Efficient Cancellable Biometric Key Generation Scheme for Cryptography

Sunil V. K. Gaddam [1] and Manohar Lal [2]
(Corresponding author: Sunil V. K. Gaddam)
Department of CSE, Meerut Institute of Engineering & Technology, Meerut, U. P., India[1]
School of Computer and Information Sciences, IGNOU, New Delhi, India[2]
(Email: sunilvkg@yahoo.com)
(Received June 24, 2008; revised and accepted Feb. 12, 2009)

Abstract

This paper puts forth a fresh methodology for the secure storage of fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of cancellable biometric features. Conventional techniques depend on biometric features like face, fingerprint, hand geometry, iris, signature, keystroke, voice and the like for the extraction of key information. If a Biometric Key is missing or stolen, it is lost perpetually and possibly for every application where the biometric is utilized, since a biometric is permanently linked with a user and cannot be altered. In this paper we propose a technique to produce cancellable key from fingerprint so as to surmount these problems. The flexibility and dependability of cryptography is enhanced with the utilization of cancellable biometric features. There are several biometric systems in existence that deal with cryptography, but the proposed cancellable biometric system introduces a novel method to generate Cryptographic Key. We have as well discussed about the Security analysis of the projected Cancellable Biometric System.

Keywords: Biometrics, cancellable biometrics, cryptography, fingerprint, key generation, minutiae points, security analysis

1 Introduction

Progress of communication technologies in contemporary times has resulted in huge quantities of digital data in the publicly shared media. This has necessitated the drastic development of cryptographic techniques. Cryptography is considered to be one of the fundamental building blocks of computer security. Data can be encoded with the aid of cryptographic techniques in order to ensure that it appears unintelligible to the public or third party and coherent only to the intended receivers of it (Data Confidentiality). DES, AES [1, 2, 4] and public key architectures such as RSA [17] is a notable few among the widely utilized cryptographic techniques.

Regrettably cryptographic security is conditioned by an authentication step that characteristically depends on long pseudo-random keys (of at least 128 bits in symmetric encryption), which are nearly impossible to keep in mind. The inability of human users to remember powerful cryptographic keys has been a feature restraining the security of systems for decades. Numerous historical instances illustrate that a person is capable of remembering only tiny passwords or keys, and even then have a tendency to aspire for passwords or keys that are easily deduced by dictionary attacks (e.g., see [8, 15, 18, 19, 23]) or obtained using social engineering methods.

Typically we write down and store keys in an insecure place that can possibly be communal among users, and thus is not capable of ensuring non-repudiation. Moreover many people are intended towards using identical keys or password for a variety of applications and as a result breaching one system lead to the breaching of many others. This makes the work of an attacker simple by shockingly reducing the general security of the data being protected. It is possible to solve this in a variety of applications by producing powerful cryptographic keys from biometric data, possibly in combination with the entry of a password [10, 12, 24].

Biometrics provides a person with a distinct characteristic that is always prevalent. It is the technique of authenticating a person's individuality from one or more behavioral or physiological features. Diverse biometric techniques that are under research include fingerprints, facial, palm prints, retinal and iris scans, and hand geometry, signature capture and vocal features.

Cryptography is merged with biometrics in Biometric cryptosystems, otherwise known as crypto-biometric systems [25]. It is possible to carry out the integration of biometrics and cryptography broadly in two distinct steps. In case of biometrics-based key generation, a biometric matching amid an input biometric signal and a registered template is utilized in the release of the secret key. The

biometric signals are immensely bounded to the keys in case of biometrics-based key generation.

A chief issue with regard to biometrics is that resetting is intricate. The uniformity of biometric data over time is one of its huge merit and demerit at the same instant. In case of a missing credit card, it is possible to issue a new one but it is impossible to substitute the biometric characteristics and it is fully evident since it is not feasible to provide a person with a fresh fingerprint when the old one is stolen.

We have introduced the concept of "cancellable biometrics" [3] so as to simplify the problem. The procedure ensures the planned, repeatable distortion of a biometric signal on basis of a predefined transform. The distortion of biometric signal recurs in the same method at every presentation, for enrollment and for every key generation. This approach facilitates the every incidence of enrollment to utilize a distinct transform thus making expose cross matching unachievable. Furthermore, once a variant of the transformed biometric data is compromised it is enough to merely change the transform operation to produce a new variant for re-enrollment, in effect, a new person. Generally, the transforms utilized for distortion are chosen to be non-invertible. Thus it is not possible to recover the original (undistorted) biometrics despite knowing the transform method and the resulting transformed biometric data.

The organization of the paper is as follows: A brief review of the researches related to our proposed approach is given in Section 2. The proposed methodologies and the steps are detailed in Section 3. In Section 4, the security analysis of the proposed algorithm is presented. The experimental analysis and the results are given in Section 5 and conclusions are summed up in Section 6.

2 Related Works

Our work is inspired from a number of previous works related to cancellable biometrics and the generation of cryptographic key from cancellable biometric features. A brief review of some of the works is given below.

Cancellable biometrics proffers a greater level of privacy by facilitating more that one template for the same biometric data and thus the non-linkability of user's data stored in diverse databases. The measurement of the success of a particular transformation and matching algorithm for fingerprints was described by Ang et al. [3]. A key dependant geometric transform was employed on the features obtained from a fingerprint, so as to produce a key-dependent cancellable template for the fingerprint. Besides, they have also studied the performance of an authentication system that utilizes the cancellable fingerprint matching algorithm detection purposes. Experimental evaluation of the system was carried out and the results illustrated that it was possible to bring about a good performance when the matching algorithm remains unaltered.

Hao et al. [12] presented a realistic and secure way to incorporate the iris biometric into cryptographic applications. They deliberated on the error patterns within iris codes and developed a two-layer error correction technique that merges Hadamard and Reed-Solomon codes. The key was produced from the iris image of the subject through the auxiliary error correction data that do not disclose the key and can be saved in a tamper-resistant token like a smart card. The evaluation of the methodology was performed with the aid of samples from 70 different eyes, 10 samples being obtained from every eye. It was established that an error-free key can be reproduced reliably from genuine iris codes with a success rate of 99.5 percent. It is possible to produce up to 140 bits of biometric key, more than adequate for 128-bit AES.

The application of handwritten signature to cryptography was analyzed by Freire-Santos et al. [10] on basis of recent works displaying the likelihood of key generation by means of biometrics. A cryptographic construction called the fuzzy vault was employed in the signature-based key generation scheme. The analysis and evaluation of the usability of distinctive signature features appropriate for the fuzzy vault was carried out. Results of experimental evaluation were reported. The reports also included the error rates to release the secret data with the aid of both random and skilled forgeries from the MCYT database.

An on-line signature-based biometric authentication system, where non invertible transformations were applied to the acquired signature functions ruling out the possibility to derive the original biometrics from the stored templates at the same time maintaining the same recognition performances of an unprotected system was projected by Maiorana et al. [21]. Precisely the probability of producing cancellable templates from the same original data, thereby proffering an appropriate solution to privacy concerns and security problems was intensely explored.

Teoh et al. [22] have presented a two-factor cancellable formulation that facilitates data distortion in a revocable yet non-reversible manner by first converting the raw biometric data into a fixed-length feature vector followed by the projection of the feature vector onto a sequence of random subspaces that were obtained from a user-specific Pseudorandom Number (PRN). The process was revocable making the replacement of biometrics seem as easy as replacing PRNs. This formulation was confirmed under numerous scenarios (normal, stolen PRN, and compromised biometrics scenarios) with the aid of 2400 Facial Recognition Technology face images.

A cancellable biometric approach called PalmHashing was projected by Tee et al. [7] in order to address the non-revocable biometric issue. This technique hashes palmprint templates with a set of pseudo-random keys to acquire a unique code known as the palmhash. It is possible to store the palmhash code in portable devices such tokens and smartcards for authentication. Moreover, PalmHashing also provides numerous advantages over other modern day approaches including clear separation of the genuine-

imposter populations and zero EER occurrences. They outlined the implementation facts besides emphasizing its capabilities in security-critical applications.

A fuzzy commitment method working on lattice mapping for cryptographic key generation from biometric data was proposed by Zheng et al. [27]. Despite providing high entropy keys as output the method as well obscures the original biometric data such that it becomes unfeasible to recover the biometric data besides the stored information in the system being open to an attacker. Results of simulation illustrated that the method's authentication accuracy was analogous to that of the renowned.

Jo et al. [14] presented a simple technique for the generation of digital signatures and cryptography communication with the aid of biometrics. It has been termed necessary to generate the signature in such a way that it becomes possible to verify the same with a cryptographic algorithm in existence like the RSA/ElGamal without altering its own security constraint and infrastructure. It was anticipated that the mechanism will be capable of guaranteeing security on the binding of biometric information in the signature scheme on telecommunication environments.

A framework for stable cryptographic key generation from unstable biometric data was projected by Chang et al. [5]. The chief difference between the proposed framework and the prior work is that here, user-dependent transforms are employed to produce more compact and distinguishable features. Thus a longer and highly stable bit stream can probably be produced. Experiments were carried out on one face database to demonstrate the practicability of the framework.

Chen et al. [6] have presented a technique that makes use of entropy oriented feature extraction procedure together with Reed-Solomon error correcting codes that are capable of generating deterministic bit-sequences from the output of an iterative one-way transform. The evaluation of the methodology was done with the 3D face data and was illustrated to be capable of producing keys of suitable length for 128-bit Advanced Encryption Standard (AES) in a reliable fashion.

3 Proposed Methodology

Recently, crypto-biometric systems have been studied for solving the key management problem of cryptographic systems and protecting templates in biometric systems at the same time. In general, the identity theft problem is drastically exacerbated for the biometric systems, since the biometric data and the corresponding feature vectors are non-renewable. To overcome this we generate a secured feature matrix from the fingerprint template and strengthened this by AES Encryption/Decryption algorithm. Besides that, this paper discusses how keys can be generated and demonstrates the technique using fingerprint images.

3.1 Key Generation from Fingerprint

This section confers the feature generation from fingerprint biometric data. The stages are discussed below

- Extracting minutiae points from Fingerprint;
- Secured Feature Matrix generation;
- Key generation from Secured Feature Matrix.

3.1.1 Extracting Minutiae Points from Fingerprint

For extracting minutiae points from fingerprint, a three-level approach is broadly used by researchers. These levels are listed as follows

- Preprocessing.
- ROI selection Separation.
- Minutia extraction.

For the fingerprint image preprocessing, Histogram Equalization [26] and Filters [11] are used to do image enhancement. Binarization is applied on the fingerprint image. Locally adaptive threshold method [13] is used for this process. Then Morphological operations [13, 20] are used to extract Region of Interest [ROI]. In a morphological operation, the value of each pixel in the output image is based on a comparison of the equivalent pixel in the input image with its neighbors. By selecting the size and shape of the neighborhood, we can construct a morphological operation that is sensitive to specific shapes in the input image.

1) **Preprocessing**
Histogram Equalization. This method usually increases the local contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram.

Perceptional information of the image is increased through histogram equalization which permits pixel value to expand the distribution of an image. The original histogram of a fingerprint image has the bimodal type, the histogram after the histogram equalization converts all the range from 0 to 255 and the visualization effect is improved.

Gabor Filters. The Gabor filter is applied to the fingerprint image obtained by the previous step by spatially convolving the image with the filter.

A two-dimensional Gabor [11] filter consists of a sinusoidal plane wave of a specific orientation and frequency, modulated by a Gaussian envelope. Gabor filters are employed as they have frequency-selective and orientation-selective properties. These properties permit the filter to be tuned to give maximal

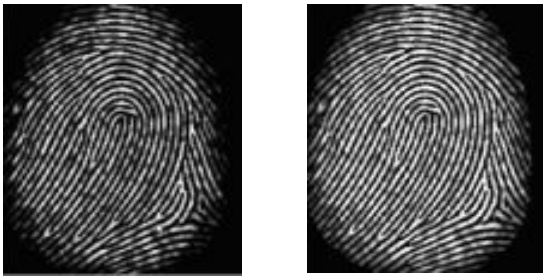

Figure 1: Captured fingerprint and after histogram equalization

Figure 2: After binarization

response to ridges at a specific orientation and frequency in the fingerprint image. So, a properly tuned Gabor filter shall be used to effectively retain the ridge structures while reducing noise. The even-symmetric Gabor filter is the real part of the Gabor function, which is yielded by a cosine wave modulated by a Gaussian.

A Gaussian function multiplied by a harmonic function defines the impulse response of the linear filter, the Gabor filter. Because of the multiplication-convolution property (Convolution theorem), the Fourier transform of a Gabor filter's impulse response is the convolution of the Fourier transform of the harmonic function and the Fourier transform of the Gaussian function.

$$g(x, y; \lambda, \theta, \psi, \sigma, \gamma) = exp(-\frac{x'^2 + \gamma^2 y'^2}{2\sigma^2})cos(2\pi\frac{x'}{\lambda} + \psi).$$

Where,

$$x' = xcos\theta + ysin\theta,$$

and

$$y' = -xsin\theta + ycos\theta.$$

In this equation, λ represents the wavelength of the cosine factor, θ represents the orientation of the normal to the parallel stripes of a Gabor function, ψ is the phase offset, and γ is the spatial aspect ratio, and specifies the ellipticity of the support of the Gabor function.

2) **ROI Selection**

Binarization. Nearly all minutiae extraction algorithms function on binary images where there are only two levels of interest: the black pixels that denote ridges, and the white pixels that denote valleys. Binarization is the process that translates a grey level image into a binary image. This enhances the contrast between the ridges and valleys in a fingerprint image, and consequently makes it possible the extraction of minutiae.

One practical property of the Gabor filter is that it has a DC component of zero, which means the resultant filtered image has a mean pixel value of zero. Hence, straightforward binarization of the image can be achieved using a global threshold of zero. The binarization process involves analyzing the grey-level value of each pixel in the enhanced image, and, if the value is greater than the global threshold, then the pixel value is set to a binary value one; otherwise, it is set to zero. The result is a binary image holding two levels of information, the foreground ridges and the background valleys.

ROI Extraction by Morphological Operations. We perform morphological opening on the grayscale or binary image with the structuring element. We also performed morphological closing on the grayscale or binary image resulting in closed image. The structuring element is a single structuring element object, as opposed to an array of objects for both open and close. Then as the result this approach throws away those 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) **Minutiae Extraction**

The last image enhancement step normally performed is thinning. Thinning is a morphological operation that successively erodes away the foreground pixels until they are one pixel wide. Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide [16] uses a Ridge Thinning algorithm, which is used for Minutiae points' extraction in our approach. The image is divided into two distinct subfields in a checkerboard pattern. In the first sub-iteration, delete pixel p from the first subfield if and only if the conditions G1, G2, and G3 are all satisfied. In the second sub-iteration, delete pixel p from the second subfield if and only if the conditions G1, G2, and G3' are all satisfied.

Condition G1:

$$X_H(P) = 1,$$

where

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

$$b_i = \left\{ \begin{array}{l} 1 \text{ if } x_{2i-1} = 0 \text{ and} \\ \qquad (x_2 i = 1 \text{ or } x_{2i+1} = 1) \\ 0 \text{ otherwise} \end{array} \right\}$$

Here, 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:

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

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:

$$(x_2 \vee x_3 \vee \overline{x_8}) \wedge x_1 = 0.$$

Condition G4:

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

The two sub-iterations together make up one iteration of the thinning algorithm.

3.2 Secured Feature Matrix Generation

The steps involved in the generation of Secured Feature Matrix are discussed in this sub-section. We assume that the extracted minutiae point's co-ordinates are maintained in a vector.

- $M_p \longrightarrow$ Minutiae point set.
- $N_p \longrightarrow$ Size of Minutiae point set.
- $V_k \longrightarrow$ Key Vector.
- $L_k \longrightarrow$ Length of the AES key.
- $p \longrightarrow (x, y)$ co-ordinate of a minutiae point.

The Extracted minutiae points are represented as

$$P_m = \{p_i\} = 1, \ldots, N_p.$$

Initially the is transformed to a Key vector as follows

$$V_k = \{x_i : p(x_i)\}\ i = 1, \ldots, L_k,$$

where

$$p(x) = P_m \lfloor P_m[i] mod N_p \rfloor\ i = 1, \ldots, L_k.$$

Then the initial key vector (V_k) is converted into a matrix BK_m of size $\sqrt{(L_k)} \times \sqrt{(L_k)}$.

Then the resultant matrix BK_m is encrypted with the AES algorithm to form Secured Feature matrix SF_m.

$$SF_m = E_{vk}(BK_m).$$

The key used in the AES encryption is the generated key from the whole process. Once after the key is generated, AES encryption progressed to generate a secured feature matrix, but initially encryption process doesn't occur in the key generation from the whole process.

The generated Secured feature matrix is irreversible, moreover it cannot be hacked by an attacker because of the strength of AES and the mathematical operations involved in the generation.

3.2.1 Key Generation from Secured Feature Matrix (SF_m)

The key is generated as follows. The Secured Feature Matrix is decrypted by AES Decryption to form the deciphered matrix.

Then the resultant matrix BK_m is given as

$$BK_m = D_{vk}(SF_m),$$

where

$$BK_m = (a_{ij}\sqrt{(L_k)} \times \sqrt{(L_k)}).$$

Then an intermediate key vector is generated as follows

$$I_v = \{K_i : p(k)\}\ i = 1, \ldots, L_k,$$

where

$$p(k) = |SM_{ij}|, SM_{ij} = BK_m i : i + size, \\ j + size, -1 < i < sqrt(L_k) SM_{ij},$$

is an extracted matrix formed from the key matrix. Then the final key vector is formed as

$$FBK_y = \left\{ \begin{array}{l} 1, \text{ if } l_v[i] > mean(I_v) \\ 0, \text{ otherwise.} \end{array} \right\}$$

The extracted final key vector is more secured and it is non-reversible. That means the final key cannot be traced back from the template. This irreversible property makes the key unbreakable, because we processed through minutiae points and secured feature matrix.

4 Security Analysis

Security of the proposed algorithm is strengthen by these three robust features

- Cancellable Transform;
- Feature Matrix Security Analysis;
- Irreversible Analysis.

4.1 Cancellable Transform

Cancellable transform [9] is used to generate a cancellable template. The core intention of the cancellable transformation is to provide cancellable skill a "non-invertible" transform. Normally, it decreases the discriminative power of the original template. Therefore, the cancellable templates and the secure templates of an individual in different applications will be different. In turn, the cross matching across databases will not be feasible. Moreover, the secure template can be cancelled and reissued by changing the cancellable transform parameters.

4.2 Feature Matrix Security Analysis

In our algorithm security is more strengthened by AES encryption. Once after the template is formed and minutia points are acquired, a feature matrix is generated by following a sequence of steps. This feature matrix is then encrypted using AES. Reinforced by AES, the feasibility of decrypting the ciphered feature matrix is almost negligible. Anticipating a worst-case scenario, that if a hacker succeeds in decrypting the AES encryption with an intend to obtain the feature matrix; the chances of reorganizing the minutia point and the templates are almost nil. Furthermore, there is no possibility of conjecturing the steps we followed to generate the feature matrix and it is absolutely chanceless to restructure the template by any means.

The key thus formed cannot be traced back to the origin i.e. to the template and moreover the key itself cannot be regenerated falsely using the template. This irreversible aspect makes the key armored and reliable and even resistant to brute force attacks. This shatter-proof property emanates from the very essence of preserving the confidentiality of the battery of operations we follow in transforming minutia points to a Feature matrix.

To decrypt the key we generated, the steps we followed to create it have to be performed in the reverse order. First the feature matrix encrypted using AES, have to be deciphered, then the sequence of steps proceed for forming the feature matrix should be executed from bottom-up. These operations will yield the minutia points acquired from the template in the inception.

4.3 Irreversible Analysis

To enunciate the concept further tracing out the matrix using the determinant or reorganizing shuffled data is totally infeasible just like attempting to generate an original document using a hashed bits after hashing function is applied.

The security of our algorithm is strengthened by the inherent irreversible nature, by this tracing the minutiae points from the keys generated is practically impossible. The proposed algorithm is more suitable and specific for data like the ones used for handling minutiae points arrived using the above process.

5 Experimental Results

The experimental analysis of our proposed approach is presented in this section. Our approach is programmed in Matlab (Matlab 7.4). We have tested our proposed approach with different fingerprint images. The minutiae points are extracted from the fingerprint images using the three level approach presented in the paper. Initially, in the preprocessing stage, histogram equalization and Gabor filtering are performed on the fingerprint images to enhance them. Secondly, the binarization is applied on the fingerprint images and then the region of interest is determined. Subsequently minutiae points are extracted. Later, the secured feature matrix is generated based on the co-ordinates of minutiae points. Eventually, the 256-bit key is generated from the secured feature matrix. The input image, extracted minutiae points and the intermediate results of five different fingerprint images are shown in Figure 3. The 256-bit key generated from the five fingerprint images given in Figure 3 are depicted in Figure 4.

6 Conclusion

Biometrics-based Key Generation outperforms traditional systems in usability domain. Precisely it is not possible for a person to lose his/her biometrics, and the biometric signal is intricate to falsify for steal. The proposed cancellable biometric Crypto System is an all-new technique for the authentication that yields the synergistic control of biometrics. The proposed system employs intentional distortion of fingerprint in a repeatable fashion and the fingerprint thus obtained is utilized in the cryptographic key generation. When the old finger print is "stolen" it is possible to obtain a "new" fingerprint just by altering the parameters of the distortion process. Subsequently, enhanced privacy for the user results as his true fingerprint is not utilized anywhere and diverse transformations for distortions can be utilized for a variety of accounts.

A notable enhancement in terms of decrease in the consumed time is attained with the elimination of more steps that are redundant with the mixture of the proposed methodology. Integration of the projected technique with the existing cryptographic methodologies is uncomplicated and as well decreases key-generation and key-release issues in a remarkable manner. This methodology can be further made efficient and sophisticated with the combination of any of the evolving cryptographic systems.

References

[1] *Advanced Ecryption Standard.* (http://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

[2] *AES Encryption Information.* (http://www.bitzipper.com/aes-encryption.html)

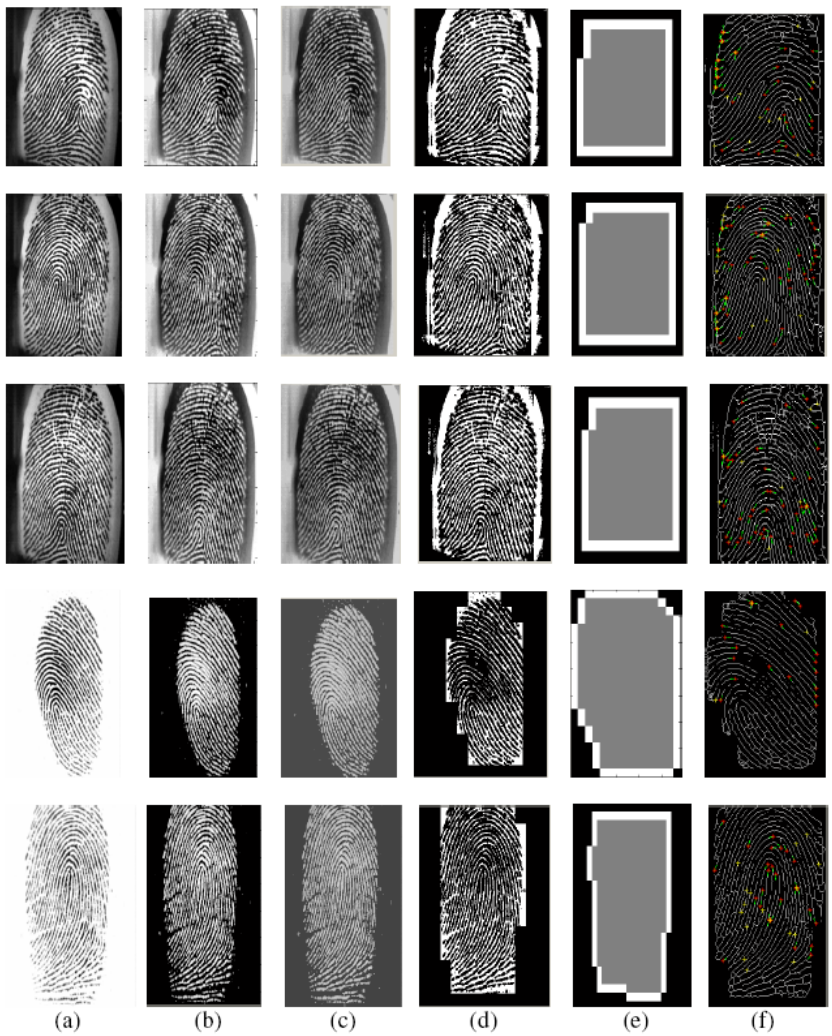

Figure 3: (a) Input Fingerprint Image (b) Histogram equalized image (c) Gabor Filtered Image (d) Binarized Image (e) Region of Interest (ROI) (f) Fingerprint Image with minutiae points

[3] R. Ang, R. Safavi-Naini, L. McAven, "Cancellable key-based fingerprint templates," *ACISP 2005*, pp. 242-252.

[4] *Announcing the Advanced Encryption Standard (AES)*, Federal Information, Processing Standards Publication 197, Nov. 26, 2001.

[5] Y. J. Chang, Z. Wende, and T. Chen, "Biometrics-based cryptographic key generation," *IEEE International Conference on Multimedia and Expo*, vol. 3, pp. 2203-2206, 2004

[6] B. Chen, and 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.

[7] T. Connie, A. Teoh, M. Goh, and D. Ngo, "Palmhashing: A novel approach for cancellable biometrics," *Information processing letters*, vol. 93, no. 1, pp. 1-5, 2005.

[8] D. Feldmeier, and P. Karn. "UNIX password security-Ten years later," *Advances in Cryptology Crytpo '89*, LNCS 435, pp. 44-63, Springer-Verlag, 1990.

[9] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid aApproach for face template protection," *Proceedings of SPIE Conference of Biometric Technology for Human Identification*, Orlando, USA, vol. 6944, pp. ca. 325, 2008.

[10] M. F. Santos, J. F. Aguilar, and J. O. Garcia, "Cryptographic key generation using handwritten signature," *Proceedings of SPIE*, vol. 6202, pp. 225-231, Orlando, Fla, USA, Apr. 2006.

[11] *Gabor Filter*. (http://en.wikipedia.org/wiki/Gabor_filter)

[12] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Transactions on Computers*, vol. 55, pp. 1081-1088, 2006.

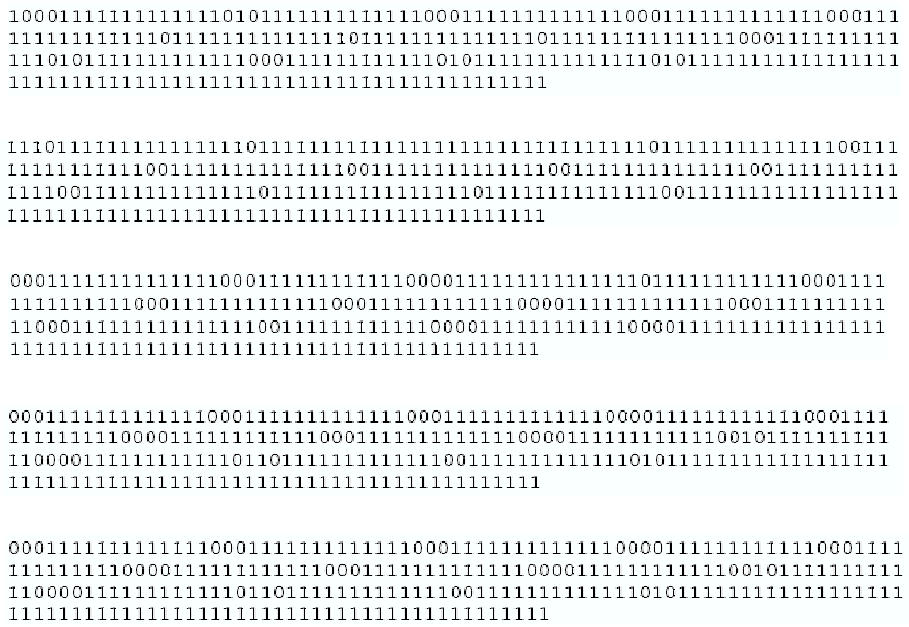

Figure 4: Generated 256-bit key

[13] L. C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S.Tsutsui, *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, CRC Press, 1999.

[14] J. G. Jo, J. W. Seo, and H. W. Lee, "Biometric digital signature key generation and cryptography communication based on fingerprint," *First Annual International Workshop 2007*, LNCS 4613, pp. 38-49, Springer-Verlag, 2007.

[15] D. Klein, "Foiling the cracker: A survey of, and improvements to, password security," *Proceedings of the 2nd USENIX Security Workshop*, pp. 5-14, Aug. 1990.

[16] 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. 879, Sep. 1992.

[17] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, pp. 180, 1997.

[18] R. Morris, and K. Thompson, "Password security: A case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594-597, Nov. 1979.

[19] E. Spafford, "Observations on reusable password choices," *Proceedings of the 3rd USENIX Security Symposium*, pp. 299-312, Sep. 1992.

[20] D. Maio, and D. Maltoni, "Direct gray-scale minutiae detection in fingerprints,," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 1, pp. 27-40, 1997.

[21] E. Maiorana, P. Campisi, J. O. Garcia, and A. Neri, "Cancellable biometrics for HMM-based signature recognition," *2nd IEEE International Conference on Biometrics: Theory, Applications and Systems*, pp. 1-6, 2008.

[22] A. B. Teoh, and C. T. Yuang, "Cancellable biometrics realization with multispace random projections," *IEEE Transactions on Systems*, vol. 37, no. 5, pp. 1096-106, 2007.

[23] T. Wu, "A real-world analysis of Kerberos password security," *Proceedings of the 1999 Network and Distributed System Security Symposium*, pp. 13-22, Feb. 1999.

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

[25] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proceedings of the IEEE*, vol. 92, pp. 948-960, 2004.

[26] T. Yeo, W. P. Tay, and Y. Y. Tai, *Image Systems Engineering Program*, Stanford University, Student project. (http: //scien.stanford.edu /class /ee368 /projects2001/)

[27] G. Zheng, W. Li, and C. Zhan, "Cryptographic key generation from biometric data using lattice mapping," *Proceedings of the 18th International Conference on Pattern Recognition*, vol. 4, pp. 513-516, 2006.

Sunil VK Gaddam received his B. Tech. from Sri Venkateswara University (SVU), Tirupati, India, in 1993, Post Graduate Diploma in Computer Engineering (PGDCE) from Jawaharlal Nehru Technological University (JNTU), Hyderabad, India, in 1994, and M. Tech. (Computer Science) from Jawaharlal Nehru University (JNU), New Delhi, India, in 1997.

He has over 10 years of experience of teaching courses in the discipline of Computer Science in various Indian Universities. He is currently a Professor & Head in the Department of Computer Science & Engineering, Meerut Institute of Engineering & Technology (MIET), Meerut, U.P. Earlier, he worked at RGMCET, Nandyal, A.P., as an Associate Professor, and at KSRMCE, Kadapa, A.P., as an Assistant Professor. His areas of Interest include Computer Networks, Network Security, Data Structures and Operating Systems.

He also worked as Software Engineer for Expert Software Consultancy (ESC), Noida, India, for over a year. He has a number of publications in National and International Conferences and Journals. He organized many National Conferences, Seminars and Workshops for faculty as well as for students. He is also the member of professional bodies like ISTE and CSI.

Manohar Lal is the Director, School of Computer & Information Sciences, Indira Gandhi National Open University, New Delhi (India). He has teaching and research experience of more than 30 years at various Indian universities including University of Delhi and Jawaharlal Nehru University (JNU), New Delhi.

Prof. Manohar Lal is a product of reputed Indian academic institutions including IIT Kanpur, IIT Delhi and University of Delhi. He completed his M. Tech in Computer Science and Engineering from IIT Kanpur and pursued his second Ph. D. in Computer Science and Engineering from IIT, Delhi. Earlier, he completed his master's and Ph. D. programmes in Mathematics from University of Delhi. During 1982-83, he visited North Carolina State University for Post-Doctoral work. In context of academic work, he has visited a number of countries including U.S.A, U.K, Germany and France.

Prof. Lal has long research experience. Earlier, he worked in the area of 'Error-Correcting Codes'. Currently, he is working in the areas of E-Learning, Automation of Reasoning and Computer Networks.