IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Cryptographic key Generation from Multimodal Biometrics using MIPT Method

R. Ramji*[1] and S. Devi[2]

*[1]Assistant Professor, Electronics and Communication Engineering, Government College of Engineering, Thanjavur, Tamil Nadu, India

[2]Professor, Electronics and Communication Engineering, PRIST deemed to be University, Thanjavur, Tamil Nadu, India

Abstract: Cryptography is often used in an information technology security environment to protect data that is sensitive, has a high value, or is vulnerable to unauthorised disclosure or undetected modification during transmission or while in storage. Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a cryptographic key. This Recommendation discusses the generation of the keys to be managed and used by the approved cryptographic algorithms. This paper proposed first approach method Minutiae points from fingerprint using Image Processing and Texture features from iris (MIPT) for 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. Simulation and experimental results are verified using MATLAB/Simulink platform.

***Index Terms* - Biometric systems, CSLF, Cryptography key generation, MIPT.**

I. INTRODUCTION

Cryptographic keys are widely used in access control to computing resources, bank accounts in ATM systems, and user validation in e-business. Conventionally, system random-selected or user-determined PINs and passwords are utilised to generate unique keys for access control. However, system random-selected keys are easy to forget, and user-determined keys are subject to dictionary attacks and also easy to transfer (Saad et al. 2015). Biometrics, such as the face, voice, iris, and fingerprint, contribute specific characteristics of each individual. Therefore, biometric data potentially can be taken as good alternatives, or supplements, to PINs and passwords (Subhas Barman et al. 2015). Multimodal biometric authentication has lately evolved as an interesting research area. In addition to this it is more consistent as well highly proficient than knowledge-based (e.g. password) and token-based (e.g. key) techniques by Nageshkumar et al. (2009). Multiple biometric traits are successfully utilised by quite a few researchers to attain user authentication Tianhao et al. (2008), Yan & Yu (2008), Muhammad & Jiashu (2008) and Donald & John (2008). Security-conscious customers have set stringent performance requirements, and thereby multimodal biometrics was expected to convene this requirement. The advantages of multimodal biometrics are improved accuracy, in case if sufficient data is not extracted from a given biometric sample, it can serve as a secondary means of enrollment as well as verification or identification and the capability to identify endeavours to spoof biometric systems via non-live data sources particularly fake fingers. The preference of the biometric traits to be combined and the application area both serves as the major constraints to find out the efficacy of the multimodal biometrics. The extraction of Minutiae points from fingerprint using Image Processing and Texture features from Iris (MIPT) approach, for a cryptographic key generation, fingerprint and iris features are combined. Since it is intricate for an intruder to spool multiple biometric traits concurrently, there are possibilities to bestow prominent security with the utilisation of multimodal biometrics for key generation. The necessity to memorise or carry lengthy passwords or keys is averted by the integration of biometrics within the cryptography. The steps involved in the proposed approach based on multimodal biometrics for cryptographic key generation are extraction of minutiae points from fingerprint using image processing, extraction of texture features from Iris, feature level fusion of fingerprint and iris features and the cryptographic key generation from fused features (Jain & Rose, 2008, Balakumar & Venkatesan, 2012).

This paper describes the key generation from multimodal biometrics for cryptography using MIPT approach, and the performance analysis are compared with the existing methods of CSLF proposed by Asim et al. (2009) and FAFFI method proposed by Vincenzo et al. (2010). The experimental results of the proposed and existing methods are evaluated and compared.

II. MULTIMODAL BIOMETRIC SYSTEM

The multimodal biometric system uses multiple sensors or biometrics to overcome the limitations of unimodal biometric systems. For instance, iris recognition systems can be compromised by ageing rides and finger scanning systems by worn-out or cut fingerprints. While unimodal biometric systems are limited by the integrity of their identifier, it is unlikely that several unimodal systems will suffer from identical limitations. Multimodal biometric systems can obtain sets of information from the same marker (i.e., multiple images of an iris, or scans of the same finger) or information from different biometrics (requiring fingerprint scans and, using voice recognition, a spoken passcode). Multimodal biometric systems can integrate these unimodal systems sequentially, simultaneously, a combination thereof, or in series, which refers to sequential, parallel, hierarchical and serial integration modes, respectively (Choubisa et al. 2012).

In certain uses, more than one biometric feature is used for attaining developed security and for handling disappointment to register locations for particular handlers. Such organisms are known as multimodal biometric systems. Performance of a biometric system is measured by their identifying power, which is calculated using the false rejection and false acceptance rates. Single modality biometric identification systems force users to a trade-off between these two rates, as both of them cannot be reduced simultaneously. Knowing and optimising system's identifying power and making sure that it is acceptable for the application are critical to a system's success. Recently there has been a lot of interest in multimodal biometrics (Varamachaneni et al. 2003). The multimodal biometric system utilises two or more individual modalities, e.g., face, gait, iris and fingerprint, to improve the recognition accuracy of conventional unimodal methods. Using multiple biometric modalities has been shown to decrease error rates, by providing additional useful information to the classifier. Different features can be used by a single system or separate systems that can operate independently and their decisions may be combined. The aim of multi-biometrics is to improve the quality of recognition over an individual method by combining the results of multiple features, sensors, or algorithms. The key to multimodal biometrics is the fusion (i.e., combination) of the various biometric model data on the feature extraction, match score, or decision level.

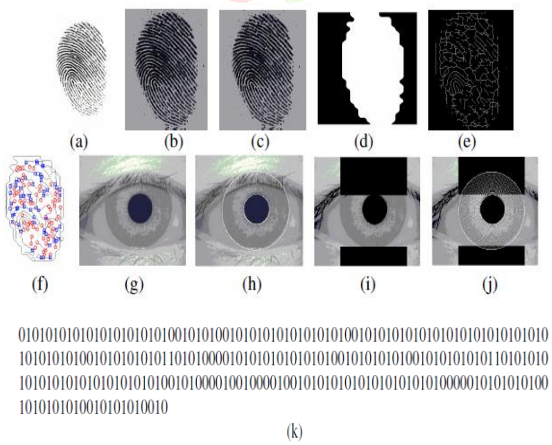
Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a 'live' user is indeed present at the point of data acquisition (Jayalakshmi et al. 2012). Another step ahead for improved security is to employ multimodal biometrics for generating cryptographic keys. Biometric cryptography based on multiple modalities is a technique that makes use of the multimodal biometric features to encrypt data, which can improve the security of the encrypted data and overcome the shortcomings of the biometric cryptography (Nemanja et al. 2015).

III. CRYPTOGRAPHIC KEY GENERATION FROM MULTIMODAL BIOMETRICS

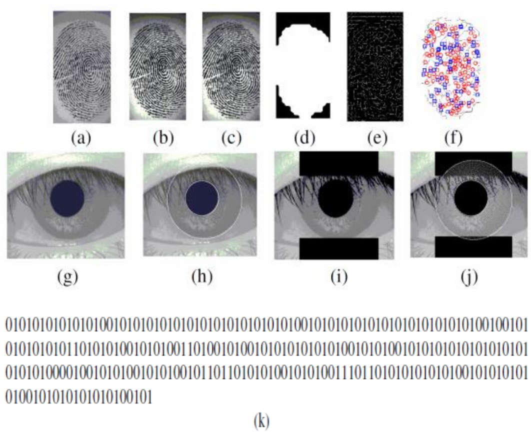
MIPT Approach

The proposed multimodal biometrics based MIPT approach (iris and fingerprint) is utilised for a secure cryptographic key generation. The proposed approach comprises three modules namely feature extraction, multimodal biometric template generation and cryptographic key generation. Firstly, the features, minutiae points and texture properties are extracted from the fingerprint and iris images respectively. After that, the extracted features are combined together at the feature level to build the multi-biometric template. Finally, a 256-bit secure cryptographic key is formed from the multimodal biometric template. The fingerprint images acquired from publicly available sources and the iris images from CASIA iris database have been used for testing. The experimental result (lesser EER values) shows the efficiency of the proposed system. The obtained results through the experimentation from the sample images of databases DB1, DB2, DB3 and DB4 are depicted in Fig. 3.

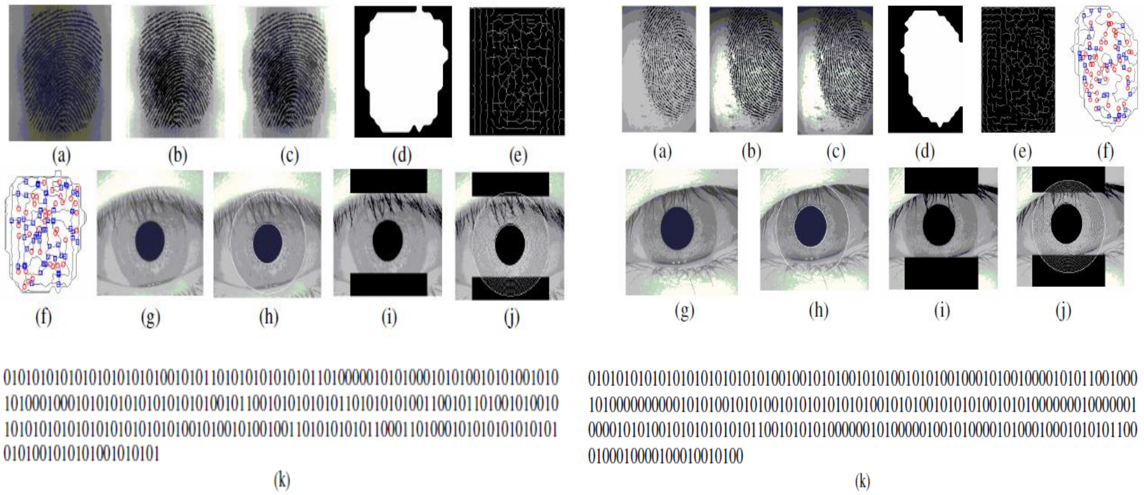
The Fig.1 shows all the intermediate results obtained before generating the cryptographic key from the multimodal biometric template using proposed MIPT approach. From this figure it is observed that (a) Input fingerprint image (b) Histogram equalized image (c) Wiener filtered image (d) Segmented image (e) Morphological processed image (f) Fingerprint image with minutiae points (g) Input iris image (h) Located pupil and iris boundary (i) Detected top and bottom eyelid region (j) Segmented iris image (k) Generated cryptographic key for DB1, DB2, Db3 and DB4 respectively.



For DB1



For DB2



For DB3 For DB4

Fig.1 Cryptographic Key Generation from Multimodal Biometrics using proposed MIPT approach

IV. EXPERIMENTAL ANALYSIS

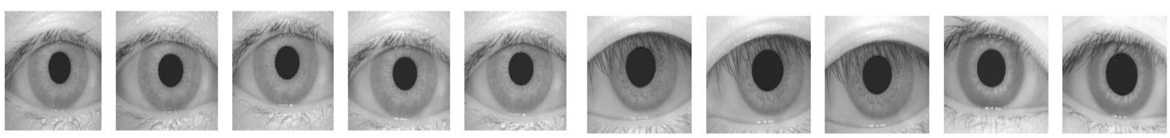
The proposed multimodal biometric system for a secure key generation from the fingerprint and iris template has been implemented in Matrix Laboratory (MATLAB). The experimentation has been carried out on a 3.20 GHz i5 Personal Computer (PC) machine with 8 GB main memory running on a 64-bit version of windows 2007. The experimental analysis of the approaches has been done on a standard FVC fingerprint database and CASIA iris databases, which contains real and synthetic images. It's more difficult to find out the fingerprint and iris images for the same person in the publicly available sources. Thus, it has pushed to generate the databases which contain fingerprint and iris images. So, it has been utilized in the standard databases for generating the combination of fingerprint and iris databases. The main objective is to compare the performance of the proposed multimodal biometric systems with the existing methods with the aid of the standard fingerprint and iris databases. By combining both the fingerprint and the iris image databases, it has formed a new set of four databases DB1, DB2, DB3 and DB4 which comprises of 140 images (70 fingerprint images and 70 iris images). Here, some of the sample fingerprint and iris images taken from the chosen databases are shown in Figs. 2 and 3 respectively.

The system performance evaluation can obtain the insights on system tuning setup adjustment and the selection of the system and risk mitigation procedures that are suitable for the operational needs. On the other hand, the performance evaluation protocols and metric should be suitable for the task and scenario to which the systems are applied. The evaluation metrics are a vital factor in evaluating the effectiveness of the multimodal biometric systems. The right choice of deciding the evaluation metrics is very important for comparing the performance of the multimodal biometric systems. Based on the fact, two standard evaluation metrics, FMR and FNMR have been chosen to analyse the biometric systems with the aid of the FVC fingerprint database and the CASIA iris database. Since the proposed system is not an ordinary biometric-based recognition system, the conventional metrics of an ordinary biometric system such as FMR-FNMR representation and ROC curves are not suitable for distinguishing the performance of the system. There is a severe tradeoff among FMR and FNMR. If the threshold is decreased to make the system more liberal regarding input variations and noise, then the FMR increases conversely, if the threshold is increased to make the system more secure, then the FNMR increases accordingly. Hence the system performance was noted at all operating points, i.e., the threshold in ROC curves where FNMR is plotted as a function of FMR in Maltoni et al. (2003).

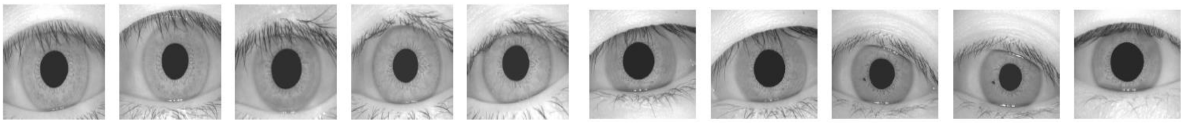
For DB1 For DB2

For DB3 For DB4

Fig. 2 Sample input images of fingerprint databases



For DB1 For DB2



For DB3 For DB4

Fig. 3 Sample input images of iris databases

The FMR shows the proportion of persons who were falsely accepted during the characteristics comparison. Those efforts that were previously refused, Failure to Acquire (FTA) rate due to a low quality (e.g. of the image), contrary to FAR, are not taken into consideration. It depends on the application whether a falsely accepted feature contributes to increasing the FAR or FRR. The FNMR shows the proportion of persons who were falsely not accepted during the characteristics comparison. Those efforts that were previously rejected FTA due to a low quality (e.g. of the image), contrary to FRR, are not taken into consideration. Again, it relies on the application whether a falsely non-accepted feature contributes to increasing the FRR or FAR.

The background Information with the aid of the fingerprint and iris image databases has generated the biometric cryptographic key from the computed biometric templates of fingerprint and iris. Subsequently, bio-crypto key K_{ij} is generated from the multimodal biometrics system, which is matched against the fingerprint and iris images F_{ki} ($j< k \leq 8$) and the genuine matching score (gms) is obtained. The number of obtained matches is known to be the Number of Genuine Recognition Attempts (NGRA). Generally, three types of rejection may happen for each fingerprint and iris images F_{ij} and these rejections are summed up, and it is stored in an index REJ_{ENROLL}. Where REJ_{ENROLL} is the rejection ratio in the enrollment phase, Fail (F) is the enrollment which cannot be possible by the algorithm, Timeout (T) is the enrollment that goes above the maximum allowed time, Crash (C) is the algorithm that crashes during fingerprint matching.

$$FNMR(t)=\frac{card\{gms_{ijk} \mid gms_{ijk} < t\} + REJ_{NGRA}}{NGRA} \quad (1)$$

where, card represents the cardinality

gms_{ijk} - genuine matching score matrix

t - threshold

REJ_{NGRA} - Rejection ratio in the number of genuine recognition attempts

NGRA - Number of genuine recognition attempts

In addition to, each key from the fingerprint and the iris key K_{1i} , i = 1,2,…..10 is matched against with the first set of fingerprint and iris image from database F_{1k} ($i< k\leq 10$) and the corresponding impostor matching score (ims) is computed. The number of matches denoted as Number of Imposter Recognition Attempts (NIRA) is ((10x9) /2) = 45 only if, $REJ_{ENROLL} = 0$.

$$FMR(t)=\frac{card\{ims_{ik} \mid ims_{ik} \geq t\}}{NIRA} \quad (2)$$

where, card represents the cardinality

ims_{ik} - Imposter matching score matrix

t - threshold

NIRA - Number of imposter recognition attempts

Furthermore, the FMR (t) and FNMR (t) are calculated from the above distributions for t ranging from 0 to 1. Then, the ROC curve is plotted FMR versus FNMR for varying threshold t. The plotted ROC curve is extensively used in the contest to compare the performance of different algorithms. One more parameter used for comparison is, EER that is computed as the point where FNMR (t) = FMR (t). The analysis of the proposed multimodal biometric systems and the existing approaches is performed on four databases DB1, DB2, DB3 and DB4 with the aid of the evaluation metrics like FMR, FNMR and EER values. The details of the works and the obtained graphs are given below.

Equal Error Rate analysis by MIPT approach

The performance analysis of the enhanced description of the first proposed secure cryptographic key generation from multimodal biometrics is given. It extracted the minutiae points and texture properties from the fingerprint and iris images respectively. The extraction process utilised the subsequent steps such as image preprocessing by histogram equalisation 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 utilising the following steps namely, segmentation, estimation of iris boundary and normalisation. 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 database are employed. Then, the matching process is carried out against the genuine fingerprint and iris with the impostor 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 Fig.4. The EER values obtained are given as, EER= 0.55 (DB1), EER= 0.53 (DB2), EER= 0.5 (DB3) and EER= 0.5 (DB4) and the EER values are tabulated in the Table 3.

Table 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

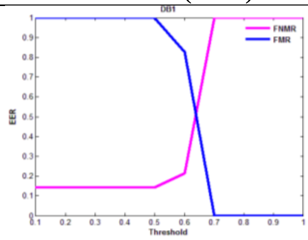
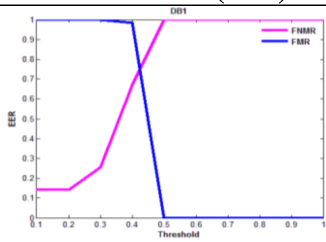
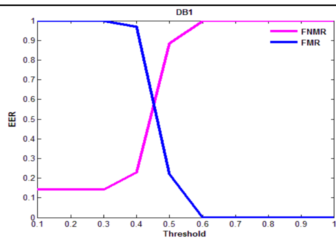
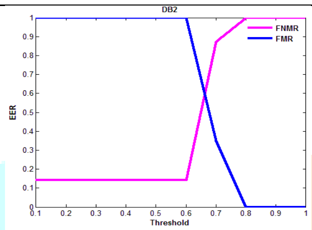
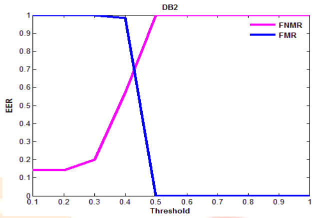
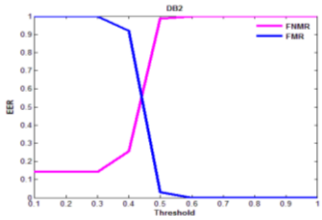
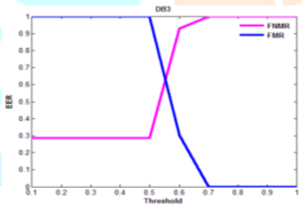
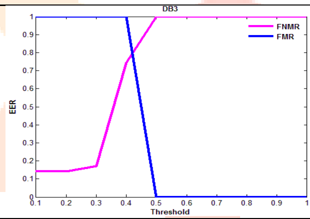
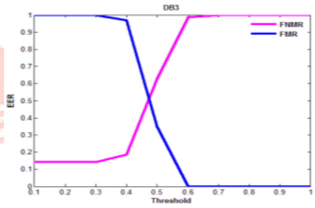
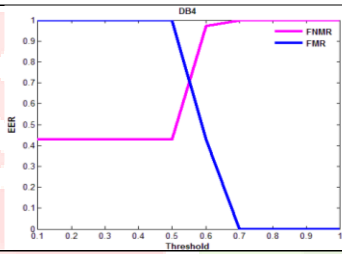
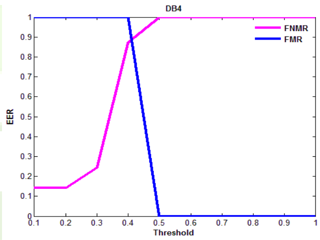
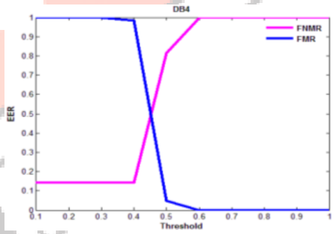
Database	**Existing Approaches**		**MIPT (Proposed method)**
	CSLF Asim et al. (2009)	FAFFI Vincenzo et al. (2010)	
DB1			
DB2			
DB3			
DB4			

Fig. 4 Performance analysis graph with FMR and FNMR values on four databases DB1, DB2, DB3 and DB4 for various approaches

Table 2 Compared EER values for the existing approaches and the first proposed approach

S.No	Input databases (fingerprint and iris Images)	EER values by		
		Existing approaches		First proposed approach
		CSLF Approach Asim et al. (2009)	FAFFI approach Vincenzo et al. (2010)	**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**

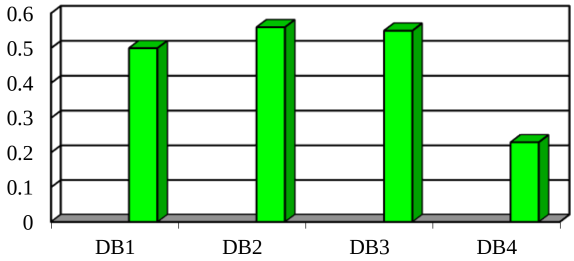


Fig. 5 Graphical analysis graph with FMR and FNMR values on four databases DB1, DB2, DB3 and DB4 for MIPT approach

Table 2 shows the comparative EER values of first proposed approach and the two existing methods. From this table, the first proposed approach has less EER value. The EER results ensure the accuracy of the first proposed approach, and the graphical representation also shows the same in Fig.5.

V. SUMMARY

In this paper, the first proposed approach of secured cryptographic key generation from multimodal biometrics has been discussed. It extracted the minutiae points and texture properties from the fingerprint and iris images respectively. The extraction process utilised the subsequent steps such as image preprocessing by histogram equalisation 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 utilising the steps namely, segmentation, estimation of iris boundary and normalisation. 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 a cryptographic key from multimodal biometrics for different databases for the first proposed system and the two existing approaches. From the performance analysis curves, the EER values are calculated for the proposed multimodal biometric system and the two existing approaches. The EER values in Table 2 clearly show that the proposed MIPT method is more effective than the existing methods CSLF and FAFFI.

REFERENCES

[1] Asim Baig, Ahmed Bouridane, Fatih Kurugollu & Gang Qu, 2009, 'Fingerprint – iris fusion based identification system using a single Hamming distance match', Symposium on Bio-inspired Learning and Intelligent Systems for Security, Edinburgh, Scotland, United Kingdom, pp. 9-12.

[2] Balakumar, P, VenkatesanR, 2012. "A Survey on Biometrics-based Cryptographic Key Generation Schemes", International Journal of Computer Science and Information Technology & Security, Vol. 2, No. 1, pp. 80-85.

[3] Choubisa, T, Sahoo SK & Mahadeva Prasanna, SR 2012, 'Multimodal biometric person authentication: a review', IETE tech rev, vol. 29, pp. 54-75.

[4] Donald, E, Maurer & John, P, Baker 2008, 'Fusing Multimodal biometrics with quality estimates via a bayesian belief network', in Pattern Recognition Elsevier Journal, vol. 41, no. 3, pp. 821-832.

[5] Jain, AK, Ross, A, 2008. "Introduction to Biometrics. In "Handbook of Biometrics", Springer.

[6] Jaya Lakshmi, A, Ramesh Babu, I, and Sai Kiran, P, 2012. Multimodal biometrics in identity Management, International Journal of Information Technology and Knowledge Management, Vol. 5, No. 1, pp. 111-115.

[7] Maltoni, D, Maio, D, Jain AK & Prabhakar, S 2003, Handbook of Fingerprint Recognition, Springer-verlag, New york, USA.

[8] Muhammad Khurram Khan & Jiashu Zhang 2008, 'Multimodal face and fingerprint biometrics authentication on space-limited tokens', NeuroComputing Elsevier Journal, vol. 71, no.13-15, pp. 3026-3031.

[9] Nageshkumar, M, Mahesh, PK & Shanmukha Swamy, MN 2009, 'An efficient, secure multimodal biometric fusion using palmprint and face image', International Journal of Computer Science, vol. 1, pp.49-53.

[10] Nemanja Macek, Borislav Dordevic, Jelena Gavrilovic, Komlen Lalovic, 2015. "An Approach to Robust Biometric Key Generation System Design, Acta Polytechnica Hungarica", Vol. 12, No. 8.

[11] Saad Abuguba, Milan M. Milosavljević and Nemanja Maček, 2015. "An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level", IJCSNS International Journal of Computer Science and Network Security, Vol.15, No.6.

[12] Subhas Barman; Debasis Samanta; Samiran Chattopadhyay, 2015. "Approach to cryptographic key generation from fingerprint biometrics", International Journal of Biometrics (IJBM), Vol. 7, No. 3.

[13] 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.

[14] Veeramachaneni, Kalyan; Osadciw, Lisa Ann; and Varshney, Pramod K., 2003. "Adaptive Multimodal Biometric Fusion Algorithm using Particle Swarm", Electrical Engineering and Computer Science.

[15] 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.

[16] Yan Yan & Yu-Jin Zhang 2008, 'Multimodal biometrics fusion using correlation filter bank', Proceedings of the nineteenth international conference on pattern recognition, Florida, United States, pp. 1-4.