RESEARCH ARTICLE OPEN ACCESS

Fingerprint Matching For Privacy Protection

Dora Angel. M,
PG Scholar, Department of information technology,
Francis Xavier engineering college, Tirunelveli.

Andrew Rayan.T,
Assistant professor, Department of information technology, Francis Xavier engineering college, Tirunelveli.

Abstract
In this project, we propose a new concept for preserving fingerprint confidential. This is done by joining two various fingerprints into a single fingerprint. In the enrollment phase, two fingerprints are taken from two different fingers. To obtain information from two fingerprints, we need minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. A combined minutiae template is created with the use of obtained information. Then the created minutiae template is stored in the database. In the authentication phase, we need the same two fingerprints which are used in enrollment phase. For matching the two fingerprints with a combined minutiae template (which is stored in the database),a two stage fingerprint matching process is used. The minutiae characteristics of one fingerprint will not be satisfied when database is stolen by unauthorised users. The attackers cannot easily find out a combined. Two different fingers are picked up randomly.

I. INTRODUCTION

Network security mainly begins with authentication, such as a username and a password. The authentication means to keep our original information from unauthorized users. There are three types of authentication in network security. These are one factor authentication, two factor authentications, and three factor authentications. One-factor authentication means passwords. The example of two factor authen tication is ATM Card. Three-factor authentication means the user ‘is’ (e.g. a fingerprint) which is discussing in this paper. In this project we are discussing about fingerprint concepts. A Fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. In a wider use of term, fingerprints are the traces of an impression from the friction ridges of any part of a human or other primate hand. Impressions of fingerprints may be left behind on a surface by the natural secretions of sweat from the accrue glades that are present in friction ridge skin.

A human fingerprint has three important characteristics. The main purpose of Characteristics in human fingerprints is basically used for identifying something. These are classified into levels. The overall pattern of ridge flow (a whorl or a loop) is defined in the first level. The ridge flow such as bifurcations and ridge endings are described in the second level. The third level is having more properties such as shape of ridges or pore configurations. Fingerprint ridges are having the three basic patterns, such as the arch, loop, and whorl:

Arch: From one side of the finger, the ridges are started, increase in the centre part of the finger forming an arc, then in the other side of the finger, it exits. In our fingerprints Arches are found in about 5% only.

Loop: From one side of a finger, the ridges are stared, then it forms a curve, finally on that same side, it exits. In our fingerprints Loops occur in about 60-70%. Loops are classified into two types: ulnar loop and radial loop.

Whorl: In our fingerprint patterns, the whorls are found in about 25-35%. The types of whorl patterns are plain whorl, central pocket whorl, double pocket whorl and accidental whorl.

II. THE FINGERPRINT PRIVACY PROTECTION SYSTEM

Fig.1 shows our fingerprint privacy protection system. In our privacy system, there are two phases are proposed. Such as enrollment phase and authentication phase respectively. In the enrollment phase two fingerprints are taken from two various fingers. Two fingerprints are named as Fingerprint A and fingerprint B. From fingerprint A, minutiae positions are obtained. From fingerprint B Orientation is obtained. Finally reference points are obtained from both fingerprints.ie, from fingerprint A and B. A combined minutiae template is created with the use of obtained information from the fingerprints. This created template is stored in the database.

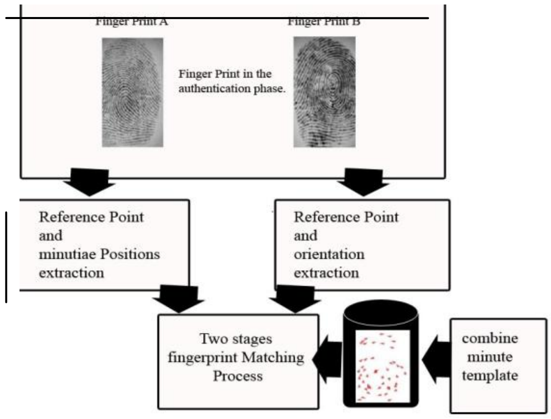
Finger Print A
Finger Print B
Finger Print in the authentication phase.
Reference Point and minutiae Positions extraction
Reference Point and orientation extraction
Two stages fingerprint Matching Process
combine minute template

Fig. 1. Fingerprint Privacy System

The above diagram shows the authentication phase. In the authentication phase, two fingerprints (that are used in the enrollment phase) are required for matching with the combined minutiae template. The fingerprints in the authentication phase are taken as A' and B'.As the process done in the enrollment phase, the minutiae positions from fingerprint A' and the orientation from fingerprint B' are obtained. The reference points are also obtained from the both fingerprints. These obtained information will be matched with the corresponding combined template which is stored in the database. A two- stage fingerprint matching process is used for matching process. The fingerprint privacy protection system contains the modules. Such as reference point's detection, combined minutiae template generation and two stage fingerprint matching.

A. Reference points detection

Reference points are very important in the both enrollment phase and authentication phase. The reference points are detected using the following steps.

- The orientation is detected from the fingerprint with the help of the orientation estimation algorithm.
- The maps of reference points are calculated.
- The improved certainty is calculated for reference point detection.
- Find a reference point based on the following conditions (i) the amplitude of the point is a local maximum (ii) The local maximum should be over a fixed threshold.
- Until all reference points are positioned, repeat the above step.
- In both steps 4) and 5), if no reference point is detected for the fingerprint, discover a reference point with the maximum certainty value in the whole fingerprint image.

B. Combined Minutiae template Generation

Combined minutiae template generation consists of two steps.

- Minutiae position alignment
- Minutiae direction alignment

1) Minutiae Position Alignment: Here minutiae position from fingerprint A is aligned. It defines a reference point with the maximum certainty value. Therefore, It has two primary reference points and for fingerprints A and B respectively. By interpreting and rotating each minutiae point, the alignment is performed properly.

***2)* Minutiae Direction Assignment:** There are many minutiae directions are used in the enrollment phase and authentication phase also. Every minutiae directions are aligned. Here the fingerprint template's direction is assigning by using integer value that is 0 and1.

C. Two-Stage Fingerprint Matching

Two-stage fingerprint matching is mainly used in the authentication phase. This two-stage fingerprint matching is used for matching the two query fingerprints (used in the enrollment phase) with the combined minutiae template (stored in the database) in the authentication phase. Two-stage fingerprint matching process consists of the following steps,

A) Query minutiae determination:

The query minutiae determination is a very important step during the fingerprint matching. Here local and global features of the fingerprints are used. In order to reduce this algorithm, we introduce the local characteristics obtained from a minutiae.

B) Matching score calculation:

Here for removing the randomness we do modulo operation for all the minutiae directions. After the modulo operation, we use an existing minutiae matching algorithm to find out a matching score .

III. COMBINED FINGERPRINT TEMPLATE GENERATION

In combined minutiae template generation, From two fingerprints the minutiae positions and minutiae directions are obtained separately. The obtained minutiae positions and minutiae directions from the fingerprints are having the same characteristics of the original fingerprint. Therefore, the characteristics of combined minutiae template are same as an original minutiae template. The following Figure shows the process to create a combined fingerprint template for two various fingerprints. Here we take any two various fingerprints as input, first create a combined minutiae template using our combined minutiae template generation algorithm. Then, By using existing reconstruction approach, a combined fingerprint is reconstructed from the combined minutiae template . Here reconstruction approach is used. The reconstruction approach is used for the following purpose. A minutiae-based template is having small information about a fingerprint image. The minutiae based template does not contain enough information for reconstructing the original fingerprint.

Our experimental results show that the reconstructed images are very realistic. it can cheat a human expert. Whether the following is possible, The main aim of this research is to learn the reconstruction of fingerprint images from templates

- To cheat a human expert
- To fulfil pretend attacks against automatic fingerprint recognition system.

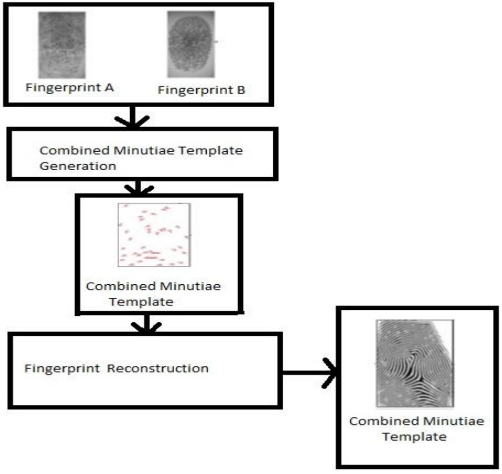
Fingerprint A
Fingerprint B
Combined Minutiae Template Generation
Combined Minutiae Template
Fingerprint Reconstruction
Combined Minutiae Template

Fig. 2. Combined Minutiae Template Generation

The fig 2 shows the combined minutiae template generation. Here Fingerprint A and Fingerprint B are extracted from the two different fingers. From these fingerprints a combined minutiae is generated. The generated combined minutiae template is shown in the above figure. This constructed fingerprint template is again reconstructed. Since a minutiae-based template is having limited information of a fingerprint image. It does not contain enough information about the reconstruction of the original fingerprint. So that this created combined minutiae template is reconstructed again using a reconstruction approach. Then the combined minutiae template is generated which is shown in the above figure. The combined minutiae template is a real one. But not a combined one.

IV. CONCLUSION

In this paper, we introduce a concept for fingerprint privacy protection. Our combined minutiae template (by combining two fingerprints into a new identity) has a similar topology to an original minutiae template. Since in Fingerprint matching, we use combined minutiae template to combine two fingerprint and create an single template, here we are creating multiple combination of the fingerprint of an single finger and get the same procedure for other finger and create an multiple template so that we can able to provide accurate information of the person and we use this information for the data transferring in data centric network. So, that the privacy of the information can't be traced because we encrypt the data with the possible template of the finger print, thus the data will be secured and thus proper authentication of finger will be obtained which reduces the fraud activities.

REFERENCES

[1] S. Li and A. C. Kot, "A novel system for fingerprint privacy protec-tion," in *Proc. 7th Int. Conf. Inform. Assurance and Security (IAS)*, Dec. 5–8, 2011, pp. 262–266.

[2] B. J. A. Teoh, C. L. D. Ngo, and A. Goh, "Biohashing: Two factor au-thentication featuring fingerprint data and tokenised random number," *Pattern Recognit.*, vol. 37, no. 11, pp. 2245–2255, 2004.

[3] A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, "An analysis of biohashing and its variants," *Pattern Recognit.*, vol. 39, no. 7, pp. 1359–1368, 2006.

[4] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 29, no. 4, pp. 561–72, Apr. 2007.

[5] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template trans-formation: A security analysis," in *Proc. SPIE, Electron. Imaging, Media Forensics and Security*, San Jose, Jan. 2010.