Reducing Vulnerability of a Fingerprint Authentication System

A. Athira Ram(✉) and T.S. Jyothis(✉)

Jyothi Engineering College, Trissur, India
athiraram@gmail.com, jyothis@jecc.ac.in

Abstract. A fingerprint authentication system usually suffers from privacy problem. A third party intruder can steal the information stored in the database and try to recreate the original fingerprint. Here a system is proposed which prevents the possibility of generating fingerprints from the information in the database. Two different fingerprints are acquired from a person. Then the orientation of ridges is calculated from the first fingerprint and minutiae points are extracted from a reference area in second fingerprint. They are combined to form a mixed template which is encrypted using blowfish cipher. The encrypted template serves as a virtual biometric. This prevents the revealing of original fingerprints to third party intruders. Moreover the attacker may not be aware that it is a mixed template that is used rather than the original fingerprint.

Keywords: Authentication · Biometric · Enrollment · False acceptance rate · False rejection rate · Feistel network · Ridge · Skeletonization

1 Introduction

A fingerprint authentication system is the most commonly used Biometric Authentication systems. A fingerprint is an impression left by the friction ridges found on the inner surface of human fingers. A friction ridge is a raised portion of the epidermis on the surface of the palms [1]. The ridges and the furrows constitute the fingerprint pattern. Fingerprints are one of the unchangeable and infallible means of human identification because the ridge patterns are detailed, unique, never repeat, difficult to alter and persist throughout life. It is because of these characteristics fingerprint technology is widely used in authentication systems. The uniqueness of fingerprint patterns made it to be used as to differentiate the legitimate users with frauds. Certain features from fingerprint are extracted during authentication and they are stored on databases. As time moved on, people started even to fool these systems by making an artificial pattern of fingerprints from the stolen data stored in the database. The issue that arises in this type of system is protection of fingerprint privacy [2]. The work in [3] proposes a bio-hashing method in which a pseudo random number is mixed with fingerprint features. The accuracy of this approach depends on key which is assumed to be never stolen. In [4] some transformation which uses a key is proposed. Here use of key reduces the matching accuracy. A fuzzy vault is used to secure fingerprint in [5]. But this method is vulnerable to key inversion attack. In [6] a biometric mixing method is proposed where each person gives two fingerprints. Minutiae points from them are

J.H. Abawajy et al. (Eds): SSCC 2015, CCIS 536, pp. 157–167, 2015.
DOI: 10.1007/978-3-319-22915-7_15

found and superimposed. Combined minutiae list becomes the combined biometric ID. Compared with other techniques, combined biometric is more secure since the attacker may not be aware that a combined template is stored in database. Here a system is proposed such that it is capable to provide privacy to the stored fingerprints. In the proposed system instead of using a single fingerprint, two different fingerprints are used. From both of them different features are extracted and then a combined template is formed which is then encrypted using a private key.

2 Proposed System

Two different fingerprints are to be acquired from two different fingers of a person during the enrollment process. From the first fingerprint, orientation of ridges is estimated. Then from the second fingerprint, a reference area is selected and from there minutiae points are extracted. Then using these, a combined fingerprint sample area is created. This combined fingerprint sample is undergone encryption using a secret key.

2.1 Fingerprint Sensing

Fingerprint Sensing is the process of acquiring fingerprint of a person through either live scan method or inked fingerprint method. For the proposed system, two fingerprints are to be obtained from two different fingers.

2.2 Pre-processing of Fingerprints

Fingerprints are pre-processed before processing them to enhance poor fingerprint patterns. The very first step in the pre-processing of fingerprints is the conversion to black and white images. In this step all the pixel values in the fingerprint images are converted either to 0 or 1. The bi-level conversion of image is depicted in Fig. 1.

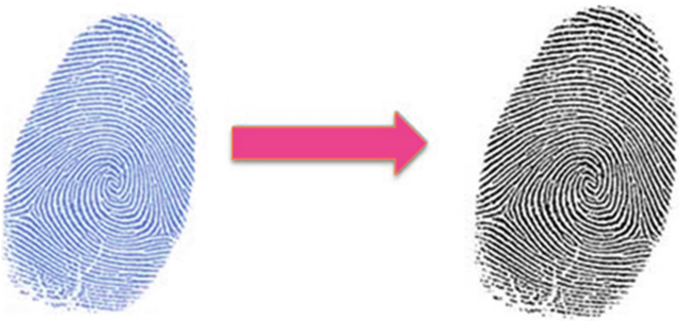

Fig. 1. Conversion to bi-level image

The next pre-processing step is to skeletonize the fingerprints. Fingerprint skeletonization is the thinning of ridges in fingerprint to one pixel width. The thinning process is shown in Fig. 2.

Fig. 2. Thinning of fingerprint

In the proposed system, both the fingerprint images are to be made bi-level and to be thinned.

2.3 Orientation Estimation

The first step is to find the orientation of the first fingerprint. Orientation is the direction of ridges [7].Orientation is not estimated for a pixel alone but for a block of pixels. For that the fingerprint image is divided into N x N set of non-overlapping block of pixels. An example orientation image is shown in Fig. 3.

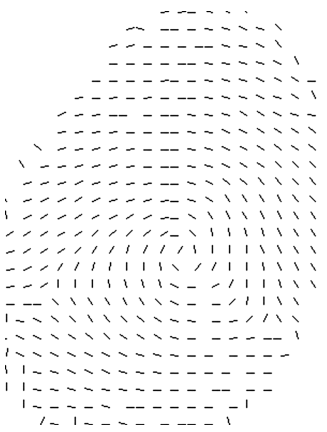

Fig. 3. Orientation image

2.4 Reference Area Detection

Next step is to detect the reference area in the second fingerprint patterns. Basically there are four different fingerprint patterns which are shown in Fig. 4.

Fig. 4. Fingerprint patterns: Arch, Tent, Whorl, Loop

Based on the fingerprint patterns, certain points can be detected which is called as singular points. They are the points where there is a sudden change in ridge direction. There are two types of singular points: Core and Delta points shown in Fig. 5

Fig. 5. Core and Delta in fingerprint patterns

In the proposed system, a reference area is selected around the singular point in second image. The size of area depends on the size of fingerprint image.

2.5 Minutiae Point Extraction

Minutiae are small precise details of a fingerprint pattern [8]. They are of two types: Ridge endings and Ridge bifurcations which are shown in Fig. 6. Ridge endings are the points where the ridges end abruptly and ridge bifurcations are the points where the ridges split into two ridges.

The minutiae points are obtained by scanning the local neighbor pixels of each pixel in the skeletonized fingerprint image, using a 3×3 window. The crossing number is calculated which is the sum of pixel value and its neighbouring pixel values as shown in Fig. 7.

Fig. 6. Minutiae points

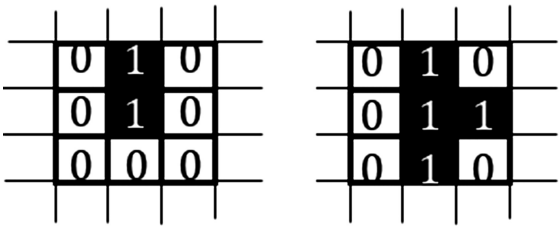

Fig. 7. Crossing number calculation

If the crossing number equals 2, then it is a ridge ending and if it equals 4 then it is a ridge bifurcation.

A minutiae m_i is described by four parameters: $m_i = (x_i, y_i, \Theta_i, t_i)$ where x_i, y_i are coordinates of the minutiae point, Θ_i is minutiae direction and t_i is type of the minutiae point (ridge ending or ridge bifurcation)

2.6 Combined Fingerprint Generation

Using the orientation of first fingerprint and the minutiae points in the reference area of second fingerprint, a combined fingerprint template is generated as in Fig. 8. The minutiae point $(x_i, y_i, \Theta_i, t_i)$ in the second fingerprint originally has an orientation of value Θ_i which is rotated to value α_i, the orientation value at the (x_i, y_i) point in first fingerprint.

Fig. 8. Combined template generation

2.7 Encrypting the Combined Fingerprint

The created combined fingerprint template is encrypted using blowfish cipher. Blowfish is a secret key block cipher which uses Feistel network and iterate a simple encryption function 16 times. The key is meant only to be known by the administrator of the fingerprint authentication system. The cipher of combined fingerprint is stored in database which is used later in authentication process. This cipher acts as a virtual biometric.

3 Enrollment and Authentication

The enrollment process of the proposed system is shown in Fig. 9

After fingerprint acquisition, they are pre-processed in order to enhance the fingerprints and to reduce noise. From the first fingerprint orientation is found and from the second fingerprint minutiae points are extracted in the reference area detected. A quality estimation module is added in this phase which calculates the trustiness value

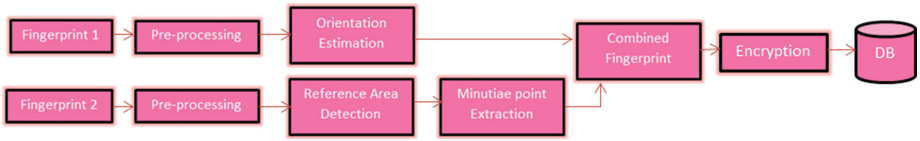

Fig. 9. Enrollment phase

of estimated orientations and minutiae points. If the difference between orientation value of a pixel and that of its neighbor's is more than 30, then the orientation is considered spurious. Similarly if the number of minutiae points in a particular area is more than normal then minutiae points detected at that area are considered as false points. If the total number of spurious orientation and minutia points so detected are less than 30 % of total area of fingerprint then enrollment is done. Using orientation values and minutia points, a combined template is generated which is encrypted and stored in database.

The authentication process has the same steps and is shown in Fig. 10. Two query fingerprints are needed. From the first fingerprint orientation is estimated and from the second fingerprint a reference area is detected and then within that area minutia points are detected. These are compared with the decrypted fingerprint templates stored in database. If matching occurs more than to a particular threshold value then the fingerprints are authenticated.

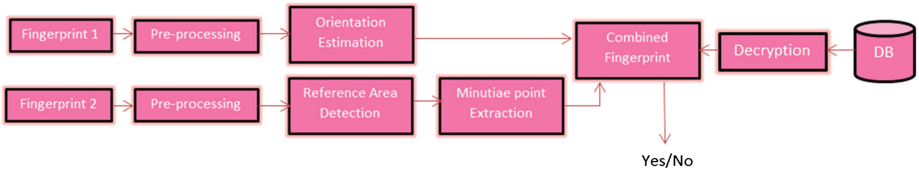

Fig. 10. Authentication phase

4 Simulation Results

The proposed system is simulated using Java 7. The Database used is MySql. The experiment is conducted on a collection of 50 different fingerprint patterns from which 2^{50} different combinations can be made. Both live scan and inked fingerprints are included in the collection.

During the enrollment process, after fingerprints acquisition, they are converted to bi-level images and are thinned. From the first fingerprint the orientation is estimated. The block size used for orientation estimation is block of 16 pixels. This can be varied according to the size of fingerprint image used. The reference area is detected around the singular point which is illustrated in Fig. 11

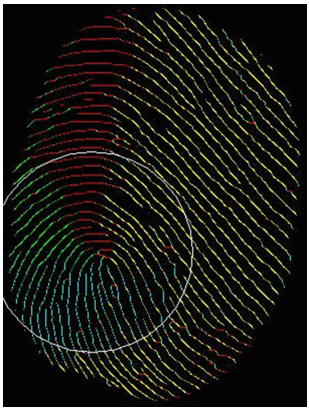

Fig. 11. Reference area detected

Here in the experiment the radius is taken as the one-third of the total width of fingerprint image pattern. Then the minutiae points are found out. But if the reference area concentrates over any edge area of the pattern then some unwanted endpoints will be detected by the system. An example is in Fig. 12.

To avoid this, a feature selection module is added to the system during the enrollment. There the system minutiae point extraction can be enhanced using manually selecting the minutiae points as shown in user interface shown in Fig. 13.

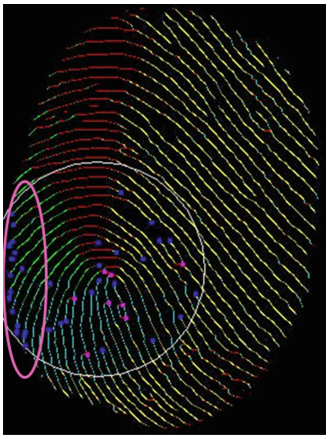

Fig. 12. Non minutiae points detected

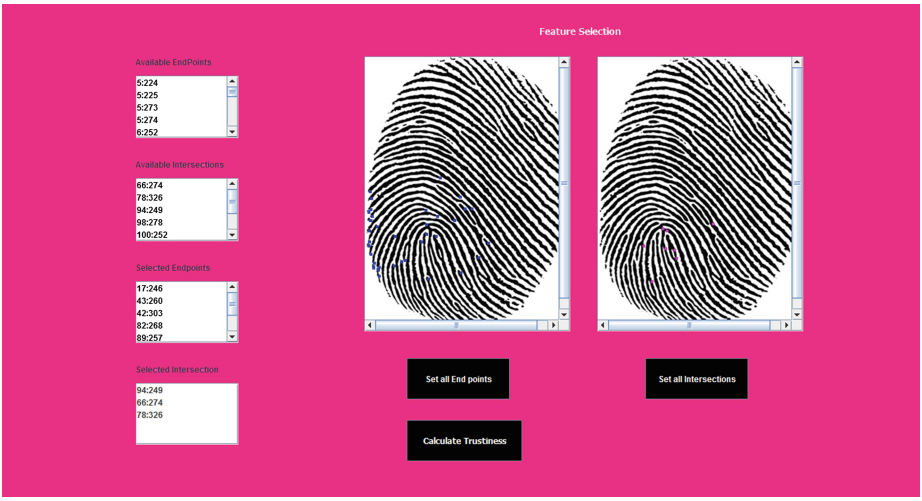

Fig. 13. User interface to manually select minutiae points

After selecting the genuine minutiae points a combined template is generated. The combined template is a java object of class fingerprint.

```
class fingerprint
{
Point referencepoint;
ArrayList minutiae;
ArrayList orientation;}
```

After creating the combined template it is encrypted using blowfish cipher. The cipher of combined cipher is stored in database which is used later in authentication process. This cipher acts as a virtual biometric.

During the authentication phase also two different fingerprints are required. The query fingerprints are pre-processed. Then from the first query fingerprint the orientation is estimated. From the second query fingerprint, a reference area is found out and within which the minutiae points are detected. The virtual biometrics stored in database are taken one by one and decrypted. The original templates thus obtained are compared with the query template.

The orientation values of query fingerprint are directly compared with the orientation values in the template. The minutiae points in query are compared with Euclidean distance between the points and the reference points to that in templates in database.

The percentage of total number of matched minutiae point and percentage of total number of orientation values are calculated. The average of these two is taken as the match score.

To find the threshold value of match score, a randomly selected fingerprint is combined with all other fingerprints to form 49 combined templates. The match score-frequency obtained during 49 genuine tests is shown in Fig. 14.

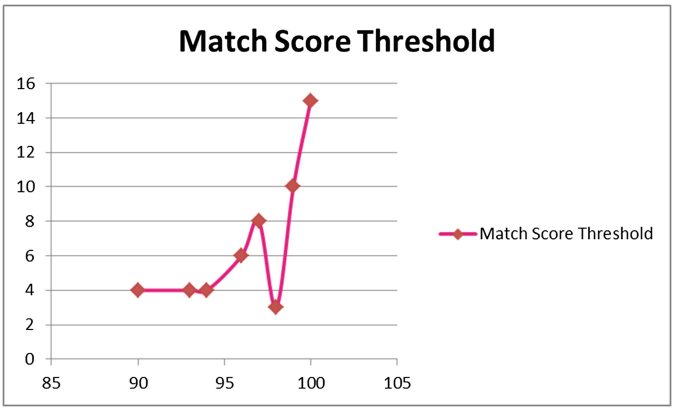

Fig. 14. Match score-frequency

Match score obtained during different genuine and imposter test are shown in Fig. 15.

The False Acceptance and False Rejection in a range of threshold, 90–100 is shown in Fig. 16.

Equal Error Rate (EER) is obtained at 95 %. The threshold value can be set to 95 % to minimize the false acceptance. During the experiments the threshold value is set to 90 % to optimize false acceptance rate and false rejection rate.

If matching occurs above 90 % it is authenticated. The matching score is set in accordance with the quality and size of image quality and size of image.

From the encrypted templates stored in database the intruder cannot recreate any fingerprint templates. If somehow an intruder obtains the encryption key and decrypts

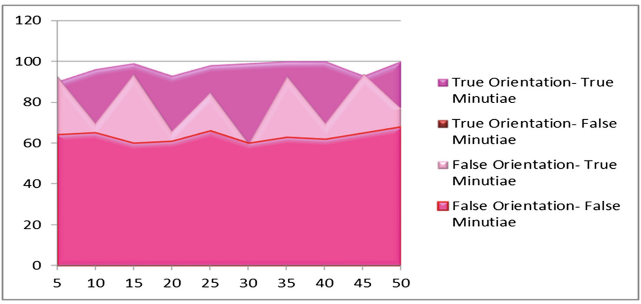

Fig. 15. Match score threshold

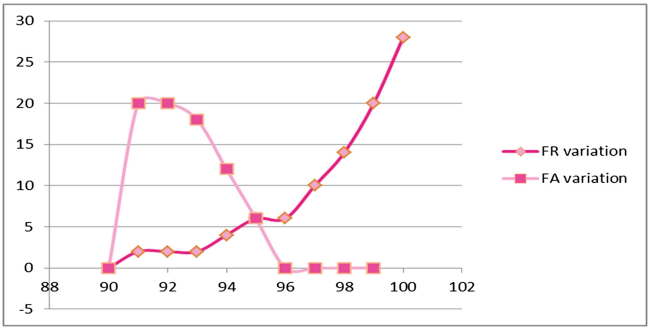

Fig. 16. FA and FR variations

the template, he/she can never recreate the original fingerprints since the template contains only orientation details or minutia details of either fingerprint.

5 Conclusion

To protect the privacy of fingerprints stored in database, a method is proposed which encrypts a mixed template formed of orientation of one fingerprint and minutiae points of other fingerprints. The system prevents intruders from recreating the original fingerprint from the virtual biometric stored. The system is able to provide low error rate also.

References

1. Lee, H.C., Gaensslen, R.E: Advances in Fingerprint Technology, 2nd edn., p. 426. CRC Press, New York (2001)
2. Nagar, B., Nandakumar, K., Jain, A.K: Securing Fingerprint Template: Fuzzy Vault with Minutiae Descriptors (2008)

3. Chen, H., Chen, H.: A novel algorithm of fingerprint encryption using minutiae-based transformation. Pattern Recognit. **32**(11), 305–309 (2011)
4. Teoh, B.J.A., Ngo, C.L.D., Goh, A.: Biohashing: two factor authentication featuring fingerprint data and tokenised random number. Pattern Recognit. **37**, 2245–2255 (2004)
5. Yanikoglu, B., Kholmatov, A.: Combining multiple biometrics to protect privacy. In: Proceedings ICPR- BCTP Workshop, Cambridge, U.K. (2004)
6. Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. **40**, 614–634 (2001)
7. Liu, L., Dai, T.: A reliable fingerprint orientation estimation algorithm. J. Inf. Sci. Eng. **27**, 353–368 (2011)
8. Łukasz, W.: A minutiae based matching algorithm in fingerprint recognition systems. J. Med. Inf. Tech. **13**, 1642–6037 (2009)
9. Li, S., Kot, A.C.: Attack using reconstructed fingerprint. In: Proceedings of the IEEE International Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil (2011)