Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 03, pp. 28284-28288, March, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

PRESERVATION OF BIOMETRIC PRIVACY BY COMBINED MINUTIAE TEMPLATE

[1]Mary Linda and [2,*]Kalaiprasath, R.

[1]Assistant Professor, Aksheyaa College of Engineering, Chennai, India
[2]Research Scholar, Bharath University, Assistant Professor, Aksheyaa College of Engineering, Chennai, India

ARTICLE INFO

Article History:
Received 08th December, 2015
Received in revised form
24th January, 2016
Accepted 26th February, 2016
Published online 31st March, 2016

Key words:

Minutiae,
Extraction,
Orientation,
Reference Point.

ABSTRACT

In current trends protecting the privacy of the Fingerprint is an important one, here a novel system propose protecting fingerprint by combining two different fingerprints. It will create a new identity. In the enrollment stage, fingerprints will be captured from two different fingers. Minutiae positions are extracted from one fingerprint. The orientation, (it indicates the flow of ridges and valleys) from other fingerprint, and the reference points are calculated from both the two fingerprints. Extracted combined minutiae templates are stored into database. In the authentication, two query fingerprints are needed which are all used in enrollment. For matching purpose Two-stage fingerprint matching process is used. Even when the database is stolen, the complete feature of single fingerprint will not be used for authentication, because the combined minutiae template is stored. Single fingerprint is not sufficient for the authentication. Attackers can't easily identify such a new identity. By using the fingerprint reconstruction algorithm, real-look alike combined fingerprint are generated.

Citation: Mary Linda and Kalaiprasath, R. 2016. "Preservation of biometric privacy by combined minutiae template", *International Journal of Current Research*, 8, (03), 28284-28288.

INTRODUCTION

Nowadays, fingerprints are most widely used in so many applications. So protecting the fingerprint privacy is becomes an important one. Therefore, in recent years more techniques are developed for protecting the privacy of the fingerprint in efficient manner. Most of the existing technique creates some inconvenience for protecting the fingerprint privacy. Keys are used for the security purpose. Accuracy is mainly depends on the key. When the keys and stored template are stolen it's to be vulnerable. Theo *et al.* (2004) propose a biohashing approach this technique mainly depends on key. When the key is stolen by the attacker it is to be vulnerable. Some few techniques are used for protecting fingerprint privacy without using a key. Ross and Othman *et al.* (2011) propose a visual cryptographic technique for protecting biometric privacy. The fingerprint image is decomposed into two noises - like images by using visual cryptography scheme. Then the decomposed images are stored in two separate databases. During the Authentication, the system requires two query fingerprints image which are used in enrollment. The two fingerprint images are overlaid to create a temporary fingerprint image for matching. If it is not matched, user can't enter in to the system.

Corresponding author: Kalaiprasath, R.
Research Scholar, Bharath University, Assistant Professor, Aksheyaa College of Engineering, Chennai, India.

The main drawback of this system is, it requires two separate databases to work together, which creates inconvenience for using visual cryptographic. To increase the efficiency and security of fingerprint more techniques are introduced. By combining two different fingerprints into a new identity .It provide more security than using of single fingerprint. Combining two different fingerprints into a new single identity is done at two levels either image level or feature level. In (Yanikoglu and Kholmatov, 2004) the concept of combining two different fingerprints at feature level is introduced. Here the minutiae positions of both two different fingerprints are extracted. Minutiae points are the detailed pattern of the fingerprint. It will provide more security than the image level. But this approach also has some drawbacks that are attacker can easily identify a new identity.

Because it contains many more minutiae points than the original fingerprint. In (Othman and Ross, 2011) combining two different fingerprints at the image level is introduced. Mixing fingerprint concepts are introduced to protect the fingerprint privacy by combining two different fingerprints in image level. To mix two different fingerprints, each fingerprint is decomposed into two different fingerprints (Continuous, spiral components). Helmholtz techniques are used for decomposition.

After some alignment continuous component of one fingerprint is combined with spiral component of other fingerprint it will create a new identity which is denoted as a mixed fingerprint. It has the advantage of; hackers can't easily distinguish the original fingerprint from mixed fingerprint. The main drawback of this paper is, when the two different fingerprints are randomly chosen it will create high error rate. So selection of two fingerprints is considered to be an important one. When the two different fingerprints are randomly chosen their experimental results shows that the EER of matching two mixed fingerprints is about 15%.Then the EER of matching two mixed fingerprint is reduced to 4% when the two different fingerprints are carefully chosen.

Compared with existing techniques, this paper has more advantages. Some of the advantages over existing fingerprint combination techniques are listed below:

- When compared with the existing technique, our proposed system is able to create very low error rate.
- Compared with the feature level based technique (Yanikoglu and Kholmatov, 2004), our system able to create a new identity which is difficult for the attacker to distinguish original fingerprint from combined minutiae templates.
- Compared with the image level technique (Othman and Ross, 2011), our system able to create a new virtual identity. Even when the two different fingerprints are randomly chosen.

The rest of the paper is organized as follows: Section 2 briefly summarizes the previous literature and highlights the novelty of the proposed technique. Section 3 explains how to generate combined fingerprint for two different fingerprints. Section 4 presents the experimental results. Section 5 shows our conclusions.

The Proposed System

During the enrollment stage, system captures two different fingerprints from two different fingers, were fingerprints are called A and B respectively from fingers A and B. By using some existing technique of minutiae extraction (http://www.neurotechnology.com), minutiae positions are extracted from one fingerprint that is fingerprint A and orientation from other fingerprint B using some existing techniques (Hong et al., 1998).Then the reference points are detected from both fingerprints by using our coding schemes. Eventually the combined minutiae template, is stored into a database. In the authentication stage, system requires two query fingerprints which are used in enrollment phase that is fingerprint A' and B' from finger A,B respectively.

To the same what we have done at the enrollment, we extract the minutiae positions from fingerprint A' and calculate orientation from fingerprint B' and reference points are discover from both query fingerprints. Finally the Two-stage fingerprint matching algorithm used for matching the extracted information against stored template. If query fingerprints are matched with stored template, authentication will be successful. User can enter into the system. Fig. 1 shows our proposed our proposed fingerprint privacy system.

Reference Points Detection

For the alignment of two different fingerprints certain reference points are needed. In (Hong *et al*., 1998) complex filters, applied to find the reference points. Some steps are needed to calculate reference points for the appropriate fingerprint. Reference points are calculates as follows:

- By using the orientation estimation algorithm proposed in (Hong *et al*., 1998), orientation *O* estimated from fingerprint. Obtain the orientation *Z* in complex domain.
- Calculate the certainty map (C_{ref}) of reference points proposed in (Hong *et al*., 1998).
- Determine the improved certainty map (C'_{ref}) proposed in (Nilsson and Bigun, 2003).
- Determine the place of a reference point satisfying two main standard :(i) the boundary of C'_{ref} of the point is a local maximum,(ii)the local maximum should be over a fixed threshold *T*.
- Repeat step (4) until all reference points are detected.
- If no reference points are detected at the steps 4 and 5, determine a reference point for the whorl fingerprint image with maximum certainty value.

Combined Minutiae Template Generation

Combined minutiae templates are generated by determining the position of minutiae and minutiae direction assignment. For a given set of N minutiae points P_A , and orientation of O_B of fingerprint B then reference points of fingerprints A and B are generated. By using minutiae position alignment and minutiae direction assignment, a combined minutiae template M_C is generated.

Minutiae Position Alignment

Which reference points have the maximum certainty value that reference points are selected as the primary reference point. Therefore, we have two maximum certainty value which is denoted as R_a and R_b for fingerprints A and B respectively. Let's denote R_a is located at position $r_a = (r_{xa}, r_{ya})$ with the angle β_a ,and R_b is located at position $r_b = (r_{xb}, r_{yb})$ with the angle β_b. The alignment is performed by rotating and translating each minutiae point P_{ia} to P_{ic} . $P_{ia} = (x_{ia}, y_{ia})$ and $P_{ic} = (x_{ic}, y_{ic})$.

$$(P_C)^T = H.(P_{ia} - r_a)^T + (r_b)^T \quad (1)$$

T is the transpose operator and H is the rotation matrix where

$$H = \begin{pmatrix} \cos(\beta_b - \beta_a), \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a), \cos(\beta_b - \beta_a) \end{pmatrix} \quad (2)$$

Minutiae Direction Assignment

Aligned position of P_{ic} is assigned with a direction as follows:

$$\theta_{ic} = O_B((x_{ic}, y_{ic}) + \rho_i \pi \quad (3)$$

Where ρ_i is an integer that is either 0 or 1. Then the orientation of O_B is from 0 to π. The rage of $\theta_{ic\ is}$ from 0 to 2π.

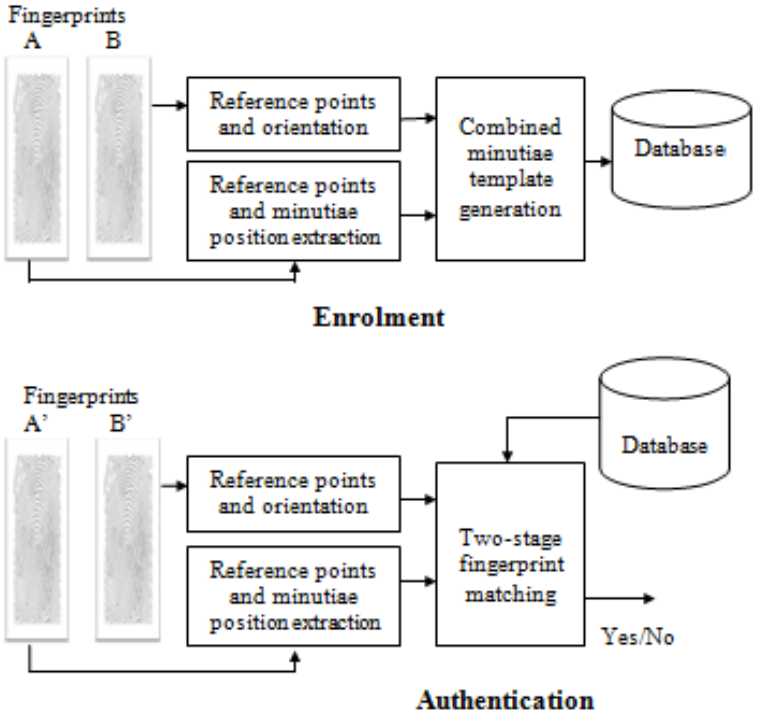

Fig. 1. Proposed fingerprint privacy protection system

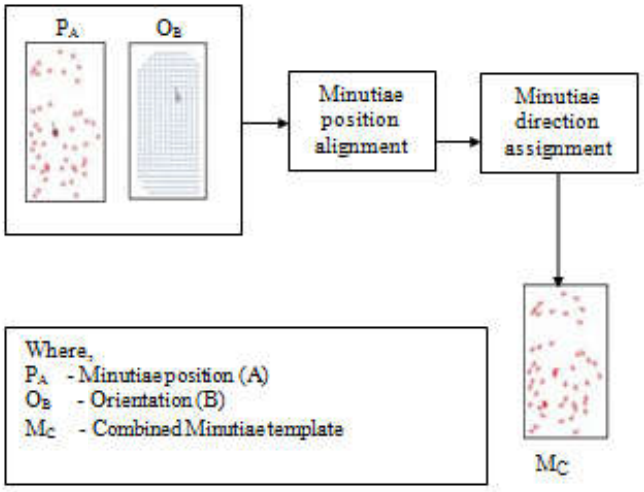

Fig.2. Combined Minutiae Template Generation

Two-Stage Fingerprint Matching

After calculating combined minutiae template generation, Two-stage fingerprint scheme is proposed. During the authentication stage two-stage fingerprint matching is used to match the query fingerprints against stored template. Minutiae positions of fingerprint A' and orientation of fingerprint B' and the reference points for the both A' and B' are matched against the Mc. Fig. 3 shows our proposed Two-Stage fingerprint matching.

Query Minutiae Determination

During the fingerprint matching query minutiae determination is a very important one. Then the local feature for a minutiae points in M_C , are calculated by using local feature extraction technique proposed in (8).

Then calculate the distance between two minutiae points. Then calculating the direction between two minutiae points. Repeat steps until all possible reference points of pairs to be selected. Which has the maximum difference from M_C will be considered as the query minutiae M_Q.

Matching Score Calculation

To calculate the Matching score between M_C and M_Q using the existing technique proposed in (9).In (9), minutiae matching algorithm was proposed.

Combined Fingerprint Generation

In combined minutiae template generation, minutiae position and direction assessments are calculated.

Sometimes minutiae position and direction assessment has same topology of the original fingerprint. After calculating combined minutiae template generation and two-stage fingerprint matching, combined fingerprint generation to be considered. Some existing works shows that, it is possible to reconstruct the original fingerprint. Some of these reconstruction techniques can only generate a partial fingerprint. By using minutiae based scheme, we can generate a full fingerprint. In (Feng and Jain, 2011), the full fingerprint will be generated by using minutiae based scheme. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image. Fig. 4 shows our process to generate a combined fingerprint for two different fingerprints. Then take two different fingerprints as an input, we first generate a combined minutiae template by using our combined minutiae template generation algorithm. Finally the combined fingerprint will be reconstructed by using some fingerprint reconstruction approaches from combined minutiae template.

We choose first 2 impressions for each finger totally 200 fingerprints of 100 different fingers. We choose Veri Finger 6.3 (http://www.neurotechnology.com) algorithm for feature extraction and matching. We choose 50 different pairs of fingerprint from the above said database. We conduct the experiment based on reference point detection, combined minutiae template generation separately. Finally we evaluate the performance of our proposed system. Among 200 fingerprint based on our experiment which fingerprint has 5 reference points has full accuracy and efficiency compare to the other fingerprints.

From our experiment the average Euclidian distance between the marked topmost loop and the nearest reference point is 5.65 pixels. In the verification stage a rotation function is needed to accurately place the extracted feature. We adopt -30 degree to 30 degree angle for rotation based on singular points. For experiment on combined minutiae template generation we conduct two different test cases named as Type-I and Type-II.

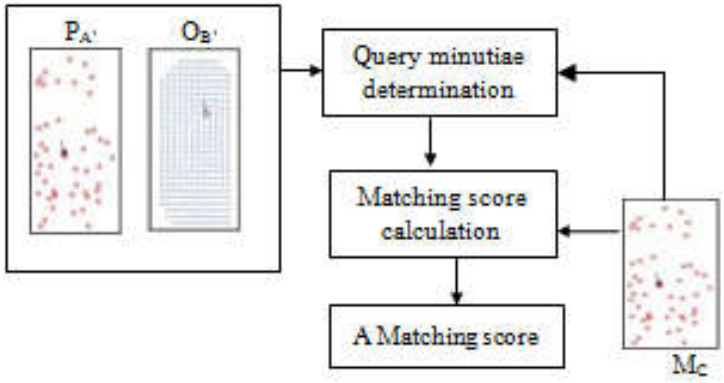

Fig. 3. Two-stage fingerprint matching process

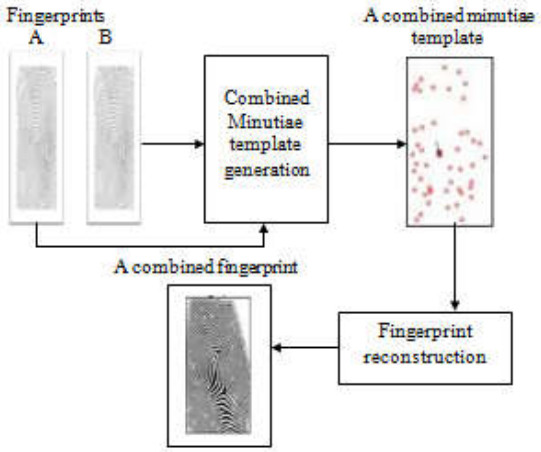

Fig. 4. Generating a combined fingerprint for two different fingerprint

In existing techniques, partial fingerprint will be generated. But our proposed system will produce full fingerprint image.

Experimental Result

We conduct the experiment on FVC2002 DB2_A database. It contains 800 fingerprints from 100 different fingers.

Based upon the test case our experiment provides good result compare to previous techniques. Type-I test takes the first impressions of each finger pair are used to produce only one combined minutiae template for enrollment. To compute the False Rejection Rate (FRR), the second impressions of a finger pair are matched against the corresponding enrolled template, producing 50 genuine tests.

To compute the False Acceptance Rate (FAR), the first impressions of a finger pair are matched against the other 49 enrolled 50 * 49 = 2450 templates, producing imposter tests. Whereas the Type-II test conducted as taking the first impressions of each finger pair are used to produce two combined minutiae templates for enrollment. We also analysis the security of proposed method by two type of attack named as Type A and Type B. The first type of attack is conducted by taking combined minutiae template for attack the system which stores the corresponding fingerprint A (mainly provides the minutiae positions). The second type of attack is conducted by taking combined minutiae template for attack the system which stores the corresponding fingerprint (mainly provides the minutiae directions).If the attacker knows that a stolen template has been protected by using our technique, he would try to launch the aforementioned attacks based on the minutiae positions only, i.e. he would try to modify the minutiae matcher such that the minutiae directions are ignored during the matching. We implement a minutiae matcher based on the work proposed in (8), where we only use the minutiae positions for the matching. By using this matcher, the successful rates of Attack Type A and Attack Type B are 86.0% and 0.3% at FAR = 0.1%, respectively.

Conclusion

In this paper, we introduce a novel system for fingerprint privacy protection by combining two different fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template.

The experimental results show that our system achieves a very low error rate with FRR = 0.4% at FAR = 0.1%. It is also difficult for an attacker to break other traditional systems by using the combined minutiae templates. Compared with the state-of-art technique, our technique can generate a better new virtual identity when the two different fingerprints are randomly chosen. The analysis shows that it is not easy for the attacker to recover the original minutiae templates from a combined minutiae template or a combined fingerprint.

REFERENCES

Feng, J. and Jain, A. K. 2011. "Fingerprint reconstruction: From minutiae to phase," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 33, no. 2, pp. 209–223, Feb.

Hong, L., Wan, Y. F. and Jain, A. 1998. "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal.Mach. Intell.*, vol. 20, no. 8, pp. 777–789, Aug.

Jiang, X. andYau, W. 2000. "Fingerprint minutie matching based on the local and global structures," in *Proc. 15th Int. Conf. Pattern Recognition*, vol. 2, pp. 1038–1041.

Nilsson, K. and Bigun, J. 2003. "Localization of corresponding points in fingerprints by complex filtering," Pattern Recognition. Lett., vol. 24, no. 13, pp. 2135–2144.

Nilsson, K. and Bigun, J. 2003. "Localization of corresponding points in fingerprints by complex filtering," *Pattern Recognit. Lett.*, vol. 24, no. 13,pp. 2135–2144.

Othman, A. and Ross, A. 2011. "Mixing fingerprints for generating virtual identities," in Proc. IEEE Int. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2.

Ross, A. and Othman, A. 2011. "Visual cryptography for biometric privacy,"*IEEE Trans. Inf. Forensic Security* vol. 6, no. 1, pp. 7 0–81, Mar.

Teoh, B. J. A., Ngo, C. L. D. and Goh, A. 2004. "Biohashing: Two factor authentication featuring fingerprint data and tokenized random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255.

VeriFinger 6.3. Available: http://www.neurotechnology.com

Yanikoglu, B. and Kholmatov, A. 2004. "Combining Multiple biometrics to protect privacy," in *Proc.ICPR-BCTP workshop,* Cambridge,U.K. Aug.

****