Wavelet Based Feature Level Fusion Approach for Multi-biometric Cryptosystem

Patel Heena, Paunwala Chirag(✉), and Vora Aarohi

Electronics and Communication Engineering Department, SCET, Surat, India
hpatell323@gmail.com, cpaunwala@gmail.com,
vaarohi@gmail.com

Abstract. Biometric cryptosystems incorporates the benefits of both cryptography as well as biometrics i.e. higher security levels and elimination of memorizing passwords or carrying tokens. The threat of breaching the security of the confidential data motivates the development of the data hiding techniques in this paper. This paper contributes in enhancing the security of biometric systems by incorporating the concept of wavelet decomposition along with the fusion of biometric traits. The concept of wavelet decomposition of feature templates helps in reduction of template size as well as it increases the compatibility of the templates of different biometric traits. The biometric key is generated from a biometric construct using proposed cryptographic key extraction algorithm and then the key is applied on fused template to protect the template from various attacks. The implementation results obtained provides 100% GAR at 17% FAR i.e. authentication performance of the system is better as compared to other systems.

Keywords: Authentication · Biometric encryption/decryption
Biometric template protection · Cryptography · Wavelet

1 Introduction

Data security stresses over the certification of secrecy, trustworthiness and accessibility of personal information [1, 2]. Biometric is one of the advancements utilizing the exceptional behavioral or physical components of a person to identify the distinguished user [3]. Utilizing biometrics to authenticate human is easy to use, demands less cost and offers better security measures to maintain a strategic distance from information theft and security provocation [4]. Unimodal biometric Systems are developed to get privacy and security but it is highly influenced by different attacks like function creep, intrusion attacks, etc. Hence, use of multiple biometrics (e.g., Fingerprint, Iris and face) together is generally utilized as a part of some large scale biometric applications (e.g., FBI-IAFIS). It is beneficial as compare to single biometric system as it provides lower error rate, enhanced accessibility, a higher level of flexibility, and less susceptible to spoof attacks. Cryptography is the art of utilizing mathematical concepts to encode or translate the original biometric information [5]. It permits the storage of confidential information on an unreliable system like the web so that nobody can fetch it without the permission.

Z. Patel and S. Gupta (Eds.): ICFITT 2017, LNICST 220, pp. 264–273, 2018.
https://doi.org/10.1007/978-3-319-73712-6_28

Multi-biometric Cryptosystem is the science and innovation of deciding and quantitatively assessing various biological information particularly utilized for authentication purposes. Physical as well as behavioural biometric features are acquired from accurate sensors and individual features are extracted to form a biometric template for the enrolment process. At the time of identification or authentication, the system processes another biometric input which is compared against the stored templates yielding acceptance or rejection of the user. This system is commonly utilized for reducing misuse and storage of the private biometric templates which offers an advanced solution for the era of the cryptographic key, encryption procedure and protection of the biometric templates [6].

In this framework, unique biometric templates are changed into biometric- subordinate data which helps in recovering cryptographic keys [7, 8]. Matching is specifically performed by confirming the legitimacy of reconstructed keys.

The method based on multiple fingerprint is first proposed by Soutar [9]. In enrolment stage, unique features from the acquired biometrics are extracted. Correlation function between each individual input is calculated by applying inverse Fourier transform on the product of applied biometric inputs. Technique is advantageous due to ease of implementation but it has very poor accuracy.

Fuzzy commitment scheme is a combination of error correcting code and cryptography to achieve cryptographic primitive proposed by Juels and Wattenberg [10]. This method is advantageous because of good accuracy but it is not able to perform well with multi-modal biometrics.

Table 1. Comparison analysis on different techniques

Techniques	Author	Year	Char.	FAR/FRR
Biometric encryption	Soutar [9]	1998	Iris	0.03/0.054
Fuzzy commitment	Juels & Wattenberg [10]	1999	Iris	0.47/0
Fuzzy vault	Juels & Sudan [11]	2002	Fingerprint	5/0.01
Quantization	Feng & Wah [12]	2003	Online signature	28/1.2
Bio-hashing	Teoh [13]	2006	Face	0.93/0
Shielding function	Tuels [14]	2003	Fingerprint	0.054/0.03
Hybrid template protection	Y.J. Chin & T.S. Ong [15]	2014	Palmprint & Fingerprint	1/0

Fuzzy vault scheme uses cryptography construction proposed by Juels and Sudan [11], designed to work with unique features from multiple biometrics e.g. iris pattern, minutiae from fingerprints, etc. In this method, features are represented as an unordered set. Main advantage of this method is that due to the variation in biometric data at authentication side, the ability of the biometrics to work with an unordered set of Fuzzy vault scheme provides the promising solution to improve the security [16–18] but disadvantage is that security of this technique decreases because of infeasible reconstruction of the polynomial generated from the Reed-Solomon code. For the authentication of online signature, Shielding function is proposed by Tuels [19, 20] but it does not work well on multiple-biometric template.

2 Proposed Framework for Multi-biometric Cryptosystem

The paper proposes a technique to implement a framework for Wavelet- decomposition based feature level fusion for Multi-biometric cryptosystem as shown in Fig. 1. The system comprises of two basic modules: (1) Multi-biometric fusion and (2) Private template protection. Our aim is to reduce the FAR and FRR of the system as low as possible with optimum EER. The proposed system is implemented by using the concept of wavelet decomposition for fusion process and normal encryption algorithm is used for generation of the key. Wavelet decomposition is applied to each extracted feature templates and approximate coefficients are taken from each individual template to fuse multiple biometric templates and the key is added to make the fused template more secure. Single secure sketch is stored in the system database. Whenever, user comes for the authentication, system requires enrolled biometrics and it will compare with the stored database. If system generates the same key which was used at enrollment process then the user will be genuine otherwise it will reject the user to access the system. System is divided in individual block and all blocks are described below

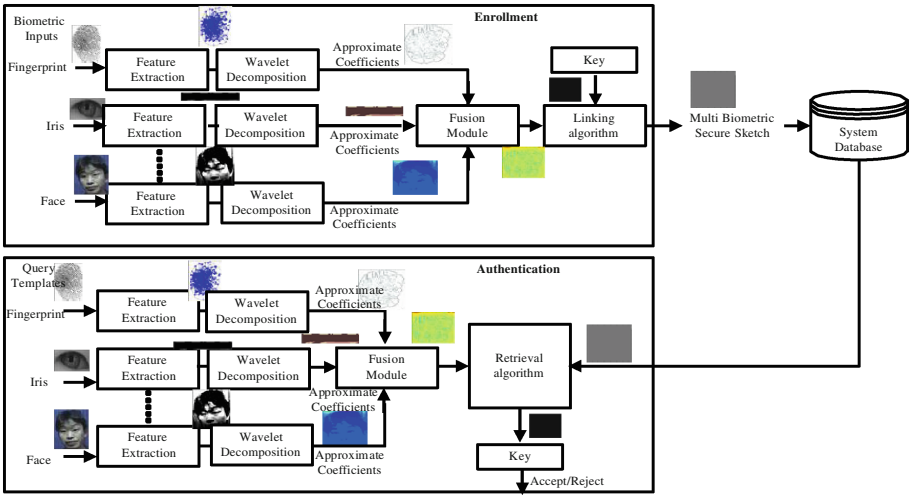

Fig. 1. Proposed multi-biometric cryptosystem using wavelet decomposition approach

2.1 Feature Extraction

Feature extraction methods for fingerprint, iris and face are described below.

Fingerprint feature extraction
It will extract ridges and bifurcation i.e. minutiae points from the fingerprint images using fingerprint image enhancement algorithm [21]. This technique requires less preprocessing and works better even with low-quality images.

Iris feature extraction
The image of iris includes undesirable data such as the pupil, sclera, eyelid, and eyelashes. Hence, before feature extraction, it must be pre-processed to remove unwanted portion. So, the preprocessing unit for the iris is required to perform image enhancement, iris segmentation, and iris normalization [22].

Face feature extraction
An important feature of the face extracted by applying 2D Principal Component Analysis (PCA) on the original biometric template. Suppose that there are training samples of images of $m \times n$ size, then the covariance matrix is calculated by

$$C = \frac{1}{N}\sum_{j=1}^{N}\left(A_j - \overline{A}\right)\left(A_j - \overline{A}\right)^T \tag{3}$$

Where, A is the sample image and $\overline{A}$ is a mean of sample images. The eigenvectors is calculated from the covariance matrix. The Eigen decomposition needs to be obtained by applying Singular Value Decomposition (SVD) then the data is simply projected onto the largest eigenvectors. To reduce the dimensionality, let V be the matrix whose columns contain the largest eigenvectors and D be the original biometric data. Then the projected data D′ is obtained as $D' = V^T D$ [23].

2.2 Wavelet Decomposition

Wavelet decomposition provides the decomposition matrix of applied feature template. The approximation and detailed coefficients are extracted from the decomposition matrix and approximate coefficient is taken for further processing of data because detailed decomposition matrix reduces the visibility of the biometric template [24]. In this paper, a single level of decomposition is used. Here, low-pass approximation coefficients and high-pass detailed coefficients are extracted. By using n level of decomposition the wavelet decomposition produced2n different sets of coefficients. Due to the down-sampling, the number of coefficients produced by decomposition process is same and there is no redundancy present.

2.3 Fusion of Feature Templates

Fusion of templates in the biometric system is not only the solution to the problem of single biometric, but it enhances the matching accuracy of the system. In order to extract relevant features and to remove the unwanted noise from raw biometrics, pre-processing and feature extraction is performed prior to fusion which overcomes the weakness of decision level fusion [25]. It is formed when feature vectors generated by multiple biometric templates are fused as a unified entity [25–27] so it has a prerequisite to first identify their nature and then apply only suitable algorithm to the biometrics. Here, the fusion is done by finding the contribution parameter (c_i) from each feature template $I(x, y)$ i.e. $c_i = \text{mean}\ (\text{mean}\ (I(x, y)))$ multiply by approximate

coefficient produced by wavelet decomposition method i.e. $I_A(x, y)$ [27]. Mathematically, it is represented by

$$f(x, y) = \sum_{i=1}^{n} c_i * I_A(x, y) \tag{4}$$

2.4 Key Generation Technique

Keys are directly generated from the fused feature templates. In existing methods, key is generated by applying random matrix and linear block coding on fused template i.e. RS encoder, BCH Encoder, etc. Hence, it is easy to detect by intruder. To improve the security of the system, instead of using one concept, multiple concepts are used to generate the key in proposed algorithm.

1. Generate the random matrix (R) of size of fused template.
2. Multiply the randomize matrix (R) by fused template (f).

$$\text{i.e.} \quad I_r = R(x, y) * f(x, y) \tag{5}$$

3. Perform the transform order (α) along the fused template [34] i.e.

$$\alpha = \frac{1}{M_1}\left[\left(\sum_{i=0}^{length(f)} f(i)\right) mod\left(2^L - 1\right)\right] \tag{6}$$

   Where, M_1 is the length of fused template and L is the number of bits used to represent the fused template.
4. Perform Hessenberg decomposition on the I_r to get orthogonal matrix Q_1.
5. The encrypted image is generated by

$$I_e = Q_1 * \alpha * Q_1' \tag{7}$$

6. Perform wavelet decomposition on I_e and find the approximate coefficient I_A. The key is generated by $k = I_A(x, y)$.

2.5 Key Binding Technique

Binding of the key (W_i) and fused template improve the privacy of feature templates in the system so that intruder cannot directly attack on the fused template. It is done by finding the average between fused template and generated key

$$W = avg\,(k(x, y), f(x, y)) \tag{8}$$

W is stored as a hash function in the system for further processing the data.

2.6 Key Retrieval Technique

By applying query templates at authentication side, the system calls the database template which is stored in secured form W_i to retrieve the key which is used to register the biometric templates. So it is the process between function of Hash value and query templates f' applied to verify the user. It is represented by

$$k' = 2 * W(x, y) - f'(x, y) \tag{9}$$

3 Experimental Results and Discussion

The fingerprint database for the design of the system is obtained from FVC 2004 while iris and face databases are obtained from CASIA. The experiment has been carried out in 4 set with 50 users in each technique. In set 1, the fusion of multi- fingerprint has been utilized. In set 2, the fusion of multi-iris has been utilized. Similarly, In set 3, a fusion of fingerprint and iris have been utilized. In set 4, a fusion of fingerprint, iris and face have been utilized. The ROC curves using different algorithm of fusion and template protection method is shown in below figures.

It shows the fusion of multi-biometric done using wavelet decomposition approach and Fourier transform of the concatenation of each template. Template protection methods use RS encoder and encryption algorithm to generate the key.

The parameter analysis of this cryptosystems is done by False Acceptance Rate (FAR) - It is the probability of an imposter being accepted as an authorized user, False Rejection Rate (FRR) - It is the probability of a legitimate user being rejected as an imposter, Equal Error Rate (EER) – It is the rate on which equal FAR and FRR is achieved, Genuine Acceptance Rate (GAR) – It is the rate at which the correct information is retrieved by the genuine user. Biometric cryptosystems require the helper data so even if it is attacked also it won't reveal the original information [7].

Table 1 shows the comparative performance analysis of different techniques proposed by different authors for multi-biometric cryptosystem.

Figure 2 shows that fusion is done by using wavelet decomposition approach and RS encoder is used to generate the key as a template protection method. It is observed that there is 50% EER with very high threshold i.e. very poor accuracy and GAR is also poor. So, we modified the fusion strategy by using Fourier transform of the concatenation of each template and encryption algorithm to generate the key as a template protection method. It is observed that there is 20% EER with low threshold i.e. very good accuracy and GAR is also 100% on FAR 57% as shown in Fig. 3.

Figures 4, 5 and 6 show that fusion is done by using wavelet decomposition approach and encryption algorithm is used on derived fusion template to generate the key as a template protection method for Multimodal, multi-finger, multi-iris respectively. It is observed that there is 0% EER with very low threshold i.e. very good accuracy and GAR is also increasing with 17% FAR i.e. maximum security for Multimodal case.

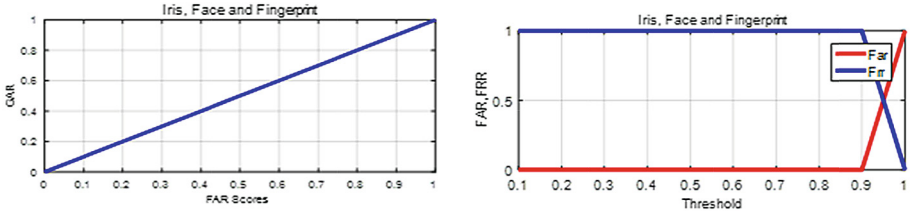

Fig. 2. Combination of wavelet decomposition on fusion and RS encoder as a key

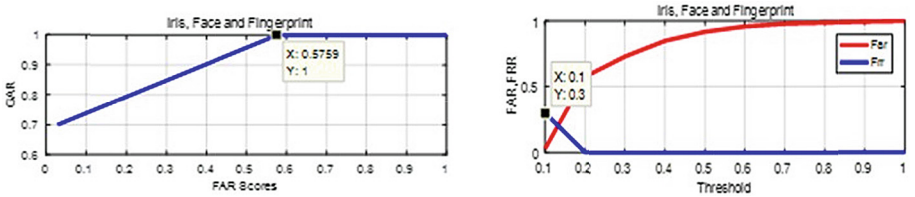

Fig. 3. Combination of fourier transform on concatenation of feature template and encryption algorithm on derived fused template

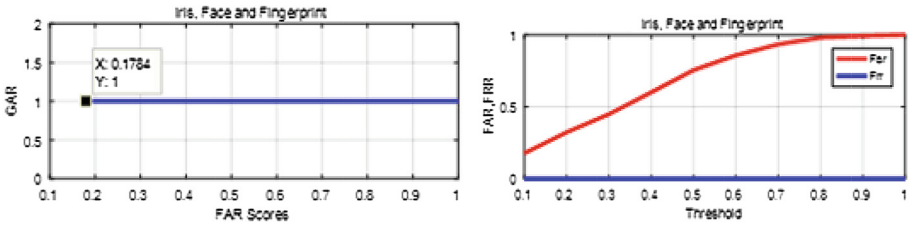

Fig. 4. Combination of wavelet decomposition on extracted feature in fusion process and encryption algorithm on derived fused template as a key based on fingerprint, Iris and Face

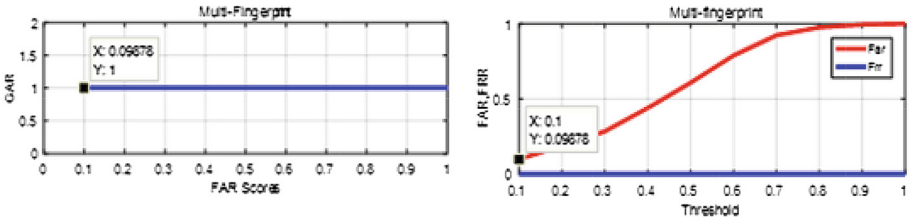

Fig. 5. Combination based on multi-fingerprint

Results show that proposed method gives better performance and security than existing technique. The hybrid approach gives 28% EER and 46% FAR with 100% GAR (threshold rate 13%) based on a combination of Fingerprint, Iris, and Face.

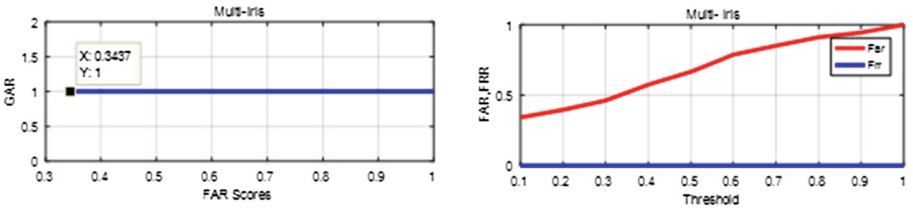

Fig. 6. Combination based on multi-iris

Wavelet decomposition approach gives 0% EER and 17% FAR with 100% GAR (threshold rate 0%). Here, threshold indicates the security levels. Lower threshold level indicates more security. Hence, wavelet decomposition approach provides lower FAR, FRR and better security on multi-modal biometrics. Proposed method along with existing techniques implemented using database mentioned above.

Tables 2, 3 and 4 show the comparison analysis on different techniques using multiple sets of biometrics.

Table 2. Comparison based on different fusion and private template protection technique

	Normal encryption [16]	Fuzzy commitment [17]	Fuzzy vault [18]	Shielding function [23]	Hybrid method [35]	Proposed method
Multi-finger	0.49/0.58	0.46/0.25	0.50/0.82	0.56/0.53	0.35/0.23	Error rate 0% with minimum threshold level i.e. maximum security
Multi-iris	0.50/0.70	0.42/0.59	0.43/0.48	0.42/0.26	0.5/0.63	
Finger & Iris	0.5/0.14	0.5/0.77	–	0.38/0.17	–	
Finger, Iris & Face		0.50/0.36	0.32/0.11	0.52/0.36	0.28/0.13	

Table 3. Comparison of different techniques with different combination of biometric trait in terms of EER/threshold

Fusion		Template protection technique (key)		Performance based on Iris, fingerprint, and face	
Concatenation [19]	Wavelet decomposition approach [24]	RS encoder [10]	Encryption algorithm [28]	EER/th	FAR/GAR
✓		✓		0.28/0.13	0.46/1
✓			✓	0.20/0.13	0.57/1
	✓	✓		0.5/0.95	1/1
	✓		✓	0	0.17/1

Table 4. Comparison of different techniques with different combination of biometric trait in terms of FAR/GAR

	Normal encryption [9]	Fuzzy commitment [10]	Fuzzy vault [11]	Shielding function [19]	Hybrid method [29]	Proposed method
Multi Finger	0.46/0.48	0.46/0.54	0.46/0.47	0.46/0.49	0.46/0.88	0.07/1
Multi Iris	0.46/0.47	0.46/0	0.46/0	0.46/0.66	046/0.46	0.34/1
Finger & Iris	0.46/0.46	0.46/055	0.46/0.93	0.46/0.75	0.46/1	0.7/1
Finger, Iris & Face	0.46/0	0.46/0.44	0.46/0.92	0.46/0.40	0.46/1	0.17/1

4 Conclusion

The proposed method developed multi-biometric system using the wavelet decomposition based fusion and Encryption algorithm on fused template as a template protection method that is accurate, reliable and secured. The proposed algorithm provides almost 0% EER and 100% GAR with 17% FAR on multimodal biometric and 0.9% FAR on same modal of biometric i.e. multi fingerprint. It is efficient compared to existing methods in terms of FAR, FRR and GAR.

References

1. Hellman, M., Deffie, W.: New direction in cryptography. IEEE Trans. Inf. Theory **22**(6), 644–654 (1976)
2. Devi, T.: Importance of cryptography in network security. In: International Conference on Communication Systems and Network Technologies (CSNT), April 2013
3. Jain, A.K., Ross, A., Prabhakar, S.: An introduction to biometric recognition. IEEE Trans. Circuits Syst. Video Technol. **14**(1), 4–20 (2004)
4. Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.: Biometric cryptosystems: issues and challenges. Proc. IEEE **92**(6), 948–960 (2004)
5. Fu, B., Yang, S.X., Li, J., Hu, J.: Multibiometric cryptosystem: model structure and performance analysis. IEEE Trans. Inf. Forensics Secur. **4**(4), 867–882 (2009)
6. Wild, P., Radu, P., Chen, L., Ferryman, J.: Towards anomaly detection for increased security in multibiometric systems: spoofing-resistant 1-median fusion eliminating outliers. In: IEEE International Joint Conference on Biometrics (IJCB), September 2014
7. Jain, A., Nandakumar, K.: Biometric authentication: system security and user privacy. IEEE Comput. Soc. **45**(11), 87–92 (2012)
8. Toli, C.-A., Preneel, B.: A survey on multimodal biometrics and the protection of their templates. In: Camenisch, J., Fischer-Hübner, S., Hansen, M. (eds.) Privacy and Identity 2014. IFIP AICT, vol. 457, pp. 169–184. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-18621-4_12

9. Soutar, C., Roberge, D., Stoianov, A., Gilroy, R., Vijaya Kumar, B.V.K.: Biometric encryption using image processing (1998)
10. Juels, A., Wattenberg, M.: A fuzzy commitment scheme. In: ACM Conference on Computer and Communications Security, December 1999
11. Juels, A., Sudan, M.: A fuzzy vault scheme. J. Designs Codes Cryptogr. **38**, 237–257 (2006). Springer
12. Feng, H., Wah, C.C.: Private key generation from on-line handwritten signatures. Inf. Manag. Comput. Secur. **10**, 159–164 (2002)
13. Teoh, A., Kim, J.: Secure biometric template protection in fuzzy commitment scheme. IEICE Electron. Express **4**, 724–730 (2007)
14. Huixian, L., Man, W., Liaojun, P., Weidong, Z.: Key binding based on biometric shielding functions, August 2009
15. http://www.scholarpedia.org/article/Cancelable_biometrics
16. Moon, D., Choi, W., Moon, K., Chung, Y.: Fuzzy fingerprint vault using multiple polynomials. In: IEEE 13th International Symposium on Consumer Electronics, May 2009
17. Jain, A.K., Pankanti, S., Nandakumar, K.: Fingerprint-based fuzzy vault: implementation and performance. IEEE Trans. Inf. Forensics Secur. **2**(4), 744–757 (2007)
18. Yang, X., Cao, K., Tao, X., Wang, R., Tian, J., Li, P.: An alignment-free fingerprint cryptosystem based on fuzzy vault scheme. J. Netw. Comput. Appl. **33**(3), 207–220 (2010)
19. Uhl, A., Rathgeb, C.: A survey on biometric cryptosystems and cancelable biometrics. J. Inf. Secur., January 2011. Springer International Publishing
20. Chikkerur, S., Cartwright, A.N., Govindaraju, V.: Fingerprint enhancement using STFT analysis. J. Pattern Recogn. **40**(1), 198–211 (2007). Elsevier
21. Hong, L., Wan, Y., Jain, A.: Fingerprint image enhancement: algorithm and performance evaluation. IEEE Trans. Pattern Anal. Mach. Intell. **20**(8), 777–789 (1998)
22. Zaveri, M., Kapur, A., Gawande, U.: A novel algorithm for feature level fusion using SVM. In Hindawi Publishing Corporation (2013)
23. Tokumoto, T., Lee, M,. Ozawa, S., Choi, Y.: Incremental two dimensional two directional principal component analysis for face recognition. In: IEEE Conference on Acoustics, Speech, and Signal Processing (ICASSP 2011) (2011)
24. Pavithra, C., Bhargavi, S.: Fusion of two images based on Wavelet transform. Int. J. Innov. Res. Sci. Eng. Technol. **2**(5), 1814–1819 (2013)
25. Kaur, H., Rani, E.J.: Analytical comparison of various image fusion techniques. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(5), 442–448 (2015)
26. Purushotham, A., Usha Rani, G., Naik, S.: Image fusion using DWT & PCA. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **5**(4) (2015)
27. Ramli, D.A., Jaafar, H.: A review of multibiometric system with fusion strategies and weighting factor. Int. J. Comput. Sci. Eng. **2**(4), 158–165 (2014)
28. Bhatnagar, G., Wu, Q.M.J.: Biometric inspired multimedia encryption based on dual parameter fractional fourier transform. IEEE Trans. Syst. Man Cybern. **44**(9), 1234–1242 (2014)
29. Patel, H., Paunwala, C., Vora, A.: Hybrid feature level approach for multi- biometric cryptosystem. In: IEEE International Conference on Wireless Communications, Signal Processing and Networking (Wispnet-2016), Chennai, 23–25 March (2016)