

Novel Shift-Phase Transformation based Cancelable and Irrevocable Biometric Template Generation for Fingerprints

K.Kanagalakshmi,

Research Scholar, Dept. of Comp. Sci.
DJ Academy for Managerial Excellence,
Coimbatore

E.Chandra, Ph.D

Director, PG Dept of Computer Applications,
Dr. SNS Rajalakshmi College of Arts and Science,
Coimbatore

ABSTRACT

Cancelable biometrics expresses multiplicity. Now-a-days conventional authentications and identifications are advanced with biometrics. Since biometrics is unique in nature of a person, he/she must be aware on tracking the original features and also the cross matching of the same when his/her biometrics is used in different applications; and once the biometrics is compromised, those cannot be reset again. These problems are addressed by our proposed novel approach called "Shift-Phase Transformation". It is designed for irrevocable and cancellable biometric template generation. In this paper, the proposed method is used to generate a cancelable and irrevocable biometric template for fingerprint. Series of experiments are followed to test the performance of the proposed method. The factors considered for performance evaluation are the cross matching rate through ROC (using GAR and FAR), Cancelability, Irrevocability, Security, Average time of template generation and matching and also space complexity. The experimental results show the efficiency of proposed method and also show that it is a best method.

Keywords

Bit-shifting, Cancelable template, Chaff Points, Irrevocability, Phase

1. INTRODUCTION

Cancelable biometrics expresses multiplicity. Now-a-days conventional authentications and identifications are advanced with biometrics. Since biometrics is unique in nature of a person, he/she must be aware on tracking the original features and also the cross matching of the same when his/her biometrics is used in different applications; and once the biometrics is compromised, those cannot be reset again. These problems are addressed by our proposed novel approach called "Shift-Phase Transformation". It is designed for irrevocable and cancellable biometric template generation.

In General, protecting information and ensuring privacy of personal identity is a growing concern. Conventional authentication and identification schemes mainly utilize tokens depends on the users secret knowledge to verify his or her identity. These techniques are even though trendy, they contain numerous limitations. Biometric based authentication and identification systems are the extension of conventional systems. Biometrics is used in different applications such as [37]:

1. Commercial Applications , like computer network logins, Internet access, ATMs, electronic data security, credit cards, physical access control, PDAs, Cellular phones, Medical records management and diagnosis, e-commerce and distance learning;
2. Government applications such as National ID cards, social security, border control, passport control and welfare-disbursement;
3. Forensic applications such as corps identification, missing children and parenthood determination.

Biometric raise several security and privacy concerns such as [1]:

1. Biometric is authentic but not secret: Biometrics such as voice, face, Fingerprints and signatures can be easily captured and recorded. They are misused without the consent of users rather than passwords and cryptographic keys that are known only to the user. There have been several instances where artificial fingerprints [2] have been used to circumvent biometric security systems.
2. Biometrics cannot be revoked or canceled. Once the passwords, PINs etc. are compromised then those are reset but the biometrics cannot be reset.
3. If a biometric is lost once, it is compromised forever.
4. Tracking Individuals without their authority are possible through cross-matching: Since the same biometric might be used for various applications and locations, the user can potentially be tracked if the organization shares their respective biometric database.

Biometric based applications guarantee numerous security risks [3]. The brute- force attacks both the biometric based and password based systems [4]. Those problems are addressed by the cancelable and irrevocable biometric technique. Cancelable biometrics refers to an intentional and systematically repeatable distortion (transformations) of biometrics data for the purpose of protecting sensitive user-specific features. The principal objectives of cancellable biometrics templates are [5]:

1. Diversity (Cancelability): A user can use same biometric for more than one applications through

the cancelable templates generated from the original.

2. Reusability: If the templates are compromised then there is an alternate way to produce template from the original biometrics.
3. Non-invertability (Irrevocability): Prevents the recovery of original biometric and external factors because of noninvertible characteristics.
4. Performance: The cancelable biometric template should not weaken the performance of recognition or identification.

In this paper, a novel cancelable and irrevocable biometric template generation technique for fingerprint is designed and implemented. Fingerprint biometric is preferable for the authentication and identification purposes due to the reasons of persistence and individuality properties fingerprints [6]. The proposed system uses the fingerprints for cancelable biometric template generation.

2. RELATED WORK

The related areas of cancelable biometric generation schemes were studied in prior and described in [7]. Summary of the study into different categories of cancelable systems are:

1. Biometric Transformations: This method is based on the transformations of biometric features. It is further categorized into two: Bio-Hashing (Salting) [8], [13], [15], [16], [19], [20], [21] and Non-invertible approach [1]. Our proposed method falls under this category of Non-invertible transformation.
2. Biometric Crypto Systems: In this approach, helper data are generated from the biometrics. Further, it is classified into two: Key-Binding biometric cryptosystem and Key-generation biometric crypto system [9], [10], [11], [12], [14], [17], [23], [27].
3. Hybrid Approach: It follows both the transformation and cryptosystems; and also fuzzy schemes [18], [22], [25], [26], [38].

3. PROPOSED METHOD: SHIFT-PHASE TRANSFORMATION

The flow graph notation of the proposed method is shown in figure 1. Each stage comprises of some process to achieve their objectives. It includes five stages: Image Preprocessing, Image enhancement and Minutiae Extraction, Post-processing, True Phase-minutia Extraction and Cancelable and irrevocable biometric template generation.

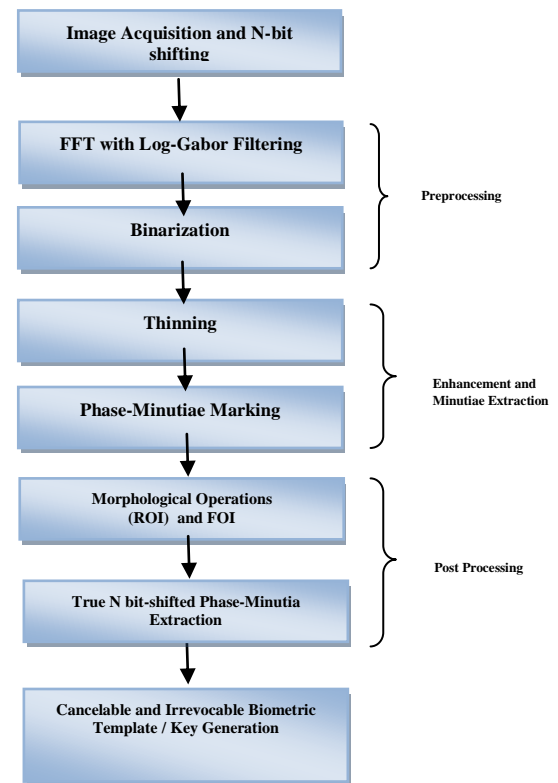


Figure 1 Flow graph of the proposed system

4. CANCELABLE AND IRREVOCABLE TEMPLATE GENERATION FOR FINGERPRINT

4.1 Protocols

In this section, the proposed method is designed and described. The primary objectives of the proposed method are cancelability and irrevocability (one way approach). The requirement of cancelability has some protocols on the parametric functions [1]:

1. The transformation should be locally even to make certain changes in a minutiae position before transformation leads to a small change in the minutiae position after transformation.
2. There should be no global smoothness in transformation: the changes in minutiae positions after transformation should not be correlated to the minutiae positions before transformations. Because the transformation can be inverted simply. Moreover, there should be many-to-one approach while performing transformation to make sure it cannot be uniquely inverted to recover the original minutiae pattern.
3. There should be a high complexity in minimal transformations.

4.2 Proposed Model - Shift-Phase Transform Method: Function Design

By considering the above three protocols, the author proposes a novel Shift-Phase Transform method which is a cancelable and irrevocable biometric template generation method. The functional design comprises of the following stepladder:

1. The primary step of the proposed method is to perform an N-bit shifting of Input fingerprint image. The parametric value N is a positive natural number. Shifting returns an image $I(x,y)$ shifted by N bits.

$$x(j) = Sh_n[I(x,y)] \quad (1)$$

The Sh_n function shifts the pixel value of each coordinates of an image N times.

2. Image enhancement is done in spatial [28], [29], [30] or frequency domain. The proposed method focuses on frequency domain enhancement. The next step of the proposed method is to perform the Fast Fourier Transformation on the shifted image using the equations 2 and 3 to get the frequency values of an input image.

$$\text{FFT: } X(k) = \sum_{j=1}^N x(j) \omega_N^{(j-1)(k-1)} \quad (2)$$

$$\omega_N = e^{(-2\pi i)/N} \quad (3)$$

where ω_N is an Nth root of unity.

The returned Fast Fourier Transformed image is enhanced. That is the frequency domain enhancement is made using the Log-Gabor filter. It is designed by associating two components such as radial and angular components. These enhancement tasks are discussed in [31], [32].

- a) The Radial component:

$$LG(F) = e^{\left(-\frac{\log\left(\frac{r}{rf_o}\right)}{2 \log\left(\frac{\sigma}{rf_o}\right)}\right)} \quad (4)$$

where r is the normalized radius from centre, rf_o is the normalized radius from centre of frequency plane corresponding to the wavelength.

- b) The angular Component:

$$FC = e^{\left(\frac{-d\theta^2}{2\theta\sigma^2}\right)} \quad (5)$$

where FC is the angular filter component; it is obtained by calculating angular distance $d\theta$ of sin and cosine. The Log-Gabor filter as shown in eqn. (6) is derived from the product of eqn. 4 and 5.

$$LGF(f) = LG(f) \times FC \quad (6)$$

Now, the filter is applied on the frequency domain for the enhancement as in eqn. 7.

$$I_{FDE} = X(k) \times LGF(f) \quad (7)$$

Then, the Inverse Fast Fourier Transformation is performed to get back the original enhanced image using eqn. 8.

$$\text{IFFT: } x(j) = \left(\frac{1}{N}\right) \sum_{k=1}^N X(k) \omega_N^{-(j-1)(k-1)} \quad (8)$$

The $x(j)$ is the function which returns an enhanced version of the shifted image. The output image is a complex image. From the enhanced cum shifted complex image, phase-minutiae are marked by Run-Length Coding method and performed post-processing. Finally the shifted phase-minutiae (X, Y) of Terminations and Bifurcations only are extracted using eqn. (9) and (10).

$$X' = K \cos[\Phi_F(x(i,j))] \quad (9)$$

$$Y' = K \sin[\Phi_F(x(i,j))] \quad (10)$$

where Φ_F is the phase value.

3. In third step, two parameters such as shuffling and chaffing are used. That is the extracted phase-minutiae (X' , Y') of bifurcations such as X coordinate with Y and vice versa are shuffled randomly; and chaff (synthetic) points are also added. The chaff points are generated by adding constant floating point along with the extracted shifted phase-minutiae value using the following equations (11) and (12).

$$B_{X'}(n1) = B_{Y'}(i) + C_{f1} \quad (11)$$

$$B_{Y'}(n2) = B_{X'}(j) + C_{f2} \quad (12)$$

where $B_{X'}(n1)$ and $B_{Y'}(n2)$ are the X and Y coordinate points of bifurcations respectively; C_{f1} and C_{f2} are the different floating point constants; and $n1$, $n2$ are positive integers.

4. From third step, finalized cancelable and irrevocable biometric template is generated as shown in appendix C.

4.3 Experimental Study

In order to analyze the cancelable transformations on the fingerprint image, an empirical study is also followed with benchmark databases such as FVC in 2000, 2002, 2004, and real time database. Each database contains 880(Set A: 100×8, Set: 10×8) fingerprints and fifty different real time fingerprints are obtained from untrained volunteers. The same finger is needed to give 5 impressions.

In this experimental study, the following criteria are concerned about the cancelable transformations:

1. Performance impact on cancelability.
2. Strength against an invertible attack.
3. Distinctiveness
4. Performance of the choice of parameters.

4.3.1 Performance impact on cancelability

The first experimental study is on the performance impact on cancelability. It is observed that, the transformed version of the fingerprint template is derived from the complex transformations along with chaff points. The proposed “Shift-phase transform” method starts the version transfer of an input In the initial level itself, changes on pixel values of an input image are occurred. It increases the strength on irrevocability of the original features. Figure 3 shows changes occurred among the pixels. It is clearly shown that the pixel value before and after shifting is varied.

fingerprint image at the entry level. That is the captured image is N-bit shifted primarily. Bit shifting causes the change of black pixels into white and vice versa. So the shifted image gives a scattered pattern of an image. Fig 2 shows the ridge patterns and their orientations before and after bit-shifting.



Figure 2 (a) Fingerprint image before shifting (b) N-bit Shifted image

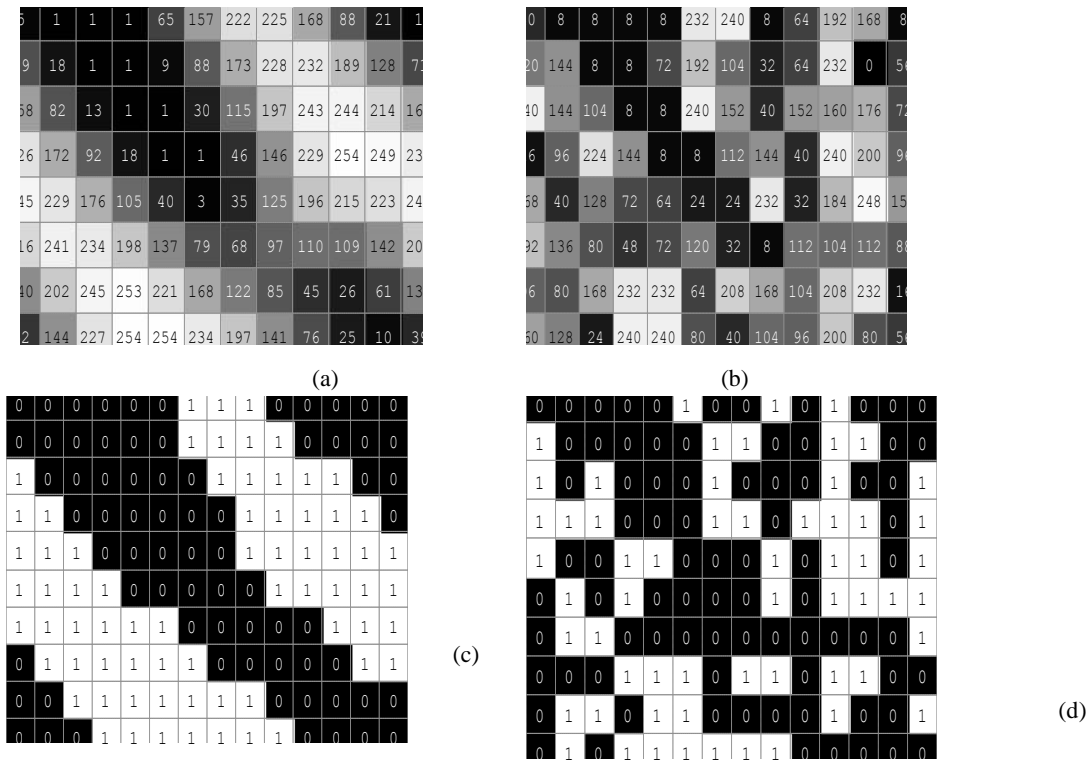


Figure 3 left Column figures (a and c) are the respective original gray and binary pixel values of an image before shifting; right column figures (b and d) are their N-bit shifted gray and binary pixel images respectively. By referring binary pixel values, it clearly visualizes the orientations of ridges and valleys before shifting; but the same are scattered (shuffled: 0's and 1's) after shifting(c).

Empirically it is found that there are more terminations and less bifurcation before shifting; but there are more bifurcations and very few, sometimes no terminations are found after performing N-bit shift

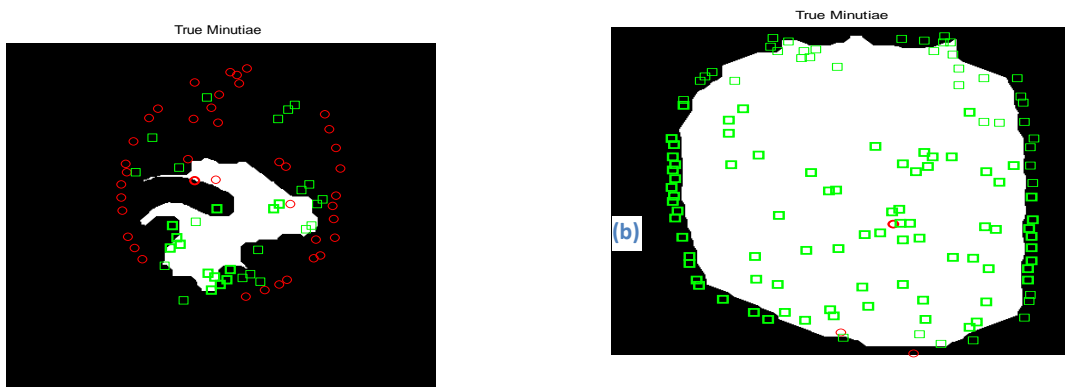


Figure 4 Minutiae Extraction (a) Before Shifting (b) After Shifting

The cancelable property of the proposed method is tested with the matching impact on intra fingerprints (8 impressions per person) and inter-fingerprints (8×10). It is found that there is no cross matching occurrence. Multiple transformations on single images are carried out and no one shows the similarity. It application. Hence, the cancelable property is proved.

4.3.2 Strength against an invertible attack

minutiae of an image. It extracts only the phase minutiae instead of magnitude. The phase possesses very less sensitive information of an image. But the magnitude possesses all sensitive values (data) of an image. Moreover an association of the magnitude and phase values alone makes the meaningful and accurate image pattern. This method focuses only on the phase minutiae which will not be used for the derivation of original features. This property integrates robustness and irrevocability of original features from the stored phase-minutiae templates. The primary benefit of the proposed method is the template with the fields of only the X and Y co-ordinates of bifurcations without orientations. These minutiae fields are shuffled and stored. It adds an additional strength along with N-bit shifting to comprise the irrevocability. So the stored (N-bit shifted phase-minutiae) template is helpless to generate original features of an image.

Figure 5 shows the attempt for an invertible attack against the original image at the entry level. It is clearly shown that the pixels after performing the reverse shifting do not match with pixels of original image. This is because of the compatible type conversion of an image occurred internally. This first attempt is made to prove the irrevocability at the entry level. The second attempt is to invert the stored biometric template to get back the original one. Though it is impossible to get original version of an image from the phase value as stated early, the stored biometric templates are used to revoke the original. Attempts are failed because of the insufficient parameters (X, Y coordinates) to derive original image and also template data posses shuffled chaff points.

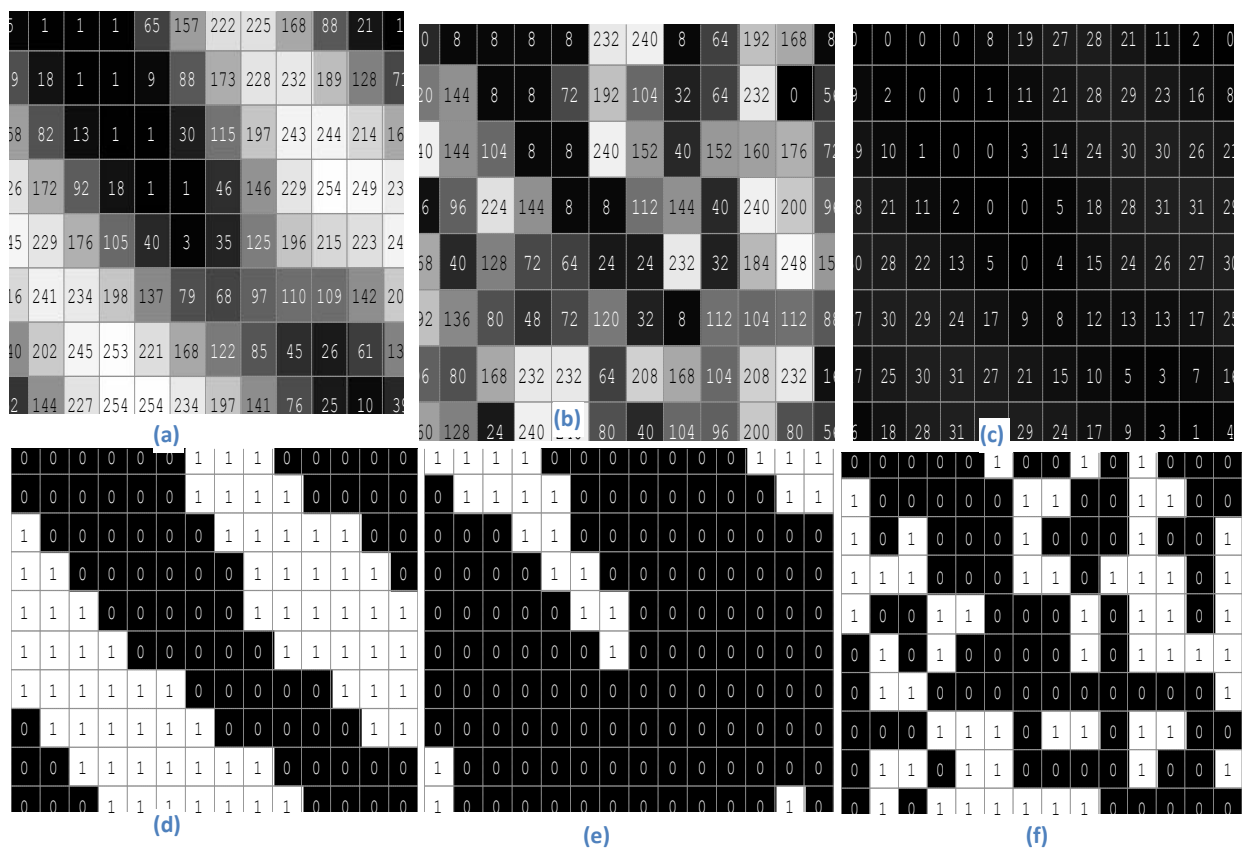


Figure 5 comparisons of images according to shifting and reverse shifting process (a) original gray image (b) N-bit Shifted gray image (c) Reverse shifting of (b) to get original image pattern (d) Original Binary image (e) N-bit shifted binary image (f) reverse shifting of (e) to get original binary image (d). The pixel values of reverse shifting do not coincided with the same of the original image (compare (a) and (c) in gray image; and (d) and (f) in binary image).

Experiments on reverse shifting are performed in order to get original image pattern; it results different pixels which are not coincided with the pixels of original image.

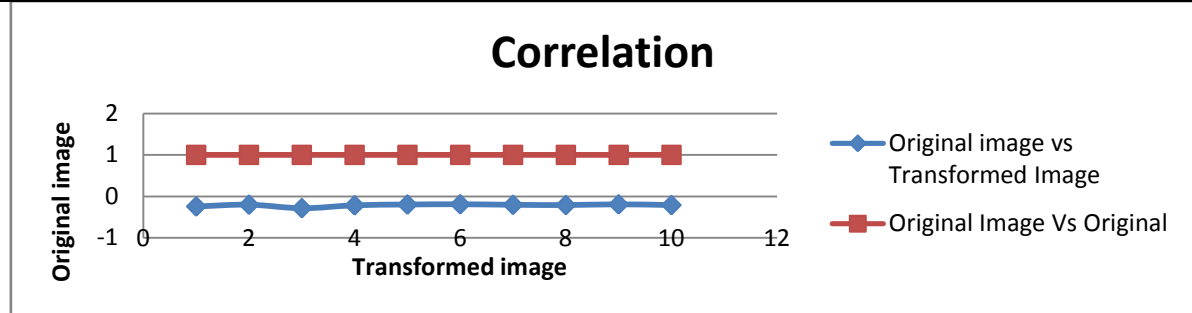
4.3.3 Distinctiveness

The third criterion is to check the distinctiveness. That is to ensure whether the original fingerprint and the transformed version are correlated or not. To prove this phenomenon, the author performed the transformations on the database sets individually and compared the original

fingerprint image with transformed version. Through the correlation factor and matching statistics, it is proved that the transformed versions are no more likely to match the original images. Thus, the uniqueness is proved. Correlation between the Original and transformed version of images are shown in table 1 and it is plotted in fig. 6. It shows the distinctiveness of both original image and its unique transformed version. If the two images are not same then its correlation factor is non-zero negative number otherwise 1.

Table 1 correlation between original and transformed image

	Correlation of image #									
	101_1	102_1	103_1	104_1	105_1	106_1	107_1	108_1	109_1	110_1
Original image Vs Transformed Image	-0.0008	0.003	0.0037	0.0024	-0.0041	-0.0025	0.0046	-0.0014	-0.019	-0.0033
Original Vs Original Image	1	1	1	1	1	1	1	1	1	1

**Figure 6 correlation chart: correlation between Original and the transformed version of the same image**

4.3.4 Performance of the choice of parameters

The choices of parameters are analyzed in this section. The selected parameters of the proposed method are chaff points and shuffling minutiae. The strength of the cancelability and irrevocability is described and proved in the previous sections. In addition to that the chaff points are introduced in association with the extracted phase-minutiae as given in fig. 7. They are generated by adding a floating point parametric key with the extracted minutiae randomly; and also the shuffling parametric keys such as X and Y coordinates. Chaff points introduced in the phase-minutiae cannot be easily identified and they are shuffled. It is not possible to separate true and chaff points from the shuffled minutiae set. Hence, the performance of the choice of parameters are strengthen and sensitive. The floating point parameters derive the micro level to macro level distinctiveness of minutiae.

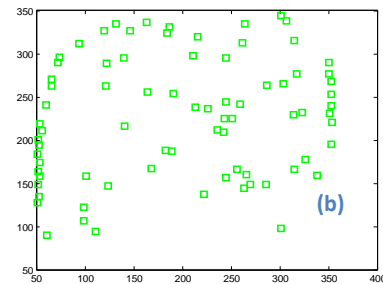
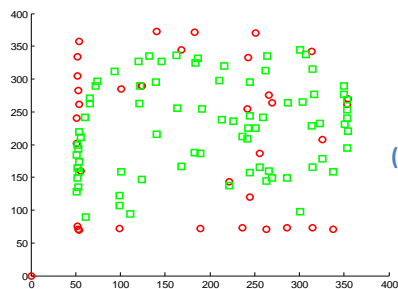


Fig 7 (a)Extracted final shifted phase-minutiae set (b) Chaff (synthetic) minutiae in association with shuffled final shifted phase-minutiae .Chaff points are indicated by circle and shifted phase-minutiae are indicated by square

4.4 Performance Evaluation Of Proposed Method

The performance of the proposed Shift-Phase transform method is evaluated based on genuine (matching two benchmark templates of the same finger) and impostor (matching two benchmark templates originating from different fingers) attempts. They are performed to compute False Rejection Rate (FRR), False Acceptance Rate (FAR) and Genuine Accept Rate (GAR). Fingerprint minutiae descriptors can be used to perform matching. There are two types of descriptors: Texture-based (orientations and Frequency values) and Minutia-based (Local minutiae structures) [33]. Minutiae based matching (through the visual difference and correlation) method is followed in our proposed work to match the cancelable templates. Figure 8 shows the Receivers Operating Curve. The ROC is a graph that expresses the relationship between the Genuine Accept Rate (GAR) and the False Accept Rate (FAR), and the same can be used to report the performance of a biometric authentication system. Minimum number of samples is required to achieve confidence bands of desired width for the

ROC curve [34]. GAR is calculated through FAR. $GAR = (1 - FAR)$.

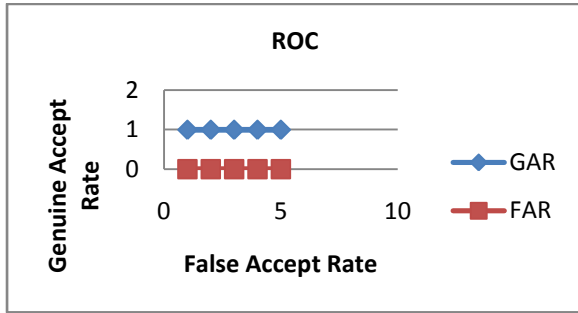


Figure 7.8 ROC on Cancelable transforms performance

In addition to ROC analysis, the performance evaluations are carried out on proposed method in the following aspects too:

1. Space complexity (Maximum amount of memory)
2. Time Complexity
3. Security.

4.4.1 Space Complexity

Since the cancelable template possesses selective minutiae point, it occupies very less space in memory than the raw image. Table 2 reports the memory space required to store the original image and the cancelable biometric template of fingerprints. The average ratio of memory space between biometric template and raw image is about 0.005 only. Figure 9 shows the space complexity plot.

Table 2 Memory space of an image and cancelable biometric template

Image #	Fingerprint Image		Fingerprint Template	
	Size of Image (KB)	Size on disk (KB)	Size of template in bytes	Size on disk (KB)
1	142	144	858	4
2	142	144	946	4
3	142	144	429	4
4	142	144	781	4
5	142	144	902	4
6	142	144	671	4
7	142	144	693	4

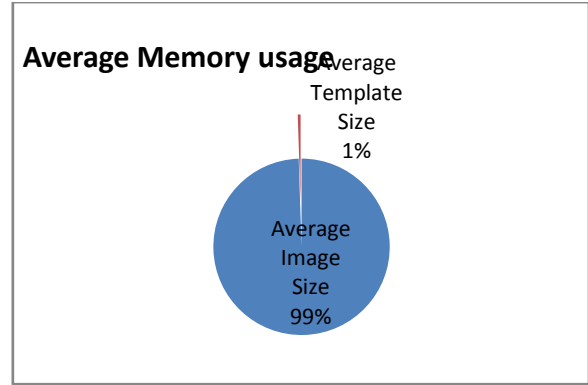


Figure 9 space complexity: Maximum amount of memory is used by an image and less amount of memory by template

4.4.2 Time Complexity

Time complexity is also considered as an evaluation factor. Table 3 reports the time taken to generate cancelable biometric template and also match. The average time taken by the proposed method to generate cancelable biometric template of fingerprint is 25.66 seconds in Intel i3 processor which is plotted in fig. 10. In accumulation to that the average matching time is also calculated (0.007 seconds). The matching time is calculated exclusively.

Table 3 average template generation and matching time

Image #	Template Generation time in seconds	Template Matching Time in seconds
1	18	0.001
2	26	0.001
3	28	0.016
4	28	0.001
5	27	0.001
6	27	0.016
7	25	0.016
Average Time	25.66	0.007

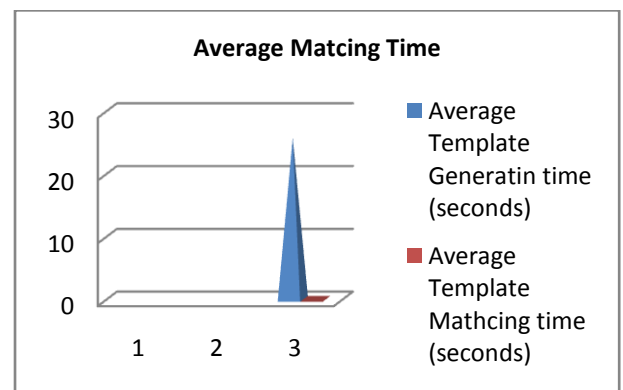


Figure 10 Average matching times of Template generation and Matching

4.4.3 Security

Preferably, biometric secrecy systems leak a negligible amount of information due to sending the helper data [35]. There is no helper data usage in the proposed method. Internal chaff point generation is only followed. It doesn't require any helper data externally. Thus, the secrecy and security are enforced. Biometric template security is an important issue. Enhancing the security of the biometric templates is essential [36]. The proposed method uses only the cancelable biometric template with minutiae of the transformed version of an image to store and not the original features; Furthermore, it follows one-way approach (irrevocable) as described in section 4. Due to the property of irrevocability, the original image or features can't be derived because of the extraction and storage of the phase value of an image not the magnitude. Most of the sensitive features of an image are based on magnitude but not phase value. At the same time both magnitude and the phase combinations only make the original and accurate image. So the original features cannot be derived from the phase-minutiae. Hence a cancelable and irrevocable biometric key can be derived; and also the security is robust.

5. CONCLUSION

The traditional password and token based security systems are advanced with biometric systems. A novel cancelable and irrevocable biometric template generation method is explained and series of experiments were followed. The proposed method "Shift-Phase Transform" is tested based on the properties like Cancelability, Irrevocability and Security. In addition to that, average time of biometric template generation and matching are calculated. Maximum memory usage of the biometric template is also measured. The results show that proposed Shift-Phase transform achieves a better performance and it is an efficient method in different aspects.

6. REFERENCES

- [1] Nalini K.Ratha, Sharat Chikkerur, Jonathan H. Connell, and Ruud M. Bolle, Generating Cancelable Fingerprint Templates, *IEEE Transactions and Pattern Analysis and Machine Intelligence*, Vol. 29, No. 4, April 2007.
- [2] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, Impact of Artificial Gummy Fingers on Fingerprint Systems, *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677, pp. 275-289, 2002.
- [3] Younhee Gil, Dosung ahn, Sungbum Pan, and Yongwha Chung, Access Control System with High Level Security using fingerprints, *Proc. Of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03)*, 2003, IEEE.
- [4] Ruud M. Bolle, Jonathan H. Connell, Nalini K.Ratha, *Pattern Recognition*, Vol. 35, 2727-2738, 2002, Elsevier.
- [5] D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, pp. 301-307, Springer.
- [6] Sharath Pankanti, Salil Prbhakar, and Anil K. Jain, On the Individuality of Fingerprints, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 24, NO. 8, 2002.
- [7] E. Chandra and K. Kanagalakshmi, Cancelable Biometric Template Generation of Protection Schemes: a Review, *Proceedings of ICECT -2011, Third International Conference on Electronics Computer Technology*, Vol. 5, pp. 15-20, E-ISBN: 978-1-4244-8679-3, Published by IEEE
- [8] C. Soutar, D. Roberge, Astoinav, A. Gilroy, and B.V.K. Kumar, Biometric Encryption using image processing, *Proc. SPIE*, vol. 3314, pp. 174-188, 1998.
- [9] A. Juels and M. Wattenberg, "A fuzzy commitment schemes", *Proceedings of 6th ACM Conference on Computer and Communication Security*, pp. 28-36, Singapore, November 1999.
- [10] F. Monrose, M.K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics", *proceedings of the 6th ACM Conference on Computer and Communication security*, pp. 73-82, Singapore, November 1999.
- [11] F. Monrose, M.K. Reiter, Q. Li, and S. Wetzel, "Cryptographic key-generation from voice", *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, pp. 202-123, USA, May 2001.
- [12] C. Vielhauer, R. Steinmetz, and A. Mayrhofer, "Biometric hash based on statistical features of online signatures", *Proceedings of the International conference on Pattern Recognition*, Vol. 1, pp. 10123-10126, Canada, August 2002.
- [13] A. Goh and D.L. Ngo, Computation of Cryptographic Keys from Face Biometrics, *Proc. IFIP: Int'l Federation for information processing*, pp. 1-13, 2003.
- [14] J.P. Linnartz and P. Tuyls, NewShielding Functions to enhance privacy and prevent misuse of biometric templates, *Proc. Fourth Int'l cong. Audio and Video-based biometric person authentication*, pp. 393-402, 2003.
- [15] M. Savvides, B.V.K. Vijayakumar, and P.K. Khosla, Cancelable biometric filters for face recognition, *Proc. Int'l Conf. Pattern Recognition*, pp. 922-925, 2004.
- [16] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, Biohashing: Two factor authentication featuring fingerprint data an tokenized random number, *Pattern Recognition*, Vol. 37, No. 11, pp. 2245-2255, 2004.
- [17] U. Uludag, S. Pankati, S. Prabhakar and A.K. Jain, "Biometric Crypto systems: issues and challenges", *Proceedings of the IEEE*, Vol. 92, no. 6, pp. 984-960
- [18] Y. Dodis, L. Reuzin, and A. Smith, "Fuzzy extractor: how to generate strong keys from biometrics and other noisy data", *Proceedings of International Conference of the Theory and Applications of cryptographic Techniques: Advances in Cryptology*, vol. 3027 of Lecture Notes in Computer Science, pp. 523-540, Switzerland, May 2004.
- [19] T. Connie, A.B.J. Teoh, M.K.O. Goh, and D.C.L. Ngo, Palm Hashing: A Novel approach for cancelable biometrics, *Information Processing Letters*, Vol. 93, no. 1, pp. 1-5, 2005.

- [20] R.Ang, R.Safav-Naini, and L.McAven, Cancelable Key-based Fingerprint Templates, Proc. 10th Australian Conf, Information Security and Privacy, pp. 242-252, 2005.
- [21] Y. Sutcu, H. T. Sencar, and N. Memon, “A secure biometric authentication scheme based on robust hashing,” in Proc. 7th Workshop Multimedia and Security, New York, 2005, pp. 111– 116.
- [22] P. Tuyls, A.H. Makermans, T.A.M. Kevenaar, G.J. Schrijen, A.M. Bazen, and R.N.J. Veldhuis, “Practical biometric authentication with template protection”, ”, Proceedings of the 5th International Conference on Audio and Video based biometric person authentication, Vol. 3546 of Lecture Notes in Computer Science, pp.436-446,USA,July 2005.
- [23] F.Hao,R. Anderson, and J. Daugman, “Combining crypto with biometrics effectively”, IEEE Transactions on Computers, Vol. 55, no. 99, pp.1081-1088, 2006.
- [24] Chun-I Fan and Yi-Hui Lin, “Provably secure remote truly three-factor authentication scheme with privacy Protection on biometrics”, IEEE Transactions on Information Forensics and Security Vol. 4, Issue 4, Pages: 933-945, December 2009.
- [25] Bian Yang and Christoph Busch, “Parameterized geometric alignment for minutiae-based fingerprint template protection”, Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems, Washington, DC, USA, pp. 340-345 , 2009.
- [26] Abhishek Nagar, Karthik Nandakumar, and Anil K. Jain, “A hybrid biometric cryptosystem for securing fingerprint minutiae templates”, Pattern Recognition Letters, Elsevier Science ,Vol. 31 , Issue 8 , pages 733-741, June 2010.
- [27] Feng Hao, Ross Anderson and John Daugman, Combining Crypto with Biometrics effectively, IEEE Transactions on Computers, Vol. 55, No. 9, 2006.
- [28] K.Kanagalakshmi and E.Chandra, 2011.Performance Evaluation of Filters in Noise Removal of Fingerprint Image, Proceedings of ICECT-2011, 3rd International Conference on Electronics and Computer Technology, pp vol.1: 117-123, ISBN: 978-1-4244-8677-9, Published by IEEE,
- [29] E.Chandra and K.Kanagalakshmi, Noise Elimination in Fingerprint Images using Median Filter, Int. Journal of Advanced Networking and Applications, Vol. 02, Issue:06, pp:950-955, 2011.
- [30] E.Chandra and K.Kanagalakshmi, Noise Suppression Scheme using Median Filter in Gray and Binary Images, International Journal of Computer Applications, Volume 26– No.1, pp. 49-57, 2011.
- [31] E.Chandra and K.Kanagalakshmi, Frequency Domain Enhancement Filters for Fingerprint Images: A Performance Evaluation”, CIIT International Journal of Digital Image Processing, Vol.3, No. 16, 2011.
- [32] K.Kanagalakshmi, and E.Chandra, Frequency Domain Enhancement algorithm based on Log-Gabor Filter in FFT Domain, European Journal of Scientific Research, Vol. 74, No. 4, pp. 563-573, 2012.
- [33] JianJiang Feng, Combining minutiae descriptors for fingerprint matching, Pattern Recognition, Vol. vol. 41: 342-352, 2008, Elsevier.
- [34] Sardt C.Dass, Yongfang zhu, Anil K. Jain, Validating a biometric authentication systems sample size requirements, IEEE Transactions on pattern analysis and machine intelligence, Vol. 28, No. 12, 2006
- [35] Tanya Ignatenko, and Frans M.J. Willems, Biometric Systems: Privacy and Secrecy Aspects, IEEE Transactions on Information Forensics and security, Vol. 4, No. 4, 2009.
- [36] Anil K. Jain, Karthik Nandakumar and Abhishek Nagar, Biometric Template Security, EURASIP Journal on Advances in Signal Processing, Special issue on Biometrics, Jan. 2008.
- [37] Salil Prbhakar, Sharath Pankanti, and Anil K. Jain, Biometric Recognition: Security and Privacy concerns, IEEE Security and Privacy, Vol. 1 no.2, pp. 33-42, 2003.

APPENDIX A

(a)

(b)

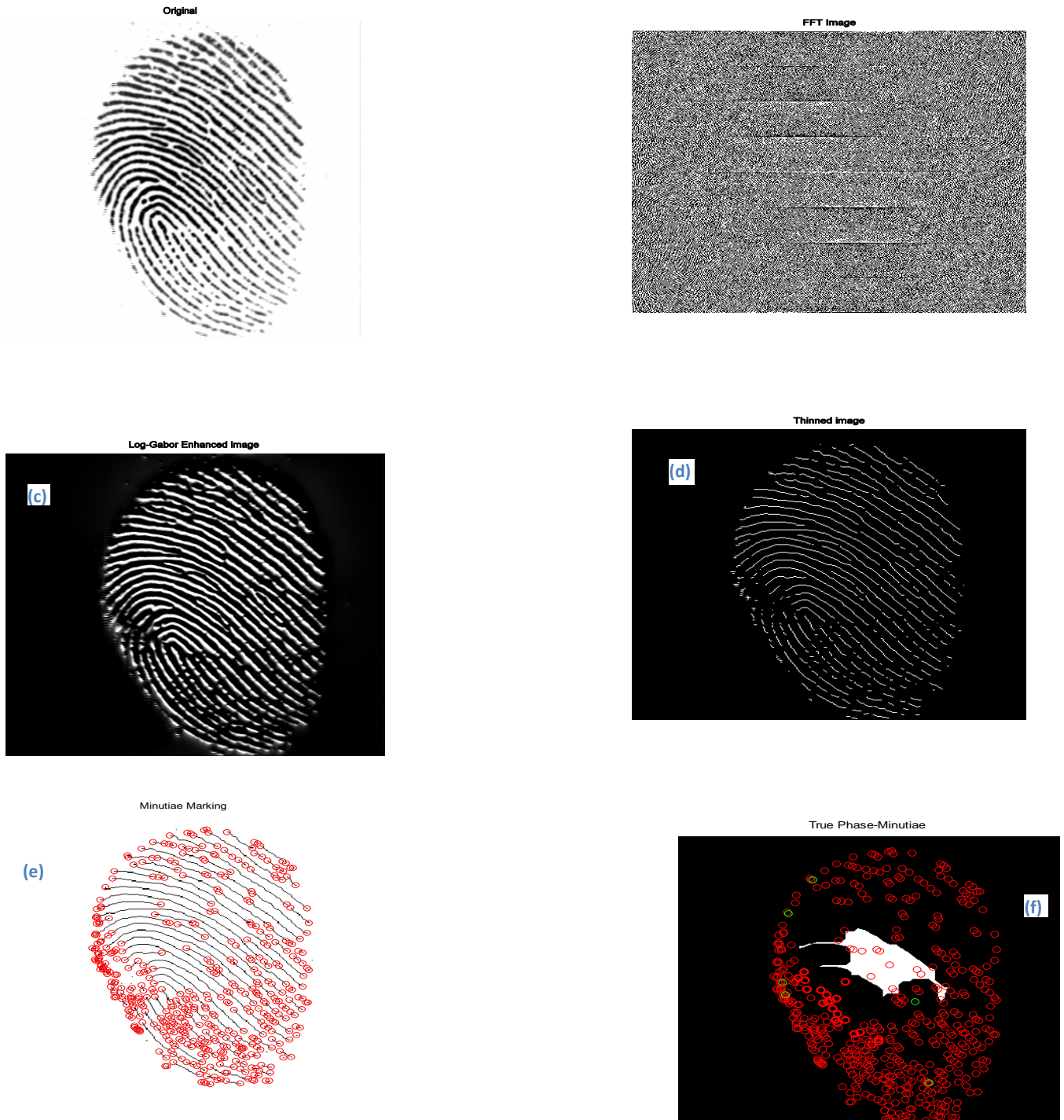


Figure 11 Minutiae Extraction stages before N-bit Shifting: (a) Original image (b) FFT Image (c) Log-Gabor filtered image (d) Enhanced cum thinned image (e) Minutiae Marking (before Post Processing) (f) True Phase-Minutiae set (after post processing)

APPENDIX B

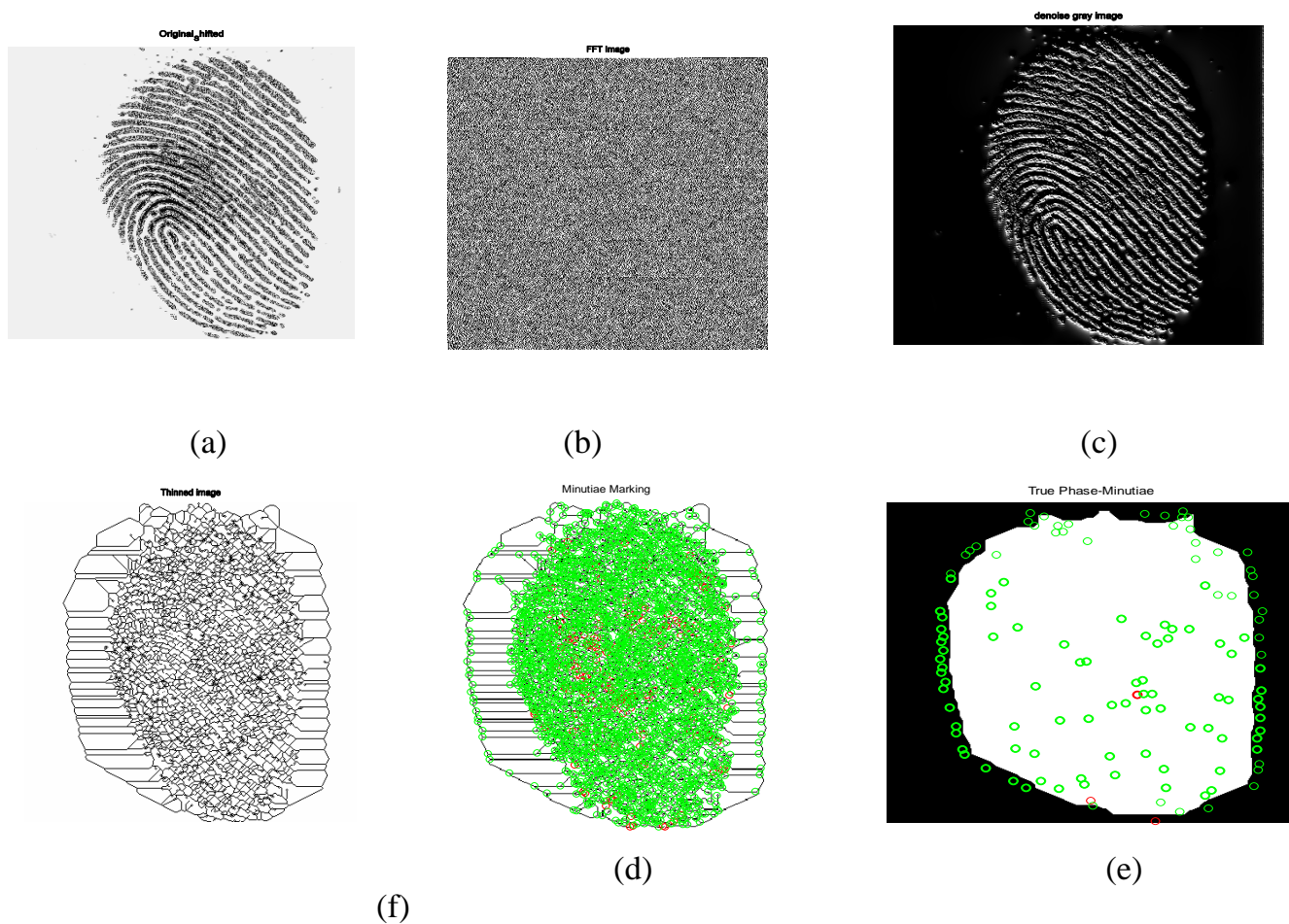
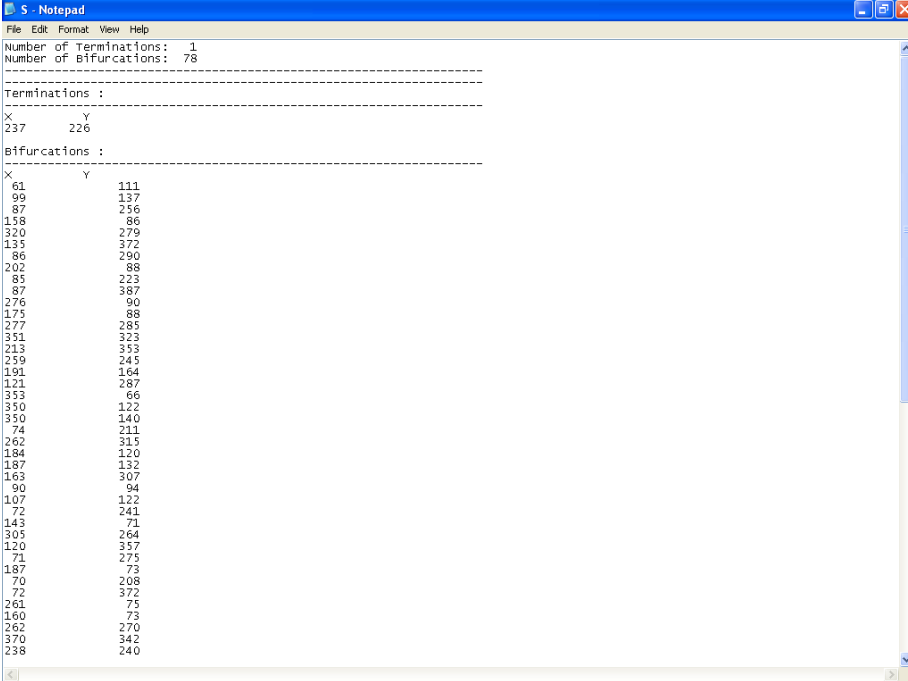


Figure 12 Minutiae Extraction stages: (a) N-bit shifted image (b) FFT Image (c) Log-Gabor filtered image (d) Enhanced cum thinned image (e) Minutiae Marking (before Post Processing) (f) True shifted Phase-Minutiae set (after post processing)

APPENDIX C

Cancelable and irrevocable biometric template generated from fingerprint



S - Notepad

File Edit Format View Help

Number of Terminations: 1
Number of Bifurcations: 78

Terminations :

X	Y
237	226

Bifurcations :

X	Y
61	111
99	137
87	256
158	86
320	279
135	372
86	290
202	88
85	223
87	387
276	90
175	88
277	285
351	323
213	353
259	245
191	164
121	287
353	66
350	122
350	140
74	211
262	315
184	120
187	132
163	307
90	94
107	122
72	241
143	71
305	264
120	357
71	275
187	73
70	208
72	372
261	75
160	73
262	270
370	342
238	240