ISSN:0975-9646

A Novel Method for Cryptographic Key Generation Fusing Dual Finger Vein Images

Saritha Reddy Venna [1], Ramesh Babu Inampudi [2]

[1]*Assistant Professor, Dept. of CSE, Acharya Nagarjuna University, AP, India*

[2]*Professor, Dept. of CSE, Acharya Nagarjuna University, AP, India*

***Abstract*— The ever growing needs of securing sensitive data in the presence of attackers and intruders has always been an existing issue of concern. Bio-cryptography is a new and embryonic field that combines cryptography with biometrics. The use of biometric traits in cryptography is a novel and promising area of research. The creation of a stable encryption key is one of the key challenges of bio-cryptography. A new cryptographic key generation method using dual finger vein images is proposed in this paper. This new approach not only simplifies the key generation process but also reduces the complexity involved in a traditional cryptosystem. Finger vein is a hidden biometric trait that resides underneath the skin surface which is invisible to the naked eye. The desirable characteristics of finger vein such as universality, distinctiveness, permanence and acceptability makes it a suitable biometric for the key generation process. Cryptographic key generated from the biometric template of an individual can be used as a personal key to encrypt and decrypt the information for secure transmission. Cryptographic keys of different sizes can be generated using this method with minimal amount of time complexity and space complexity. These keys can be used in many real time applications for secure data transmission.**

***Keywords*—Cryptographic Key, Biometrics, Finger Vein, Minutiae, Security**

I. INTRODUCTION

In recent days providing security to information has become more essential to safeguard the data from unintended users and intruders. Cryptography plays an essential role in providing security to the information being transmitted with the help of cipher keys. The process of encryption and decryption of data is done with the help of cipher keys which poses some problems [1]. Simple keys are very easy to remember as well as easy to crack. Complex keys are lengthy and are eventually difficult to crack as well. But such keys have to be stored in a secure place as they are difficult to remember and can easily be lost, stolen or illegally shared to unauthorized personnel and hence they are weak at providing non-repudiation. A better way to solve this problem would be to combine cryptography with biometrics known as bio-cryptography. A Biometric Cryptosystem can be either a key generation system or a key binding system that combines a high level of security provided by cryptography and non-repudiation provided by biometrics. A key generation system is one that produces stable cryptographic key using biometric features [2, 3]. Key binding system is one that binds a randomly generated cryptographic key to the biometric template [4, 5]. The notable problem of Bio-cryptography would be to generate a random cryptographic key with sufficient length and entropy [6].

Biometrics is the science of establishing the identity of an individual based on physical or behavioral characteristics of a human being [7]. Biometrics enhances the security of the entire system in which it is being implemented as they are distinct in nature [8] and offers non-repudiation [9]. The system could be either an authentication system or a crypto biometric system. Recently, biometric authentication is widely used for security purposes, as it is more secure and convenient to use. A biometric authentication system is an automated method of identifying or verifying an individual based on a physiological or behavioral trait [10]. Physiological traits such as fingerprint, iris, hand vein, retina, finger texture, finger vein, or the DNA refers to something an individual is. Behavioral traits such as gait, typing, speech, signature writing characteristics and keystroke dynamics are the ones that an individual can do. Of all the existing biometric traits, finger vein is an efficient and new physiological biometric trait which is being used in emerging biometric authentication systems [11, 12]. The seven factors such as universality, permanence, measurability, uniqueness, performance, acceptability and circumvention determines the suitability of a biometric trait to be used in a biometric based application [13]. Experiments indicate that equal error rate(ERR) of Miura "Repeated Line Tracking " finger vein method is 0.145% whereas the ERR of fingerprint based systems ranges from 0.2% to 4% which indicates that finger vein based recognition is much more efficient [14].

Riley et al. study [15] indicates that vein technology is very much suitable even to the elderly people in comparison to fingerprint biometric. Fingerprint has many disadvantages that includes susceptibility to the environmental conditions such as dust, temperature, ageing, fluctuation etc., lower image quality, can be easily forged, enrolment and scanning process is more difficult. The main objective of this paper is to generate a cryptographic key using dual finger vein patterns of an individual.

The rest of the paper is organized as follows. Finger Vein biometric characteristics are discussed in Section II. The survey of existing methods for feature level fusion and cryptographic key generation is provided in Section III. The proposed methodology for the generation of cryptographic key is presented in Section IV. Conclusion of the paper is given in Section V.

II. FINGER VEIN CHARACTERISTICS

A. *Uniqueness:* Each individual possesses a unique finger-vein pattern, even identical twins have distinct finger-vein patterns and these vein patterns help us to recognize individuals distinctly.
B. *Universality:* Finger vein pattern is inherent, unique and natural, and can be captured from any living human being using a finger vein scanner.
C. *Permanence:* The vein pattern remains stable over a long period of time without deterioration and cannot be changed even by a surgical operation.
D. *Acceptability:* It is widely accepted as the size of the capturing device is relatively small and the recognition accuracy is also high in comparison with other biometric authentication systems.
E. *Convenience:* The finger vein image acquisition process is simple and user-friendly as the images can be captured using contact-less sensors thereby ensuring convenience to the user.
F. *Liveness Detection:* As the finger vein is acquired from a living subject, it doesn't require additional computational effort.
G. *Difficult to Forge:* As vein patterns reside beneath the skin surface, they are difficult to be observed with the naked eye, forged or damaged.

III. LITERATURE SURVEY

A number of cryptographic algorithms are at present available to secure information, but all of these algorithms are essentially dependent on the security of the encryption or decryption key. A variety of biometric based techniques can be used for generating and also securing the keys and documents.

The first method uses stored template matching to unlock a cipher key storage. On the successful authentication of the user, the key gets released but the drawback would be using an insecure storage media for cipher key storage [16].

The second method uses the enrolment template itself to hide the cipher key using a bit-replacement algorithm. If the user is successfully authenticated, the key bits are extracted using this algorithm and the key is released [17].

Another method uses the biometric data derived directly from a biometric image to generate the cryptographic key [18].Biometric data acquired in general is of low quality since it depends on the person's physiological or behavioural characteristics and many external factors such as environment, sensor quality etc. Hence the biometric images are noisy and only an approximate comparison is possible with the stored template.

The core of bio-cryptography lies in the generation of cryptographic keys from the uncertain biometrics. Below discussed are a few works that describe different methods to generate the cryptographic key from biometric data.

Ushmaev et al. [19] proposed a topological fingerprint minutiae point neighbourhood descriptors based approach that has the following advantages. Topological descriptors are very stable minutiae that are independent of finger image noise and elastic deformations that allow varying length of keys and decryption rates.

Hu et al. [20] investigated the effect on the generated keys when an original fingerprint image is rotated. Analysis indicates that information integrity of the original fingerprint image can be significantly compromised by image rotation transformation process. It was discovered that the quantization and interpolation process can change the fingerprint features to a greater extent without affecting the original image.

Costanzo [21] proposed an approach that eliminates the need for template storage and demonstrates how a cryptographic key can be constructed through the use of biometric feature and parametric aggregation along with certain mathematical combinatorial and permutation constructs.

Zheng et al. [22] proposed a method for cryptographic key generation from biometric data using a lattice mapping based fuzzy commitment method. This method not only generates high entropy keys, but also conceals the original biometric data such that it is highly impossible to recover the stored biometric data even when the stored information is exposed to an attacker or an unauthorized user.

Wu et al [23] proposed a novel biometric cryptosystem based on the most accurate biometric feature - iris. In this method, a 256-dimension textural feature vector is extracted from the pre-processed iris image by using a set of 2-D Gabor filters. Later a modified fuzzy vault algorithm is used to encrypt and decrypt the data.

A.Jagadeesan et al. [24] proposed the feature level fusion of fingerprint and iris for cryptographic key generation. Fingerprint and iris image are initially subjected to preprocessing and then the feature vectors are generated for both the fingerprint and iris images. Then both the feature vectors are fused at the feature level to generate the cryptographic key.

IV. PROPOSED METHODOLOGY FOR CRYPTOGRAPHIC KEY GENERATION

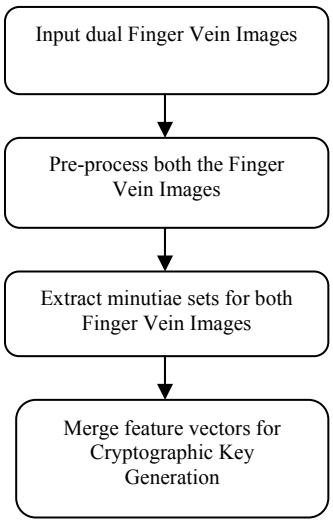


Fig.1 Methodology for Cryptographic Key Generation

Cryptographic Key Generation consists of the below mentioned steps.

A. Two finger vein images are taken as input from a benchmark database.
B. The dual vein images are subjected to pre-processing to enhance the image quality.
C. The features are then extracted and fused at the feature level to create a merged template.
D. Cryptographic key is generated using the features from the merged feature vector.

B. PREPROCESSING OF FINGER VEIN

Preprocessing of finger vein includes various steps such as region of interest (ROI) extraction, normalizing it interns of size and intensity, noise removal and image contrast enhancement. The preprocessing phase plays an essential role in the subsequent extraction of the vein pattern from the finger vein image.

1) Region of Interest extraction: Firstly, the input vein image is converted to a gray-scale image. Then the required region of the finger is extracted from the vein image eliminating the unwanted regions. ROI image is then resized so that the computational time decreases for subsequent processing.

2) Denoising and Background removal: To remove unwanted noise from the input vein image, Gaussian filter is used to smooth the ROI image. A Gaussian filter is a low pass spatial filter used to reduce high frequency image components and is represented as $G(x,y;\sigma) = Ke^{-\frac{x^2+y^2}{2\sigma^2}}$, where σ denotes the Gaussian kernel width and $K=\frac{1}{2\pi\sigma^2}$ is the normalization constant. Let us assume that $I(x,y)$ denotes the ROI image, $F_G(x,y)$ denotes the Gaussian filtered image of $I(x,y)$, we can get

$$F_G(x,y) = G(x,y;\sigma) * I(x,y) \qquad (1)$$

where * is the two-dimensional convolution operation.

The background of the vein image is removed using Otsu's segmentation algorithm [25]. In order to classify the pixels into two classes: C1, the finger vein pixels and C2, the background pixels, the Gaussian filtered image has to be thresholded. Let $F_R(x,y)$ denote the Gaussian filtered image with background pixels removed, we can express the finger vein segmentation as

$$F_R(x,y) = \begin{cases} F_G(x,y), & \text{if } F_G(x,y) \geq u; \\ 0, & \text{otherwise.} \end{cases} \qquad (2)$$

where $u = [0, \overline{255}]$ the threshold value that maximizes the Otsu's cost function for the separation of vein and background pixels.

3) Image Contrast enhancement: The vein image has to be enhanced in order to extract the vein pattern efficiently. A guided filter [26] is an edge preserving smoothing operator which is used to enhance the vein network. A Gabor filter [27] is an excellent band pass filter to remove noise along with preservation of ridges. Hence, a combination of guided filtering followed by multichannel Gabor filtering [28] is used to enhance the vein pattern.

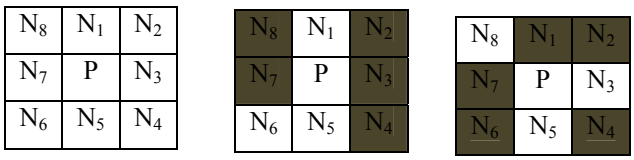
4) Image Segmentation and Thinning: After the image enhancement process, the filtered finger vein image has two kinds of pixels (finger vein and non-finger vein).Then the image is subjected to generic global segmentation which produces a binary image. Then morphological opening operations are performed on the segmented image to reduce the segmentation noise. Then a thinning algorithm is applied on the binarized vein pattern image that helps in proper extraction of the vein pattern [29].

(a) (b) (c) (d) (e) (f) (g)

Fig.2: (a) Raw Finger vein image. (b) Preprocessed image. (c) Guided filtered image. (d)Multichannel Gabor filtered image.(e)Segmented image. (f)Post morphological operations. (g)Thinned image.

C. FEATURE EXTRACTION

Feature extraction is a kind of dimensionality reduction mechanism that represents the required parts of an image as a compact feature vector. The intersection points of vein pattern in the thinned image are considered as the basis for minutiae extraction. To locate the intersection points in the vein pattern, 8 neighborhood connectivity is used. The thinned image after preprocessing is taken as the input and a simple procedure is applied in order to trace these locations. Assuming a pixel neighborhood shown in Fig. 3, a vein pixel P is considered an intersection point if it has 3 pixels as vein neighbors N_w, it means three white pixels. To determine that a pixel is a real intersection point, N_w pixels must not be adjacent between them as illustrated in Fig. 3. A false intersection point is depicted in Fig. 3(b) and Fig. 3(c) depicts a real intersection point. All the real intersection points are extracted and a feature vector is created based on the extracted minutiae.



(a)Neighbourhood Connectivity (b) Not a real intersection point (c)Real intersection point

Fig.3: Intersection Point Localization. $N_1, N_2, \ldots, N_8$ are the neighborhood pixels of the intersection candidate pixel P.

D. CRYPTOGRAPHIC KEY GENERATION USING FEATURE LEVEL FUSION

The feature vectors generated from the two finger vein images are fused at the feature level to generate a new merged feature vector. Then the cryptographic key is generated from the merged feature vector. The strength of cryptography can be measured based on the stability of cryptographic keys generated from uncertain biometrics. The message being transmitted is being encrypted and decrypted using the generated dual finger vein cryptographic key. The process of encryption and decryption is as discussed below.

1) Encryption: Encryption is a process of converting the original plain text message into cipher text in order to protect the information from various kinds of attacks. The finger vein true minutiae are stored as finger vein feature template in the database in the form of minutiae positions as x and y coordinate positions.

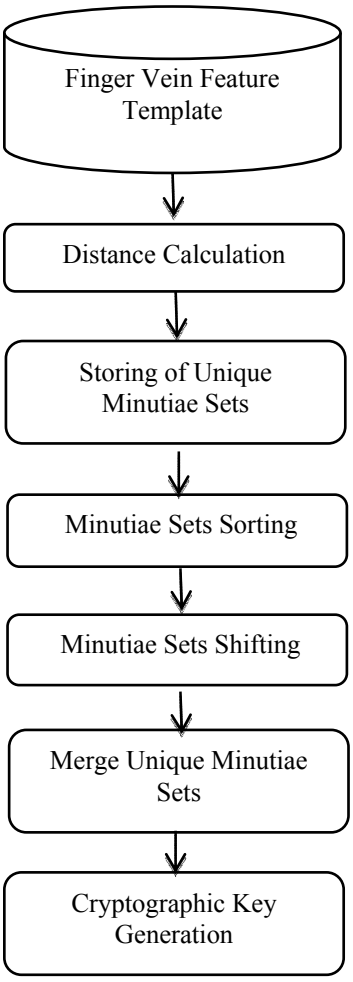


Fig.2 Steps involved in Cryptographic Key Generation

Figure 2 describes the below steps for cryptographic key generation for secured communication. Let us consider two finger vein images of the same individual for cryptographic key generation. The feature vectors generated for both the finger vein images FV_a and FV_b are represented as

$$FV_a = \{FV_1, FV_2, FV_3, ..., FV_m\} \text{ and}$$

$$FV_b = \{FV_1, FV_2, FV_3, ..., FV_n\}$$

where $FV_1, FV_2, FV_3, ..., FV_m$ and $FV_1, FV_2, FV_3, ..., FV_n$ represents the finger vein minutiae points with x and y co-ordinate values.

The distance D between two minutiae points FV_i and FV_j is computed using the below equation as suggested by Karthik Nandakumar et al [30].

$$D(FV_i, FV_j) = \sqrt{(U_i - U_j)^2 + (V_i - V_j)^2} \qquad (2)$$

where (U_i, V_i), (U_j, V_j) are co-ordinates of points P_i and P_j respectively. The distance value between the minutiae points is calculated and unique minutiae values are stored in two different arrays for both the finger vein images.

$DV_1 = [D_1, D_2, ..., D_m]$ and $DV_2 = [D_1, D_2, ..., D_n]$ are the arrays used to represent the distance between the minutiae for both the finger vein images. Sorting the values of the first array in ascending order and the second array in descending order we get the respective arrays as

$$Asc\,[DV_1] = [AscD_1, AscD_2, AscD_3, ..., AscD_m] \text{ and}$$

$$Desc\,[DV_2] = [DescD_1, DescD_2, DescD_3, ..., DescD_n]$$

Performing right shift by one bit on $Asc\,[DV_1]$ gives $RS\,[DV_1] = [RSD_1, RSD_2, RSD_3, ..., RSD_m]$ and shifting $Desc\,[DV_2]$ to the left by one bit generates the matrix $LS\,[DV_2] = [LSD_1, LSD_2, LSD_3, ..., LSD_n]$. This eventually increases the complexity to retrieve the key and also enhances the user security. Then, these two matrices are sorted and merged to generate a new fused matrix as $FusedD_M = RS\,[DV_1] \cup LS\,[DV_2]$

The matrix $FusedD_M$ is used for generating cryptographic key which can be used to transfer information in a more secure manner. Lastly, the 256-bit cryptographic key generated from the proposed approach is depicted in the below figure.

```
11110001111111111110001111110111111101101111111111111
11001111110111111111110011111111111111110011001101111
01111111101111111011111111101111111111110011111111111
11111111111101111011111011111111011111001111101111111
00111111100111111001000111111011111110111111
```

2) Decryption: The process of converting the cipher text back to its original form is known as Decryption. The key values used to encrypt the message should be communicated to the receiver in order to decrypt the encrypted message.

V. CONCLUSION

In this paper we have proposed a method for generating a user-specific cryptographic key using two finger vein images of the same individual. Both the vein images are subjected to preprocessing and then the features are extracted. Lastly, the feature vectors of both the vein images are fused at the feature level to create a 256 bit length cryptographic key. This key can be used in the subsequent process of encryption and decryption for secure transmission of information. The future scope would be to create a crypto-biometric system that involves finger vein authentication for user identification and using the generated cryptographic key for encrypting and decrypting the information for invulnerable communication in the context of network security.

REFERENCES

[1] A. Venckauskas, N. Jusas, I. Mikuckiene, S. Maciulevicius, ―Generation of the secret encryption key using the signature of the embedded system‖, Information technology and control, T. 41, nr. 4, pp. 368–375, 2012.

[2] G. I. Davida, Y. Frankel, B. J. Matt: On Enabling Secure Applications through Off-Line Biometric Identification. In Proceedings of the IEEE Symposium on Privacy and Security, pp. 148-157, 1998

[3] Yao-Jen Chang, Wende Zhang, Tsuhan Chen, Biometrics-based cryptographic key generation," Multimedia and Expo, 2004. ICME '04. 2004 IEEE International Conference on , vol.3, pp. 2203,2206 Vol.3, 27- 30 June 2004.

[4] A. Juels, M. Sudan: A fuzzy vault scheme. In Proc. IEEE Int. Symp. Information Theory, IEEE Press, p. 408, 2002

[5] Y. Dodis, L. Reyzin, A. Smith: Fuzzy Extractors: How to Generate Strong Keys from Biometrics and Other Noisy Data. In Proceedings of the Eurocrypt 2004, pp. 523-540, 2004

[6] C. Tilborg (Ed). Encyclopedia of Cryptography and Security. Springer, 2005.

[7] A. K. Jain, A. Ross: Introduction to Biometrics. In "Handbook of Biometrics", A. Jain et al. (Eds), Springer, 2008.

[8] Y. C. Feng, P. C. Yuen, A. K. Jain: A Hybrid Approach for Face Template Protection. In Proceedings of SPIE Conference of Biometric Technology for Human Identification, Orlando, USA, Vol. 6944, pp. 325, 2008.

[9] P. Balakumar, R. Venkatesan: A Survey on Biometrics-based Cryptographic Key Generation Schemes. International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85, 2012.

[10] A. K. Jain, A. Ross, S. Prabhakar: An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, pp. 4-20, 2004

[11] J. Hashimoto, Finger ―Vein Authentication Technology and Its Future‖,VLSI Circuits, Digest of Technical Papers. – pp. 5–8, 2006.

[12] A. Venckauskas, N. Morkevicius, K. Kulikauskas, ―Study of Finger Vein Authentication Algorithms for Physical Access Control‖, Electronics and Electrical Engineering, No. 5(121). – pp. 101–104, 2012.

[13] A. K. Jain, R. Bolle, and S. Pankanti, "Biometrics: Personal Identification in Networked Society", 1999, Kluwer Academic Publishers.

[14] N. Miura, A. Nagasaka ir T. Miyatake, ―Automatic Feature Extraction from non-uniform Finger Vein Image and its Application to Personal Identification‖ IAPR Workshop on Machine Vision Applications, Dec. 11 - 13.2002, Nara- ken New Public Hall, Nara, Japan, 2002.

[15] C. Riley, H. McCracken, K. Buckner, ―Fingers, veins and the grey pound: accessibility of biometric technology‖, Proceedings of the 14th European conference on Cognitive ergonomics (ECCE'07). – New York, NY, USA, 2007. – pp. 149–152, 2007.

[16] Handbook of Information and Communication Security, P. Stavroulakis, M. Stamp (Eds.), Springer, 2010.

[17] U. Uludag, "Secure biometric systems," Ph.D. dissertation, Michigan State University, http://biometrics.cse.msu.edu/Publications/Thesis/UmutUludag_SecureBSecureBio_PhD06.pdf, 2006.

[18] M. S. Al-Tarawneh, L. C. Khor, W. L. Woo, and S. S. Dlay, ―Crypto key generation using contour graph algorithm‖, in Proceedings of the 24th IASTED international conference on Signal processing, pattern recognition, and applications (SPPRA'06), M. H. Hamza (Ed.). ACTA Press, Anaheim, CA, USA, pp. 95-98, 2006.

[19] O. Ushmaev, V. Kuznetsov, V. Gudkov, "Extraction of Binary Features from Fingerprint Topology," Hand-Based Biometrics (ICHB), 2011 International Conference on , vol., no., pp.1,6, 17-18 Nov. 2011.

[20] Peng Zhang, Jiankun Hu, Cai Li, Mohammed Bennamoun, Vijayakumar Bhagavatula, ―A pitfall in fingerprint bio-cryptographic key generation‖, Computers & Security, Volume 30, Issue 5, July 2011, pp. 311–319, 2011.

[21] C. R. Costanzo, "Active Biometric Cryptography (ABC): Key Generation Using Feature and Parametric Aggregation," Internet Monitoring and Protection, 2007. ICIMP 2007. Second International Conference on , vol., no., pp.28,28, 1-5 July 2007.

[22] Gang Zheng, Wanqing Li, Ce Zhan, "Cryptographic Key Generation from Biometric Data Using Lattice Mapping," Pattern Recognition, 2006. ICPR 2006. 18th International Conference on , vol.4, pp.513–516,2006.

[23] Xiangqian Wu, Ning Qi, Kuanquan Wang, Zhang D., "An Iris Cryptosystem for Information Security", Intelligent Information Hiding and Multimedia Signal Processing, 2008. IIHMSP '08 International Conference on, pp. 1533–1536, 2008.

[24] A.Jagadeesan Dr. K.Duraiswamy, Secured Cryptographic Key Generation From Multimodal Biometrics: Feature Level Fusion of Fingerprint and Iris, (IJCSIS) International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010, pp.296-305.

[25] N. Otsu, "A threshold selection method from gray-level histograms," Automatica, vol. 11, no. 285-296, pp. 23–27, 1975.

[26] K. He, J. Sun, and X. Tang, "Guided image filtering," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 6, pp. 1397–1409, 2013.

[27] J. Yang, J. Yang, and Y. Shi, "Finger-vein segmentation based on multichannel even-symmetric gabor filters," in IEEE International Conference on Intelligent Computing and Intelligent Systems, 2009. ICIS 2009., vol. 4. IEEE, 2009, pp. 500–503.

[28] S. J. Xie, J. Yang, S. Yoon, L. Yu, and D. S. Park, "Guided gabor filter for finger vein pattern extraction," in 2012 Eighth International Conference on Signal Image Technology and Internet Based Systems (SITIS). IEEE, 2012, pp. 118–123.

[29] L. Lam, S.-W. Lee, and C. Y. Suen, "Thinning methodologies-a comprehensive survey," IEEE Transactions on pattern analysis and machine intelligence, vol. 14, no. 9, pp. 869–885, 1992.

[30] Karthik Nandakumar, Anil K. Jain, Sharath Pankanti, Fingerprint-Based Fuzzy Vault: Implementation and Performance, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007, pp.744-757.