JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol-6, Special Issue-3, Apr 2018 E-ISSN: 2347-2693

On Biometrics Feature Extraction and Template Security Schemes

Mahapara Khurshid[1*], Arvind Selwal[2]

[1*] Department of Computer Science and IT, Central University of Jammu, Jammu, India
[2] Department of Computer Science and IT, Central University of Jammu, Jammu, India

[*] *Corresponding Author: mahaparakhurshid@gmail.com, Tel.: +91-94197-38616*

Available online at: www.ijcseonline.org

Abstract—Effective response to identification and authentication of individuals in complex environment demands replacement of traditional authentication techniques. It should occur concurrently with the increased pace of the digital world and increasing population. Many unimodal template security systems have been published, but in one or the other way, they are associated with some technical flaws, which prevents them from claiming to be reliable models. After doing the critical review of many published articles and case studies, many design characteristics of template security systems like security level, reliability, privacy level, acceptability, performance, uniqueness and cost, were taken into consideration for analyzing the various available models. However, no model was found to be associated with all the design parameters, which could claim to be a highly secure and reliable model. On review basis, it was found that many design characteristics were underestimated, if taken into consideration for development and implementation, could revolutionize biometric based template security systems.

***Keywords*—**Biometrics, Feature Extraction, Unimodal systems, Multimodal systems, Template Security Scheme

I. Introduction

In last two or three decades, there were many traditional methods to identify and authenticate an individual like passwords, signatures, pictures, PINs etc. In recent past, all works from personal level to organizational level were almost in offline mode and chances of fraud were less. In present era, almost everything is real time and in an online fashion. The traditional human recognition systems are not much reliable as the attributes can be stolen, shared or misplaced [1]. This led to the development of biometric systems based on the persons' physical, chemical or its behavioral attributes [2].

The Figure 1 shows the typical modules of a biometric system. A biometric based system consists of four modules, [3] namely;(a) sensor module which is used to sense the trait & get raw information (b) pre-processing or feature extraction module which is used to enhance the quality of image(if required) and extract the unique features (c) matcher module which is to compare the presented feature with the stored ones (d) decision module which is used to make a final decision about the validity of the user. These systems prove to be very handy for authentication as these are based on something you are and that too unique for every individual. The unimodal biometric systems (UBS) has been designed by researchers who prove to be successful to some extent. But, UBS has shortcomings which includes the lack of universality, susceptible to circumvention, insider attacks etc, which makes them less reliable. In order to overcome these shortcomings, the researchers started showing interest in designing the multimodal systems comprising of more than one trait. These systems not only prove to overcome the limitations but also prove efficient in terms of accuracy & reliability.

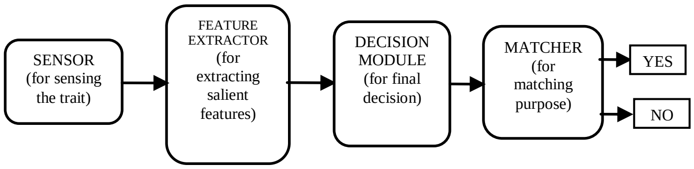
SENSOR (for sensing the trait)
FEATURE EXTRACTOR (for extracting salient features)
DECISION MODULE (for final decision)
MATCHER (for matching purpose)
YES
NO

Figure 1: A biometric System

The Figure 2 shows the taxonomy of multi-biometric authentication systems [4];

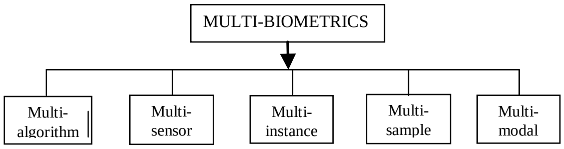

Figure 2.Multi-biometric Systems

(i) Multi-algorithm systems – different algorithms are applied on same biometric data of an individual (ii) Multi-sensor systems – more than one sensor is employed to capture single biometric trait (iii) Multi-instance systems – different instances of the same biometric trait are captured

(iv) Multi-sample systems – multiple samples are capture by a single sensor (v) Multi-modal systems – more than one biometric trait is acquired from user.
The biological traits can be merged together by employing any of the fusion techniques [5], namely; sensor level, feature level, match score level, rank level or decision level. The resulting template is stored in the database for matching purpose. In the authentication phase, the stored template is matched against the query template in order to arrive at a final decision for the individual.

The section I present an overview of the biometric based systems. The section II explains the feature extraction process of fingerprint and hand geometry. Different vulnerabilities and various template security techniques present in the biometric systems are discussed in section III. The section IV and V is dedicated for the different template security schemes (TSS) designed by various researchers for unimodal and multimodal biometric systems. Comparative analysis of the various TSS based on different performance metrics is given in section VI. Finally, the section VII provides conclusion and future scope of this research.

II. FEATURE EXTRACTION PROCESS IN FINGERPRINT AND HAND GEOMETRY

A. *Feature Extraction in Fingerprint*

The Fingerprint is the most widely used biometric trait in case of biometric based systems and accounts for about one-third of total share in biometric world. The characteristic points in case of the fingerprint are the minutia points which may be ridge ending or ridge bifurcation. The feature extraction in the fingerprint is a three step process [6], namely estimation of orientation field, ridge extraction, minutia point extraction.

Let the fingerprint image sensed be F(y,z). The captured image is first divided into blocks having size N*N. Then at each pixel (c,d), the local orientation M_y and M_z are calculated as per the following equations:

$$M_y(c,d) = \sum_{k=c-N/2}^{m+N/2} . \sum_{l=d-N/2}^{n+N/2} 2g_y(k,l)g_z(k,l) \qquad (1)$$

$$M_z(c,d) = \sum_{k=c-N/2}^{m+N/2} \sum_{l=d-N/2}^{n+N/2} 2(g_y^2(k,l) - g_{yz}^2(k,l)) \qquad (2)$$

$$\Theta(c,d) = \frac{1}{2}\tan^{-1}\left(\frac{M_Y(c,d)}{M_z(c,d)}\right) \qquad (3)$$

Then the consistency levels of the calculated field in the local neighbourhood of block (c,d) are computed using the equations 4 and 5.

$$CL(c,d) = \frac{1}{T}\sqrt{\sum_{(c',d')\in H} \left|\Theta'(c',d') - \Theta(c,d)\right|^2} \qquad (4)$$

$$\left|\Theta - \Theta'\right| = \begin{cases} e & (if\ e = (\Theta - \Theta' + 360) \bmod 360) < 180 \\ e - 180 & otherwise \end{cases} \qquad (5)$$

Here, H is local neighbourhood, T is the number of blocks in H. The ϴ’s are the local ridge orientations of the respective blocks. Then the image is subjected to a segmentation algorithm so as to slash the area of interest.

In the second step, the ridges are detected by using an important property that gray level values are maximum along the direction normal to local ridge orientation. The convolution process with two masks is applied on the image. The gray value at each pixel is compared with the threshold and if it is found to be more, then it is declared as ridge.

In the last step, the minutia points are detected. If the pixel is eight connected and is on a thinned ridge, its value is 1 otherwise 0. Let a pixel (x,y) be on a ridge and H_0:H_7 its eight neighbours.

$$\text{Ridge type=} \begin{cases} (\sum_{i=0}^{7} H_i) = 1 & (x, y)\text{is } \textit{ridge ending} \\ (\sum_{i=0}^{7} H_i) > 2 & (x, y)\text{is } \textit{ridge bifurcatio n} \end{cases} \qquad (6)$$

The identified minutia points are measured and recorded and the feature vector is denoted as an m*3 vector. The feature vector is stored in the database as a template representing the identity of the enrolled user.

B. *Feature Extraction in Hand Geometry*

The process of feature extraction in hand geometry based verification can be viewed as following steps [7]- image acquisition, image pre-processing, feature extraction.

In acquisition step, a color image is acquired by a scanner with the mode set as 300 dot/inch. The acquired image is reduced to 25% both horizontally and vertically. The fingers must lie adjacent to one another, and overlapping is not permitted.

In the preprocessing step, the image is normalized. Subsequently, the image is converted to grayscale image.

© 2018, IJCSE All Rights Reserved

After that, the edge of the hand is detected using an edge detection algorithm.

In the last step, the feature points are detected. The feature points include top points of four fingers and the midpoint of the first stripe of the little finger and the index finger are detected. These six points are considered as the vertices of the complete graph and hence the number of edges will be 15. These fifteen edges are regarded as the feature vectors and are stored in the database.

III. BIOMETRIC SYSTEM VULNERABILITY AND TEMPLATE PROTECTION TECHNIQUES

A variety of vulnerabilities exist in the biometric systems, which needs to be addressed properly to preserve the privacy of the user and also mitigate the attacks [8]. The fish bone model [8] is used to summarize the various causes of biometric system failure. For this, we need to develop the schemes which will secure the stored template. Different types of template security schemes are present in literature with their advantages & limitations. A template security scheme must exhibit the four ideal properties i.e., Diversity, Revocability, Reversibility, Performance. The schemes for securing the templates may be categorized as: biometric cryptosystems or cancelable biometrics.

A. *Biometric cryptosystems* [9]

It combines the concepts cryptography with biometrics. In this scheme, a key is either bound with (key-binding) or generated (key-generation) from the template. The key cannot be revealed without successful authentication of the individual. Hence, is used for securing the template.

B. *Cancelable biometrics* [9]

It distorts the biometric data using some transformation function (invertible or non-invertible) & then the transformed template is stored in database. Based on the characteristics of the transformation function, these schemes can be subdivided into salting (function is invertible) & non-invertible transform (function is non-invertible). When any of the template is compromised, we can discard it & a fresh transformed template will be regenerated.

IV. UNIMODAL TEMPLATE SECURITY SCHEMES

N. K. Ratha et al. [10] presented the study of various methods for generating multiple cancelable templates of fingerprints. Moreover, they also presented the comparative analysis of different transformation algorithms i.e., Cartesian, polar, and surface folding. They carry out the experiments by extracting the feature points through Cartesian transformation, polar transformation, and surface folding and it was found that functional transformation achieves a good performance. Also by plotting the curves, it was clear that surface folding was preferred over the Cartesian and polar transform is comparable to it. The authors concluded that one may generate the cancelable template at feature level having less effort on overall performance.

V. Rani et al. [11] proposed a technique for improving the security of iris template. They used run length encoding, RLE, for compression and state transition optimization for security. The methodology used was: for data hiding, they extract the feature vector of the iris image and then perform the data hiding process. Due to this, the data was hidden under the cover image, and the corresponding results were calculated. For data extraction, the authors selected the desired image from the database and extract the embedded information from it. Then the extracted information is matched against query template. The results obtained shows that traditional techniques has less PSNR & high error rates than this approach.

Ashish MM et al. [12] have proposed an encryption technique to secure the templates. The methodology used by them was that they filtered the image using Gabor filters and minutiae extraction was done by finding the ridge ending and ridge bifurcation. The encrypted template was constructed by using an encryption key and the key is discarded later. Hence, no one can guess the meaning of the stored template. Then, during authentication the stored template is decrypted using the corresponding decryption key and the query template is matched against it. The MSE and PSNR obtained after matching were equal to 255 and 24.0654 respectively. Hence, this safety scheme provides the adequate protection and suitable recognition.

C. Rathgeb et al. [13] addresses the issue of cross-matching in case of bloom filter-based representation by proposing a process based on fuzzy vault scheme. The mapping takes place from the set of bloom filters to the unordered set of unique features. Then the indexes of bloom filters were protected using fuzzy vault scheme so as to achieve unlinkability. The experiments were carried out using Iris database version 1.0, and the results obtained showed that the practical performance rates and reasonable polynomial degrees were obtained for the different configurations of column sizes and block sizes of bloom filters. Also, due to the use of fuzzy vault scheme, the irreversibility was avoided and records have become unlinkable.

R. Alvarez Marino et al. [14] proposed a cryptographic scheme based on fuzzy extractors to protect the iris template by hiding and retrieving a secret from it. In their work, they hide the key S in the coefficients of a ‘d’ degree polynomial at the time of enrollment. At verification, the polynomial must be reconstructed. Here, they have used Lagrange interpolation process and the database used was CASIA iris database. For experiments they used two values for length of S and obtained two results as for |S|=256, FAR=0.97% and for |S|=64, FRR=1.28%. Moreover, the authors found the most balanced bit-length as |S|=192 with following values- FAR=4.42%, FRR=9.67% & GAR=90.33%.

B. Choudhary et al. [15] proposed a cancelable scheme for iris based on steganographic technique shown in Figure 1 by combining the Huffman encoding & DCT into a non-invertible function and hence achieve non-invertibility property. The authors unwrapped the image and perform DCT on it. They also found the Huffman code of the original image. The encoded bit-stream was embedded in the coefficients of DCT of unwrapped iris image. Then, they performed the inverse DCT operation and generate its transformed template. They consider three different types of features for extraction purpose i.e., energy, entropy, standard deviation of the coefficients of Haar wavelet, combination of Haar wavelet and PCA ,and statistical features extracted by gray level co-occurrence matrix (GLCM) for calculating the matching score between the templates. The results show that the accuracy rate becomes equal to 99.71%, EER equal to 1.2% and recognition rate equal to 98.8% which were excellent than traditional techniques.

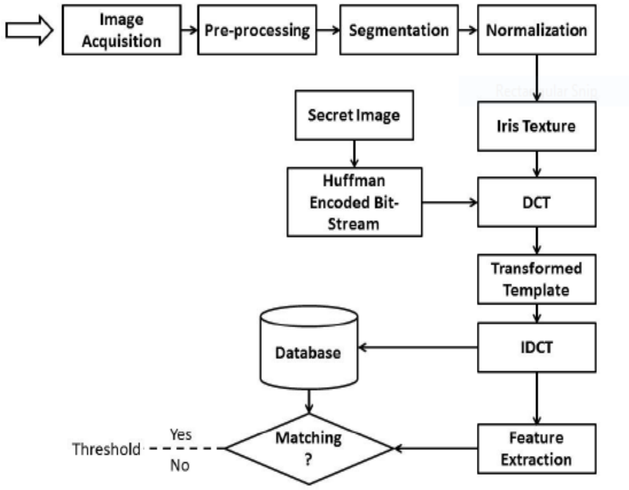

Figure 1. Flow Diagram of Proposed Cancelable Iris Recognition (Adopted from [13])

V. MULTIBIOMETRIC TEMPLATE SECURITY SCHEMES

Ren-He Jeng et al. [16] presented a scheme based on shuffle coding for feature level fusion namely shuffle coding-based feature level fusion (SC-FLF). This scheme aims to fuse the features either from same feature space or different feature space. In their work, they address two methods- SC-FLF with feature scaling and SC-FLF with hashing. The proposed approaches were applied to three modalities- face, iris and palm print. The databases used for testing were- FEI face database, UBIRIS.v1 Session 1 iris database, CASIA-IrisV4 Interval subset iris database and VIPCCL-hand database. The method was compared with the serial & parallel combination methods and the results show that this method achieves a better performance than others. Also, it was demonstrated that the results were better than 1D log-Gabor technique with values as- HFU=0.74%, HFL=0.37%, HFR=0.38%.

A Selwal et al. [17] has proposed a novel NN-based hybrid technique to improve the storage of the protected templates in multimodal systems. In their work, they have used the binary feature vectors obtained by bio-hashing and feature level fusion. On the intermediate vector obtained, they applied their octet indexing technique to reduce its size. After performing experiments, it was found that this technique proves to be better than others both in terms of security and storage overhead. The recognition rate was 98.4% and EER= 0.48%.

J. Aravinth et al. [18] presented the concept of using multimodal biometric recognition in remote biometric authentication. They have used multiple classifiers and score level fusion. The biometric traits taken were the fingerprint, face and iris. There were three classifiers whose scores were fused together to get the final result. After doing experiments, they have demonstrated that the overall performance was improved and the maximum accuracy of the system was 95%. S. Sojan et al. [19] proposed a template security scheme in case of a multi-instance biometric system by taking the fingerprint as the trait. From one instance of the fingerprint, they extracted the minutiae points and from other they extracted the orientation features. Then the two were mixed to get the single mixed template. The datasets were taken from FVC 2000 and NIST respectively. Matching of templates was done by using correlation based method. Moreover, the accuracy was computed by taking the statistical parameters like precision (P), recall (R), and F-measure (F). The results show that the system was accurately able to identify the correct user.

A. M. P. Canuto et al. [1] proposed a cancellable transformation method for template protection. They used the double sum (DS) method, which performs a sum procedure over original attributes and make it hard to get the definition of original data. The DS method consists of summing the three attributes of the same sample which are chosen randomly. Hence, if the imposter gets access to the transformed data, he will not be able to determine the original data. An empirical analysis was also carried out so as to evaluate the feasibility of the method. From results, it was shown that the proposed scheme was slightly better.

D. Jagadiswary et al. [20] proposed an authentication scheme which proves useful in protecting the template also. They fused the three biometric traits i.e., fingerprint, retina, finger vein at feature level. Moreover, the authors used the cryptographic algorithm RSA to protect the templates. During experimentation, it was found that the systems using RSA show better performance than others that don’t use it. The overall performance was increased, and the GAR & FAR came to be equal to 95.3% and 0.01% respectively.

A. Selwal et al. [6] proposed a novel approach for template security in multi instance biometric system. Figure 2 summarizes their working. The authors presented the two instances of fingerprints. In their work, they segment the ROI and assign codes to each based on the angle. Each code consists of 3 bits- $b_2b_1b_0$ representing their position with respect to x-axis, y-axis and position. They used weighted sum rule by keeping $\lambda=0.5$. After experimentation, the results were compared with existing schemes and it was found that FRR and FAR error rates were significantly reduced.

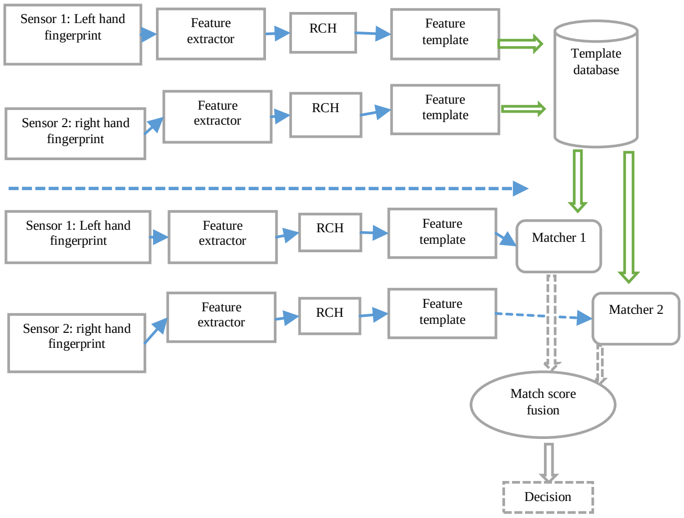

Figure 2. The proposed MBS template security framework [6]

Meng-Hui et al. [21] proposed a feature transformation scheme in order to transform an unordered feature set to an ordered feature vector. This enables fusion of heterogeneous feature sets. The unordered feature set is converted into histogram feature representation whose bins are estimated from the group correspondences of legitimate and imposter users. The experimental results show that the proposed scheme achieves performance that outperforms the already existing transformation schemes. Moreover, the proposed one is able to preserve the power of discriminability of the unordered features.

A Selwal et al. [22] presented the analysis of three conceptual designs for bimodal systems. The biometric traits used were the fingerprint and hand geometry. The analysis was carried out using Fuzzy based Analytical Hierarchy based on different decision parameters. In design 1, they have captured the two traits and extract features from them. The resulting template was stored in the database. During testing, the query template was matched against the stored one. Here, the decision level fusion was used. In decision 2, they used two feature extraction algorithms and then the feature vectors were combined. During verification, the query undergoes the same process and the result is matched with stored one and the person is authenticated based on result. In design 3, multiple feature extraction algorithms were used and 4 feature templates were generated. The results were combined based on rank. After analysis, the results show that the design 2 was optimal having overall ranking of 0.73438.

A Selwal et al. [23] proposed the three design frameworks for multimodal systems. Different template security issues were also analyzed in this system. The proposed system uses two modalities- fingerprint, hand geometry. In 1st framework, the different feature extractors were used. The resultant templates were fused and then stored in database. In 2nd framework, the two templates were stored in separate databases. In 3rd framework, multiple feature extractors were used for both the traits and then their templates were combined. As a result, four different templates were produced and the result was combined on the basis of rank. After experimentation, it was found that framework 1 was suitable with overall value of 0.72796 which was better than other frameworks.

C. Rathgeb et al. [24] proposed a template protection scheme for multi-biometric system. In their work, they used the adaptive bloom filters to get the iris-codes of the two instances of iris of the same subject done at feature level. One advantage of this scheme is to some extent it is alignment-free and also the data is compressed down upto 20% of the original size. The performance was evaluated and was found to be improved by yielding EER below .5%. In addition, this scheme is suitable in identification mode because of fast comparison of secured templates.

VI. COMPARATIVE ANALYSIS

Table 1 shows all the information like techniques and performance measures like FAR, FRR, EER, MSE etc used in different articles and case studies, which were considered during the review analysis. Various techniques were developed for multimodal biometric systems employing different traits and their performance was computed. This led to the research community a path to develop more robust techniques which will improve the overall performance.

Table 1. Survey of Template Security Schemes

Year	Name of Technique/ Method	Performance Measures	Author	Trait
2014	Double Sum	--	A M P Canuto et. al	Face, voice
2007	Cartesian, Polar, Surface Folding	--	N. K. Ratha et. al	Fingerprint
2016	Shuffle coding-based feature level fusion	HFU=0.74%, HFL=0.37%, HFR=0.38%.	Ren-He Jeng et. al	Face, Iris, Palmprint
2017	RLE, State Transition Optimization Algorithm	PSNR=high, MSE, BER= less	V. Rani et.al	Iris

2016	Region Coded Hashing	FAR=0.2%
		FRR=0.05%
			Arvind Selwal et. al	Fingerprint

2016	String Re-arrangement	--	Ashish MM et. al	Fingerprint
2017	NN-based Octet Indexing Technique	Recognition rate= 98.4%, EER=0.48%	A Selwal et. al	Fingerprint, Hand geometry
2016	Rule classifier (fuzzy classifier), lazy classifier (Naïve Bayes), learning classifiers (ABC-NN).	Accuracy=95%	J. Aravinth et. al	Fingerprint, Face, Iris
2016	Correlation		S. Sojan et. al	Fingerprint

2016	Huffman Coding, DCT	Accuracy=99.71%,
		EER= 1.25,
		Recognition Rate=98.8%
			B. Choudha-ry et.al	Iris

2016	RSA	GAR= 95.3%,
		FAR= 0.01%.
			D. Jagadisw-ary et. al	Fingerprint,
				Retina, Finger-vein

2015	Bloom filter, Fuzzy vault		C. Rathgeb et. al	Iris
2016	Histogram		M. H. Lim et. al	
2012	Cryptography, Fuzzy extractor	For |S|=256, FAR=0.97% & For |S|=64, FRR=1.28%	R. Álvarez Mariño et. al	Iris
2016	Fuzzy based Analytic Hierarchy Process	Overall rank= 0.73438	A Selwal et. al	Fingerprint, Hand Geometry
2016	Fuzzy based Analytic Hierarchy Process	Overall value= 0.72796	A Selwal et. al	Fingerprint, Hand geometry
2014	Adaptive bloom filters	EER below .5%.	Rathgeb et. al	Iris

Furthermore, the comparison of template security schemes clearly reveals that most of the schemes has been developed for the multibiometric systems involving either fingerprint or iris traits. It is also observed that the design of an ideal template security scheme with considerably high performance is still a challenging task for the researchers.

VII. CONCLUSION

After going through the variety of techniques which has been proposed by different authors, it has been concluded that the template protection scheme for unimodal biometric systems may not work for another biometric modality. It is mainly because of the fact that there is a variation among the dimensionality as well as the domain of variations among the domain of various feature vectors generated by different biometric modalities. So, this problem leads the research community to design and develop the template security scheme which is efficient in terms of performance as well as satisfy the properties of an ideal template security scheme. The transformation based template security scheme has an upper edge over their counterparts- cryptosystem based schemes. The survey also indicates that there is a trade-off between template security, template size, and overall performance of the biometric based system. Most of the survey also reveal that most of the template security techniques has been developed for multi-instance or multimodal biometric based on the fingerprint, finger vein, iris or face trait. Very few techniques have been designed for a multimodal biometric system based on fingerprint and hand geometry which exhibits high performance in terms of security and identification accuracy. Below mentioned observations could be implemented in future research areas related to biometric based security systems:

- Apart from using the fingerprint, iris and hand geometry traits, brain and heart signal templates can be also used for design of high security biometric system.
- Size of biometric systems should be made compact, by using model order reduction techniques.

- The biometric systems should be able to auto adapt with new templates.
- These systems can be used to detect power thefts.
- Social crimes can be reduced, by increasing application of biometric systems.
- In new biometric template security systems, privacy and discrimination should be given due attention.

ACKNOWLEDGMENT

Authors are highly grateful to the Central University of Jammu administration for providing infrastructural facilities for carrying out this work.

REFERENCES

[1] A. M. P. Canuto, F. Pintro, and M. C. Fairhurst, "An effective template protection method for face and voice cancellable identification," vol. 11, pp. 157–166, 2014.

[2] *Handbook of Biometrics Handbook of Biometrics*. .

[3] 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*, 2013.

[4] D. T. Meva, "Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication," vol. 66, no. 19, pp. 16–19, 2013.

[5] S. R. S. Sree and N. Radha, "A Survey on Fusion Techniques for Multimodal Biometric Identification," pp. 7493–7497, 2014.

[6] A. Selwal and S. K. Gupta, "Region Coded Hashing based Template Security Scheme for Multi-biometric System," no. 3, 2016.

[7] M. A. Rahman, F. Anwar, and M. S. Azad, "A simple and effective technique for human verification with hand geometry," *Proc. Int. Conf. Comput. Commun. Eng. 2008, ICCCE08 Glob. Links Hum. Dev.*, pp. 1177–1180, 2008.

[8] K. Nandakumar, A. K. Jain, and A. Nagar, "Biometric template security," *EURASIP J. Adv. Signal Process.*, vol. 2008, no. January, pp. 1–20, 2008.

[9] C. Lee and J. Kim, "Journal of Network and Computer Applications Cancelable fingerprint templates using minutiae-based bit-strings," *J. Netw. Comput. Appl.*, vol. 33, no. 3, pp. 236–246, 2010.

[10] N. K. Ratha, S. Chikkerur, and S. Member, "Generating Cancelable Fingerprint Templates," vol. 29, no. 4, pp. 561–572, 2007.

[11] V. Rani, M. Kaur, and M. Student, "TC," vol. 3, no. 9, pp. 351–355, 2017.

[12] A. Mm and S. Gr, "Biometric Template Protection," vol. 1, no. 2, pp. 1–8, 2016.

[13] C. Rathgeb, J. Wagner, B. Tams, and C. Busch, "PREVENTING THE CROSS-MATCHING ATTACK IN BLOOM FILTER-BASED CANCELABLE BIOMETRICS da / sec - Biometrics and Internet Security Research Group , Hochschule Darmstadt , Germany Institute for Mathematical Stochastics , University of G ¨," 2015.

[14] R. Á. Mariño, F. H. Álvarez, and L. H. Encinas, "A crypto-biometric scheme based on iris-templates with fuzzy extractors," vol. 195, pp. 91–102, 2012.

[15] B. Choudhury, P. Then, V. Raman, B. Issac, M. K. Haldar, and G. L. Co-, "Cancelable Iris Biometrics Based on Data Hiding Schemes," pp. 1–6, 2016.

[16] R. Jeng and W. Chen, "Two Feature-Level Fusion Methods with Feature Scaling and Hashing for Multimodal Biometrics," vol. 4602, no. March, 2016.

[17] A. Selwal, S. K. Gupta, and Surender, "Low overhead octet indexed template security scheme for multi-modal biometric system," *J. Intell. Fuzzy Syst.*, vol. 32, no. 5, pp. 3325–3337, 2017.

[18] J. Aravinth, S. Valarmathy, J. Aravinth, and S. Valarmathy, "modal biometric recognition and its application to remote biometrics authentication Multi classi fi er-based score level fusion of multi-modal biometric recognition and its application to remote biometrics authentication," vol. 2199, no. December, 2016.

[19] S. Sojan and R. K. Kulkarni, "Mixing Fingerprint Features for Template Security," no. 7, pp. 355–359, 2016.

[20] D. Jagadiswary and D. Saraswady, "Biometric Authentication using Fused Multimodal Biometric," *Procedia - Procedia Comput. Sci.*, vol. 85, no. Cms, pp. 109–116, 2016.

[21] M. Lim, S. Verma, G. Mai, and P. C. Yuen, "Learning discriminability-preserving histogram representation from unordered features for multibiometric feature-fused-template protection," *Pattern Recognit.*, vol. 60, pp. 706–719, 2016.

[22] 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.

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

[24] Rathgeb C, Busch C, "Cancelable Multi-Biometrics: Mixing Iris-Codes based on Adaptive Bloom Filters," *Computers & Security* (2014), doi: 10.1016/j.cose.2013.12.005.

Authors Profile

Mahapara Khurshid has completed Bachelor of Technology in Computer Science and Engineering from Baba Ghulam Shah Badshah University, Rajouri, Jammu in 2015 . She is currently pursuing MTech (Computer Science) from Central University of Jammu, Jammu.. Her main research work focuses on Biometrics template security, Cryptography, Network Security, Cloud Security and Privacy, Bioinformatics.

Arvind Selwal is presently working as Assistant Professor in Department of Computer Science and IT in Central University of Jammu, J&K, India. He holds B.Tech., M.Tech. and Ph.D. degrees in Computer Science and Engineering. He has authored two books on the topic theory of computation and database systems. He has published more than 14 research publications in reputed international journals indexed in popular databases like SCI, Scopus and DBLP. He has more than 13 years of experience in teaching.