Novel Complex Conjugate-Phase Transform technique for cancelable and irrevocable biometric template generation for fingerprints

Ms. K.Kanagalakshmi[1] and Dr.E.Chandra[2]

[1] Doctoral Research Scholar, DJ Academy for Managerial Excellence, Coimbatore, Tamilnadu, India.

[2] Supervising Guide, Dr.SNS Rajalakshmi College, Coimbatore, Tamilnadu, India

Abstract

This paper introduces a novel method for cancellable and irrevocable biometric template generation. The proposed method named as complex conjugate phase transform takes the main components like bit shifted-phase, twin complex conjugate transpose and chaff point generation along with it. The strength of the proposed method is tested in different aspects such as cancelability, irrevocability and security. The performance of the same is also calculated in terms of time and space complexity; ROC analysis is also carried out. The proposed method achieves higher matching scores; and the experimental results show that the proposed complex conjugate phase transform is better in all the aspects of performance.

Keywords: *Cancelability, Hermitian transpose, Irrevocability, Phase, Shifting.*

1. Introduction

Traditional Password and advanced biometric systems are in authentication and identification systems. Biometrics is the science and technology which is measuring and analyzing biological data. According to information technology, biometrics is referred as technologies which measure and analyze characteristics of human (both physical and behavioral characteristics), such as fingerprints, iris, face, voice, traits and signatures. They are used for the authentication and identification purposes [37] [7]. Authentication and identification through biometric confirmation are becoming famous and increasingly common in corporate and public security systems. But the security of the stored biometric data is theft. To prevent the identity theft, biometric data is generally encrypted when it is gathered and stored. Now-a-days, the cancelable biometric template or key generation techniques are emerging to meet these security issues and identity thefts. Biometric based applications guarantee numerous security risks [3]. The brute-force attacks both the biometric based and password based systems [4].

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 Diversity, Cancelability, Reusability, Non-invertability, and Performance [5]. In this paper, a novel cancelable biometric template generation technique is proposed. Section 2 describes the background work on the related areas. A new proposed method is developed and described in section 3. Section 4 gives the experimental study in different aspects. In section 5, the performance evaluation on proposed method is done and explained. Section 6 concludes the paper.

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: Complex Conjugate-Phase Transform Technique (CCPT)

Fingerprint biometric is preferred for the authentication and identification purposes due to the reasons of persistence and individuality properties fingerprints [6], [39]. Our system uses the fingerprints for cancelable biometric template generation. The Bifurcations and endings of ridge or valley are used to identify the uniqueness of the fingerprint. So, the proposed method makes use of the bifurcations and endings for the template generation [40]. In this section, the proposed method called complex conjugate phase transform is designed and described. It comprises of five stages: Image preprocessing, image enhancement, Minutiae extraction, Post-processing, True Phase-minutia extraction and Cancelable and irrevocable biometric template generation. The System level design of the proposed method is given in figure 1.

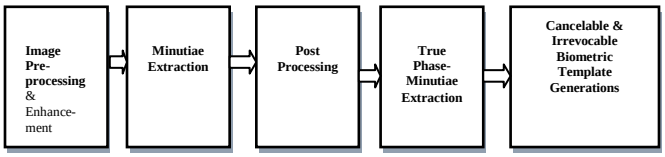


Fig. 1 System Level Design.

The flow graph notation of the proposed method is shown in figure 2. Each stage follows some sub functions to meet their objectives. Before the extraction of minutiae to generate biometric templates, the pre and post processing stages are crossed.

3.1 Constraints for Cancelable and Irrevocable Biometric template generation

The main objectives of the proposed method are cancelability and irrevocability (one way approach). Those are achieved by considering some constraints. 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.

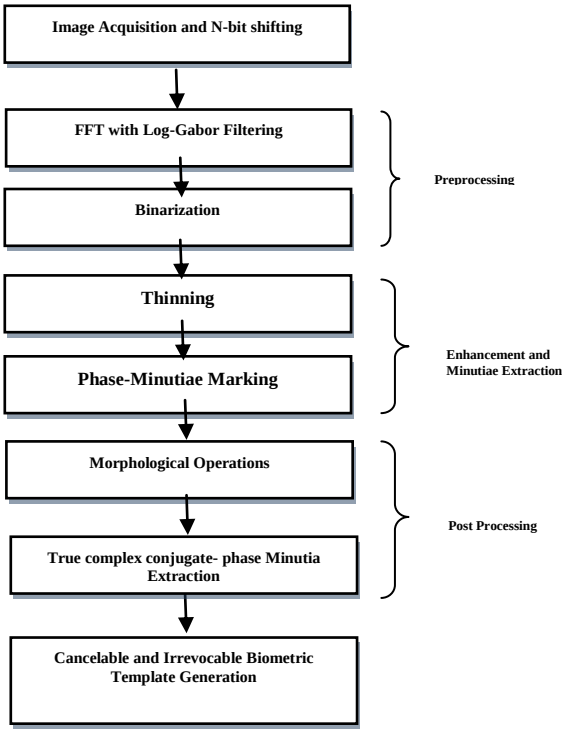


Figure 2 Flow graph of the CCPT

3.2 Complex Conjugate Phase Transform Method: Function Design

A new method is proposed and its functional design is described in this section. A novel complex conjugate phase transforms method which is a cancelable and irrevocable biometric template generation method. The functional design comprises of the following hierarchy:

1. The primary step of the proposed method is to perform an N-bit shifting of Input fingerprint image as shown in eqn. (1). 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 [31], [32]. 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.

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

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

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 [31], [32]. It is designed by associating two components such as:

a) The Radial component:

$$LG(F) = e^{\left(-\frac{\log\left(\frac{r}{rf_0}\right)}{2\log\left(\frac{\sigma}{rf_0}\right)}\right)} \quad (4)$$

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:

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

where FC is the angular filter component; it is obtained by calculating angular distance $d\theta$ of sin and cosine. The Log-Gabor filter 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.

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

The x(j) is the function which returns an enhanced version of the shifted image. The output image is a complex image. Then the enhanced cum shifted complex image is applied twin conjugate transpose. Next the complex conjugated phase-minutiae are marked by Run-Length Coding method and performed post-processing. Then the shifted phase-minutiae (X, Y) of Terminations and Bifurcations only are extracted using eqns. (9) , (10) and (11).

$$X` = [Kcos[\Phi_F\left(x(i,j)\right)]]' \quad (9)$$

$$Y` = [Ksin[\Phi_F\left(x(i,j)\right)]]' \quad (10)$$

where Φ_F is the phase value; X` and Y` gets the complex conjugate transposed (also called Hermitian transpose) phase value.

$$CCPh = f((X`, Y`)') \quad (11)$$

CCPh is a twin conjugate transposed phase.

3. In third step, two parameters such as shuffling and chaffing are used. That is the extracted twin complex conjugated 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 (12) and (13).

$$B_{X`}(n1) = B_{Y`}(i) + C_{f1} \quad (12)$$

$$B_{Y`}(n2) = B_{X`}(j) + C_{f2} \quad (13)$$

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 which is shown in table 1.

Table 1: Cancelable and irrevocable biometric template generated from fingerprint

Bifurcations Coordinates	
X	Y
116	129
85	109
275	114
175	295
227	234
241	54
255	55

4. Experimental Study

An empirical study is performed to test the cancelability and irrevocability of the proposed method. Sequence of experiments are made on the proposed method using benchmark databases such as FVC (Fingerprint Verification Contest) 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. Properties of all the selected image databases are shown in the table 2.

Table 2: Property of Databases

Database Name	Sensor Types	Size of the Image	Resolution in dpi
2000 DB1	Low-cost Optical Sensor	300×300	500
2000 DB2	Low-cost Capacitive Sensor	256×364	500
2000 DB3	Optical Sensor	448×478	500
2002 DB1	Optical Sensor	388×374 (142 Kpixels)	500
2002 DB2	Capacitive sensor	296×560 (162 Kpixels)	569
2002 DB3	Capacitive Sensor	300×300 (88 Kpixels)	500
2004 DB1	Optical Sensor	640×480 (45 Kpixels)	500
2004 DB2	Optical Sensor	328×480 (100 Kpixels)	500
2004 DB3	Thermal Sweeping	300×480 (56 Kpixels)	500
Real Time DB	Optical Sensor	300×300	500

While performing empirical study, the following standards are taken into account.

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

4.1 Performance impact on cancelability

The primary study is about the cancelability of biometrics. From the experiment, it is observed that, the transformed version of the fingerprint template is derived from the multiple complex transformations along with chaff points. The proposed "Complex Conjugate Phase transform" method starts the version transfer of an input 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 due to the change of pixel value. So the shifted image gives a scattered pattern with conjugate phase of an image. Fig 3 shows the ridge patterns and their orientations before and after bit-shifting.

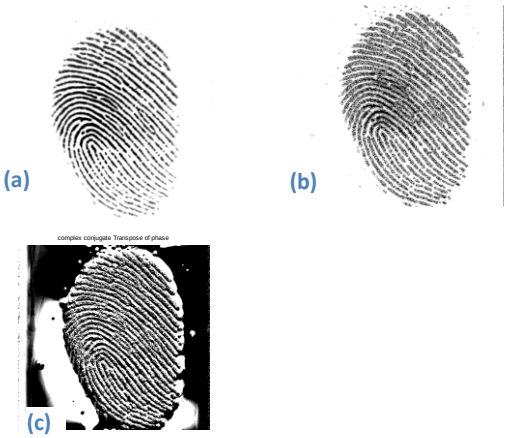


Figure 3 image comparison (a) Fingerprint image before shifting (b) N-bit Shifted image (c) twin complex conjugate phase image.

In the initial level itself, changes on pixel values of an input image is occurred. It increases the strength on irrevocability of the original features. Figure 4 shows changes occurred among the pixels. It is clearly shown that the pixel value before and after shifting is varied.

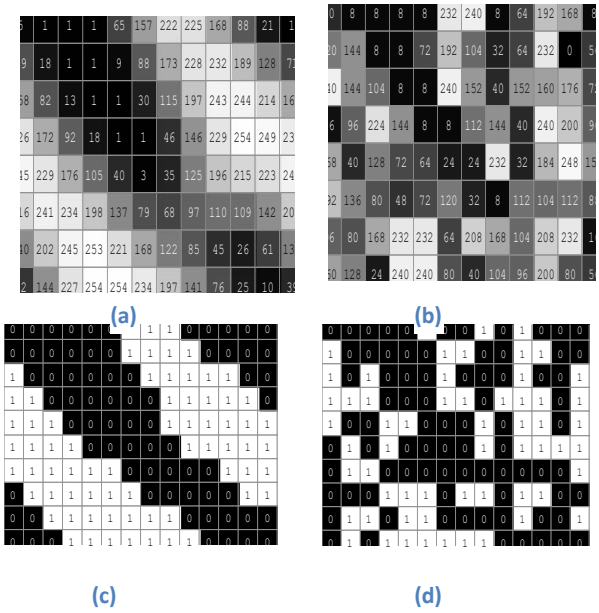


Figure 4 left Column figures (a and c) are the respective original gray and binary pixel values of an image before shifting; right column figures (b and d) are their N-bit shifted gray and binary pixel images respectively. By referring binary pixel values, it clearly visualizes the orientations of ridges 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 on an image as in fig 5. This is because of scattering of ridge pixels (0's and 1's) as described in figure 4.

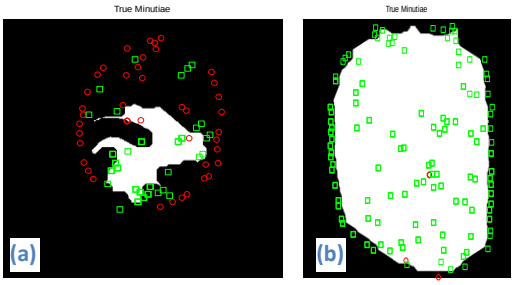
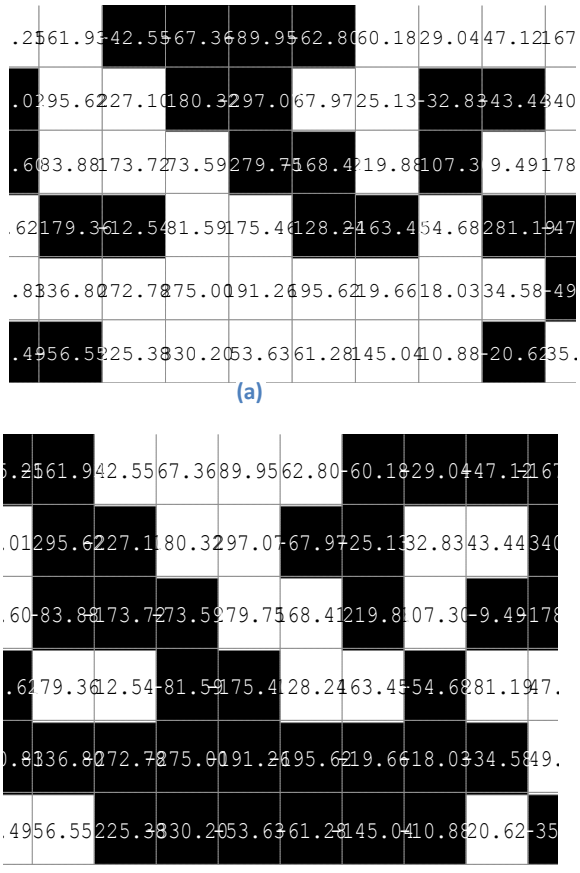


Figure 5 Minutiae Extraction (a) Before Shifting (b) After Shifting.

The bit-shifted phase values are used to perform the complex conjugate transpose on phase. Here, twin transpose is carried out. Through this twin transpose, the sign of the phase are changed. That is, change of positive sign into negative and vice versa. So the phase value gets changed. Figure 6 clearly shows the change of sign of individual pixels.



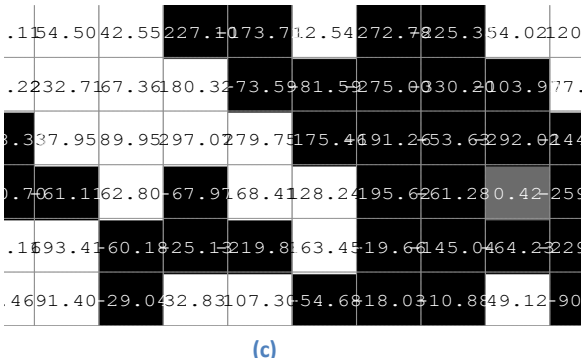


Figure 6 the complex conjugate phase transform technique (a) Before complex conjugate Transpose of an image (b) First level complex conjugate Transform (also called Hermitian transpose) transpose (Row and Column pixels are transposed and sign values are changed) (c) Second level transpose (Row and Column pixels are transposed and not the sign); compare the sign of each pixel of fig. (a) and (c) :**Pixels of Fig (a): 11.0370; 28.9340; 237.7815; 194.9182; -333.0076; -8.8610. Pixels of Fig (a): -11.0370; -28.9340; -237.7815; -194.9182; 333.0076; 8.8610.**

Through this experiment, 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 proves that one-into-many property. That is the single person's fingerprints are allowed to generate multiple transformed versions of the original image. Due to this property, a person's biometric can be used for more than one application. Hence, the cancelable property is proved.

4.2 Strength against an invertible attack

The second criterion to be considered is strength against an invertible attack. The primary objective of the proposed method is Non-inevitability (Irrevocability). This method makes it impossible to invert the transformed version of the minutiae into the original 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.

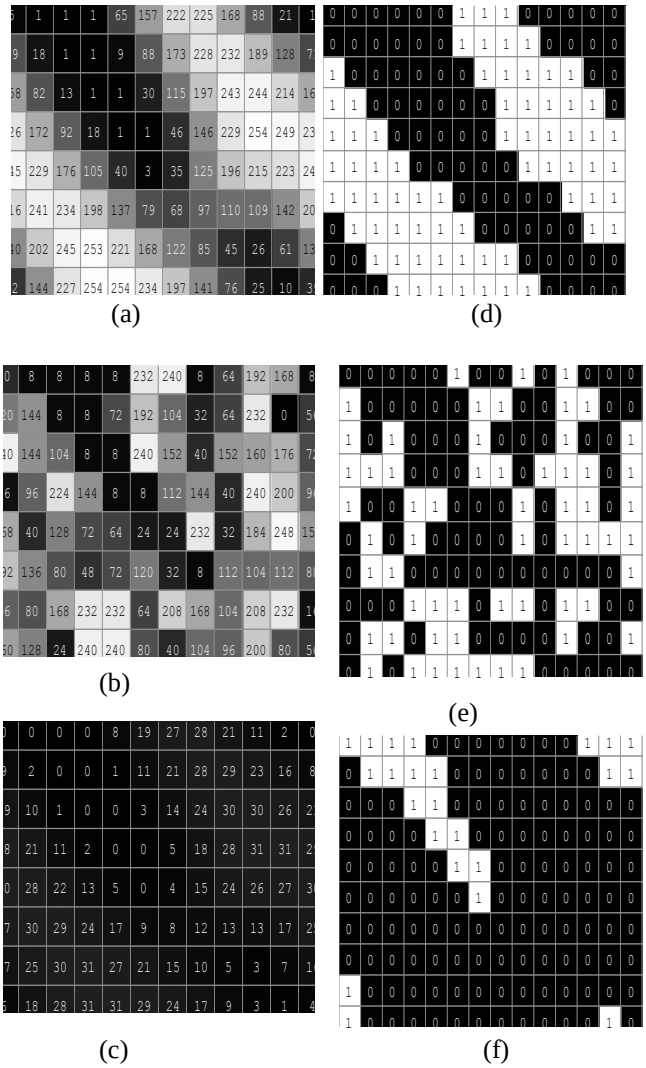


Figure 7 comparisons of images according to shifting and reverse shifting process (a) original gray image (b) N-bit Shifted gray image (c) Reverse shifting of (b) to get original image pattern (d) Original Binary image (e) N-bit shifted binary image (f) reverse shifting of (e) to get original binary image (d).

Our method focuses only on the phase minutiae which will not be used for the derivation of original features; and also the complex conjugate twin-transpose changes the sign value of each pixel. Here, the change of sign makes major changes in properties of an image. For instance, pixel value 86 is changed into -86 and -333 into 333. 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 7 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 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. 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 Distinctiveness

The third constraint is the individuality of the templates which is checked by using the correlation factor and also matching scores. The transformed version should not be correlated with the original one. The distinctiveness is proved in the experiments. That is to ensure whether the original fingerprint and the transformed version are correlated or not. To prove this phenomenon, we performed the transformations on the database sets individually and compared the original fingerprint image with transformed version. 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 as in fig.8 shows the distinctiveness of both original image and its unique transformed version. If the two images are not same then its correlation factor is zero or negative number otherwise 1.

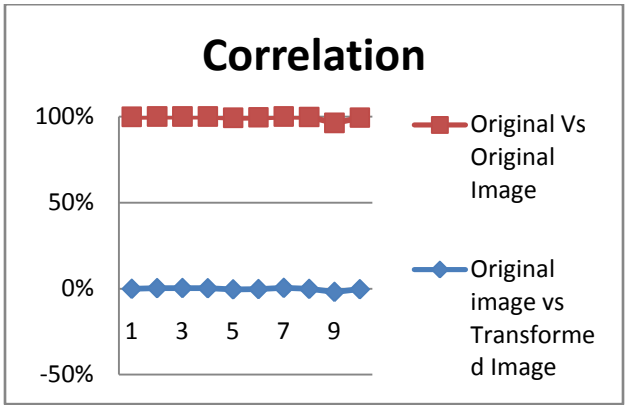
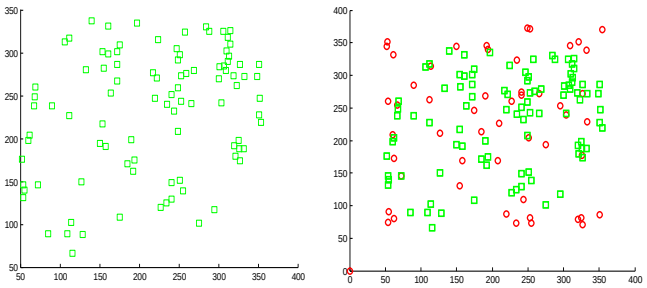


Figure 8 correlations between Original and the transformed version of the same image

4.4 Performance of the choice of parameters

The choice of parameters always boosts the performance. Conjugate Twin transpose, Chaff points and shuffling minutiae are the parameters of the proposed method. The potency of the parameters leads both cancelability and irrevocability. The chaff points generated are derived from the addition of the floating point values with the extracted bit-shifted and complex conjugate transposed phase image randomly along with the shuffling parametric keys such as X and Y coordinates. Identification of chaff points is not easy in our case. The shuffled minutiae set contain both the synthetic and conjugate phase minutiae as shown in fig. 9. So the separation or filtering of true minutiae is not possible. Hence, the performance of the choice of parameters are strengthen and sensitive.



(a) (b)

Fig 9 (a)Extracted final shifted and conjugate phase- minutiae set (b) Chaff (synthetic) minutiae in association with shuffled final shifted and conjugate phase-minutiae .Chaff points are indicated by circle and shifted conjugate phase-minutiae are indicated by square

5. Performance Evaluation of Proposed Method

The performance of the proposed complex conjugate 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), Minutia-based (Local minutiae structures) [33], [41] and hybrid method such as local and global based [42]. Minutiae based matching (through the visual difference and correlation) method is followed in our proposed work to match the cancelable templates Figure 10 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).

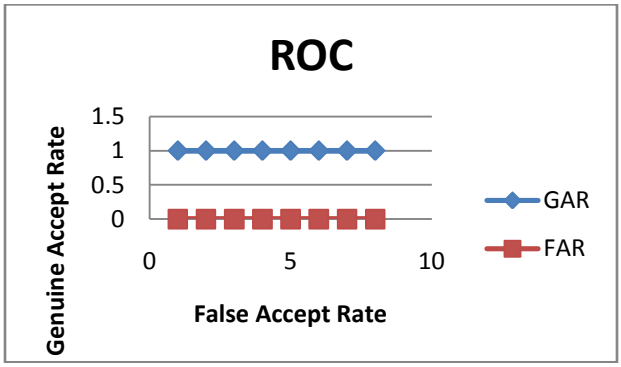


Figure 10 ROC on Cancelable transforms performance

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.

5.1 Space Complexity

Since the cancelable template possesses selective minutiae point, it occupies very less space in memory than the raw image. Table 3 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 11 shows the space complexity plot.

Table 3 Memory space of an image and cancelable biometric template

	Fingerprint Image		Fingerprint Template	
Image #	Size of Image (KB)	Size on disk (KB)	Size of template in bytes	Size on disk (KB)
1	142	144	1045	4
2	142	144	671	4
3	142	144	594	4
4	142	144	781	4
5	142	144	847	4
6	142	144	770	4
7	142	144	671	4
8	142	144	693	4

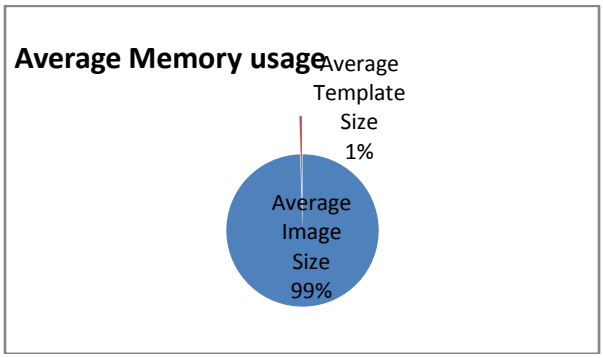


Figure 11 space complexity: Maximum amount of memory is used by an image and less amount of memory by Template

5.2 Time Complexity

Time complexity is also considered as an evaluation factor. Table 4 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 26.37 seconds in Intel i3 processor which is shown in fig. 12 . In accumulation to that the average matching time is also calculated (0.00677 seconds). The matching time is calculated exclusively.

Table 4 average template generation and matching time

Image #	Template Generation time in seconds	Template Matching Time in seconds
1	19	0.016
2	26	0.001
3	28	0.0016
4	27	0.001
5	27	0.0016
6	29	0.001
7	25	0.016
8	30	0.016
Average Time	**26.375**	**0.006775**

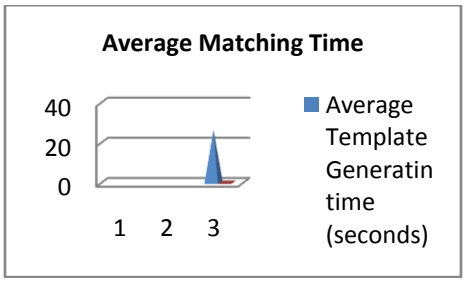


Figure 12 Average matching times of Template generation and Matching

5.3 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 shifted and complex conjugated phase minutiae (twin transposed) to generate template and the same is stored not the original features; Furthermore, it follows one-way approach (irrevocable) as described in section 5. Due to this property, the original image or features can't be derived. The phase contains only very little image feature information but most of the sensitive features of an image are based on magnitude. 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.

6. Summary And Conclusions

A novel cancelable and irrevocable biometric template generation method is designed and introduced. The proposed method: complex conjugate phase Transform is assessed in different aspects like Cancelability, Irrevocability and Security. In addition to that, average time of biometric template generation and matching are also calculated. Maximum memory usage of the biometric template is also calculated. The results show that proposed complex conjugate phase transform achieves a better performance and it is observed as an efficient method.

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, N0. 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, 2011,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, pp174-188, 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. Viellhauer, R. Steinmetz, and A. Mayyerhofer, " 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, NewSheilding 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 DC.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. Makkermans, 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 ane 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: A New Human-Secuirty Interface (Transcript of Discussion), LNCS, Springer, Vol. 4631/2007, pp. 133-138, 2007.

[28] K.Kanagalakshmi and E.Chandra, 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, 2011, 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 Filer 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. 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.

[38] Salvador Mandujano and Rogelio Soto, Deterring Password Sharing: User Authentication via Fuzzy c-Means Clustering Applied to Keystroke Biometric Data, Proc. of the fifth Mexican International Conference in Computer Science (ENC'04), 2004.

[39] Jun Gao, Huo-ming Dong, Ding-Guo Chen, Long Gan, Wen-Wen Dong, Research on Synergetic Fingerprint Classification and Matching, Proceedings of the Second International Conference on Machine Learning and Cybernetics, 2003.

[40] Sen Wang Wei Wei Zhang and Yang Sheng Wang, Fingerprint Classification by Directional Fields, Proceedings of the fourth IEEE International Conference on Multimodal Interfaces (ICM'02), 2002.

[41] Anil .K. Jain, Hong L., Bolle.R, On-line fingerprint Verification, IEEE Trans. On Pattern Analysis and Machine Intelligence, Vol. 19, No. 4, 302-313, 1997.

[42] Ross.A, Anil K. Jain, Reisman.J, A Hybrid Fingerprint Matcher, Pattern Recognition, Vol. 36, No. 7, 1661-1673, 2003.

Ms.K.Kanagalakshmi, completed her B.Sc. in Madurai Kamaraj University, Madurai, and MCA degree in Bharathiar University, Coimbatore, and M.Phil Degree in Madurai Kamaraj University, Madurai. She is working as an Assistant Professor in the Department of Computer Science, Vidyasagar College of Arts and Science, Udumalpet, Thirupur (DT), Tamilnadu. She is a Doctoral research scholar of DJ Academy, Coimbatore. She has produced two M.Phil Scholars and four are under guidance. She has presented 30 papers in National and International conferences and published 4 papers in International Journals. Her Area of research is Biometrics and security. Other areas of interest are Computer and Information Security, Image Processing. She is an Associate Member of CSI.

Dr.E.Chandra received her B.Sc., from Bharathiar University, Coimbatore in 1992 and received M.Sc., from Avinashilingam University, Coimbatore in 1994. She obtained her M.Phil, in the area of Neural Networks from Bharathiar University, in 1999. She obtained her PhD degree in the area of Speech recognition system from Alagappa University Karikudi in 2007. At present she is working as a Director in the PG Department of Computer Applications at Dr.S.N.S Rajalakshmi College, Coimbatore. She has published more than 30 research papers in National, International journals and conferences. She has guided more than 30 M.Phil, research scholars. She produced one Ph.D. Scholar. Her research interest lies in the area of Data Mining, Artificial intelligence, neural networks, speech recognition systems and fuzzy logic. She is an active member of CSI, Currently management committee member of CSI, Life member of Society of Statistics and Computer Applications.