NOVATEUR PUBLICATIONS
INTERNATIONAL JOURNAL OF INNOVATIONS IN ENGINEERING RESEARCH AND TECHNOLOGY [IJIERT]
ISSN: 2394-3696
VOLUME 4, ISSUE 2, Feb.-2017

COMBINING FINGERPRINTS FOR SECURITY PURPOSE: ENROLLMENT PROCESS

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

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

ABSTRACT
Here a novel system is shown for protecting fingerprints by combining two different fingerprints to a new identity. The enrollment process is executed here in which two different fingerprints are captured. Then extract the minutiae position from one fingerprint and orientation from other fingerprint. Compute reference points from both the fingerprints. After this combine both the fingerprints to form a new identity. By using the existing fingerprint reconstruction technique the fingerprint is reconstructed. Thus a new virtual identity is formed from two different fingerprints. This formed new virtual identity is then stored in database.

KEYWORDS: Combination, fingerprints, minutiae, orientation, and reference point.

INTRODUCTION
Fingerprint identification is one the most important biometric technologies. Among all the biometric techniques, fingerprint-based identification is the oldest method which has been successfully used in numerous applications. Everyone is known to have unique, immutable fingerprints. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. The two most prominent ridge characteristics called minutiae are (i) ridge ending and (ii) ridge bifurcation. A ridge ending is defined as the point where a ridge ends abruptly. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. A good quality fingerprint typically contains about 40-100 minutiae. Example of minutiae is shown in below fig 1.1.

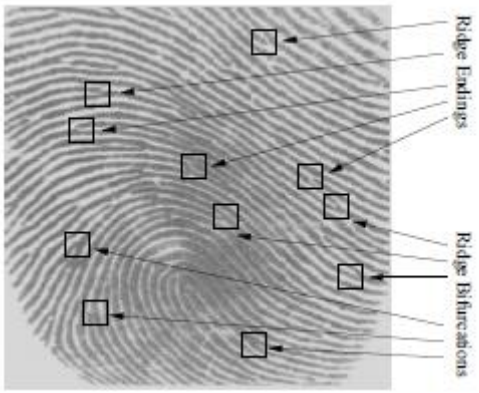


Fig 1: Ridge Endings & Ridge Bifurcations

Automatic fingerprint matching depends on comparison of these local ridge characteristics and their relationships to make a personal identification. A critical step in fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images, which is difficult task. The performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In an ideal

fingerprint image, ridges and furrows alternate and flow in locally constant direction and minutiae are anomalies of ridges i.e. ridge endings and ridge bifurcations.
In this paper we introduce a novel system for protecting fingerprints by combining two different fingerprint into new identity. During the enrollment process we capture two different fingerprints from two different fingers. We propose a combined minutiae template generation algorithm to create a combined minutiae template from two fingerprints.

PRE - PROCESSING

In the enrollment phase we capture two fingerprints and first of all do the following process on it.
Load Image
The general shape of the fingerprint is generally used to pre-process the images, and reduce the search in large databases. This uses the general directions of the lines of the fingerprint, and the presence of the core and the delta. Several categories have been defined in the Henry system: whorl, right loop, left loop, arch, and tented arch. Most algorithms are using minutiae, the specific points like ridges ending, bifurcation. Only the position and direction of these features are stored in the signature for further comparison.
RGB to Gray conversion
Here we are going to convert the RGB image into grayscale image as we need grayscale image here.
Enhancement
A critical step in automatic fingerprint matching is to automatically and reliably extract minutiae from the input fingerprint images. However, the performance of a minutiae extraction algorithm relies heavily on the quality of the input fingerprint images. In order to ensure that the performance of an automatic fingerprint identification/verification system would be robust with respect to the quality of the fingerprint images, it could be essential to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. In our case, the quality of the image is really good, and we won't need to enhance our image.
Binarization
In Binarization, the gray scale image is converted into binary image. Binary images are easy to process. The basic principle of converting an image into binary is to decide a threshold value, and then the pixels whose value are more than the threshold are converted to white pixels, and the pixels whose value are below or equal to the threshold value are converted to black pixels.
After the operation, ridges in the fingerprint are highlighted with black color while furrow are white.
Thining
After we get the binary image, the next task is to thin the image. It is easy to develop algorithm for minutiae detection in thinned image. If the width of ridge is more than one pixel, then it is very hard to develop algorithm for minutiae detection. In thinned image we have a single pixel width ridges.
Ridge thining is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.

PROPOSED MODEL

In the enrollment phase we capture two fingerprints say fingerprint A and fingerprint B from two different fingers say finger A and finger B. Fig 4.1 below shows our proposed model

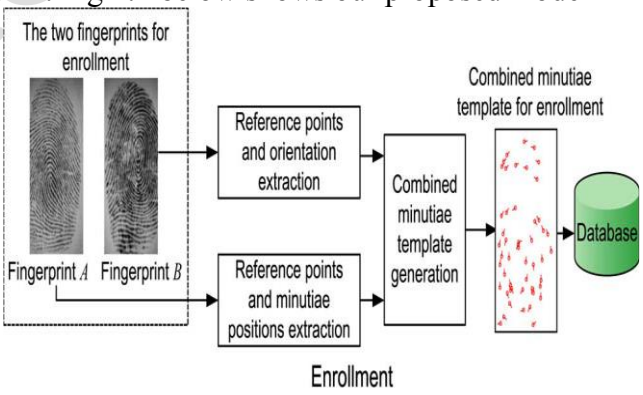


Fig 2 : Enrollment phase

We extract the minutiae positions from fingerprint A and the orientation from fingerprint B using some existing techniques. Then, by using our proposed coding strategies, a combined minutiae template is generated based on the minutiae positions, the orientation and the reference points detected from both fingerprints. Finally, the combined minutiae template is stored in a database.

Steps of Reference Points Detection

The reference points detection process is motivated by Nilsson et al., who first proposed to use complex filters for singular point detection. Given a fingerprint the main step of the reference point detection are as follows:

i. Compute the orientation O from the fingerprint. The orientation in complex domain where,

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

ii. Calculate a certainty map of reference points,

$$C_{ref} = Z * \bar{T}_{ref}$$

Where "*" is the convolution operator and $\bar{T}_{ref}$ is the conjugate of

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

This is the kernel for reference points detection.

iii. Calculate the reference points using the following equation

$$C'_{ref} = \begin{cases} C_{ref} \cdot \sin(Arg(C_{ref})) & \text{if } \mathrm{Arg}(C_{ref}) > 0 \\ 0 & \text{otherwise} \end{cases}$$

Combined Minutiae Template Generation

Here the combined minutiae template is generated based on the external information from the fingerprints and the minutiae position alignment and minutiae direction assignment.

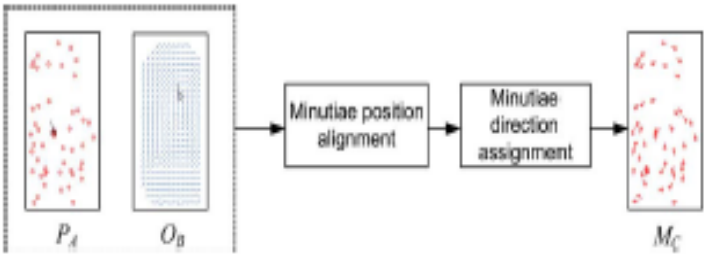


Fig 3 : Combined minutiae template generation process

Minutiae position alignment

The alignment is performed by translating and rotating each minutiae point. Two primary reference points are overlapped both in the position and the angle after the minutiae position alignment.

Minutiae direction assignment

Here each aligned minutiae position is assigned with a direction. Once all the aligned minutiae position are assigned with directions, a combined minutiae template is created for enrollment.

EXPERIMENTAL RESULTS

The experiment is conducted on the first two impression of the database which contains 10 fingerprints from 5 fingers (with 2 impressions per finger)

1. First capture any two fingerprints from the database say fingerprint A and fingerprint B

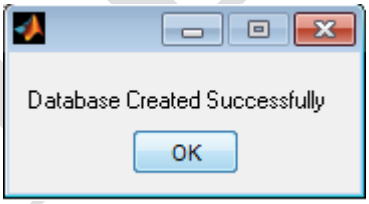
Fingerprint A

Fingerprint B

2. After capturing the fingerprint we have to enter the name of the account holder so that we can save it for future use.

3. Then we are going to combine both the fingerprints

4. After combining the fingerprints the data is saved in the database for future use and we get a message that database created successfully.



CONCLUSION

In this paper we introduced a novel system for fingerprint combination. Here two different fingerprint and combined it to form a new identity. In the experimental result we observe that two different fingerprints are combined and stored in database. The advantage of using this system is that new identity is generated which is difficult to be distinguished from the original minutiae template. Compared with image level based technique our system performs better when two different fingerprints are randomly chosen.

REFERENCES

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) 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) Ankita Mehta and Sandeep Dhariwal Electronics &Communication Engineering Department, HCTM, Kaithal, India "Design & Implementation of Features based Fingerprint Image Matching System" Int. J. of Multidisciplinary and Current research, Nov/Dec 2014