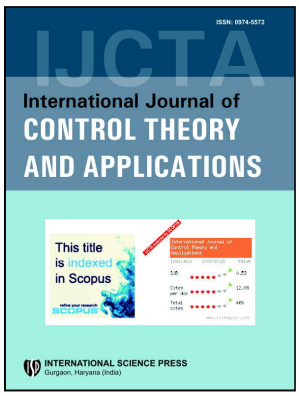

International Journal of Control Theory and Applications

ISSN : 0974-5572

Volume 10 • Number 15 • 2017

A Hybrid Template Security Scheme for Multimodal Biometric System based on Fingerprint and Hand Geometry

Arvind Selwal[1], Sunil Kumar Gupta[2] and Surender Jangra[3]

[1] Department of Computer Science & IT, Central University of Jammu, Jammu-181143 cum I.K. Gujral Punjab Technical University, Jalandhar, India, Email: arvind.cuj@gmail.com
[2] Department of Computer Science &Engineering BCET, (Autonomous institute of Punjab Govt. & IKGPTU), Gurdaspur, India, Email: skgbcetgps@gmail.com
[3] Department of Computer Applications Guru Tegh Bahadur College, Bhawanigarh (Sangrur) Punjab, India, Email: jangra.surender@gmail.com

Abstract: The emergence of biometric as a security method in various computing application has led to many fresh challenges. The security of feature templates extracted from various biometrical traits is one the key issues for the researcher community. A Multimodal biometric system (MBS) uses multiple biological traits captured from the human body for establishing the identity. The increase in the dimensionality of the traits not only improves overall accuracy and security of the MBS but poses challenges for feature template security before and after storage in the database. In this article, a novel template security technique is presented, which is based on applying the transformation on the real value feature vectors of the fingerprint and hand geometry modalities. The scheme use weighted match score level fusion with different weights, λ and (1-λ) respectively for fingerprint and hand geometry. The false acceptance rate (FAR) of the proposed scheme lies in the range of 5.06-12 %.Whereas, the false reject rate (FRR) in the range of 7.4-15.6%.The proposed template security scheme results in improvement of template security with low error rates of FAR and FRR. The security analysis of the proposed algorithm is performed, which revealed that the hybrid scheme meets the required characteristics of an ideal template security technique. The scheme is suitable for extending the scalability of thefingerprint system by using hand geometry biometric modality.

Keywords: Multi-modal biometric system, fingerprint, hand geometry, fusion, feature template security, region codes

1. INTRODUCTION

The widespread growth in the information based systems has led to the design of accurate and efficient means of authentication.One of the major information technology applications these days is to provide security using biometric based-systems. The traditional authentication tools have proved inferior as compared to modern biometric-based approach, mainly because of their exposure to a variety of failures. A biometrics-based recognition system may be defined as a pattern recognition activity where measurable biological or behavioral traits of human being are used for identification. The important and unique features are extracted from the

biological traits, which are captured througha sophisticated sensing device. The unique feature points are denoted as a feature vector (FV) and termed as feature template. A system database is used to stock upthe feature templates of all the enrolled users in the biometric based system[1]. The research studies show that, not all parts of human body may be used for biometrical recognition. Moreover, a trait of human body, chemical composition or behavioural patterns may be used for biometric purpose if and only if, it meets certain conditions, which are termed as biometric characteristics. The first condition is based on uniqueness, which means that the trait must be unique for every human being. The universality is also another property, which ensures that trait must be possessed by every prospective user. The trait which is used for biometric must be easy to capture, measure or record[2], [3]. For instance fingerprint is captured through ink impression, but in modern computing variety of sensors is available to capture high quality fingerprints. Similarly, high resolution camera may be used to capture facial biometric trait. Biometric traits also must be acceptable to large number prospective with intrinsic faith. Additionally, it must be difficult to spoof the given biometric modality and less vulnerable to security threats. Biometric trait of human must not change over time; therefore it needs to be permanent. It has been observed not all characteristics are satisfied by all the available biometrics. The fingerprint based biometric seems to be very stable and easy to use while face biometric is difficult to use due to large interclass and intra class variations. A Hand geometry based system is easy to use but interclass variation is less which makes it suitable only for small systems. Iris has very good interclass variation but difficult to capture the sample. It is interesting to know that these modalities are used in conjunction with each other, which led to emergence of multi modal biometric systems[4].A Biometric system may operate either in verification or identification mode. In case of identification mode the query template is compared with every template stored in the database in as one to one manner. It is used in cases, where identity of a person is to be searched in database, given that same user was already enrolled. On the other side, in verification mode the query template is compared only with template of same user.

The purpose of this mode is to verify the identity of a user during recognition. The performance of a biometrics-based system is measured through parameters like recognition accuracy, false match rate (FMR), false non-match rate (FNMR), equal error rate (EER), cost, template security, receiver operating curve (ROC)[2], [5].A biometric based system is susceptible to a variety of attacks or errors[6]. Ratha et. al. (2001), discovered that there may be eight susceptiblepoints in a biometric based system, where it may be attacked. The research studies show that a single BMS is not only sufficient but also vulnerable to a large numbers of security failures[7]. The increase in the tradition of biometric based system and population density has forced researchers to focus on modification and accuracy of these technologies. In order to mitigatethe problem of security threats and scalability,the unibiometric based systems are being replaced by multibiometric counterparts. A multimodal biometric system (MBS) works by using more than two modalities of an individual during the recognition process[8]. A variety of MBS have been developed with a range of grouping of biometric traits and resulted into improved performance. The backbone of any MBS is a fusion method,where information obtained from multiple modalities is consolidated. The fusion in a MBSmay be applied at various steps like feature level, match score level, rank level or decision level. A template data analysis of multimodal frameworks is presented in our earlier work, where fuzzy analytic hierarchy process (FAHP). However, template security is acentral issue, which needs greater importance in multi-modal systems[9][3]. The introduction of multimodal or multibiometric technologies has led to design and development of hybrid template security schemes.

The performance of a template security schemes depends upon the type and number of modalities as well as type of application. The fingerprint biometric is one of the most popular, accurate and widely deployed biometric system. The most of attacks has been attempted by the imposters on a fingerprint system. The attack on the templates may result in degradation of overall performance and security issues. In the worst case, if the feature template of a user in a fingerprint system is compromised, it may be used to reconstruct the fake biometric trait. In order to address these issues, the researchers have developed a variety of template security schemes for different BM systems.

In this paper, we propose a template security scheme for a fingerprint and hand geometry based multimodal biometric system. The rest of the paper is organized as follows. The section-IIgives an overview of feature extraction method of fingerprint and hand geometry biometric systems.The section-III highlightsbrief background of various template security schemes. In section-IV, the proposed system framework and the region coded hashing template security algorithm are presented. The section-V discusses the performance of the proposed scheme in terms of FAR/FRR and a security analysis is also presented. In the last, section-VI briefly highlights the key findings of this work followed by conclusion.

2. PRELIMNARIES

The increased use of biometric technology has made researchers to make these systems more accurate, secure and scalable. These issues may be overcome by using the concept of multibiometric systems. A variety of multimodal biometric systems has been designed and developed over the time during last decades. In this section, we discuss the process of template generation in a typical fingerprint and hand-geometry system.

2.1. Feature extraction in hand-geometry

The measurable structures related to human hand are relatively invariant and may be used for recognition. These measurements of human hand are finger lengths and widths at various points, presents the unique identity of an individual. As shown in the fig.1, there are sixteen features of the hand of an individual and constitute a feature vector (FV).

The hand geometry features are not very distinctive and systems are suitable in the applications where lies in the range of 100-200 number of users. The hand geometry based-biometric systems can be deployed in those applications which don't require extreme security but where robustness and low-cost are the primary issues.

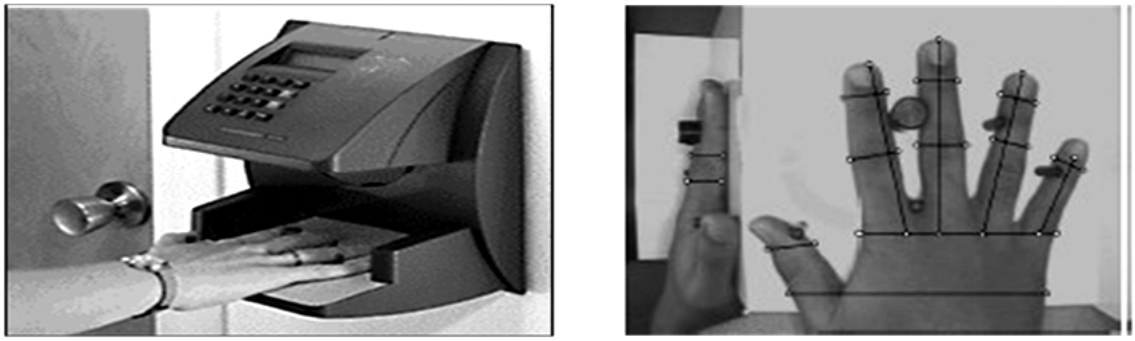

Figure1: A sensor and feature points in the hand geometry

a. Binarization: The captured image I(x,y) of the hand geometry is converted to black and white B(i, j) image by comparing the intensity value of each pixel with a predefined threshold. The transformation function for binarization is shown in the eq.1

$$B(i,j) = \begin{cases} 1, & if \quad I(i,j) > threshold \\ 0, & otherwise \end{cases} \tag{1}$$

b. Border tracing: In this phase the contour of the hand is obtained by applying a border tracing algorithm. The process begins by scanning the pixels of the binary image from the bottom-left to the right. As the firstblack

pixel is found the border tracing algorithm using eight neighborhood pixels is initiated to trace the borderof the hand in clockwise directions. In this step, all the coordinates of the border pixelsare recorded.

c. Feature point extraction: In this step, the tips and roots of all the fingers are detected and this is achieved by computing the first order differential of vertical coordinates of the image B(i,j). The point is marked as tip of finger if differential sign changes from -1 to +1 and finger tip if differential sign changes from +1 to-1.

d. Template generation: In this step, we generatea one dimensional feature vector FV_{HG}, including five lengths of fingers, ten widthsof fingers, and the width between v1 to v2.

2.2. Feature extraction process in fingerprint biometric system

In the modern day authentication the fingerprint based biometric has become vaery popular among all the biometrics. The fingerprint biometric has been in use since ancient times for identification of finger marks. A typical FP based system works by identifying the important feature points from the image of captured fingerprint. The typical feature points are minutia points and generally identifies as either ridge ending or a ridge bifurcation. The minutia points may be extracted from FP image using different methods. In the proposed security scheme, we have adopted the method as adopted by Jain et. al. proposed in their research work for fingerprint based identification system. The feature point extraction in this case, is a three step process. The complete procedure of feature extraction and template generation for fingerprint is shown in the Fig.2. Firstly, estimation of the orientation field, next step is extraction of the ridges and finally extraction of the minutia points.

i. Estimation of the orientation field: Suppose I(x,y) be the FP image captured through a sensor. The mage I is firstly divided into blocks of size P×P. Then, local orientation L_x and L_y are calculated at each pixel (a,b) of the image I(x,y), using eq 2-4.

$$L_x(a,b) = \sum_{k=1-\frac{p}{2}}^{m+\frac{P}{2}} \sum_{l=b-\frac{p}{2}}^{a+\frac{P}{2}} 2g_x(k,l)g_y(k,l) \tag{2}$$

$$L_y(a,b) = \sum_{k=a-\frac{p}{2}}^{m+\frac{P}{2}} \sum_{l=b-\frac{p}{2}}^{n+\frac{P}{2}} 2\left(g_x^2(k,l) - g_{xy^2}(k,l)\right) \tag{3}$$

$$\ominus(a.b) = \frac{1}{2}\tan^{-1}\left(\frac{L_x(a,b)}{L_y(a,b)}\right) \tag{4}$$

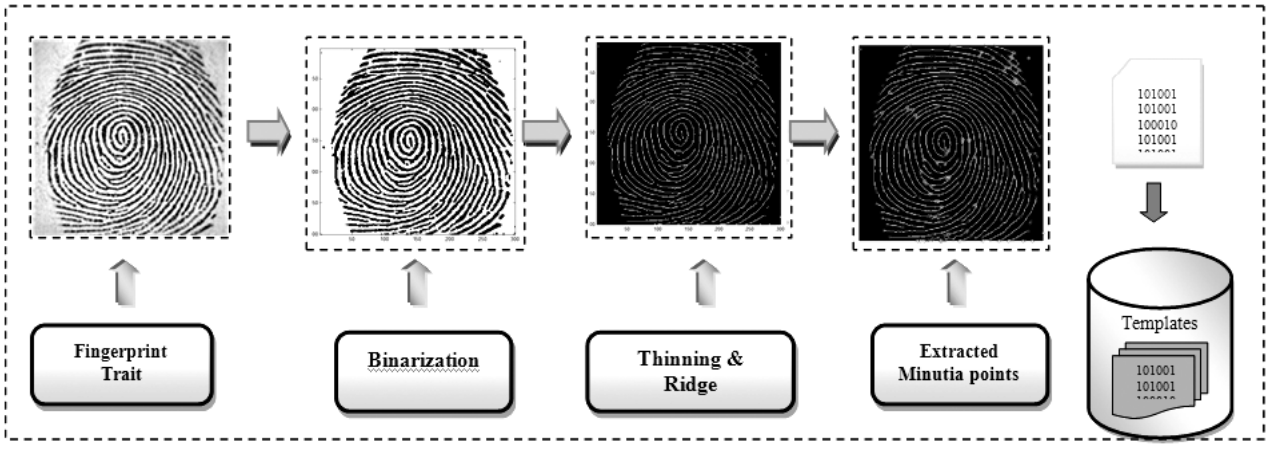

Figure 2: The fingerprint feature extraction and template generation process

In the next step, the consistency levels of the orientation field in local neighbourhood of a block (a, b), is computed using the eq. 5 and eq.6.

$$C(a,b)=\frac{1}{M}\sqrt{\Sigma_{(a',b')\in H}\left|(a'.b')-(a.b)\right|^2} \tag{5}$$

$$\left|\ominus-\ominus'\right|=\begin{cases} e & if\left(e=-'+360\right)\bmod 360)<180 \\ e-180 & otherwise \end{cases} \tag{6}$$

H is the local neighbourhood around the block (a, b) and M is the number of blocks in the H. (a′,b′) and (a, b) are the local ridge orientations are the respective blocks. A segmentation algorithm is applied on the image, in order to slash the area of interest, after the orientation fields is computed.

ii. Detection of ridges: The ridges are detected from the image obtained from the step-i, by using important characteristics that gray level value is maximum on a ridge along a direction which is normal to the local ridge orientation. The number of pixels on a ridge may be detected by using this property. The convolution is applied on the fingerprint image by using two masks. Then, the gray level value at a particular pixel in the convolved image is compared with a threshold. If the gray level value of a pixel found to be more than a threshold then it is declared as a ridge.

iii. Detection of minutia feature points: If a pixel is on a thinned ridge and eight connected, its value is 1 otherwise it is 0. Consider a pixel (m, n) lying on a ridge and suppose H_0 : H_7 be the eight neighbours of the pixel.

$$Classification\ of\ ridge\ type=\begin{cases} \left(\sum_{j=0}^{7}H_j\ \&\right)=1,(m,n)\ is\ ridge\ ending \\ \left(\sum_{j=0}^{7}H_j\ \&\right)>2,(m,n)\ is\ ridge\ bifurcation \end{cases} \tag{6}$$

In the last, the pixels position and angular dimension ofthe detected minutia points are measured. The feature is now denoted a collection of m feature points as a m×3 vector. The extracted feature vector is stored in the system database as template and represents the identity of the enrolled user. The template security is an important design issue and if compromised may result in serious failure of the overall system.

3. BACKGROUND OF BIOMTERIC TEMPLATE SECURITY

The template security schemes for biometric systems may be broadlycategorised as transformation based or cryptosystem based. The transformation based techniques are based on applying an invertible or non-invertible function to get the secured feature templates before actual storage on to the system database. On the other hand, the cryptosystem based techniques are based on encrypting the feature templates during enrolment phase and decrypting the templates during the testing in recognition phase. The encryption or decryption may be completed by deriving a key from biometric traits of human being or from any other information of the same user[10], [11]. The derived key may be combined with the original biometric template to create the key binding scheme or key may be generated from the templates resulting into key generation schemes.

Yi C. Feng et. al. [12]used a single secure sketch as a cryptosystem to secure multiple feature templates of a user extracted from fingerprint as a multi-instance biometric system. An efficient bit extraction algorithm is introduced for the transformation of biometric templates. The experimental results promise the improved

security and recognition performance as compared to uni-biometric systems. In order to secure the finger print templates a hybrid approach is proposed by Chouaib Moujahdi et. al. (2014)[13]. In this work, a crypto-system based fuzzy vault for fingerprint is designed for improving the both recognition and security of the system. A fuzzy commitment approach is proposed to build the vault and minutiae descriptors are added, which captures orientation of ridge and information of frequency in the neighbourhood of a minutia's. The experimental results looks good, that by usage of minutiae descriptors, the matching performance of the fingerprint system improved from an false acceptance rate(FAR) from 0.7% to 0.01% with a Genuine accept rate(GAR) of 95% which also improved security of system.V.S.Meenakshi et. al.[14]developed a method for providing template data security. The approach was implemented and tested on the fingerprint uni-biometric system. In this case, the authors developed an alignment free method for generating the concealable secured templates. The neighbouring relation around every reference minutiae were used to produce the secured feature templates.An important template protection technique is proposed by Peng et. al. [15], for multi-biometric system. This work attempts to protect multiple templates of a user as a single score at feature level fusion. The technique was implemented using crypto system-based method and exhibits trade-off between the two key parameters namely, security and recognition rate of the systems. The results indicate that proposed crypto-systems technique for multi-biometric has better security as compared to unibiometric system.

4. PROPOSED HYBRID TEMPLATE SECURITY SCHEME

The proposed hybrid scheme is used to secure the feature template of a multi-modal biometric system based on fingerprint and hand geometry. The framework of proposed scheme is shown in Fig.3. The method use a hybrid approach where the feature vectors are converted into secured template by using a non- invertible transformation. The fingerprint modality uses a hashing based transformation by using the region codes (RC) derived from the image of the trait. The transformation is used to convert the original value minutia points which are displaced in given plane. The hand geometry trait uses a transformation method where fingertips and finger roots are displaced and hence the actual 16 widths and length of the feature vector are transformed.The proposed hybrid scheme for template protection in a multi-modal biometric system is summarised in algorithm-1, where feature vectors corresponding to two modalities are denoted as F_1 and F_2. The fingerprint feature vector comprised of n features and each with positional and rotational characteristics. on the side, the hand geometry feature vector contains 16 different measurements of the human hand.

Algorithm1: Hybrid template security algorithm

1. Begin
2. Input : $FV_{FP=}|n\times3|$, $FV_{HG}=|1\times m|$
3. Output: Secured template T_1 and T_2
4. Start
5. $F_1 \leftarrow FV_{FP}$
6. $F_2 \leftarrow FV_{HG}$
7. $T_1 \leftarrow$RHC(FV_{FP}) // Apply region coded hashing on fingerprint feature vector
8. $T_2 \leftarrow$BioHashing(FV_{HG}) // Apply bio- hashing on hand geometry feature vector
9. Store T_1 and T_2 in the template database
10. Stop

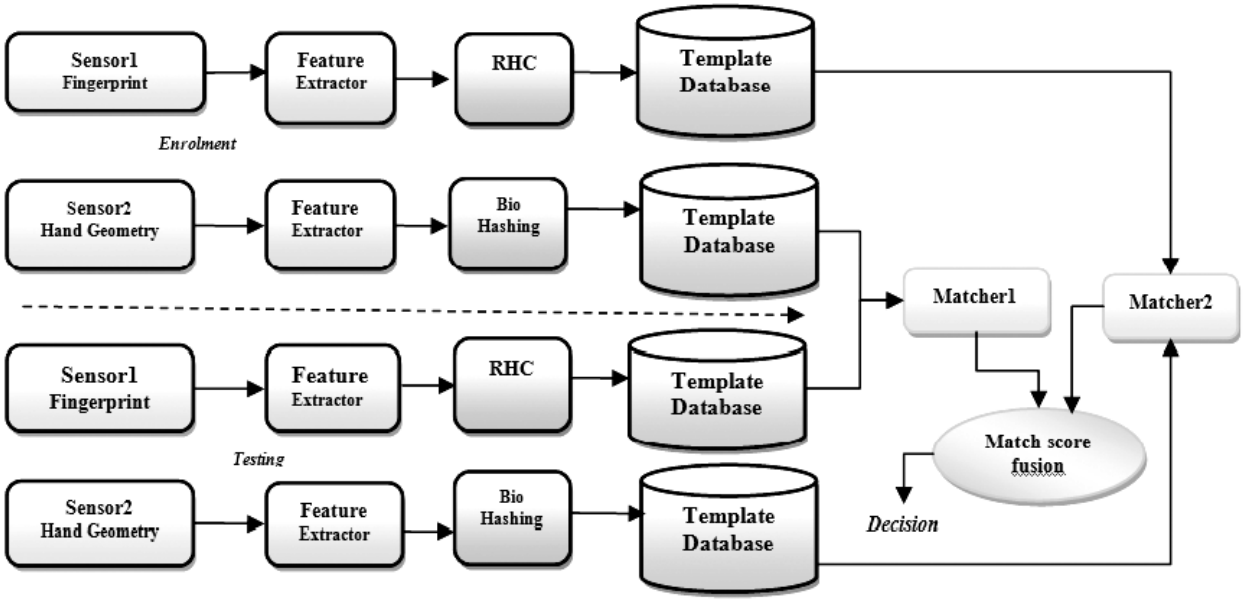

Figure3: The framework for proposed template security scheme

Algorithm2: Region coded hashing (RCH)

1. Begin
2. *Input*: FV_{FP} , Feature vector of Fingerprint biometric modality
3. *Output*: Secured template S_{FP}
4. Divide the region of interest of fingerprint image into 8 regions
5. Assign three bits binary codes to each region $R_i \leftarrow RC_i$ where i=1,2,3....8
6. for j=1 to p repeat step 6-9
7. pick a minutia point from FV_{FP} m_p $(x_p,y_p,Ø_p)$
8. if $Ø_p \in R_i$ // if minutia is located in ith region
9. compute new values of x_f, $y_f$using region codes of R_i
10. Add m_f $(x_f,y_f,Ø_f)$ to S_{FP}
11. End

Algorithm3: Biohashing to compute binary feature vector of hand geometry

1. Begin
2. *Input*: FV_{HG} , feature vector of hand geometry biometric modality with size of 16.
3. *Output*: Bio-coded hand geometry feature template.
4. For p=1to n create n random vectors of length n by using some random seeds. In this case n=16, as size of feature vector is 16 bits.
5. By using Gram-Schmidt algorithm on the n vectors convert these into orthogonal vectors $<OG_1,OG_2.....OG_n>$.
6. Compute the scalar products $S_k = <HG_k, OG_k>$ of hand geometric feature and orthogonal vectors.

7. Compute the n bit bio-code (b_1 , b_2,.....b_n) with the threshold ô.

8. $$b_k = \begin{cases} 0, & Sk < \tau \\ 1, & Sk \geq \tau \end{cases}$$

9. Store the secured template of the user as $S_{HG.}$

10. End

Algorithm 4: Matching algorithm

1. Begin
2. Input: FV_{FP}, FV_{HG}
3. Output: Accept or reject decision
4. Use algorithm-1 and compute feature templates of the proposed modalities of a user, say X_{FP} , $X_{HG.}$
5. Compute match scores using matcher1 and matcher-2
6. Suppose results of matcher are M_{FP} and M_{HG}.
7. FS= λ M_{FP} + (1-λ) M_{HG}. //Use match score fusion to find final score.
8. $$Decision_k = \begin{cases} Accept, & FS \geq \tau \\ Reject, & Sk < \tau \end{cases}$$
9. End

5. RESULTS DISSCUSSION

The experimental setup consists of standard sensors for collection of biometric traits from subjects with different age, profession and gender. The fingerprint images were captured through a sensor with a dpi of

Table 1
Security analysis of Hybrid Template Security Scheme

Sr. No.	*Characteristics*	*Comments*
1	Diversity	The hybrid scheme ensures that the feature template generated for a user is not for another user. It pertinent to learn that fingerprint is unique up to about 10000 of users and hand geometry is so for about 100-200 users. The combination of 10000 and 100 -200 different feature vectors (FVs) may result in generating 10^6 - 2× 10^6 diverse templates.
2	Revocability	It is an important characterises of any ideal template security scheme, which means that the templates may be revoked in the case of any attack and new template may be generated. The proposed scheme uses different transformation mapping functions to convert the fingerprint and hand geometry modalities. In the case of attack by an adversary on hand geometry a new bio-code may be generated by using random orthogonal vectors. Whereas, in other case the new template may be generated by using a new FP image of the user and distorting the minutia points by using the local region codes. As the templates of both the modalities are independent of each other, it is not necessary to revoke other modality in the case of attack on it.
3	Accuracy	The present scheme results in good performance with low error rates in terms of FAR/FRR, therefore it is accurate.
4	Security	The resultant hybrid template is secured and can't be reconstructed, in the case compromised by the adversary. The stored final template is difficult to understand by the imposter.

500×500. Whereas hand geometry traits were captured by using a HD digital camera installed on a stand with hand of subject rested on the base. In order to maintain the privacy of the subjects involved in the experimentation, the images of both the traits were captured in a confidential manner. The digital input images captured were converted to binary format. The proposed hybrid algorithm is implemented using MATLAB 7.6.0 (2008Ra) version. In order to evaluate the performance of proposed scheme three different errors level parameters are computed. The security analysis of the proposed scheme is carried out to evaluate for the characteristics of an ideal scheme. The Table 1 highlights various parameters and evaluation results of the proposed scheme.

The performance of the proposed template security scheme is summarised in theTable-2 and Table3.The results clearly reveals that the proposed algorithm performs well at λ=0.5, where both the modalities are assigned equal priority.

Table 2
FAR/FRR of Hybrid Template Security Scheme at different λ

Sr. No	*Weight λ*	*FAR(%)*	*FRR(%)*
1.	λ= **0.30**	12.1	15.6
2.	λ= **0.35**	10.0	14.2
3.	λ= **0.40**	10.1	13.1
4.	λ= **0.45**	10.0	13.0
5.	λ= **0.50**	6.9	8.6
6.	λ= **0.60**	5.06	8.4
7.	λ= **0.65**	5.06	7.4

Table 3
Performance comparison of Hybrid Template Security Scheme

Sr. No	*Scheme*	*FAR(%)*	*FRR(%)*
1.	Face, Palm print(N. Saini et.al), 2015	2.07-3.07	2.07-3.07
2.	Transformation & Quantization scheme Zhe Jin et.al.(2012)	15%	15%
3.	Proposed hybrid scheme(FP, HG)	~5.06-12.1	~7.4-15.6

6. CONCLUSION

A single template security scheme is not adequate for a BMS, especially in the cases which use multipletraits for human recognition. The hybrid template security scheme, presented in this paper mainly focused on addressing the issue of meeting all the characteristics of an ideal technique. The introduction of multibiometric systems have led to an vital issue of template security and hence a challenge for researchers. The proposed scheme is based on the use of two different template security algorithms for heterogeneous feature vectors of distinct sizes. The presented scheme perform well in the case of a bimodal system where equal weight is assigned to both the modalities with λ= 0.50. The hybrid scheme also uses the merits of our previous work based on region coded hashing (RCH, which was implemented on multi-instance fingerprint system. The scheme employs bio-hashing with random vectors which provides revocability, in the case of attack by an adversary. The performance (e.g. FAR=5.06-12.1% and FRR=7.4-15.6%) of the hybrid template scheme is comparatively better than other schemes and may be further enhanced to protect the template database of the system. Furthermore, the proposed scheme may be implemented in other multimodal biometric systems based on different traits.

ACKNOWLEDGEMENT

The authors extend their thank to the Department of Research, Innovation & Consultancy (RIC), I.K. Gujral Punjab Technical University, Jalandhar, for everlasting help, and encouragement for carrying out this research work.

REFERENCES

[1] K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, 2008.

[2] A. Adler, "Biometric System Security," in *Handbook of Biometrics*, 2008, pp. 381–402.

[3] A. Selwal and S. Kumar, "Fuzzy Analytic Hierarchy Process based Template Data Analysis of Multimodal Biometric Conceptual Designs," *Procedia - Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 899–905, 2016.

[4] K. Nandakumar and A. K. Jain, "Biometric Template Protection: Bridging the performance gap between theory and practice," *IEEE Signal Process. Mag.*, vol. 32, no. 5, pp. 88–100, 2015.

[5] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: security and privacy concerns," *IEEE Secur. Priv. Mag.*, vol. 1, no. 2, pp. 33–42, 2003.

[6] A. K. Jain and K. Nandakumar, "Biometric authentication: System security and user privacy," *Computer (Long. Beach. Calif).*, vol. 45, no. 11, pp. 87–92, 2012.

[7] Y. N. Singh and S. K. Singh, "A taxonomy of biometric system vulnerabilities and defences," *Int. J. Biom.*, vol. 5, no. 2, p. 137, 2013.

[8] A. Ross and A. A. K. Jain, "Multimodal Biometrics/ : an Overview," *Signal Processing*, no. September, pp. 1221–1224, 2004.

[9] Arvind Selwal and S. Kumar Gupta, Surender, "Template security analysis of multimodal biometric frameworks based on fingerprint and hand geometry "," *Perspect. Sci.*, vol. 8, pp. 705–708, 2016.

[10] T. Ramu and T. Arivoli, "Biometric Template Security: An Overview," vol. 65, 2012.

[11] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP J. Inf. Secur.*, vol. 2011, no. 1, p. 3, 2011.

[12] Y. C. Feng, P. C. Yuen, and A. K. Jain, "A hybrid approach for generating secure and discriminating face template," *IEEE Trans. Inf. Forensics Secur.*, vol. 5, no. 1, pp. 103–117, 2010.

[13] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell/ : Secure representation of fingerprint template q," *PATTERN Recognit. Lett.*, vol. 45, pp. 189–196, 2014.

[14] V. S. Meenakshi and G. Padmavathi, "Security analysis of password hardened multimodal biometric fuzzy vault with combined feature points extracted from fingerprint, iris and retina for high security applications," in*Procedia Computer Science*, 2010, vol. 2, pp. 195–206.

[15] P. Li, X. Yang, H. Qiao, K. Cao, E. Liu, and J. Tian, "An effective biometric cryptosystem combining fingerprints with error correction codes," *Expert Syst. Appl.*, vol. 39, no. 7, pp. 6562–6574, 2012.