ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering

NCDSPICE 2016
National Conference on Digital Signal Processing, Information and Communication Engineering
Govt. Polytechnic College, Kasaragod
Vol. 5, Special Issue 4, November 2016

Secure ATM Transactions through Fingerprint

Neena .M.K

Lecturer in Computer Engineering, Govt. Women's Polytechnic College, Nedupuzha, Thrissur, Kerala, India

Abstract: In these prevailing globalized times; we are more connected with the plastic money where our economic transactions are carrying out through debit or credit cards. The prevailing ATM (Automatic Teller Machine) systems founded on magnetic card & a static PIN. The breaching into the existing system by skimming devices, card trapping, etc. revealing the vulnerability of existing siting creates a hostile atmosphere for the transactions. The proposed system introduces an alternative for the magnetic card and PIN. The proposed system doesn't need any other complex component other than fingerprint sensor additional to existing traditional ATM. Instead of magnetic ATM debit/credit card use chip enabled card which contain only Account number, Name of the customer, Fingerprint and PIN. A fingerprint sensor is an electronic device used to capture a digital image of the fingerprint pattern. The captured image is called a live scan. This live scan is digitally processed to create a biometric template (a collection of extracted features) which is stored and used for matching. The input fingerprint retrieved from the sensor is directly compared with template stored on the card issued by the bank after this authentication, the embedded code initiate the communication with the data server to complete the financial transaction.

Keywords: Fingerprint, Authentication, live scan, template

I. INTRODUCTION

Humans life is integrated with the finical transactions, nowadays these transactions are largely done with the help of plastic money especially the debit and credit cards these cards and ATM. These transactions help people to save their time and makes bank as easy practice. ATM is a computerized machine that permits bank customers to gain access to their accounts with a magnetically encoded plastic card and PIN (Personal Identification Number). It enables the customers to perform several banking operations without the help of a teller such as to withdraw cash, make deposits, pay bills, obtain bank statements. User can change at any time through ATM. This password is static type, once set access will be done after using this so the chances to hack it more, and if ATM card is lost and password is stolen then, anyone can easily access that account by making financial losses of customer so there are chances of security threats in existing system like shoulder surfing, data skimming, card trapping.

In keypad jamming the fraudster tampering the ATM keys caused for an unfinished transaction and opened the account for seconds which help the plotters to obtain the account and caused for financial lost, in card trapping fraudster place a device on the machine that uses tape, cable in order to hold a card in. Criminals can then retrieve cards using tweezers. The PIN can be obtained through observation or by putting an overlay device on the keypad that can record PIN. Card swapping is a more technical mode of deceiving; the criminals plant a small skimming device in the debit card slot of the ATM and it can read the magnetic tape information of the card when the card goes through the skimming device. With the copied magnetic information, and reproduce a duplicate card (on any plastic card) to be used later to withdraw cash. In order to access the PIN, they also install a small camera at the ATM cabin that can capture the ATM pin when it is entered by the cardholder. In these cases, the banks generally take the liability onto themselves and refund the customer for the financial fraud. In these scenario, the biometrics techniques offering alternative safeguards for ATM transactions capable to substitute the existing magnetic strips system.

II. BIOMETRICS

Biometrics is the science of measuring and analyzing biological information. Biometrics uses characteristics that can be physical such as finger prints, face, voice, and iris scan. Advantage of biometric is that Features such as fingerprints, retina patterns, and hand geometry are something almost all people already have and are all naturally unique [1]. It is also something that is with the person at all times and thus available whenever required. The main purpose to use biometrics is for uniquely identify an individual with the help of characteristics of the human body. Biometrics uses characteristics that can be physical and they are known to be very secure and are used in special organization.

Instead of artificially attaching some type of uniqueness to the subject biometrics make using the uniqueness is determined through an intrinsic quality that the subject already possesses. For very high-security applications, or situations where an extremely high assurance level for

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering

NCDSPICE 2016
National Conference on Digital Signal Processing, Information and Communication Engineering
Govt. Polytechnic College, Kasaragod
Vol. 5, Special Issue 4, November 2016

identification or authentication is required, this built-in uniqueness gives biometrics the edge it needs over its traditional identification and authentication counterparts.

Biometric refers to any and all of variety of identification technique Biometric ATM support only at ATM machine which is facilitates these types of services. The ATMs are network connected centralized computer system with controls ATMs. The use of any Biometrical characteristics as a biometric is both the oldest mode of computer-aided, personal identification and the most predominant in use today. In the world, today, Biometrical characteristics is used for implementing security and upholding a consistent identification of any individual and used as variables of security during voting, examination, procedure of bank accounts among others. They are also used for controlling access to highly secured places like offices, equipment rooms, and control centers and so on.

FINGERPRINT

A fingerprint is the feature pattern of one finger. Fingerprint contains complex patterns of stripes, called ridges. There exists some gap between the ridges, called valleys. There exists some gap between the ridges, called valleys. In a fingerprint, the dark lines of the image are called the ridges and the white area between the ridges is called valleys

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips (Babler, 1991). This property makes fingerprints a very attractive biometric identifier.

Fingerprint based identification is the oldest of all biometric techniques. Fingerprint characteristics were studied since mid-1600s, but the use of fingerprints to identify dates back to mid- 1800s. Each person is known to have unique, immutable fingerprints. Finger prints have been used for personal identification or verification since long. Fingerprints are used for identification because of the following reasons:

1. The friction ridge detail of the epidermis on the palm side of the hands remains unchanged during the lifetime of an individual, except for accidental or intentional scarification or alteration;
2. Friction ridge pattern areas exhibit much variety of detail that no two patterns are ever found to be exactly the same on the digits (palms or soles of feet) of one individual or on the digits (or palms or soles of feet) of other individuals;
3. While these friction ridge patterns exhibit an infinite variety of detail, they nevertheless fall within certain broad classes or categories that permit police to store and retrieve millions of prints according to classification formulae

Fingerprint Sensing and Storage

Based on the mode of acquisition, a fingerprint image may be classified as off-line or live scan. An off-line image is typically obtained by smearing ink on the fingertip and creating an inked impression of the fingertip on paper. The inked impression is then digitized by scanning the paper using an optical scanner or a high-quality video camera. A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact. A special kind of off-line images, extremely important in forensic applications, are the so-called latent fingerprints found at crime scenes. . A live-scan image, on the other hand, is acquired by sensing the tip of the finger directly, using a sensor that is capable of digitizing the fingerprint on contact.

The image is stored as an acceptable scan in flash memory, ready to be transmitted (by USB cable, wireless, Bluetooth, or some similar method) to a "host" computer where it can be processed further. Typically, images captured this way are 512×512 pixels (the dimensions used by the FBI), and the standard image is 2.5cm (1 inch) square, 500 dots per inch, and 256 shades of gray. The host computer can either store the image on a database (temporarily or indefinitely) or automatically compare it against one or many other fingerprints to find a match.

III. FINGERPRINT VERIFICATION

Fingerprint verification is to verify the authenticity of one person by his fingerprint. Each person has his own fingerprints with the permanent uniqueness. Matching of fingerprint consists of comparing two fingerprints and find out if they belong to the same finger fig 1. . To prepare for verification, a person initially enrolls his or her fingerprint into the verification system. A fingerprint verification system checks whether a person really is who he claims to be Pre-processing is an important step for (Fingerprint Recognition System) Fingerprint verification.

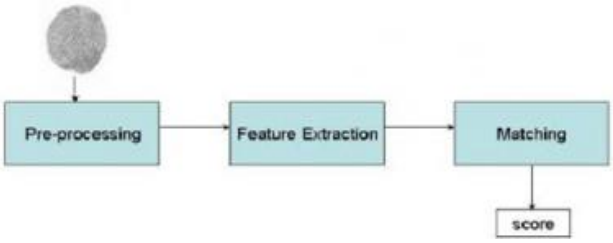

Fig 1: Fingerprint verification

It enhances the quality and produces an image in which features can be detected correctly. The final result of Fingerprint verification also depends on this step.

The response of a matcher in a fingerprint recognition system is typically a matching score s (without loss of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering

NCDSPICE 2016
National Conference on Digital Signal Processing, Information and Communication Engineering
Govt. Polytechnic College, Kasaragod
Vol. 5, Special Issue 4, November 2016

generality, ranging in the interval [0,1]) that quantifies the similarity between the input and the database template representations. The closer the score is to1, the more certain is the system that the two fingerprints come from the same finger; the closer the score is to 0, the smaller is the system confidence that the two fingerprints come from the same finger. The system decision is regulated by a threshold t: pairs of fingerprints generating scores higher than or equal to t are inferred as matching pairs (i.e., belonging to the same finger); pairs of fingerprints generating scores lower than t are inferred as non-matching pairs (i.e., belonging to different fingers)

Verification Methods

Many algorithm have been proposed in the pattern recognition literature for fingerprint verification. The large number of approaches can be classified in the following three classes: correlation based matching, minutiae based matching and ridge feature based matching [2].

Minutiae Extraction Technique

Most of the finger-scan technologies are based on Minutiae [3]. Among the variety of minutiae types reported in literature, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive in fig 2.

Ridge ending Ridge bifurcation
Fig: 2 Finger print

These steps need to be followed so that accurate matching of fingerprints can be performed. These steps involve: - 1. Image Pre-processing 2. Minutiae detection and feature extraction 3. Minutiae Matching. The most popular technique of minutiae detection is through the use of the crossing numbers approach. Minutiae matching [2], the third step involves matching the template image with the input image. Template image is collected during enrolment and saved in the database. During matching phase, the input image is compared against template image. Minutiae are extracted from the two fingerprints and stored as sets of points in the two-dimensional plane. Minutiae matching essentially consists of finding the alignment between the template and the input minutiae sets that results in the maximum number of minutiae pairings; This phase decides whether the two images are from the same finger or not

Ridge feature-based matching

Ridge Feature Based Techniques also known as Pattern Matching. Feature extraction and template generation are based on series of ridges as opposed to discrete points which forms the basis of Pattern Matching Techniques. The advantage of Pattern Matching techniques over Minutiae Extraction is that minutiae points may be affected by wear and tear and the disadvantages are that these are sensitive to proper placement of finger and need large storage for templates.

Minutiae extraction is difficult in very low-quality fingerprint images, whereas other features of the fingerprint ridge pattern (e.g., local orientation and frequency, ridge shape, texture information) may be extracted more reliably than minutiae, even though their distinctiveness is generally lower. The approaches belonging to this family compare fingerprints in term of features extracted from the ridge pattern.

Correlation Based Technique

Two fingerprint images are superimposed and the correlation (at the intensity level) between corresponding pixels is computed for different alignments (e.g., various displacements and rotations).

The correlation-based methods spatially or in frequency domain correlate two fingerprint images to compute the similarity between them. It is an advanced and newly emerging method for fingerprint recognition. It is useful to solve some intractable problems of the first approach. This method is also capable of dealing with fingerprints of badimage quality from which no minutiae can be extracted reliably. The correlation-based checking is carried out by means of template matching, this method consumes a lot of computational power. This makes it a less attractive method to use.

FINGERPRINT SCANNER

Fingerprint scanners are digital input devices that read a (human) fingerprint and output a 2D/3D image dataset. There are several different ways in which an instrument can bring out the details in the pattern of raised areas (called ridges) and branches (called bifurcations) in a human finger image.

Capacitive fingerprint Scanners.

Capacitive sensors use electric current to sense a fingerprint and capture the image. As sensors apply a small voltage to the finger, a real fingerprint is required rather than a visual impression of it. It's simple, very robust and only works with skin. We can't fool it with a piece of paper, and if we try to make a mold of a real fingerprint, you need to find a material that has the same

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE
International Journal of Advanced Research in Computer and Communication Engineering

NCDSPICE 2016
National Conference on Digital Signal Processing, Information and Communication Engineering
Govt. Polytechnic College, Kasaragod
Vol. 5, Special Issue 4, November 2016

conductivity as skin. That is not impossible. The downside of capacitive fingerprint readers is that they can't work if the finger isn't clean, or has water/sweat on it because that changes the conductivity upon which the system is built. Also, they don't work behind metal. That's why there's always a visible fingerprint reader.

Optical fingerprint readers

Optical fingerprint readers are older, and they use the simplest technology. Optical sensors use arrays of photodiode or phototransistor detectors to convert the energy in light incident on the detector into electrical charge. The sensor package usually includes a light-emitting-diode (LED) to illuminate the finger.

There are two detector types used by optical sensors, charge-coupled-devices (CCD) and CMOS based optical imagers. CCD detectors are sensitive to low light levels and are capable of making excellent grayscale pictures. A light shines the fingerprint from the side to reveal the ridges and valleys of the fingerprint for an optical sensor to read.

This is reliable simple and affordable to build on large surfaces (to print several fingers or a whole palm). The downside is that it requires a larger volume to accommodate the light, and it's not very secure because a printed image, a prosthetic, or a molded fingerprint could lead to a match: they are the easiest to fool because they are essentially like Photocopiers.

IV PROPOSED METHOD

Instead of magnetic ATM debit/credit card use chip enabled card which contain only Account number, Name of the customer, and Fingerprint (templates of fingerprint) and PIN (Personal Identification Number). A fingerprint sensor is an electronic device which is attached to ATM used to capture a digital image of the fingerprint pattern. The captured image is called a **live scan**.

This live scan is digitally processed to create a biometric template (a collection of extracted features) it is used for matching [6]. The input fingerprint retrieved from the sensor is directly compared with template stored on the card issued by the bank after this authentication the embedded code (PIN) initiate the communication with the data server to complete the financial transaction. It also avoids memorizes PIN.

Many methods developed for fingerprint verification described above minutiae based, ridge feature based, and correlation based. Most commonly used method for feature extraction and verification is minutiae [8] since correlation based method requires lot of computation, since it needs entire image may be processed for verification.

This is one way of decentralize a biometric system is by storing the biometric information/ fingerprint template of a user in a chip enabled ATM card that is issued to the user. After the input fingerprint retrieved from the sensor can directly compared with the template on the smart card and the decision delivered (possibly in encrypted form) to the outside world.

Feature extraction component is performed on the host PC. If the fresh fingerprint matches any one of the templates stored in chip, then customer is allowed to perform bank transaction. Otherwise customer fails to do. The Host ATM establish communication with bank database using the account information in chip enabled ATM card.

V. CONCLUSION

Fingerprint technology is the most widely accepted and mature biometric method and is the easiest to deploy and for a higher level of security at your fingertips. The technology restricts chance of skimming during transaction and provide ultimate security to the customer.

Thus, fingerprint verification is considered among the least intrusive of all biometric verification techniques. The fingerprint-based card offers better security compared with magnetic strip cards with PIN since it is difficult to duplicate data.

ACKNOWLEDMENT

The author would like to express her gratitude to Head of the Institution for constant support and motivation to prepare the paper. Also, like to thank Head of the Department and Colleagues and family members for the encouragement.

REFERENCES

[1] **Handbook of Fingerprint Recognition** Davide Maltoni Dario Maio Biometric Systems Laboratory DEIS-CSITE University of Bologna University of Bologna Cesena, 47023 Bologna, 40136Italy Italymaltoni@csr.unibo.it dmaio@deis.unibo.it;Anil K. Jain SalilPrabhakarDepartment of Computer Science DigitalPersona. Inc. and Engineering Redwood City, CA 94063 Michigan State University USA East Lansing, MI 48824 salil@digitalpersona.com USAjain@cse.msu.edu

[2] **An Approach to Fingerprint Image PreProcessing** Om PreetiChaurasia Amity School of Engineering and Technology, Amity University, Noida, India E-mail: preeti.princy.chaurasia@gmail.com I.J. Image, Graphics and Signal Processing, 2012, 6, 29-35 Published Online July 2012 in MECS (http://www.mecs-press.org/) DOI: 10.5815/ijigsp.2012.06.05

[3] Miroslav Baþa, KornelijeRabuzin University of Zagreb, Faculty of Organization and Informatics, Varaždin, Croatia {tonimir. kisasondi, alen.lovrencic}@foi.hr ZvonkoMerkašAutohrvatska, Zagreb, Croatia zmerkas@autohrvatska.hr **FINGERPRINTS PREPROCESSING USING WALSH FUNCTIONS** Journal of information and organizational sciences, Volume 30, Number1 (2006)

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

NCDSPICE 2016

National Conference on Digital Signal Processing, Information and Communication Engineering

Govt. Polytechnic College, Kasaragod

Vol. 5, Special Issue 4, November 2016

[4] Jatinder N.D. GuptaThe University of Alabama in Huntsville, USA,Sushil K. Sharma Ball State University, USA **Handbook of Research on Information Security and Assurance**

[5] **Digital Image Processing**3rd edRafael C. Gonzalez, Richard Eugene Woods

[6] **Automated Teller Machine – Its Benefits and Challenges** IRACST – International Journal of Commerce, Business and Management (IJCBM), ISSN: 2319–2828 Vol. 4, No.6, December 2015 Name of the Author: Ms. Meena R Official Address: Assistant Professor, Center for Management Studies, Jain University, # 133, Lalbagh Road, Bangalore – 560027. Karnataka, India

[7] Vaibhav R. Pandit Assistant Professor Dept. of Electronics & Tel., J.D.I.E.T., Yavatmal. SGB Amravati University Kirti A. Joshi M.Tech Scholar Dept. of Electronics, S.B.J.I.T.M.R., Nagpur RTM Nagpur University Narendra G. Bawane, Ph.D Principal, Dept. of Electronics, S.B.J.I.T.M.R., Nagpur RTM Nagpur University. **ATM Terminal Security using Fingerprint Recognition** International Journal of Applied Information Systems (IJAIS) – ISSN: 2249-0868 Foundation of Computer Science FCS, New York, USA 2nd National Conference on Innovative Paradigms in Engineering & Technology (NCIPET 2013) – 14www.ijais.org

[8] Yuliang He, Jie Tian, Xiping Luo, Tanghui Zhang. **Image enhancement and minutiae matching in ingerprint verification**. Pattern Recognition Letters 24 (2003)1349-1360. [10] Wei Wang, Jianwei Li, Feifei Huang, Hailiang Feng. Design and implementation of Log-Gabor filter in fingerprint image enhancement. Pattern Recognition Letters 29 (2008)301-308. [13]

[9] Lin Hong, Wan Yifei, Anil Jain. **Fingerprint image enhancement: algorithm and performance evaluation**[J]. IEEE Transactions on Pattern Analysis and Machine intelligence. 1998, 20(8): 777-789.

[10] Avinash Kumar Ojha MCA Department, Mumbai University, Maharashtra, India **ATM Security using Fingerprint Recognition** International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 6, June 2015

BIOGRAPHY

Mrs. Neena .M.K, Lecturer in Computer Engineering, Govt. Women's Polytechnic College Nedupuzha, Thrissur, Kerala, India. She Worked as Lecturer in several institutions in Kerala. She graduated in Computer Engineering from Model Engineering College, Kochi. She took M Tech in Computer Science from Kerala University in 2009