Securing Retina Fuzzy Vault System using Soft Biometrics

GJCST Computing Classification
D 4.6, I 2.3

N. Radha[1] Dr. S. Karthikeyan[2] P.Anupriya[3]

***Abstract*-The major concern of almost all the verification system is user authentication and security. This necessitates the development of a mechanism that ensures user security and privacy. A lot of research has been carried on this developing field and numerous techniques have been proposed earlier in literature. These traditional methods use tokens and passwords to provide security to the users. Uncertainly, it can be easily compromised by attackers and therefore it is significant to design verification system that ensures authentication. In recent years, technology has turned in favor of combining soft biometrics and cryptographic key generation technique. The principal feature of using soft biometric template is that it cannot be easily revoked by any unauthorized user. Most commonly used soft biometric features are iris, retina, face, fingerprint, voice and so on. Fuzzy vault is the framework which comprises of the combination of soft biometrics and cryptographic key generation technique. This fuzzy vault acts as an additional layer of security. This overcomes the limitation met by a biometrics system when implemented individually. This paper proposes a biometric verification system investigating the combined usage of soft biometrics features hardened by fuzzy vault scheme. This approach uses retina as a soft biometric since it is capable of providing best results. Experiments were conducted to investigate the performance of the proposed authentication system in ensuring the user security and privacy.**

Keywords-Authentication, Cryptography, Fuzzy Vault Scheme, Retina Feature Extraction, Retinal Soft Biometrics.

I. INTRODUCTION

Biometric technology identifies individuals automatically by using their biological or behavioral characteristics. There is growing interest in the use of biometrics for a large spectrum of applications, ranging from governmental programs to personal applications such as logical and physical access control. Since biometric properties cannot be lost or forgotten in contrast to tokens and passwords, they offer an attractive and convenient alternative to identify and authenticate user information.

The initial step of providing biometric authentication to user is enrollment. In this enrollment stage a user registers with the system where one or more measurements of user biometric data are obtained. Each such measurement is then processed by some algorithm to obtain a ―template", and stored in a database. Some of the user biometrics that is extensively used for authentication is face, fingerprint, hand geometry, keystroke dynamics, hand vein, iris, retina, signature, voice, facial thermogram, and DNA.

The use of above mentioned biometrics for recognizing individuals is becoming increasingly accepted and many applications are already accessible. These applications can be hardly classified in to one of the following two categories, verification and identification [1] [2] [3]. The verification systems validate a person's identity by comparing the captured biometric characteristic with that of person's own biometric template previously stored in the system whereas the identification systems recognize an individual by searching the entire template database for a match with the captured biometric characteristic.

The substitution of biometric features in the place of passwords provides an assortment of advantages in verification systems such as access control and so on. Although biometrics provides a variety of advantages it has some limitations. Once a biometric image or template is stolen, it is stolen forever and cannot be reissued, updated, or destroyed. An additional problem associated with the use of biometrics is that once a biometric is chosen, the same biometric will be used to access many different systems. This means that, if it is compromised, the attacker will have right to use all the accounts/services/applications of that particular user [6]. This is the correspondent of using the same password across multiple systems, which can lead to some very serious problems in terms of security. Recently, novel cryptographic techniques such as fuzzy commitment and fuzzy vault were proposed to provide a secure storage for the reference biometric template [4] [5]. The soft biometric template of the user is vault with the randomly generated key by a cryptographic framework so called ―Fuzzy Vault Scheme." This overcomes the limitation met by a biometric system when implemented individually. Moreover it improves user authentication and security.

This paper proposes a biometric verification system, exploring the combined usage of soft biometrics features hardened by fuzzy vault scheme. This proposed approach, which will have enhanced security on comparison with the traditional systems. The soft biometric feature used in this method is retina, since it has been reported to provide some of the best results for verification systems and it remains fairly unaltered during a person's lifetime. Experiments were conducted to examine the performance of the proposed authentication system in ensuring security and privacy.

The remainder of this paper is organized as follows. Section 2 discusses the related work proposed earlier in literature for soft biometric authentication systems. Section 3 explains our proposed system for providing authentication-using retina as

About-[1]Ph.D.Scholar,Department of Computer Science Karpagam University,Coimabtore-21 (e-mail-Lakshmin07@sify.com)
About-[2]Director,Department of Computer Science Karpagam University,Coimbatore-21(e-mail- skaarthi@gmail.com)
About-[3]Lecturer,MCA Department PSGR Krishnammal college for women Peelamedu,Coimabtore-4 (e-mail-anupriya@grgsact.com)

soft biometric feature by hardening the fuzzy vault scheme. Section 4 illustrates the experimental results with necessary explanations and Section 5 concludes the paper with fewer discussions.

II. Related Work

Numerous research works has been proposed previously, which suggests the combination of biometrics and cryptography for developing a verification system [7] [8]. These are referred to as cancelable biometrics since it makes use of a one way transformation to convert the biometric signal into irreversible form. This section of the paper discusses some of the relevant work proposed earlier in literature for developing a user authentication system using soft biometric characteristics and fuzzy vault scheme. The hardening of soft biometric features with fuzzy vault scheme improves user security and privacy.

Moi et al. in [9] put forth an approach for identity document using iris biometric cryptography. They presented an approach to create a distinctive and more secure cryptographic key from iris template. The iris images are processed to generate iris template or code to be utilized for the encryption and decryption tasks. The international standard cryptography algorithm – AES has been adopted in their work to produce a high cryptographic strength security protection on the iris information. Their proposed approach comprises of two processes. They are encryption and decryption process. Template matching is the process used for pattern recognition. The utilization of biometric as a key is to enhance security in a more efficient way, decrease human mistakes during identification, increase user convenience and automation of security function. Their experimental results revealed that their proposed approach out performed some of the traditional techniques in providing authentication for the user.

A two-phase authentication mechanism for federated identity management systems was described by Abhilasha et al. in [10]. The first phase consists of a two-factor biometric authentication based on zero knowledge proofs. They employed techniques from vector-space model to engender cryptographic biometric keys. These keys are kept secret, thus preserving the confidentiality of the biometric data, and at the same time make use of the advantages of a biometric authentication. The second authentication combines several authentication factors in concurrence with the biometric to make available a strong authentication. A key advantage of their approach is that any unexpected combination of factors can be used. Such authentication system leverages the information of the user that is available from the federated identity management system. Their proposed approach improves privacy, reliability, security of the biometric data.

Uludag et al. in [11] discussed the issues and challenges in implementing the biometric system for user authentication. They presented a variety of methods that monolithically combine a cryptographic key with the biometric template of a user stored in the database in such a manner that the key cannot be revealed without a successful biometric authentication. They assessed the performance of one of these biometric key binding/generation algorithms using the fingerprint biometric. Moreover they illustrated the challenges involved in biometric key generation principally due to extreme acquisition variations in the representation of a biometric identifier and the imperfect nature of biometric feature extraction and matching algorithms. They sophisticated on the suitability of these algorithms for digital rights management systems. Experiments were conducted to explore the performance of there discussed methods in improving user security.

A Biometric Verification System was proposed by Cimato et al. in [12]. In their proposed work they presented a biometric authentication technique based on the combination of multiple biometric readings. The authentication control can be performed offline and the stored identifier does not disclose any information on the biometric traits of the identified person, so that even in case of loss or steal of the document, privacy is guaranteed. Their proposed approach ensures high level of security because of the association of multiple biometric readings. Biometric techniques are more and more exploited in order to fasten and make more consistent the identification process. The combination of cryptography and biometrics increases the confidence in the system when biometric templates are stored for verification.

Sunil et al. in [13] put forth a novel methodology for the secure storage of fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption with the aid of cancelable biometric features. They proposed a technique to produce cancelable key from fingerprint so as to surmount the limitations of traditional approaches. Cryptography is merged with biometrics in Biometric cryptosystems, otherwise known as crypto-biometric systems [11]. They have introduced the concept of cancelable biometrics that was earlier proposed in [14]. Their approach facilitates the every incidence of enrollment to utilize a distinct transform thus making expose cross matching unachievable. Generally, the transforms utilized for distortion are chosen to be non-invertible. Thus it is not possible to recover the original (undistorted) biometrics despite knowing the transform method and the resulting transformed biometric data.

An effective authentication scheme by combining crypto with biometrics was projected by Hao et al. in [15]. They projected the first practical and secure way to integrate the iris biometric into cryptographic applications. A repeatable binary string, which we call a biometric key, is generated reliably from genuine iris codes. The key is generated from a subject‘s iris image with the support of auxiliary error-correction data, which do not disclose the key and can be saved in a tamper-resistant token, such as a smart card. The reproduction of the key depends on two factors: the iris biometric and the token. The attacker has to get hold of both of them to compromise the key. Moreover they evaluated the technique using iris samples from 70 different eyes, with 10 samples from each eye. As a result they found that an error-free key can be reproduced reliably from genuine iris

codes with a 99.5 percent success rate. One can generate up AES. The extraction of a repeatable binary string from biometrics opens new possible applications, where a strong binding is required between a person and cryptographic operations.

Apart from above mentioned works numerous researches has been done in this field of combining fuzzy and cryptographic key generation techniques [23, 24, 25]. Establishing the identity of a person is a critical task in any identity management system. Karthick Nandakumar et al. in [16] [17] showed the password hardened finger print fuzzy vault in which password acts an additional layer of security. This additional layer of security improves the security and privacy of users' biometric template data. The same concept mentioned in [16] was suggested to iris based hardened fuzzy vault scheme [17]. The approach discussed in [17] applies a sequence of morphological operations to extract minutiae points from the iris texture. Chen et al in [26] proposes the use of a Higher Order Spectral (HOS) Transform that can be applied to biometric data as a secure hash function. This HOS transform is non-invertible, is robust to noise in the input allowing it to tolerate the natural variations present in a biometric and can be made to produce a large number of significantly different outputs given an identical input.

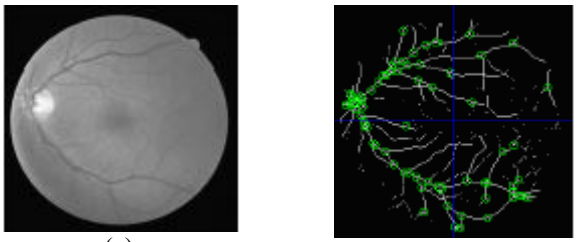
III. Our Proposed Approach

Our proposed methodology of fuzzy vault construction using retina as a soft biometric feature involves three steps. In the initial step the retinal template is subjected to undergo a random transformation. The approach makes use of the advantages provided by both the fuzzy framework and the soft biometrics, thereby enhancing the security and privacy. In the next step the obtained transformed template is secured with the assistance of constructing a fuzzy vault. The final step comprise of hardening the constructed fuzzy vault by encrypting the vault with the key randomly generated from soft biometric features and the user password. The password pretends as an additional layer of security. Fig 1 shows the soft biometric hardening of retina-based fuzzy vault scheme

A. Retinal Bifurcation Feature Point Extraction

The technique described by Chen et al. in [19] is utilized in this paper, for extracting the bifurcation feature points from retina. The retinal bifurcation points are extracted to improve the security and privacy of the user. The combination of soft biometrics characteristics and fuzzy vault scheme exploit the performance of the authentication system that was developed in recent years. In our approach the bifurcation feature of retina were obtained form vascular pattern of retina. The two major operations to be performed on the retinal template are thinning and joining operation, in order to extract the retina vascular pattern. As a result of this operation the bifurcation feature points are extracted from the retinal template. Fig .2 (a) represents the original retinal template. Fig.2 (b) shows the highlighted bifurcation feature points in a retinal vascular tree after performing thinning and joining operations

to 140 bits of biometric key, more than enough for 128-bit



(a) (b)

Fig. 2 (a). Original Retinal Template (b) Highlighted Bifurcation Feature

B. Hardening the retinal fuzzy vault using password

This is the significant step in the design of an authentication system. This makes use of the retinal template samples obtained from the database. The proposed system is implemented using MATLAB. The retinal samples that are obtained from the database are first resized as per our requirement. By highlighting the retinal bifurcation feature points the proposed method identifies the lock/unlock data. The bifurcation feature points are subjected to mathematical operation like permutation and translation using password. The principal requirement of this step is to achieve the three tuple parameters (u, v, θ). In which _u' and _v' signifies the row and column indices respectively of the image found out and θ symbolizes the orientation parameter. These transformed feature points are then secured in the fuzzy vault using the 128 bit randomly generated key. A 64 bit user password is used to transform the randomly generated key. Additionally, the same can be used to encrypt the vault.

C. Transformation of Extracted Bifurcation Feature Points

As mentioned previously the retinal vascular tree holding the bifurcation points are destined to under go mathematical operations like permutation and translation. As a result of this process the original bifurcation points will get transformed into new points. There is a constraint on the number of characters used for user password. The user password is of 8 characters in length. Therefore a total of 64

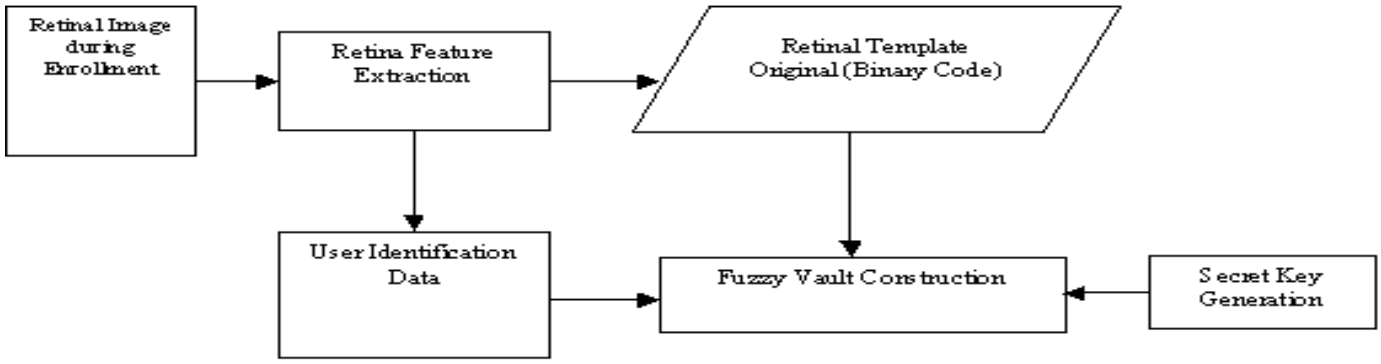
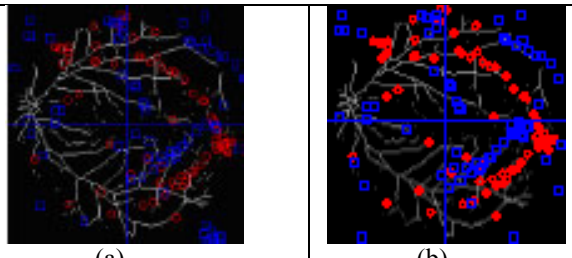


Fig.1 Soft biometric hardening of retina-based fuzzy vault scheme

bits are considered for randomization. These 64 bits are further divided into 4 blocks each block consisting of 16 bits. The first five characters resemble the password and the last three characters denote the soft biometric feature of the user. The five-character password used in our implementation is ―TOKEN." The last three characters that indicate the user soft biometric characteristics are as follows. The sixth character denotes the height, the seventh stand for gender, and the eighth character resembles iris color of the user.

As an initial stage of implementation the bifurcation points are divided into 4 quadrants. Each quadrant is then processed with one password prior to permutation and translation operations. Care must be taken while applying the permutation operation. Note that there should not be any change in the relative position of the bifurcation points. The 16 bits of each quadrant is segmented into two bit block, one containing 9 bits and the other containing 7 bits. Tu denote the segment with 7 bits and Tv denote the segment with 9 bit length. Tu and Tv represents the amount of translation in the horizontal and in the vertical directions, respectively. Fig 3 shows transformed retinal bifurcation points.



(a) (b)

Fig 3. (a) and (b) Transformed bifurcation Points. (Blue-Transformed, Red-Original Points)

The transformation that is utilized to derive at the new retinal points is $X_u' = (X_u+T_u) \bmod (2^7)$

$Y_v' = (Y_v+T_v) \bmod (2^9)$

In which Xu and Xu' represents the horizontal distance before and after transformation respectively. In the similar manner, Yv and Yv' represents the vertical distance before and after transformation respectively.

D. Encoding the vault

This step secures the vault from being modified by an imposter from the knowledge of the password. The approach substitutes Reed-Solomon reconstruction step by Lagrange interpolation and cyclic redundancy check (CRC) based error detection. The obtained feature points are consistently quantized and articulated as binary strings. Therefore this can be represented as an element in Galois Field GF (216). A large number of the chaff points are generated by the method mentioned in [4] [20]. Finally these chaff points are combined with the obtained feature points to make the imposter unaware of the genuine points in the retina.

E Decoding the vault

The user password is used to decrypt the encrypted fuzzy vault and the bifurcation feature points of the retina in this authentication phase. The helper data or a set of high curvature points are created in order to make possible the alignment of query minutiae to the biometric template. A transformation based on the password is implemented on the query feature points and the vault is unlocked.

IV. Experiments And Results

The proposed work is implemented in MATLAB 7.0. The essential parameters used in this implementation are the number of chaff points (c), number of genuine points (r), and the total number of points (r+c). More the number of chaff points used, more is the privacy and security. It is remarkable that the number of chaff points introduced must be ten times the total number of genuine points that are available in the retinal template. The number of chaff points

TABLE I Bifurcation points before and after transformation

I[st] Quadrant and soft biometric features	Feature Points				Transformation code obtained from soft biometrics	
	Before Transformation		After Transformation			
	Horizontal Distance X_u	Vertical Distance Y_v	Horizontal Distance X_u'	Vertical Distance Y_v'	Row index with respect to horizontal axis T_u	Column index with respect to horizontal axis T_v
'VAULT' Height=157 Iris Color='B' Gender='M'	105	18	55	84	78	322

used determines the security and authentication provided by the developed system.

The revocability is evaluated by transforming the retinal (biometric) template for user password and soft biometric features. The proposed approach makes use of 8 characters to secure the vault as mentioned earlier. These 8 characters comprises of both the user password and the soft biometric characteristics of the user. The 8 characters can be grouped into two parts one containing the password of five characters. The sixth character denotes the height, the seventh and the eighth represents the gender and the color of iris respectively. Table 1 shows an example bifurcation points for one quadrant before the transformation and after performing the transformation for user password ―VAULT", and user soft biometrics features namely height, gender and iris color.

The corresponding ASCII values of the 8 characters are utilized to secure the fuzzy vault. For the user password set as ―VAULT" the corresponding ASCII values are determined as (86, 65, 85, 76 and 84). The remaining three characters are represented by the soft biometric features of the user. The value of the user height can be used as one parameter, and the remaining two ASCII values are calculated using the gender and the iris color of the user. With the change in the password variety of transformed templates can be obtained for same original biometric template. A variety of applications can use the soft biometric features with different passwords thus averting the cross matching.

V. CONCLUSION

As the decades pass by, improving the security and the privacy of the verification system is a challenging issue in recent years. Therefore, it is necessary to design a verification system that is more users friendly and secure. The proposed approach determines to combine the soft biometrics features and the cryptographic framework to develop a verification system that suits for a wide variety of applications. The biometric template that is taken into consideration in this approach is retina because of the advantage that the retinal based genuine point determination pose a great challenge to all most all the attackers. Fuzzy vault is the framework which comprises of the combination of soft biometrics and cryptographic key generation technique. User password is used to improve the security and privacy of the authentication system. This password acts as an additional layer of security. Even if the password is compromised by an imposter it is hard to match the biometric template. Thereby, the security provided by biometric feature is not affected. In future, works to improve the performance of the vault can be carried out by applying non-invertible transformation and multiple biometric traits [21] [22]. This considerably reduces the failure to capture rate thus improving the performance of fuzzy vault

VI. REFERENCES

1) Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, ―Biometrics: A Grand Challenge", Proceedings of the International Conference on Pattern Recognition, Vol. 2, pp. 935–942, September 2004.
2) Wayman, A. Jain, D. Maltoni, and D. Maio, ―Biometric Systems: Technology, Design and Performance Evaluation," Springer-Verlag, 2005.
3) Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, ―Handbook of Fingerprint Recognition," Springer, 2003.
4) Juels, and M. Sudan, ―AFuzzy Vault Scheme", Proceedings of the International Symposium on Information Theory, p. 408, Lausanne, Switzerland, June 2002.
5) Juels, and M. Wattenberg, ―AFuzzy Commitment Scheme," Proceedings of the 6th ACM Conference on Computer and Communications Security, pp. 28-36, New York, NY, USA, 1999.
6) Tiago Santos, Gonçalo Lourenço, Luís Ducla Soares, and Paulo Lobato Correia, ―Enhancing Biometrics Security," 2009.

7) N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating Cancelable fingerprint templates," IEEE Transactions on Pattern Analysis and Machine Learning, vol. 29, no. 4, pp. 561-572, 2007.
8) Savvides, B. V. K. V. Kumar, and P. K. Khosla, "Cancelable Biometric filters for face recognition," Proceedings of ICPR, Vol. 3, pp. 922-925, Cambridge, UK, September 2004.
9) Sim Hiew Moi, Nazeema Binti Abdul Rahim, Puteh Saad, Pang Li Sim, Zalmiyah Zakaria, and Subariah Ibrahim, "Iris Biometric Cryptography for Identity Document," IEEE Computer Society, International Conference of Soft Computing and Pattern Recognition, pp. 736-741, 2009.
10) Abhilasha Bhargav-Spantzel, Anna Squicciarini, and Elisa Bertino, "Privacy preserving multi-factor authentication with biometrics," Conference on Computer and Communications Security, pp. 63-72, 2006.
11) U. Uludag, S. Pankanti, S. Prabhakar, A. K. Jain, "Biometric cryptosystems: issues and challenges," vol. 92, no. 6, pp. 948-960, 2004.
12) Stelvio Cimato, Marco Gamassi, Vincenzo Piuri, Roberto Sassi, and Fabio Scotti, "A Biometric Verification System Addressing Privacy Concerns," International Conference on Computational Intelligence and Security (CIS 2007), pp.594-598, 2007.
13) Sunil V. K. Gaddam, and Manohar Lal, "Efficient Cancelable Biometric Key Generation Scheme for Cryptography," International Journal of Network Security, vol. 11, no. 2, pp. 57-65, 2010.
14) R. Ang, R. Safavi-Naini, and L. McAven, "Cancelable key-based fingerprint templates," ACISP 2005, pp. 242-252, 2005.
15) Feng Hao, Ross Anderson, and John Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081-1088, 2006.
16) Karthik Nandakumar, Abhishek Nagar, and Anil K.Jain, "Hardening Fingerprint Fuzzy Vault Using Password", International conference on Biometrics, pp. 927 – 938, 2007.
17) Srinivasa Reddy, and I. Ramesh Babu, "Performance of Iris Based Hard Fuzzy Vault", Proceedings of IEEE 8th International conference on computers and Information technology workshops, pp. 248 – 253, 2008.
18) Karthick Nandakumar, Sharath Pankanti, and Anil K. Jain, "Fingerprint-Based Fuzzy Vault Implementation and Performance", IEEE Transacations on Information Forensics and Security, vol. 2, no. 4, pp.744 – 757, December 2007.
19) Li Chen, and Xiao-Long zhang, "Feature-Based Image Registration Using Bifurcation Structures", Matlab Central.
20) K. Jain, L. Hong, and R. Bolle, "On-line Fingerprint Verification," IEEE Transaction on Pattern Analysis and Machine Learning, vol. 19, no. 4, pp. 302-314, April 1997.
21) Jain, Anil K. Jain and Arun Ross, "Multibiometric systems," Communications of the ACM," January 2004, Volume 47, no. 1, 2004.
22) K. Jain and A. Ross, "Learning User-specific parameters in a Multibiometric System", Proceedings of IEEE International Conference on Image Processing (ICIP), Rochester, New York, pp. 57 – 60, 2002.
23) Monrose, M. K. Reiter, Q. Li, and S. Wetzel, "Cryptographic Key Generation from Voice," in Proceedings IEEE Symposium on Security and Privacy, Oakland, pp. 202-213, May 2001.
24) Dodis, L. Reyzin and A. Smith, "Fuzzy Extractors: How to generate Strong Keys from Biometrics and other Noisy Data," in Proceedings of International Conference on Theory and Application of Cryptographic Techniques, pp. 523-540, May 2004.
25) Jain, A. K., Nandakumar, K., and Nagar, A. Biometric template security. EURASIP J. Adv. Signal Process 2008, Jan 2008.
26) Chen, Brenden Chong and Chandran, Vinod Biometric template security using higher order spectra. In: International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2010, 14-19 March 2010