EER Analysis of Multimodal Biometric Identification System

Dr.A.Jagadeesan[1] | R.M.Madhumathi[2]

[1]Asst.Prof. (Sr.G)/EIE, Bannari Amman Institute of Technology, Erode,India,mails4jagan@gmail.com

[2] Instrumentation Engineering, Bannari Amman Institute of Technology, Erode,India,madhurm27@gmail.com

Abstract— *People find difficult to remember long cryptographic keys. Therefore researchers for a long time have been investigating ways to use biometric features of the user rather than memorable password or passphrases, in an attempt to produce tough and repeatable cryptographic keys. The goal is to integrate the volatility of the user's biometric feature into the generated keys, so as to construct a key unpredictable to a hacker who is deficient of important knowledge about the user's biometric .In earlier research, they have incorporated multiple biometric modalities into cryptographic key generation to provide better security. In this proposed approach, extraction of Minutiae points from fingerprint using Image Processing and Texture (MIPT) feature from iris are fused for the cryptographic key generation. The multimodal biometric identification system's effectiveness is measured by its accuracy and security. Performance analysis is carried out by calculating Equal Error Rate (EER) values for different databases between the existing and the proposed approach. Lower values of EER indicate the proposed approach accuracy. For providing better security, the False Not Matching Rate (FNMR) values of the proposed approach are less than the existing approaches.*

Keywords— ***Chinese Academy of Sciences Institute of Automation (CASIA) iris database, Fingerprint Verification Competition (FVC), Equal Error Rate (EER), False Matching Rate (FMR), False Non-matching Rate (FNMR)***

INTRODUCTION

Nowadays, it is widely accepted that biometrics, particularly image-based biometric will produce an error-free recognition results. But it is recognized that by proper system tuning and setup adjustment, the error of the biometrics systems can be reduced to the level needed for the operational use. The system performance evaluation can be achieved by insights on system tuning, setup adjustment, selection of the system and risk mitigation procedures that are suitable for the operational needs. The performance evaluation protocols and merits should be suitable for the task and scenario to which the system is applied. The evaluation merits are a vital factor for evaluating the effectiveness of the multimodal biometric system. The right choice of deciding the evaluation metric is very important for comparing the performance of the multimodal biometric system. The steps involved in the first proposed approach [12] of cryptographic key generation from multimodal biometrics, extraction of Minutiae points from fingerprint using Image Processing, extraction of Texture features from iris, feature level fusion of fingerprint and iris features. The cryptographic key generation from the fused features with the fingerprint databases and iris samples are taken from Chinese Academy of Sciences Institute of Automation (CASIA) dataset. The data set consists of 756 images comprising of 108 classes with 7 images per class. Images were captured at a resolution of 320 x 280. The images in this data set are strongly occluded and defocused. For each eye, 7 images are captured in two sessions, where three samples are collected in the first session and four in the second session. Finally a 256-bit secure cryptographic key is formed from the multimodal biometric template. It also deals with the analysis of the first proposed approach with the two existing methods. For the experimental analysis EER values are calculated from the performance analysis graphs, for the MIPT approach and the existing methods (Conventional Score Level Fusion (CSLF) [2] and Frequency based Approach for features Fusion in Fingerprint and Iris (FAFFI) [11]) .The analysis of the proposed system is significant in terms of effectiveness over the existing ones.

2.REVIEW OF RELATED LITERATURE

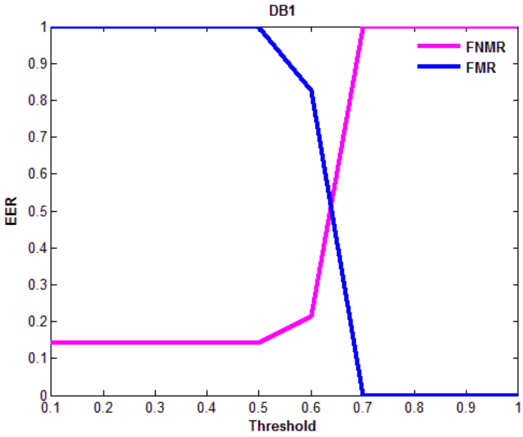
A copious number of researches are available in the literature for generating cryptographic keys from biometric modalities and multimodal biometrics based user authentication. Recently, among researchers, a great deal of attention have been received on developing approaches for cryptographic key generation from biometric features and authenticating users by combining multiple biometric modalities. A concise review of few recent researches is presented here. Simple effort in the literature is to inspect the performance of an adaptive multimodal fusion algorithm [1] on authentic biometric data. An evolutionary approach has been presented in an adaptive combination of several biometrics to provide the optimal performance for the desired level of security. The optimal fusion strategy and the corresponding fusion parameters have been determined by using the adaptive combination of multiple biometrics. Their experimental results have demonstrated that the score-level approach can accomplish better and stable performance than the decision level approach can accomplish better and stable performance than the decision level approach. Experimental results have demonstrated that the score-level approach can accomplish better and stable performance than the decision level approach. Multimodal biometric identification system based on conventional score level fusion [2]. It contains two sets of sensors, feature extractors, matchers, and score normalization functions. Also, the proposed framework is designed to function in sequential input mode i.e. Both biometric inputs are obtained independently. The framework operates in the following sequence. Initially one biometric input is obtained and sent to the feature extractor. The processed reference is compared with the templates in the database by means of the provided matcher. When the matcher finishes the processing of the first biometric and produce the matching output, the second biometric input is processed and kept ready for matching. Then the second biometric reference is compared with the templates by using the same matcher and produces the output one of the major benefits of using the single matcher for both modalities is that both the output scores will be in the same format and so there is no need for any normalization functions. This framework is designed to be flexible so that any set of biometrics, matcher and fusion technique can be utilized in the execution of the framework. Some of their perspectives are given in detail. In security applications, [5]have proposed a modular, effective multimodal biometrics security authentication and monitoring system that employs a bio- dynamic physiological profile, unique for each individual, and advancements in behavioral and other biometrics, such as face, speech, gait identification, and seat-based anthropometrics. Human Monitoring and Authentication using Biodynamic Indicators and Behavioral Analysis (HUMABIO) have addressed several limitations in biometric authentication that provides the basis for enhancing existing sensors, develop algorithms, and design applications for generating new, unobtrusive biometric authentication procedures in security sensitive, controlled environments. Detailed evaluation and summarization for using multi-scale edge detection technique[6] as a pre- processing step to effectively localize the iris followed by a feature extraction technique which is based on a combination of some multi-scale feature extraction methods. A special Gabor filters and wavelet maxima components have been used by this combination. Lastly, they have proposed a promising feature vector representation using moment invariants. This has resulted in a compact and competent feature vector. Also, an exclusive OR operation based fast matching scheme has been developed to calculate bits similarity. Here the testing was performed using CASIA database. The experimental results have proved that their system has robust performance and could be employed for personal identification in an effectual manner and comparable to the best iris recognition algorithm found in the current literature. provided by multiple domain experts based on the rank-level fusion integration technique[7]. The proposed multimodal biometric system holds a number of distinct qualities, which verifies the individual matcher (face, ear, and signature) identity by employing Principal Component Analysis (PCA) and Fisher's Linear Discriminate (FLD) techniques. Also a rank-level fusion technique has been used by this system to combine the results acquired from diverse biometric matchers. They have also discussed the multi-biometric design of rank level fusion and its performance over a variety of biometric databases. An overview of the iris and retina biometrics and discussed the merits and demerits of each technology [9]. They have assumed that the fusion of these two metrics can possibly enhance the biometric system, and the system built as such would obtain no or little additional cost to hold both metrics. This is instinctively true because both technologies are related to the eye and a single image acquisition device may be designed to enroll both biometrics at the same time. A Geometry Preserving Projections (GPP) approach is subspace selection, which is capable of selecting different classes and maintaining the intra-modal geometry of samples within an identical class [10]. By means of GPP, classification has been performed by projecting all raw biometric data from various identities and modalities onto a unified subspace. Here, the training stage has been performed once and a unified transformation matrix has been used in order to project multiple modalities. Their proposed system functions well even though some modalities are not available. The efficacy of the GPP for individual recognition tasks has been demonstrated by their experimental results. Multimodal biometric identification systems based on iris and fingerprint traits [11]. The multimodal biometric system is an advancement of multi-biometrics, which provides a different perspective on features fusion in more detail, a frequency-based approach results in a homogeneous biometric vector by combining iris and fingerprint data. Then, a matching algorithm based on hamming-distance uses the combined homogenous biometric vector. More engaging results are obtained by the multimodal system with the aid of several widely used databases. Multimodal biometric fusion is performed by fusing the biometric template extracted from each pair of fingerprints and irises of a user. Initially, the identifiers taken from the original images are stored in diverse feature vectors. Then, each vector is normalized in polar coordinates and then combined. Lastly, the matching score calculation is ROI shows a uniform level of brightness by equalizing the histogram.

3. EQUAL ERROR RATE ANALYSIS OF FIRST EXISTING METHOD

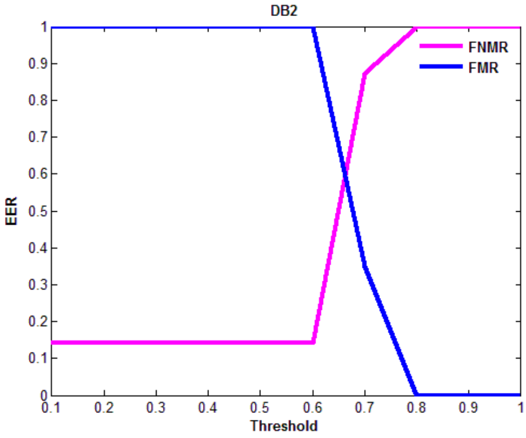
The performance of the fingerprint iris fusion based identification system proposed [2] is discussed in this section. With the aid of the methods utilized in the presented multimodal system, the template was constructed and then, the template is used to generate the bio-crypto key vector of the fingerprint and the iris image from the corresponding fingerprint and iris databases. Then, the matching process is done against the genuine fingerprint and imposter fingerprint and genuine iris and imposter iris is carried out to find the FMR and FNMR of the approach in fingerprint and iris identification system. The graph is drawn to find the efficiency of the approach in different data bases. The performance analysis graph with FMR and FNMR values on four databases DB1, DB2, DB3 and DB4 is shown in figure 3.1(a) 3.1 (b) 3.1(c) and 3.1(d) respectively and the EER values are tabulated in the table 3.1.

For experimentation, the fingerprint images obtained from FVC sources and the iris images from CASIA iris databases are employed. Then, the matching process is carried out against the genuine fingerprint and iris with the imposter fingerprint and iris images to find the FMR and FNMR of the approach in the multimodal biometric identification system.

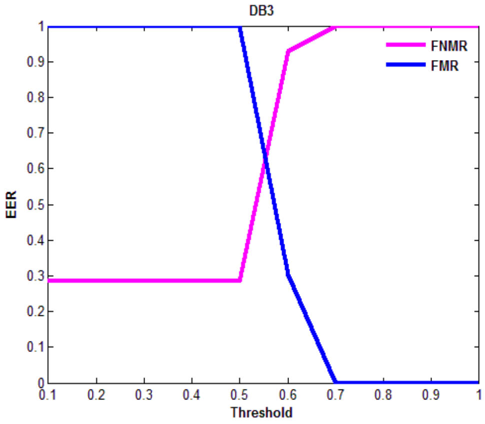
Figure 3.1 EER analysis curves for different database by CSLF approach



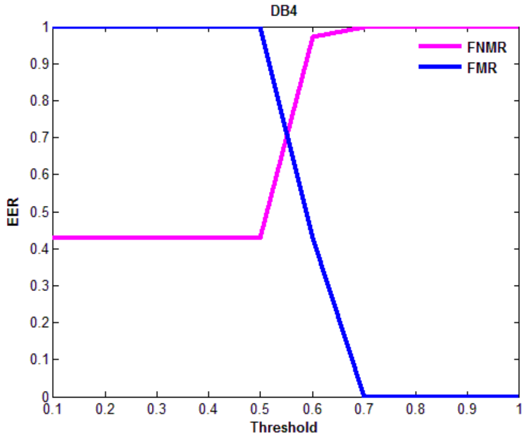
(a) EER value for DB1



(b) EER value for DB2



(c) EER value for DB3



(d) EER value for DB4

Table 3.1 EER values of different databases by CSLF approach

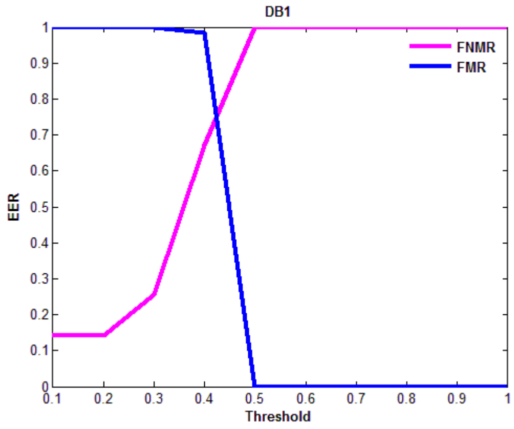
S.No	*Databases*	*EER*
1	DB1	0.5
2	DB2	0.6
3	DB3	0.61
4	DB4	0.7

4.Equal Error Rate Analysis For Second Existing Method

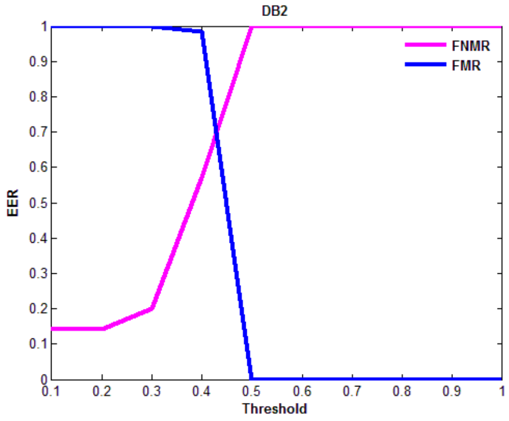
The performance of the frequency-based approach for features fusion in finger prints and iris multimodal biometric identification system presented by Vincenzo et al (FAFFI) [11] is discussed in this section. In order to compute the efficiency of this multimodal biometric system, the genuine and imposter matching score is composed for different fingerprint and iris images. The composed values are further utilized to find the FMR and FNMR values by matching the features of the fingerprint and the iris images with corresponding features stored in the databases. The graph is plotted for the computed values to find the efficiency in acceptance of the genuine user and rejection of the imposter user for different threshold levels, The performance analysis graph with FMR and FNMR values on four databases DB1, DB2, DB3 and DB4 is shown in figure 4.1(a), 4.1(b), 4.1(c), and 4.1(d) respectively and the EER values are tabulated in the Table 4.1

For experimentation, the fingerprint images obtained from FVC sources and the iris images from CASIA iris databases are employed. Then, the matching process is carried out against the genuine fingerprint and iris with the imposter fingerprint and iris images to find the FMR and FNMR of the approach in the multimodal biometric identification system.

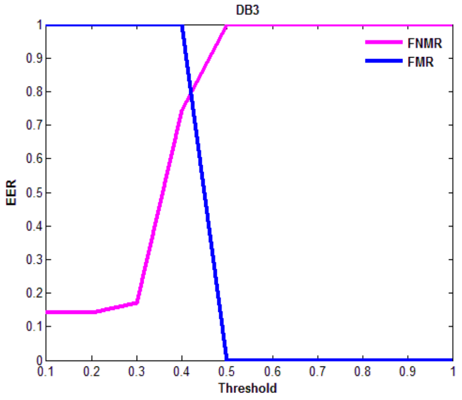
Figure 4.1 EER analysis curves for different database by FAFFI approach



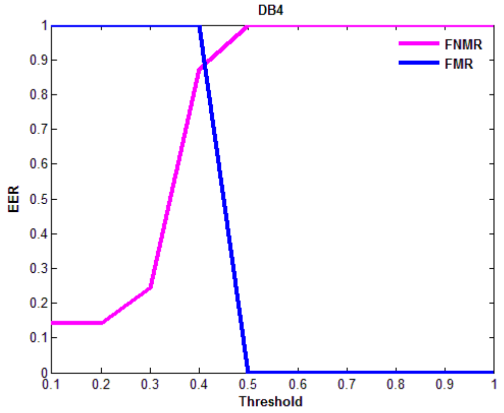
(a) EER value for DB1



(b) EER value for DB2



(c) EER value for DB3



(d) EER value for DB4

Table 4.1 EER values of different databases by FAFFI approach

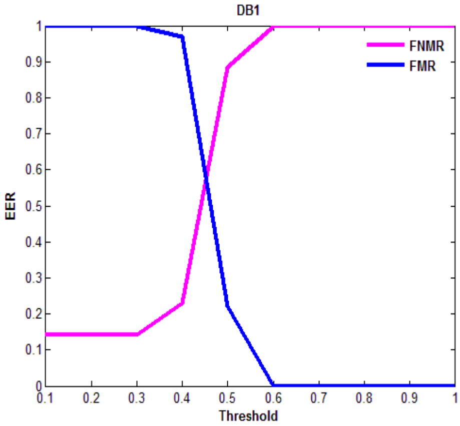
S.No	*Databases*	*EER*
1	DB1	0.73
2	DB2	0.7
3	DB3	0.75
4	DB4	0.88

5. EQUAL ERROR RATE ANALYSIS OF PROPOSED APPROACH

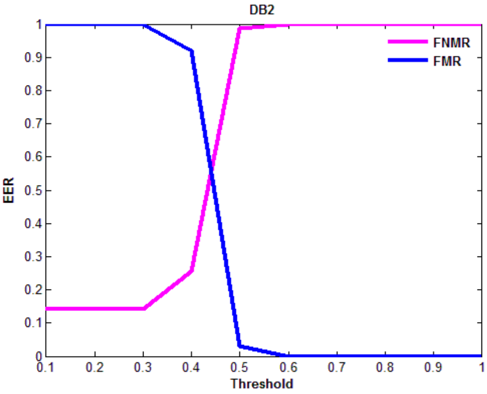
The performance analysis of the enhanced description of the proposed secured cryptographic key generation from multimodal biometric is given in detail here. It extracted the minutiae points and texture properties from the subsequent steps such as image preprocessing by histogram equalization and Wiener filtering ,image segmented by orientation field estimation and image enhancement by binarization and morphological process. On the other hand, the texture feature is extracted of iris image utilization the following steps namely, segmentation, estimation of iris boundary and normalization. Then, the extracted features are used to perform the fusion process, in which it will make use of the feature level fusion technique. Then, it has fused the extracted features at the feature level to obtain the multi biometric template and subsequently generated a 256-bit secure cryptographic key from the multi-biometric template.

For experimentation, the fingerprint images obtained from FVC sources and the iris images from CASIA iris databases are employed. Then, the matching process is carried out against the genuine fingerprint and iris with the imposter fingerprint and iris images to find the FMR and FNMR of the approach in the multimodal biometric identification system. The performance analysis graph with FMR and FNMR values on four databases DB1, DB2, DB3 and DB4 are shown in figure 5.1 (a), 5.1(b), 5.1(c) and 5.1(d) respectively and the EER values are tabulated in the Table 5.1

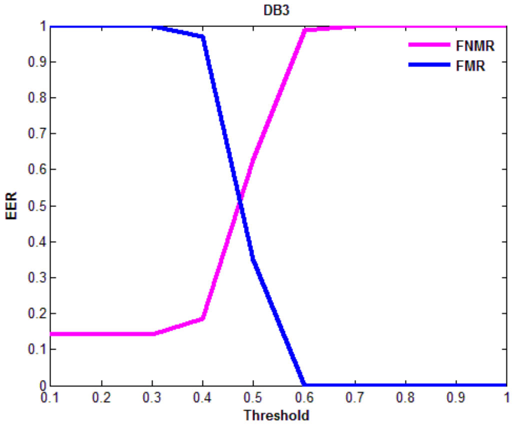
Figure5.1 EER analysis curves for different database by MIPT approach



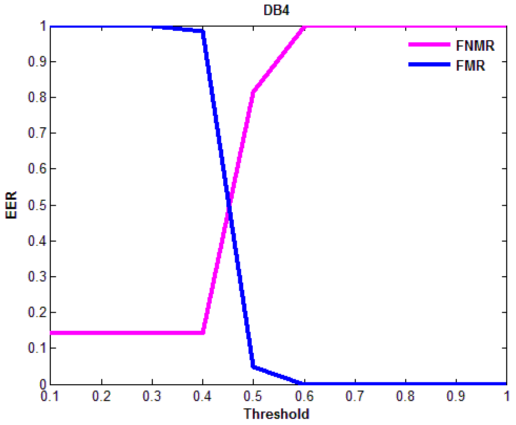
(a) EER value for DB1



(b) EER value for DB2



(c) EER value for DB3



(d) EER value for DB4

Table 5.1 EER values of different databases by MIPT approach

S.No	*Databases*	*EER*
1	DB1	0.55
2	DB2	0.53
3	DB3	0.5
4	DB4	0.5

Table 5.2 Comparative EER values for the existing approaches and the proposed approach

S.No	**Input databases (fingerprint and iris images)**	**EER values by**		
		Existing approaches		***Proposed approach***
		CSLF approach	***FAFFI approach***	***MIPT Approach***
1	DB1	0.5	0.73	**0.5**
2	DB2	0.6	0.7	**0.56**
3	DB3	0.61	0.75	**0.55**
4	DB4	0.7	0.88	**0.53**

The table 5.2 shows the comparative EER values of first proposed approach and the two existing methods From this table the first proposed approach is having less EER value compared with the existing method .The EER results ensure the accuracy of the first proposed approach method.

6.CONCLUSION

In this paper the MIPT approach of secured cryptographic key generation from multimodal biometric is discussed .It extracted the minutiae points and texture properties from the fingerprints and iris images respectively. The extraction process utilized the subsequent steps such as images preprocessing by histogram equalization and Wiener filtering, image segmented by orientation field estimation and image enhancement by binarization and morphological process . On the other hand, the texture features are extracted from the iris image utilizing the steps namely, segmentation, estimation of iris boundary and normalization. Then, the extracted features are used to perform the fusion process, in which it will make use of the feature level fusion technique. Then, it has fused the extracted features at the feature level to obtain the multi-biometric template and subsequently generated a 256-bit secure cryptographic key from the multi-biometric template. It also describes the experimental results of generating cryptographic key from multimodal biometric for different databases for the proposed approach (MIPT) and the two existing approaches. From the performance analysis curve the EER values are calculated for the MIPT approach and the two existing approaches. The EER values in table 5.2 clearly show that the proposed MIPT method is more effective than the existing methods CSLF and FAFFI.

REFERENCES

1. Ajay Kumar, Vivek Kanhangad & David Zhang 2010, ‘A New framework for adaptive multimodal biometrics management’, IEEE Transactions on Information Forensics and Security, vol. 5, pp. 92-102.
2. Asim Baig, Ahmed Bouridane, Fatih Kurugollu & Gang Qu, 2009, ‘Fingerprint – iris fusion based identification system using a single hamming distance matcher’, Symposium on bio-inspired learning and intelligent systems for security, Edinburgh, Scotland, United Kingdom, pp. 9-12.
3. Chinese Academy of Sciences - Institute of Automation (CASIA), CASIA iris image database. Available from: http:// www. idealtest. org/db DetailForUser.do?id=4 [8 August 2005]
4. Choubisa, T, Sahoo SK & Mahadeva prasanna, SR 2012, ‘Multimodal biometric person authentication: a review’, IETE tech rev, vol. 29, pp. 54-75.
5. Ioannis, G, Damousis, Dimitrios Tzovaras, & Evangelos Bekiaris 2008, ‘Unobtrusive multimodal biometric authentication: the HUMABIO project concept’, Eurasip Journal on Advances in Signal Processing, vol. 2008, pp.1-11.
6. Makram Nabti, Lahouari Ghouti & Ahmed Bouridane 2008, ‘An effective and fast iris recognition system based on a combined multi-scale feature extraction technique’, Pattern Recognition Elsevier Journal, vol. 41, pp. 868-879.
7. Maltoni, D, Maio, D, Jain AK & Prabhakar, S 2003, Handbook of Fingerprint Recognition, springer-verlag, New york, USA.
8. Monwar, MM & Gavrilova, ML 2009, ‘Multimodal biometric system using rank-level fusion approach’, IEEE Transactions on Systems, Man and Cybernetics, Part B: Cybernetics, vol. 39, no. 4, pp. 867-878.
9. Sadowitz, M, Latifi, S, & Walker, D 2008, ‘An overview of iris and retina scans and their fusion in a biometric system’, Proceedings of the international conference on image processing, computer vision, and pattern recognition, Nevada, USA, pp. 119-123.
10. Tianhao Zhang, Xuelong Li, Dacheng Tao & JieYang 2008, ‘Multimodal biometrics using geometry preserving projections’, Pattern Recognition Elsevier Journal, vol. 41, no. 3, pp. 805-813.
11. Vincenzo Conti, Carmelo Militello, Filippo Sorbello & Salvatore Vitabile 2010, ‘A frequency-based approach for features fusion in fingerprint and iris multimodal biometric identification systems’, IEEE Transactions on Systems, Man and Cybernetics, Part C: Applications and Reviews, vol. 40, no. 4, pp. 384-395.
12. Jagadeesan A & Duraiswamy K 2011, ‘Protected bio-cryptographic key invention from multimodal modalities: feature level fusion of fingerprint and iris’, European Journal of Scientific Research, vol.49 no.4, pp.484-502.
13. Jagadeesan A, Thillaikkarasi T & Duraiswamy K 2010, ‘Cryptographic key generation from multiple biometric modalities: fusing minutiae with iris feature’, International Journal of Computer Application,vol.2,no.6,pp.16-26.