DEVELOPMENT OF BIO-CRYPTO KEY FROM FINGERPRINTS USING CANCELABLE TEMPLATES

Prof. Sunil VK Gaddam
Head, Department of CSE
Meerut Institute of Engineering & Technology
MEERUT - 250 005, (U. P.), INDIA.

Prof. Manohar Lal
Director, SOCIS
Indira Gandhi National Open University
New Delhi – 1100068.

ABSTRACT

Identity theft can be effectively solved by the integration of biometrics and cryptography. Lately, researchers and experimenters have been greatly attracted by the improved performance (protection) of cryptographic keys produced from biometrics. However, there exists an eternal association between the biometric and the user, where in, alteration is not viable. Hence, a compromise of the biometric feature will consequently lead to a perpetual and possible loss of biometric for all the applications that employ it. The generation of replaceable biometric templates through cancelable biometrics has emerged as a possible solution to the aforesaid problem. In this paper, we propose an efficient approach for cryptographic key generation from fingerprint biometrics using cancelable templates. The proposed approach is composed of three phases namely: 1) Extraction of minutiae points from the fingerprint image, 2) Generation of cancelable biometric templates with added security and 3) Cryptographic key generation from the Secured cancelable template. The resultant cryptographic key thus generated is irrevocable and unique to a particular cancelable template, making the generation of new cancelable templates and cryptographic keys feasible. The experimental results portray the effectiveness of the cancelable template and the cryptographic key generated.

Keywords: Biometrics, Cancelable Biometrics, Fingerprint, Minutiae points, Cryptography, Key generation, Advanced Encryption Standard (AES).

1. INTRODUCTION

Preserving personal privacy and dissuading identity theft are national priorities. These objectives are vital to our democracy and our economy, and innately significant to our citizens. Biometrics, a promising set of technologies, offers an effective solution [1]. A biometric system is fundamentally a pattern recognition system that works by obtaining individual's biometric data, extracting a feature set from the obtained data, and comparing the extracted feature set against the template set in the database. Even though the field of biometrics is still in its early stages of development, it's inevitable that the biometric systems will take an active part in the future of security [1]. The term 'biometric' refers to an individual's physical or behavioral characteristic that is inherent, such as their voice, face, fingerprint, keystroke dynamics and more. The principal advantages of the biometrics over the traditional security mechanisms using passwords are: cannot be forgotten, hard to copy or forge, unfeasible to share and proffer better security than a normal eight character password [26, 2].

Over the past decades, biometrics has generally been used for verifying the individual's identity. In the realm of computer security, biometrics denotes the authentication techniques that depend on measurable physiological and individual characteristics that can be verified automatically [1]. The accomplishments of biometrics in user authentication have signified that, a number of advantages could be gained by the incorporation of biometrics with cryptography [26]. In cryptography, the incapability of human users to bear in mind strong cryptographic keys has been a factor restraining the security of systems for decades. The above cryptographic curb could be addressed in an extensive range of applications by the generation of strong cryptographic keys from biometric data, probably in juxtaposition with the entry of a password [3, 4]. The inabilities to copy or falsify and share are the chief factors that influence the use of biometrics in cryptographic key generation. In modern times, with the purpose of eliminating the necessity for key storage using passwords, researchers have focused on merging biometrics with cryptography as a possible means to improve overall security [6, 7].
In a basic cryptographic system, user authentication is primarily possession based. A user is generally authenticated based on the possession of unique identifier, for instance, the possession of the decrypting key. As

the cryptographic keys commonly employed are long and random, (e.g., keys in Advanced Encryption Standard (AES) [8, 9]), they are hard to memorize and remember. Consequently, the cryptographic keys are stored in someplace (for example, on a computer or a smart card) and released on the basis of some alternative authentication (e.g., password) mechanism, that is, upon making certain that they are being released only to the authorized users. And, in most cases, the passwords used for key storage are every simple that they can be effortlessly guessed (particularly on the basis of social engineering methods) or broken by simple dictionary attacks [10]. A more significant solution to the problem is to design cryptosystems based on biometrics, necessitating neither storage nor remembrance of passwords. The system devised by integrating biometrics with cryptographic security is known as Biometric cryptosystems, or Crypto-biometric systems [11]. Lately, a number of researchers have attempted to devise biometric cryptosystems to overcome some of the problems faced by generic cryptosystems, but they have not yet been triumphant in utilizing the full power of biometrics [13].

In spite of offering usability advantages and non-repudiation over traditional token and password based authentication schemes, biometrics, itself, raises privacy and security concerns. One of the concerns with biometrics is that only a limited number of biometrics can be obtained from a person and their compromise would signify that the particular biometric is made useless forever. As, the biometrics are eternally associated with a user and cannot be replaced, the compromise of the biometric implies that it cannot be revoked or replaced as we do with credit cards and passwords [16]. The above stated problem could well be overcome by employing the concept of “cancelable biometrics”. In cancelable biometrics, the biometric feature is deformed in a repeatable but irreversible manner prior to template generation. When a cancelable template is compromised, its distortion characteristics are modified, and the same biometrics is mapped to a fresh template, which is utilized for future purposes [12, 15]. Cancelable biometrics also provides a higher level of privacy by allowing multiple templates for the same biometric data [14]. A good cancelable biometric template should possess the following characteristics namely, 1) Diversity, 2) Reusability, 3) Non-invertibility and 4) Performance [12]. In recent times, cancelable biometric systems are gaining in popularity for providing user authentication for applications where the privacy and security of biometric templates are important considerations.

The proposed research is an enhanced version of our earlier research [35] on cryptographic key generation from fingerprint biometrics; here, we propose an efficient approach for the generation of an irrevocable cryptographic key using a cancelable template from fingerprint biometrics. The proposed approach takes as input a fingerprint and extracts the minutiae points from the preprocessed fingerprint image. Subsequently, a cancelable template is generated from the extracted minutiae points with the help of the one-way transformation function. Ultimately, a cryptographic key is generated based on the cancelable template constructed. The cryptographic key thus generated will be irrevocable and also will provide increased protection in cryptography based security systems. The effectiveness of the proposed approach is depicted by the experimental results obtained as a result of testing with different fingerprint images.

The organization of the paper is as follows: A brief review of the recent researches related to the proposed approach is given in Section 2. The proposed methodology and its steps are detailed in Section 3. The experimental results are given in Section 4 and conclusions are summed up in Section 5.

2. REVIEW OF RELATED RESEARCHES

Our research work has been motivated by a number of earlier researches existing in the literature concerning cancelable biometrics and cryptographic key generation. A brief explanation of some noteworthy contributions is mentioned below:

Ratha, N.K et al. [17] have established numerous methods to generate multiple cancelable identifiers from fingerprint images. A user can be provided with as many biometric identifiers as per the need by giving out a new transformation “key”. The identifiers can be eliminated and returned when a trade-off is obtained. The performance of numerous algorithms namely Cartesian, polar, and surface folding transformations of the minutiae positions were compared empirically. The transforms were noninvertible and it was shown that the original biometric identifier was difficult to recover from a transformed version by means of random guessing. From the empirical results and theoretical analysis, it was established that feature-level cancelable biometric construction can be applied in large biometric deployments.

Biometric-key generation can be defined as a procedure that is used to transform a portion of live biometric data into key with the help of auxiliary information (biometric helper). To generate a biometric-key continually was

made possible and to store the biometric physically was not essential. Beng, A. et al. [18] proposed a biometric-key generation system that worked based on a randomized biometric helper. A randomized feature discretization process and a code redundancy construction were the part of the scheme. The discretization process allows managing of intra-class variations of biometric data to the minimal level and the code redundancy construction brings down the errors. The randomized biometric helper ensures that a biometric-key was easy to be made void when the key was acknowledged.

Sanaul Hoque et al. [19] exemplified the production of biometric keys straight from live biometrics as per the conditions, by categorizing feature space into subspaces and again categorizing these into cells, where each cell subspace adds to the overall key generated. They evaluated the scheme on real biometric data, by symbolizing real samples as well as its limitations. Experimental results showed the level to which the technique could be implemented reliably in likely practical conditions.

Andrew B. J. Teoh et al. [20] proposed the notion of cancelable biometrics to state biometric templates which can be eliminated and re-established by appending another independent authentication factor. BioHash is a type of cancelable biometrics that combines a set of user-specific random vectors along with biometric features. The quantized random projection collection is based on the Johnson-Lindenstrauss Lemma and it was used to achieve the mathematical foundation of BioHash. On the basis of this model, they have described the characteristics of BioHash in pattern recognition besides security perspective and have offered few methods to solve the stolen-token issue.

Cancelable biometrics was proposed by A.T. Beng Jin and Tee Conniea [21] and they detailed about biometric templates that can be canceled and restored. BioHash is a cancelable biometric that combines a set of user-specific random vectors with biometric features. The major drawback of BioHash was its drop in the performance when the legitimate token is removed and employed by the pretender to be declared as the legitimate user. A probabilistic neural network was employed as a classifier to address the abovementioned issue.

Huijuan Yang et al. [22] have presented a non-invertible transform to perpendicularly project the distances between a pair of minutiae to a circle and to generate the characteristics. Additional local features like relative angles between the minutiae pair, and global features like orientation, ridge frequency and total number of minutiae of the randomly sampled blocks around each minutia were also employed to obtain better performance. Finally, the Bin-based Quantization (BQ) generates the cancelable templates. The feature extraction and cancelable template generation are controlled by a secret key to ensure revocability and security. Experimental results on FVC 2002 data set showed that the proposed scheme provides better performance.

A technique to generate an irrevocable cryptographic key from the biometric template of the palm vein was proposed by B. Prasanalakshmi and A. Kannammal [23]. 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 cancelable templates which consecutively are employed for irrevocable key generation.

H. A. Garcia-Baleon et al. [24] proposed an approach for cryptographic key generation which is on the basis of keystroke dynamics and the k-medoids algorithm. Training-enrollment and user verification are the stages in the aforementioned approach. The approach checks the identity of individuals off-line by not using a centralized database. From the simulation results, a false acceptance rate (FAR) of 5.26% and a false rejection rate (FRR) of 10% were obtained. The cryptographic key obtained from the approach may be applied in diverse encryption algorithms.

Chang Yao-Jen et al. [25] have presented a framework with the intention of generating a fixed cryptographic key from the biometric data which is liable to change. In comparison with the proposed framework and the earlier works, the user-dependent transforms are employed to generate more solid and noticeable features. Hence, to generate a prolonged and much stable bit stream is made possible. To exemplify the practicability of the framework, experiments were conducted on a face database.

B. Chen et al. [26] have presented a technique that uses the entropy oriented feature extraction procedure and Reed-Solomon error correcting codes that are able to generate deterministic bit-sequences from the output of an iterative one-way transform. The assessment of the methodology was done with the 3D face data. The

methodology was also established to be competent of generating keys of proper length for 128-bit Advanced Encryption Standard (AES) in a dependable way.

3. AN EFFECTUAL APPROACH FOR CRYPTOGRAPHIC KEY GENERATION USING CANCELABLE BIOMETRICS

In modern times, crypto-biometric systems have been proposed as an effective solution to the problems of cryptographic key management and biometric template protection. The only limiting factor with biometrics is that once a biometric feature is compromised, it is hard to be replaced or substituted. In the proposed research, we devise an efficient approach for irrevocable cryptographic key generation using a secured cancelable template obtained from fingerprint biometrics. The various steps and techniques used in the proposed approach are detailed in this in this section. The approach comprises of three phases namely.

- Extraction of minutiae points from Fingerprint
- Secured Cancelable template generation
- Key generation from Secured Cancelable template

3.1 Extraction of minutiae points from Fingerprint

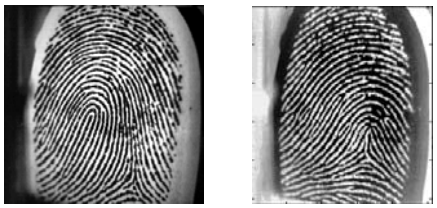
In the proposed approach, the process of extracting the minutiae points from the fingerprint is composed of three processing steps namely,

- Preprocessing
- Region of Interest (ROI) selection
- Minutiae extraction

Histogram Equalization [28] and Wiener Filters [31] have been made use to achieve image enhancement in fingerprint images. Subsequently, the locally adaptive threshold method [29] is applied to perform binarization on the fingerprint image. Morphological operations [29], [30] are then utilized to extract the Region of Interest [ROI] from the fingerprint image. Eventually, minutiae points are extracted using the Ridge Thinning algorithm [27].

3.1.1 Preprocessing

i) Histogram equalization: The method of histogram equalization typically increases the local contrast of images, particularly when the relevant data of the image is represented by close contrast values. The intensities on the histogram can be better distributed through proper adjustments. Moreover, histogram equalization increases the perceptional information of the image by permitting the pixel values to expand the distribution of an image. The original histogram of a fingerprint image will be of bimodal type, and the histogram after the equalization converts all the range values from 0 to 255 and the visualization effect is improved. Here, the Figure 1 depicts the original fingerprint image and its corresponding histogram equalized image.



(a) (b)

Figure 1: (a) Original Fingerprint image (b) Histogram Equalized image

ii) Wiener Filtering: Wiener filter can be defined as a Mean Squared Error (MSE)-optimal stationary linear filter for images degraded by additive noise and blurring. In order to perform wiener filtering, [32] we assume that the signal and noise processes are second-order stationary (in the random process sense). Generally, the wiener filters are made use of in the frequency domain. When the stationary nature of the concerned signals is presumed, the average squared distance between the filter output as well as a desired signal is lessened by means of computing the coefficients of a wiener filter [31]. This can be accomplished with ease in the frequency domain.

$$\hat{S}(f) = W(f)Y(f)$$

where $\hat{S}(f)$ is the wiener filter output, $Y(f)$ is the wiener filter input, $W(f)$ is coefficient of wiener filter and $W(f) = (P_{DY}(f)/P_{YY}(f))$, $P_{YY}(f)$, $P_{DY}(f)$ are the power spectrum of $Y(f)$ and the cross power spectrum of $Y(f)$, $D(f)$ (desired signal) respectively.

3.1.2. Region of Interest (ROI) Selection

i) Binarization: Almost all the minutiae extraction algorithms function on binary images. In binary fingerprint images there are only two levels of interest: the black pixels that indicate ridges, and the white pixels that indicate valleys. Translation of a grey level image into a binary image is done by a process called binarization. Binarization improves the contrast between the ridges and valleys in a fingerprint image for effectual extraction of minutiae points.

ii) Adaptive Thresholding: The adaptive thresholding method [33] is on the basis of the analysis of statistical parameters. This includes arithmetic mean, geometrical mean and standard deviation of the sub-band coefficients. Local adaptive thresholding scheme has been the most commonly used, by researchers due to the fact that it binarizes and improves the poor quality of the images for locating the meaningful textual information [34].

iii) ROI extraction by morphological operations: For ROI extraction from the binary fingerprint image, we apply the morphological opening and closing operations using a structuring element. The morphological operators will throw away the leftmost, rightmost, uppermost and bottommost blocks out of the bound, so as to get the tightly bounded region just containing the bound and inner area.

3.1.3. Minutiae extraction

Finally, the minutiae points are extracted from the preprocessed fingerprint image using Thinning. Thinning is defined as a morphological operation in which the foreground pixels are eroded in succession till they are one pixel wide. The Ridge Thinning algorithm [27] is made use of in the proposed approach for Minutiae points' extraction. It extracts minutiae points by getting rid of the redundant pixels of ridges until the ridges become just one pixel wide. The steps followed in the Ridge Thinning algorithm are: first, the image is segmented as in a checkerboard pattern into two different subfields. In the first sub-iteration, only if the conditions G1, G2, and G3 are satisfied, pixel 'p' is deleted from the first subfield. In the second sub-iteration, only if the conditions G1, G2, and G3' are satisfied, pixel 'p' is deleted from the second subfield. The two subiterations together make up one iteration of the thinning algorithm.

Condition G1:

$$X_H(P) = 1$$

Where

$$X_H(P) = \sum_{i=1}^{4} b_i$$

$$b_i = \begin{Bmatrix} 1 \text{ if } x_{2i-1} = 0 \text{ and } (x_{2i} = 1 \text{ or } x_{2i+1} = 1) \\ 0 \quad \text{otherwise} \end{Bmatrix}$$

$x_1, x_2, ..., x_8$ are the values of the eight neighbors of p, starting with the east neighbor and numbered in counter-clockwise order

.

Condition G2:

$$2 \le \min\{n_1(p), n_2(p)\} \le 3$$

where

$$n_1(p) = \sum_{k=1}^{4} x_{2k-1} \vee x_{2k}$$

$$n_2(p) = \sum_{k=1}^{4} x_{2k} \vee x_{2k+1}$$

Condition G3:

$$(x_2 \vee x_3 \vee \bar{x}_8) \wedge x_1 = 0$$

Condition G3':

$$(x_6 \vee x_7 \vee \bar{x}) \wedge x_5 = 0$$

3.2 Secured Cancelable Template Generation

In this sub-section, we have presented the steps involved in the generation of the secured cancelable template from the extracted minutiae points. The steps involved are as follows:

The extracted minutiae points P and their corresponding x, y co-ordinates M_p are represented as

$$P = [P_1 \;\; P_2 \;\; P_3 \;\; \ldots \;\; P_n]$$

$$M_p = [x_1 \;\; y_1 \;\; x_2 \;\; y_2 \;\; \ldots \;\; x_n \;\; y_n]$$

Subsequently, a set R_N is created with random values of size $|M_p|$.

$$R_N = [r_1 \;\; r_2 \;\; r_3 \;\; \ldots \;\; r_n]; where \;\; \mathrm{n} = |\mathrm{M_p}|, \mathrm{r_i} = random(); \; 1 \le i \le n$$

Then, exponential values are computed for each individual element in the vector R_N and stored in ER_N.

$$ER_N = [e^{r_1}, e^{r_2}, \cdots, e^{r_n}]$$

For every element in ER_N, choose a set of '*x*' subsequent prime numbers to form a row of the matrix P_N. Every row of the matrix P_N will have distinct number of elements. The number of elements '*x*' will be equal to the coordinate value of the elements in M_p.

$$P_N = \begin{Bmatrix} (P_1 & P_2 & P_3 & \cdots & P_{n=x_1}) \\ (P_1 & P_2 & P_3 & \cdots & P_{n=y_1}) \\ \vdots & & & & \\ (P_1 & P_2 & P_3 & \cdots & P_{n=x_n}) \\ (P_1 & P_2 & P_3 & \cdots & P_{n=y_n}) \end{Bmatrix}$$

Subsequently, a prime number pair is selected randomly from the two succeeding rows of P_N, such that a prime number from each row, and is multiplied to obtain the transformed point TP. The transformed points are stored in a vector PF_V.

$$PF_V = [TP_1 \;\; TP_2 \;\; TP_3 \;\; \cdots \;\; TP_{n/2}] \;\; ; where \;\; TP_i = (P_l * P_m)$$

Since each transformed point TP is formed by the multiplication of two prime numbers P_l and P_m, it is almost computationally infeasible to determine the factors P_l and P_m from TP, as described in RSA factoring challenge [5].

The size of the cryptographic key FK_v to be generated is decided previously and is set as a pre-defined key value k_v. From the vector PF_V, a transformed point TP is chosen randomly and its distance with respect to all other transformed points is computed and stored in a vector D_V. The above process is repeated until $|D_V| = k_v$. The distance between any two transformed points is computed using the following equation,

$$Distance \;\; (TP_i, TP_j) = \sqrt{(TP_i - TP_j)^2}$$

$$D_V = [d_1 \;\; d_2 \;\; d_3 \ldots d_{k_v}]$$

The vector D_V is then transformed into a matrix to form the cancelable template T_M.

$$T_M = | D_{V\,ij} |_{\sqrt{kv} \times \sqrt{kv}}$$

Henceforth, the cancelable template, eventhough irrevocable, serves as the source for the generation of the cryptographic key. This necessitates the secure storage of the cancelable template such that it is either unmodifiable or unaccessible to the people other than authorized users. Hence, the resultant cancelable template T_M is encrypted with the AES algorithm to form the encrypted cancelable template.

$$CT_M = Enc[T_M]$$

The generated cancelable template T_M is irreversible; also, the security of the cancelable template created is increased by the strength of AES.

3.3 Cryptographic Key Generation from Secured Cancelable Template

The steps involved in the generation of the cryptographic key from the secured cancelable template are as follows: Initially, the encrypted cancelable template is decrypted with the AES Decryption algorithm to obtain the cancelable template T_M.

$$T_M = Dec(CT_M)$$

An intermediate key vector I_k is then generated from T_M, by employing matrix operation (Computing determinants of 4x4 matrices). Subsequently, a threshold is determined by computing the mean value of I_k.

$$I_k = (v_i : P(v)), \qquad i = 1, \cdots, n$$

Where $P(v) = \left| T_{ij} \right|_{4X4}; i, j : i + size, j + size; -1 < i, j < \sqrt{n}$

Based on the values in I_k and the threshold, the individual values of the final key vector FK_v are computed. The vector FK_v is created using the following equation,

$$FK_v = \begin{cases} 1 & ;\ if\ \ I_{k(i)} > mean(I_k) \\ 0 & ;\ else \end{cases}$$

The final key FK_v generated is also irrevocable and complex consisting of 256 bits. The irreversible property makes the key almost unbreakable, because it is very intricate to compute the cancelable template from the final cryptographic key FK_v generated.

5. EXPERIMENTAL RESULTS

This section presents the experimental evaluation of the proposed approach. The proposed approach is programmed in Matlab (Matlab7.4). The proposed approach was tested with different fingerprint images obtained from publicized databases. Initially, minutiae points are extracted (after Preprocessing and ROI selection) from the input fingerprint images, followed by the irrevocable cancelable template generation. Eventually, a 256-bit irreversible and strong cryptographic key is generated from the cancelable template. The experimental results (including the input image, the intermediate results and the final cryptographic key) obtained for three different fingerprint images are depicted in Figure 2.

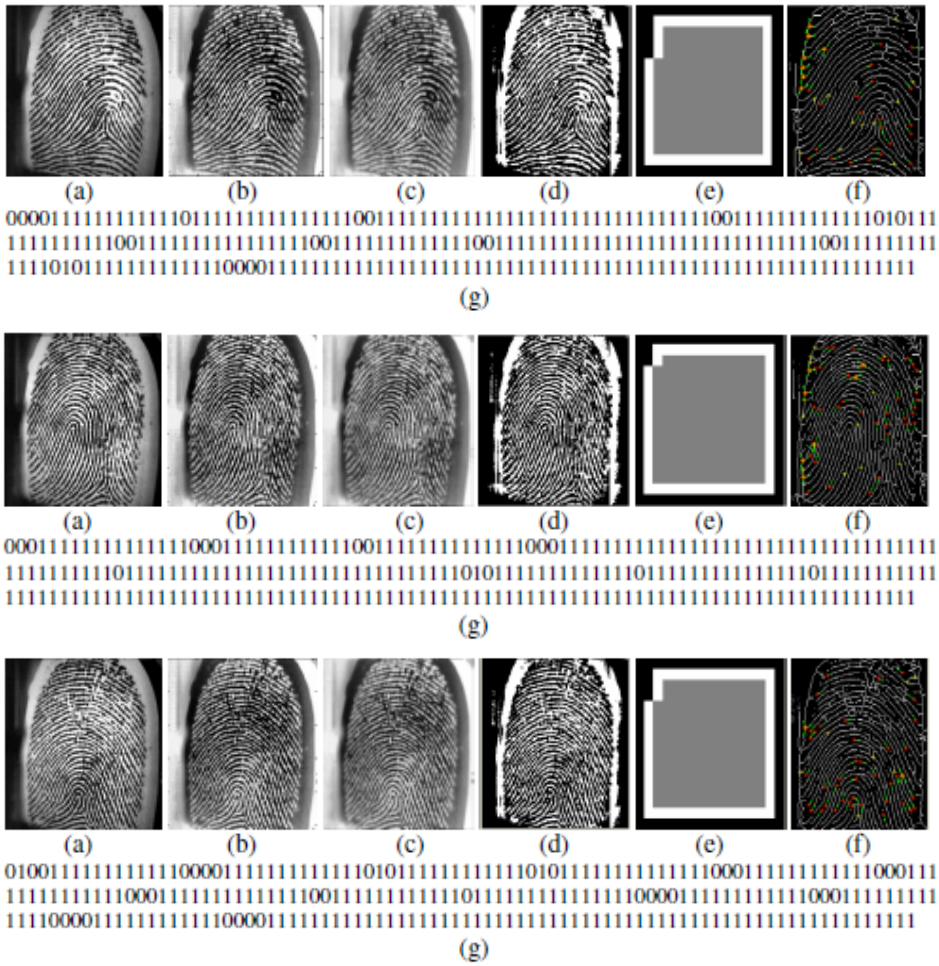


Figure 2 : (a) Input Fingerprint Image (b) Histogram equalized image (c) Wiener Filtered Image (d) Binarized Image (e) Region of Interest (ROI) (f) Fingerprint Image with minutiae points (g) Generated 256-bit key.

6. CONCLUSION

Biometrics-based Key Generation has been found to outperform traditional cryptographic systems, chiefly because, it is impossible for a person to lose his/ her biometrics, and also the biometrics are intricate to falsify or steal. In this paper, we have presented an efficient approach for generation of irrevocable cryptographic keys from fingerprint biometrics using cancelable biometric templates. The approach has been composed of three phases namely: 1) Minutiae points' extraction from the fingerprint image, 2) cancelable template generation with added security and 3) Cryptographic key generation from Secured Cancelable template. The resultant cryptographic key thus generated has been irrevocable and unique to a specific cancelable template, availing better protection and replacement features for lost or stolen biometrics. The experimental results have portrayed the effectiveness of the proposed approach in generating an irrevocable cryptographic key.

REFERENCES

[1] John Chirillo and Scott Blaul, "Implementing Biometric Security," Wiley Red Books, ISBN: 978-0764525025, April 2003.
[2] Anil K. Jain, Arun Ross, Salil Prabhakar, "An Introduction to Biometric Recognition", IEEE Transactions On Circuits And Systems For Video Technology, Vol. 14, No. 1, 2004.
[3] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," In Proceedings of the 6th ACM Conference on Computer and Communication Security, pages 28–36, November 1999.
[4] F. Monrose, M. K. Reiter, and S. Wetzel. "Password hardening based on keystroke dynamics", In Proceedings of the 6th ACM Conference on Computer and Communications Security, pages 73–82, November 1999.
[5] "RSA Factoring Challenge" from http://en.wikipedia.org/wiki/RSA Factoring _Challenge.
[6] F. Hao, C.W. Chan, "Private Key generation from on-line handwritten signatures," Information Management & Computer Security, Issue 10, No. 2, pp. 159–164, 2002.
[7] A. Goh, D.C.L. Ngo, "Computation of cryptographic keys from face biometrics," International Federation for Information Processing 2003, Springer-Verlag, LNCS 2828, pp. 1–13, 2003.

[8] Advanced encryption standard (AES), Federal information processing standards publication 197, National Institute of Standards and Technology. (2001).
[9] W. Stallings, Cryptography and Network Security: Principles and Practices, 3rd ed. Upper Saddle River, NJ: Prentice-Hall, 2003.
[10] D. V. Klein, “Foiling the cracker: a survey of, and improvements to, password security,” in Proc. 2nd USENIX Workshop Security, pp. 5–14,1990.
[11] U. Uludag, S. Pankanti, P. S., and A. Jain, “Biometric cryptosystems: Issues and challenges,” Proceedings of the IEEE 92, pp. 948–960, June 2004.
[12] Andrew Beng Jin Teoh, Kar-Ann Toh and Wai Kuan Yip,”2^N Discretisation of BioPhasor in Cancelable Biometrics”, Advances in Biometrics, Springer Berlin / Heidelberg, Vol. 4642, 2007.
[13] Nagar, A. and Chaudhury, S, "Biometrics based Asymmetric Cryptosystem Design Using Modified Fuzzy Vault Scheme," 18th International Conference on Pattern Recognition, Vol. 4, pp: 537-540, 2006.
[14] Russell Ang, Reihaneh Safavi-Naini, Luke McAven: “Cancelable Key-Based Fingerprint Templates.”, Australasian conference on information security and privacy, vol. 3574, pp. 242-252, 2005.
[15] Y C Feng.. Pong C Yuen. and Anil K Jain., “A Hybrid Approach for Face Template Protection,” , In Proc. of SPIE Conference of Biometric Technology for Human Identification , Vol. 6944, 2008.
[16] Nalini Ratha, Jonathan Connell, Ruud M. Bolle, Sharat Chikkerur, "Cancelable Biometrics: A Case Study in Fingerprints", International Conference on Pattern Recognition, Vol. 4, pp. 370-373, 2006.
[17] 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.
[18] Beng, A., Jin Teoh, Kar-Ann Toh, "Secure biometric-key generation with biometric helper”, 3rd IEEE Conference on Industrial Electronics and Applications, pp: 2145-2150, 2008.
[19] Sanaul Hoque, Michael Fairhurst, Gareth Howells "Evaluating Biometric Encryption Key Generation Using Handwritten Signatures", Bio-inspired, Learning and Intelligent Systems for Security, pp: 17-22, 2008.
[20] Andrew B. J. Teoh, Yip Wai Kuan, Sangyoun Lee," Cancelable biometrics and annotations on BioHash ", Pattern Recognition, Vol: 41, No:6, pp: 2034-2044, 2008.
[21] Andrew Teoh Beng Jin, Tee Conniea, "Remarks on Bio-Hashing based cancelable biometrics in verification system", Neurocomputing, Vol: 69, No: 16-18, pp:2461-2464, 2006.
[22] Huijuan Yang, Xudong Jiang, Alex C. Kot, "Generating secure cancelable fingerprint templates using local and global features", 2nd IEEE International Conference on Computer Science and Information Technology, 2009.
[23] B. Prasanalakshmi ,A. Kannammal, "A secure cryptosystem from palm vein biometrics", ACM International Conference Proceeding Series; Seoul, Korea , Vol. 403 , pp: 1401-1405, 2009.
[24] 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: Progress in Pattern Recognition, Image Analysis, Computer Vision, and Applications, Vol. 5856, pp: 85 - 94, 2009.
[25] Chang Yao-Jen, Wende Zhang, Chen Tsuhan, "Biometrics-based cryptographic key generation", IEEE International Conference on Multimedia and Expo, Vol: 3, pp: 2203- 2206, 2004.
[26] B. Chen, V. Chandran, "Biometric Based Cryptographic Key Generation from Faces", Proceedings of the 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp: 394-401, 2007.
[27] Lam, L., Seong-Whan Lee, and Ching Y. Suen, "Thinning Methodologies-A Comprehensive Survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol 14, No. 9, pp: 869-885, September 1992.
[28] Joseph W. Goodman, Brian A. Wandell, “Image Systems Engineering Program, Stanford University”, International Conference on Image Processing (ICIP), Vol: 1, pp: 435-438, 1996.
[29] C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui., “Intelligent biometric techniques in fingerprint and face recognition”, The Crc International Series on Computational Intelligence, CRC Press, 1999.
[30] D.Maio and D. Maltoni. “Direct gray-scale minutiae detection in fingerprints”, IEEE Trans. Pattern Anal. And Machine Intell., Vol: 19, No:1, pp: 27-40, 1997.
[31] Amir Hussain, Stefano Squartini, and Francesco Piazza, "Novel Sub-band Adaptive systems incorporating Wiener filtering for Binaural Speech Enhancement", A ISCA tutorial research workshop on Non-Linear Speech processing, NOLISP, Barcelona, April 19-22, 2005.
[32] Saeed V. Vaseghi, "Advanced signal processing and digital noise reduction (Paperback)", John Wiley & Sons Inc, pp: 416, July 1996.
[33] D.Gnanadurai, and V.Sadasivam, An Efficient Adaptive Thresholding Technique for Wavelet Based Image Denoising, International Journal of Signal Processing, vol: 2, No: 2, 2005.
[34] Yahia S. Halabi, Zaid SA”SA, Faris Hamdan, Khaled Haj Yousef, "Modeling Adaptive Degraded Document Image Binarization and Optical Character System", European Journal of Scientific Research, Vol. 28, No.1, pp.14-32, 2009.
[35] Sunil V. K. Gaddam and Manohar Lal, "Efficient Cancelable Biometric Key Generation Scheme for Cryptography", International Journal of Network Security, Vol: 10, No: 3, pp: 223-231, 2010 [Accepted for publication].