Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

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

K.Kanagalakshmi[1]

[1] DJ Academy for Managerial Excellence, Coimbatore

Received: 11 December 2012 Accepted: 5 January 2013 Published: 15 January 2013

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..

Index terms— cancelability, conjugate transpose, irrevocability, phase, reciprocate, shifting.

1 Introduction

ancelable 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.

2 II.

3 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 Noninvertible transformation.

4 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].

5 c) Hybrid Approach

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

6 III.

7 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 (D D D D D D D D) 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. 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) 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.

()**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.

FFT:

(

Where ? 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: Cancelable and Irrevocable Biometric Template Generation 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.

()**2**

Where r is the normalized radius from centre, 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.

() N rf o**5**

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

8 (6)

Now, the filter is applied on the frequency domain for the enhancement as in eqn. 7. (7) Then, the Inverse Fast Fourier Transformation is performed to get back the original enhanced image using eqn. 8. (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 (9) (10) where is the magnitude and ?F 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).

(11) (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).

9 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 **??**000, **??**002, **??**004, 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. 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 **??**.

10 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 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.

11 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 conjugatephase 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.

12 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. 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.

13 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. 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.

14 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 [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). 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 **??** 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 **??** : Memory space of an image and cancelable 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. 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.

15 VI.

16 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.

2

Figure 1: Figure 2 :

Figure 2:

Figure 3: FA

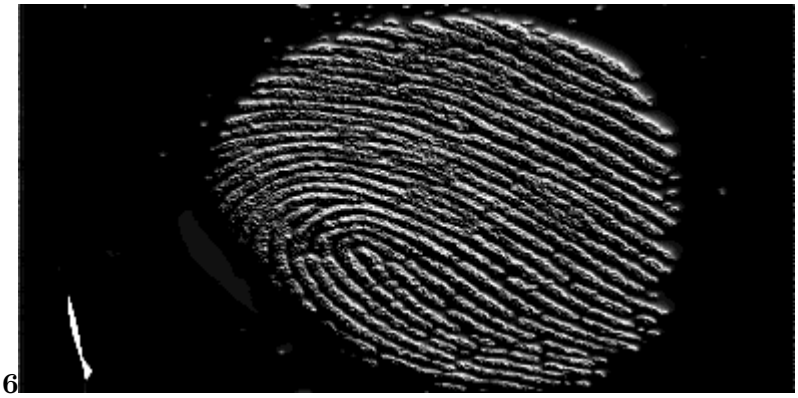
344

Figure 4: Figure 3 :Figure 4 :FAFigure 4 left

Figure 5:

5

Figure 6: Figure 5 :FA



6

Figure 7: Figure 6 :FA

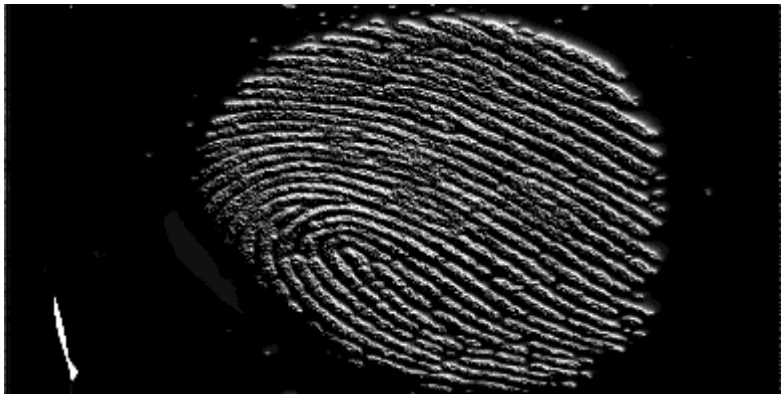
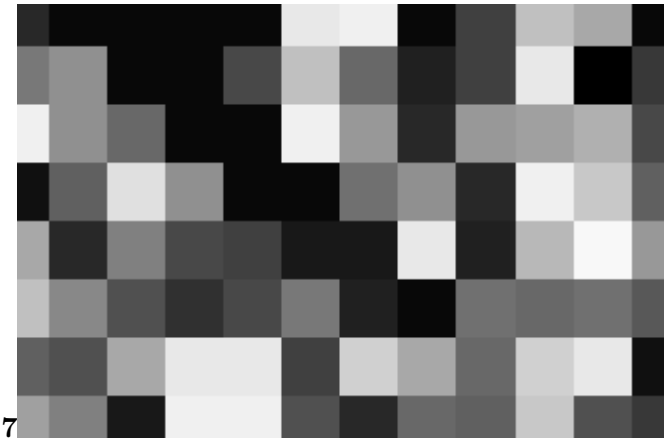
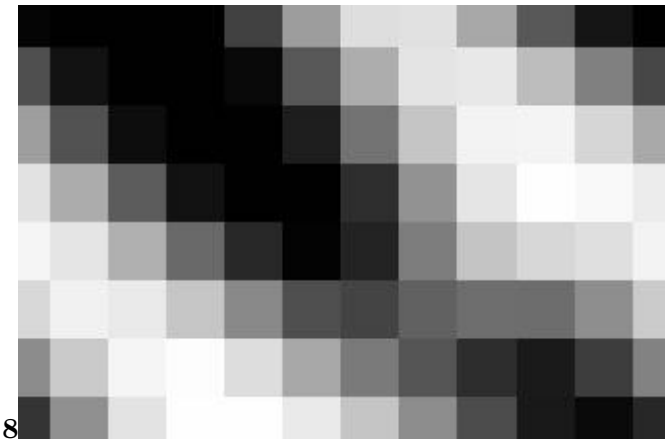


Figure 8:



7

Figure 9: Figure 7 :



8

Figure 10: Figure 8 :

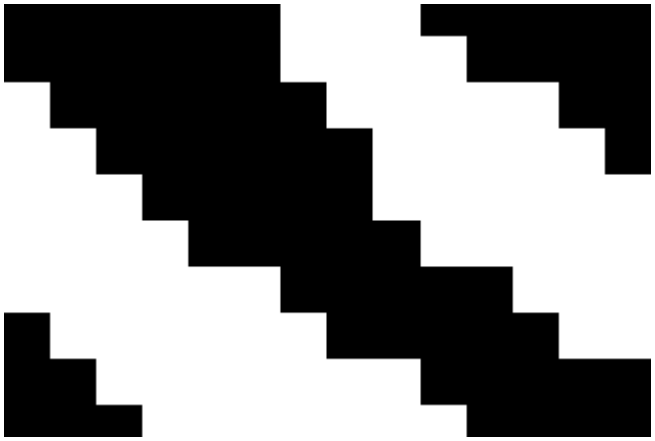
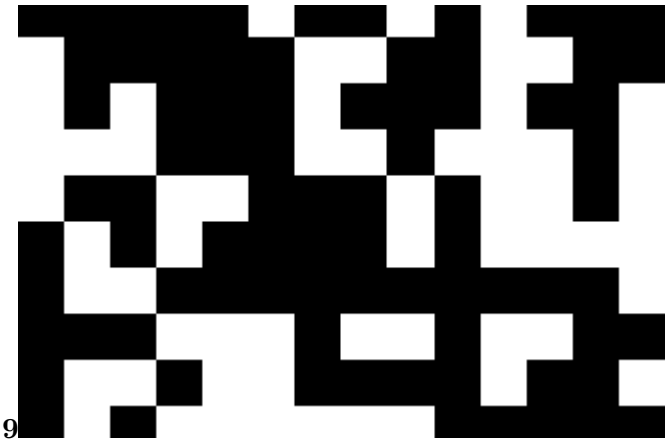
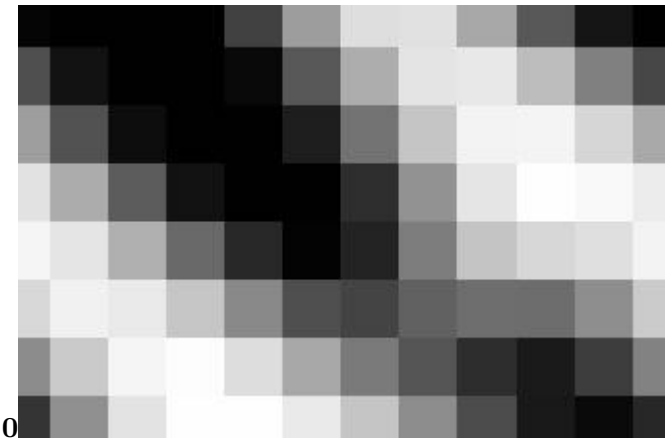


Figure 11: FA(



9

Figure 12: Figure 9 :

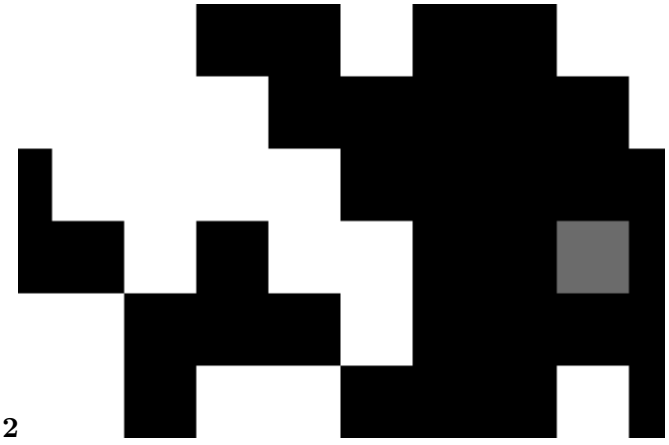


10

Figure 13: Figure 10 :

11

Figure 14: Figure 11 :



2

Figure 15: FA 2 FA

Figure 16: True Reciprocated conjugate-phase Minutia Extraction Preprocessing Enhancement and Minutiae Extraction Post Processing

1

generated from fingerprint

Figure 17: Table 1 :

3

time Image #

Figure 18: Table 3 :

[Ross et al. ()] , K A Ross , Jain , . J Reisman , Hybrid Fingerprint , Matcher . *Pattern Recognition* 2003. 36 (7) p. .

[Teoh et al. ()] , A B J Teoh , W K Yip , S Y Lee . *Cancellable Biometrics and Annotations on BioHash* 2008. Elsevier -Pattern Recognition. 41 (6) p. .

[Ruud et al. ()] , M Ruud , Jonathan H Bolle , Nalini K Connell , Ratha . *Pattern Recognition* 2727-2738, 2002. Elsevier. 35.

[Juels and Wattenberg (1999)] 'A fuzzy commitment schemes'. A Juels , M Wattenberg . *Proceedings of 6th ACM Conference on Computer and Communication Security*, (6th ACM Conference on Computer and Communication SecuritySingapore) November 1999. p. .

[Huang et al. ()] 'A generic frame work for Three-Factor Authentication: Preserving security and privacy in distributed systems'. Xinyi Huang , Yang Xiang , . A Chonka , Jianying Zhou , R Deng . *IEEE Transactions on Parallel and Distributed systems* 2011. 22 (8) p. .

[Feng et al. ()] 'A Hybrid Approach for Face Template Protection'. Y C Feng , P C Yuen , A K Jain . *SPIE Defense and Security Symposium*, 2008. 102 p. .

[Nagar et al. (2010)] 'A hybrid biometric cryptosystem for securing fingerprint minutiae templates'. Abhishek Nagar , Karthik Nandakumar , Anil K Jain . *Pattern Recognition Letters* June 2010. Elsevier Science. 31 p. .

[Sutcu et al. ()] 'A secure biometric authentication scheme based on robust hashing'. Y Sutcu , H T Sencar , N Memon . *Proc. 7th Workshop Multimedia and Security*, (7th Workshop Multimedia and SecurityNew York) 2005. p. .

[Gil et al. ()] 'Access Control System with High Level Security using fingerprints'. Younhee Gil , Sungbum Dosung Ahn , Yongwha Pan , Chung . *Proc. of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03)*, (of the 32nd Applied Imagery Pattern Recognition Workshop (AIPR'03)) 2003. IEEE.

[Lee et al. ()] 'Alignment-Free Cancelable Fingerprint Templates Based on Local Minutia Information'. C H Lee , C Y Choi , K A Toh . *IEEE Transactions on Systems, Man and Cybernetics* 2007. 37 (4) p. . (Part B)

[Kong ()] 'An analysis of Biohashing and its variants'. B Kong . *Pattern Recognition* 2006. Elsevier. 39 (7) p. .

[Australian Conf, Information Security and Privacy ()] *Australian Conf, Information Security and Privacy*, 2005. p. .

[Teoh et al. ()] 'Biohashing: Two factor authentication featuring fingerprint data an tokenized random number'. A B Teoh , D C L Ngo , A Goh . *Pattern Recognition* 2004. 37 (11) p. .

[Uludag et al.] 'Biometric Crypto systems: issues and challenges'. U Uludag , S Pankati , S Prabhakar , A K Jain . *Proceedings of the IEEE* 92 (6) p. .

[Soutar et al. ()] 'Biometric Encryption using image processing'. C Soutar , D Roberge , A Astoinav , B V K Gilroy , Kumar . *Proc. SPIE*, (SPIE) 1998. 3314 p. .

[Viellhauer et al. (2002)] 'Biometric hash based on statistical features of online signatures'. C Viellhauer , R Steinmetz , A Mayyerhofer . *Proceedings of the International conference on Pattern Recognition*, (the International conference on Pattern Recognition) August 2002. 1 p. .

[Prbhakar et al. ()] 'Biometric Recognition: Security and Privacy concerns'. Salil Prbhakar , Sharath Pankanti , Anil K Jain . *IEEE Security and Privacy* 2003. 1 (2) p. .

[Ignatenko et al. ()] 'Biometric Systems: Privacy and Secrecy Aspects'. Tanya Ignatenko , M J Frans , Willems . *IEEE Transactions on Information Forensics and security* 2009. 4 (4) .

[Anil et al. (2008)] 'Biometric Template Security'. K Anil , Karthik Jain , Abhishek Nandakumar , Nagar . *EURASIP Journal on Advances in Signal Processing, Special issue on Biometrics* Jan. 2008.

[Savvides et al. ()] 'Cancelable biometric filters for face recognition'. M Savvides , B V K Vijayakumar , P K Khosla . *Proc. Int'l Conf. Pattern Recognition*, (Int'l Conf. Pattern Recognition) 2004. p. .

[Chandra and Kanagalakshmi ()] 'Cancelable Biometric Template Generation of Protection Schemes: a Review'. E Chandra , K Kanagalakshmi . *Proceedings of ICECT-2011, Third International Conference on Electronics Computer Technology*, (ICECT-2011, Third International Conference on Electronics Computer Technology) 2011. 5 p. . (Published by IEEE)

[Hirata and Takahashi ()] 'Cancelable Biometrics with Perfect Secrecy for Correlation-Based Matching'. S Hirata , K Takahashi . Lecture Notes in Computer Science 2009. 5558 p. .

[Ang et al.] 'Cancelable Key-based Fingerprint Templates'. R Ang , R Safav-Naini , L Mcaven . *Proc. 10th*, (10th)

[Hao et al. ()] 'Combining crypto with biometrics effectively'. F Hao , R Anderson , J Daugman . *IEEE Transactions on Computers* 2006. 55 (99) p. .

[Hao et al. ()] 'Combining Crypto with Biometrics effectively'. Feng Hao , Ross Anderson , John Daugman . *IEEE Transactions on Computers* 2006. 55 (9) .

[Feng ()] 'Combining minutiae descriptors for fingerprint matching'. Jianjiang Feng . *Pattern Recognition* 2008. Elsevier. 41 p. .

[Goh and Ngo ()] 'Computation of Cryptographic Keys from Face Biometrics'. A Goh , D L Ngo . *Proc. IFIP: Int'l Federation for information processing*, (IFIP: Int'l Federation for information processing) 2003. p. .

[Connie et al. ()] T Connie , A B J Teoh , M K O Goh , Dc L Ngo . *Palm Hashing: A Novel approach for cancelable biometrics*, 2005. 93 p. .

[Monrose et al. (2001)] 'Cryptographic key-generation from voice'. F Monrose , M K Reiter , Q Li , S Wetzel . *Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy*, (IEEE Computer Society Symposium on Research in Security and PrivacyUSA) May 2001. p. .

[Shin et al. ()] 'Dictionary Attack on Functional Transform-Based Cancelable Fingerprint Templates'. S W Shin , M.-K Lee , D S Moon , K Y Moon . *ETRI Journal* 2009. 31 (5) p. .

[Kanagalakshmi and Chandra ()] 'Frequency Domain Enhancement algorithm based on Log-Gabor Filter in FFT Domain'. K Kanagalakshmi , E Chandra . *European Journal of Scientific Research* 2012. 74 (4) p. .

[Chandra and Kanagalakshmi ()] 'Frequency Domain Enhancement Filters for Fingerprint Images: A Performance Evaluation'. E Chandra , K Kanagalakshmi . *CIIT International Journal of Digital Image Processing* 2011. 3 (16) .

[Dodis et al. (2004)] 'Fuzzy extractor: how to generate strong keys from biometrics and other noisy data'. Y Dodis , L Reuzin , A Smith . *Proceedings of International Conference of the Theory and Applications of cryptographic Techniques: Advances in Cryptology*, Lecture Notes in Computer Science (International Conference of the Theory and Applications of cryptographic Techniques: Advances in CryptologySwitzerland) May 2004. 3027 p. .

[Gao et al. ()] 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.

[Nalini et al. (2007)] 'Generating Cancelable Fingerprint Templates'. K Nalini , Sharat Ratha , Jonathan H Chikkerur , Ruud M Connell , Bolle . *IEEE Transactions and Pattern Analysis and Machine Intelligence*, April 2007. 29.

[Maltoni et al.] *Handbook of Fingerprint Recognition*, D Maltoni , D Maio , A K Jain , S Prabhakar . Springer. p. .

[Matsumoto et al. ()] 'Impact of Artificial Gummy Fingers on Fingerprint Systems'. T Matsumoto , H Matsumoto , K Yamada , S Hoshino . *Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques IV*, (SPIE, Optical Security and Counterfeit Deterrence Techniques IV) 2002. 4677 p. .

[Linnartz and Tuyls ()] *NewSheilding Functions to enhance privacy and prevent misuse of biometric templates, Proc. Fourth Int'l cong. Audio and Videobased biometric person authentication*, J P Linnartz , P Tuyls . 2003. p. .

[Chandra and Kanagalakshmi ()] 'Noise Elimination in Fingerprint Images using Median Filter'. E Chandra , K Kanagalakshmi . *Int. Journal of Advanced Networking and Applications* 2011. 02 p. .

[Chandra and Kanagalakshmi ()] 'Noise Suppression Scheme using Median Filer in Gray and Binary Images'. E Chandra , K Kanagalakshmi . *International Journal of Computer Applications* 2011. 26 (1) p. .

[Pankanti et al. ()] 'On the Individuality of Fingerprints'. Sharath Pankanti , Salil Prbhakar , Anil K Jain . *IEEE Transactions on Pattern Analysis and Machine Intelligence* 2002. 24 (8) .

[Anil et al. ()] 'On-line fingerprint Verification'. . K Anil , Hong L Jain , Bolle . *IEEE Trans. On Pattern Analysis and Machine Intelligence* 1997. 19 (4) p. .

[Yang and Busch ()] 'Parameterized geometric alignment for minutiae-based fingerprint template protection'. Bian Yang , Christoph Busch . *Proceedings of the 3rd IEEE international conference on Biometrics: Theory, applications and systems*, (the 3rd IEEE international conference on Biometrics: Theory, applications and systemsWashington, DC, USA) 2009. p. .

[Monrose et al. (1999)] 'Password hardening based on keystroke dynamics'. F Monrose , M K Reiter , S Wetzel . *proceedings of the 6th ACM Conference on Computer and Communication security*, (the 6th ACM Conference on Computer and Communication securitySingapore) November 1999. p. .

[Kanagalakshmi and Chandra ()] 'Performance Evaluation of Filters in Noise Removal of Fingerprint Image'. K Kanagalakshmi , E Chandra . *Proceedings of ICECT-2011, 3rd International Conference on Electronics and Computer Technology*, (ICECT-2011, 3rd International Conference on Electronics and Computer Technology) 2011. 1 p. . (Published by IEEE)

[Tuyls et al. (2005)] 'Practical biometric authentication with template protection'. P Tuyls , A H Makkermans , T A M Kevenaar , G J Schrijen , A M Bazen , R N J Veldhuis . *Proceedings of the 5th International Conference on Audio and Video based biometric person authentication*, Lecture Notes in Computer Science (the 5th International Conference on Audio and Video based biometric person authenticationUSA) July 2005. 3546 p. .

[Chun-I Fan Ane and Lin (2009)] 'Provably secure remote truly three-factor authentication scheme with privacy Protection on biometrics'. Yi-Hui Chun-I Fan Ane , Lin . *IEEE Transactions on Information Forensics and Security* December 2009. 4 p. .

[Nanni and Lumini ()] 'Random Subspace for an improved BioHashing for Face authentication'. L Nanni , A Lumini . *Pattern Recognition Letters* 2008. Elsevier. 29 (3) p. .

[Sardt et al. ()] 'Validating a biometric authentication systems sample size requirements'. C Sardt , Yongfang Dass , Anil K Zhu , Jain . *IEEE Transactions on pattern analysis and machine intelligence*, 2006. 28.

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