International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 11, November-2014, pp: (13-17), Impact Factor: 1.252, Available online at: www.erpublications.com

Cardless Cash Access Using Biometric ATM Security System

Neenu Preetam. I[1], Harsh Gupta[2]
[1, 2]M.Tech. (Microelectronics), Department of ECE, SEEC, Manipal University Jaipur (MUJ), Rajasthan, India

Abstract: Cardless cash Biometric ATM System enables cash withdrawal at an ATM without using the existing magnetic swipe cards which makes it possible to quickly authorize a person to withdraw money. Biometric Automatic Teller Machine (BioATMs) seems to be an effective way of preventing card usage and is also a channel to expand our reach to rural and illiterate masses. These BioATMs can talk to the people in their native languages and provides high security in authentication which prevents service users from unauthorized access. In this model, the user is required to authenticate himself with a two phase security solution by first providing an individual's biometric identification (Thumb/Fingerprint/Iris etc.), followed by Personal Identification Number (PIN), and select the bank branch from the displayed list if applicable. This system also provides an alternative approach to access cash via an OTP (One Time Password) generation on user's cellphone in case of loss of PIN. It saves time, cost and efforts compared with existing card based ATMs thereby eliminating environmental problem of disposing plastic waste. It also reduces the user's dependency on bank officials in sending money to distant relatives at home and abroad.

Keywords: Biometric ATMs, OTP, Two phase security, PIN.

I. INTRODUCTION

This Biometric automated teller machine or automatic teller machine (ATM) is a computerized telecommunications device that provides the clients of a financial institution with access to financial transactions in a public space without the need for a cashier, human clerk or bank teller. On most modern ATMs, the customer is identified by inserting a plastic ATM card with a magnetic strip or a plastic smart card with a chip that contains a unique card account number and some security information such as an expiration date, CVV number, card holder's name. Authentication is provided by the customer entering a personal identification number (PIN). Using a biometric ATM, customers can access their bank accounts in order to make cash withdrawals, debit card cash advances, and check their account balance just by using a simple finger print technology.

We hence propose the verification method using fingerprint biometric feature in addition to cash card and PIN. This biometric feature is obtained by usual ATM operation without special other operation. In addition, because this biometric feature is the dynamic feature which changes with time, it is hard to counterfeit. Typical biometric features (Face, Iris and DNA, etc.) may supply high precision, however these biometric features are not perfect for verification on ATM. Because they require user's special other operation and dedicated device, and they give physical load and psychological burden to ATM user. These static biometric features have also the possibility of being copied [1,2].The Finger print approach can be more commonly utilized by the ATM systems because of its advantages in providing non-intrusive environment, and less time consumption in making a transaction.

II. CRYPTOGRAPHY

Cryptography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. Coding secret messages in digital images is by far the most widely used of all methods. This is because it can take advantage of the limited power of the human visual system (HVS). The advantage of cryptography over steganography is that messages do not attract attention to themselves.

There are two types of compression techniques used in digital image processing, i.e. lossy and lossless. Lossy compression

such as (.JPEG) greatly reduces the size of a digital image by removing excess image data and calculating a close approximation of the original image. Lossless compression techniques, as the name suggests, keeps the original digital image in tact without the chance of loss. It is for this reason, lossless compression technique is chosen for steganographic uses. Least significant bit (LSB) encoding is by far the most popular of the coding techniques used for digital images. By using the LSB of each byte (8 bits) in an image for a secret message, we can store 3 bits of data in each pixel for 24-bit images and 1 bit in each pixel for 8-bit images. Masking and filtering techniques for digital image encoding such as Digital Watermarking are more popular with lossy compression techniques such as (.JPEG). This technique actually extends images data by masking the secret data over the original data as opposed to hiding information inside of the data. The beauty of Masking and filtering techniques are that they are immune to image manipulation which makes these possible uses very robust.

III. ENCIPHER ALGORITHM

Advanced Encryption Standard (AES) is used to encrypt digital data worldwide. Cracking an AES encrypted code is close to impossible, since the combinations of keys are massive. It uses a symmetric key algorithm, since it uses the same key for encryption and decryption. Based on the principle of substitution- permutation network, it is fast in both software and hardware platforms. The AES algorithm makes use of three cipher keys, each of difference strengths namely 128, 192 and 256 bit encryption. Each encryption key size causes the algorithm to behave slightly differently, so the increasing key sizes not only offer a larger number of bits with which you can scramble the data, but also increase the complexity of the cipher algorithm. AES operates on a 4x4 column major order matrix of bytes, termed the state, although some versions have a larger block size and an additional column in the state. The key size used for an AES cipher specifies the number of repetitive transformation rounds that convert the input, called the plaintext into the final output, called the cipher text. The number of repetitive cycles are as follows:

- 10 cycles of repetition for 128 bit keys
- 12 cycles of repetition for 192 bit keys
- 14 cycles of repetition for 256 bit keys

Each round consists of several processing steps, including one that depends on the encryption key itself. A set of reverse rounds are applied to transform cipher text back into the original plaintext using the same encryption key.

A. Performance Estimation of AES Algorithm

High speed and low RAM requirements are the criteria for AES selection process. Thus AES performs well on a wide variety of hardware, from 8-bit smart cards to high performance computers. On a Pentium Pro, AES encryption requires 18 clock cycles / byte, equivalent to a throughout of about 11 MB/s for a 200 MHz processor. On a Pentium M 1.7 GHz throughput it is about 60 MB/s. On Intel i5/i7 CPUs supporting AES-NI instruction set extends its throughput to about 400 MB/s per thread.

B. AES Encryption vs. Triple DES Algorithm

To enhance the security, a more powerful version of DES algorithm called Triple DES is used. To start encrypting with Triple-DES, two 56-bit keys are selected. Data is encrypted via DES three times, the first time by the first key, the second time by the second key and the third time by the first key once more.

AES has more elegant mathematical formulas behind it, and only requires one pass to encrypt data. AES was designed from the ground up to be fast, unbreakable and able to support the tiniest computing devices imaginable. The difference between AES and Triple-DES are not strength of security, but superior performance and better use of resources.

IV. NEURAL NETWORKS FOR FINGERPRINT RECOGNITION

Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity.

Figure 1: Whorl Pattern, Loop Pattern, and Arch Pattern Fingerprint ridges

In order to be used for recognizing a person, the human trait needs to be unique and not subjected to any changes. Fingerprints are imprints formed by friction ridges of the skin and thumbs. The patterns are permanent and unchangeable on each finger.

The three basic patterns of fingerprint ridges are the arch, loop, and whorl.

The major Minutia features of fingerprint ridges are: ridge ending, bifurcation, and short ridge (or dot):

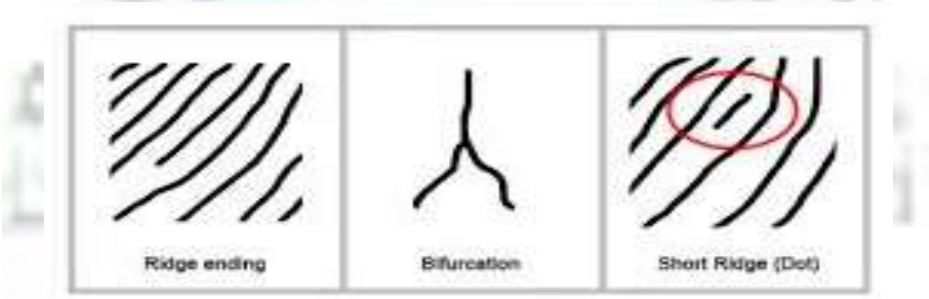

Figure 2: Ridge ending, Bifurcation, and Short ridge (Dot) features of Fingerprint ridges

The various processes that are involved in fingerprint recognition using neural networks are as follows:

- Image acquisition: Converts a scene into an array of numbers that can be manipulated by a machine.
- Edge detection and thinning: They are parts of the preprocessing which involves removing noise, enhancing the picture quality and if necessary, segmenting the image into meaning regions through erosion or dilution.
- Feature extraction: The image is represented by a set of numerical "features" to remove numerous redundancies from the data and reduce image dimensions.
- Classification: A class label is assigned to the image by examining its extracted features and comparing them with the class that the classifier has leaned during its training stage.

The initial phase of the work is to capture the fingerprint image and convert it to a digital representation. Histogram equalization and Histogram Specification techniques are used to increase the contrast if the illumination condition is poor. Binarization is usually performed by using Laplacian edge detection operator. The binary image is further enhanced by a thinning algorithm which reduces the image ridges to a skeleton structure. Selection of good feature is a crucial step in the process since the next stage only sees these extracted features and acts upon them accordingly. A multilayer perceptron network of three layers is trained to detect the minutiae in the thinned part image. Contour tracing is used to find one or more turning points which are used as reference points of the resulting image. The recognition rate of the fingerprints depends on the quality of the fingerprints and effectiveness of the preprocessing subsystem.

The main purpose of this proposed system is to establish a highly secured Biometric money transaction system. Existing system possess lot of threat, due to lack of security features. In this system, protection to user integrity is given the highest priority. In addition to the existing peripherals, all we need is a good quality fingerprint scanner. These days, fingerprint devices are the most popular form of biometric security methodology used. Small, low power fingerprint scanning devices can be incorporated into the existing ATM machines so that the current transactions can be made almost secure and threat-free.

In this proposed system, the user has to first input his/her fingerprint using the biometric scanner embedded into the existing ATMs. Fingerprint scanning essentially provides an identification of a person based on the data acquisition and recognition of those unique patterns and ridges in a fingerprint. Once the fingerprint has been read by sensor mounted on the scanner, the screen prompts the user to enter the secret PIN. The secret PIN can be set according to user's choice, if needed. Once the user enters the 4-digit secret PIN, the interface prompts for the OTP. OTP (One Time Password) is a random 6-digit number sent to the user's registered mobile number by the server. The user has to enter the 6-digit OTP sent to the mobile number. Only if all the details entered by the registered user is accurate, the user can access his own transaction page.

With the addition of a Biometric fingerprint component, an enhanced secured and threat-free money transaction can be obtained. The algorithm that needs to be incorporated into the system is highly secure. In this system, we intend to make use of two techniques, namely Cryptography and Steganography.

Cryptography is process of encrypting the information using a key. The current techniques uses the AES 256 algorithm to encrypt the PIN and the OTP. AES 256 encryption is better than Triple DES algorithm, which is currently in use.

Steganography is the art of hiding the existence and the content of confidential messages by embedding it inside a media file such as an image, video, or audio. In the proposed system, we intend to use the finger print image captured by the fingerprint scanner as the BASE image. Using the underlying concept of steganography, the AES 256 encrypted code (PIN + OTP) is hidden inside the fingerprint image.

All the above mentioned process takes place at the client side (ATM machine) and the steganographed image is sent to the server. At the server side, the image is de-steganographed to retrieve the fingerprint image and the encrypted code of the registered user. Then, the process of decryption takes place to extract the PIN and the OTP sent to the registered user's mobile number. Once all the data is made available, the server makes cross verification to the data stored in the System database. Each fingerprint is associated with a Bank account credential. All the details of the user that are associated with the bank account are stored in the system database. The account details are retrieved using the de-steganographed fingerprint. If all the data provided by the registered user gives a successful match, the user is shown the transaction page and cash access can be made.

V. ADVANTAGES OF BIOMETRIC ATMs

- One huge change incorporated to the system, is the use of Biometrics. The user does not have to carry a separate ATM card to make the transaction. The user can simply make a transaction using his finger. Using a Biometric is a far more secure system than using a magnetic strip card, as every fingerprint is unique.

- In addition to securing the system using a PIN, an additional security can be provided through an OTP feature which further increases the complexity of the system. Even if the PIN of the user is available to the wrong person, he may not have access to the OTP generated on the registered user, as the OTP is only sent to the authorized mobile number registered to the user.

- Use of AES 256 algorithm provides concrete protection to the system. "AES can encrypt data much faster than Triple-DES, as DES essentially encrypts a message or document three times."

- During the communication between the client and the server, even if the intruder hacks the connection line and gets access to the data, he may only get the steganographed fingerprint image. The thief will never be able to decode the encrypted data within the image. Only with a decrypted data, the hacker may forge a transaction.

CONCLUSION

This paper concludes that the conventional ATM systems needs to be replaced with Biometric systems where the transaction process becomes easier, reliable, secure, and eliminating the need of carrying any kind of swipe cards. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. It is based on the characteristics of user's fingerprint, like stability and reliability. Fingerprint allows the recognition of a registered person through quantifiable physiological characteristics that verify the identity of an individual. AES 256 encryption algorithm provides solid security features required for this proposed system. Steganography mechanism enhances the security to four folds. With the availability of low cost, memory efficient biometric scanners, this system would be able to provide a new user friendly inexpensive experience unleashing the security aspects of the proposed biometric ATM systems.

REFERENCES

[1]. Federal Information Processing Standards Publication 197, Advanced Encryption Standard (AES), Nov 26, 2001.
[2]. "Related-key Cryptanalysis of the Full AES-192 and AES-256",AlexBiryukov and Dmitry Khovratovich, , University of Luxembourg, 29 May 2009.
[3]. "Implementation of ATM security by using Fingerprint recognition and GSM", Pennam Krishnamurthy and Maddhusudhan Reddy, International Journal of Electronic and computing Engineering Volume 3, Issue (1).
[4]. "A brief Introduction of Biometric and fingerprint payment technology", Dileep Kumar and YeonseungRyu, International Journal of Advance Science and Technology Vol. 4 , March 2009.
[5]. "Online Credit Card Transaction using fingerprint Recognition", M.Umamaheshwari, S.Sivasubramanian and B.Harish Kumar, International Journal of Engineering and Technology Vol. 2 (5), 2010, 320-322.
[6]. "Novel technique for steganography in fingerprints Images: Design and Implementation", Hanan Mahmoud and Aljoharah Al-Dawood.