Region Coded Hashing based Template Security Scheme for Multi-biometric System

Arvind Selwal [1, 2], Sunil Kumar Gupta [3] and Surender [4]

[1] Department of Computer Engineering, I.K .Gujral Punjab Technical University, Jalandhar, India
[2]Department of Computer Science & IT, Central University of Jammu, Jammu, India
[3] BCET, (Autonomous Institute of Punjab Govt. & IKGPTU), Gurdaspur, India
[4] Guru Teg Bahadur College, Bhawanigarh, Sangrur, Punjab, India

Abstract: *The biometric-based systems (BMS) have proved enormously superior and accurate authentication mechanism as compared to conventional methods. The accuracy of recognition systems is further enhanced by using multi-modal biometric systems (MBS) with additional cost overhead. The BS based human recognition works by extracting unique feature points from the raw biological trait of the user, captured through a sensor. The important feature points are stored in a system database and referred as feature template of the enrolled user. The template security, before its storage or after storage in database has become an important design issue and attracted attention of most of the researchers. In this paper, a novel region coded hashing (RCH) based template security scheme for a multi-instance biometric system is presented. The proposed scheme is based on two instances of biometric traits, i.e the left and right hand index fingerprints. In the enrolment phase biological information captured from sensing devices are used to extract important feature points using the feature extractors. The extracted real feature vector of the fingerprints BMS are passed through proposed RCH scheme to get transformed templates. The transformed vectors are fused together at the matching score level. The proposed template security results in good overall performance with false accept rate (FAR) of 0.2 % and 0.05% false reject rate (FRR).*

Keywords: *Multi-biometrics, fingerprint, fusion, template security, feature transformation, hashing, region codes.*

1. Introduction

The widespread expansion in the information based systems has led to the development of accurate and efficient means of authentication. The conventional authentication systems have proved inferior as compared to modern biometric-based approach, mainly because of their exposure to a variety of failures. The biometrics-based system may be formally defined as an automatic tool, which use measurable biological or behavioral traits of human being to distinguish their identity[1][2]. The key feature points are extracted from captured biological trait through a sensor. These unique feature points are represented as a feature vector and termed as feature template. A template database is used to store feature templates of all legitimate users in the biometric system[1]. The performance of a typical biometrics system is computed by using typical parameters like its recognition accuracy, false accept rate, false reject rate, equal error rate, cost, template security, receiver operating curve (ROC).The typical biometric system performance parameters are defined as follows:

Definition-I*: The threshold depending fraction of the falsely accepted samples divided by the number of all impostor samples is called false acceptance rate (FAR shown in eq1.)*

$$FAR = \frac{Number\ \ of\ Accepted\ \ Imposters}{Total\ \ Imposters\ \ trials} \times 100 \qquad (1)$$

Definition II*: In some case, a genuine user is falsely rejected by the system and the fraction of the number of rejected enrolled user patterns divided by the total number of user patterns is defined as false reject rate (FRR is shown in eq.2).*

$$FRR = \frac{Frequency\ \ of\ Genuine\ \ users\ rejected}{Total\ \ numbe\ r\ of\ Genuine\ \ trials} \times 100 (2)$$

Definition III: *The score distribution of false accepts and false reject rates overlaps at a particular point which is termed as Equal Error Rate (ERR is shown in eq.3).*

$$EER = FAR, Such\ that\ FAR=FRR \qquad (3)$$

Definition IV: *The performance of a verification system is computed by a parameter called as Recognition Accuracy (RA is shown in eq.4).*

$$RA = \left(100 - \frac{FAR+FRR}{2}\right)\% \quad (4)$$

Definition V: *The fraction of genuine users accepted by the biometric system is defined as genuine accept fraction (GAF is shown in eq.5).*

$$GAF = (100\text{-}FRR)\% \quad (5)$$

Definition VI*: The measure which is used to compare GAF with FAR is termed as Receiver operating curve (ROC). This measure is generally used to discriminate a genuine user with an imposter user.*

The biometric systems are susceptible to a variety of security threats and failures[1][2]. Ratha et. al. (2001), found that there may be eight vulnerable attack points in a BM based system. The research studies have revealed that a single BMS is not only inadequate but also vulnerable to large numbers of security attacks. Invariant increase in biometric usage and population density has forced researchers to think about modification in biometric technologies. In order to address the problem of security threats, unibiometric systems are being replaced by multibiometric counterparts. A multimodal biometric system works on the principle of using more than two modalities of the user's for recognition. A large number of multimodal systems have been developed with a range of grouping of biometric traits and resulted into improved performance. The backbone of multimodal system is a fusion step whereby information obtained from multiple modalities is consolidated into one. The fusion in a MB based systems may be applied at various stages like feature level, match score level, rank level or decision level. However, template security is still an issue, which needs greater emphasis in multimodal systems. The introduction of multimodal or multibiometric technologies 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 number 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 based multimodal biometric system. The rest of the paper is organized as follows. The section-2 provides an overview of feature extraction process of fingerprint biometric system and a brief summary of various template security schemes. In section-3, the proposed system framework and the region coded hashing template security algorithm are presented. The section-4 discusses the performance of the proposed scheme in terms of FAR/FRR. In the last, section-5 briefly highlights the key findings of this work followed by conclusion.

2. Related Works

The fingerprint based biometric has become most popular among all the biometrics and has almost one third of the total share in the world market. The fingerprint biometric has been in use since ancient times. 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 process of feature extraction is depicted in Fig.1 (a-d). Firstly, estimation of the orientation field, next step is extraction of the ridges and finally extraction of the minutia points.

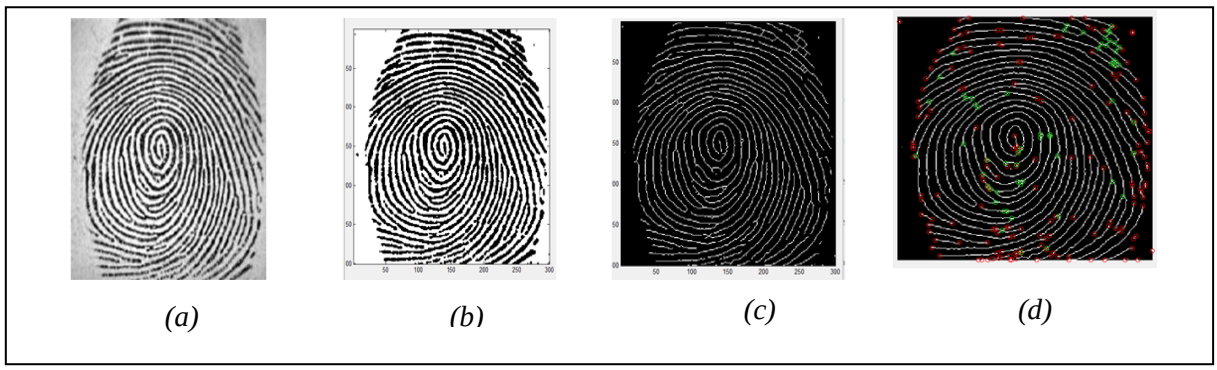

Fig1. (a) Original Fingerprint (b) Binarization (c) Thinning & orientation (d) Extracted minutia feature points

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 following equations.

$$L_x(a,b) = \sum_{k=a-\frac{p}{2}}^{m+\frac{P}{2}} \cdot \sum_{l=b-\frac{p}{2}}^{a+\frac{P}{2}} 2\, g_x(k,l)\, g_y(k,l) \quad (6)$$

$$L_y(a,b) = \sum_{k=a-\frac{p}{2}}^{m+\frac{P}{2}} \cdot \sum_{l=b-\frac{p}{2}}^{n+\frac{P}{2}} 2(g_x{}^2(k,l) - g_{xy}{}^2(k,l)) \quad (7)$$

$$\Theta(a.b) = \frac{1}{2}\, tan^{-1}\left(\frac{L_x(a,b)}{L_y(a,b)}\right) \quad (8)$$

In the next step, the consistency levels of the orientation field in local neighbourhood of a block (a, b) , is computed using the eq. 9 and eq.10.

$$C(a,b) = \frac{1}{M} \sqrt{\sum_{(a',b')\in H} |\Theta(a'.b') - \Theta(a.b)|^2} \quad (9)$$

$$|\Theta - \Theta'| = \begin{cases} e & if\ (e = \Theta - \Theta' + 360) \bmod 360) < 180 \\ e - 180 & otherwise \end{cases} \quad (10)$$

H is the local neighbourhood around the block (a, b) and M is the number of blocks in the H. $\Theta(a'.b')$ and Θ(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.

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

The identified minutia pixels positional and angular dimension, at this time is measured and recorded. 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. The template security schemes for unibiometric systems may be typically classified as transformation based or cryptosystem based[3][4]. Transformation based techniques are based on applying an invertible or non invertible function to secure the templates before actual storage into

database. Cryptosystem based techniques are based on encrypting the templates during enrolment and decrypting the templates during template matching.

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. 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[5]. A variety of template security schemes has been developed during the last decade and a summary is given in Table.1. U. Uludag et. al.(2003) describes in details about how biometric cryptosystem works and highlights various issues and limitations [6]. A comprehensive study of various template security techniques along with requirements of template protection techniques is presented [7]. A brief background is presented in table-2 about the development of template security schemes by various authors during last decade. Significant work is presented on how biometric data may be hidden using watermarking. Two applications of an amplitude modulation based watermarking method, in which a user's biometric data is hidden in a range of images. This method is applied on face and fingerprint images and leads to low visibility of the embedded pointer [8]. Y. C. Feng et. al.[9], highlights comprehensive details of binarization process and gives an analysis of various techniques based on security, accuracy and performance. In [10], authors focus is on biometric systems that combine cues obtained from multiple biometric sources and these systems are commonly referred to as multibiometric systems. Method uses fuzzy vault to improve the security of feature template. The modalities are the fingerprint and palm print inputs which are firstly processed in order to enhance the quality of the image and build it well for extraction of features. The system gives good performance with FRR of 88% and FAR of 12%. It acts well even after adding salt and pepper noise to result in a FRR of 72.2% and FAR of 27.8%. Authors in their work [11] propose a method to bind the biometric template in a cryptographic key which does not reveal any information about the original biometric trait when it is compromised by the attacker. Another advantage of the proposed method is in terms of security as well as improvement on recognition accuracy. Y.J. Chin et.al.(2014) developed a technique to secure templates during feature fusion in a multimodal biometric system based on fingerprint and palm print. In this work, authors used a transformation method called a Random tiling and equal probable discretization technique [12]. An approach to improve the security of templates in fingerprint has been developed by authors [13]. The main goal of the system is to build a non-invertible transformation of fingerprint template which meets the requirements of revocability, diversity, security and performance. Here, a key is generated from the minutiae extracted from the image, in the form of a special spiral curve. Multi-modal biometric systems as employs multiple biometric traits of human, therefore combination of template security schemes are used to design hybrid techniques.

Table-1: Summary of biometric template security schemes

Technique	Biometric Trait	False Match Rate/ False Non Match Rate	Authors
Password Hardening	Voice	>2 /2	Manrose et.al(2001)
Quantization	Online Signature	1.2/28.0	Feng Wah (2002)
Quantization	Online Signature	0.0/7.05	Vielhauer (2002)
Fuzzy Vault	Fingerprint	0.0/20-30	Clancy et al.(2003)
Bio Hashing	Face	0.0/0.0	Teoh et al. (2004)
Fuzzy Commitment	Iris	0.0/0.42	Hao et al. (2006)
Bio Hashing	Face	0.0002	Goh et al. (2006)

		(Equal Error Rate)	
Fuzzy Commitment	Iris	0.0/5.62	Bringer et al. (2007)
Block Permutation, Surface folding	Fingerprints	0.0004/15-35	Ratha et al. (2007)
[19] Bio-Convolving	Signature/Iris	10.81 EER	Maiorana et al. (2010)
Transformation & Quantization	Fingerprint	15% EER	Zhe Jin et.al.(2012)
Cryptosystem of Fuzzy vault	Fingerprint	0.7-0.01%	C. Moujahdi,(2014)
Hash Functions	Fingerprint	0.01/0.02	Y. Yang et al.(2015)

3. Proposed template security scheme

The framework of the proposed system is shown in fig.2, in which fingerprints of the left and right hands of a user are captured through a sensor during the enrolment phase. The feature extraction process as discussed in section II, is applied on the FP images and the feature vectors are extracted. Let us assume that the feature vectors of i^{th} user be denoted as X_1^i and X_2^i Then, the proposed region coded hashing technique (RCH) is applied on these vectors and transformed vectors are obtained as X^1_{RHC} and X^2_{RHC}. The matching score level fusion is applied to merge both the feature vectors during the verification or testing phase. The proposed RCH scheme works by segmenting area of interest of the captured biometric image into eight regions by allocating 45^o to each segment as shown in the Fig.3.Then, each region is given a binary code of three bits based upon its geometrical structure. The binary code is assigned to a region is based upon three position criterion as shown in table2. Suppose that, the segment binary code be *'$b_2b_1b_0$'*, where bit b_0 denotes right or left portion of the total area with respect to y-axis. Therefore, bit b_0 indicates location of a minutia point on either positive x or negative x side. The bit b_1 tells about, where a particular segment is lying in a particular quadrant. It is assumed that segment may be lying on upper side or on lower side in a quadrant. If segment is lying on upper side then binary value of b_1 is 1 otherwise it is 0. Bit b_2 indicates whether segment on positive y-axis or negative y-axis. If segment is on + y-axis side then b_2 is 1 otherwise it is 0. The table-3 gives a list of regions together with their locations and binary codes. The algorithm1 explains how the region coded hashing technique is applied to a feature vector to convert it to a secured vector and method is based on evaluating the thresholdΦ.

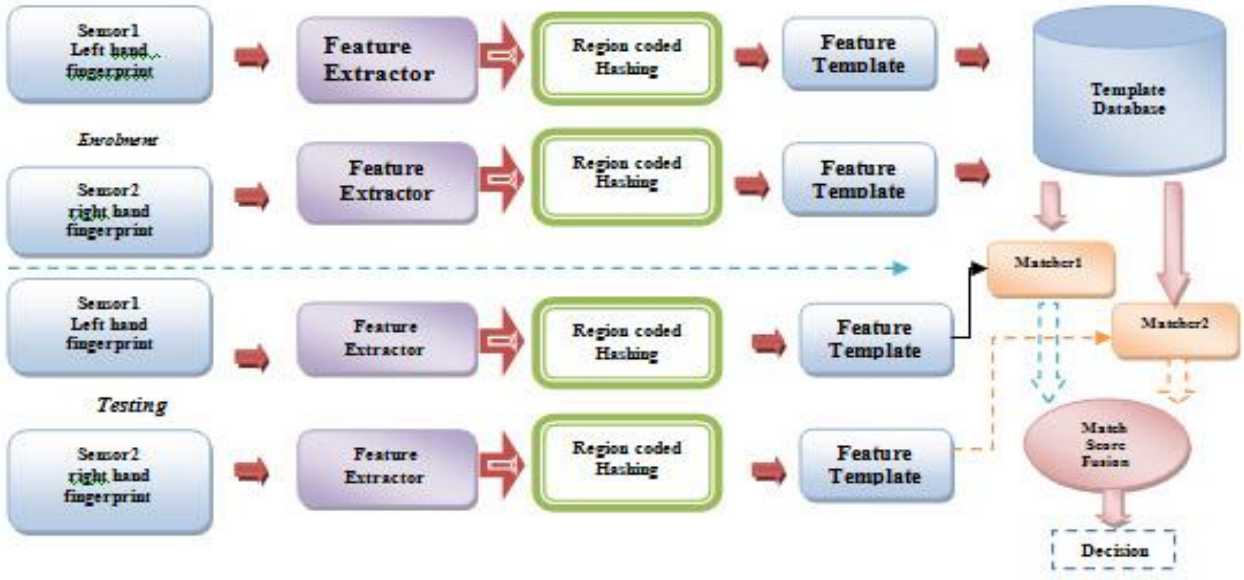

Figure2: The proposed MBS template security framework

Table 2: Regions and their positions

Region No.	Region position/location	Binary encoding of respective location
1	Top, Top ,Right	Top: 1 Low: 0 Left: 0 Right: 1
2.	Top, Low, Right	
3.	Low, Top, Right	
4.	Low, Low, Right	
5.	Low, Low, Left	
6.	Low, Top, Left	
7.	Top, Low, Left	
8.	Top, Top, left	

Table 3: Regions and their binary codes

Region No.	Region position/location	Region Code
1	TTR	111
2.	TLR	101
3.	LTR	011
4.	LLR	001
5.	LLL	000
6.	LTL	010
7.	TLL	100
8.	TTL	110

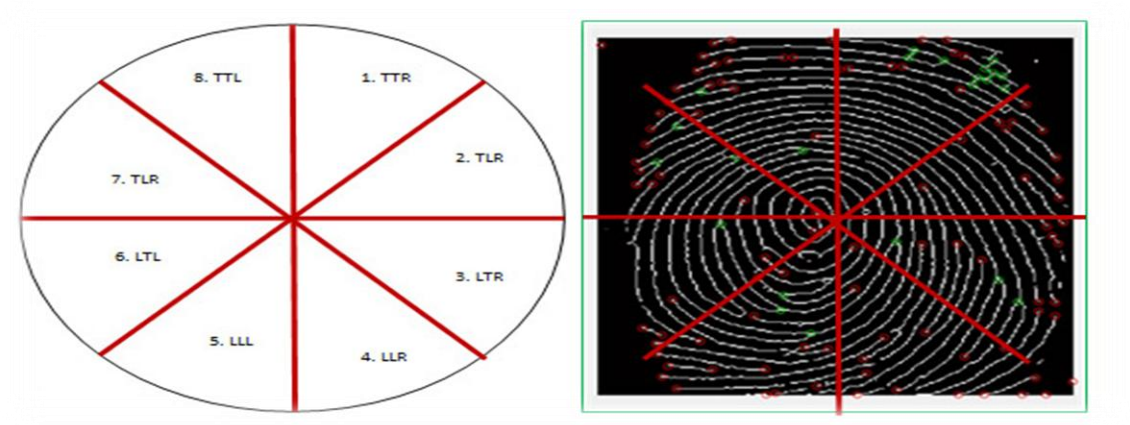

Figure.3. The proposed region segments and region codes (RC)

Algorithm1: Proposed region coded hashing (RCH)

Algorithm1: Proposed region coded hashing (RCH)

Input: Tow feature vectors X_1^i and X_2^i extracted from feature extractor for user-i, X_t^i, **Output:** Encoded template of user-i , X_{RHC}

1. Let n=| X_t^i|, be the total number of minutia points in a feature vector.
2. For j=1 to n, perform step 2 to 5
3. Read jth minutia point from template say $F_i(x,y,\Phi)$, check Φ, perform step 3.
4. Compute encoded feature $F_i'(x', y',\Phi')$, with case
5. **Case1: $0<\Phi\leq 45$**
6. x'= h(x, TLR)= x+1, x-1, x +1
7. y'= h(y, TLR)= y+1, y-1, y+1
8. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
9. **Case2: $46<\Phi\leq 90$**
10. x'= h(x, TTR)= x+1, x+1, x+1
11. y'= h(y, TTR)= y+1, y+1, y+1
12. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
13. **Case3: $91<\Phi\leq 135$**
14. x'= h(x, TTL)= x+1, x+1, x-1
15. y'= h(y, TTL)= y+1, y-+1, y-1
16. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
17. **Case4: $136<\Phi\leq 180$**
18. x'= h(x, TLL)= x+1, x-1, x-1
19. y'= h(y, TLL)= y+1, y-1, y-1
20. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
21. **Case5: $181<\Phi\leq 225$**
22. x'= h(x, LTL)= x-1, x+1, x-1
23. y'= h(y, LTL)= y-1, y+1, y-1
24. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
25. **Case6: $226<\Phi\leq 270$**
26. x'= h(x, LLL)= x-1, x-1, x-1
27. y'= h(y, LLL)= y-1, y-1, y-1
28. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
29. **Case7: $271<\Phi\leq 315$**
30. x'= h(x, LLR)= x-1, x-1, x+1
31. y'= h(y, LLR)= y-1, y-1, y+1
32. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
33. **Case8: $316<\Phi\leq 360$**
34. x'= h(x, LTR)= x+1, x-1, x+1
35. y'= h(y, LTR)= y-1, y+1, y+1
36. $\Phi'= \tan^{-1}(\frac{x}{y}) - \tan^{-1}(\frac{x'}{y'})$
37. Store the transformed minutia $F_j'(x', y',\Phi')$ in X_{RHC}

The matching algorithm for the proposed system is shown as algorithm2. In the testing phase, two extracted feature RCH feature templates are compared with corresponding stores feature vectors in the database. The similarity scores of the both instances of the fingerprint are computed as D_1 and D_2. Then weighted sum rule base scheme is used to assign the priority to both the biometric instances of the fingerprint. In this case, we assign equal weight to both the modalities and weight λ=0.5 is fixed. In order to take a decision, consolidated match score, D, is computed and compared with a predefined threshold, e.g. Φ.

Algorithm2: Matching algorithm

Input : Two RCH coded feature vectors Y^1_{RHC} and Y^2_{RHC}
Output: Match score level fusion and decision

1. Start
2. Let us assume that, X^1_{RHC} and X^2_{RHC} be the two stored template vectors of the user to verified in the database.
3. Compute the similarity score between the respective

vectors X^1_{RHC} , X^2_{RHC} and Y^1_{RHC} and Y^2_{RHC}
4. Let as assume the match score is denoted by D_1 and D_2.
5. Compute the weighted sum rule based matching score
6. $D= \lambda D_1+(1-\lambda) D_2$, where λ is the weight assigned to each biometric modality.
7. Assume $\lambda=0.5$
8. Compare D with predefined threshold Φ to arrive at a decision of accept or reject the user.
9. Stop

4. Result analysis

The proposed algorithm is implemented in MATLAB 7.6.0 and the source code is openly available for feature extraction process in fingerprint system. The experiments were performed on a fresh multi-instance dataset of 300 samples collected from 100 different subjects. The left and right hand fingerprint biometric traits were collected from heterogeneous population covering subjects from different backgrounds, gender and age. The impressions of fingerprint were obtained from each subject at three different times on a day. The fingerprint images were captured with a high quality sensor at 300×300 and 500dpi. The performance of the proposed system is shown in table-4. The False accept rate (FAR) and false reject rates (FRR) of the proposed scheme are computed and compared with previously developed techniques by various authors. The proposed scheme shows comparatively fair performance with respect to other schemes. The proposed scheme is evaluated for various security parameters as described in ISO/IEC24745 standard. The proposed RCH template security scheme provides security at multiple levels, from template generation to, the time before storage on to the device. An adversary may triy to attack the secured template by tempering the system database. In this case the stored secured template may be revoked and another secured template may be generated. One of the limitations of the proposed technique is that, it uses an invertible transform.

Table 4: Performance comparison of proposed system

Sr. No	Template security scheme	FAR(%)	FRR(%)
1.	Fingerprint Cryptosystem of Fuzzy vault C. Moujahdi,(2014)[15]	0.7%	0.01%
2.	Transformation & Quantization scheme Zhe Jin et.al.(2012)	15%	15%
3.	Face, Palm print(N. Saini et.al), 2015	2.07-3.07.6% (EER)	2.07-3.07.6% (EER)
4.	Proposed RCH template security scheme	~0.2	~0.05

5. Conclusion

In this paper, a template security scheme for multiple -instance biometrics system is developed, where templates are secured using a novel region coded hashing technique. The proposed scheme achieves a recognition rate of 99.1% with false accept rate (FAR) of 0.2 % and false reject rate (FRR) of 0.05%,which is fairly better than other previous schemes. Further studies may be carried out to evaluate the proposed system using standard biometric available datasets of fingerprint biometrics. The template security is transformation based and revocable in the case when it is compromised by an adversary. The computational efficiency of the proposed algorithm may be improved in future by using a suitable optimization technique. The proposed template may be extended and implemented in other multi-modal biometric systems. Furthermore, the limitation of the proposed template security scheme may be overcome by making the scheme as a non-invertible. The proposed scheme will be tested on the standard fingerprint databases like FVC2002. A thorough security analysis of the proposed scheme may be carried out in the future.

Acknowledgement

Authors express their deep sense of gratitude to the Department of Research Innovation and Consultancy (RIC), I.K. Gujral Punjab Technical University (Jalandhar), for providing the essential support to carry out this research work.

References

[1]. 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.

[2]. C. Roberts, "Biometric attack vectors and defences," *Comput. Secur.*, vol. 26, no. 1, pp. 14–25, 2007.

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

[4]. A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric Template Transformation: A Security Analysis," *Proc. SPIE - Int. Soc. Opt. Eng.*, vol. 7541, p. 75410O–75410O–15, 2010.

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

[6]. U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," in *Proceedings of the IEEE*, 2004, vol. 92, no. 6, pp. 948–959.

[7]. 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.

[8]. A. K. Jain and U. Uludag, "Hiding biometric data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 25, no. 11, pp. 1494–1498, 2003.

[9]. Y. C. Feng, M. H. Lim, and P. C. Yuen, "Masquerade attack on transform-based binary-template protection based on perceptron learning," *Pattern Recognit.*, vol. 47, no. 9, pp. 3019–3033, 2014.

[10]. V.E. Brindha, "Biometric template security using fuzzy vault," in *Proceedings of the International Symposium on Consumer Electronics, ISCE*, 2011, pp. 384–387.

[11]. S. Argyropoulos, D. Tzovaras, D. Ioannidis, Y. Damousis, M. G. Strintzis, M. Braun, and S. Boverie, "Biometric template protection in multimodal authentication systems based on error correcting codes," *J. Comput. Secur.*, vol. 18, no. 1, pp. 161–185, 2010.

[12]. Y. J. Chin, T. S. Ong, A. B. J. Teoh, and K. O. M. Goh, "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion," *Inf. Fusion*, vol. 18, no. 1, pp. 161–174, 2014.

[13]. M. V. N. K. Prasad and C. Santhosh Kumar, "Fingerprint template protection using multiline neighboring relation," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6114–6122, 2014.

[14]. Li Lu and Jialiang Peng,"Finger Multi-biomettic Cryptosystem using Feature level fusion, Intenational Journal of Signal Processing amd Pattern Recognition, vol7 No.3(2014) pp223-236.

[15]. 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.

[16]. N. Saini and A. Sinha, "Face and palmprint multimodal biometric systems using Gabor – Wigner transform as feature extraction," *Pattern Anal. Appl.*, vol. 18, no. 4, pp. 921–932, 2015.

Arvind Selwal completed his B.Tech and M. Tech. degrees from Kurukshetra University, Haryana, India in the years 2002 and 2008 respectively. He is currently working as Assistant Professor in the department of Computer Science & IT, at Central University of Jammu and continuing his Ph.D. degree in Computer Science & Engineering from I.K. Gujral Punjab Technical University, Punjab, India. His research interests include Biometric Security, Image Processing and Advanced Database Systems. He has contributed more than 15 research articles in reputed International/National Journals. He is also active member of Computer Society of India (CSI).

Dr. Sunil Kumar Gupta did B.E. in Computer Science from Gorakhpur University, Gorakhpur, UP, India in 1988, M.S. in 1991 and completed Ph.D. in Computer Science from Kurukshetra University, Kurukshetra, India. He possesses 28 years of teaching experience. He has worked as teaching faculty in many reputed institutions in India including N.I.T., Hamirpur (HP). Presently, he is working as Associate

professor in the department of Computer Science & Engg. at Beant College of Engineering and Technology, Gurdaspur (India).He has more than 40 research publications. His work is published and cited in highly reputed journals of Elsevier, Springer, Taylor and Francis and IEEE. His areas of interest include Database management systems, Distributed systems, Cloud computing, Mobile computing and Biometric security.

Dr. Surender completed his M.Tech degree in Computer Science and Engineering from Ch. Devi Lal University Sirsa (Haryana in 2006, Ph.D in Computer Science from Kurukshetra University, Kurukshetra in the year 2011. He has also qualified UGC-NET exam in Computer Science and Applications in Oct. 2013. He has more than 11 years of teaching experience and recently working as Assistant Professor in the Department of Computer Science at Guru Teg Bahadur College, Bhawanigarh, Punjab, India. His research interests include Fault Tolerance in Mobile Distributed Systems, Ad-HOC Network, Data Mining, Cloud Computing, Biometric System Security and Cryptography. He has more than 30 publications in various International Journals and Conferences of repute.