Secure Biometric Cryptosystem Which Follows Multimodal Approach for Biometric Key Generation

[1]Ankit Joshi,[2]Nitesh Singh,[3]K Vijayakumar
[1]Student, [2]Student, [3]Assistant Professor
[1]SRM University,Chennai.

Abstract **- Securing the confidential information has become a challenging task in today's world of advance technology. The traditional security system uses passwords for authentication and protection of confidential data. But those passwords are easily cracked. Cryptography provides protection of information with the help of secure cryptographic keys addressing the above issue. Management of cryptographic keys is a major issue faced by cryptography. To overcome this issue, the field of biometrics was introduced which uses human characteristics to provide security. But the biometrics information can be forged, resulting in breaking down of the system security which in turn makes the information easily accessible. Solution to this problem can be obtained by a combination of two or more biometrics (multimodal biometrics) to provide better security. Due to more than one biometrics it becomes difficult to crack all the biometrics at once.**
We propose a novel algorithm, which involves generation of secure biometric key with the help of multi modal biometric characteristics (Iris, Fingerprint and Palm print). The approach introduced helps to provide better security and follows process of authentication in an effective manner.

IndexTerms **- Multimodal biometrics, security, iris, fingerprint, palmprint, score generation, biometric key generation,formatting,style,styling,insert.**

I. INTRODUCTION

The most common form of security provided by using passwords is known as knowledge based security. The password system has its own drawback such as when the user needs to remember lengthy passwords in order to access information. In order to eliminate this drawback, secure cryptographic key approach was implemented. But cracking of shared keys became one of the major threats faced among cryptographic techniques.

In orderto follow secure authentication and authorization of user, the field of biometrics was introduced. Biometrics is the field which involves usage of physiological/behavioral and biological characteristics in order to identify an individual. The distinguishing characteristic information's like Iris, Ear, Fingerprint, Palmprint, Face, Gait, Pulse-rate, Voice etc are known as biometric traits. Biometric systems which uses single biometric trait at any given instance have limitations like uniqueness, high error rate, non-universality and noise [1]. Later, these limitations were reduced by multimodal biometrics. With the advancement of technology transition from unimodal biometric (one single trait at a given instance) to multi-modal biometric systems, (combinations of two or more traits) has been observed in order to enhance the security level [2].

The combined performance of cryptography and biometrics in order to generate cryptographic key has gained much reputation among the researchers in order to enhance security [3]. The enhanced performance of bio cryptosystems eliminates the necessity of traditional password system and provides combined strength of both the fields [4-7].

Multimodal biometrics involves fusion of traits or characteristics at various stages[8]: 1)sensor level extracts information from different sensors;2)feature level extracts biometric information in the form of features; 3)score level extracts match scores of individual biometric comparisons;4)decision level extracts the results of individual biometric comparisons;5) rank level when the output of each biometric system is a subset of possible matches (i.e., identities) sorted in decreasing order of confidence. Biometric features extracted are unique to each individual and cannot be altered for life. Cracking and spoofing of such information becomes more difficult especially when more than two traits are fused. This paper follows score level fusion by generating matching scores against each individual scores present in the database.

Score Generation and Normalization:The score generated are matched for distinguishing between an imposter anda genuine user. Score level fusion is preferable as well as feasible among several other fusions because matching scores can also be generated without the information of feature extraction [9-10].Scores generated can be in the form of distance scores or similarity scores. For the purpose of fusion, scores are converted into one of these forms. This technique is called normalization. Score level fusion can be of three different forms: 1) Transformation based, 2) Classifier based, 3) Density.

Transformation is a sum rule-based fusion which follows the maximum to minimum normalization [9-10].

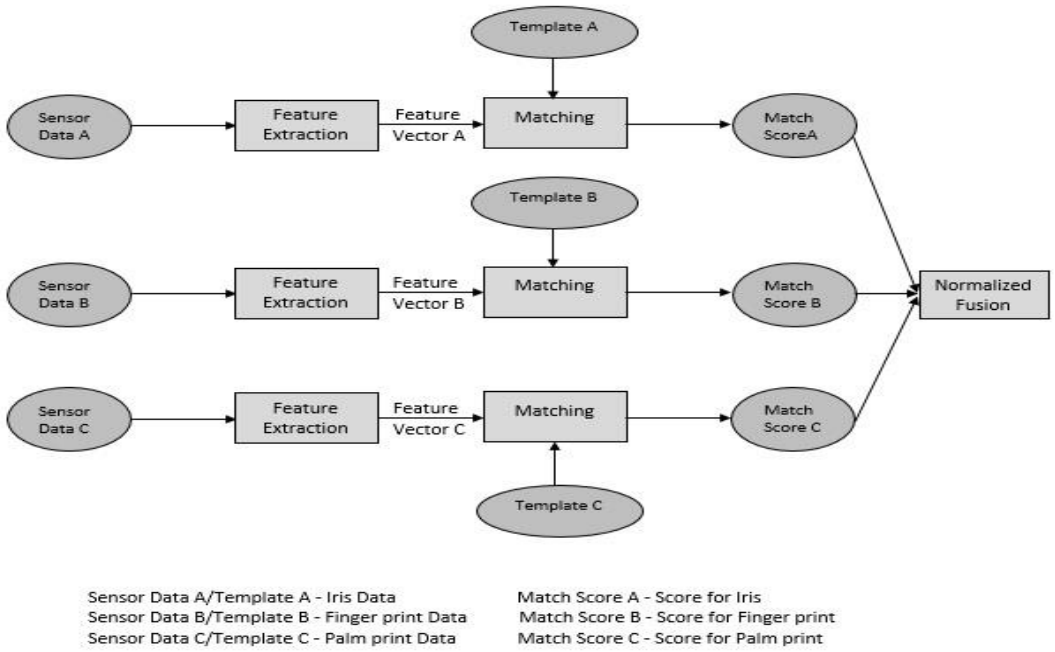

Figure 1 Score Generation and Normalization from given samples

As it can be observed from the Fig. 1, information is given as input via sensors to the system, later with the help of feature vector matching process is followed. Matching scores are generated based on database and the sample data being analyzed. The individual scores generated undergoes normalization to follow fusion.

In this paper individual scores generated for each features as well as normalized scores are considered for generation of biometric keys.

II. Related Work

An approach to feed Iris biometric information into cryptography to generate a biometric key is proposed by Feng Hao, Ross Anderson and John Daugman [11]. A Biometric key, was generated from the sample Iris codes. The codes were generated with the help of ECC (error correcting codes). The generation of key is based on Iris biometrics (minutiae).70 different samples were experimented in order to generate 140-bit key with attainment of 99.5 percent achievement rate. Another approach to form entropy based feature extraction via Reed-Solomon error codes has been discussed by B.Chen and V.Chandran [12].

Cancellable biometrics gives high performance in terms of security due to usage and involvement of one or more templates for same type of biometric. According to R. Ang, R. Safavi-Naini, L. McAven [13] dependent key-cancellable template was produced by implementation of dependent geometric transform with the help Fingerprint features obtained.

J. G. Jo, J. W. Seo, and H. W. Lee [14] proposed a unique technique by generating the digital signatures followed by cryptography communication with the biometrics information. The generation of signature can be verified by the cryptographic algorithm like RSA. Hong and Jain [15] proposed an identification system based on face and Fingerprint, where Fingerprint matching is done with the help of facial features. The process of authentication is proposed using multimodal biometric system using two features i.e. face and Palmprint by Nageshkumar.M, Mahesh.PK and M.N. ShanmukhaSwamy [16]. Combination of information's have shown improved robustness. The matching score level fusion technique where features are converted to vectors follows evaluation in the form of enrolment template.

K.A. Nishimura, S. J. Wen strand and G. Panotopoulos [17] have detailed the symmetric key encryption with public and private keys of asymmetric approach. This developed approach ensures doubly-encrypted message receipt as per authenticated user. Rupam Kumar Sharma [18] introduced approach which gathers information from Fingerprint to generate biometric key for DES encryption. Encryption/Decryption of Message with help of 16 digit Hexa-Decimal key using DES Approach Key is extracted from Thinned image using Binarization technique.

Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari [19] uses Multi- biometric with fusion Fingerprint and Iris, better result is accepted. A new method which involves fuzzy logic is proposed which includes Fuzzification, (process of each input convert to linguistic variance). The fuzzy inference system gives an output and accepts the main output. If we have two inputs, 1 for Fingerprint and 5 for Iris, system gives accuracy 99.4%. A multi- modal biometric system (Fingerprint & Iris) is used after converting Fingerprint and Iris image to its respective binaries.

III. Proposed Work

Biometric cryptosystems combines the fields of cryptography and biometrics in order to produce the combined effects which strengthens the security. This paper introduces a novel approach which helps to generate a biometric key with the help of multimodal biometrics. The biometrics consists of three levels which includes Iris, Fingerprint and Palmprint. The output of this algorithm are two keys (Key A1 and Key A2) which are used to carry out encryption and decryption process.

In this method, the individual features of biometric data are extracted and converted into decimal scores. These bits are compressed and crossed over into biometric keys. These combined biometric keys is used to bind each bit of the cryptographic key. The resulting binary keys produced as a result are used as encryption key for carrying out the encryption of the original message into cipher. The combined biometric key generated is highly secure as the features extracted are unique for each individual and cannot be cracked easily.

Thealgorithm consists of following main stages:

1. Input of information and Score Generation/Normalization

- The biometric information of the user are collected in the form of images. Three different levels of biometric information which consists of Iris, Fingerprint and Palmprint are collected. The input information is then stored in the database successfully.
- Matching scores of each type of biometric are generated based on the database formed.
- Score generated are later normalized using normalization technique.

2. Conversion and Fusion

- The scores are normalized to decimals within the range of 0 to 1.
- The highest matched score of each biometric is taken and converted into binary form.
- Later fusion of these binaries are carried by xor operation.
- At first, Iris and Fingerprint binaries undergoes xor operation. The result of this process again follows xor operation with the Palmprint binaries in order to obtain biometric key A2.
- Hence it can be summarized as XOR (XOR (Iris+ Fingerprint) +Palmprint) = Key A2.

3. Generation of Biometric key

Transformation fusion which follows the maximum to minimum normalization is a sum rule based technique [9-10] given by the formulae below.

$$N_{iris} = \frac{X_{iris} - minX_{iris}}{maxX_{iris} - minX_{iris}} N_{finger} = \frac{X_{finger} - minX_{finger}}{maxX_{finger} - minX_{finger}} N_{palm} = \frac{X_{palm} - minX_{palm}}{maxX_{palm} - minX_{palm}} \quad (1)$$

In Eq.1 minXiris and maxXiris are the minimum and maximum scores for Iris recognition, minXfinger and maxXfinger are the corresponding values obtained from Fingerprint trait whereas minXpalm and maxXpalm are generated using Palmprint recognition. For multi modal approach we follow the similarity fusion which includes

$$N_{fusion} = \alpha N_{iris} + \beta N_{finger} + \gamma N_{palm} \quad (2)$$

In Eq. 2 α,β,γ are weighted constants to normalize overall scores.

Among the normalized scores the highest score is taken as the reference. The score is then converted to its binary form which is considered as the biometric key A1.

4. Secure Cryptography

Encryption-After the generation of key A1 and key A2 we follow a secure encryption technique. At first, original message passed as input generates cipher 1 with key A1 via AES encryption. Later cipher 1 is taken as input message and again encryption is done with key A2 to produce cipher

Decryption: Similarly, at first cipher 2 is decrypted to cipher 1 with key A2. Then cipher 1 is converted back to original message with key A1.

The above process from 1 to 3 can be summarized with the help of Fig. 2:

The above process 4 can be summarized with the help of Fig. 3 as shown below:

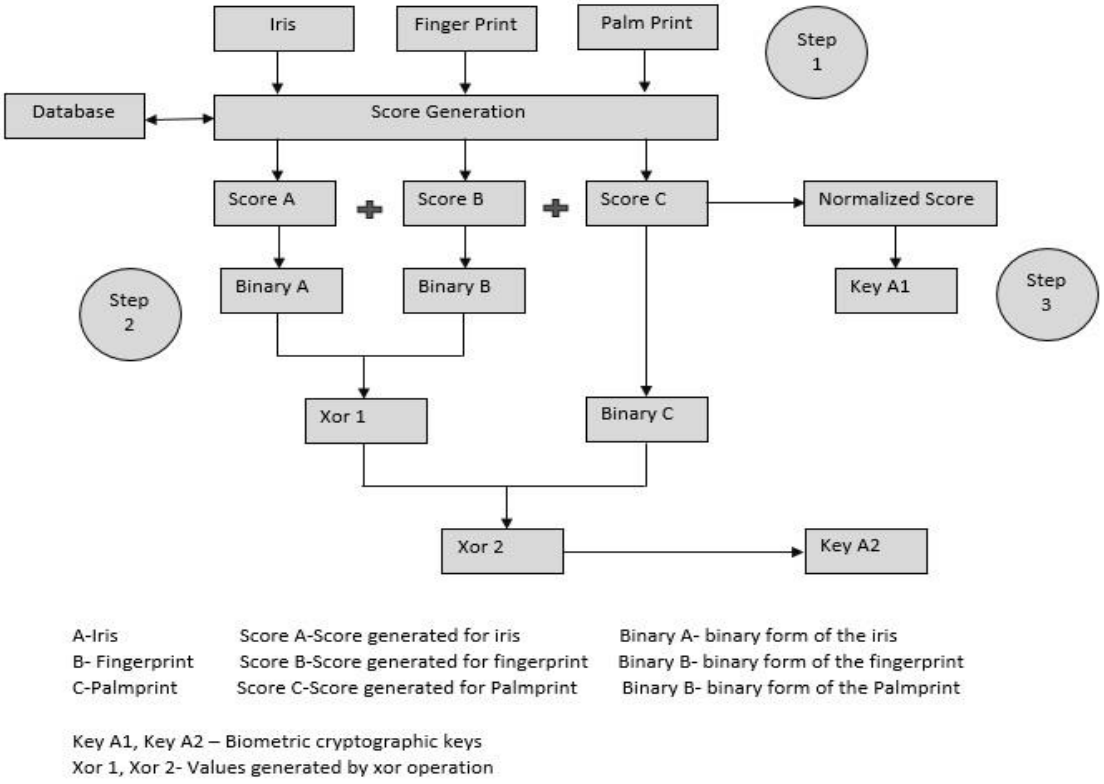

Figure 2 Proposed approach for generation of biometric keys.

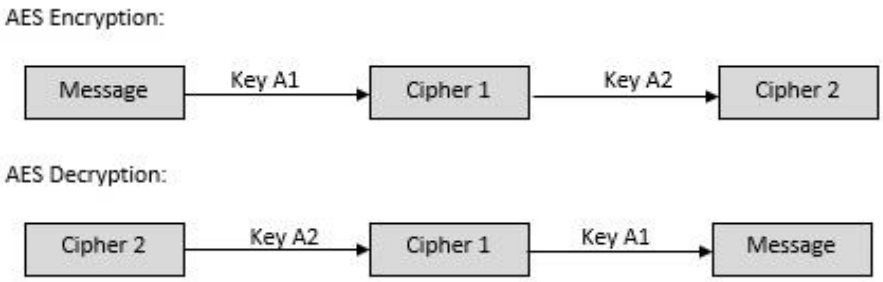

Figure 3 Process of Encryption and Decryption

IV. Experimental Results

The proposed technique provides better security due to 3 levels of multimodal biometrics. This paper combines the scores based on fusion of Iris, Fingerprint and Palmprint data to generate biometric cryptographic keys. The analysis done provides information about the performance and estimate measures of the combined (proposed) biometric techniques. The Iris, Fingerprint and Palmprint data are collected from about 70 individuals and used for evaluation. Scores for each biometric traits are generatedrespectively. The calculation of analysis parameters such as FAR, FRR are estimated. The biometrics features for Iris, Fingerprint and Palmprint are collected separately. Then, scores are obtained followed by the fusion technique discussed.FAR is False Acceptance Rate and FRR is False Rejection Rate.

Table 1 and Fig. 4 shows the False Acceptance Rate (FAR) analysis of biometrics for the combined (proposed) technique compared against the existing technique. As it can be observed the proposed approach results in lesser value compared to existing technique.

Table 2 and Fig. 5 shows the False Rejection Rate (FRR) analysis of biometrics for the combined (proposed) technique compared against the existing technique. Again, based on the observed scenario the proposed approach results in lesser value compared to existing technique.

As both the parameters are less compared to existing technique, it can be concluded that the proposed approach provides better as well as effective security.

Table 1

User	Iris	Finger print	Palm print	Combination (All three)
1-10	0.40	0.44	0.35	0.12
11-20	0.37	0.43	0.34	0.13
21-30	0.38	0.42	0.33	0.09
31-40	0.39	0.47	0.31	0.10
41-50	0.39	0.48	0.29	0.08
51-60	0.38	0.41	0.33	0.03
61-70	0.40	0.45	0.36	0.11

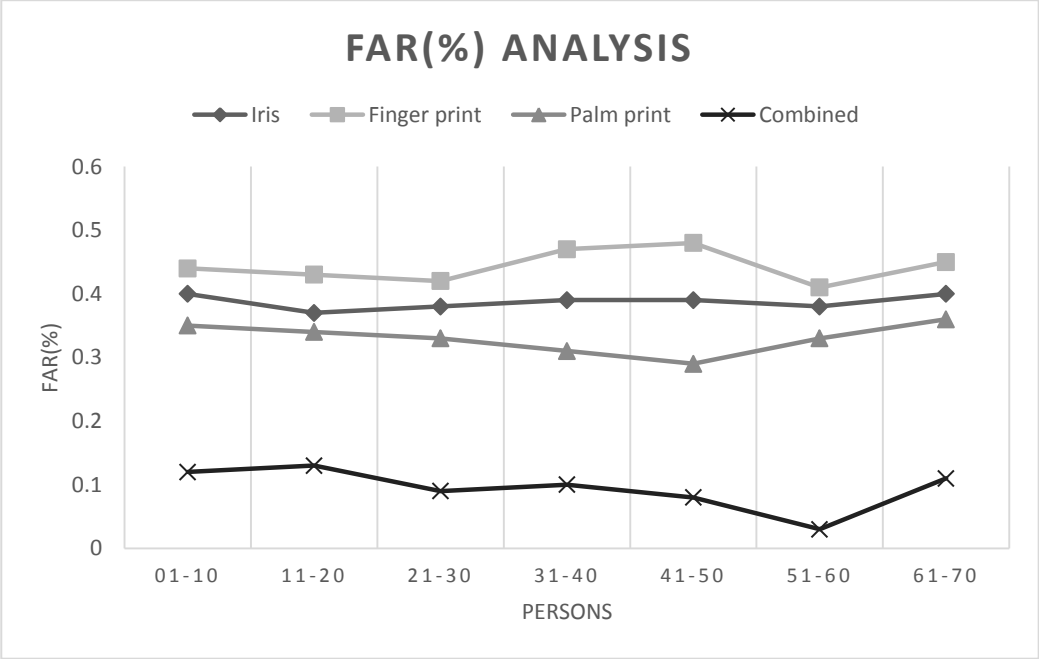

Figure 4 Comparative analysis of FAR (False Acceptance Rate)%

Table 2

User	Iris	Finger print	Palm print	Combination (All three)
1-10	88.3	91.5	87.8	85.5
11-20	88.5	91.1	87.3	84.7
21-30	88.7	92.7	88.1	86.2
31-40	91.4	93.4	89.6	84.3
41-50	90.6	91.3	88.8	83.6
51-60	90.3	91.6	89.2	84.3
61-70	89.2	92.3	88.5	85.3

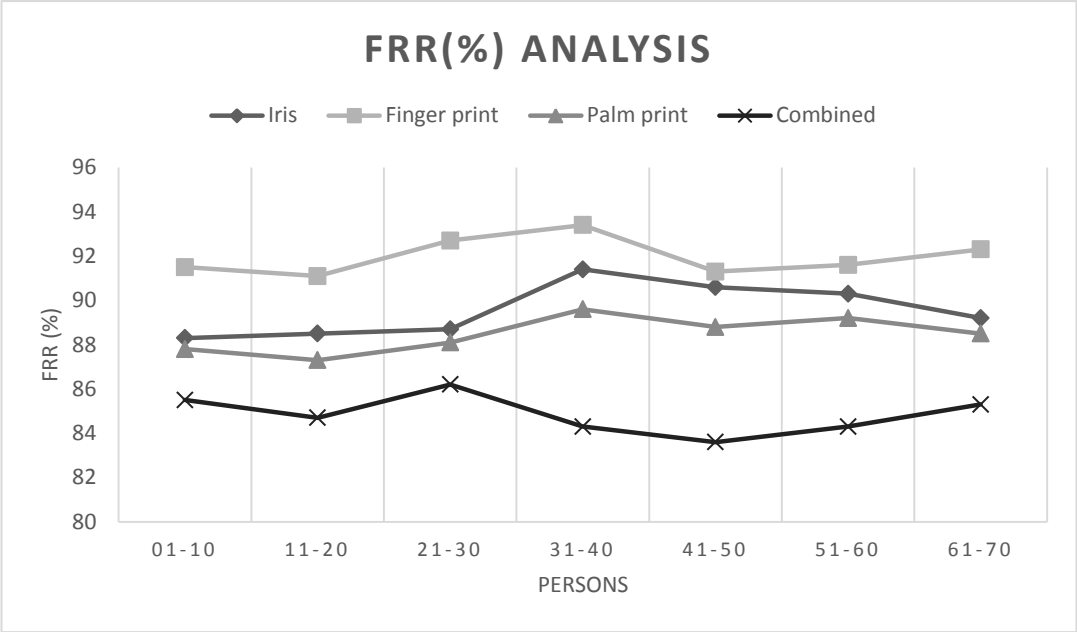

Figure 5 Comparative Analysis of FRR (False Rejection Rate)%

V. Conclusion And Future Work

Security plays a vital role for various systems which are used by everyone on a daily basis. Biometrics recognizes the problems associated with security. It provides enhanced security by incorporation of various human behavioural features such as Iris, Fingerprint, Palmprint, Voice, facial structure etc. Problems associated with biometrics includes non-revocability and privacy compromise. Such problems are overcome by introduction to multi-modal biometrics which involves combination of two or more biometric features to strengthen the existing security. Combining complementary characteristics of biometrics and cryptographic systems provides much more secure systems as it addresses individual issues and helps to produce a more efficient system.

This paper proposes an algorithm for generating biometric key using more than two biometrics. The biometric key is generated with the score level fusion which is not observed till now. Based on the analysis done, the experimental result shows that proposed technique is better and reliable as well as more secure due to involvement of three levels of biometrics. Security can be enhanced by improving the normalization techniques. More such innovative approaches may be used to enhance performance and security.

References

[1] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari, "Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.

[2] A.K. Jain, R. Bolle, and S. Pankanti, (Eds.), "Biometrics: Personal Identification in Networked Society," Kluwer Academic Publishers, 1999.

[3] N. Lalithamani and K.P. Soman, "Irrevocable Cryptographic Key Generation from CancelableFingerprint Templates: An Enhanced and Effective Scheme," European Journal of Scientific Research, vol.31,no.3, pp.372-387, 2009.

[4] Goh and D.C.L. Ngo, "Computation of cryptographic keys from face biometrics," International Federation for Information Processing 2003,Springer-Verlag, LNCS 2828, pp. 1–13, 2003.

[5] F. Hao, C.W. Chan, "Private Key generation from on-line handwritten signatures," Information Management & Computer Security, vol. 10, no. 2, pp. 159–164, 2002.

[6] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007.

[7] N. Lalithamani and Dr. K.P. Soman, "An Effective Scheme for Generating Irrevocable Cryptographic Key from Cancelable Fingerprint Templates," International Journal of Computer Science and Network Security, vol. 9, no.3, March 2009.

[8] Arun A. Ross, KarthikNandakumar, and Anil K. Jain. "Handbook of Multibiometrics. International Series on Biometrics," Springer, 2006.

[9] S.C. Dass, K. Nandakumar, A.K. Jain, "A principled approach to score level fusion in multimodal biometric systems," in: Proceedings of AVBPA, Rye Brook, July 2005, pp. 1049–1058.

[10] K. Jain, K. Nandakumar, & A. Ross, "Score Normalization in multimodal biometric systems,"The Journal of Pattern Recognition Society, 38(12), 2005, 2270-2285.

[11] Feng Hao, Ross Anderson and John Daugman, "Combining Crypto with Biometrics Effectively," IEEE Transactions on Computers, vol. 55, no. 9, pp. 1081 - 1088, September 2006.

[12] Chen, B. and Chandran, V., "Biometric Based Cryptographic Key Generation from Faces," in proceedings of 9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications, pp. 394 - 401, December 2007.
[13] R. Ang, R. Safavi-Naini, L. McAven, "Cancellable key-based Fingerprint templates," ACISP 2005, pp. 242-252.
[14] J. G. Jo, J. W. Seo, and H. W. Lee, "Biometric digital signature key generation and cryptography communication based on Fingerprint," First Annual International Workshop 2007, LNCS 4613, pp. 38-49, Springer Verlag, 2007.
[15] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEE Trans. PAMI, vol. 20, no. 12, pp. 1295-1307, 1998.
[16] Nageshkumar.M, Mahesh.PK and M.N. ShanmukhaSwamy, "An Efficient Secure Multimodal Biometric Fusion Using Palmprint and Face Image," IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.
[17] K.A. Nishimura, S. J. Wen strand and G. Panotopoulos,"Biometric identification device," European patent, July 2007.
[18] Rupam Kumar Sharma,"Generation of Biometric Key for Use in DES IJCSI International Journal of Computer Science," Issues, Vol. 9, Issue 6, No 1, November 2012 ISSN (Online): 1694-0814.
[19] Mohamad Abdolahi, Majid Mohamadi, Mehdi Jafari,"Multimodal Biometric system Fusion Using Fingerprint and Iris with Fuzzy Logic," International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, January 2013.