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

Design and Development of a Multi-Instance Fingerprint Template Security Scheme

Sheikh Imroza Manzoor[1*], Abdul Rouf Wani[2], Arvind Selwal[3]

[1]Department of Computer Science & IT, Central University of Jammu, India
[2]C.E.O. Kashmosoft, Down Town, Dubai, UAE
[3]Department of Computer Science & IT, Central University of Jammu, India

[*]*Corresponding Author: imrozamanzoor222@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 20/Jun/2018, Published: 30/Jun/2018

***Abstract*—** Cancellable biometrics is one of the productive areas of biometrics and it guarantees the non-invertibility and revocability properties of an ideal template security scheme. In this paper, various cancellable fingerprint template security schemes, their comparison and a novel method for securing the multi-instance fingerprints have been discussed. The pseudocode of the proposed scheme is also presented. The proposed technique produces one fused secured template and this template is formed with the help of feature level fusion technique. The division method is used to secure both of the templates in order to make them non-invertible. The calculated EER and GAR for the proposed technique are 2.87% and 89.937% respectively.

***Keywords*—**Cancellable Biometrics, Many-to-one mapping, Non-Invertible transforms, Biometric Salting

I. INTRODUCTION

Biometrics is an innovative and logical validation technique in view of science and utilized as a part of Identification Accuracy (IA) [1]. Biometric distinguishing proof validates secure passage, information or access through human natural data, for example, DNA or fingerprints. Biometric frameworks incorporate a few connected segments for compelling usefulness. The biometric framework associates an occasion to a solitary individual, while other ID shapes, for example, an individual recognizable Personal Identification Numbers (PIN), might be utilized by anybody. Biometrics is utilized for security frameworks and substitution frameworks for ID cards, tokens or PINs [2], [3].

A biometric framework shown in figure 1 incorporates the accompanying segments and has following features [4]:

- A sensor module is one the basic module of the biometric framework. It is used to capture the important information from the biological trait. The captured information is an image. Image comprises of pixels and each pixel has its own value.
- The image captured with the help of the sensor module are pre-processed with the help of segmentation, image enhancement, etc. techniques in order to get the important feature values called as minutiae points in case of fingerprint from the image with the help of the programming tools. And, this information points known as minutiae points in fingerprint forms the vector called as template.
- The vector template is passed to the matching module and matching module comprises of various programming algorithms with the help of which the query input template feature points are matched with the stored template feature points.
- Finally, a decision module is used to determine the user into the genuine or imposter class on the basis of some threshold value.

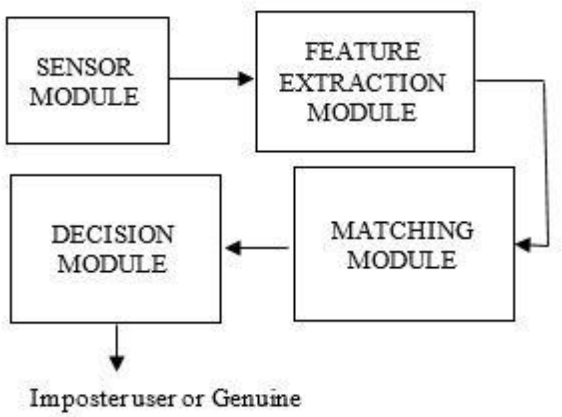

Figure 1: A General Framework of Biometrics

A. Biometric/Biological Traits

The biological traits are categorised into two types namely physiological traits and behavioural traits. The physiological characteristics are derived from the structural information of the body part where as behavioural characteristics are derived from the behaviour of the person. Some of the physiological and behavioural traits are shown in figure 2.

B. Modes of operation of biometrics

The biometrics operates in two modes namely verification mode and identification mode. Both of these modes are explained below:

- *Verification mode*

  In this mode, the 1-to-1 mapping function is used. It means that the query features are compared to the stored trait features of that user only.

- *Identification mode*

  In this mode of biometrics, one-to-many mapping function is used. It means that the query template features are matched with all other feature templates present in the database. This operating method of biometrics is very time consuming but at the same time it yields more accurate results in identifying an individual.

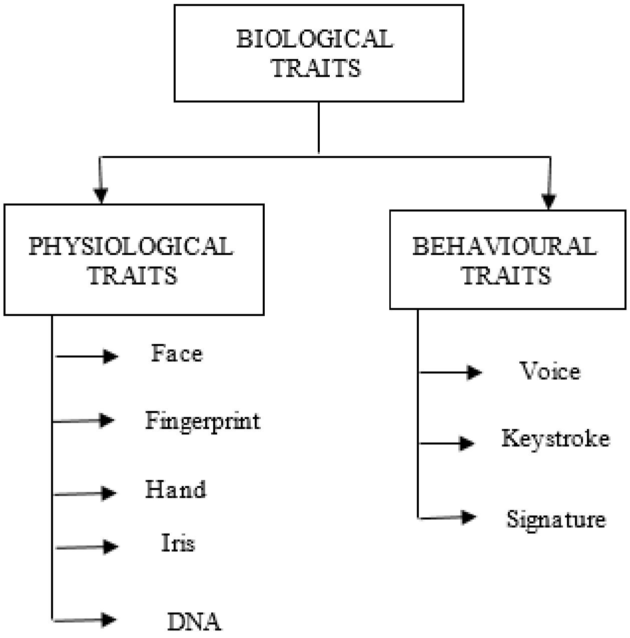

Figure 2: Various Types of Biological Traits

II. CANCELLABLE FINGERPRINT BIOMETRIC TEMPLATE PROTECTION SCHEMES

The cancellable biometrics basically focuses on the two properties namely non-invertibility and revocability [5]. The two types of cancellable biometrics are non-invertible transforms and biometric salting. The previous class applies non-invertible change capacity to the biometric information with the goal that the first biometric information can't be reproduced regardless of whether the cancellable format and change technique are endangered. The revocability of this approach is acknowledged by altering the parameters of the change work. Then again, biometric salting applies change which might be invertible if the client specific mystery key is imperilled [6]. For this situation, the biometric template subjected to the change might be extricated through a non-invertible technique. The mystery key guarantees the uniqueness of the changed format amongst clients and must be displayed upon confirmation. In this subsection, the examples of cancellable biometric plans are talked about with regards to fingerprint biometrics as indicated by each having a place class.

A. Non-Invertible Transforms [5]

Non-invertible transforms are very hard to break. These are one way transformations. Non-invertible transforms are of three types namely projection-based, square remapping and function based. Projection-based transforms are used to convert the single point of consideration into the two dimensional plane with randomised direction and position. Function-based consists of the random parameters and maps these random parameters to the unique number or point in space. Square remapping separates the details of the minutiae points into different squares and assembles their places. All the three discussed techniques of non-invertible transforms are many-to-one.

Sergey Tulyakov et.al have proposed a novel method for the security of fingerprint minutiae points. The authors have used the hashing methods for securing the feature points of fingerprint and have performed the matching of these minutiae points of the fingerprints in hash space. The proposed hash functions do not depend on the location of the various minutiae points like delta and core. The authors have calculated EER for the proposed technique and is found to be equal to 3% [7]. A mystery key is familiar with seed the decisions and request of hash capacities for different fingerprints. This work was reached out by consolidating in excess of one hash capacities amid execution to expand the security of the layout [8]. Additionally, k-plets of particulars were utilized rather than triplets, where k can be more than three. In spite of the fact that it is difficult to switch the hashed information, an extensive number of high power hash capacities are expected to guarantee the revocability of the layout, which prompts high many-sided quality.

Ratha et. al. has presented several methods to generate the multiple fingerprint templates to overcome the several limitations of the traditional password-based and token-based methods. The authors have compared the performance of several proposed methods like polar, Cartesian and surface folding transformation methods of minutiae representations of the fingerprint. The authors have also presented the approximate analysis of the various used method strengths. Further, the authors have concluded that surface folding transformation shows better results than other two proposed transformation-based schemes [9].

Fenq Quan et.al have proposed three methods to recover the original information from the Ratha's template. These three methods or attacks are ARM attack, Brute-Force attack and solving equation attack. The authors have recovered original information from the Ratha's secured template by finding the vulnerable points in the Ratha's secured template strategy. The Ratha has used many-to-one mapping for the non-invertible transformation of the fingerprint but F.Quan et.al found that the many-to-one function is vulnerable at some points and found the original feature values with the help of three proposed attacking methods[10].

B. *Biometric Salting* [5]

The two common techniques used for biometric cancellable salting are Random Projection (RP) and Permutation. These two techniques may be invertible. Both of these techniques are used to extract the fingerprint features so that it would be difficult to convert them back into the original features.

Song Wang and J. Hu have proposed a cancellable fingerprint technique for securing the extracted feature points of the fingerprint. The proposed alignment free scheme is based on the densely infinite-to-one mapping which guarantees the non-invertibility property of an ideal template security scheme. The proposed scheme also satisfies the revocability and template diversity property [11].

On the permutation side, Lee and Kim have presented a novel method known as bit-string representation of fingerprint for generating the cancellable templates [12]. In this approach every minutia is depicted by three dimensional array. And in this array a reference minutiae point is chosen so that all other minutiae can be found and their bit is set to 0 nor 1 accordingly. The authors have shown that the method provides the high revocability, if simple permutation is used.

Zhe Jin et.al have presented the similar approach as discussed above. The only difference is a polar grid is used to quantize the neighbouring minutiae instead of cuboid representation [13].

III. COMPARISON OF VARIOUS CANCELLABLE FINGERPRINT TEMPLATE SECURITY SCHEMES

The various types of above discussed cancellable fingerprint template security schemes are summarized in table I. From the table, it is very clear that some of the techniques are non-invertible based and some are salting based. The mapping function used in all the proposed methods by various authors are many-to-one type. The thoroughly study of such schemes reveals that none of the template security scheme satisfies all the properties of an ideal scheme and are prone to various types of attacks through which the original information of the fingerprint is recovered. In order to overcome such limitations of the present cancellable template security schemes there is a need of development of much more transformation based schemes with powerful non-invertible functions. This is a very big challenge in front of the research community now-a-days. The researchers need to address these types of limitations and continue to work for securing the important information of the user by developing more and more non-invertible as well as salting based methods.

Table 1: Summary of fingerprint cancellable methods

Type of Cancellable Biometrics	**Proposed Methods**	**Mapping Function**	**EER (%)**	**Reference**
Non-Invertible transform	ARM Attack, Brute-force Attack, Solving Equation Attack	Many-to-one	-	[10]
Biometric Salting	Polar Grid Method	Many-to-one	5.19 for FVC2002DB1 and 5.65 for FVC2002DB2	[13]
Non-Invertible transform	Combination of Symmetric Hash Functions	K-plets-to-one	4.98	[8]
Non-Invertible transform	Symmetric hash Function	-	3	[7]
Biometric Salting	Alignment Free Scheme	Infinite-to-one	-	[11]

IV. PROPOSED MULTI-INSTANCE FINGERPRINT (MIF) TECHNIQUE

After reviewing the several cancellable fingerprint techniques, it has been observed that these techniques suffer from the scalability problem. In order to overcome this limitation, a multi-instance fingerprint technique has been developed. The proposed multi-instance fingerprint framework is shown in figure 3. The proposed framework comprises of various steps and these are explained below:

- The left hand and right hand fingerprint minutiae points are represented by FV1 and FV2 respectively.
- From these minutiae points of both the fingerprints, the keys are generated and are given in equation 1 and 2 respectively:

$$K1 = \text{Concatenate}\ (xi,\ yi,\ \theta i) \quad (1)$$

$$K2 = \text{Concatenate}\ (xj,\ yj,\ \theta j) \quad (2)$$

- The division method is used to form the secure fused template T1 and is given in equation 3:

$$T1 = K1 \bmod K2 \quad (3)$$

- The final secured template T1 formed by division method is finally, stored into the database.

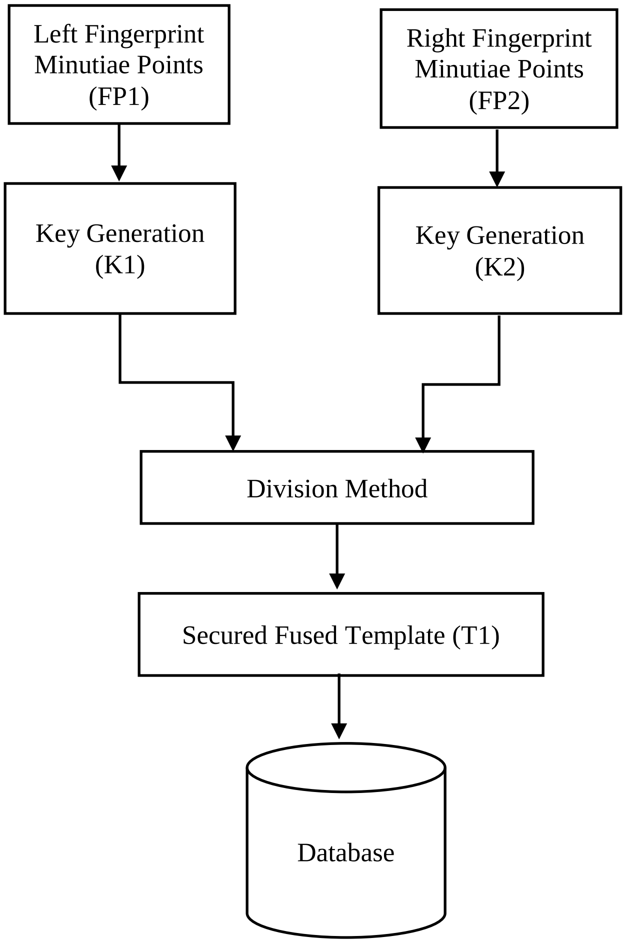
Left Fingerprint Minutiae Points (FP1)
Right Fingerprint Minutiae Points (FP2)
Key Generation (K1)
Key Generation (K2)
Division Method
Secured Fused Template (T1)
Database

Figure 3: The Proposed multi-instance fingerprint Framework

A. Pseudocode of Proposed multi-instance fingerprint technique

The pseudocode of the proposed MIF technique is shown in table II.

Table 2: The pseudocode of proposed MIF

```
Pseudocode of MIF
Input: Two fingerprint templates FV1 and FV2
Output: Secured fused template T1
$FV1 = (xi, yi, \theta i)^n$
$FV2 = (xj, yj, \theta j)^m$
 Where n, m represents the number of minutiae points in each fingerprint
If n = m then
For i= 1 to n
K1 = Concatenate (xi, yi, θi)
K2 = Concatenate (xi, yi, θi)
T1[i] = K1 mod K2
End for

Else if n < m
A = m – n
A1[] = original feature values – A
For i = 1 to n
K1 = Concatenate (xi, yi, θi)
K2 = Concatenate (A1xi, A1yi, A1θi)
T1[i] = K1 mod K2
End for

Else
A = n – m
A1[] = original feature values – A
For i = 1 to n
K1 = Concatenate (xi, yi, θi)
K2 = Concatenate (A1xi, A1yi, A1θi)
T1[i] = K1 mod K2
End for
End if
```

V. Experimental results

The proposed algorithm is evaluated on the DB1 database. Various performance metrics like Equal Error Rate (EER) and Genuine Accept Rate (GAR) are calculated. It is found that the EER is less than the other template security schemes. The comparison of the calculated algorithm's EER with the other template security schemes is shown in table III. The calculated GAR for the proposed technique is 89.937%. The graphical representation of EER and GAR with varying number of subjects for the proposed MIF technique is shown in figure 4 and figure 5 respectively.

Table 3: Comparison of proposed MIF technique with others

Type of Mapping Function	**EER (%)**	**Reference**
Many-to-one	5.19	[13]
K-plets-to-one	4.98	[8]
-	3	[7]
Many-to-one	**2.87**	**Proposed MIF**

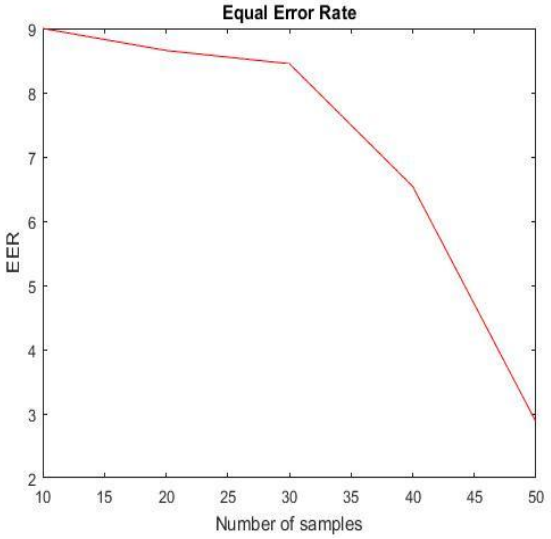

Figure 4: EER Curve for MIF technique

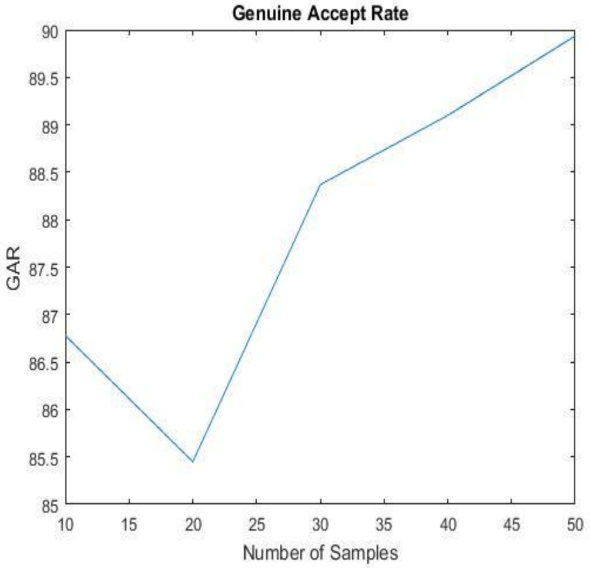

Figure 5: GAR Curve for MIF technique

VI. Conclusion

To provide security to the important feature points of a fingerprint, cancellable biometrics play an important role. In this paper, it has been noticed that all of the fingerprint cancellable template security schemes are developed for uni-biometrics. So, in order to overcome the scalability problem in these techniques, a multi-instance fingerprint framework and its security algorithm has been introduced. It has been found that due to the presence of various vulnerable points in many-to-one mapping functions, there is a need of developing more and more non-invertible many-to-one mapping functions by taking the vulnerable points of that function into the consideration so that original information of the fingerprint's, are not recovered back. The proposed MIF technique shows better results for EER than other fingerprint security schemes.

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] A. K. Jain and A. Kumar, "Biometrics of Next Generation: An Overview," *Second Gener. Biometrics Ethical, Leg. Soc. Context*, vol. 11, pp. 49–79, 2010.

[3] O. Ogbanufe and D. J. Kim, "Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment," *Decis. Support Syst.*, vol. 106, pp. 1–14, 2018.

[4] Introduction to biometrics. "A.K, jain". .

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

[6] C. Rathgeb and A. Uhl, "A Survey on Biometric Cryptosystems," pp. 1–25, 2011.

[7] G. Kumar *et al.*, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognit. Lett.*, vol. 28, no. 16, pp. 2427–2436, 2007.

[8] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of symmetric hash functions for secure fingerprint matching," *Proc. - Int. Conf. Pattern Recognit.*, pp. 890–893, 2010.

[9] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–572, 2007.

[10] F. Q. F. Quan, S. F. S. Fei, C. A. C. Anni, and Z. F. Z. Feifei, "Cracking Cancelable Fingerprint Template of Ratha," *2008 Int. Symp. Comput. Sci. Comput. Technol.*, vol. 2, pp. 572–575, 2008.

[11] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design : A densely infinite-to-one mapping (DITOM) approach," *Pattern Recognit.*, vol. 45, no. 12, pp. 4129–4137, 2012.

[12] 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.

[13] Z. Jin, T. S. Ong, and C. Tee, "Generating Revocable Fingerprint Template Using Polar Grid based 3- Tuple Quantization Technique," pp. 0–3, 2011.

Authors Profile

Sheikh Imroza Manzoor is presently pursuing master of technology in Computer Science and Technology 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, Algorithms, IOT, wireless sensor networks and soft computing techniques.

Abdul Rouf Wani is presently CEO of the Kashmosoft, company in Downtown Dubai, UAE. He has completed his Bachelor of Engineering in Computer Science from Model Institute of Engineering and Technology Kotbhalwal Jammu. He has worked on more than 20 live projects and has developed more than 35 websites alone.

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.