanner as the BASE image. Using the concept of steganography, they hide the AES 256 encrypted code (PIN + OTP) inside the fingerprint image. In our system, AES encryption algorithm has slow performance and the images are slightly distorted. The key size will determine the time taken to encrypt and decrypt the message which hinders efficient communication. Steganography causes significant damage to the picture appearance and thus it is difficult to recover [3].

IBIO stands for Iris recognition based Biometric verification is also provided for ATM banking system. 2D-Gabor filter AND hamming distance was chosen as a matching metric. Encryption and decryption is performed on test image. The Hamming Distance measures the same bit patterns. A 2D Gabor wavelet is implemented in the feature extraction is formed based on the Iris rectangular block. This system is also based on cloud. The methods used in this system are very slow. It is not financially feasible on such a large scale [4].

Encryption - decryption, Blowfish algorithm, hit and miss algorithm and biometric authentication are well known concepts used for authentication processes. The client's biometric image is captured and it is encrypted using blowfish algorithm at the client's side. The methods involving the minutiae extraction are binaries fingerprint images and Gray Scale Fingerprint Images. The encrypted image is then sent through secured network to the server. In the server side the image is decrypted. While performing the transaction, the hit and miss algorithm is used to identify the core points since the image fed may vary in angle from the enrollment image. When the data is available in the cloud, data can be easily retrieved for fraudulent activity, which is the drawback. Blowfish implementations use 16 rounds of encryption, and are not susceptible to known-plain-text attack [5].

All the fusion techniques which have been done on the particular biometric traits were discussed. Finally, the normalization methods and the metrics used for evaluating the biometric system are discussed. Handling of data in all dimensions creates more problems. Thus, to reduce this problem Dimensionality methods are used. There are two types' linear and nonlinear methods. The fusion techniques are used when two or more biometric characteristic are taken into consideration for authentication or authorization. An important problem with biometrics is compromised biometrics with somebody else. To solve this problem biometric crypto system, (BCS), and cancellable biometric systems can be used [6].

Fingerprint recognition approach can be investigated by local robust features extraction and matching. First the local features are extracted using Speeded-Up Robust Feature (SURF) algorithm. The Euclidean Distance is used to verify the test Fingerprint with data base fingerprint. The input fingerprint images are compared with two or more exiting template image features for matching. The matching method uses a matching threshold. The SURF relies on determinant of Hessian matrix for both scale and location. SURF is a scale and rotation invariant algorithm, it can extract features in presence of rotation, scaling and partial distortion of the test image [7].

One of the prominent methods to design and implement an Embedded Fingerprint Authentication system operates in two stages: minutia extraction and minutia matching. Hardware-software co-design responsible for matching two fingerprint minutiae sets and suggests the use of reconfigurable architectures for Automatic Fingerprint Authentication System. This paper explains the detail implementation of a fingerprint algorithm using a Spartan-6 FPGA, as an appropriate portable and low cost device. The microprocessor runs with high accuracy, but with less speed for applications which are using the minutiae based fingerprint matching algorithm. The measurement on Laptop may not be accurate due to problems of real-time constraints not supported by

magnitude order [8].

Studying several of IEEE papers, we analyzed various advantages and disadvantages of methods used in the past systems. The fingerprint images that were captured with a Futronic fingerprint scanner produced a stream of distortions and misalignments. Steganography causes a huge damage to the picture's appearance and thus it is difficult to recover. IBIO system is slow and it is not financially feasible. Some systems used cloud for storage, when the data is available in the cloud, data can be easily retrieved for fraudulent activity, which is the drawback. Blowfish algorithm uses 16 rounds of encryption, and is not susceptible to known-plain-text attack. SURF is a scale and rotation invariant algorithm, it can extract features in presence of rotation, scaling and partial distortion of the test image. Embedded Fingerprint Authentication system uses microprocessor that runs with high accuracy, but with less speed for applications which are using the minutiae based fingerprint matching algorithm. The measurement on Laptop may not be accurate due to problems of real-time constraints not supported by Windows 7 Operating System (Win 7 OS), but this evaluation wants to emphasize the response time difference in terms of magnitude order.

III. PROPOSED SYSTEM

There are two main phases in our system i.e. enrollment phase and authentication phase.

A. Enrollment Phase

Enrollment phase is also known as the registration phase. In this phase an individual registers his fingerprint using the fingerprint scanner and stores it into the database.

B. Authentication Phase

In authentication phase, an individual is authenticated by matching the test image provided by him with the stored image i.e. it is checked that he is who he claims to be.

Detailed working of the subunits is as follows:

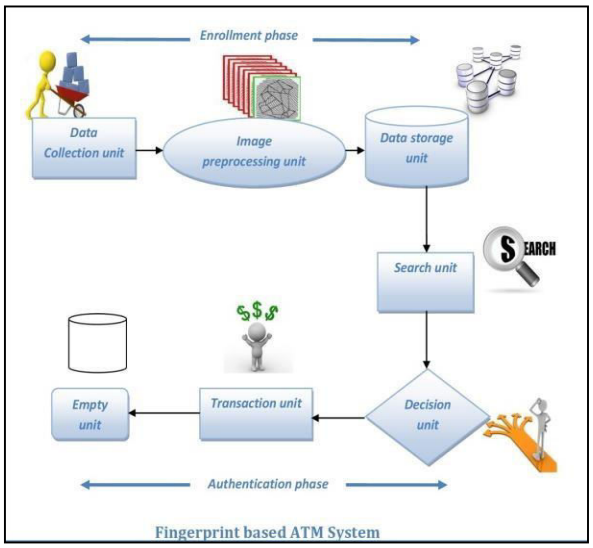

Fig. 1: Fingerprint based ATM System (*FlowChart)*

- Data collection unit: The most basic and equally important requirement for this stage is that of an optical sensor i.e. r305 optical scanner. The user fingerprints are collected in this unit. This unit adds a fingerprint of the user to database unit and further returns a byte every newly added ID. The return values range from 0x00 to 0xFE. The return code is 0xFF in case when there is an error, i.e. no finger is placed on the sensor. Here 0xFF means error executing function.

  Image preprocessing unit: The Scanner takes input of the image then the preprocessing is done on the image in the scanner during the processing time, test image is in the form of analog that is converted into digital form and if the quality of the preprocessed image is sufficient then the image is converted into the template.

  Data storage unit: Each preprocessed image is of certain template size (approximately 512 bytes per template). And the template is stored into the database for further use. This unit allows the user to store the fingerprint data in the module and further configure it in 1:1 mode for storing an individual's fingerprint.

  Search unit: A finger is placed on the fingerprint module (sensor) and the search function is called. The existing memory is then checked and returns a matching ID if found.

  Decision unit: The system compares the input image with those stored in the database. The database image is stored after several processes, so it would be easier during transaction. Stored template and test image is compared and the needed resolution of the test image is 500dpi (dot per inch). When the image comparison gets satisfied, then the user of the input is an authorized user.

- Transaction unit: if the decision making unit authorizes the user then the transaction is successfully carried out.
  Empty function: This function is used to empty the database containing fingerprints stored in it. After executing this function, you will get following:
  - 0xCC if operation was successful.
    0xFF in case of error.

There are various ways to authenticate the biometric data fed. Combination of biometric data along with the pin number is used to increase the security. Since the biometric data cannot be stolen or forged, the transaction would be safe and secured. While there may be chances for the pin number to be forged. The transaction time of the proposed system is about 10 seconds. This is achieved with greater care, as the clients desire and expect low transaction time.

IV. METHODOLOGY, TECHNIQUE AND ALGORITHM

In this system, we are implementing ATM system based fingerprint authentication. The system features with SEA/RSA accelerator engines and the embedded non-volatile memory (Flash). The system keeps aside a certain space within Flash memory for storing fingerprint template, i.e. fingerprint library. Fingerprint template's storage in Flash is in a systematic order. Let's consider the fingerprint capacity N, then the serial number of template followed in the library is 0, 1, 2, 3 ... N. The library can be used by an individual by template number, so the images are stored as a template in database and then the saved image is matched with the input image. If the image does not match further authentication is done to proceed with the transaction. The system features with SEA/RSA accelerator engines and the embedded non-volatile memory (Flash).

A UART (Universal Asynchronous Receiver/Transmitter) is the microchip with programming that controls a computer's interface to its attached serial devices. It allows the computer with the RS-232C Data Terminal Equipment (DTE) interface so that it can "talk" to and exchange data with modems and other serial devices. As part of this interface, the UART also:

Changes the bytes it receives from the computer along parallel circuits into a single serial bit stream for outbound transference.
On inbound transference, changes the serial bit stream into the bytes that the computer handles.
Adds parity bit (if selected) on outbound transference and checks the parity of incoming bytes (if selected) and discards the parity bit.
Adds start and stop delineators on outbound unit and strips them from inbound transferences.
Handles interrupts from the devices such as keyboard and mouse (which are serial devices with special port s)
May handle other kinds of interrupt and device management as well that require coordinating the computer's speed of operation with that of the device speed.

V. CONCLUSION

It is vital step to understand the basics, i.e. the advantages, disadvantages, requirements and most importantly the feasibility of a biometric based security system. The implementation of ATM security system by using biometric method is a crucial procedure, as well as very challenging and difficult. But for security purposes and to have a control on the criminal records it is very important to bring this system in motion. Fingerprints have intrinsic features that do not change for whole life and are different individually. They are easy to use, cheap and provide the most suitable miniaturization. Biometrics is one of the most popular and effective means for identification/verification of an individual and is used as forensic evidence. It becomes important to take help of two technologies, namely embedded system and biometrics in order to provide enough security. Hybridization, along with the above two technologies is useful for fingerprint verification since it refers to the automated method of verifying/ identifying a match or similarities between two human fingerprints.

REFERENCES

[1] Dr. V. Vijayalakshmi, R.Divya and K. Jaganath, "Finger and Palm print based Multibiometric Authentication System with GUI Interface" International conference on Communication and Signal Processing, April 3-5, 2013, India, 978-1-4673-4866-9/13/$31.00 ©2013 IEEE
[2] O.A.Esan and S.M.Ngwira "Bimodal Biometrics for Financial Infrastructure Security" I.O.Osunmakinde School of Computings, College of Science, Engineeringand Technology, University of South Africa, UNISA Pretoria, South Africa, 978-1-4799-0808-0/13/$31.00 ©2013 IEEE.
[3] Rishigesh Murugesh, "ADVANCED BIOMETRIC ATM MACHINE WITH AES 256 AND STEGANOGRAPHY IMPLEMENTATION", IEEE-Fourth International Conference on Advanced Computing, ICoAC 2012 MIT, Anna University, Chennai. December 13-15, 2012, 978-1-4673-5584-1/12/$31.00©2012 IEEE.
[4] Rajesh.V and Vishnupriya.S, "IBIO-A New Approach/or ATM Banking System" 2014 International Conference on Electronics and Communication Systems (ICECS-2014), Feb.13-14, 2014, Coimbatore, INDIA.
[5] G. Renee Jebaline and S. Gomathi , "A Novel Method to Enhance the Security of ATM using Biometrics" , 2015 International Conference on Circuit, Power and Computing Technologies [ICCPCT], 978-1-4799-7075-9/15/$31.00 ©2015 IEEE
[6] A.Muthukumar and N.Sivasankari,"A Review on Recent Techniques in Multimodal Biometrics", 2016 International Conference on Computer Communication and Informatics (ICCCI -2016), Jan. 07 – 09, 2016, Coimbatore, INDIA ,978-1-4673-6680-9/16/$31.00 ©2016 IEEE
[7] Umma Hany and Lutfa Akter,"Speeded-Up Robust Feature Extraction and Matching for Fingerprint Recognition", 2nd Int'l Conf. on Electrical Engineering and Information & Communication Technology (ICEEICT) 2015.Jahangirnagar University, Dhaka-1342, Bangladesh, 21-23 May 2015, 978 4673 6676 2115/$31.00 ©20151EEE.
[8] Ms. Archana S. Shinde and Prof. Varsha Bendre, "An Embedded Fingerprint Authentication System", 2015 International Conference on Computing Communication Control and Automation, 978-1-4799-6892-3/15 $31.00 © 2015 IEEE DOI 10.1109/ICCUBEA.2015.45