NVSS Scheme Based ATM Authentication Using Fingerprint Matching

Nasla K[1], Hemand E P[2]

[1]Computer Science And Engineering, University of Calicut/ Kmct College of Engineering Calicut, Calicut, India 9947018162

Abstract: ***The growth in electronic transactions has resulted in a greater demand for fast and accurate user identification and authentication. Access codes for buildings, banks accounts and computer systems often use personal identification numbers (PIN's) for identification and security clearances. Conventional method of identification based on possession of ID cards or exclusive knowledge like a social security number or a password are not all together reliable. An embedded fingerprint biometric authentication scheme for automated teller machine (ATM) banking systems is proposed in this paper. In this scheme, a fingerprint biometric technique is fused with the ATM for person authentication to ameliorate the security level. Here the fingerprint is hidden using NVSS Scheme ie., natural image based visual secret sharing scheme. In that secret images are transferred through various media to secure the secret and participant. The proposed scheme can share one digital secret image over n- 1 arbitrary selected natural images and one noise-like share.***

Keywords: visual secret sharing scheme, natural image based visual secret sharing scheme, natural images ,fingerprint matching, Automated teller machine.

1. Introduction

Rapid development of banking technology has changed the way banking activities are dealt with. One banking technology that has impacted positively and negatively to banking activities and transactions is the advent of automated teller machine (ATM). With an ATM, a customer is able to conduct several banking activities such as cash withdrawal, money transfer, paying phone and electricity bills beyond official hours and physical interaction with bank staff. In a nutshell, ATM provides customers a quick and convenient way to access their bank accounts and to conduct financial transactions. Personal identification number (PIN) or password is one important aspect in ATM security system. PIN or password is commonly used to secure and protect financial information of customers from unauthorized access [1]. An ATM (known by other names such as automated banking machine, cashpoint, cash machine or a hole in the wall) is a mechanical system that has its roots embedded in the accounts and records of a banking institution [1]-[2]. It is a computerized machine designed to dispense cash to bank customers without need of human interaction; it can transfer money between bank accounts and provide other basic financial services such as balance enquiries, mini statement, withdrawal and fast cash among others [3].

2. Research Background

Crime at ATMs has become a nationwide issue that faces not only customers, but also bank operators and this financial crime case rises repeatedly in recent years [4]. A lot of criminals tamper with the ATM terminal and steal customers' card details by illegal means. Once users' bank card is lost and the password is stolen, the users' account is vulnerable to attack. Traditional ATM systems authenticate generally by using a card (credit, debit, or smart) and a password or PIN which no doubt has some defects [5]. The prevailing techniques of user authentication, which involves the use of either passwords and user IDs (identifiers), or identification cards and PINs (personal identification numbers), suffer from several limitations [6]. Passwords and PINs can be illicitly acquired by direct covert observation. When credit and ATM cards are lost or stolen, an unauthorized user can often come up with the correct personal codes. Despite warning, many people continue to choose easily guessed PIN's and passwords - birthdays, phone numbers and social security numbers. Recent cases of identity theft have heightened the need for methods to prove that someone is truly who he/she claims to be. Biometric authentication technology may solve this problem since a person's biometric data is undeniably connected to its owner, is nontransferable and unique for every individual. The system can compare scans to records stored in a central or local database or even on a smart card.

Biometrics can be defined as a measurable physiological and behavioral characteristic that can be captured and subsequently compared with another instance at the time of verification. It is automated methods of recognizing a person based on a physiological or behavioral characteristic [7]. It is a measure of an individual's unique physical or behavioral characteristics to recognize or authenticate its identity [8]. Common physical biometrics characteristics include fingerprint, hand or palm geometry, retina, iris and face while popular behavioral characteristics are signature and voice. Biometrics technologies are a secure means of authentication because biometrics data are unique, cannot be shared, cannot be copied and cannot be lost.

Basic natural image based visual [9] secret sharing scheme is having three process. The feature extraction algorithm consist of three steps a) Binarization b) Stabilization c) chaos. In binarization process image is converted into 0's and 1's . Stabilization is used for searching black and white pixel from image. In last chaos introduce noise. In encryption algorithm with the help of secret image and feature extracted from natural image combine to form noise like share and at last generate the quick response code. QR code is used to store amount of data.In this system we add an extra image stacking module before the feature extraction step.

3. Related Works

Shaikh and Rabaiotti [10] analyzed the United Kingdom identity card scheme. Their analysis approached the scheme from the perspective of high volume public deployment and described a trade-off triangle model. They found that there is a trade-off between several characteristics, i.e., accuracy, privacy and scalability in biometric based identity management system, where emphasis on one undermines the other.

Amurthy and Redddy developed an embedded fingerprint system, which is used for ATM security applications. In their system, bankers collect customers' finger prints and mobile numbers while opening accounts, then customer only access ATM machine. The working of the ATM machine is such that when a customer place a finger on the finger print module it automatically generates every time different 4-digit code as a message to the mobile of the authorized customer through GSM modem connected to the microcontroller. The code received by the customer is entered into the ATM machine by pressing the keys on the touch screen. After entering it checks whether it is a valid one or not and allows the customer further access.

Schouten and Jacobs presented an evaluation of the Netherlands' proposed implementation of a biometric passport, largely focusing on technical aspects of specific biometric technologies (such as face and fingerprint recognition) but also making reference to international agreements and standards (such as ICAO and the EU's ''Extended Access Control'') and discussed the privacy issue in terms of traditional security concepts such as confidentiality. Debbarma [1] proposed an embedded Crypto-Biometric authentication scheme for ATM banking system.

4. Basic NVSS Scheme

.
As Fig. 1(a) shows, the encryption process of the proposed (*n*, *n*)-NVSS scheme, *n*-2, includes two main phases: feature extraction and encryption. In the feature extraction phase,24 binary feature images are extracted from each natural share.The natural shares ($N_1,\ldots, N_{n-1}$ include n_p printed images (denoted as ***P***) and n_d digital images (denoted as ***D).*** The feature images ($F_1,\ldots, F_{n-1}$that were extracted from the same natural image subsequently are combined to make one feature image with 24-bit/pixel color depth.In the encryption phase, the *n*-1 feature images ($F_1,\ldots, F_{n-1}$ with 24-bit/pixel Color depth and the secret image execute the XOR operation to generate one noise-like share S with 24-bit/pixel color depth.

Then, to reduce the transmission risk of share S, the share is concealed behind cover media or disguised with another appearance by the data hiding process. The resultant share S'is called the generated share. The *n*-1 innocuous natural shares and the generated share are *n* shares in the (*n*, *n*)-NVSS scheme. When all *n* shares are received, the decryption end extracts *n*-1 feature images from all natural shares and then executes the XOR operation with share S' to obtain the recovered image, as shown in Fig. 2(b).

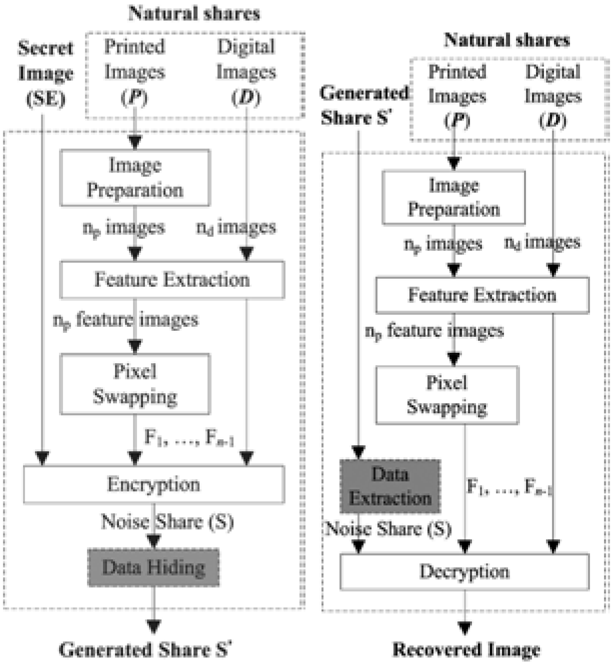

Figure 1(a) **Figure 1.(b)**

Figure 1: The encryption/decryption process of the (*n*, *n*)-NVSS scheme: (a) encryption process, (b) decryption process

5. Proposed Application

Assume we require assembling the Automated Fingerprint Identification System on the ATM Machine. During Opening of an account (fig. 2) administrator will collect the fingerprints of the customers. She will consider each fingerprint as a secret image. Also collects his photograph and a security image as the natural shares for hiding the fingerprint and saved securely in the database. The fingerprint will be then encrypted using the NVSS scheme. Then the generated share will be converted to QR code and then printed on the ATM card along with the Photograph.

During withdrawal of cash from the ATM Machine (fig 3)the User inserts his ATM card and provides his fingerprint for Scanneing.The ATM machine then will scan the photograph and the QR code and then Decrypts the hidden fingerprint. This hidden fingerprint is then matched along with the new fingerprint given during withdrawal. If it matches then the user is allowed to withdraw the Cash.

6. Conclusion

This system provides four major contributions.

- First, this is the first attempt to authenticate ATM user by NVSS scheme.
- This enhances the security of the transaction to a higher extend.

- This study proposes a useful concept and method for using unaltered images as shares in a VSS scheme.
- Fourth, No one can use the ATM card except the user.

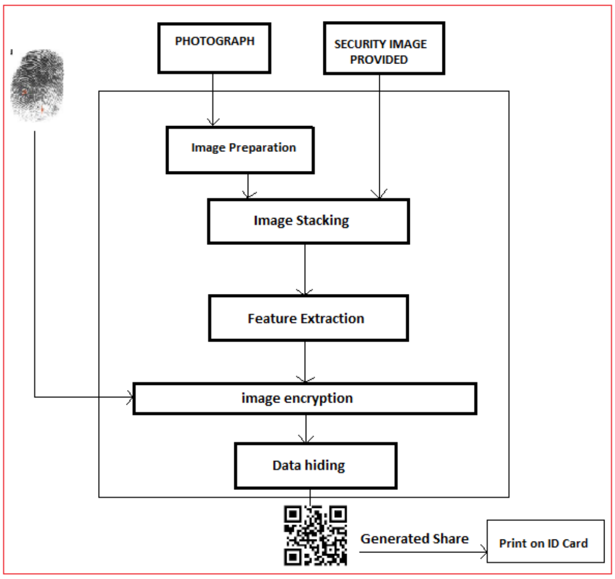

Figure 2: The encryption process during Account opening.

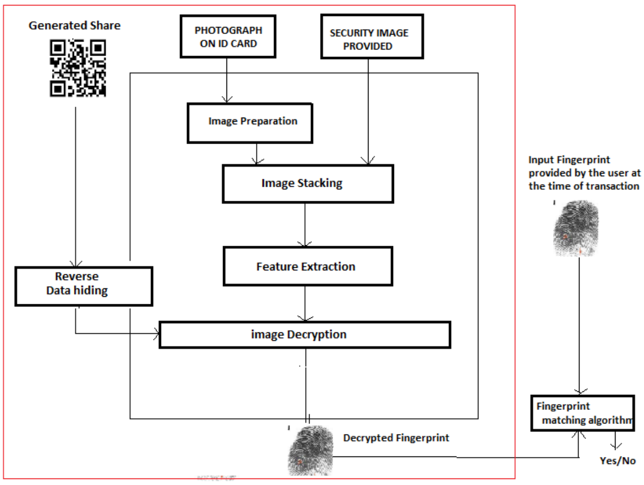

Figure 3: The decryption process during cash withdrawal.

Looking back to the existing problems with fingerprint readers we achieve the following results:

- There is no more problem with the falsification of the finger, because the entrance will succeed only in case if the participant will provide the ID card.
- There is no need for the administrator to maintain a large data base of the fingerprints.

We overcome the problems stated above without reintroducing the problems associated with the non-biometric authentication techniques. These security problems inherent in the knowledge- and possession-based techniques: that is, a password can be forgotten or guessed, a key may be lost or stolen, and both can be shared (D. Maltoni, 2003).

We affirm that the cost difference of the techniques involved in our application is negligible as in compare with techniques used by the existing Fingerprint Based Authentication Systems. Moreover it is luckily slightly reduced. The statistical cost analysis is our future task..

References

[1] S.S, Das and J. Debbarma, “Designing a Biometric Strategy (Fingerprint) Measure for Enhancing ATM Security in Indian e-banking System”, International Journal of Information and Communication Technology Research, vol.1, no. 5, pp.197-203, 2011.

[2] W.W.N. Wan, C.L. Luk, and C.W.C. Chow, “Customers Adoption of Banking Channels in Hong Kong”, International Journal of Bank Marketing, vol. 23, no. 3, pp. 255-272, 2005.

[3] Wikipedia the free encyclopedia, “Biometrics”, Downloaded March 20, 2012 from http://en.wikipedia.org/wiki/Biometrics.

[4] B. Richard and M. Alemayehu, “Developing E-banking Capabilities in a Ghanaian Bank: Preliminary Lessons. Journal of Internet Banking and Commerce, vol. 11, no. 2, 2006. Downloaded March 15, 2012 from http://www.arraydev.com/commerce/jibc/

[5] P.K. Amurthy and M.S. Redddy, “Implementation of ATM Security by Using Fingerprint recognition and GSM”, International Journal of Electronics Communication and Computer Engineering vol.3, no. 1, pp. 83-86, 2012.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, “Enhancing Security and Privacy in Biometrics-based Authentication Systems, IBM Systems Journal, vol. 40, no. 3, pp. 614-634, 2001.

[7] N.K. Ratha, S. Chikkerur, J.H. Connell and R.M. Bolle. “Generating Cancelable Fingerprint Templates”, IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, 2007.

[8] B, Schouten and B. Jacobs, “Biometrics and their use in e-passport”, Image and Vision Computing vol. 27, pp. 305–312. 2009

[9] Kai-Hui Lee and Pei-Ling Chiu, “Digital Image Sharing by Diverse Image Media” IEEE Transactions Vol. 9, No. 1, January 2014.

[10] S.A. Shaikh and J.R. Rabaiotti,. “Characteristic trade-offs in designing large-scale biometric-based identity management systems”. Journal of Network and Computer Applications vol. 33, pp. 342–351, 2010.

Author Profile

Nasla k received the B.Tech degree in Computer Science and Engineering from the University of Calicut,Kerala, India, in 2013, and pursuing her M.Tech degree in Computer Science and Engineering in the same University.Her research interests include image processing, software engineering.

Hemand EP received the B.Tech degree in Computer Science and Engineering from the University of Kannur,Kerala, India, and M.Tech degree in Computer network Engineering from Visvesaraya technological university.