Advances in Science and Technology
Research Journal
Volume 10, No. 31, Sept. 2016, pages 23–30
DOI: 10.12913/22998624/64062

Research Article

A SCHEME FOR TEMPLATE SECURITY AT FEATURE FUSION LEVEL IN MULTIMODAL BIOMETRIC SYSTEM

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

[1] Central University of Jammu, Jammu and Kashmir 181143, India, e-mail: arvind.cuj@gmail.com
[2] I.K. Gujral Punjab Technical University, Jalandhar, Punjab, India, e-mail: skgbecetgsp@gmail.com
[3] Guru Teg Bahadur College, Sangrur, Punjab, India, e-mail: ssjangra20@rediffmail.com

Received: 2016.04.16
Accepted: 2016.07.05
Published: 2016.09.01

ABSTRACT

Biometrics is the science of human recognition by means of their biological, chemical or behavioural traits. These systems are used in many real life applications simply from biometric based attendance system to providing security at a very sophisticated level. A biometric system deals with raw data captured using a sensor and feature template extracted from raw image. One of the challenges being faced by designers of these systems is to secure template data extracted from the biometric modalities of the user and protect the raw images. In order to minimize spoof attacks on biometric systems by unauthorised users one of the solutions is to use multi-biometric systems. Multi-modal biometric system works by using fusion technique to merge feature templates generated from different modalities of the human. In this work, a novel scheme is proposed to secure template during feature fusion level. The scheme is based on union operation of fuzzy relations of templates of modalities during fusion process of multimodal biometric systems. This approach serves dual purpose of feature fusion as well as transformation of templates into a single secured non invertible template. The proposed technique is irreversible, diverse and experimentally tested on a bimodal biometric system comprising of fingerprint and hand geometry. The given scheme results into significant improvement in the performance of the system with lower equal error rate and improvement in genuine acceptance rate.

Keywords: feature template, biometric data, feature vectors, multimodal biometrics, fuzzy sets, database, feature fusion.

INTRODUCTION

In the world of digital technology, accurate and reliable system of authentication is very important for human computer interaction. These days the paradigm is shifting from conventional methods of individual's identification to biometrics systems. Biometrics systems like fingerprint, face, hand geometry, voice, Iris etc. constitutes an important security infrastructure in today's modern life. Biometric systems are also gaining applications in homeland and biometric security. Biometric authentication is also being used to implement national identity or voter identity registration systems. An important application of biometric authentication is in military security checkpoints. Biometrics system is an automatic system which uses measurable, biological or behavioural traits of human to recognize his/her identity [1, 2].

The key features points are extracted from captured image of the biological trait. These features are represented in a feature vector which is called as template. Template is a set of numerical values which represents identity of the enrolled user in the system. A template database is used to store templates of all enrolled users in the biometric system. Multibiometric system is a modification over unibiometric system which uses either multiple instances of the same biological trait or

multiple modalities of same person. In some cases multiple sensors, multiple feature extractors or matching algorithms are also used [1].

In such systems, the results obtained from different sources are combined to get one representation by a fusion process. Multibiomtric systems are used to overcome problems of non universality, low interclass variation, spoofing and accuracy in unibiometric systems. A multi modal biometric system is able to reduce the recognition errors (FAR or FRR) and overall improvement in the performance of the system.

There are four widely used parameters which are used [1, 5]:

1. False Accept Rate (FAR). It may be defined as the chances that a biometric system accepts an imposter or it fails to reject an unauthorised person. It may be expressed as the percentage of accepting an unauthorised user by the biometric system. It is also called as false match rate (FMR).

$$FAR(\%) = \frac{False\ accept\ numbers}{Number\ of\ imposters\ tested} \times 100 \quad (1)$$

2. False Reject Rate (FRR). It may be defined as the chances that a biometric system rejects an already enrolled genuine user. In such cases system falsely refuses to accept an already enrolled person. It is also called as false non match rate (FNMR).

$$FRR(\%) = \frac{Number\ of\ rejections}{Number\ of\ users\ tested} \times 100 \quad (2)$$

3. Genuine accept rate (GAR) is may be defined as the percentage of times actually enrolled users are successfully recognised by the system.

$$GAR\ (\%) = 100 - FRR(\%) \quad (3)$$

4. Equal error rate (EER): It is a point on the curves plot of false accepts rate versus false reject rate where both curves intersects.

$$EER = FAR \text{ where } FAR = FRR \quad (4)$$

Biometric systems for human recognition have proved their superiority compared to traditional password based authentication in many respects. But a biometric system is also prone to different types of spoof attacks. The stored biometric template in database attack is the most dangerous of all possible threats. Therefore providing security to templates in database is one of the most important challenges. This challenge becomes more scalable when multimodal biometric systems are in use for providing the security.

BACKGROUND

In past significant work have been done by many researchers, to secure templates in biometric systems. Templates security techniques for biometric systems are broadly classified in to two categories, namely; (a) Cryptosystems based schemes or helper data based technique (b) feature transformation technique or Cancelable biometrics. In cryptosystems biometric a key is derived and then fused with template to produce a secured template [1]. For securing the finger print templates a hybrid approach is used by the authors in [2]. In their work, a crypto system of fuzzy vault for fingerprint is used to improve the recognition rate as well as the security of the system.

A fuzzy commitment approach is used to construct vault and minutiae descriptors are added, which captures orientation of ridge and information of frequency in the neighbourhood of a minutia's. Experimental results were promising, that by usage of minutiae descriptors, the matching performance of fingerprint system improved from an false accept rate from 0.7% to 0.01% with a Genuine accept rate of 95% which also improved security of system. For providing better accuracy and security to unibiometric systems one of the techniques is to use Multibiomtric systems. One such multi-modal system has been proposed by authors in [3]. The work proposed here is a contactless hand based biometric system which uses visible and infrared imagery. The sensor, here is developed in such a way that it is capable of capturing both color and infrared images of hand. The sensor is capable of capturing the subcutaneous and epidermal features from the hand of a user at the same time. In this five different features are captured from the hand of same user for recognition. It was concluded in results that accuracy in such multimodal systems may be high but security of such systems is always a big concern. In case of transformation based schemes we use intentional and repeatable distortions of biometric signals based on transformation which provides a comparison of various biometric templates in the transformed domain. These schemes have been designed to meet the requirements of an important standard for protection of biometric information given by ISO also called as ISO/IEC- 24745 standards. These two requirements are irreversibility and unlink ability. First property means that original

template must not be easily reconstructed from the stored reference information of user. The second parameter means different versions of secured biometric templates may be generated which are based on the same information of legitimate user. The secured templates must also satisfy the diversity property.

The similar type of classification of template protection schemes is also given by the author in [6], which broadly classify template security schemes into feature transformation and biometric cryptosystems. A Slepian Wolf coding system is proposed in [5] which provide a mean of storing biometric templates in secured way. It also provides a robust biometric authentication for all genuine users of the system and protects it from attacks of imposters. A quantitative parameter has been calculated to show trade-off between performance and security of system. A design has been presented to secure biometric systems using two modalities, namely iris and fingerprint. This design shows that it is easy to achieve security without significant decrease in recognition performance when compared to conventional unibiometric systems. In [6], the author proposed a multimodal biometric system which is based on the fuzzy vault generation. In this system a template and its key is applied to generate a fuzzy vault. During decoding process, the template is fed as an input and it is integrated with the stored fuzzy vault in the database to get corresponding key of user template. The author in [12] provides a framework for the multimodal biometric templates by using the crypto based fuzzy vault. In this system fuzzy vault is used with a password to address some problems in the previous system. System has been implemented on a multi-modal system using three modalities. Two layers of security have been provided one layer is using password another layer is fuzzy vault. A method for providing template data security has been developed recently by [13]. The approach is implemented on fingerprint unibiometric system. These authors proposed an alignment free method for creating the concealable templates. The neighbouring relation around every reference minutiae may be used to generate the secured templates.

To implement the security in biometric authentication, one of the techniques is to use biometrics and cryptography in combination. Among all fuzzy commitment method has been found an efficient and effective technique. In [14], a new fixed feature generation technique for fingerprint biometric system has been proposed by authors, which is based on binary length. Experiments were conducted on three types of fingerprint databases one was picked in house and another two from public domain. The result shows that the proposed binary feature generation technique is more effective and promising. A recent approach to improve security of templates in fingerprint has been developed by authors in [15]. 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 on the image in the form of a special spiral curve.

When dealing with a large template database in multi modal biometric systems, the access time is one of the important performance parameters. In biometric systems, during the identification process the identity of an enrolled user is achieved by comparing it with every template stored in the database. This is a very lengthy matching process which results into poor response rate of the biometric system and, sometimes, false match rate of the system. In [16], authors have used a distributed framework for matching to improve access time while dealing with large template database in fingerprint biometric systems. The access time of the templates in database is considerably improved by the work and 400,000 fingerprints are matched in approximately half a second.

PROBLEM DESCRIPTION

Multimodal biometric systems has been mainly introduced to deal with the problems of inter class variation, accuracy and spoof attacks in unibiometric systems. It is observed that a multi-modal biometric system is also vulnerable to security threats. A very destructive threat is on the template database by the attackers. If an unauthorized user is able to access the template database then using this, original biometric modalities may be reconstructed. Reconstructed fake modalities may be used by attacker for spoofing the system.

Given two feature templates, say T1 and T2 generated from different biometric modalities. The goal is to apply some transformation func-

tion so that a new template T is generated from given templates, such that T is non recoverable. Once T is computed then it is stored in database and represents the identity of the enrolled user.

If f: (T1, T2) → T, Where T1, T2 are the templates in a bimodal system and T is secured template. Objective of this work is to design the mapping function f which generate a secured cancelable template

As shown in the Figure 1, given two biometric modalities; say fingerprint and hand geometry, goal is to design a scheme for securing templates during the feature fusion level.

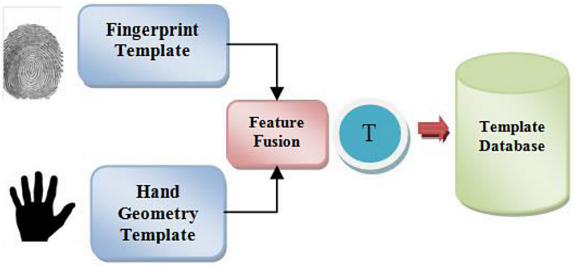

Fig. 1. Template security during fusion of feature vector

PROPOSED SCHEME

A technique for selecting an efficient & cost effective conceptual design where uncertainty lies in the performance parameters is based on fuzzy theory. A fuzzy set is mathematically defined as by assigning to each possible item in the universe of discourse a value representing its rank of membership in the fuzzy set [L. Zadeh, 1965]. The proposed scheme to secure template data is shown in Figure 2. Let T1 and T2 be two template vectors generated from different biometric modalities. Suppose T1 be a n×3 dimensional feature template generated from fingerprint biometric system. The fingerprint biometric extracts the features points from the raw image of the user and these feature points are denoted by a triplet (x, y, ∅), where (x, y) is the positional parameter of a feature point and ∅ is the angular dimension of feature point with x axis. If there are n feature points then feature vector consists of n×3 numerical values which are actually stored in database.

$$T_1 = \begin{matrix} X1 & Y1 & \emptyset 1 \\ \ldots. & \ldots & \ldots \\ Xn & Yn & \emptyset n \end{matrix} \quad (5)$$

Suppose T_2 be a 1×m dimensional feature vector generated from hand geometry biometric system. The feature points in hand geometry are either length or width of five fingers. If there are m numbers of such measurements then feature vector is simply one dimensional array of size m.

$$T_2 = [v_1, v_2, v_3, v_4 \ldots\ldots\ldots\ldots v_m] \quad (6)$$

These feature vectors are normalized using any available score normalization technique. Suppose after normalization, vectors are T_3 and T_4 respectively. Let x and x′ denote a feature value before and after normalization, respectively. The min-max technique computes x′ as:

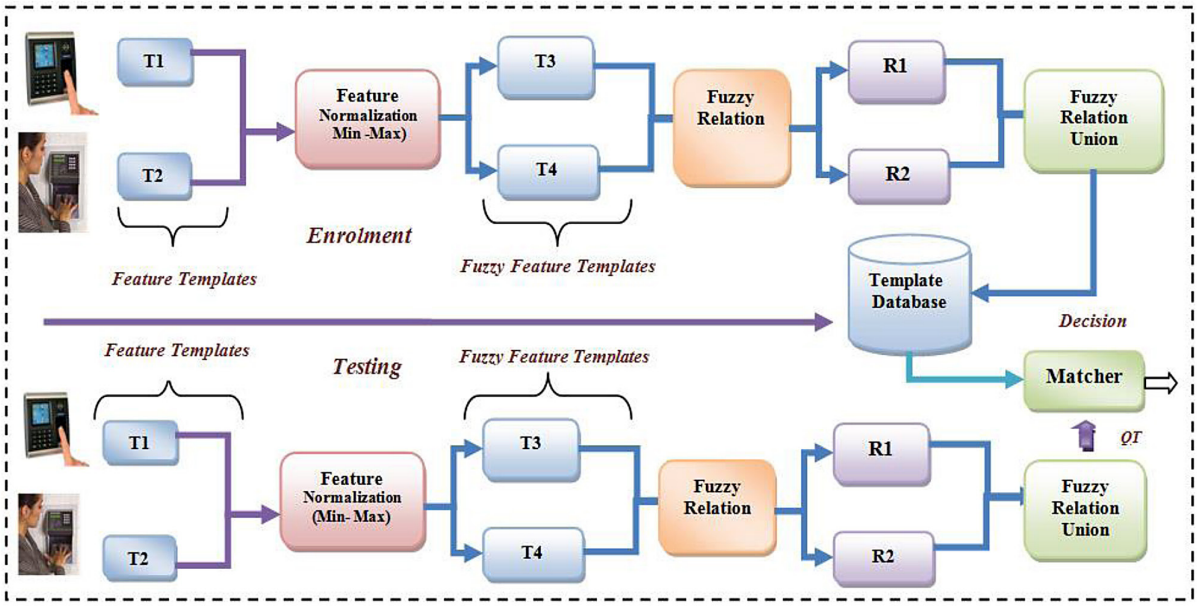

Fig. 2. Proposed fuzzy relation based template security scheme

$$x' = \frac{x - \min F(x)}{\max(Fx) - \min(Fx)} \quad (7)$$

After normalization, these templates are termed as T_3 and T_4 respectively. It is noticed that values are lying in a range of [0,1]. It shows fuzziness of intermediate values after normalization. Fuzzy operation may be applied on these two intermediate feature templates.

$$\begin{aligned} T_3 = \{&(\mu(a_{11}), \mu(a_{12}), \mu(a_{13}), \mu(a_{14}) \ldots\ldots\ldots\ldots \mu(a_{1n}) \\ &\mu(a_{21}), \mu(a_{22}), \mu(a_{23}), \mu(a_{24}) \ldots\ldots\ldots\ldots .\mu(a_{2n}) \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\mu(a_{m1}), \mu(a_{m2}), \mu(a_{m3}), \mu(a_{m4}) \ldots\ldots\ldots\ldots .\mu(a_{mn})\} \\ T_4 = \{&\mu(b_{11}), \mu(b_{12}), \mu(b_{13}), \mu(b_{14}) \ldots\ldots\ldots\ldots \mu(b_{1n})\} \end{aligned} \quad (8)$$

Equation 8 shows that dimensions of intermediate feature vectors, T_3 and T_4 are different. To convert feature vector T_3 into one dimensional vector simply applying row major and column major representation schemes. Let called these feature vectors are T_3' and T_3''. We are ready to make two fuzzy relations; one from T_3' and T_4 and another T_3'' and T_4 fuzzy sets.

$$R_1 = T_3' \times T_4 = \min(\mu(T_3'), \mu(T_4)) \quad (9)$$

$$R_2 = T_3'' \times T_4 = \min(\mu(T_3''), \mu(T_4)) \quad (10)$$

For fusion of these two templates into one union of fuzzy relation may be used. Union of fuzzy relations R_1 and R_2 into T is given by Eq. 11.

$$T = \mu_T = \mu_{R1 \vee R2} = \text{maximum}[\mu_{R1}(x,y), \mu_{R2}(x,y)] \quad (11)$$

Algorithm: Pseudo code of proposed template security

Input: Two feature templates T_1 and T_2 generated from different biometric modalities.

Output: Secured template T to be stored in database.

1: $[T_1]$ be a feature template vector of size n×3 and $[T_2]$ is another feature template vector of size 1×n.

$[T_1] \leftarrow \partial_1(x)$

$[T_2] \leftarrow \partial_2(x)$

Where: $\partial_1(x)$ and $\partial_2(x)$ are two feature vector extractors for two respective biometric modalities.

2: Feature normalization

$f\text{Norm} : [T_3] \leftarrow ([T_1])$

$f\text{Norm} : [T_4] \leftarrow ([T_2])$

3: Fuzzy relations conversion

$T_3' = \text{Convert row major}([T_3])$

$T_3'' = \text{Convert row major}([T_3])$

$[R_1] \leftarrow Fz([T_3' \times T_4])$

$[R_2] \leftarrow Fz([T_3'' \times T_4])$

4: Fuzzy relation union: Let T be the final template which is to be stored in database

$T \leftarrow R_1 \vee R_2$

5: Stop

RESULT ANALYSIS

In this section steps of the proposed scheme are explained with an example. Let T1 be a template vector extracted from fingerprint biometric and T2 be another feature vector derived from hand geometry biometric. Figures 3 and 4 shows source images with feature point representation in a bimodal biometric system.

For example templates T1 have 3 samples feature points.

$$T_1 = \begin{matrix} 15 & 05 & 30 \\ 04 & 20 & 50 \\ 70 & 03 & 90 \end{matrix} \quad (12)$$

Now let us assume T2 is another feature template of 16 feature points extracted from hand geometry modality.

$$T_2 = [4, 20, 15, 6, 15, 22, 40, 25, 20, 8, 9, 20, 5, 6, 7, 10] \quad (13)$$

Looking at templates T_1 and T_2, it is clear that values in both are falling in different ranges. Before fusion we need to normalize these two templates so that both falls between range [0,1]. For feature normalization one of the popular techniques called as min-max technique is used.

After using Equation 7 for normalization the templates will have following values:

$$T_3 = \begin{matrix} \underline{\mathbf{70}} & \underline{\mathbf{20}} & \underline{\mathbf{90}} \\ 0.12 & 0.01 & 0.30 \\ 0.00 & 0.18 & 0.58 \\ 0.76 & 0.01 & 1.0 \end{matrix} \quad (14)$$

$$T_4 = [0.0, 0.4, 0.30, 0.05, 0.36, 0.44, 1.0, 0.58, 0.44, 0.11, 0.13, 0.44, 0.02, 0.05, 0.08, 0.16] \quad (15)$$

Convert vector T3 to one dimensional vector T3 first using row major representation and then by using column major representation method. Now let intermediate feature vectors be named as T3' and T3'' respectively.

$$T3' = [0.12, 0.01, 0.30, 0.0, 0.18, 0.58, 0.76, 0.01, 1.0] \quad (16)$$

$$T3'' = [0.12, 0.00, 0.76, 0.01, 0.18, 0.01, 0.30, 0.58, 1.0] \quad (17)$$

Applying eq. 9 and 10 on vectors in equation 14 and 15, the fuzzy relations R1 and R2 are constructed as shown below:

Fuzzy Relation R_1								
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.12	0.01	0.30	0.0	0.18	0.4	0.4	0.01	0.4
0.12	0.01	0.30	0.0	0.18	0.30	0.30	0.01	0.30
0.05	0.01	0.05	0.0	0.05	0.05	0.05	0.01	0.05
0.12	0.01	0.30	0.0	0.18	0.36	0.36	0.01	0.36
0.12	0.01	0.30	0.0	0.18	0.44	0.44	0.01	0.44
0.12	0.01	0.30	0.0	0.18	0.58	0.76	0.01	1.0
0.12	0.01	0.30	0.0	0.18	0.58	0.58	0.01	0.58
0.12	0.01	0.30	0.0	0.18	0.44	0.44	0.01	0.44
0.11	0.01	0.30	0.0	0.11	0.11	0.11	0.01	0.11
012	0.01	0.11	0.0	0.13	0.13	0.13	0.01	0.13
0.12	0.01	0.13	0.0	0.18	0.44	0.44	0.01	0.44
0.02	0.01	0.30	0.0	0.02	0.02	0.02	0.01	0.02
0.05	0.01	0.02	0.0	0.05	0.05	0.05	0.01	0.05
0.08	0.01	0.08	0.0	0.08	0.08	0.08	0.01	0.08
0.16	0.01	0.16	0.0	0.16	0.16	0.16	0.01	0.16
Fuzzy Relation R_2								
0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
0.12	0.0	0.4	0.01	0.18	0.30	0.0	0.4	0.4
0.12	0.0	0.30	0.01	0.18	0.30	0.0	0.30	0.30
0.05	0.0	0.05	0.01	0.05	0.05	0.0	0.05	0.05
0.12	0.0	0.36	0.01	0.18	0.30	0.0	0.36	0.36
0.12	0.0	0.44	0.01	0.18	0.30	0.0	0.44	0.44
0.12	0.0	0.76	0.01	0.18	0.30	0.0	0.58	1.0
0.12	0.0	0.58	0.01	0.18	0.30	0.0	0.58	0.58
0.12	0.0	0.44	0.01	0.18	0.30	0.0	0.44	0.44
0.11	0.0	0.11	0.01	0.11	0.30	0.0	0.11	0.11
12	0.0	0.13	0.01	0.13	0.11	0.0	0.13	0.13
0.12	0.0	0.44	0.01	0.18	0.13	0.0	0.44	0.44
0.02	0.0	0.02	0.01	0.02	0.30	0.0	0.02	0.02
0.05	0.0	0.05	0.01	0.05	0.02	0.0	0.05	0.05
0.08	0.0	0.08	0.01	0.08	0.08	0.0	0.08	0.08
0.16	0.0	0.16	0.01	0.16	0.16	0.0	0.16	0.16

Finally applying the formula given in equation-11 to the fuzzy relations R1 and R2, secured template T is stored in database as shown in Figure 5. The proposed scheme is implemented in MATLAB with openly available source code of fingerprint and hand geometry biometric systems. The performance of the proposed system is evaluated experimentally for two important parameters namely; equal error rate (EER) and genuine accept rate (GAR). The proposed algorithm is run on a primary multimodal dataset of 100 users with 3 samples from each user and results are summarized in Table 1.

Equal error rate of proposed scheme is 3.30%, which is low as compared to unibiometric systems. Genuine accept fraction of the proposed scheme is approx. 97.3%, which is a significant improvement in performance. The results clearly indicate that proposed scheme not only secure the template but also improves the recognition rate as well as accuracy during feature fusion level. The proposed algorithm takes O(n2) time to convert and fuse the templates generated from different biometric modalities. Irreversibility is also ensured by the proposed scheme, which is an important feature of template security scheme, as listed in ISO/IEC24745 standard. Developed scheme removes the problem of an attacker learning the original minutia position in fingerprint and various measurements of hand geometry. If an attacker is successful in getting access to the secured template T stored in database, then it is almost impossible to reconstruct the original biometric modality. The proposed template security scheme offers sufficient interclass variation among the template of legitimate users and also diverse in nature. On the flip side, the proposed scheme is comparatively less revocable and therefore difficult to cancel the secured and stored template in the case, it is compromised.

CONCLUSIONS

Template data security is one of the issues while designing accurate biometric system. Research studies have already shown that there is a trade-off between computational complexity and accurate template security scheme. In this work feature fusion process is used to serve dual purpose of combining templates generated from two biometric modalities as well as securing the templates. The proposed technique is beneficial, particularly because of the fact that templates are secured during feature fusion step. A transformation based template security scheme is used to protect the template from attackers. The proposed template security scheme improves the overall performance of the multi-modal bio-

Table 1. Experimental results

Sr. No.	Biometric modalities	Equal Error Rate (EER %)	Genuine Acceptance Rate (GAR %)
1.	Typical fingerprint unibiometric systems	~5–10	~87.2–93
2.	Most hand geometry systems	~11.50	~76.0
3.	Proposed template security scheme for multi-modal biometric system	~3.30	~97.7

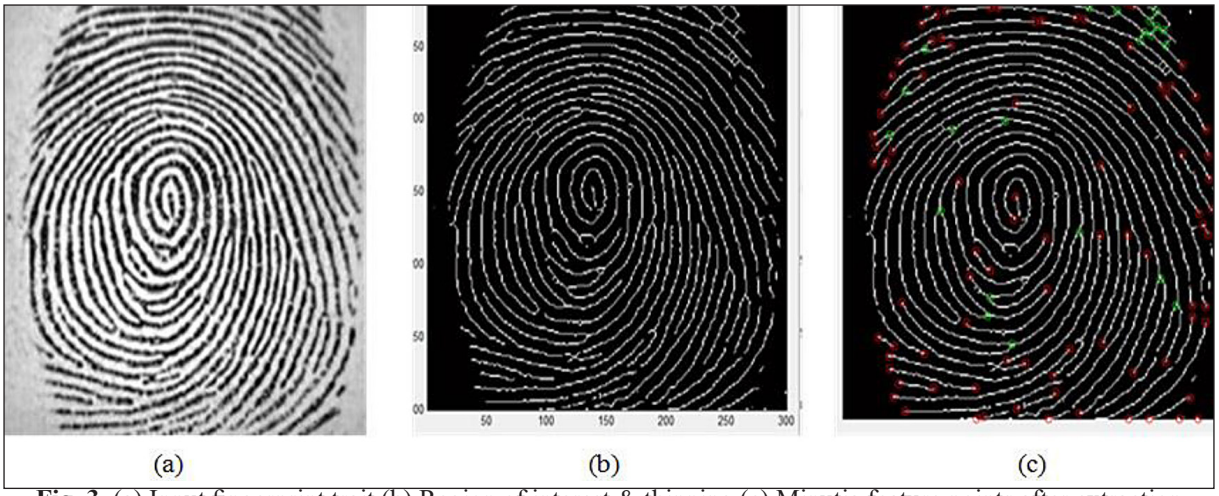

Fig. 3. (a) Input fingerprint trait (b) Region of interest & thinning (c) Minutia feature points after extraction

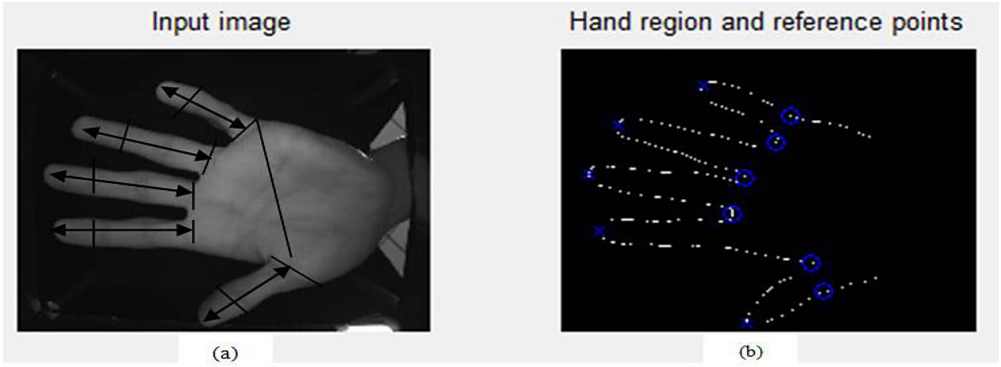

Fig. 4.:(a) Input hand geometry trait (b) Finger's tips and roots points for features computation

Secured template T								
0	0	0	0	0	0	0	0	0
0.12	0.01	0.4	0.01	0.18	0.4	0.4	0.4	0.4
0.12	0.01	0.3	0.01	0.18	0.3	0.3	0.3	0.3
0.05	0.01	0.05	0.01	0.05	0.05	0.05	0.05	0.05
0.12	0.01	0.36	0.01	0.18	0.36	0.36	0.36	0.36
0.12	0.01	0.44	0.01	0.18	0.44	0.44	0.44	0.44
0.12	0.01	0.76	0.01	0.18	0.58	0.76	0.58	1
0.12	0.01	0.58	0.01	0.18	0.58	0.58	0.58	0.58
0.12	0.01	0.44	0.01	0.18	0.44	0.44	0.44	0.44
0.11	0.01	0.3	0.01	0.11	0.3	0.11	0.11	0.11
0.12	0.01	0.13	0.01	0.13	0.13	0.13	0.13	0.13
0.12	0.01	0.44	0.01	0.18	0.44	0.44	0.44	0.44
0.02	0.01	0.3	0.01	0.02	0.3	0.02	0.02	0.02
0.05	0.01	0.05	0.01	0.05	0.05	0.05	0.05	0.05
0.08	0.01	0.08	0.01	0.08	0.08	0.08	0.08	0.08
0.16	0.01	0.16	0.01	0.16	0.16	0.16	0.16	0.16

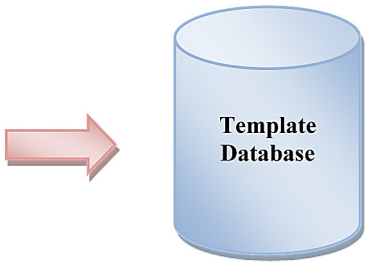

Fig. 5. Proposed secured template T in database

metric system with significantly low equal error rate of 3.3% (EER) and increase in genuine acceptance rate of 97.3% (GAR). Future scope is to evaluate the proposed system using standard biometric datasets and some other biometrics system performance parameters may be analyzed.Computational efficiency of the proposed algorithm may also be improved in the future by using some optimization techniques. As a future research, an appropriate indexing technique may be used to reduce the storage requirement of the secured template.

Acknowledgements

Authors extends their sincere thanks to Department of Research, Innovation and Consultancy (RIC), I.K. Gujral Punjab Technical University, Jalandhar, India for providing all necessary infrastructural help and support to carry out this research work.

REFERENCES

1. Cavoukian A., Stoianov A.: Biometric encryption. Encyclopedia of Biometrics, Springer Verlag, 2009, 1–14.
2. Chouaib Moujahdi, George Bebis, Sanaa Ghouzali, Mohammed Rziza: Fingerprint shell: Secure Representation of Fingerprint Template. Journal homepage: www.elsevier.com/locate/patrec, Pattern Recognition Letters 45, 2014, 189–196.
3. Abhishek Nagar, Karthik Nandakumar, Anil K. Jain: A Hybrid Biometric Cryptosystem for Securing Fingerprint Minutiae Templates. Pattern Recognition Letters 31, 2010, 733–741.
4. Ann Cavoukian: Keynote Paper: Biometric Encryption: Technology for Strong Authentication, Security and Privacy. The International Federation for Information, Springer Verlag, Vol. 261, 2008, 57–77.
5. Vetro A., Draper S.C., Rane S., Yedidia J.: Securing Biometric Data. Preprint of A Chapter. In: Distributed Source Coding, P.L. Dragotti & M. Gastpar (Eds.), Academic Press, Feb. 2009, 1–16. DOI: 10.1016/B978-0-12-374485-2.00016-0.
6. Jain A.K., Karthik Nandakumar, Abhishek Nagar: Review Article Biometric Template Security", Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing, Vol. 5, 2008.
7. Brindha V.E., Natrajan A.M.: Multi Modal Biometric Template security: Finger Print and PalmPrint base Fuzzy Vault. Journal of Biometrics and Biostatistics, 3(3), 100–150.
8. Hani M.K., Marsono M.N., Bakhteri R.: Biometric encryption based on fuzzy vault scheme with a fast chaff generation algorithm. Journal homepage: www.elsevier.com/locate/fgcs, Future Generation Computer Systems 29, 2013, 800–810.
9. Feng Y.C., Yuen P.C., Jain A.K.: A Hybrid Approach for Generating Secure and Discriminating Face Template. IEEE Transactions on Information Forensics and Security, 5(1), 2010.
10. Li Lu, Jialiang Peng: Finger Multi-biometric Cryptosystem using Feature-Level Fusion. International Journal of Signal Processing, Image Processing and Pattern Recognition, 7(3), 2014, 223–236.
11. Nagar A., Nandakumar K., Jain A.K.: Multibiomtric Cryptosystems Based on Feature-Level Fusion, IEEE Transactions on Information Forensics and Security, 7(1), 2012, 255–268.
12. Mihailescu M.I.: New Enrollment Scheme for Biometric Template using Hash Chaos-Based Cryptography. Procedia Engineering, 69, 2014, 1459–1468. DOI: 10.1016/j.proeng.2014.03.142,
13. Meenakshi V.S., Padmavathi G.: Security Analysis of Password Hardened Multimodal Biometric Fuzzy Vault with Combined Feature Points Extracted from Fingerprint, Iris and Retina for High Security Applications. Computer Science 2, 2010, 195–206.
14. Prasad M.V.N.K., Kumar S.: Fingerprint template protection using multiline neighboring relation. www.elsevier.com/locate/eswa, International Journal of Expert Systems with Applications, 41, 2014, 6114–6122.
15. Peng Li, Xin Yang, Hua Qiao, Kai Cao, Eryun Liu, Jie Tian: An effective biometric cryptosystem combining fingerprints with error correction codes. Expert Systems with Applications, 39, 2012, 6562–6574.
16. Petralta D., Triguero I., Sanchez-Reillo R., Herrera F., Bentez J.M.: Fast Fingerprint Identification for Large Databases. Pattern Recognition, 47, 2014, 588–602.