International Conference on Recent Innovations in Engineering and Management
Dhananjay Mahadik Group of Institutions (BIMAT) Kolhapur, Maharashtra (ICRIEM-16)
23rd March 2016, www.conferenceworld.in ISBN: 978-81-932074-5-1

SECURE PRIVACY PROTECTION USING FINGERPRINT COMBINATION

Amber Anal[1], Aishwarya Adhikari[2], Jatin Garg[3], Snehal D'mello[4]

[1,2,3,4] Computer Engineering, St. John College of Engineering and Technology, (India)

ABSTRACT

Fingerprint techniques have been widely used in authentication systems, but fingerprint signatures can be stolen from the database by attackers. Hence protecting the privacy of the fingerprint becomes an important issue. Here is a novel system for privacy protection of fingerprint by combining two different fingerprint images into a new virtual identity. In the enrollment process two fingerprint images are taken from two different fingers. The system extracts the minutiae from one fingerprint image and the orientation from the second fingerprint image and the reference points from both. Based upon the information extracted, system combines the minutiae and orientation together and generates a new virtual fingerprint image. The authentication process will take two fingerprint images which were used in the enrollment stage. Finally, a two-stage fingerprint matching process will take place which will take two fingerprint images from two different fingers and then perform the matching process which matches the fingerprints using minutiae-based fingerprint matching algorithm.

Keywords: Fingerprint Combination, Minutiae, Orientation, Privacy, Reference Points

I. INTRODUCTION

Fingerprint techniques have been widely used in authentication systems. Hence protecting the privacy of the fingerprint becomes vital issue. Conventional cryptographic methods are not sufficient for protecting the privacy and security of the fingerprint, as decryption technique is needed before the fingerprint matching process. This technique exposes the fingerprint to the malicious users or attackers. Therefore, to avoid this problem, many methods have been developed which helps to develop specific fingerprint protection techniques. In order to protect the privacy of the fingerprint the existing methods uses key. This creates much inconvenience in the privacy protection. If both the key and fingerprint are stolen then the existing techniques become inefficient. Therefore, in recent years, significant efforts have been put into developing secure protection techniques for fingerprint.

The advantages of proposed technique over the existing fingerprint combination techniques are as follows:

- Compared with the feature level based technique [1], [2], this technique is able to create a new identity which is difficult to be distinguished from the original minutiae templates.
- Compared with the image level based technique [3], [4], this technique is able to create a new virtual identity which performs better when the two different fingerprint images are randomly chosen.

The basic organization of the paper is as follows: Section II introduces related work of the system. Section III explains the proposed system. Section IV explains how to generate a combined fingerprint using two different

fingerprint images, section V represents the conclusion of proposed system followed by the references in the last section.

II. RELATED WORK

In existing Fingerprint Reconstruction methods [5], Minutiae-based representation is widely used fingerprint representation technique. But, the minutiae template does not provide adequate information for reconstruction of the original fingerprint image perfectly. It becomes very hard to reconstruct the original fingerprint image, only with the help of minutiae template. But, it may result into many spurious minutiae in reconstructed image, which are not present in the minutiae template and it is helpful only to reconstruct a partial fingerprint image from the minutiae.

Fingerprint image enhancement is used to extract minutiae from the input fingerprint images using existing algorithms [6]. Ridge ending and ridge bifurcation are the two most important local ridge characteristics which are called as minutiae. The enhancement algorithm improves the accuracy of the ridge patterns of fingerprint images in recoverable regions and it helps to remove unrecoverable regions.

III. PROPOSED MODEL

Fig 1 and 2 shows the proposed system model, in the first stage i.e. the enrollment stage; our system takes two fingerprint images of two dissimilar fingers say X and Y. Then system selects minutiae positions from first fingerprint image X, and orientation from second fingerprint image Y or vice verse. Reference points are extracted from both the fingerprints. With the help of proposed coding technique, minutiae template is being produced and the signature of combined minutiae template is saved in a database.

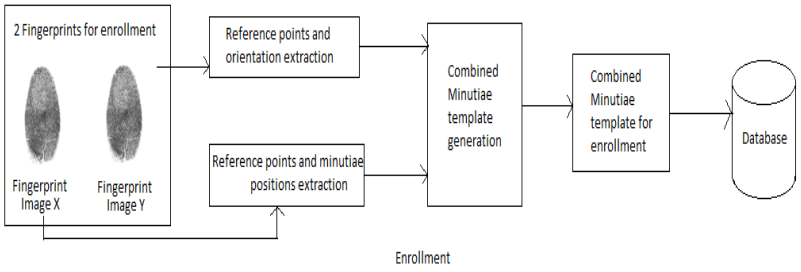

Fig.1. Enrollment Phase

In the second stage i.e. the authentication stage, two fingerprint images are required from same two fingers used in enrollment phase say X' and Y' . Same way as of enrollment stage, we capture minutiae positions from fingerprint image X' and orientation from fingerprint image Y' or vice versa, also the reference points from both query fingerprint images are detected. For proper authentication, two-stage authentication procedure is being followed. This procedure gives successful result if equivalent score is above the predefined value of the threshold.

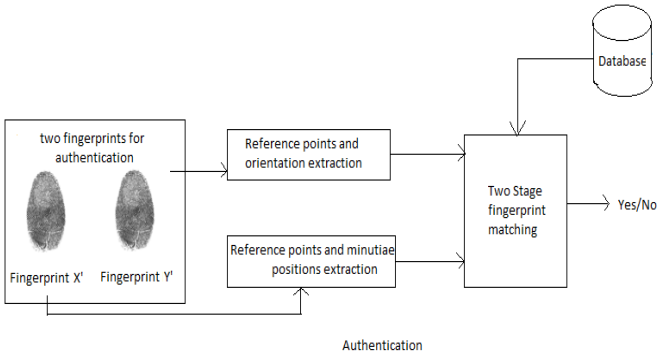

Fig.2. Authentication Phase

- **Minutiae extraction:**

The fingerprints are combination of different ridges and valleys, where each fingerprint is different from the other. The singularity of fingerprint is mainly decided by characteristics of ridges and their relations. Two most important ridge characteristics are ridge ending and the ridge bifurcations, which are also called as minutiae. If a fingerprint has 4-100 minutiae points then it is considered as good quality fingerprint. In Minutiae extraction phase, system firstly select the fingerprint image, then by applying binarization and thinning algorithm it will produce a binarized and thinned fingerprint image. After this the minutiae points are extracted by using the concept of crossing number. In crossing number minutiae can be selected by scanning neighboring ridge pixel using 3x3 window in Fig.3.

P4	P3	P2
P5	P	P1
P6	P7	P8

Fig. 3.The 3x3 window

Calculation of crossing number is explained in Fig.4.

$$CN = 0.5 \sum_{i=1}^{8} | P_i - P_{i+1} |$$

CN	Property
0	Isolated point
1	Ridge ending point
2	Continuing ridge point
3	Bifurcation point
4	Crossing point

Fig.4. Crossing Number Calculation

- **Combined Minutiae Template Generation**

The Combined Fingerprint Template is generated by combining the minutiae points extracted from the first fingerprint image and the orientation field extracted from the second fingerprint image. The combined fingerprint template is generated for various combinations of fingerprint images. The template's signature can then be stored in a database which can be used as a reference during the authentication.

- **Two-stage Fingerprint Matching Technique**

Given minutiae positions $P_{A'}$ of first fingerprint image A' and the orientation $O_{B'}$ of second fingerprint image B' and reference points of both the fingerprint images. For matching of combined minutiae template, we have introduced a two-stage fingerprint matching process as follows:

1) Query Minutiae Determination: It is very important step for fingerprint matching. We first extract local features of minutiae points in combined minutiae template. Then we select the pair

of reference points: one from fingerprint A' and second from fingerprint B'. Perturb the angle of reference points of A' which is labeled as $R_{a'}$. Generate the combined minutiae template for testing from $P_{A'}$, $O_{B'}$, $R_{a'}$. By selecting every point from the reference points, perform the above steps.

2)Matching Score Calculation: We perform modulo pi operation and then by using existing minutiae matching algorithms we calculate the matching score for authentication with the help of existing minutiae matching algorithm [7].

The two –stage fingerprint matching technique is described in Fig. 5.

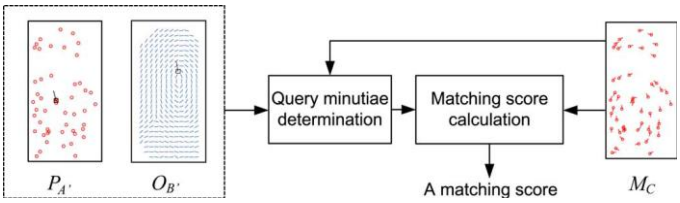

Fig 5.Two-Stage Fingerprint Matching

IV. COMBINED FINGERPRINT GENERATION

In case of combined minutiae template, the minutiae positions and proper directions are selected from two different query fingerprint images. They share a similar topology with an original fingerprint image. Hence, combined minutiae template has similar topology as the original minutiae template image. By using one of the existing fingerprint reconstruction techniques we can convert the combined minutiae template into a combined fingerprint image. Fig. 6 shows process that is used to generate a combined fingerprint image.

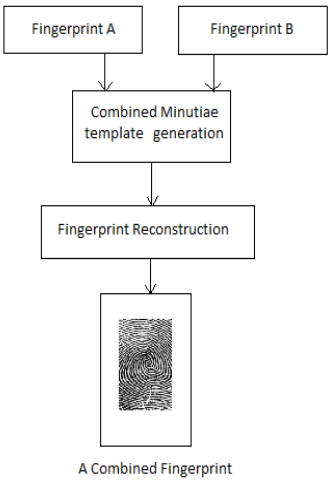

Fig. 6.Combined Fingerprint image Generation

First generate a combined minutiae template image using minutiae template generation algorithm. Then using one of the existing fingerprint reconstruction techniques [8] the combined fingerprint is reconstructed from template image.

Following steps are followed for combined minutiae image generation:

- Estimate an orientation from the set of minutiae points by using the orientation reconstruction algorithm.
- Generate a binary ridge pattern ridge frequency using Gabor filtering.
- Evaluate the phase image of the binary ridge pattern using fingerprint FM-AM model.
- By removing the spirals, reconstruct the continuous phase image.
- Combine the continuous phase image and the spiral phase image to produce the reconstructed phase image.
- A refined phase image is been produced by refining the reconstructed phase image by removing the spurious minutiae.
- Noising and rendering steps are performed on, so as to create a real-look alike fingerprint image.

V. RESULTS

The proposed system generates the combined fingerprint image using two different fingerprint images. Firstly, the system generates combined minutiae template using the existing techniques. Then the fingerprint reconstruction technique is applied on combined minutiae template to generate the fingerprint image which is indistinguishable from the two fingerprint images used for enrollment.Finally, by using a conventional minutiae matching algorithm [7], combined minutiae template is matched against the corresponding enrolled template . The VeriFinger [7] is used for the minutiae positions extraction and the minutiae matching. The algorithm proposed in [6] is used for the orientation extraction

Fig.7. The second row (from left to right): the combined minutiae template, the combined fingerprint from proposed method (without noising and rendering), and the combined fingerprint image

VI. CONCLUSION

In this paper, a secure system for fingerprint privacy protection by combining two fingerprint images into a new virtual identity is introduced. With the help of this system it will be difficult for an attacker to break traditional systems by using the combined minutiae templates. Also it is difficult to recover original minutiae template from the combined one. It provides more choices for a single user for the enrollment and authentication.

REFERENCES

[1] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR- CTP Workshop, Cambridge, U.K.,Aug. 2004.

[2] E. Camlikaya, A. Kholmatov, and B. Yanikoglu, "Multi-biometric templates using fingerprint and voice," Proc. SPIE, vol. 69440I, pp.69440I-1–69440I-9, 2008.

[3] A. Ross and A. Othman, "Mixing fingerprints for template security and privacy," in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona,Spain, Aug. 29–Sep. 2, 2011.

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

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

[6] 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.

[7] VeriFinger 6.3. [Online]. Available:http://www.neurotechnology.com

[8] 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.