*IOSR Journal of Computer Engineering (IOSR-JCE)*
*e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 2, Ver. V (Mar – Apr. 2015), PP 75-78*
*www.iosrjournals.org*

# Biometric Fingerprint Combination to Improve Anonymity Protection

Urmila M. Sawant[1], Kalyan K. Pattekar[2], Prof. S. D. Sapkal[3], Dr. R. R. Deshmukh[4]

[1](PG Scholar, Department of CSE, Government College of Engineering, Aurangabad, India)
[2](PG Scholar, Department of CSE, Government College of Engineering, Aurangabad, India)
[3](Assistant Professor, Department of CSE, Government College of Engineering, Aurangabad, India)
[4](Professor, Department of Computer Science & Information Technology, Dr. BAMU, Aurangabad, India)

***Abstract:*** *Fingerprint techniques are widely used in authentication systems, therefore its privacy protection becomes an important issue. Securing a stored fingerprint template is very important because once fingerprints are compromised, it cannot be easily revoked. So, we review here a new system for preserving fingerprint confidentiality. In this system, the fingerprint privacy is maintained by combining two different fingerprints into a new identity. In the enrollment phase, two fingerprints are taken from two different fingers. We obtain the minutiae positions of one fingerprint, the orientation of another fingerprint, and the reference points from both fingerprints. Based on the obtained information, a combined minutiae template is generated and stored in a database. In the authentication phase, we use the fingerprints of the same fingers that are already used in enrollment phase. For matching the two query fingerprints against a combined minutiae template, a two-stage fingerprint matching process is used. By storing the combined minutiae template in the database, the complete minutiae characteristic of a single fingerprint will not be compromised when the database is stolen by the attackers. The attacker cannot distinguish a combined minutiae template from the original minutiae templates as there is a similarity in topology. The combined minutiae template is converted into a real-look alike combined fingerprint by using existing fingerprint reconstruction approach. This results into a new virtual identity for the two different fingerprints. This new virtual identity can be matched using minutiae-based fingerprint matching algorithms. The main objective of this paper is to review the fingerprint privacy protection schemes.*

***Keywords:*** *Combination, Fingerprint, Minutiae, Privacy protection.*

## I. Introduction

In the field of biometric identification, fingerprints are the most widely used form of biometric trait. Therefore its privacy becomes an important issue. Conventional encryption is not enough for protecting fingerprint privacy as decryption is necessary before the fingerprint matching, which reveals the fingerprint to the attacker. In recent years, different techniques have developed to maintain the privacy of the fingerprint. Some of these techniques are based on keys and some of them are used without using key. Most of these techniques that uses key create inconvenience. The schemes [2] – [5] are used to protect fingerprint privacy using a key. Teoh et al. [2] propose a biohashing approach which is mainly depends on key. This technique is vulnerable if key is stolen by the attacker. Ratha et al. [3] propose to create cancelable fingerprint templates by applying noninvertible transforms on the minutiae, this noninvertible transfom is guided by a key. If both the key and transformed template are stolen, the work in [2] and [3] are vulnerable to intrusion and linkage attacks. Nandkumar et al. [4] propose to create fuzzy fault on the minutiae, which is vulnerable to key-inversion attack. Sheng Li et al. [5] propose to hide the user identity on the thinned fingerprint using a key. If both the key and protected thinned fingerprint are stolen, the identity of the user may be compromised.

The schemes [6] – [10] are used to protect fingerprint privacy without using a key. Ross and Othman [6] propose to use visual cryptography for privacy protection of biometrics. It uses two separate databases to store two noise-like images, formed by decomposing the fingerprint image by using visual cryptography. The identity of the biometrics is never reveled to the attacker in a single database. Practically, it is impossible that two separate databases to work together. The work in [7] – [9] combine two different fingerprints into a new identity either in feature level [7] or in the image level [8], [9]. In [7], two minutiae positions of two different fingerprints are combined to create a new identity. In new identity, the original minutiae positions of each fingerprint can be protected. The newly created identity is distinguished from the original fingerprint because it contains more minutiae positions than that of original fingerprint. And therefore it is not difficult for an attacker to identify such a newly created identity. When we manually label the original minutiae positions from the original fingerprint, the EER of matching new identities is 2.1%. In [10], the combination of minutiae positions

extracted from a fingerprint and the artificial points created from the voice are used to generate a new identity. In this case, the EER is under 2%.

In [8], [9], two different fingerprints are combined in the image level. Based on FM-AM model, each fingerprint is disintegrated into the continuous component and the spiral component. To create mixed identity, the continuous component of one fingerprint and spiral component of other fingerprint are combined. This technique has two advantages over techniques [7] and [10]: (i) it is difficult for the attacker to differentiate between mixed fingerprint and original fingerprint, (ii) to match two mixed fingerprints, existing fingerprint matching algorithms are applicable. But because of the change in form or amount or position of orientation and frequency between the two different fingerprints, this technique generates visually improper mixed fingerprints. The EER of matching two mixed fingerprints is about 15% and 4% if selection of fingerprints for forming mixed fingerprint is random and manual respectively [9].

## II. The Fingerprint Privacy Protection System

Fig. 1 displays fingerprint privacy protection system. In the enrollment phase, two fingerprints A and B are captured from two different fingers A and B respectively.

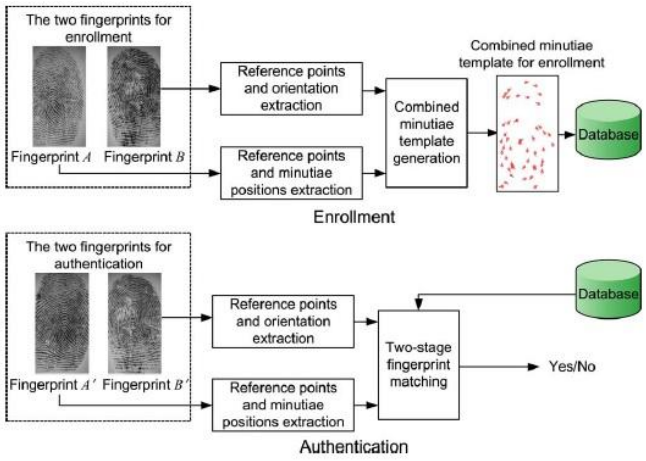


**Fig. 1.** Fingerprint Privacy Protection System.

Minutiae positions and orientation are obtained from fingerprint A and B respectively. Reference points are obtained from both the fingerprints A and B. A combined minutiae template is created by using minutiae positions from fingerprint A, orientation from fingerprint B, and reference points from both fingerprints A and B. Finally, this template is stored in the database. In the authentication phase, two query fingerprints A' and B' are captured from the same two fingers A and B. The information like minutiae positions from fingerprint A', orientation from fingerprint B', and reference points from both the fingerprints A' and B' are obtained. This information is matched against the corresponding template which is stored in the database by using two-stage fingerprint matching. If the matching score is over a predefined threshold, the authentication process will be successful. With this technique, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen by the attackers. And therefore, it maintains the fingerprint privacy.

### 1. Reference points detection

The reference points are detected in both enrollment and authentication phase as follows:

- The orientation is determined from the fingerprint by using orientation estimation algorithm.
- The certainty map of reference map is determined.
- Improved certainty map is determined.
- Detect a reference point based on two conditions: (i) the amplitude of the point is a local maximum, and (ii) the local maximum should be over a fixed threshold.
- Until all reference points are detected, repeat the above step.
- In any case, if no reference point is detected in above two steps, detect a reference point with maximum certainty value in the entire fingerprint image.

### 2. Combined minutiae template generation

It consists of minutiae position alignment and minutiae direction assignment.

**2.1 Minutiae Position Alignment**

Here, a reference point with the maximum certainty value is defined as the primary reference point. Therefore, two primary reference points for two different fingerprints are detected. Each minutiae point of fingerprint A is translated and rotated to have a proper alignment. Therefore, minutiae position from fingerprint A is aligned.

**2.2 Minutiae Direction Assignment**

Every aligned minutiae position is assigned with a particular direction which is the same as that of the minutiae directions from an original fingerprint.

**3. Two-stage fingerprint matching**

Two-stage fingerprint matching is used to match the two query fingerprints used in enrollment phase against a combined minutiae template stored in the database. This process includes query minutiae determination and matching score calculation.

**3.1 Query Minutiae Determination**

The query minutiae $M_Q$ is determined by taking into consideration the local features extracted for a minutiae point in combined minutiae template $M_C$. All possible pairs of reference points from fingerprint A and fingerprint B are selected and processed to determine query minutiae. The query minutiae $M_Q$ is the one which has minimum difference from combined minutiae template $M_C$.

**3.2 Matching Score Calculation**

Minutiae matching algorithm is used to calculate the matching score between query minutiae $M_Q$ and combined minutiae $M_C$.

## III. Combined Fingerprint Generation – A Virtual Identity

The minutiae positions and directions are obtained from two different fingerprints separately in a combined minutiae template generation process. These obtained minutiae positions and directions share similar topology to those from an original fingerprint. Therefore, a combined minutiae template and an original minutiae template are similar in their topology. A full fingerprint image can be reconstructed from a minutiae template [11]. By using fingerprint reconstruction technique, the combined minutiae template is converted into a real-look alike combined fingerprint image. Fig. 2 shows process to create a combined fingerprint for two different fingerprints.

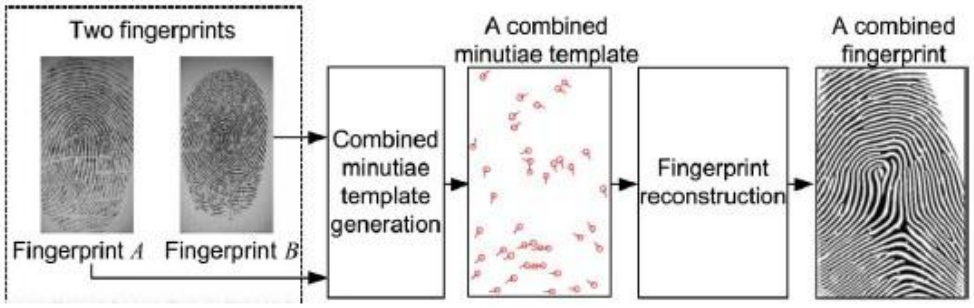


**Fig. 2.** Generating a combined fingerprint for two different fingerprints.

Initially, two different fingerprints A and B are used to generate a combined minutiae template by applying a combined minutiae template generation algorithm. Then, by applying fingerprint reconstruction technique on this combined minutiae template, a combined fingerprint is generated. This combined fingerprint issues a new virtual identity for two different fingerprints, which should be matched using minutiae-based fingerprint matching algorithms.

## IV. Conclusion And Future Scope

In this paper, we analyzed the technique for fingerprint privacy protection. It provides high level security and ensures right authentication of genuine user. Two fingerprints are combined to form a combined minutiae template which will be stored in the database. The combined minutiae template is similar in topology to an original minutiae template. Therefore, this combined minutiae template will be converted into a real-look alike combined fingerprint image. This results into a new virtual identity for the two different fingerprints. This

new virtual identity can be matched using minutiae-based fingerprint matching algorithm. To create more secured system against intruders, the present system can be enhanced by using multimodal biometric technique.

## References


[1]. Sheng Li and A. C. Kot, "Fingerprint combination for privacy protection", IEEE Transactions on Information Forensics and Security, vol. 8, no. 2, Feb 2013.

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

[3]. 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.

[4]. K. Nandakumar, A. K. Jain, and S. Pankanti, "Fingerprint-based fuzzy vault: Implementation and performance," IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–57, Dec. 2007.

[5]. S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.

[6]. A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.

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

[8]. 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.

[9]. 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.

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

[11]. S. Li and A. C. Kot, "Attack using reconstructed fingerprint," in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.