FINGERPRINT COMBINATION SYSTEM BASED ON PROTECTION OF VIRTUAL IDENTITY

R. Malathy and K. Senthil Prasad
Department of Computer Science, SVS college of Engineering, Coimbatore, India
E-Mail: malathy.r98@gmail.com

ABSTRACT

A fingerprint authentication system for the privacy protection of the virtual identity is introduced. By extracting minutiae points from one fingerprint, orientation from other fingerprint and reference points from both the fingerprints, a new biometric authentication framework is proposed for identifying an individual. With the help of these three combined features a new virtual identity is generated. A combined biometric composed of two fingerprints is stored in the server database, and query fingerprints from both fingers are required in the verification process which reduces loss of privacy and misuse. The main intention of this paper focuses on the security and privacy of a virtual identity. In order to attain high security and privacy Liveness Detection technique is applied to distinguish legitimate and imposter user. To protect the virtual identity templates Delaunay quadrangle based fingerprint authentication system which deals with nonlinear distortion-induced local structural change. Finally the virtual identity is compressed and stored in database for further verification process.

Keywords: fingerprint, delaunay quadrangle, liveness detection, template protection, virtual identity.

1. INTRODUCTION

The Greek word “biometrics” is divided it into two roots: “bio” means life and “metrics” means to measure. Biometrics refers to technologies for measuring and analyzing a person's physiological or behavioral characteristics. These unique characteristics are used to verify and identify to individuals. Fingerprints are most commonly represented by a set of points, called minutiae. At present many Fingerprint Authentication Systems are based on minutiae matching. Minutiae are generally indicated as the terminations and bifurcations of the ridge lines in a fingerprint image. The two most important local ridge characteristics of minutiae are the ridge ending and the ridge bifurcation unique. Ridge ending is termed as the point where the ridge ends abruptly. Ridge bifurcation is termed as the point where a ridge forks or diverges into branch ridges. A fingerprint authentication system can be generally divided into two parts namely

- Enrollment
- Identification or Verification

The enrollment part is responsible for registering individuals into the biometric system. In this enrollment phase, the characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. Fingerprint verification is to verify the authenticity of one person by his fingerprint.

A novel system is proposed for providing privacy to the fingerprint biometric system by combining two different fingerprints into a new identity. The system captures two fingerprints from two different fingers which may be from same person or from different person while registering. The combined minutiae template is generated based on three features. In such a combined template, the minutiae positions are extracted from one fingerprint, while the orientation from other fingerprint and reference points from both the fingerprints. The template will be stored in a database for authentication which requires two query fingerprints during verification.

The organization of this paper is as follows. Section II introduces fingerprint combination privacy system. Section III explains the fake analysis. Section IV presents the template protection using Delaunay quadrangle. Section V describes the compression of virtual identity, followed by experimental results and the conclusions in the last section.

2. FINGERPRINT COMBINATION PRIVACY SYSTEM

Protecting the privacy of the fingerprint becomes an important issue with the widespread applications of fingerprint techniques in authentication systems. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint.

Figure-1 shows the privacy protection system. During Enrollment the system captures two different fingerprints from the same or different person say A and B respectively. Then three different features are extracted from two different fingers. Such as minutiae positions from fingerprint A and the orientation from fingerprint B then reference points [1] from both the fingerprints. The combined minutiae template is generated based on these features and coding strategies. Finally the combined minutiae template is stored in central server for further verification. During authentication, two query fingerprints A' and B' are required from the same two fingers. As done in enrollment stage, extract minutiae positions from A' and orientation from B'. The template stored in central server should match with the corresponding extracted information by using two-stage fingerprint matching. If the matching score is above the predefined threshold then the authentication will be successful.

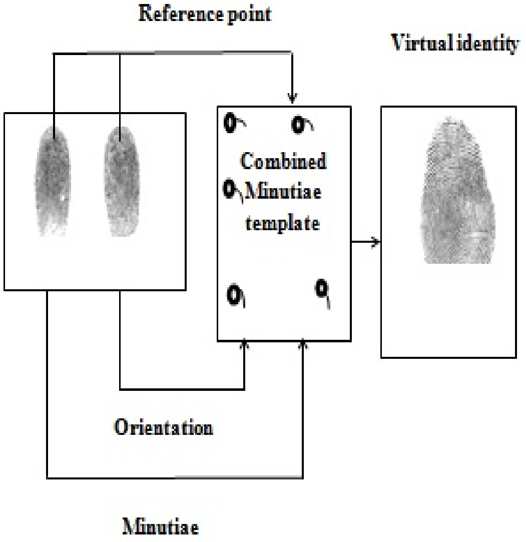

Figure-1. Fingerprint protection system.

In such a way the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen due to storing the combined minutiae template. Furthermore the attacker finds difficult to distinguish a combined minutiae template from the original minutiae templates. Then the combined minutiae template is converted to real-look alike combined fingerprint using fingerprint reconstruction approach. Thus, a new virtual identity is created for two different fingerprints that can be matched using minutiae-based fingerprint matching algorithms. This achieves a very low error rate with FRR=0.4% and FAR=0.1%

3. FAKE ANALYSIS

Each and every module of a biometric system should be protected against the attacks. It is possible to spoof a variety of fingerprint scanners with the help of some simple techniques with molds made from plastic, clay, silicone, Play-Doh, or gelatin materials which are shown in recent research. To protect against spoofing, methods of Liveness detection measure physiological signs of life from fingerprints ensuring only live fingers are captured during authentication. Examples of the images that can be found in this database are shown in Figure-2.

Liveness detection is an anti-spoofing method ensuring that only the biometric sample is from a live (authorized person) is submitted for enrollment, verification and identification. Liveness detection techniques use different physiological properties to distinguish between real and fake traits. It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal scenario. The quality between real and fake samples may include: degree of sharpness, luminance levels, color, local artifacts, and amount of information found in both real and fake images (entropy), structural distortions or natural appearance.

Fingerprint Liveness detection approaches have been broadly classified into two categories. Such as, hardware based and software based techniques. In software based technique, the fake fingerprints are detected based on the acquired sample with the standard sensor. Software-based methods can protect the system against the addition of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor. On the other hand hardware-based technique uses some special hardware device with the sensor to detect the particular properties of a living finger such as the blood pressure, the odor, the heartbeat or temperature.

The proposed approach is part of the software-based solutions as it distinguishes between images produced by real and fake fingers based only on the acquired sample, and not on other physiological measures captured by special hardware devices added to the sensor. Software-based methods can protect the system against the injection of reconstructed samples into the communication channel between the sensor and the feature extractor.

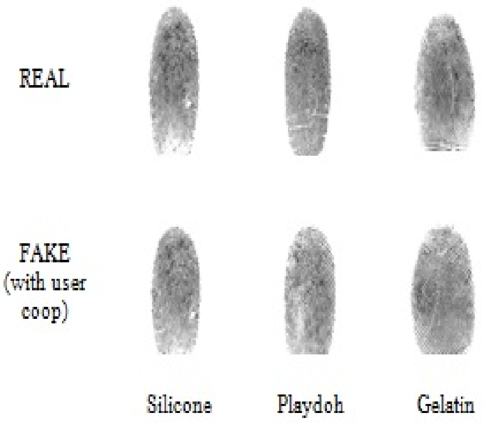

Figure-2. Examples of real and fake fingerprint images.

Liveness detection method presented in this research work provides a great importance in the biometric field as they help to prevent direct attacks thus enhancing the level of security offered to the user. Thus by using Liveness method the spoofing attack can be minimized. In this context, it is reasonable to assume that the image quality properties of real accesses and fraudulent attacks will be different. Following this “quality-difference” theory, in the present research work the potential of general image quality have been explored as an assessment of a protection tool against different biometric attacks (with special attention to spoofing). This interest has led biometric-based applications to big advances in the field of security-enhancing technologies.

4. THE TEMPLATE PROTECTION USING DELAUNAY QUADRANGLE

Fingerprint matching is not an easy task due to the fingerprint uncertainty caused by rotation, translation and nonlinear deformation at each fingerprint image acquisition. Template protection is an important issue which needs more attention during fingerprint acquisition due to nonlinear distortion. In general the templates from biometric systems are stored in a central database at the enrollment stage and compared with query fingerprint image at the verification stage.

A Delaunay quadrangle-based fingerprint authentication system [4] reduces the uncertainty and provides strong security protection to the template data. This technique is applied here in order to protect the newly generated virtual identity. Here the Delaunay quadrangle structure is occupied from the virtual identity and the unique topology code is generated for the quadrangle structure. This unique topology code provides to carry out the accurate local registration that absolute geometrical measurement usually fails when alteration is present and also enhances the security of template data.

The structural change is unavoidable by elastic finger skin always exists in fingerprint images which leads to the formation of nonlinear distortion. Due to this distortion there may exist a mismatch between enrolled fingerprint image and query fingerprint image. There arises a confusion to select the starting point in query image. To avoid this confusion a unique topology code is generated. Each angle in the quadrangle is quantized into an integer or binary number. Consider the Figure-3 for the generation of topology code and to avoid the mismatch of starting point.

Here the smallest angle and second smallest angle is quantized to the same integer. Whenever there is a distortion the structure of a quadrangle may change.

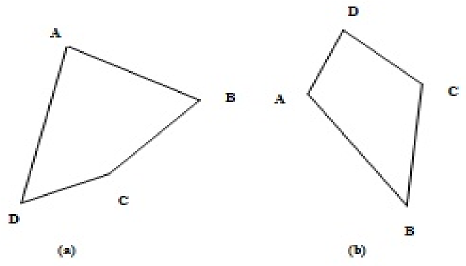

Figure-3. Corresponding delaunay quadrangles Q(ABCD) and Q(A_B_C_D_)in (a) the template fingerprint image and (b) the query fingerprint image.

The angles of Q (ABCD) are quantized into 2,2,4,5 respectively in clock-wise direction. Different code strings 2-2-4-5, 2-4-5-2, 4-5-2-2 and 5-2-2-4are generated. The same code strings are generated from a query combined image. The topology code is generated using the equation,

$$\mathbf{TC=P_1\times\Gamma^3 +P_2\times\Gamma^2+P_3\times\Gamma^1+P_4\times\Gamma^0}$$

Where $\{P_i\}$ = quantized angle values of the Delaunay Quadrangle and $\Gamma^{\mathbf{i}}$ =max (P_1, P2, P_3 ,P_4) +1 .Using this equation four different code strings are generated and choose the smallest value to be the descriptor of the Delaunay quadrangle under consideration. The four code strings are 533, 608, 1058 and 1168 respectively. Consequently, the smallest value 533, which corresponds to the starting point of *A*, is chosen as the topology code of *Q(ABCD)*. Similarly, the topology code of query image is also calculated to be 533, which is corresponding to the starting point of template image. The starting points of template and query image are just the correct corresponding points that are to be found. By this means, the templates of a virtual identity can be protected.

5. THE COMPRESSION OF VIRTUAL IDENTITY

Fingerprint recognition is very popular for personal identification due to the universality, uniqueness, collectability and invariance. Large volumes of fingerprint are collected and stored in a wide range of applications, including access control and forensics. The given new fingerprint which has the same size with the training patches is sliced into square patches. The size of the patches has a direct impact on the compression efficiency. By compressing the virtual identity, the feature minutia should be protected. The amount of storage can be reduced by means of storing a compressed image of a virtual identity in a database.

6. EXPERIMENTAL RESULTS

The online database FVC2002 DB2_A is used throughout this project. The virtual identity generated from combined features must be highly protected. For this purpose Delaunay quadrangle structure is considered and the minutiae positions are extracted from them. Those points are stored in database for further purpose. And also the considered quadrangle structure is finally compressed and stored in server. The performance of this system is calculated based on two parameters such that FRR and FAR. Thus system produces low error rate such as FRR=0.4% and FAR=0.1%. Figure-4 explains the proposed system. The proposed system combines the work in [4], [2] for the protection of virtual identity.

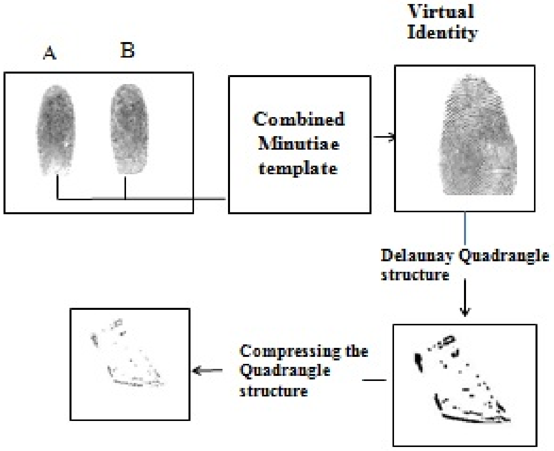
A
B
Virtual Identity
Combined Minutiae template
Delaunay Quadrangle structure
Compressing the Quadrangle structure

Figure-4. Fingerprint combination System based on template protection and compression.

7. CONCLUSIONS

In this paper, the features of two fingerprints are combined to generate a new virtual identity with the help of fingerprint reconstruction approach. The attacker finds difficult to separate the two fingerprint features. The proposed work mainly concentrated to protect the virtual identity by using Delaunay quadrangle by generating topology code. Finally the reconstructed virtual identity is compressed and stored in database for further use. Thus experimental results show that better virtual identity is generated and a very low error rate can be achieved. High privacy and security is achieved with this system. The analysis shows that it is not easy for the intruder to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

REFERENCES

[1] Sheng Li and Alex C. Kot. 2013. “Fingerprint Combination for Privacy Protection,” IEEE transactions on information forensics and security. Vol. 8, No. 2, February.

[2] “Fingerprint Compression Based on Sparse Representation”, Guangqi Shao, Yanping Wu, Yong A, Xiao Liu, and Tiande Guo, IEEE transactions on image processing. Vol. 23, No. 2, February 2014.

[3] “Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition”, Javier Galbally, Sébastien Marcel, and Julian Fierrez K .Elissa, IEEE transactions on image processing. Vol. 23, No. 2, February 2014.

[4] “A Delaunay Quadrangle-Based Fingerprint Authentication System With Template Protection Using Topology Code for Local Registration and Security Enhancement”, Wencheng Yang, Jiankun Hu, and Song Wang, IEEE transactions on information forensics and security. Vol. 9, No. 7, July 2014.

[5] S. Li and A. C. Kot. 2011. “Privacy protection of fingerprint database,” IEEE Signal Process. Lett. Vol. 18, no. 2, pp. 115–118, February.

[6] A. Ross and A. Othman. 2011. “Mixing fingerprints for template security and privacy,” in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, August 29–September 2.

[7] A. Othman and A. Ross. 2011. “Mixing fingerprints for generating virtual identities,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security(WIFS), Foz do Iguacu, Brazil, November 29–December 2.

[8] “Fake Fingerprint Detection Methods”, Tanisha Aggarwal ,Dr.Chander Kant Verma (ICFTEM-2014) May 2014 pp. 61-69 (ISSN 0973-4414).