

A Novel Hybrid Crypto-Biometric Authentication Scheme for ATM Based Banking Applications

Fengling Han¹, Jiankun Hu¹, Xinhua Yu², Yong Feng², and Jie Zhou³

¹ School of Computer Science and Information Technology,
Royal Melbourne Institute of Technology, Melbourne VIC 3001, Australia
{fengling, jiankun}@cs.rmit.edu.au

² School of Electrical and Computer Engineering,
Royal Melbourne Institute of Technology, Melbourne VIC 3001, Australia
{feng.yong, x.yu}@ems.rmit.edu.au

³ Department of Automation, Tsinghua University, Beijing 100084, China
jzhou@tsinghua.edu.cn

Abstract. This paper studies the smartcard based fingerprint encryption/authentication scheme for ATM banking systems. In this scheme, the system authenticates each user by both his/her possession (smartcard) and biometrics (fingerprint). A smartcard is used for the first layer of authentication. Based on the successful pass of the first layer authentication, a subsequent process of the biometric fingerprint authentication proceeds. The proposed scheme is fast and secure. Computer simulations and statistical analyze are presented.

1 Introduction

With rapidly increasing number of break-in reports on traditional PIN and password security systems, there is a high demand for greater security for access to sensitive/personal data. These days, biometric technologies are typically used to analyze human characteristics for security purposes [1]. Biometrics based authentication is a potential candidate to replace password-based authentication [2]. In conjunction with smartcard, biometrics can provide strong security. Various types of biometric systems are being used for real-time identification. Among all the biometrics, fingerprint-based identification is one of the most mature and proven technique [3].

Smartcard based fingerprint authentication has been actively studied [4-6]. A fingerprint based remote user authentication scheme by storing public elements on a smartcard was proposed, each user can access to his own smartcard by verifying himself using his fingerprint [4]. In [5] and [6], the on-card-matching using fingerprint information was proposed. However, these schemes require high resource on the smartcard and the smartcard runs a risk of physical attack. Together with the development of biometric authentication, incorporate biometric into cryptosystems has also been addressed [2]. However, instability of fingerprint minutiae matching hinders its direct use as encryption/decryption key. With the widely studied of automatic personal identification, a representation scheme which combines global and local information in a fingerprint was proposed [3, 7], this scheme is suitable for matching as well as storage on a smartcard.

Biometric authentication is image based. For remote biometric authentication, the images need to be encrypted before transmitted. Chaotic map used in image encryption has been demonstrated [8-10]. The permutation of pixels, the substitution of gray level values, and the diffusion of the discretized map can encrypt an image effectively.

In this paper, a biometric authentication protocol is proposed. Based on the modified Needham-Schroeder PK protocol [11], strong smartcard public key system for the first layer of authentication and then fingerprint authentication for the remaining parts are used. The primary application of our scheme is ATM based banking systems due to its popularity and trusted physical terminal that has 24 hours camera surveillance.

The rest of the paper is organized as follows: Section 2 provides the description of the new hybrid crypto-biometric authentication protocol. Generation of encryption key is studied in Section 3. Evaluation of the encryption scheme is conducted in Section 4. Conclusions are presented in Section 5.

2 Hybrid Crypto-Biometric Authentication Protocol (HCBA)

Generally, there are two basic fingerprint authentication schemes, namely the local and the centralized matching. In the central matching scheme, fingerprint image captured at the terminal is sent to the central server via the network, then is matched against the minutiae template stored in the central server.

There are three phases in HCBA: registration, login and authentication. In the registration phase, the fingerprints of a principal A are enrolled and the derived fingerprint templates are stored in the central server. The public elements and some private information are stored on smartcard. The login phase is performed at an ATM terminal equipped with a smartcard reader and a fingerprint sensor. The hybrid smartcard and ATM based fingerprint authentication protocol is shown in Fig.1.

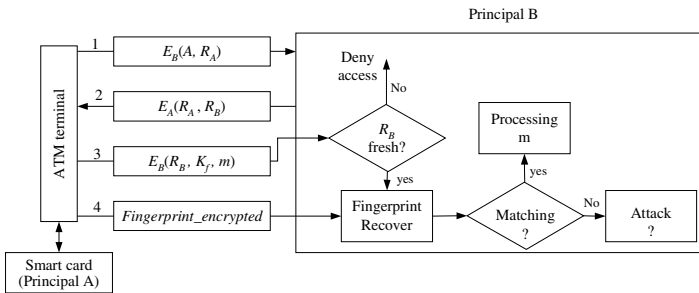


Fig. 1. Diagram of the new hybrid chaotic-biometric authentication protocol (HCBA)

The smartcard releases its ID and private key after being input at the terminal. The first layer of mutual authentication is done via messages 1 and 2 as following:

1. Alice sends message 1 $E_B(\mathbf{A}, \mathbf{R}_A)$ to identify herself \mathbf{A} together with a random number (nonce) \mathbf{R}_A , by using the principal \mathbf{B} (bank)'s public key.
2. Message 1 can only be read by principal \mathbf{B} with its private key. Then \mathbf{B} generates its own random number (nonce) \mathbf{R}_B and sends it together with \mathbf{R}_A in message 2 $E_A(\mathbf{R}_A, \mathbf{R}_B)$ encrypted with Alice's public key.

When Alice sees \mathbf{R}_A inside the message 2, she is sure \mathbf{B} is responding and it is fresh for she sent \mathbf{R}_A milliseconds ago and only \mathbf{B} can open the message 1 with \mathbf{B} 's private key. Conventional public key cryptographic protocols (modified Needham-Schroeder PK protocol [11]) can be used to exchange further challenge-response messages.

Fingerprint is integrated to complete the process of mutual authentication which is illustrated via messages 3, 4 and diagrams within the bank server as shown in Fig.1. In this process, Alice needs to provide her fingerprint, then the terminal will encrypt it. The encryption key \mathbf{K}_f can be generated from the raw fingerprint image, and is transmitted to the central server via secure channel (such as RSA cryptography).

When \mathbf{B} finds \mathbf{R}_B in message 3, it knows that the message 3 must come from Alice's smartcard and also fresh. Message 4 is the encrypted fingerprint of Alice.

After being verified that the smartcard belongs to the claimed user Alice, the $En(FP)$ in message 4 is recovered. At this stage, the bank \mathbf{B} can still not be sure the fingerprint is from Alice. The recovered fingerprint is then matched against Alice's fingerprint template. If the minutiae matching are successful, then \mathbf{B} will process the message m . Till now, the authentication phase is finished.

2 Improved Pixels Permutation and Key Generation

One complete encryption process consists of (1) One permutation with simultaneous gray level mixing, (2) One diffusion step during which information is spread over the image. The detail procedures are referred to [10]. The image encryption technique is based on [10], which assigns a pixel to another pixel in a bijective manner. The improvement of this proposed scheme is the permutation and the key generation.

3.1 Improved Permutation of Pixels

An image is defined on a lattice of finitely many pixels. A sequence of i integer, n_1, \dots, n_i such that $\sum n_i = N$ ($i \leq N$) is employed as the encryption key for the permutation of pixels. The image is again divided into vertical rectangles $N \times n_i$, as shown in Fig.2(a). Inside each column, the pixels are divided into N/n_i boxes, each box containing exactly N pixels. Take an example of 8×8 image shown in Fig.2(b), it is divided into 2 column ($n_1=3, n_2=5$). The pixels permutation is shown in Fig.2(c), the key is (3, 5).

The key is an arbitrary combination of integers, which add up to the pixels number N in a row. One can choose whatever digits in the key arbitrarily.

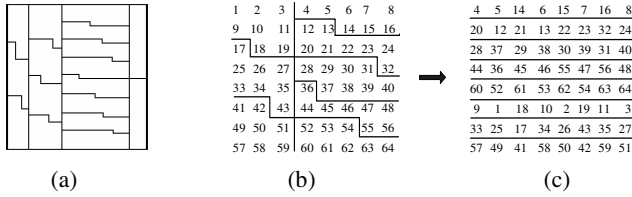


Fig. 2. Permutation of pixels. (a) $N \times 4$ blocks; (b) A 8×8 block; (c) After permutation.

If the raw fingerprint image is a $P \times Q$ rectangular, it can be reformed into a square $N \times N$ image first, where N is the integer makes $(N \times N - P \times Q)$ minimum.

3.2 Key Generation

Encryption keys are vital to the security of the cipher, which can be derived in the following three ways:

- From the randomly chosen values of pixels and their coordinates in raw image.

Randomly choose 5-10 points in the raw fingerprint image. The vertical and horizontal position of pixels, as well as the gray level values of each point is served as key. Mod operations are conducted. The key consists of the remainders and a supplementary digit that makes the sum of key equals to N . For example, in a 300×300 gray level fingerprint image, there are five points picked up, their coordinates and pixels values are: (16,17,250); (68,105,185); (155,134,169); (216,194,184); (268,271,216). After conducting mod(40) and mod(10) operations for the coordinates and the gray level values, respectively. The result is: (16,17,0); (28,25,5); (35,14,9); (16,34,4); (28,31,6). The sum of above five groups numbers is $S_8=268$. At last, a supplementary digit $N - S_m = 300 - 268 = 32$ is the last digit of the key. The encryption key is: {16, 17, 0, 28, 25, 5, 35, 14, 9, 16, 34, 4, 28, 31, 6, 32}.
- From the stable global features (overall pattern) of fingerprint image.

Some global features such as core and delta are highly stable points in a fingerprint [13], which have the potential to be served as cryptography key. Some byproduct information in the processing of fingerprint image can be used as the encryption key. For example, the Gabor filter bank parameters are: concentric bands is 7, the number of sectors considered in each band is 16, each band is 20 pixels wide; there are 12 ridge between core and delta, the charges of the core and delta point are 4.8138e-001 and 9.3928e-001, and the period at a domain is 16. Gabor filter with 50 cycles per image width. Then the key could be: {7, 16, 20, 12, 4, 8, 13, 8, 9, 39, 28, 27, 1, 16, 50, 42}. The last digit is the supplementary digit to make the sum of key equals to N .
- From the pseudo random number generator based on chaotic map.

One can also use the pseudo random number generator introduced in [10] to produce the key.

The users can choose how to generate keys in their scheme. To encrypt a fingerprint image, three to six rounds of iterations can hide the image perfectly; each iteration is suggested to use different key, and different way to generate the keys.

4 Simulation and Evaluation

In this section, the proposed encryption scheme is tested. Simulation results and its evaluation are presented.

4.1 Simulations

The gray level fingerprint image is shown Fig.3(a). The first 3D permutation is performed with the key {16, 17, 0, 28, 25, 5, 35, 14, 9, 16, 34, 4, 28, 31, 6, 32}. After first round 3D permutation, the encrypted fingerprint image is shown in Fig.3(b). The second round permutation is performed with the key {7, 16, 20, 12, 4, 8, 13, 8, 9, 39, 28, 27, 1, 16, 50, 42}. After that, the image is shown in Fig.3(c). The third round permutation is finished with a key {1, 23, 8, 19, 32, 3, 25, 12, 75, 31, 4, 10, 14, 5, 25, 13}. After this, the image is shown in Fig.3(d), which is random looking.

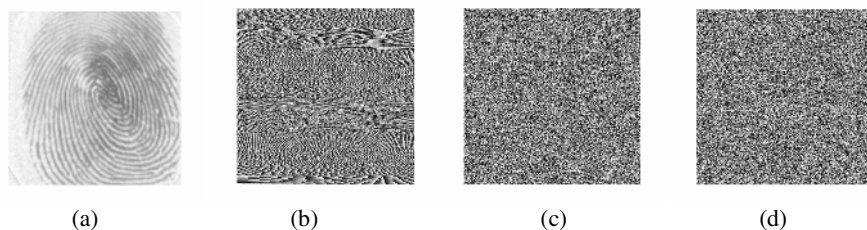


Fig. 3. Fingerprint and the encrypted image. (a) Original image; (b) One round of iteration; (c) Two rounds of iterations; (d) Three rounds of iterations.

4.2 Statistical and Strength Analysis

- Statistical analysis.

The histogram of original fingerprint image is shown in Fig.4(a). After 2D chaotic mapping, the pixels in fingerprint image can be permuted, but as the encrypted fingerprint image has the same gray level distribution, they have the same histogram as that in Fig.4(a). As introduced in Section 3, 3D chaotic map can change the gray level of the image greatly. After one round and three rounds 3D substitution, the histograms are shown in Fig.4(b) and (c) respectively, which is uniform, and has much better statistic character, so the fingerprint image can be well hidden.

- Cryptographic strength analysis.

In [10], the known plaintext and ciphertext only type of attack were studied: the cipher technique is secure with respect to a known plaintext type of attack. With the diffusion mechanism, the encryption technique is safe to ciphertext type of attack. As the scheme proposed here use different keys in different rounds of iterations, and the length is not constrained, it can be chosen according to the designer's requirement, there is a much large key space than that Fridrich claimed.

- Compared with Data Encryption Standard (DES).

The computational efficiency of the proposed fingerprint encryption scheme is compared with DES. The computation time use DES to encrypt the fingerprint image in Fig.4(a) is 24185ms in 33MHz 386 computer. To encrypt this fingerprint image with the proposed scheme in this paper, three rounds of iterations with 16 digits key in each iteration costs 5325ms with the same computer. Around one-fifth time of the DES did.

- Key transmission and decryption.

The security strength of messages 1, 2, and 3 in Fig.1 relies the asymmetric cryptography, such as RSA scheme which is widely employed. Even in the worst case that the attacker has Alice’s smartcard, he/she can successfully proceed the whole authentication process in terms of exchanging messages 1 through 4 in Fig.1, the attack will fail at the final fingerprint matching phase conducted in the bank sever **B** as the attacker does not have Alice’s fingerprint. If the attacker has Alice’s smartcard and legitimate messages from Alice’s last session, there seems a risk of breaking the security system. However as the encryption/decryption as well as key generation are within the secure ATM terminal, the attacker can not get access to the key K_f to recover the legitimate Alice’s fingerprint as only the bank **B** can open message 3. We also propose to use different keys generated with different methods in different rounds of iterations. This will make the protocol more secure.

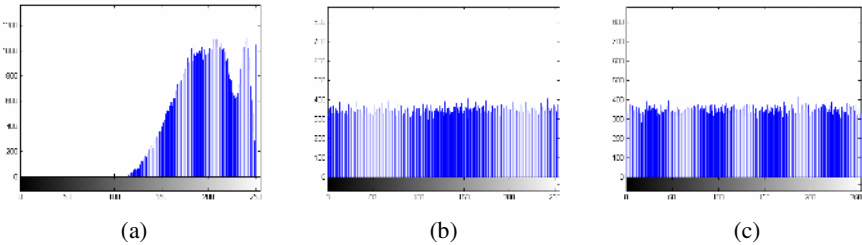


Fig. 4. Histograms of fingerprint image and the encrypted image. (a) Original fingerprint image; (b) One round of 3D iteration; (c) Three rounds of 3D iterations.

5 Conclusions

A smartcard based ATM fingerprint authentication scheme has been proposed. The possession (smartcard) together with the claimed user’s biometrics (fingerprint) is required in a transaction. The smartcard is used for the first layer of mutual authentication when a user requests a transaction. Biometric authentication is the second layer. The fingerprint image is encrypted via 3D chaotic map as soon as it is captured, and then is transmitted to the central server via symmetric algorithm. The encryption keys are extracted from the random pixels distribution in a raw image of fingerprint, some stable global features of fingerprint and/or from pseudo random number generator. Different rounds of iterations use different keys.

Some parts of the private key are transmitted to central server via asymmetric algorithm. The stable features of the fingerprint image need not to be transmitted; it can be extracted from the templates at the central server directly.

After decryption, the minutia matching is performed at the central server. The successful minutia matching at last verifies the claimed user.

Future work will focus on the study of stable features (as part of encryption key) of fingerprint image, which may help to set up a fingerprint matching dictionary so that to narrow down the workload of fingerprint matching in a large database.

Acknowledgments

The work is financially supported by Australia Research Council linkage project LP0455324. The authors would like to thank Associate professor Serdar Boztas for his valuable discussion on keys establishment protocol.

References

1. Soutar, C., Roberge, D., Stoianov, A., Gilory, R., Kumar, B.V.: Biometric encryption, www.bioscrypt.com.
2. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric cryptosystems: Issue and challenges, *Proceedings of the IEEE*, 92 (2004) 948-960
3. Jain, A.K., Prabhakar, S., Hong, L., Pankanti, S.: Filterbank-based fingerprint matching, *IEEE Trans. on Image Processing*, 9 (2000) 846-859
4. Lee, J.K., Ryu S.R., Yoo, K.Y.: Fingerprint-based remote user authentication scheme using smart cards, *Electronics Lett.*, 38 (2002) 554-555
5. Clancy, T.C., Kiyavash, N., Lin, D.J.: Secure smartcard-based fingerprint authentication, *ACM workshop on Biometric Methods and Applications*, Berkeley, California, Nov. (2003)
6. Waldmann, U., Scheuermann D., Eckert, C.: Protect transmission of biometric user authentication data for oncard-matching, *ACM symp. on Applied Computing*, Nicosia, Cyprus, March (2004)
7. Jain, A.K., Prabhakar S., Hong, L.: A multichannel approach to fingerprint classification, *IEEE Trans. on Pattern Anal. Machine Intell.*, 21 (1999) 348-359
8. Kocarev, L. Jakimoski, G., Stojanovski T., Parlitz, U.: From chaotic maps to encryption schemes, *Proc. IEEE Sym. Circuits and Syst.*, 514-517, Monterey, California, June (1998)
9. Chen, G., Mao, Y., Chui, C.: A symmetric encryption scheme based on 3D chaotic cat map, *Chaos, Solitons & Fractals*, 21 (2004) 749-761
10. Fridrich, J.: Symmetric Ciphers Based on two-dimensional chaotic maps, *Int. J. Bifurcation and Chaos*, 8 (1998) 1259-1284
11. Menezes, A., Oorschot, P., Vanston, S.A.: Handbook of Applied Cryptography. CRC Press, (1996)
12. Uludag, U., Ross, A., Jain, A.K.: Biometric template selection and update: a case study in fingerprints, *Pattern Recognit.*, 37 (2004) 1533-1542
13. Ratha, N.K, Karu, K. Chen, S., Jain, A.K.: A real-time matching system for large fingerprint databases, *IEEE Trans. on Pattern Anal. Machine Intell.*, 18 (1996) 799-813
14. Zhou, J., Gu, J.: A model-based method for the computation of fingerprints' orientation field, *IEEE Trans. on Image Processing*, 13 (2004) 821-835