COMBINATION OF FINGERPRINT FOR PRIVACY PROTECTION

MISS RATHOD LEENA ANIL
Department of Electronics and Telecommunication, V.V.P Institute of Engg and Technology, Solapur, Solapur University, Solapur, India, leenarathod28@gmail.com

PROF. MANTRI D. B.
Department of Electronics and Telecommunication, V.V.P Institute of Engg and Technology, Solapur, Solapur University, Solapur, India, dbmantri@yahoo.co.in

ABSTRACT:

Biometric refers to the authentication technique which depends on the measurement and statistical analysis of people's physical and behavioral characteristics. Among all the biometric technique fingerprint identification is consider as most reliable technique as every individual has unique fingerprint. But as fingerprint technique is used in many authentication systems so protecting it becomes an important issue. Here a system is shown to protect the privacy of fingerprint by combining two different fingerprints into a new virtual identity. In enrollment phase, extract the minutiae position from one fingerprint, orientation from another fingerprint and reference points from both fingerprints, using this extracted information from a combined minutiae template and store it in database. In authentication phase use two query fingerprints, extract the minutiae position from one fingerprint, orientation from another fingerprint and reference point from both the query fingerprint. Perform a two stage fingerprint matching process to match the two query fingerprints with the enrolled fingerprint. With the existing fingerprint reconstruction technique a new virtual identity is created.

KEYWORDS: Fingerprint combination, minutiae, orientation, reference points, protection.

I. INTRODUCTION

Biometric techniques are used in many authentication systems as it is the best way to identify a person and also it helps to protect the information which can be accessed by only the authenticated person. There are many biometric identification techniques such as fingerprint scanning, iris, face recognition, palm, and voice analysis. Among all this techniques fingerprint identification is considered as most reliable technique as it is easy and every individual is having a unique fingerprint. The uniqueness of the fingerprint depends upon it structure. Fingerprint has two structure i.e global structure and local structure. The global structure means the ridges and valleys which visible to eyes. The local structure is the minutiae points (i.e ridges ending and bifurcation).

As fingerprints are used in many authentication systems and protecting the privacy of these fingerprints become important. Firstly the encryption and decryption methods were used to protect the privacy of fingerprints. But the problem with this method is that, decryption is required before the authentication which may expose the fingerprint to the attacker. Most of the existing techniques make use of keys but it is inconvenience. This may be vulnerable when the key and protected fingerprint both gets stolen. There are very few techniques which are able to protect the fingerprint without making the use of key. Combining two fingerprints into a new virtual identity is one of those techniques. Here the fingerprints are combined either in feature level or image level. In feature level technique the two fingerprints are captured and the minutiae position of both the fingerprints is extracted and combined template is formed and stored in database. However, it is easy for the attacker to identity as there are too many minutiae points than the original fingerprint. In image level technique the fingerprint image is decomposed into, continues component and spiral component using FM-AM model. After some alignment, continues component and spiral component both are combined and a new virtual identity is formed.

In this paper system for protecting the privacy of fingerprint by combining two fingerprints into a new virtual identity is shown. In the enrollment process, the system captures two different fingerprints from two different fingers. Extract the minutiae position from one fingerprint, orientation from another fingerprint and reference points from both the fingerprints. Using this information a combined minutiae template is generated and stored in database. In the authentication process, the system captures two query fingerprints from the same fingers used in enrollment process. Extract the minutiae position from one fingerprint, orientation from another fingerprint and reference points from both the query fingerprints. Then perform a two stage fingerprint matching process to match the query fingerprints with the enrolled fingerprints. By using the combined minutiae template a new real look alike fingerprint is created.

II. METHODLOGY:

There are two phases in the proposed system. The enrollment phase and the authentication phase.

2.1 ENROLLMENT PHASE:

In the enrollment phase we are going to capture two fingerprints say fingerprint A and fingerprint B from two different fingers say finger A and finger B. Fig. 1 below shows the enrollment phase.

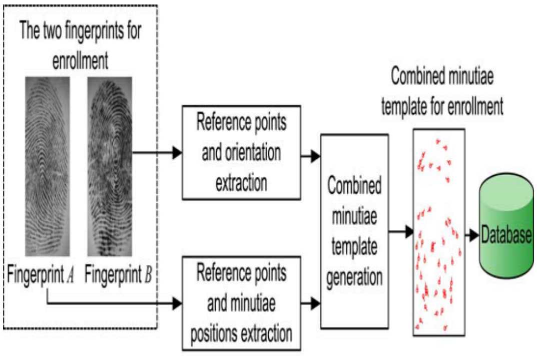

The two fingerprints for enrollment
Fingerprint A
Fingerprint B
Reference points and orientation extraction
Reference points and minutiae positions extraction
Combined minutiae template generation
Combined minutiae template for enrollment
Database

Fig 1 Enrollment phase

After capturing the two fingerprints extract the minutiae position from fingerprint A, orientation from fingerprint B and reference points from both the fingerprints. Using this extracted information generate a combined minutiae template and store the generated template in database.

Steps for reference point detection:

1. Evaluate the orientation O using the orientation estimation algorithm. Get orientation O in complex domain

$$Z = \cos(2O) + j\sin(2O)$$

2. Calculate the certainty map of reference point

$$Cref = Z * \overline{Tref}$$

where "*" is the convolution operator and $\overline{Tref}$ is the conjugate of

$$T_{ref} = (x + iy).\frac{1}{2\pi\sigma^2}.\exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right)$$

which is the kernel of reference point detection.

3) Calculate the reference point using following equation:

$$C'_{ref} = \begin{cases} C_{ref}.\sin\left(Arg\left(C_{ref}\right)\right) & if\ Arg\left(C_{ref}\right) > 0 \\ 0 & otherwise \end{cases}$$

4) Locate reference point satisfying the two criterions:

(i)The amplitude of $C^{|}_{ref}$ of the point is local maximum.

(ii)The local maximum should be over a fixed threshold T.

5) Repeat step 4) until all reference points is located.

6) If no reference points are detected locate a reference point with maximum certainty value in whole fingerprint image.

Combined Minutiae Template Generation:

The combined minutiae template is generated by applying minutiae position alignment and minutiae direction assignment. The block diagram of combined minutiae template is shown in below fig. 2.

A. Minutiae position alignment

Among all the reference points of the fingerprint for the enrollment, we define a reference point with the maximum certainty value as the primary reference point. Therefore we have two primary reference points R_a and R_b for fingerprints A and B, respectively. Let us assume that R_a is located with the angle β_a and R_b is located with the angle β_b. The alignment is performed by translating and rotating each minutiae point with the rotation matrix

$$H = \begin{bmatrix} \cos(\beta_b - \beta_a) & \sin(\beta_b - \beta_a) \\ -\sin(\beta_b - \beta_a) & \cos(\beta_b - \beta_a) \end{bmatrix}$$

As such R_a and R_b are overlapped both in the position and the angle after the minutiae position alignment.

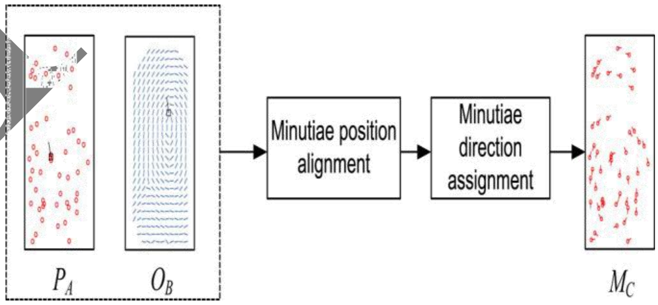


Fig. 2 Combined Minutiae Template Generation

B. MINUTIAE DIRECTION ASSIGNMENT:

Here each aligned minutiae position is assigned with the direction θ_{ic} as follows:

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

where ρ_i is an integer that is either 0 or 1. The range of O_B (x_{ic},y_{ic}) is from 0 to π. Therefore the range of θ_{ic} will be from 0 to 2π, which is the same as that of the minutiae direction from an original fingerprint. Once all the aligned minutiae position are assigned with direction a combined minutiae template is created for enrollment.

2.2 Authentication Phase

In the authentication phase we are going to capture two query fingerprints say fingerprint $A^|$ and fingerprint $B^|$ from the same fingers say finger A and finger B. Extract the minutiae position from fingerprint

A| , orientation from fingerprint B| and reference points from both the fingerprints. Then perform a two stage fingerprint matching process to match the two query fingerprint with the stored template. The authentication phase is shown in below fig. 3

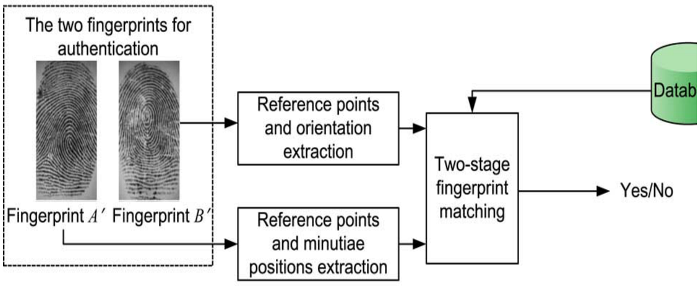

The two fingerprints for authentication
Fingerprint A'
Fingerprint B'
Reference points and orientation extraction
Reference points and minutiae positions extraction
Datab
Two-stage fingerprint matching
Yes/No

Fig 3 Authentication phase

Two stage fingerprint matching process

In the two stage fingerprint matching process we have the minutiae position of fingerprint A|, orientation of fingerprint B| and reference points of both the fingerprints. In order to match the query fingerprint we are going to perform two operation i.e query minutiae determination and matching score calculation. The two stage fingerprint matching process in shown in below fig. 4

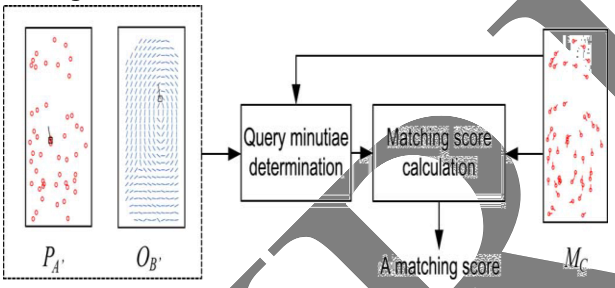


Fig 3 Two stage fingerprint matching process

A. QUERY MINUTIAE DETERMINATION:

The query minutiae determination is the very important step while fingerprint matching. The local features are extracted from the stored template M_C and the minutiae points are detected. Then select a pair of reference point from the query fingerprint A| and fingerprint B|. Then generate a combined minutiae template say M_C| for testing purpose from the minutiae position extracted from query fingerprint A| and orientation from fingerprint B|. Calculate the difference between the local features extracted from the template M_C and M_C|. Repeat the steps until all possible pairs of reference points are selected and processed. The one which has the minimum difference from M_C will be considered as the query minutiae M_Q.

B. Matching Score Calculation We directly calculates the matching score between M_Q and M_C using the existing minutiae algorithm. If the matching score is over the pre-defined threshold then the authentication will be successful.

III. COMBINED FINGERPRINT GENERATION:

In combined minutiae template the minutiae position and direction are extracted separately from two different fingerprints. This minutiae position and direction are same as that of the original fingerprints. Therefore the combined minutiae template has the similar properties to those of the original fingerprint. Hence to construct a new virtual identity and create a new look alike fingerprint we are going to use this combined minutiae template.

We are going to use the following steps to create a new fingerprint.

1. Estimate the orientation O from the combined minutiae template using the orientation reconstruction algorithm.

2. Generate a binary ridge pattern from the orientation O.

3. Estimate the phase image from the binary ridges pattern using fingerprint FM-AM model.

4. Reconstruct the continuous phase image by removing the spirals from the phase image.

5. Combine the continuous phase image and spiral phase image, reconstructing the phase image.

6. Refine the phase image by removing the spurious minutiae points and a real look alike fingerprint is created.

IV. EXPERIMENTAL RESULTS:

The experiment is conducted on the two fingerprints stored in our system which contains 10 fingerprints from 5 fingers.

1. Capture any pair of fingerprints stored in our system.

Fingerprint A

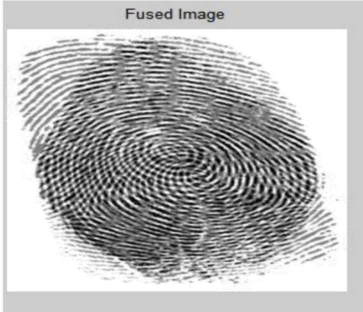
Fingerprint B

2. After capturing the fingerprint we have to enroll the fingerprints with the name of the person to whom the fingerprint belongs.

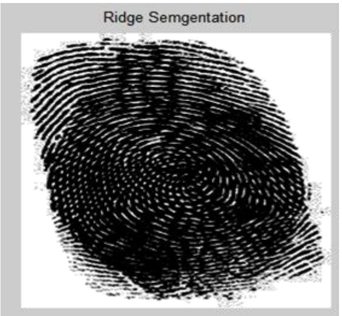
3. After enrolling the fingerprints they are combined, data test are created and stored in database.

4. In authentication process we are going to capture the same fingerprints used in the enrollment.

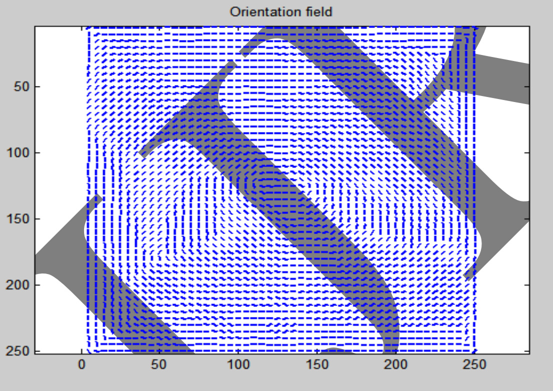
5. After capturing the two fingerprints are combined and a fused image is formed



6. The ridge segmentation of the fused image takes place



7. The orientation field is formed of this two combined fingerprint



8. Then the data test are created and matched with the existing data test.

9. If the data test matches with the existing account holder data test then the authenticated account holder name is displayed.

The performance of the system is based on the FAR and FRR of the fingerprints.

FAR – False Acceptance Rate where the system incorrectly accepts an unauthorized user.

FRR – False Rejection Rate where the system incorrectly rejects a authorized user.

As our system has very low FAR and FRR even when the fingerprints are randomly chosen which tells that our system performs better compared to other systems.

V. CONCLUSION:

Here a novel system is described which is used to protect the privacy of fingerprint by combining two different fingerprints and forming a new virtual identity. In the enrollment phase, the system captures two fingerprints from two different fingers. A combined minutiae template is generated and stored in the database. In the authentication phase we again capture two query fingerprints from same fingers. A two stage fingerprint matching process is used for matching the query fingerprint against the enrolled template. The advantage of using this system is that it has very low error rate. Compared with the feature level based technique we are able to create a new virtual identity which is difficult to distinguish from the original minutiae templates. Compared with the image level based technique we are able to create a new virtual identity which performs better when the two different fingerprints are randomly chosen.

REFERENCE:

1) Sheng Li, Student Member, IEEE, and Alex C. Kot, Fellow, IEEE, "*Fingerprint Combination for Privacy Protection*," IEEE transactions on information forensics and security, vol. 8, no. 2, February 2013.

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

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

4) Jie Zhou and Jinwei Gu, "*A Model – Based Method for the Computation of Fingerprints Orientation Field,"* IEEE Trans. On Image Processing, Vol. 13, No. 6, June 2004.

5) R. Cappelli, A. Lumini, D. Maio, and D. Maltoni, "*Fingerprint image reconstruction from standard templates*," IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 9, pp. 1489–1503, Sep. 2007.