Paper ID: VESCOMM 13

COMBINATION OF FINGERPRINT FOR PRIVACY PROTECTION: PRE-PROCESSING

Miss.Rathod Leena Anil
Department of Electronics and Telecommunication,
V.V.P. Institute of Engg & Technology,
Solapur University, Solapur, Ms, India
leenarathod05@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* – Biometrics is the measurement and statistical analysis of people's physical and behavioural characteristics. Using biometrics to verify identity means using a physical characteristic such as face, voice or fingerprints to authenticate an individual's claimed identity. Fingerprint matching is by far the most successful biometric technology because its ease of use, non-intrusiveness and reliability. Here we introduce a novel system for protecting fingerprint privacy by combining two different fingerprints into new identity. Firstly we extract the minutiae position from one fingerprint, the orientation from other fingerprint and reference point from both fingerprints. The coding strategy is applied and a combined minutiae template is generated and stored in database. In the authentication process, the system needs two query fingerprints from the same fingers which are used in enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template.**

Keywords – Fingerprint enhancement, pre-processing minutiae, orientation, combination.

I. INTRODUCTION

Recognition of person by means of biometric characteristics is an emerging phenomenon in modern society. It has received more and more attention during the last period due to the need of security in a wide range of application. Among the many biometric features the fingerprint is considered one of the most practical ones. Fingerprint recognition requires a minimal effort from the user does not capture other information than strictly necessary for the recognition process and provides relatively good performance.

Securing a stored fingerprint image is of paramount importance because a compromised fingerprint cannot be easily revoked. Traditional encryption and decryption methods are used for fingerprint privacy and protection. But this encryption method is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to attacker. In recent years significant efforts have been put into developing specific protection techniques for fingerprint. Most of the existing techniques make use of keys for the fingerprint privacy protection.

In 2004 two different fingerprints were combined together into a single new identity either in feature level or image level. The concept of combining two different fingerprints into a new identity is created by combining the minutiae positions extracted from the two fingerprints. The image level based fingerprint combination technique has two advantages: (1) it is difficult for attacker to distinguish a mixed fingerprint from the original fingerprints, and (2) existing fingerprint matching algorithm are applicable for matching two mixed fingerprints.

Here in this paper a novel system has been proposed for protecting the privacy of the fingerprints. There are two steps enrollment and authentication phase. In the enrollment phase the system captures two fingerprints from two different fingers. We propose a combined minutiae template generation algorithm to create a combined minutiae template from the two fingerprints. In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. The template will be stored in a database for the authentication which requires two query fingerprints. A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against a combined minutiae template.

II. METHODOLOGY

A. *System Design:*

The fig 1 below shows the enrollment phase of our system.

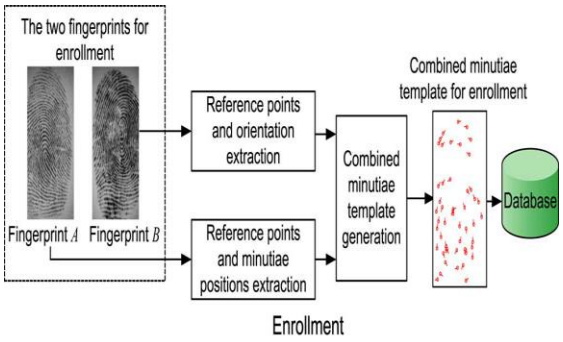

Fig 1: Enrollment phase

In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints A and B from fingers A and B respectively. 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.

The fig 2 below shows the authentication phase of our system. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints A/ and B/ from fingers A and B.

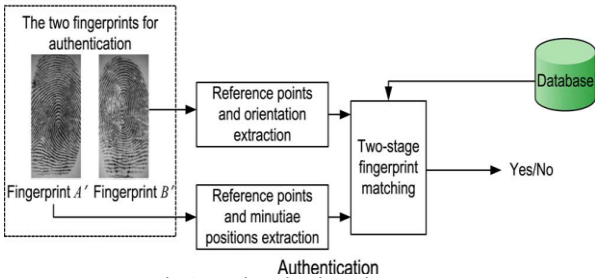

Fig 2: Authentication phase

As what we have done in the enrollment, we extract the minutiae positions from fingerprint A/ and the orientation from fingerprint B/. Reference points are detected from both query fingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching. The authentication will be successful if the matching score is over a predefined threshold.

From the above system design till now we have carried out only a few steps of the whole algorithm. They are the reading of the fingerprints and the preprocessing step. Reading of the fingerprints means we are going to take two fingerprints database images stored in our system using the MATLAB commands as we are going to perform our project in MATLAB and the preprocessing step means we are going to enhance the images of the fingerprints.

B. *Pre-processing:*

Fingerprint image quality is an important factor in performance of minutiae extraction and matching algorithms. A good quality fingerprint image has high contrast between ridges and valleys. A poor quality fingerprint image is low in divergence, noisy, exhausted, or smudgy, causing spurious and missing minutiae. Poor quality can be due to cuts, crinkles, or bruises on surface of fingertip, excessively wet or dry skin condition, uncooperative attitude of subjects, broken and impure scanner devices, little quality fingers (elderly people, manual worker), and other factors. Image enhancement techniques are employed to decrease noise and enhance the definition of ridges against valleys. In order to ensure good performance of ridge and minutiae extraction algorithms in poor quality fingerprint images, an enhancement algorithm to improve clarity of ridge structure is necessary.

Pre-processing is an important step for fingerprint recognition system. It enhances the quality and produces an image in which minutiae can be detected correctly. The pre-processing step we are going to apply separately for both the fingerprints. First we are going to carry out pre-processing of fingerprint A and then we are going to carry out the pre-processing of fingerprint B.

A fingerprint image contains regions of different excellence. They are:

1) Well-defined region
2) Recoverable region
3) Unrecoverable region.

Well-defined regions, recoverable regions and unrecoverable regions may be identified according to image contrast, alignment consistency, ridge frequency, and other local features. The principal aim of enhancement is to improve the clarity of ridge in the recoverable area in the image and to assign the unrecoverable ridges as a noisy area. Recoverable region is considered when ridges and valleys are corrupted by a small amount of dirt, ceases, or other kind of noise. Unrecoverable region are the regions which are impossible to recover them from a very corrupted and noisy image. The output of the pre-processing is a grey-

scale image or a binary image. We are going to use filters for the purpose of pre-processing. We are going to get the enhanced image at the output of the pre-processing so we can clearly identify the ridges and minutiae position of the fingerprints and we can process on this easily.

III. CONCLUSION & FUTURE WORK

We can see that pre-processing produces better images which are clearer and identifying minutiae points from them are easy. By following these steps sequentially, we can detect true minutiae points which will produce accurate results. Further we are going to extract the orientation for one fingerprint and minutiae from other fingerprint and reference point from both fingerprints and for a combined minutiae template and store it in database. In authentication we require two query fingerprints. A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against a combined minutiae template stored in database.

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

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

[5] Amber Habib, Ijlal Shahrukh Ateeq, Kamran Hameed
Sir Syed University of Engineering and Technology, Department of Biomedical Engineering, "Biometric Security System based on Fingerprint Recognition" International Journal of Scientific Engineering and Technology (ISSN : 2277-1581) Volume No.2, Issue No.9 1 Sept. 2013.

[6] 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.