International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 5, May 2016

Fuzzy Bio-Cryptography Key Generation

[1] Dr. Dayananda. R. B. [2] Dr. R. Sanjeev Kunte [3] Mr. Gowreesha. H. B. [4] Mr. Chandrashekar. B. S.
[1] Associate Professor and Head [2] Professor, [3] [4] Assistant Professor
[1][2][3][4] Department of Computer Science and Engineering
[1] GSSS Institute of Engineering & Technology for Women, Mysuru-570016
[2] Jawaharlal Nehru National College of Engineering, Shivamogga-577204
[3] Ekalavya Institute of Technology Chamarajanagar-571316
[4] RNS Institute of Technology, Bengaluru-560098

***Abstract*—Cryptography is one of the most effective ways to enhance the information security. In the traditional cryptographic algorithms, such as AES and DES etc, information is encrypted and decrypted using cipher keys. Simple keys are easy to be memorized while they are also easy to be cracked. On the other hand, the complex keys are difficult to be cracked while they are also difficult to be remembered and have to be stored in somewhere which can be stolen or lost. To solve these problems, biometric features, which cannot be forgotten, stolen, shared and cracked, have been combined with the cryptography to form biometric cryptography. Bio-cryptography integrates cryptography and biometrics to take advantage of the strengths of both fields. Bio-cryptographic techniques protects secret key by using biometric feature or generates a key from biometric features. The fingerprint biometric which is unique to the individual is used. Minutiae features are extracted from pre-processed fingerprint images. Cubic spline curve is fitted using bifurcation points of the extracted minutiae. A secret key of 128 bit length is formed by combining the control points of the cubic spline curve. This key can be used with any standard cryptography algorithm for encrypting the file. To decrypt the file, user's fingerprint image is matched with the registered database and on successful match key is released. An overall recognition rate of about 85% is obtained by the system.**

***Keywords*—Biometrics, Cryptographic key, key binding, key generation**

I. INTRODUCTION

Fingerprint recognition is one of the oldest forms of biometric identification. It has been used for over a century because of their uniqueness and consistency over time [1]. It is one of the most successful method used for person identification, which takes an advantage of the fact that, fingerprint of every individual is considered to be unique. No two people have the same set of fingerprints [2]. Even identical twins do not have identical fingerprints. Finger ridge patterns do not change throughout the life of an individual. Among the biometric features, the fingerprint is considered one of the most practical ones. Fingerprint recognition requires a minimal effort from the user and provides relatively good performance. Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. For fingerprint identification different works have been carried out.

In recent development of Information Technology, secured communication has become necessary. Cryptography is a kind of secret writing by which two parties can communicate with secret messages. Most of the researches were demonstrating that Biometric is the ultimate solution for identification and authentication, since it is proved as reliable and universally acceptable identification/authentication methods in many application areas.

The generation of cryptographic key from biometrics is used generally to secure the system. On the other hand, the storage and security for the biometric templates and the cryptographic key generation schemes make it suitable for integrating it with the biometric features.

The objective of the Biometric Encryption algorithm is to provide a mechanism for the linking and retrieval of a digital key using a biometric [4]. This biometric might be a 2D image such as fingerprint, palm print, face, iris or retina. The resulting digital key is then used as a cryptographic key.

Biometric Data from the user is collected and the Key is generated from the extracted minutiae features. The key can be used to encrypt any file containing audio, video, text information. When the system is presented with the biometric of the legitimate user the same key is regenerated which can be used to decrypt the originally encrypted file.

II. OBJECTIVES OF THE STUDY

The objectives of the proposed system are:

1. To develop suitable algorithms for Minutiae extraction from the fingerprint.
2. To design and develop suitable algorithm for generating Key.
3. To develop suitable techniques for matching the finger prints.
4. To develop Graphical User Interface for user registration and key generation.

III. ANALYSIS AND DESIGN

Biometrics

A biometric system is one kind of security system which recognizes a person based on his/her biometric characteristics. Applications include computer and network logon, physical access, mobile device security, government IDs, transport systems, medical records, etc. Biometric identifiers are the distinctive, measurable characteristics used to label and describe individuals [17]. Biometric identifiers are often categorized as physiological versus behavioral characteristics. Physiological characteristics are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and odor/scent. Behavioral characteristics are related to the behavior of a person, including but not limited to typing rhythm, gait, and voice.

Bio-Cryptography

Cryptography is one of the most effective ways to enhance the information security. In the traditional cryptographic algorithms, such as AES and DES etc, information is encrypted and decrypted using cipher keys, which may result in some problems. Biometric features, which cannot be forgotten, stolen, shared and cracked, have been combined with the cryptography to form biometric cryptography.

Bio-cryptography [3] integrates cryptography and biometrics to take advantage of the strengths of both fields. Bio-cryptographic techniques protected secret key by using biometric feature or generating a key from biometric features. In such systems, some public information is stored. Both the secret key and the templates are hidden in public information. However, it is computationally impossible to extract the key or the templates from the public information directly. There are two subcategories of bio-cryptographic techniques, they are:

(i) Key binding:

If public information derived from binding the secret key or templates, it is key binding (Figure 1), see [19, 20]. In biometrics-based key release, the biometric matching is decoupled from the cryptographic part. Biometric matching operates on the traditional biometric templates: if they match, cryptographic key is released from its secure location, e.g., a smart card or a server. Here, biometrics effectively acts as a wrapper mechanism in cryptographic domain.

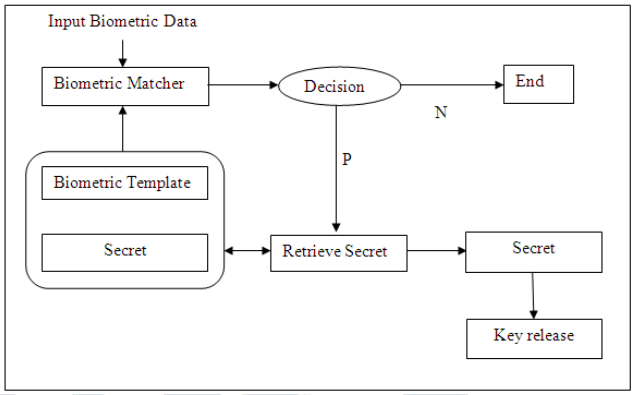

Figure 1: Key binding

Here public information derived from binding the secret key or templates. In a key-binding biometric cryptosystem, a cryptographic key and an unprotected fingerprint template are monolithically bounded together within a cryptographic framework to generate the helper data. The helper data is essentially a publicly available protected template which does not reveal any significant information neither about the key nor about the fingerprint template.

***Key generation*:**

If public information generated from templates only, while the secret key comes from the public information and query, it is key generation (Figure 2) see [21, 22, 23].

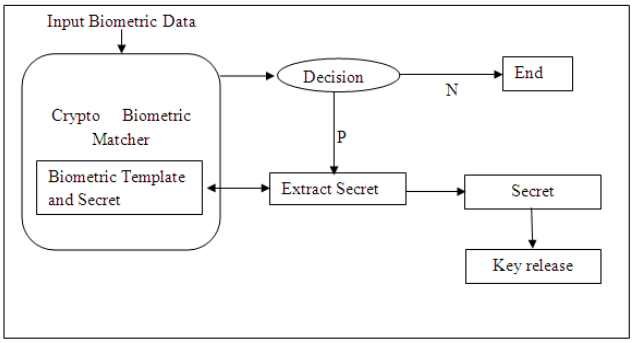

Figure 2: Key Generation

In biometrics-based key generation, biometrics and cryptography are merged together at a much deeper level. Biometric matching can effectively take place within cryptographic domain; hence there is no separate matching

operation that can be attacked; positive biometric matching extracts the secret key from the conglomerate (key/biometric template) data.

The generation of cryptographic key from biometrics is used generally to secure the system. On the other hand, the storage and security for the biometric templates and the cryptographic key generation schemes make it suitable for integrating it with the biometric features.

A technique to generate an irrevocable cryptographic key from the biometric template of the palm vein was proposed by B. Prasanalakshmi and A. Kannammal [6]. The minutiae features (including bifurcation points and ending points) that were extracted from the generated pattern were employed by the proposed technique. The other cryptographic keys are probable to theft. The keys obtained from the biometric entity are preferred more as owing to the reason that these biometric keys are connected to the user. Minutiae patterns obtained from the palm vein are changed to cancellable templates which consecutively are employed for irrevocable key generation.

Biometric Data from the user is collected and the Key is generated from the extracted minutiae features. The key can be used to encrypt any file containing audio, video, text information. When the system is presented with the biometric of the legitimate user the same key is regenerated which can be used to decrypt the originally encrypted file.

IV. SYSTEM DESIGN

The design of the Bio-Cryptographic key generation system involving different stages such as finger print image pre-processing, minutiae extraction, false minutiae removal, minutiae matching and post-processing. Algorithms for the techniques involved in the different stages of the proposed system are presented.

System Architecture

The block diagram of a general Bio-Cryptographic key generation system composed of two phases is shown in Figure 3. It mainly comprises of the section such as Biometric Phase as well as Key Generation Phase.

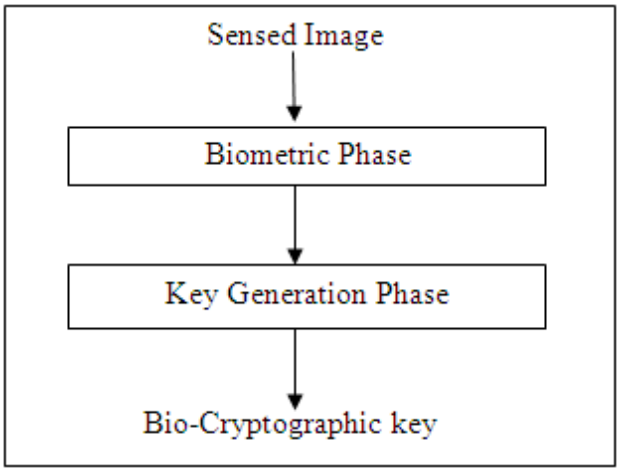

Figure 3: Bio-cryptographic key generation

The architecture of the proposed system is depicted in Figure 4. It has mainly three stages – Acquiring, Minutiae Extraction and Key Generation. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from fingerprint images. Thus, it is necessary to employ image enhancement techniques prior to minutiae extraction to obtain a more reliable estimate of minutiae locations.

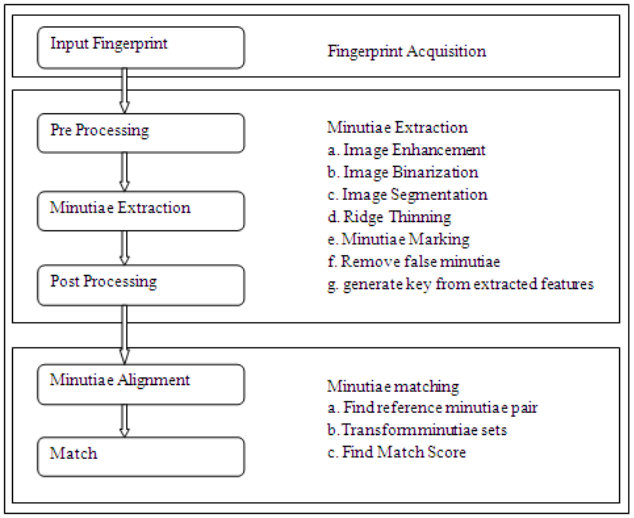

Figure 4: Proposed Bio-Cryptographic key generation system

Key Generation Phase

Algorithm: Bio-Cryptographic Key Generation
Step 1: For each input gray scale fingerprint image apply the following steps
Step 1.1: Apply minute feature vector extraction
Step 1.2: Find pixel value of minute feature vector over the fingerprint image.
Step 1.3: Save (y-axis, pixel value) to file name fingerprint.

Step 2: Apply fuzzy cubic spline for fingerprint vector elements [27].
Step 3: Save control point of the fuzzy cubic spline as the generated key.
Step 4: End.

V. RESULT AND DISCUSSIONS

Experimental Setup

To test the performance of the system a database of fingerprint is created. The database consists of eight fingerprint images of 10 persons from FVC-2004 database [28]. Each user's one fingerprint is taken for registration i.e., to register the user to the system with his key. The minutiae points are extracted from the given fingerprint image. Cubic-spline curve is fitted into minutiae points and the control points of the curve are used to generate the 128 bit secret key. The key and the fingerprint are stored in the database.

The key can be further used to encrypt any file using standard encryption algorithm. During the verification phase, another fingerprint of the same user is given as query image to retrieve the key. Fingerprint is pre-processed and minutiae features are extracted. The query minutiae points are then compared with that stored in the database. If there is a match with any of the user's fingerprint in the database, then the key will be released. The released key can be then used for decrypting the originally encrypted file by the same user.

A Graphical User Interface to provide the above functionalities is developed and implemented in MATLAB. The intermediate results and the performance analysis of the system are presented in the next section.

Experimental Results

After extracting the valid minutiae points from the fingerprint they need to be stored in some form of representation common for both ridge ending and bifurcation.

To generate the secret key, Y position (*y*, *py*) and corresponding pixel values of bifurcation points are used. Cublic spline curve is fitted into these (*y*, *py*) points. Table 4.3 shows these values in 1st and 2nd column and corresponding control points of the fitted curve in the 3rd column. 4th column gives the value of control points in Hexadecimal representation.

The secret key is formed by combining first *n* control points until the key becomes 128 bit length. So, the generated 128 bit key is:

Key = 53: D2: F2:35:0D:A9:2E:AC

TABLE I. Bifurcation points of fingerprint(X, Y), corresponding Pixel

Y position	Pixel Value	Control points	Control points(in Hex)
18	131	343343	53D2F
27	107	144653	2350D
30	40	169	A9
31	114	191183	2EACF
35	47	436	1B4

VI. CONCLUSION AND FUTURE SCOPE

In the implementation of biometric based secret key generation, the minutiae points are extracted from the given fingerprint image. Cubic-spline curve is fitted into minutiae points and the control points of the curve are used to generate the 128 bit secret key. The key and the fingerprint are stored in the database.

The developed system provides more secured secret key as it is derived from the user's biometric data (finger print) which is unique to the individual. Also the system can generate a key longer than 128 bit if stronger key is needed by combining more number of control points from the Cubic-spline fitted curve.

Future Scope

This work reported can be improved in future by following,

- Removal of all false minutiae points to improve recognition accuracy
- To make the key more random by considering ridge end points and orientation in generating the key

REFERENCES

[1] Ballan M, "Directional Fingerprint Processing", proceedings of Fourth International Conference on Communication, Networking & Broadcasting, pp. 1064-1067, 12-16 Oct. 1998.

[2] Mohamed Suliman M and Henry O Nyongesa, "Automatic Fingerprint Classification System Using Fuzzy Neural Techniques", proceedings of IEEE International Conference on Computing & Processing (Hardware/Software), pp. 12-17, May 2002.

[3] Hanaa M. A. Salman, "Fuzzy Bio-Cryptography Key Generation", proceedings of the 13th International ACIT 2012, Dec. 10-13.

[4] Kai Xi and Jiankun Hu, Bio-Cryptography - Handbook of Information and Communication Security, pp. 129-157, 2004

[5] Ratha., N. K., Chikkerur., S. Connell., J. H. Bolle., R.M., "Generating Cancelable Fingerprint Templates", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp.561 - 572, 2007.

[6] B. Prasanalakshmi, A. Kannammal, "A secure cryptosystem from palm vein biometrics", In proceedings of the ACM International, Seoul, Korea, pp. 1401-1405, 2009.

[7] H. A. Garcia-Baleon, V. Alarcon-Aquino, O. Starostenko, "K-Medoids-Based Random Biometric Pattern for Cryptographic Key Generation", proceedings of the 14th Iberoamerican Conference on Pattern Recognition, pp. 85 – 94, 2009.

[8] B. Chen, V. Chandran, "Biometric Based Cryptographic Key Generation from Faces", In Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394-401, 2007.

[9] Sangram Bana, and Dr. Davinder Kaur, "Fingerprint Recognition using Image Segmentation", International Journal of Advanced Engineering Sciences and Technologies, vol. 5, pp. 012 – 023, 2011.

[10] Sozan Abdullah Mahmood, "Fingerprint identification Based on Skeleton Minutiae extraction", proceeding of ICGST AIML Conference, pp. 161 -165, 2011.

[11] Marius Tico, Eero Immonen, Pauli Ramo, Pauli Kuosmanen, and Jukka Saarinen, "Finger print recognition using wavelet features", proceeding of IEEE International Symposium on Communication, pp. 21- 24, 2001.

[12] Jyoti Rajharia, and P.C. Gupta, "A New and Effective Approach for Fingerprint Recognition by using Feed Forward Back Propagation Neural Network", International Journal of Computer Applications, vol 52, pp. 020-028, 2012.

[13] Rajib Paul, Mustafa Sarwar Nasif, and S. M. Farhad, "Fingerprint recognition by Chain Coded String Matching technique", proceeding of International Conference on Information and Communication Technology, pp. 64-67, 2007.

[14] Ravi J, K.B. Raja, and Venugopal K.R, "Finger Print Recognition using Minutia Score Matching", International Journal of Engineering Science and Technology, vol.1, no. 2, pp. 35-42, 2009.

[15] W. Y. Leng, and S. M. Shamsuddin, "Fingerprint Identification using Discretization Technique", International Journal of Computer and Communication Engineering, pp. 205-213, 2012.

[16] L. O'Gorman, "Overview of fingerprint verification technologies", Elsevier Information Security Technical Report, vol. 3, 1998.

[17] Roli Bansal, Priti Sehgaland, Punam Bedi, Minutiae Extraction from Fingerprint Images - a Review, IJCSI International Journal of Computer Science Issues, vol. 8, Issue 5, No 3, 2011.

[18] Peter Stavroulakis, Mark Stamp, "Handbook of Information and Communication Security", Springer, ISBN 978-3-642-04116-7, 2010.

[19] A. Juels, M. Wallenberg, "A Fuzzy Commitment Scheme", In Proceeding of Sixth ACM Conference on Computer and Communications Security, Singapore, pp. 28-36, 1999.

[20] A. Juels, M. Sudan, " A Fuzzy Vault Scheme", In Proceeding of the IEEE International Symposium on Information Theory, Lau-sanne, pp. 408, 2002.

[21] Y.J. Chang, W. Zhang, T. Chen, " Biometrics Based Cryptographic Key Generation", In Proceeding of the IEEE Conference on Multimedia and Expo, Taipei, pp. 2203-2206, 2001.

[22] C. Vielhauer, R. Stcinmctz, A. Maycrhofcr, "Biomctric Hash Based on Statistical Features of Online Signatures", In Proceeding of the 16th International Conference on Pattern Recognition, Quebec, pp.123-126, 2002.

[23] Y. Dodis, R. Ostrovsky, L. Reyzin, A. Smith, "Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data", SIAM Journal on Computing, vol. 38, no. 1, pp.97–139, 2008.

[24] Kushal veer singh, "application of neural networks in fingerprint identification", thesis, 2010. [25] K. Venkateshwarlu, "Image Enhancement using Fuzzy Inference System", thesis, June 2010.

[26] Lin Hong, "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[27] Maria Cristina Floreno, Giovanni Novelli, "Implementingfuzzy polynomial interpolation (FPI) and fuzzy linear regression (LFR)".

http://www.dmi.unict.it/ojs/index.php/lematematiche/article/view/426

[28] http://bias.csr.unibo.it/fvc2004