IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol-6, Special Issue-5, Jun 2018 E-ISSN: 2347-2693

Biometric Feature Template Security Schemes: An Overview

Sheikh Imroza Manzoor[1*], Arvind Selwal[2]

[1*] Department of Computer Science and IT, Central University of Jammu, Jammu-181143, India
[2]Department of Computer Science and IT, Central University of Jammu, Jammu-181143, India

[*]*Corresponding Author: imrozamanzoor222@gmaill.com, Tel.: +919596075631*

Available online at: www.ijcseonline.org

***Abstract*—** Biometric systems are contemporary tools for human recognition, where the identity of the user is established by using his/her biological, behavioral or chemical characteristics. Biometric based systems are used to overcome many challenges of the traditional based systems. The important information of the biological traits of a user is stored into a database. In the recent past, it has been observed that the security of such biometric systems may be breached in many ways. In this paper, a brief review of various feature template security schemes has been presented. The presented study shows that template security scheme for a particular biometric system may not be suitable for its counterparts. Furthermore, it is revealed that the design of an efficient and accurate template security schemes for a biometric-based application satisfying all the ideal characteristics is still a challenge for the research community.

***Keywords*-** Biometrics, Security, Feature Template, Biometric-based applications, Biometric Cryptosystems

I. Introduction

These days one of the most popular approaches used to identify an individual based on her/his biological traits is Biometrics. The biological information can be either a fingerprint, face, hand geometry, DNA (used rarely), iris, gait, online signature, etc. The biometric-based systems may be of two types namely Uni-biometrics and Multi-biometrics as shown in figure 1. In uni-biometric systems, only one biological trait is used to classify a user into an imposter or a genuine class. In multi-biometric systems, two or more biological traits are used to identify a user into the various classes.

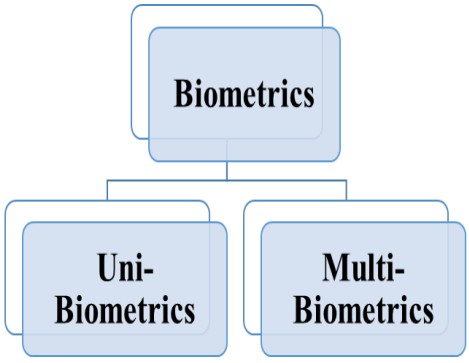

Figure 1: Types of biometric-based systems

The various types of multi-biometric systems are multi-sensor, multi-algorithm, multi-sample, multi-modal, multi-instance and hybrid biometrics. These multi-biometric system classification is shown in figure 2. The biometric system comprises of four modules, capturing module, feature extraction module, matching module and a decision module. The biological information of a trait of the user is captured by using the sensor module or capturing module of the biometric system. This image captured by the sensor module is passed to the feature extractor module. The feature extractor module extracts the important information from the captured image of the biological trait such as minutiae points from the fingerprint, heights and widths of the hand geometry, etc. These key feature points are stored in the database in the form of a feature vector called as a template. In order to ensure security to these key feature vector(FV), Biometric template security plays a key role. Security is one of the biggest challenges in biometrics or in any other information storage system. The security to the template of a user means to hide the original feature points of the feature vector in such a way that it becomes very difficult for the third party to break that template or to perform any spoof attacks using the stored template. There are various kinds of vulnerabilities that are associated with biometric based systems. A fish-bone model given by A.K Jain in 2006 is used to categorize the vulnerabilities associated with the biometric system [1]. Broadly classifying the biometric vulnerabilities into two categories namely: Intrinsic vulnerabilities and Extrinsic vulnerabilities. Intrinsic vulnerabilities are those which are caused by the system's incorrect decision. Intrinsic vulnerabilities are also called as zero-effort-attack. Extrinsic vulnerabilities are those which are caused intentionally by the third party users. These type of attacks are also called as third-party-attacks. Extrinsic vulnerabilities include insider attack, insecure infrastructure,

and biometric overtness. Insider attacks are carried out at an administrative level. To overcome such types of vulnerabilities several template security schemes were proposed for uni-biometric as well as multi-biometric systems by different authors. The four main properties of the template protection schemes are uniformity, revocability, safety, and performance and these all properties are not satisfied by any of the protection schemes till now present in the literature. Some schemes satisfy the three properties and some of them satisfies only two properties as there is a trade-off between all these properties.

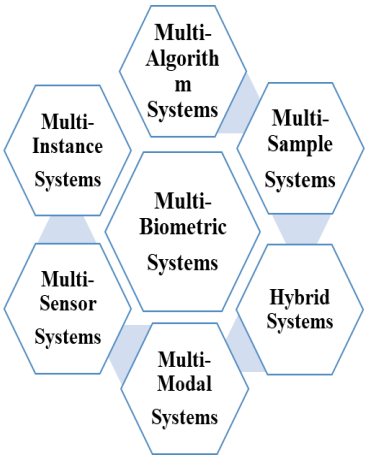

Figure 2: Types of Multi-Biometrics System.

The paper has been divided into four sections. In this paper, the review and analysis of some of the popular template security schemes are presented in section-II and section-III respectively. Furthermore, the conclusion is briefly presented in section IV.

A. Biometric Performance Metrics

There are various number of biometric performance metrics and some of them are discussed below:

- *False Accept Rate (FAR):*

FAR is defined as the total number of imposter users that are falsely accepted by the biometric system. Mathematically, it is shown in Eq. 1:

$$FAR = \frac{\text{Total number of accepted imposter users}}{\text{total number of imposter users present}} \quad (1)$$

- *False Reject Rate (FRR):*

FRR of a system is measured as the total number of genuine users falsely rejected by the biometric system. Mathematically, FRR is shown in Eq. 2:

$$FRR = \frac{\text{number of rejected genuine users}}{\text{total number of users}} \quad (2)$$

- *Genuine Accept Rate (GAR):*

GAR is defined as the total number of attempts in which a genuine user is properly accepted by the biometric system and categorized into a true class. Mathematically, GAR is given in Eq. 3:

$$GAR = (1 - FRR) \quad (3)$$

- *Equal Error Rate (EER):*

EER represents a point in the graph where FAR becomes equal to FRR.

II. Review of Biometric Template Security Schemes

Nalini K. Ratha et.al, June 2001 has identified eight points of failure in the biometric system [2]. These eight points of failure are: Fake biometric at the sensor, resubmission of the old digitally stored biometric signal, override feature extractor, tampering with the feature representation, override matcher, tampering with stored templates, channel attack between, and override the final decision. Further, Anil K. Jain et.al, July 2007 have categorized these types of attacks into four categories namely; intrusions at the sensor level, intrusions between the interface modules, intrusions at the software modules, and intrusions at the template database [3]. The various proposed template security schemes present in the literature are discussed below:

Kong-Yik Chee et.al (2017) have proposed a Uni-Biometrics Cancellable TSS for Speech called as Random Binary Orthogonal Matrices Projection (RBOMP) Hashing. This approach is inspired by Winners-Take-All (WTA) hash algorithm and after this is integrated with the Prime Factorization (PF) function, which is non-invertible. The PF function strengthens the WTA hash algorithm. This approach satisfies the non-invert-ability and revocability properties of the Template Security Scheme (TSS). WTA algorithm helps in performing the fast similarity search at the verification time [4].

Debanjan Sadhya and Sanjay Kumar Singh (2017) have proposed a cancellable biometric TSS for iris using the concept of bloom filters. Bloom filters work on the binary values. In this approach, the key matrix is maintained and size of the key is equal to the length of the bloom filter. The security is improved by randomly choosing the key per bloom filter. This approach is the variation of the predefined bloom filter technique. This scheme is more scalable and practically applicable. It follows the properties like irreversibility, unlinkability and low information leakage from the database. By this approach, the recognition rate is increased [5].

Marta Gomez-Barrero et.al (2017) have proposed a framework for multi-biometric template protection based on homomorphic probabilistic encryption method. This method only handles the encrypted data. The authors have used this Method for fingerprint and online-signature. At the time of

verification, encryption of the templates is not required. The decision is carried out at the feature-level fusion [6].

Arvind Selwal et.al (2017) have proposed a hybrid TSS for a bimodal biometric system. The scheme is a one-way transformation technique developed for hand geometry and fingerprint. In this TSS bio-hashing and octet indexing techniques are used for securing the template. The template stored in the database is of the fixed length (64-Bits) and is non-invertible. Octet indexing is implemented with the help of self-organizing maps. The decision-based matching algorithm is used to classify a user into the genuine and imposter class on a prefixed threshold value. The proposed algorithm has calculated the Equal Error Rate (EER) as 0.48% which is lower than the other schemes and recognition rate as 98.1% [7].

Meng-Hui Lim et.al (2016) have proposed a feature-based multi-biometric (fingerprint & Face) transformation TSS. In this approach, the unordered feature sets of the fingerprint templates are converted into the ordered sets with the help of the histogram representation. Each bin in the histogram represents the interval of the sample feature sets. Histogram features are inherently aligned and are of a fixed length. A histogram feature can be extracted by counting feature points that fall within a specific interval known as a bin. In this paper, the authors have done the experiment on seven unimodal biometric datasets and three bimodal biometric datasets. The proposed technique has achieved the consistent performance over the other well-known transformation-based TSS's. The main objective of this method is to maximize the inter-class variations and intra-class variations [8].

Arvind Selwal et.al (2016) have designed three different frameworks for multi-biometric systems based on fingerprint and hand geometry. Fuzzy Analytic Hierarchy Process (FAHP) with five decision parameters are applied on all the three proposed frameworks. A comparison is done among these three frameworks on the basis of security, fusion, and efficiency. Framework 1 is found to be computational more secure and efficient than other two. The result obtained with the help of FAHP for framework 1, framework 2 and framework 3 is equal to 0.72796, 0.41608, 0.54732 respectively [9].

Firas S.Assaad & Gursel Serpen (2015) have presented a simulation study for a transformation score-based fusion algorithm for multi-modal biometric user authentication with the help of ensemble classification. The ensemble classifier facilitates the multi-modal biometric user authentication. The outputs of voice and face recognition classifiers are taken as inputs to the transformation based score fusion method. The authentication decision is taken by the compatible matching scores provided to a fusion module [10].

Li Lu & Iialiang Peng (2014) have proposed a multi-biometric TSS for a fingerprint to protect the multiple templates of a fingerprint, finger vein, finger knuckle print and the finger shape traits as a single secure sketch. This multi-biometric scheme uses the feature-level fusion algorithm and thus provides the higher recognition accuracy and security. This scheme is based on fuzzy commitment [11].

Munaga V.N.K Prasad and C. Santhosh Kumar (2014) have proposed a fingerprint TSS with the help of multi-line neighboring relation algorithm. The cancellable template is generated with the help of this method. It comprises of four steps namely multi-line neighboring relation generation, plane-based quantization and bit string generation, cancellable template generation and matching. This method fulfills the four properties that are non-invertibility, accuracy, diversity, and revocability of the cancellable biometrics [12].

Zhe Jin et.al (2012) have proposed a fingerprint TSS called as polar grid based 3-tuple quantization technique. It has two advantages alignment-free and performance. This technique has four stages reference minutiae based polar transform, 3-tuple based quantization, bit-string generation and user-specific tokenized permutation and matching. diversity, revocability, and non-invertibility properties are met by this scheme [13].

K.K A. Ghany et.al (2011) have proposed a fingerprint TSS. In this approach, the symmetric bio-hash function is used to protect a template from attacks. It consists of three phases fingerprint pre-processing, fingerprint minutiae extraction and hash value generation [14].

B.J Kang and K.R Park (2009) have proposed multi-modal biometric approaches for a single finger vein and its geometry. This approach is based on score level fusion method based on Support Vector Machine (SVM) with Z-Score normalization. Finger segmentation followed by finger vein segmentation is done on the finger image captured with the help of a device consisting of near-infrared illuminators. After this, the matching score of finger vein and finger geometry is combined using a score level fusion [15].

III. Analysis of Template Security Schemes

The Table-1 is used to compare the various biometric template security schemes discussed in section two. The comparison is carried out on the basis of the modalities used, type of biometrics, type of fusion level, various properties satisfied by the security schemes and on the basis of their performance analysis and datasets used. The analysis clearly shows that the present security schemes are not applicable for all the other biological traits. The analysis clearly shows that all the ideal properties of the template security schemes are not fulfilled so, there is a need for improving these schemes to make them robust.

Table 1: Summary of biometrics template security schemes

Name of the Technique and year	Type of Biometrics and Fusion Type	Modality	Properties	Performance Analysis and Data Sets	Reference
Binary Orthogonal Matrices Projection Hashing (2017)	Uni-Biometrics	Speech	Revocability and Unlink ability	Before protection: EER=1.67%,3.81%,0.60% After protection: EER=3.43%, 7.01%, 0.89%	[4]
Bloom Filter Based biometric template security (2017)	Uni-Biometrics	Iris	Unlink-ability and Irreversibility	GAR=99.2% FAR=0.01%	[5]
Homomorphic Encryption (2017)	Multi-Biometrics and feature level fusion	Online Signature and Fingerprint	-	EER=0.12%	[6]
Low Octet Indexed Template Security (2017)	Multi-Biometrics	Fingerprint and Hand Geometry	Revocability, Diversity, Security and Verification Accuracy	EER=0.48%	[7]
Histogram Representation (2016)	Multi-Modal and Feature transformation fusion	Fingerprint & face	-	For FERET + DB4: EER=0.236 For FRGC + DB3: EER=0.174 For SDVMLA+ HMT: EER= 0.086	[8]
Ensemble Classification (2015)	Multi-Modal Biometrics and Score-Based Fusion algorithm	Voice and Face	-	False-Negative Rate and False-Positive Rate = 0.84% and 0.7% respectively	[10]
Finger Multi-Biometric Cryptosystem (2014).	Multi-Biometric and Feature-Level Fusion	Fingerprint, Finger Vein, Finger Knuckle Print and Finger Shape traits	High Recognition Accuracy and Security	GMR for FMC-Serial and FMC-MCCA = 99.79 and 100% respectively	[11]
Multi-Line Neighbouring relation (2014)	Uni-Biometrics	Fingerprint	Non-Invertibility, Diversity, Revocability and Accuracy	EER For FVC2002 DB1, DB2 and DB3 are 0.62%, 1.33% & 2.64%	[12]
Polar grid based 3-tuple quantization technique(2012)	Uni-Biometrics	Fingerprint	Diversity and irrevocability and Non-Invertibility	EER calculated for FVC2002 DB1 Set B, FVC2002 DB2 Set B, FVC2004 DB1 Set B, FVC2004 DB2 Set B are 5.19, 5.65, 16.62 and 11.64 respectively	[13]
Symmetric Bio-Hash function (2011)	Uni-Biometrics	Fingerprint	Non-Invertibilty	EER= 9.3417e + 017, 0.0136 and 0.2376	[14]
SVM with Z-score normalization (2009)	Multi-Modal and Score-Level Fusion	Single Finger Vein and its Geometry	Moderate Security and Accuracy	EER= 1.702%	[13]

Most of the schemes in the present analysis are of transformation based rather than cryptosystem based. This may be mainly because of the fact that various invertible and non-invertible functions are easily available. Therefore, there is a need for biometric cryptosystem based template security schemes also.

IV. Conclusion

A variety of Biometric applications are available in the market which provides security to various computing systems. The security and protection of various types of information provided by these systems is a challenging task before the research community. In this paper, various biometric template security schemes for protection of extracted information from the various biological traits has been reviewed. The latest trends reveal that none of the biometric template security schemes is capable of meeting all the characteristics of an ideal protection scheme. The template security scheme for one biometric system may not be suitable for its other counterparts. The analysis clearly indicates that most of the techniques have been developed for fingerprint biometric system. These schemes may not be widely used for other traits like face, ear, gait, etc. this is mainly because of the differences in the dimensions of the underlying feature vector template. Therefore, the need is to design and develop more robust schemes not only for uni-biometric systems but also for multi-biometric systems.

References

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A tool for information security," *IEEE Trans. Inf. Forensics Secur.*, vol. 1, no. 2, pp. 125–143, 2006.

[2] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An Analysis of Minutiae Matching Strength," *Audio- Video-Based Biometric Pers. Authentication*, vol. 2091, pp. 223–228, 2001.

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

[4] K.-Y. Chee *et al.*, "Cancellable Speech Template via Random Binary Orthogonal Matrices Projection Hashing," *Pattern Recognit.*, 2017.

[5] D. Sadhya and S. K. Singh, "Providing robust security measures to Bloom filter based biometric template protection schemes," *Comput. Secur.*, vol. 67, pp. 59–72, 2017.

[6] M. Gomez-Barrero, E. Maiorana, J. Galbally, P. Campisi, and J. Fierrez, "Multi-biometric template protection based on Homomorphic Encryption," *Pattern Recognit.*, vol. 67, pp. 149–163, 2017.

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

[8] M. H. 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.

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

[10] F. S. Assaad and G. Serpen, "Transformation-based Score Fusion Algorithm for Multi-modal Biometric User Authentication through Ensemble Classification," *Procedia Comput. Sci.*, vol. 61, pp. 410–415, 2015.

[11] L. Lu and P. J., "Finger multi-biometric cryptosystem using feature-level fusion," *Int. J. Signal Process. Image Process. Pattern Recognit.*, vol. 7, no. 3, pp. 223–236, 2014.

[12] 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.

[13] Z. Jin, A. B. Jin Teoh, T. S. Ong, and C. Tee, "Fingerprint template protection with minutiae-based bit-string for security and privacy-preserving," *Expert Syst. Appl.*, vol. 39, no. 6, pp. 6157–6167, 2012.

[14] A.GHANY Kareem Kamal, A.Moneim Mahmood, Ghali Neveen I., Hassanien Aboul Ella, and Hefny Heshfile, "A Symmetric Bio-Hash Function Based On Fingerprint Minutiae And Principal Curves Approach," *3rd Int. Conf. Mech. Electr. Technol. (ICMET2011)*, no. February 2014, 2011.

[15] B. J. Kang and K. R. Park, "Multimodal biometric method based on vein and geometry of a single finger," *IET Comput. Vis.*, vol. 4, no. 3, p. 209, 2010.

Gge

Authors Profile

Sheikh Imroza Manzoor is presently pursuing master of technology in Computer Science from Central University of Jammu, Jammu-181143. She has completed her Bachelor of Engineering in computer Science from Model Institute of Engineering and Technology, Kotbhalwal, Jammu. Her area of interest includes information security, wireless sensor networks and soft computing techniques.

Arvind Selwal is presently working as Assistant Professor in Department of Computer Science and IT in Central University of Jammu, Jammu-181143. 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.

