COMBINATION OF FINGERPRINT FOR PRIVACY PROTECTION

Monika Sharma
M.Tech Scholar
Vishal Vig, Kamal Kant Verma
Assistant Professor
Quantum School of Technology, Roorkee

ABSTRACT

With the increasing use of biometric technology raised many areas and of the biggest challenges to the wide applicability of biometric system is fingerprint recognition system. A fingerprint is the pattern of ridges and valleys. Traits of fingerprint are ridge ending, bifurcation and short endings. Now in this paper is to combine two different fingerprints from two fingers into a new indentify. It is carried out into two phases. The first phase combined minutiae template will be generated from two different fingers and in the next phase fingerprint matching process is used for matching query fingerprints against a combined minutiae template by using image processing algorithm.

KEYWORDS: Minutiae, fingerprint, virtual, combination, templates

I. INTRODUCTION

Fingerprint recognition is based on the imaging of the fingertips. The structure of a fingerprint's ridges and valleys is recorded as an image or digital template (a simplified data format, minutiae- based most of the time) to be further compared with other images or templates for authentication or verification. Images of fingertips are captured with specific fingerprint sensors. Among all the biometric techniques[8], fingerprint-based identification is the oldest method which has been successfully used in numerous applications for over a century, more recently becoming automated due to advancements in computing capabilities.

Biometric template refers to the information extracted from a biometric and stored as the reference. For instance, if a fingerprint is used, the biometric template may consist of features extracted from the fingerprint image (e.g. minutiae points indicating the branching and ending points of the ridges of the fingerprint). Biometric template protection [9], in turn, generally refers to protecting one's biometric data r biometric template from unauthorized access or unintended use. Biometric template protection is especially important because biometrics cannot be revoked and re-issued once compromised. So,It is important to generate better and secure fingerprints privacy protection system. In this paper we introduce here for protecting fingerprint privacy [6] by merging two different fingerprints into a new virtual identity.

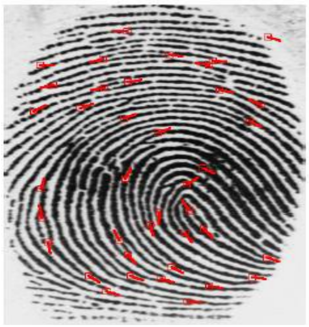

Fig 1 Fingerprint minutiae

II. VIRTUAL INDENTITY GENERATION ALGORITHM

In the proposed fingerprint privacy protection system[2] consist of two phases as enrollment phase and authentication phase during the enrolment, the system captures two fingerprints from two different fingers. Use a combined minutiae template generation algorithm to create a combined minutiae template from the two fingerprints [7]. In such a template, the minutiae positions are extracted from one fingerprint using Gabor filtering technique, and the reference points are detected from both the fingerprints. While the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. From these features generate combined minutiae template. This template is stored in database for authentication. In the authentication phase the same two fingers used in the enrollment are given as the input the reference points and the minutiae features are extracted from the fingerprint A‟ and the orientation points and the reference points are extracted from the fingerprint B‟ and the minutiae template is generated. The template is matched with the reconstructed fingerprint with two stage fingerprint matching. A two-stage fingerprint matching process is further for matching the two query fingerprints against a combined minutiae template. In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using a fingerprint reconstruction approach. The combined fingerprint issues a new virtual identity for two different fingerprints, can be matched using minutiae based fingerprint matching algorithms.

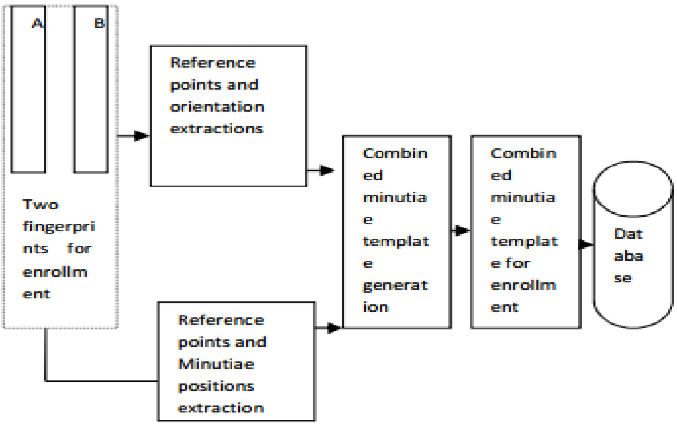
A
B
Two fingerprints for enrollment
Reference points and orientation extractions
Reference points and Minutiae positions extraction
Combined minutiae template generation
Combined minutiae template for enrollment
Database

Fig: 2 Block diagram of proposed system

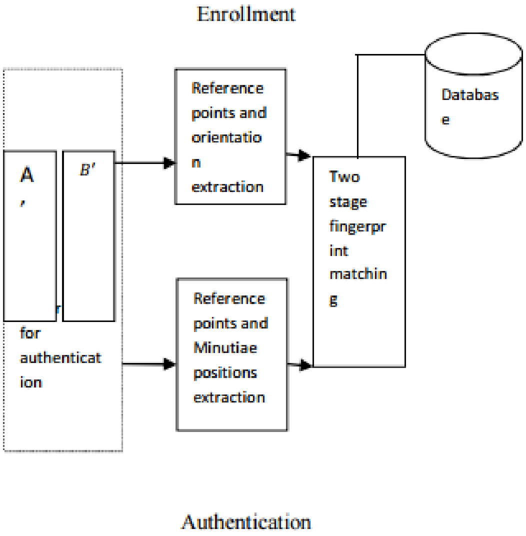
Enrollment
A ,
B'
for authentication
Reference points and orientation extraction
Reference points and Minutiae positions extraction
Two stage fingerprint matching
Database
Authentication

Fig: 3 Block diagram of virtual identity generation system

A. Reference point and orientation detection the reference point's detection process is motivated by the use of complex filters for singular point detection [3]. Given a fingerprint, the main steps of the reference point's detection are summarized as follows
1) Compute the orientation O from the fingerprint using the Orientation Estimation Algorithm.
2) Obtain the orientation Z in complex domain, In Equation (1) represents the orientation angle of the fingerprint i. Z=cos(2O)+jsin(2O) (1)
3) Calculate a certainty map of reference points as shown in Equation (2) i. Cref =Z*Tref (2) "*" is the convolution operator and Tref is the reference points detection.
4) Locate a reference point satisfying the two criterions: i. The amplitude should be a local maximum ii. The local maximum should be over a fixed threshold.
5) If no reference point is found for the fingerprint, locate a reference point with the maximum certainty value in the whole fingerprint image.

B. Reference Point and Minutiae Position Detection Most finger print minutiae extraction methods are thinning-based skeletonization process converts each ridge to one pixel wide. Minutiae points are detected by locating the end points and bifurcation points on the thinned ridge skeleton based on the number of neighboring pixels. The end points are selected if have a single neighbor and the bifurcation points are selected if have more than two neighbors. The methods based on thinning are sensitive to noise and the skeleton structure does not conform to intuitive expectation. Gabor filters are used to enhance the minutiae positions.

C. COMBINED MINUTIAE TEMPLATE GENERATION

This module is done by using Minutiae Position Alignment, Minutiae Direction Assignment.
Among the reference point of a fingerprint for enrolment the reference point of maximum certainty value is taken as the primary reference point. Let us assume Ra and Rb
Primary reference point of the fingerprint A and B is defined in the Equation (4)

$$(\mathrm{Pic})\mathrm{T} = \mathrm{H}.\ (P_{ia} - r_a)\ \mathrm{T} + (\ r_b)\ \mathrm{T}$$

...............4

Each aligned minutiae position is assigned with a direction. The range is from 0 to π. The range of will the same as that of the minutiae directions from an original fingerprint.
Θi = Oe(xi,yi)+ρπ .....(5)
In Equation (5) ρ is an integer is randomly selected from {0, 1}. The range of Oe (xi,yi) is from 0 to π.The range of Θi will be from 0 to 2π, is the same as that of the minutiae directions from an original fingerprint. pi may be located outside of the fingerprint B, Oe (xi,yi) is not well defined. In such case, predict Oe (xi,yi) before the direction assignment. Some works for modeling the fingerprint orientation can be adopted for the orientation prediction. Once the N aligned minutiae positions are assigned with directions a combine minutiae template Me= {mi = (pi, θi), 1<i 4

Each aligned minutiae position is assigned with a direction. The range is from 0 to π. The range of will the same as that of the minutiae directions from an original fingerprint.
Θi = Oe(xi,yi)+ρπ .....(5)
In Equation (5) ρ is an integer is randomly selected from {0, 1}. The range of Oe (xi,yi) is from 0 to π.The range of Θi will be from 0 to 2π, is the same as that of the minutiae directions from an original fingerprint. pi may be located outside of the fingerprint B, Oe (xi,yi) is not well defined. In such case, predict Oe (xi,yi) before the direction assignment. Some works for modeling the fingerprint orientation can be adopted for the orientation prediction. Once the N aligned minutiae positions are assigned with directions a combine minutiae template Me= {mi = (pi, θi), 1<i 4

Each aligned minutiae position is assigned with a direction. The range is from 0 to π. The range of will the same as that of the minutiae directions from an original fingerprint.
Θi = Oe(xi,yi)+ρπ .....(5)
In Equation (5) ρ is an integer is randomly selected from {0, 1}. The range of Oe (xi,yi) is from 0 to π.The range of Θi will be from 0 to 2π, is the same as that of the minutiae directions from an original fingerprint. pi may be located outside of the fingerprint B, Oe (xi,yi) is not well defined. In such case, predict Oe (xi,yi) before the direction assignment. Some works for modelling the fingerprint orientation

can be adopted for the orientation prediction. Once the N aligned minutiae positions are assigned with directions a combine minutiae template Me= {mi = (pi, θi), 1<i .

D. FALSE MINUTIAE REMOVAL

The preprocessing stage does not totally heal the fingerprint image. The false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking or totally eliminated.

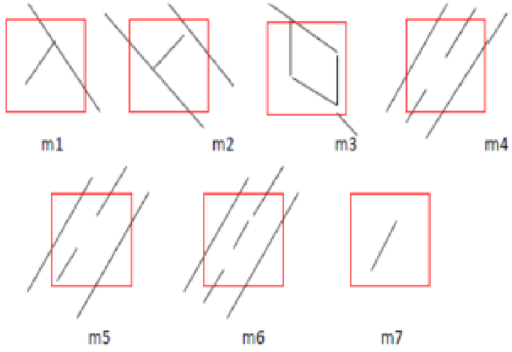

Fig: 3 False Minutiae Removal

E. 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 [4]. 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.

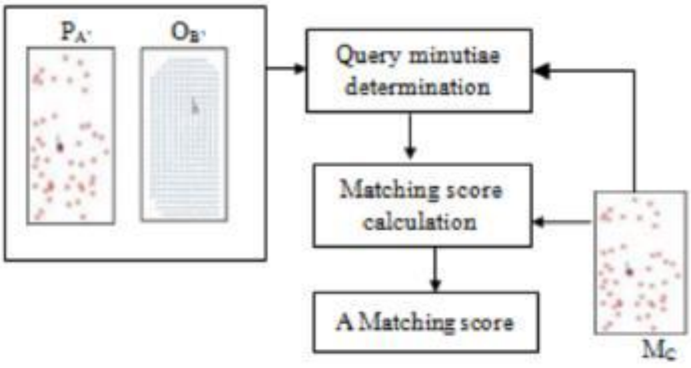

Fig: 4 Two -stage fingerprint matching

THIS MODULE CONTAINS TWO PROCESSES

Query minutiae determination

Matching score calculation

Here generating the minutiae, reference point of query image. Using this generate combined minutiae template of query image 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 of these reconstruction techniques can only generate a partial fingerprint. By using minutiae based scheme can generate a full fingerprint. In [1], the full fingerprint will be generated by using minutiae based scheme. By adopting one of these fingerprint reconstruction approaches allows to convert combined minutiae template into a combined fingerprint image. Figure 5 shows process to generate a combined fingerprint for two different fingerprints. The combined fingerprint will be reconstructed by using some fingerprint reconstruction approaches from combined minutiae template.

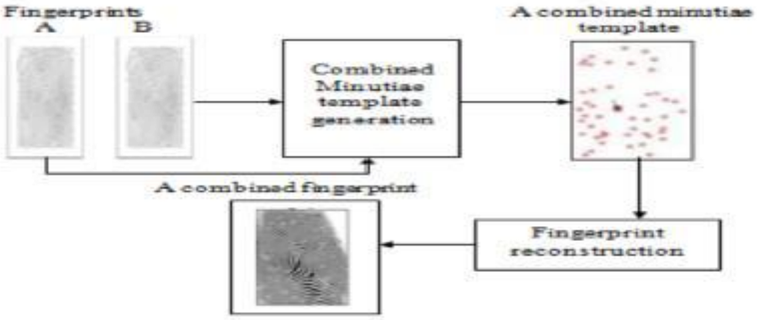
Fingerprints
A
B
Combined Minutiae template generation
A combined minutiae template
A combined fingerprint
Fingerprint reconstruction

Fig 5: Combined fingerprint generation template

For the combined minutiae templates [5] those are generated using Coding Strategy, a module for all the minutiae directions in and so as to remove the randomness. After the module operation, use a minutiae matching algorithm to calculate a matching score between and for the authentication decision.

$$\text{Match Score} = \frac{\text{No of Total matched minutiae pair}}{\text{No of minutiae in fingerprint templete}}$$

III. RESULT

The experiment is conducted on the first two impressions of the FVC2004DB2_A database which contains 400 fingerprints from 200 fingers. The VeriFinger 6.3 is used for minutiae position extraction and the minutiae matching. The reference point detection has an impact on the accuracy and efficiency of the proposed system. The two parameters need to be determined for the reference point detection; σ for complex filters and T is the threshold for the references point detection. The value for σ = 1.5 and T=5. The input images labeled A and B is taken as sample fingerprint image.

Fig 5: Input image of fingerprint

Fig 6: Input image of fingerprint 2

The minutiae points and the reference points from both the fingerprints are extracted the minutiae points referring ridge ending, bifurcation, core are extracted from the two fingerprints as shown in the figure 7.

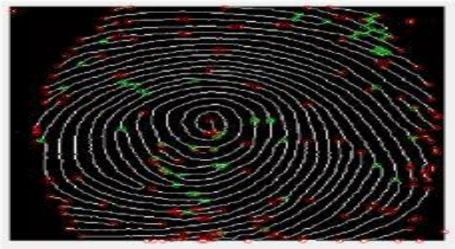

Fig: 7 Minutiae point detection

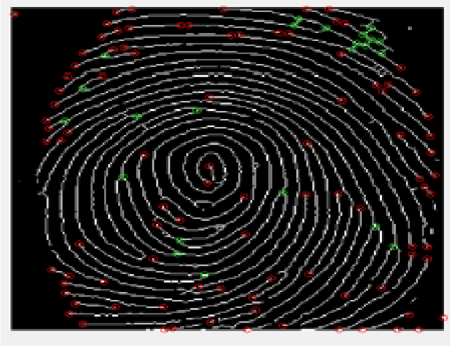

Fig: 8 False removal minutiae

The false minutiae are removed from the combined minutiae template as shown in the figure 8. The region of interest can be detected automatically or manually the manual detection is done for security as shown in the figure 9

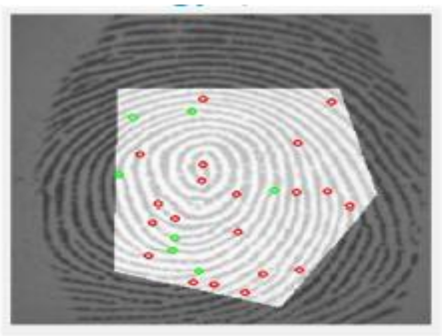

Fig: 9 Region of interest

The orientation points are detected from the combined minutiae template [10] in the basis of ridge ending, bifurcation, core points with orientation estimation algorithm by distance computation as shown in the figure 10.

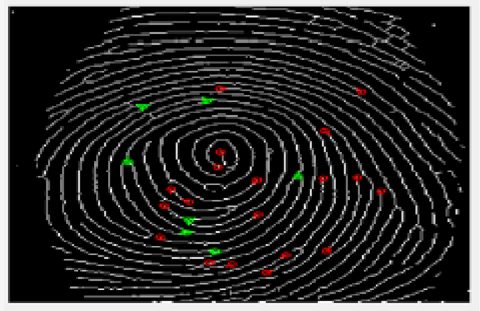

Fig: 10 Orientation point detection

The validation of the combined fingerprint and the similarity measure of matching with the combined minutiae template and the reconstructed fingerprint are shown in the figure 11 and 12

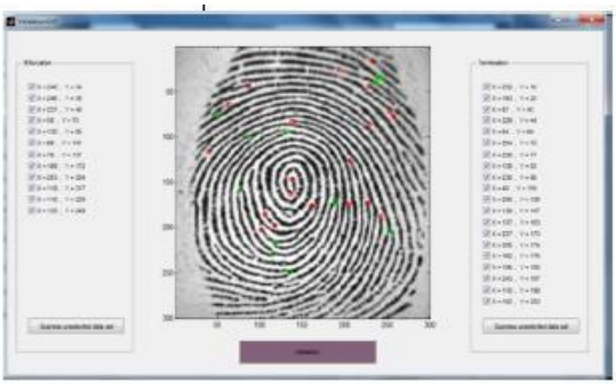

Fig: 11 Validation of fingerprint

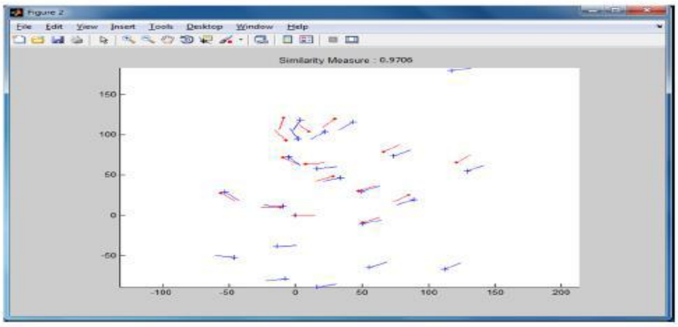
Figure 2
File Edit View Insert Tools Desktop Window Help
Similarity Measure : 0.9706
150
100
50
0
-50
-100
-50
0
50
100
150
200

Fig: 12 Similarity measure of matching

IV. CONCLUSION

A novel minutiae-based fingerprint matching approach is used in this work. The new fingerprint matching algorithms have shown enough correctness to consider this a good path. All the outcomes are shown over the same fingerprint. The results show that the extraction of the Delta and Core points and Minutiae has reached promising results at a very low operational complexity. The attacker cannot attack the database. So it will be more protecting system for the fingerprint database. In the future work the combined fingerprint can be developed in the combination of three fingers and maximum minutiae points the running time complexity arises the fingerprint enhancement algorithm can be used for maintaining the better performance and for achieving a better security.

V. REFERENCE

1. U. Uludag, S. Pankanti, S. Prabhakar, and A. Jain, "Biometric cryptosystems: Issues and challenges," in Proceedings of the IEEE, 92(6), 2004.
2. Sheng Li and Alex C. Kot, "Fingerprint combination for privacy protection," in IEEE Trans.
3. Information Forensics and Security, Vol. 8, No. 2, February 2013 L. O‟Gorman, "Comparing passwords, tokens, and biometrics for user authentication," in Proceedings of the IEEE, 91(12), pp. 2021–2040, Dec. 2003.
4. N. Ratha, S. Chikkerur, J. Jonathan Connell, and R. Bolle, "Generating cancelable fingerprint templates," IEEE Transactions Pattern Analysis Machine Intelligence 29(4), pp. 561– 572, 2007.
5. Yanikoglu B. and Kholmatov A. (2004), 'Combining multiple biometrics to protect privacy', in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug.
6. Ross A. and Othman A.(2003), 'Mixing fingerprints for template security and privacy', in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain.
7. Li S. and Kot A.C. (2012), 'A novel system for fingerprint privacy protection', in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), pp. 262–266.
8. Anthonioz NME, Champod C. Evidence Evaluation in Fingerprint Comparison and Automated Fingerprint Identification Systems – Modeling Between Finger Variability.Forens bifurification icSciInt 2014;235:86-101
9. J. Woodward, "Biometrics: Privacy's foe or privacy's friend?," Proceedings of the IEEE 85(9), p. 1487, 1997.
10. P. Tuyls, E. Verbitskiy, T. Ignatenko, D. Denteneer, and T. Akkermans, "Privacy protected biometric templates: Acoustic ear identification," in Proceedings of SPIE: Biometric Technology for Human Identification, Vol. 5404, pp. 176–182, 2004.