Fingerprint Based Symmetric Cryptography

Subhas Barman
Dept. of Computer Sc. & Engg.
Govt. College of Engg. and Textile Tech.
Berhampore, West Bengal, India
Email: subhas.barman@gmail.com

Samiran Chattopadhyay
Dept. of Information Technology
Jadavpur University
Kolkata, West Bengal, India

Debasis Samanta
School of Information Technology
Indian Institute of Technology, Kharagpur
West Bengal, India

***Abstract*—Key management is an important issue in traditional symmetric cryptography. It consists of key generation, key modification and key sharing to establish a message communication between partners. In general, a randomly generated key is shared with the counter partner by transmitting it along with the message or prior to the message communication. Maintaining privacy of cryptographic key determines the security of cryptography. Biometric is the alternate to maintain the privacy of key by protecting it with users biometric from unauthorized access. In this paper, a cryptographic key is linked with users fingerprint data. A string of binary number as cryptographic key is extracted from fingerprint template and this key is used to encrypt a message. During decryption process, the user is able to generate that cryptographic key from a fresh fingerprint instance to decrypt the encrypted message.**

I. Introduction

The growing development of *Information and Communication Technology* (ICT) demands more and more attention of information security. The information which are digitally stored in media or are needed to be sent to an intended recipient can be protected using data encryption technique. In cryptography, plain text is encrypted into cipher text with the help of encryption algorithm and cipher text is decoded to plain text with the help of decryption algorithm. In both operations, cryptographic key plays an important role. It restricts the accessing of the encrypted data such that the owner of the key can decrypt cipher text properly. In this technique, it is assumed that only the genuine user knows the decryption key. Therefore, cryptography, as a powerful tool in information security, depends on secrecy of cryptographic key. The secrecy of cryptographic key needs an efficient key management technique. The key management technique includes the process of key generation, key modification and key sharing [1]. In traditional cryptography, key is not strongly linked with its owner. It results a difficulty to the user for remembering a randomly generated long cryptographic key. As a consequence, researchers are trying to integrate biometrics with cryptography to remove the above limitation. Biometric is the most trustworthy concern with high degree of assurance for person verification [2]. Considering the reliability of biometrics, it is combined with traditional cryptography to improve the information security with a stronger cryptosystem, known as *crypto-biometric system* (CBS) [3]. Biometric helps to manage the cryptographic key by binding the key with users whereas, encryption-decryption algorithm provides the normal course of responsibility of traditional cryptography.

In CBS, either cryptographic key is generated from biometric features or key is protected using biometric data. In both cases, there are some common issues [4]. Biometric instance is not free from error due to noise and behaviour pattern of user. On the other side, cryptography demands exactness in key otherwise it becomes meaningless. In the common practice of bio-key generation [14], [12], [13], [8], [11], [10], hash based algorithm is used to extract a binary string as cryptographic key. It is the characteristic of hash function that it produces a different value for a single bit changes in the source data. Similarly, in key release method [3], [5], [7], key is encoded with biometric data and the biometric data with error does not able to extract exact key from the cryptographic construction. The error in biometric is propagated to the cryptographic key [3]. In this regard, researchers are trying to use error correction coding to handle the errors in biometric data. There must be a trade-off between error correction capacity and inter-person variability. If the error correction capacity is increased, it increases the false acceptance ratio also.

In the traditional cryptography, knowledge or token based authentication is used to protect a randomly generated long key (i.e., 128, 256 bits key). In knowledge based authentication system, cryptographic key is stored somewhere else with a protection of user specified password. If the password becomes compromised by the attacker then, the key also becomes compromised. Moreover, the traditional cryptography is not able to provide non repudiation in information security. Similarly, a token is also used in traditional cryptography to store cryptographic key. The token also may be damaged or lost or stolen out. This way, token based authentication is also unable to provide non repudiation. Nevertheless, the user can generate a weak key intentionally for cryptographic use. To overcome the above mentioned limitations, fingerprint is the best alternate to generate a key from fingerprint data. In this paper, we propose an approach of CBS to generate cryptographic key from fingerprint template of user. This approach does not require to remembering the key or storing the key. As the key is generated from user's key, it can provide non repudiation to information security. This way, the proposed CBS becomes stronger than the existing approach.

The rest of the paper is organized as follows: a brief survey of related work is discussed in Section II and Section III describes the proposed methodology. Experimental results and analysis is given in Section IV and finally, the paper is concluded in Section V.

II. Related Work

There are many work related to CBS which are reported by the researchers. The biometrics are integrated with cryp-

tography in two ways, namely, (i) biometric based key release and (ii) cryptographic key generation from biometric data.

A. Biometric Based Key Release

In this scheme, cryptographic key is a secret and biometric data is the authenticator to protect that secret. The cryptographic key is released from the cryptographic construction only when genuine biometric data is provided. Fuzzy vault [5] and fuzzy commitment schemes [3] are the popular cryptographic constructions to bind a key with biometric data. In fuzzy commitment scheme, a binary string (b_{string}) of equal size of cryptographic key (K) is derivrd from biometric template and the key which is another binary string is XORed with b_{string}, i.e., $b_{string} \oplus K$. Hao et al. [3] proposed a biometric based fuzzy commitment scheme, where randomly generated cryptographic key K is protected by a binary code derived from iris.

In the existing work of key release, fingerprint based fuzzy vault scheme is proposed by many researchers [7] . In literature, coordinate of the minutiae points are used to hide a secret key (K) using a cryptographic construction based on fuzzy vault [7]. The vault releases a cryptographic key for a user who is able to present a query instance of genuine fingerprint to the vault as input. Similarly, Nandakumar et al. proposes a fingerprint based fuzzy vault scheme [5] where (x, y)-coordinates and alignment angle of the minutiae points are used to bind cryptographic key with user's fingerprint data.

B. Biometric Based Key Generation

Biometric based cryptographic key generation systems use biometric data, i.e., biometric features to derive a binary string of required length for cryptographic application. In literature, most of the biometric traits, like face [10], fingerprint [14], [12], [13], iris [11], voice [8], signature [9] etc. are used for cryptographic key generation. In most of the fingerprint based key generation approaches, key is generated from the biometric features of user. In [12], [13], [14] fingerprint minutiae points are used to generate cryptographic key using a user defined key generation algorithm. Multi-modal biometrics are also reported in literature to generate cryptographic key [14]. In [14], fingerprint and iris are used to generate a cryptographic key with the help of feature level fusion between two modalities of biometrics. In the literature, key generation depends only on the biometric data of user in most of the existing work. If the biometric data is compromised by the adversary anyway then, the key will be compromised and it results that the biometric becomes useless forever.

III. Proposed Methodology

Our proposed approach has three components, namely, template generation, key generation and key regeneration. Each steps are stated in details in the following.

A. Template Generation

Fingerprint features (F^A) are extracted from the fingerprint image (g_A) of user (A) using feature extraction algorithm (f). In this approach, minutiae points are detected as features from the fingerprint image (i.e., $m_i = f(g_A)$ for $i = 1, 2, ..., n$ and $m_i \in F^A$, where n is the total number of minutiae detected from g_A). Minutiae points are represented by the triplet of (x_i, y_i, θ_i) where (x_i, y_i) is the coordinate values and θ_i is the alignment angle of minutiae points m_i. In our approach, (x, y)-coordinate is used as minutiae points. The fingerprint template (F_{TA}) of user A is generated from the minutiae points F^A. The steps of template generation process are given below.

1) All distances ($d_{i,j}$) between the distinct minutiae points (i.e., m_i and m_j are computed and stored in a matrix D.
$$d_{i,j} = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (1)$$
$$D = [d_{1,1}, d_{1,2}, d_{1,3}, ..., d_{k,k+1}, d_{k,k+2}, ..., d_{n-1,n}, d_{n,n}] \quad (2)$$
2) Distances are sorted and only unique distances are stored in vector U_A as follows
$$U_A = [u_1, u_2, ..., u_q] \quad (3)$$
where u_i is a distance, $u_1 \leq u_2 \leq u_3 \leq ... \leq u_q$ and there are q numbers of unique distances in the vector U.
3) The unique distances are moved to another vector F_{TA} such a way that the value of u_i will be stored at a location of that vector where the index value is equal to the u_i.
$$F_{TA}[u_k] = u_k \quad (4)$$
4) The empty positions of F_{TA} are filed with zero
$$F_{TA}[t] = 0 \quad (5)$$
where $t \notin U_A$

In this way, template F_{TA} is generated with zero and non-zero values. The size of the template depends on the maximum distance $max(U_A)$.

This process of template generation is shown in 2. In the example, six minutiae points are taken as F^A i.e., $F^A = [a, b, c, d, e, f]$. The distances are assumed as given in Fig.2(b). There are $6 \times 6 = 36$ distances shown in the matrix. The template is shown in Fig.2 (d).

B. Key generation and message encryption

Fingerprint template is used to generate cryptographic key. In this work, key generation is simple. The template F_{TA} is taken and each element of F_{TA} generates a bit of the key. Overall steps of key generation by the user are shown in Fig.1. The steps are described below.

1) User A generates fingerprint template F_{TA} from fingerprint features.
2) User selects an element $F_{TA}(i)$ of template and puts 0 or 1 in the same location of key (i.e., $K[i]$).
3) User puts 1 in the first location of key vector K (i.e., $K[1] = 1$).
4) User puts 0 at $K[i]$ if $F_{TA} = 0$ (i.e., $K[i] = 0$) and puts 1 if $F_{TA} \neq 0$ (i.e., $K[i] = 1$).

This way, cryptographic key K is generated from fingerprint template F_{TA}. The key is used for message encryption and then it is discarded. A sample key is shown in Fig.2 (e) which is generated from template F_{TA}.

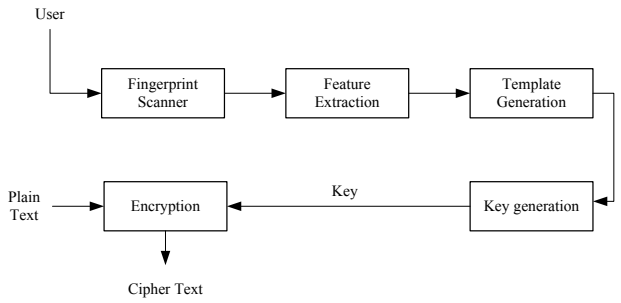


Fig. 1. Key generation and message encryption process

C. Key regeneration and cipher text decryption

The message (plain text P) is encrypted ($C = E_K(P)$) and cipher text (C) is stored in system. The key K is needed to be regenerated from the same fingerprint to decrypt the cipher text. Let us assume, the person A captures another instance of fingerprint of same fingerprint. Let, the instance is g'_A and the extracted feature set is $F^{A'}$ (i.e., $F^{A'} = f(g'_A)$ where f is the same minutiae detection algorithm used at the time of key generation for message encryption). The steps are given below.

The overall steps of the key regeneration process are shown in the Fig.3

1) User A produces his fingerprint to the fingerprint scanner and fingerprint image (g'_A) is captured.
2) Fingerprint features are extracted from the captured fingerprint image g'_A.
3) Query fingerprint template F'_{TA} is generated from extracted features $F^{A'}$ following the same process.
4) Cryptographic key K' is generated from F'_{TA}.
5) Cipher text (i.e., encrypted message) C is converted in plain text using decryption algorithm (i.e., $P = D'_K(C)$).

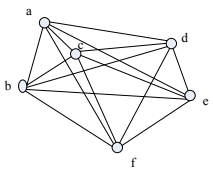
This way the cryptographic key is regenerated at the time of decryption of cipher text. The key K which is used for encryption and the key K' which is generated to use in decryption process should be exactly same otherwise the exact plain text will not be recovered.

IV. Experimental Result and Analysis

In our approach, fingerprint is used as input biometric trait. The experiment is carried out to generate fingerprint based cryptographic key for encryption and decryption. We observe the similarities between the keys generated from different instances of same fingerprint image. Our experiment also observes the strength of the key with respect to the impostor key which is generated from impostor's fingerprint.

A. Database

Fingerprint from fingerprint database FVC2004 (Set A) [15], [16] is used as input fingerprint in our experiment. The FVC2004 database consists of four datasets like DB1, DB2, DB3 and DB4. Fingerprints of DB4 dataset are synthetic fingerprint but remaining datasets consist of real fingerprints.



(a)

	a	b	c	d	e	f
a	0	15	12	28	40	35
b	15	0	14	32	35	24
c	12	14	0	20	23	22
d	28	32	20	0	10	23
e	40	24	23	10	0	20
f	35	24	22	23	20	0

(b)

Index	Distance
0	0
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	10
11	
12	12
13	
14	14
15	15
16	
17	
18	
19	
20	20
21	
22	22
23	23
24	24
25	
26	
27	
28	28
29	
30	
31	
32	32
33	
34	
35	35
36	
37	
38	
39	
40	40

(c)

Index	Distance
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	10
11	0
12	12
13	0
14	14
15	15
16	0
17	0
18	0
19	0
20	20
21	0
22	22
23	23
24	24
25	0
26	0
27	0
28	28
29	0
30	0
31	0
32	32
33	0
34	0
35	35
36	0
37	0
38	0
39	0
40	40

(d)

Key
1
0
0
0
0
0
0
0
0
0
1
0
1
0
1
1
0
0
0
0
1
0
1
1
1
0
0
0
1
0
0
0
1
0
0
1
0
0
0
0
1

(e)

Fig. 2. (a) Minutiae to minutiae distance, (b) Distance matrix, (c) Storing unique distances in a vector of size of maximum distance, (e) Non-existing distances are assumed as zero and blank locations of the vector are filled with zero. This is used as fingerprint template (e) Cryptographic key from template

Each dataset consists of 800 fingerprints of 100 persons with 8 instances of each person. The DB2 (Set-A) of FVC2004 contains 800 fingerprints and optical sensor U.are.U 4000 by Digital Persona is used to capture fingerprint image of size 328×364 at 500 dpi.

B. Experimental Setup

In our experiment, fingerprint from FVC2004 database (Set DB2A) is used as genuine and impostor fingerprints. To measure the accuracy of fingerprint based cryptographic key, a fingerprint instance of a person is considered to generate encryption key. The remaining instances of that fingerprint of the same person are taken as query fingerprint. The query

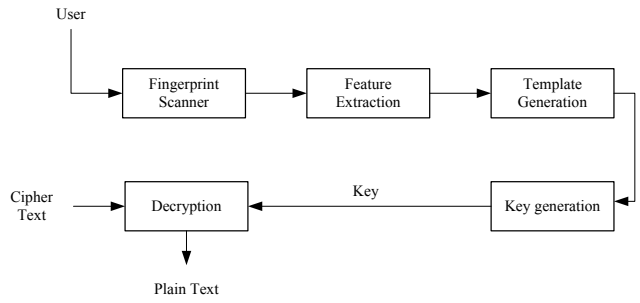


Fig. 3. Key regeneration and cipher text decryption process

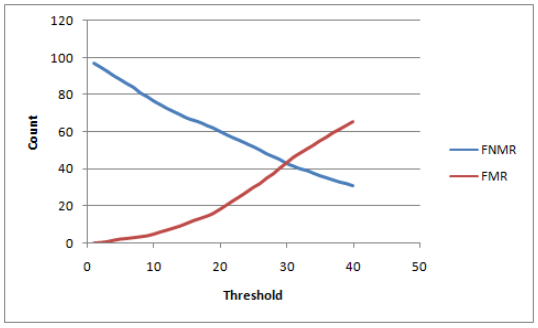


Fig. 4. FNMR vs FMR for FVC2004 DB2(A)

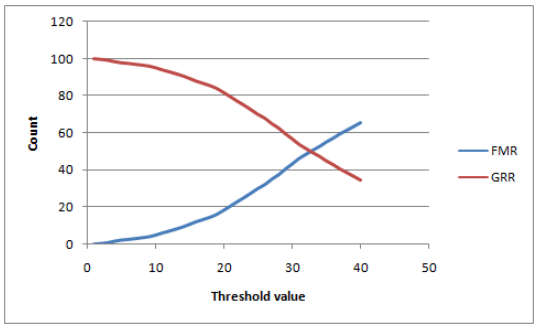


Fig. 5. FMR vs GMR for FVC2004 DB2(A)

fingerprint is used to generate test key and it is compared with the encryption key. The similarity between two keys are measured with respect to Hamming distance. If every bits of both keys are similar then the Hamming distance will be zero otherwise the distance will be similar to the total dissimilar bits. This way, the key is also compared with a key which is generated from impostor fingerprint template. Genuine key is generated from an instance of fingerprint and remaining seven instances are used to generate test key. If the keys generated from the instances of similar fingerprints are same then it is a genuine matching otherwise it is false non match. To observe genuine match and false non match ratio, total number of genuine tests is $((8 * 7)/2) * 100 = 2,800$. Similarly, False Acceptance Rate (FAR) is also observed in our experimental result. For FAR (False Acceptance Ratio) or FMR (False Match Ratio) computation, first instance of each person's fingerprint is compared with the first sample of the fingerprint of remaining person's. The total number of false acceptance tests is $((100 * 99)/2) = 4,950$.

In our approach, fingerprint features (i.e., minutiae points) are detected using MINDCT tool of NIST's NBIS software [6], [16]. The MINDTCT tool takes a fingerprint image as input and detects minutiae points as output. In our experiment, (x, y) coordinate values of minutiae points are used to generate template. Euclidean distance between two minutiae points is considered as distance between two minutiae points. The length of cryptographic key is 256 bits in our experiment.

C. Experimental Result

To measure the similarities and dissimilarities between two fingerprint based cryptographic keys, a predefined threshold value (in bits) is used as the indicator. If the difference between two keys is less than the threshold, then it is counted as a matching. Now if the test key is generated from the set of fingerprint instance of same person then it is a genuine matching. If the key is generated from different set of fingerprint instance of different person then it is taken as false matching. In our experiment, both, false rejection and false matching are investigated. According to the experimental result shown in Fig.4 the FRR is maximum when threshold value is minimum and FRR is minimum when the threshold is maximum. The maximum threshold value results maximum FMR, i.e., maximum threshold value minimizes the inter-person variability.

Similarly, we have also investigated the FMR vs GMR (Genuine Matching Rate) which is shown in Fig.5.

The FNMR of the keys is also plotted against genuine match ratio (GMR) which is shown in Fig.6.

D. Security Analysis

Fingerprint based cryptographic key is secured. The attacker does not have any knowledge about biometric of genuine user. The attackers can try to generate a key from his own fingerprint. In the experimental result, it is observed that inter-user variation of fingerprint template opposes to generate a genuine key from impostor fingerprint template. The information about fingerprint of genuine user is not recoverable as the key does not leak information about the minutiae points. Moreover, the key can be converted into revocable key by using any shuffling based transformation of the template vector.

V. Conclusion

Cryptography and biometrics are integrated with each other to improve security of cryptography. Cryptography is the strongest entity for information and network security whereas, biometric is the most trustworthy in authentication system. The problem of cryptography is with the management of cryptographic key. Biometric is used to address that problem of cryptography. In this approach, we have used fingerprint of user to generate a fingerprint based cryptographic key. There is no need to remember the key as it is generated from user's fingerprint. It also ensures the non-repudiation to information security. This approach also can be implemented using different biometric traits like iris, face, voice etc.

References

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice, 5e*, Prentice Hall, 2010.

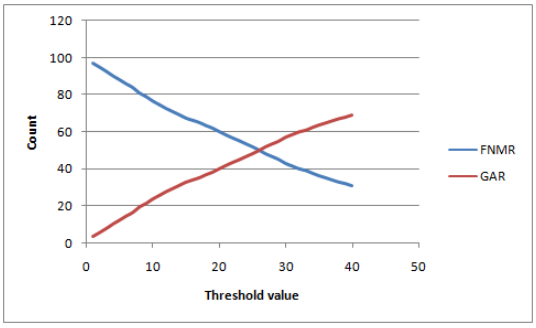


Fig. 6. FNMR vs GMR for FVC2004 DB2(A)

[2] D. Maltoni, D. Maio, A. K. Jain, S. Prabhakar, *Handbook of Fingerprint Recognition*, New York: Springer- Verlag, 2003.

[3] Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," *IEEE Transactions on Computers*, vol. 55, no. 9, pp. 1081-1088, 2006.

[4] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE (Special Issue Multimedia Security for Digital Rights Management), vol. 92, no. 6, pp. 948960, Jun. 2004

[5] K. Nandakumar, A. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance"*IEEE Trans. on Information Forensics and Security*, vol. 2, no. 4, pp. 744-757, 2007.

[6] C. Watson, M. Garris, E. Tabassi, C. Wilson, M. McCabe, S. Janet,and K. Ko *User's Guide to NIST Biometric Image Software (NBIS)*, National Institute of Standards and Technology, 2007.

[7] Yang, Shenglin, and Ingrid Verbauwhede. "Automatic secure fingerprint verification system based on fuzzy vault scheme." *Proceedings (ICASSP'05). IEEE International Conference on Acoustics, Speech, and Signal Processing,* Vol. 5. IEEE, 2005.

[8] Monrose, F., Reiter, M. K., Li, Q., and Wetzel, S. "Cryptographic key generation from voice." In *Proceedings of IEEE Symposium on Security and Privacy, 2001,* pp. 202-213.

[9] Feng, H., and Wah, C. C. "Private key generation from on-line handwritten signatures." *Information Management & Computer Security,* vol. 10, no. 4, pp. 159-164, 2002.

[10] Chen, B.; Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," In *Proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications,* vol., no., pp.394-401, 2007.

[11] Rathgeb, Christian, and Andreas Uhl. "Context-based biometric key generation for Iris." *IET computer vision.* vol. 5, no. 6, pp. 389-397. 2011.

[12] S. V. K. Gaddam and M. Lal, "Efficient Cancellable Biometric Key Generation Scheme for Cryptography," *International Journal of Network Security*' vol.11, no.2, pp.57-65, sep.2010.

[13] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from Cancelable Fingerprint Templates: An Enhanced and Effective Scheme," *European Journal of Scientific Research*, vol.31, no.3, pp.372-387, 2009.

[14] A. Jagadeesan, K. Duraiswamy, "Secured Cryptographic Key Generation from Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris," *International Journal of Computer Science and Information Security*, vol. 7, no. 2, pp.28-37, February 2010.

[15] Fingerprint Verification Competition FVC2004, [Online]. Available: *http://bias.csr.unibo.it/fvc2004.*

[16] Cappelli, M., Maio, D., Maltoni, D., Wayman, J.L., Jain, A.K., "FVC2004: Third Fingerprint Verification Competition," In *Proc of the First International Conference on Biometric Authentication*, (2004) 1-7.