Global Journal of Computer Science and Technology
Graphics & Vision
Volume 13 Issue 6 Version 1.0 Year 2013
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Novel Technique for Cancelable and Irrevocable Biometric Template Generation for Fingerprints

By K. Kanagalakshmi & Dr. E. Chandra
DJ Academy for Managerial Excellence, India

Abstract - Cancelable biometric key generation is vital in biometric systems to protect sensitive information of users. A novel technique called Reciprocated Magnitude and Complex Conjugate-Phase (RMCCP) transform is proposed. This proposed method comprises of different components for the development of new method. It is tested with the multiple aspects such as cancelability, irrevocability and security. FVC database and real time datasets are used to observe the performance on Match score using ROC, time complexity, and space complexity. The experimental results show that the proposed method is better in all the aspects of performance.

Keywords : *cancelability, conjugate transpose, irrevocability, phase, reciprocate, shifting.*

GJCST-F Classification : *I.4.8*

Strictly as per the compliance and regulations of:

A Novel Technique for Cancelable and Irrevocable Biometric Template Generation for Fingerprints

K. Kanagalakshmi [α] & Dr. E. Chandra [σ]

Abstract - Cancelable biometric key generation is vital in biometric systems to protect sensitive information of users. A novel technique called Reciprocated Magnitude and Complex Conjugate-Phase (RMCCP) transform is proposed. This proposed method comprises of different components for the development of new method. It is tested with the multiple aspects such as cancelability, irrevocability and security. FVC database and real time datasets are used to observe the performance on Match score using ROC, time complexity, and space complexity. The experimental results show that the proposed method is better in all the aspects of performance.

Keywords : cancelability, conjugate transpose, irrevocability, phase, reciprocate, shifting.

I. Introduction

Cancelable biometrics involves in repeated distortion of biometric signals or features on the noninvertible transforms. This approach reduces the compromise of the stored templates [43] using the substitution of transformed version of an image instead of original. It is very useful when a person is contributed with various applications. These kinds of approaches are used for the authentication [44] and identification purposes [37] [7]. Biometric based applications guarantee numerous security risks [3]. The brute- force attacks [47] 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]. Cancelable biometric provides a perfect secrecy [45], [50]. The rest of the paper comprises are as follows: section 2 lists and describes the related fields. In section 3, a novel method is proposed. Experimental studies are followed and they are expressed in section 4. Performance evaluations are described in section5. Section 6 concludes the paper.

Author α : Doctoral Research Scholar, Department of Computer Science, DJ Academy for Managerial Excellence, Coimbatore, Tamilnadu, India. E-mail : kkanagalakshmi@gmail.com

Author σ : Supervising Guide, Dr.SNS Rajalakshmi College, Coimbatore, Tamilnadu, India. E-mail : crcspeech@gmail.com

II. 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:

a) 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], [46], [48], [49] and Non-invertible approach [1]. Our proposed method falls under this category of Non-invertible transformation.

b) 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].

c) Hybrid Approach

It follows both the transformation and cryptosystems; and also fuzzy schemes [18], [22], [25], [26], [38], [49].

III. Proposed Method

A novel method is proposed in this section. It is name as Reciprocated Complex Conjugate-Phase transform method.

It includes the building blocks of phases such as preprocessing, minutiae extraction, post processing and cancelable and irrevocable template generation. The proposed method uses fingerprint biometric to generate cancelable template. Based on the significant properties such as persistence and individuality, the fingerprint features are widely used [6], [39]. Specifically our proposed method uses local features of fingerprints like bifurcations and endings [40] for the template generation. The System level design of the proposed method is given in figure 1.

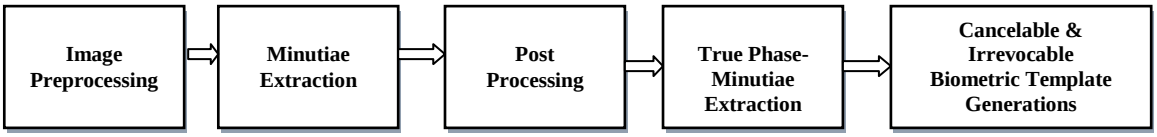


Figure 1 : System Level Design

The flow graph of the proposed method is given in figure 2 which includes main flow. Results of each stage are passed to the next level for further process. They are described in the following section.

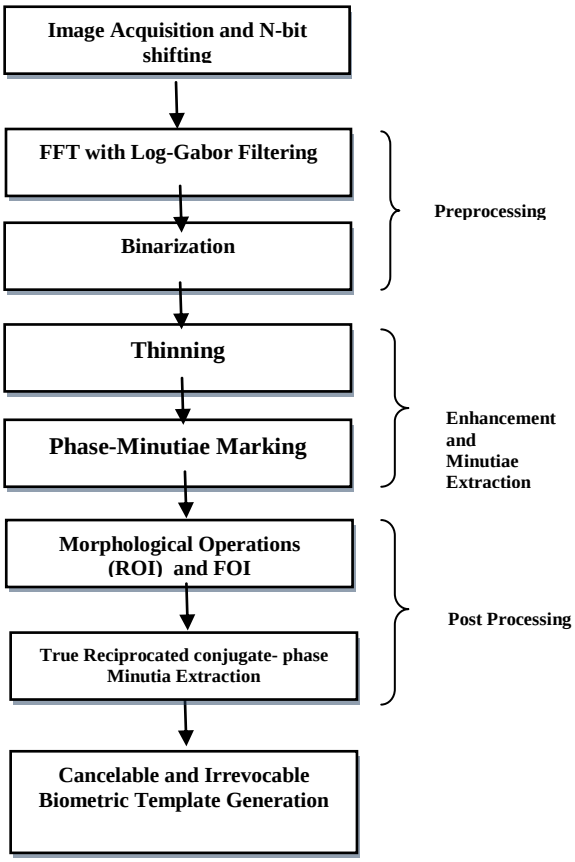


Figure 2 : Flow graph of the proposed system

Before going to design a method, the requirements and principles must be set. There are two main principles: cancelability and irrevocability. To achieve those, some conditions are followed [1]:

1. The transformation should be even while changing minutia position before transmission which leads to a small change in the minutiae position of after transformation.
2. The transformation should not lead the correlation of minutiae before and after transformation. That is the minutiae before transformation should not be matched with the minutiae after transformation
3. There should be high complexity in minimal transformations.

a) Reciprocated Magnitude and Complex Conjugate Phase (RMCCP) Transform Method: Function Design

The Reciprocated Complex Conjugate Phase transform is a proposed method which aims at the cancelability and irrevocability (One-way approach). To meet the objectives, various processing and minimal transformations are followed:

1. Initially the proposed method follows the N-bit shifting of an input fingerprint image as shown in eqn. 1.

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

Where n is a positive natural number. Shifting returns an image I(x,y) shifted by n bits. The Shn function shifts the pixel value of each coordinates of an image N times.

2. The next level is the preprocessing and an enhancement. Image enhancement can be carried out in spatial [28], [29], [30] or frequency domain [31], [32]. The proposed method focuses only frequency domain enhancement. The frequency values are obtained by applying the Fast Fourier Transformations on the shifted image using equations 2 and 3.

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

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

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

a) The Radial component: It controls the frequency band that the filter responds. Radial component of Log-Gabor function is:

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

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: It controls the orientation that the filter responds to.

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

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

$$LGF(f) = LG(f) \times FC \tag{6}$$

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

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

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

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

The x(j) is the function which returns an enhanced version of the shifted image. The output image is a complex image. By passing the enhanced cum shifted complex image to the next level, a new transformed version of an image is retrieved with the addition of reciprocated magnitude and the twin complex conjugate transposed phase image(see eqns. 9 and 10). Minutiae of the transformed version of an image are marked using Run-Length Coding method and performed post-processing. Then the RMCCP transformed minutiae (X, Y) of Terminations and Bifurcations only are extracted

$$X` = (1/M\,(x(i,j)) + [Kcos[\Phi_F\,(x(i,j))]']' \tag{9}$$

$$Y` = (1/M\,(x(i,j) + [Ksin[\Phi_F\,(x(i,j))]']' \tag{10}$$

where M is the magnitude and ΦF is the phase value of an image; X` and Y` gets the reciprocated magnitude and complex conjugate phase transposed values.

3. In third step, two parameters such as shuffling and chaffing are used. That is the extracted RMCCP 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).

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

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

Where and are the X and Y coordinate points of bifurcations respectively; and are the different floating point constants; and n1, n2 are positive integers.

4. From third step, finalized cancelable and irrevocable biometric template is generated (see table 1).

Table 1 : Cancelable and irrevocable biometric template generated from fingerprint

Bifurcations	
X	Y
285	129
85	109
275	114
175	227
234	241
54	255
.	.
.	.
.	.

IV. Experimental Study and Results

Sequence of experiments is followed to test the phenomenon of cancelability and irrevocability on the proposed method using 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.

Experiment 1 : Performance impact on cancelability

Cancelability leads multiplicity. The first criterion is cancelability of fingerprint. From the experiment, it is observed that the cancelability is trailed in the proposed method. The transformations are based on the cancelability of the biometrics. The transformed version of the image does not coincided with the original image. Multiple transformations are applied on it. No one is coincided with the original one. It seems that the product of multiple versions of the same image. The proposed RMCCP 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; additionally reciprocated magnitude and complex conjugate-phase of an image is derived. In association to that, chaff point and shuffling of the same are also implemented. Fig 3 shows the ridge patterns and their orientations before and after bit-shifting and also the RMCCP transformed image.

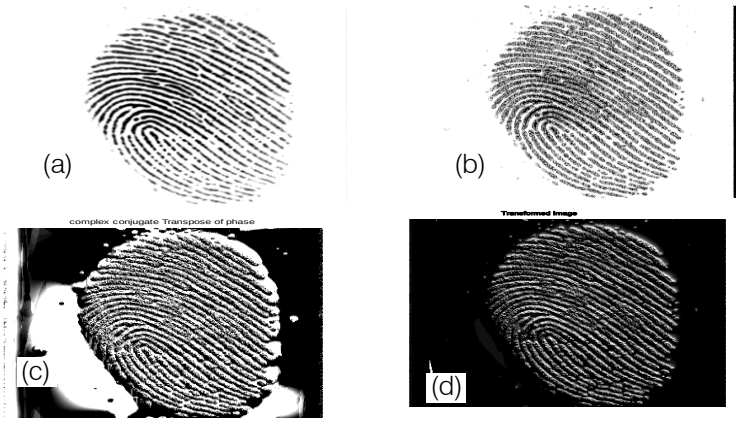


Figure 3 : Image comparison (a) Fingerprint image before shifting (b) N-bit Shifted image (c) Twin complex conjugate phase image (d) RCCP Transformed image

Figure 4 : Shows changes occurred among the pixels. It is clearly shown that the pixel value before and after shifting is varied

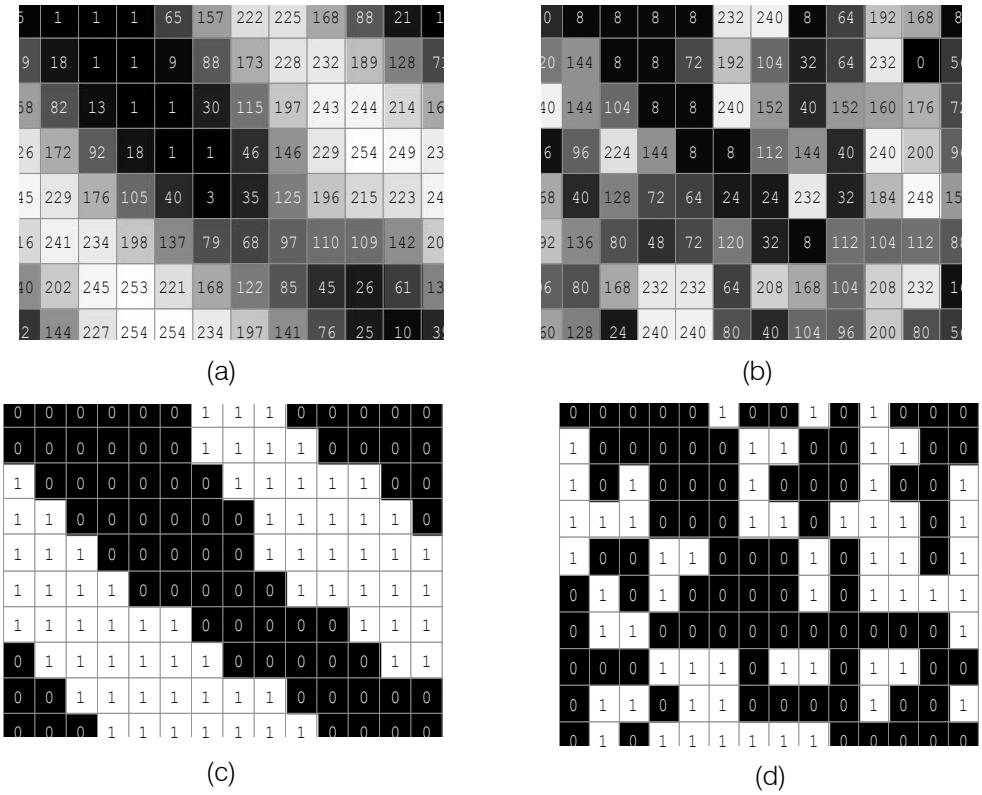


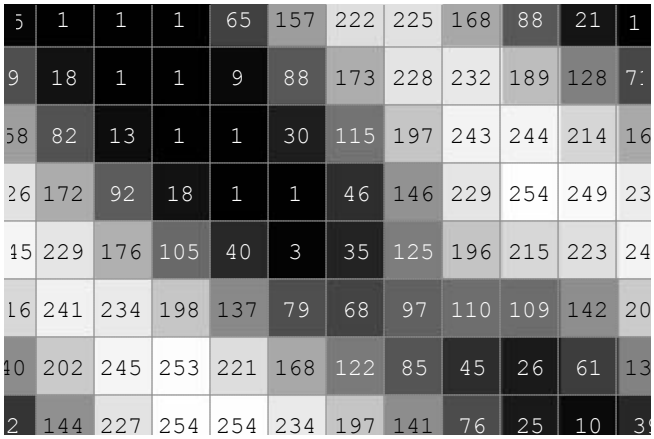
Figure 4 left Column figures (a and c) are the respective original gray and binary pixel values of an image before shifting; right column figures (b and d) are their N-bit shifted gray and binary pixel images respectively. By referring binary pixel values, it clearly visualizes the orientations of ridges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

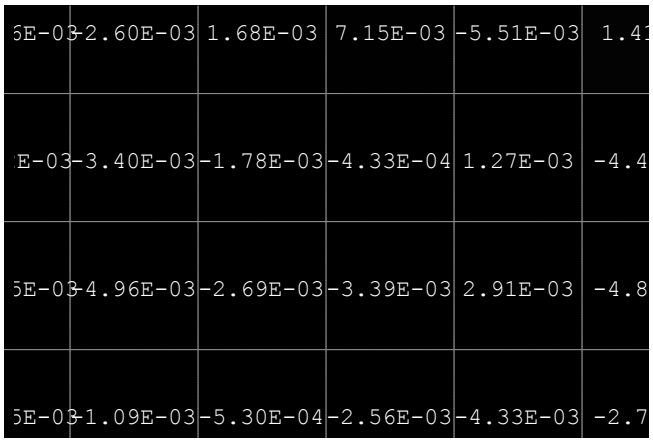
Experimental Result 1

It is observed that N-bit shifting causes scattered pattern as well as change of pixel values; if they are under RMCCP transform, then there is an occurrence of tremendous version transfer. Here, the reciprocal of the magnitude and the twin complex conjugate transpose makes a robust key for

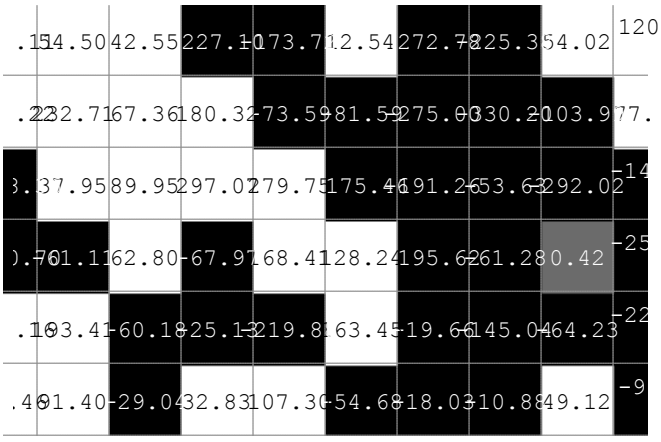
cancelability of the fingerprint features. Through the reciprocated magnitude, the originality of magnitude is affected and the same is combined with twin transposed phase where the sign of the phase is changed. That is, change of positive sign into negative and vice versa. So the phase value gets changed. This strategy further strengthens the cancelability. Figure 5 clearly shows the change of sign of individual pixels.



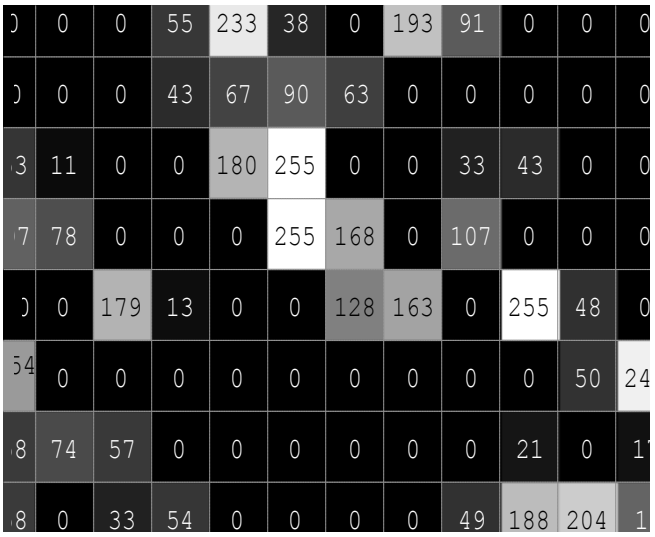
(a)



(b)



(c)



(d)

Figure 5 : Pixel regions of the RCCP transformation stages (a) Original image (b) Reciprocal magnitude (c) twin transposed (d) Final RCCP Transformed output

In summary of 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.

Experiment 2 : Strength against an invertible attack

Analyzing the strength of the invertible attack is the second criterion. Invertible attacks are impossible according to proposed method. Because it is aimed at one way approach that is non-invertible approaches. It extracts minutiae from the transformed version which is acquired from reciprocated magnitude and twin complex conjugate-phase combinations. The phase possesses very less sensitive information of an image. But the magnitude possesses all sensitive values (information) of an image. Our method focuses only on the reciprocated magnitude which results reciprocal of the original magnitude and twin complex conjugate-phase minutiae which changes the sign value of each pixel. Here, the change of magnitude and sign makes major changes in properties of an image. For instance, the original magnitude 178 is reciprocated into 0.0056 and 0 into -0.0030; according to Phase value, 52 is changed into -52 and -90 into 90 etc. This property integrates robustness and irrevocability of original features from the stored RMCCP -minutiae templates. Moreover the template is accumulated with only two

fields such as shifted and transformed locations: X and Y coordinate. While storing the coordinates, they are shuffled and added chaff points. This attempt also makes additional feature for the irrevocability.

Experimental Results 2

Figure 6 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 and 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.

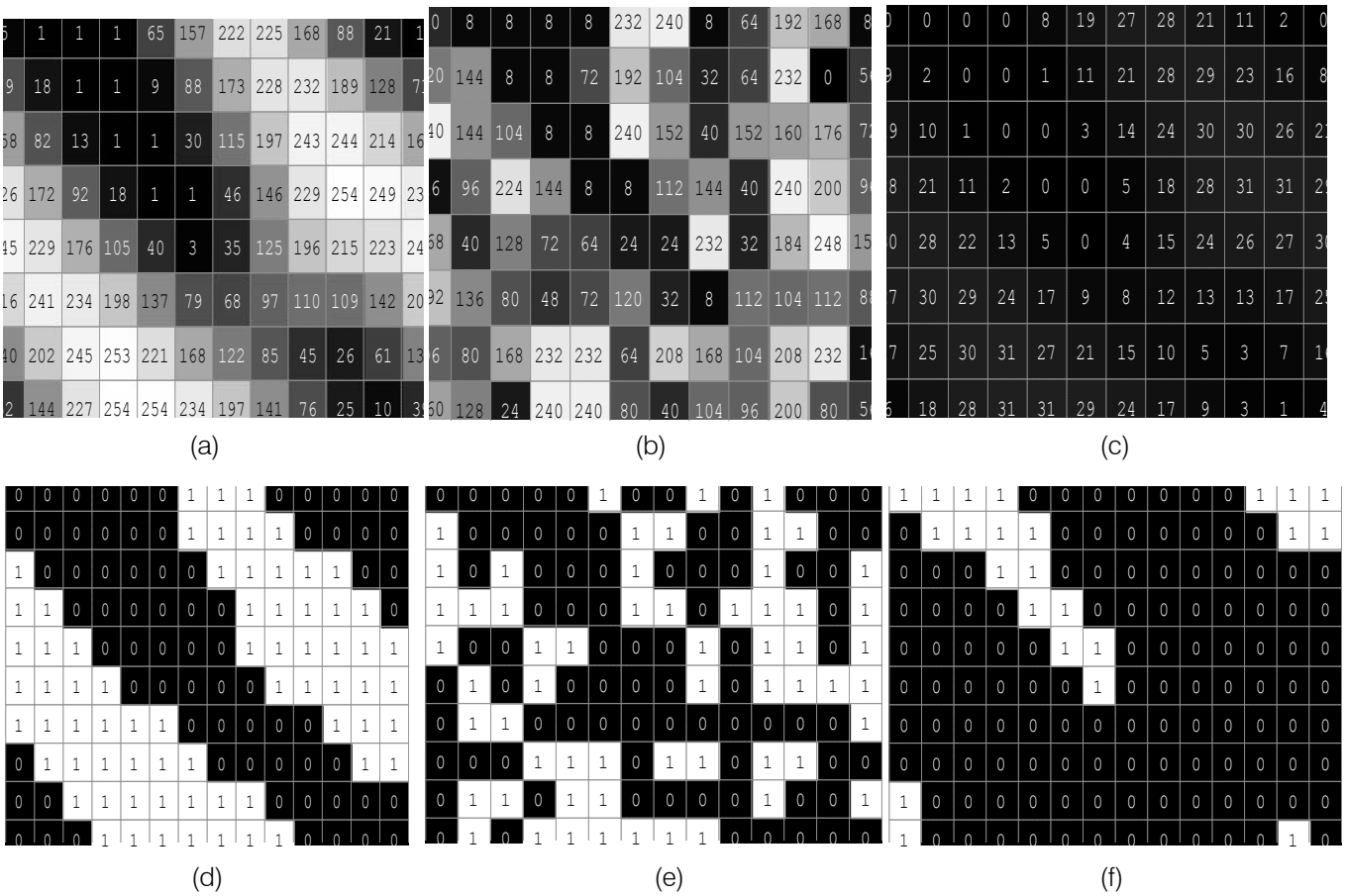


Figure 6 : Comparisons of images according to shifting and reverse shifting process (a) Original gray image (b) Nbit Shifted gray image (c) Reverse shifting of (b) To get original image pattern (d) Original Binary image (e) N-bit shifted binary image (f) Reverse shifting of (e) To get original binary 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)

Experiment 3 : Distinctiveness

The third constraint to be considered is distinctiveness of the templates which is checked by using the correlation factor and also matching scores. The transformed version of an image 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 against transformed version; and also the test is extended on transformed versions of the inter fingerprint images.

Experimental Result 3

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 (see fig.7) 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.

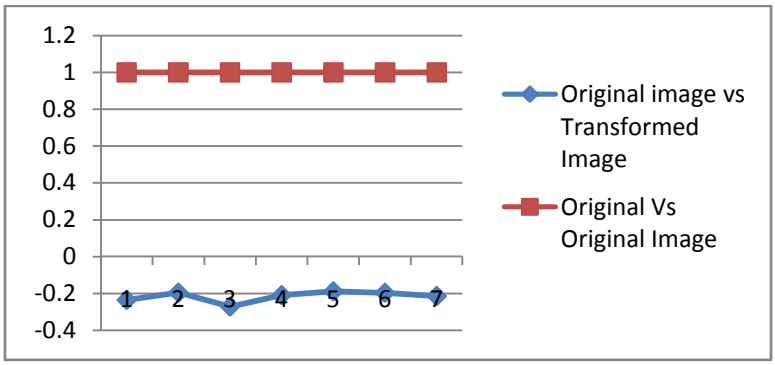


Figure 7 : Correlation chart: correlation between Original and the transformed version of the same image

a) 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 (see fig. 8). So the separation or filtering of true minutiae is not possible. Hence, the performance of the choice of parameters are strengthen and sensitive.

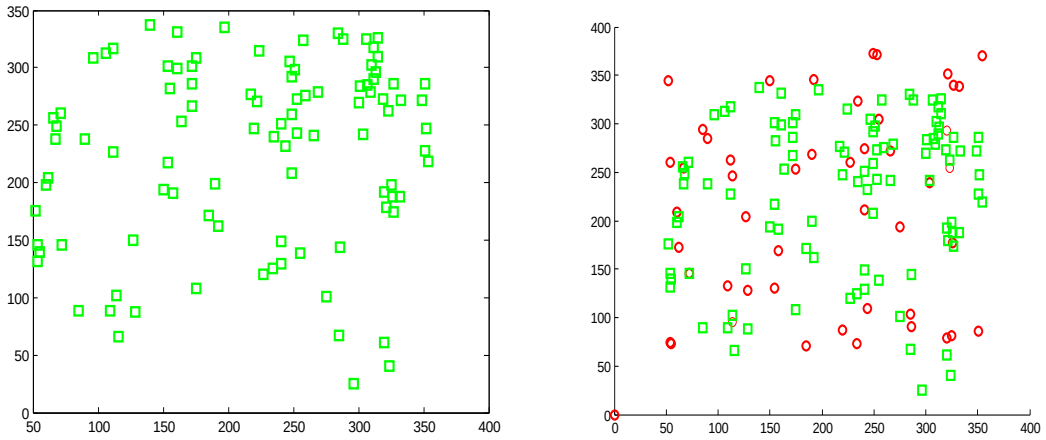


Figure 8 : (a) Extracted final shifted and RCCP-minutiae set (b) Chaff (synthetic) minutiae in association with RMCCP-minutiae. Chaff points are indicated by circle and shifted conjugate phase-minutiae are indicated by square

V. Performance Evaluation of Proposed Method

The performance of the proposed RMCCP 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 9 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).

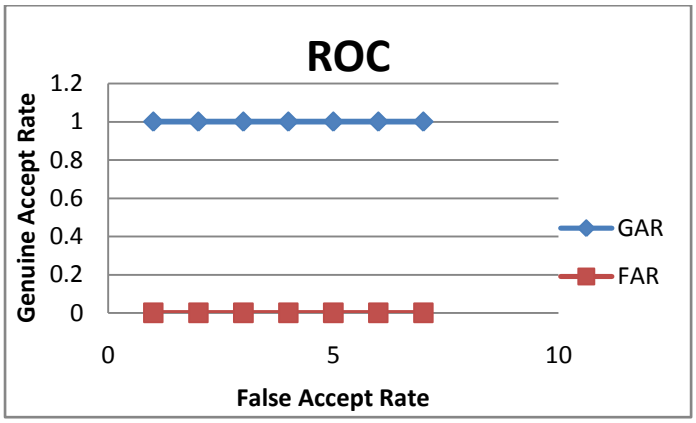


Figure 9 : ROC on Cancelable transforms performance

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.

a) Space Complexity

Normally more memory spaces are occupied by images. In order to decrease the memory usage of biometric fingerprint images, the proposed method generates only the template with dual fields such as X and Y coordinates. Since the cancelable template possesses selective minutiae point, it occupies very little space in memory than the raw image. The average ratio of memory space between biometric template and raw image is about 0.005 only. Table 2 reports the memory space required to store the original image and the cancelable biometric template of fingerprints. Figure 10 shows the space complexity chart.

Table 2 : Memory space of an image and cancelable

	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	1078	4
2	142	144	693	4
3	142	144	638	4
4	142	144	836	4
5	142	144	836	4
6	142	144	858	4
7	142	144	792	4
Average	142	144	**818**	4

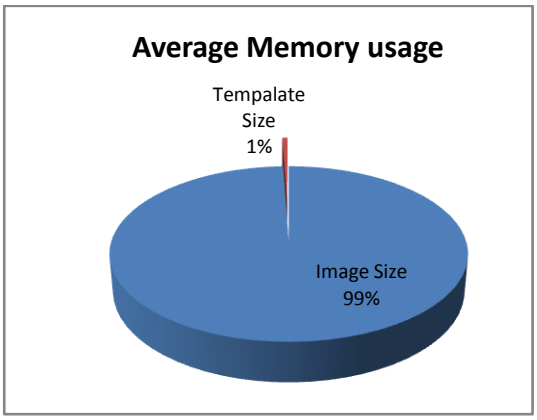


Figure 10 : Space complexity: Maximum amount of memory is used by an image and less amount of memory by template

b) Time Complexity

Performance of the method is measured in term of time complexity. The response time of the system is very important factor which integrates the performance of a system. An Average matching and template generation time is calculated (Intel i3 processor) which are reported in table 3.

Table 3 : Average template generation and matching time Image #

Image #	Template Generation time in seconds	Template Matching Time in seconds
1	19	0.001
2	25	0.016
3	28	0.0016
4	26	0.035
5	27	0.015
6	30	0.015
7	25	0.016
Average Time	**25.71**	**0.014229**

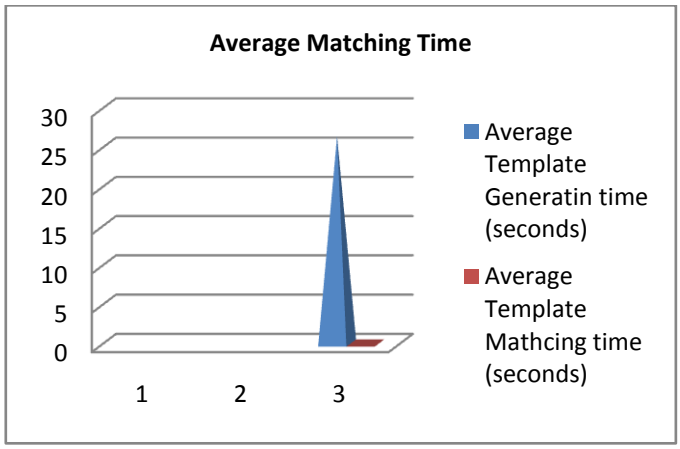


Figure 11 : Average Matching Times of Template Generation and Matching

c) Security

Preserving the stored template is a hotspot of the automatic biometric based authentication and identification systems. 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. The RMCCP transformation is performed only with the version transform of the existing features values; chaff point generation is also done with only the internal feature value transformation. 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 employs shifted and reciprocated magnitude with conjugated phase values. It creates a robust bond with one-way approach which will not be permitted the hackers to generate an original image from the transformed version's properties. The partial and transformed minutiae are helpless to derive an original image. Thus, the proposed method offers a robust and secured system.

VI. Conclusions

A novel method called Reciprocated Magnitude and Complex Conjugate-Phase transformation is proposed and implemented. It is a cancelable and irrevocable biometric template generating technique. It is assessed in different facets like Cancelability, Irrevocability and Security. In addition to that, the performance factors such as matching time and template memory usage are calculate and analyzed. The experimental results show that proposed RCCP transform gives a better performance and it is experienced as an efficient method.

References Références Referencias

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, 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. 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 effectively, IEEE Transactions on Computers, Vol. 55, No. 9, 2006.
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.
43. Feng, Y.C., Yuen, P.C. and Jain, A.K., A Hybrid Approach for Face Template Protection, SPIE Defense and Security Symposium, Vol. 102, No. 2, pp. 169-177, 2008.
44. Xinyi Huang, Yang Xiang, Chonka. A, Jianying Zhou and Deng. R.H, A generic frame work for Three-Factor Authentication: Preserving security and privacy in distributed systems, IEEE Transactions on Parallel and Distributed systems, Vol. 22, No. 8, pp. 1390-1397, 2011.
45. Hirata, S. and Takahashi, K., Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching, Lecture Notes in Computer Science, Vol. 5558, pp. 868-878, 2009.
46. Teoh, A. B. J.; Yip, W. K. and Lee, S. Y., Cancellable Biometrics and Annotations on BioHash, Elsevier - Pattern Recognition Vol. 41, No.6, pp. 2034-2044, 2008.
47. Shin, S. W.; Lee, M.-K.; Moon, D. S. and Moon, K. Y., Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates, ETRI Journal, Vol. 31, No.5, pp. 628-630, 2009.
48. Nanni, L. and Lumini, A., Random Subspace for an improved BioHashing for Face authentication, Elsevier - Pattern Recognition Letters, Vol. 29, No. 3, pp. 295-300, 2008.
49. Kong, B. et al., An analysis of Biohashing and its variants, Elsevier - Pattern Recognition, Vol. 39, No. 7, pp. 1359-1368, 2006.
50. Lee, C. H.; Choi, C. Y. and Toh, K. A., Alignment-Free Cancelable Fingerprint Templates Based on Local Minutia Information. IEEE Transactions on Systems, Man and Cybernetics, Part B, vol. 37, no. 4: 980-992, 2007.

This page is intentionally left blank