International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Combination of Fingerprints to Secure Privacy

A. N. Dalvi[1], D. G. Chougule[2]

[1]Student, Master of Engineering, Department of Electronics,
Ttyasaheb Kore Institute of Engineering & Technology, Shivaji University, Warananagar

[2]Professor, Master of Engineering, Department of Electronics, Tatyasaheb Kore Institute of Engineering & Technology Shivaji University, Warananagar

Abstract: ***In this paper the fingerprint protection security by combining two different fingerprints into another identity is discussed. Here combined template is used to strengthen the security by extracting minutiae positions and reference points from one fingerprint and orientation and reference points from other fingerprint, we generate mixed minutiae template in enrollment phase. In authentication two stage matching process is used for matching mixed template with two query fingerprints. Using existing fingerprint reconstruction technique we can convert mixed template into real combined fingerprint.***

Keywords: Fingerprint, minutiae, orientation, security, Authentication, template

1. Introduction

Distinguishing proof frameworks depend on three key components namely quality identifiers (e.g., Social Security Number, driver's permit number, and record number), personal identifiers (e.g., address, calling, training, and conjugal status), and biometric identifiers (e.g., unique mark, iris, voice, and stride, palm, face). It is fairly simple for a person to distort quality and historical identifiers; then again, biometric identifiers rely on upon inborn physiological attributes that are hard to adulterate or adjust. Computerized human recognizable proof utilizing physiological and/or behavioral attributes, biometrics, is progressively mapped to new regular citizen applications for business utilization. The life systems of human fingers is much entangled and to a great extent in charge of the singularity of fingerprints and finger veins. The high uniqueness of fingerprints has been ascribed to the arbitrary defects in the rubbing edges and valleys, which are normally eluded to as details or level-2 finger impression highlights.

As biometrics is picking up prominence, there is expanded concern over the loss of protection and potential abuse of biometric information held in focal stores. The relationship of Fingerprints with criminal raises further concerns. Then again, the option proposal of keeping biometric information in brilliant cards does not take care of the issue, since counterfeiters can simply assert that their card is broken to stay away from biometric check through and through. So it is critical to produce a superior and powerful unique fingerprint security insurance framework.

2. Literature Review

Fingerprints have long been used for person verification and identification due to their immutability and uniqueness. Minutiae-based verification approaches are the most common, compared to ridge-based and correlation based techniques. The performance of minutiae-based fingerprint verification systems heavily depend on the minutiae extraction process done before minutiae alignment. Minutiae extraction is done using image processing operations that take advantage of the rich information available in the ridge structure of a fingerprint. Fingerprint techniques in authentication employees Biohashing approach [1] where two factor authenticator based on inner products between tokenized pseudo-random number and the user specific fingerprint feature, which generated from the integrated wavelet and Fourier–Mellin transform. It produces a set of user specific compact. BioHashing highly tolerant of data capture offsets, with same user fingerprint data resulting in highly correlated bitstrings. In which there is no deterministic way to get the user specific code without having both token with random data and user fingerprint feature. The accuracy of this approach mainly depends on the key, which is assumed to be never stolen or shared [2].

Noninvertible (cancelable) transforms [3], was one of the solutions to privacy-preserving biometric authentication. Instead of storing the original biometric, it is transformed using a one-way function. The transformed biometric and the transformation are stored either distributed on a smart-card or centrally in a database. The transformation can be performed either in the signal domain or in the feature domain. This construct preserves privacy since it will not be possible (or computationally very hard) to recover the original biometric template using such a transformed version. If a biometric is compromised, it can be simply reenrolled using another transformation function, thus providing revocability. The construct also prevents cross-matching between the databases, since each application using the same biometric uses a different transformation.

Privacy is another main concern in building biometric systems, besides low error rates. Numerous architectures have been proposed in recent years, aiming to protect biometric templates stored in central repositories. Among those, fuzzy vault technique [4] is one of the most widely used methods where the fingerprint minutiae points are stored with randomly generated chaff points. A user has to provide a certain number of minutiae points to unlock the vault created by the reference fingerprints minutiae set during the enrollment session.

The use of visual cryptography [5] is explored to preserve the privacy of biometric data (viz., raw images) by decomposing the original image into noise-like which are stored in two separate databases. The original image can be revealed only when both images are simultaneously available. During the authentication process two images are overlaid (i.e., superimposed) in order to reconstruct the private image. Once the matching score is computed, the reconstructed image is discarded. But this system requires two separate databases to work together, which is not practical in same applications

High security applications require very low error rates and unimodal biometric systems are not always satisfying in that regard. In those cases, multi-modal biometric systems are useful. The combination of multiple biometrics mostly take place at the matching score or decision level. The idea of combining multiple biometrics [6] in order to increase both privacy and security. Specifically, minutiae points from two distinct fingers of the same person were combined to create a multi-biometric template which is later shown to be more unique. The original minutiae positions of each fingerprint can be protected in the new identity. Hence more privacy preserving. The system provides higher level of security as well, as it verifies both fingerprints.

Voice is a behavioral biometric which can be used in identity verification, especially over-the-phone applications such as banking. The multi-biometric template framework using fingerprint and voice-modalities [7] discusses a scheme, where the minutiae positions extracted from a fingerprint and the artificial points generated from the voice are combined to produce a new identity. Voice and fingerprint data of individuals are fused at the template level by combining minutiae points and artificially constructed points obtained from the utterance.

Image level based fingerprint combination techniques [8] [9]are used to combine two different fingerprints in the image level. First of all, each fingerprint is decomposed into the continuous component and the spiral component based on the fingerprint FM-AM model [10]. After some alignment, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint, so as to create a new virtual identity which is termed as a mixed fingerprint.

3. Proposed Methodology

3.1 Theory

The primary objective of using a biometric system is to provide authorized access. Authentication implies that (i) only legitimate or authorized users are able to access the physical or logical resources protected by the biometric system and (ii) impostors are prevented from accessing the protected resources. While a biometric system can be compromised in a number of ways, one of the potentially damaging attacks is the leakage of biometric template information. The leakage of this template information to unauthorized individuals constitutes a serious security and privacy threat. Therefore in this paper we propose a model of creating a combined minutiae template. By using the mixed minutiae template security is maintained when the database is stolen.

Fingerprints are unique to every individual. A fingerprint is the pattern of ridges and valleys on the fingertip. Each person has unique fingerprints. And this uniqueness of a fingerprint is determined by the local ridge characteristics.

- Minutiae: A Minutiae is defined as the points on a fingertip, such as bifurcations (a ridge splitting into two) and ridge endings.

- Types of ridges:
  1) Ridge Endings-A ridge that ends abruptly.
  2) Ridge Bifurcation-A single ridge that divides into two ridges.
  3) Short ridges, Island or Independent Ridge-A ridge that commences, travels a short distance and then ends.
  4) Ridge Enclosures-A single ridge that bifurcates and reunites shortly afterward to continue as a single ridge.
  5) Spur-A bifurcation with a short ridge branching off a longer ridge

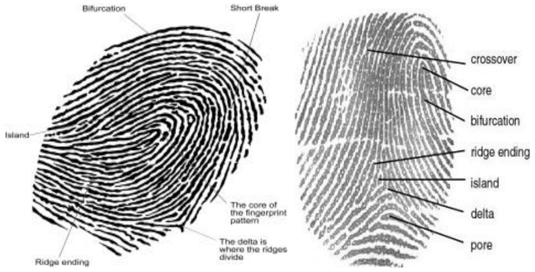

Figure 1: Minutiae Positions in Fingerprint.

3.2 Orientation

An orientation image is defined as an N x N image, where O(i, j) represents the local ridge orientation at pixel (i, j). Local ridge orientation is usually specified for a block rather than at every pixel; an image is divided into a set of w x w non-overlapping blocks and a single local ridge orientation is defined for each block. Note that in a fingerprint image, there is no difference between a local ridge orientation of 90o and 270o, since the ridges oriented at 90o and the ridges oriented at 270o in a local neighborhood cannot be differentiated from each other.

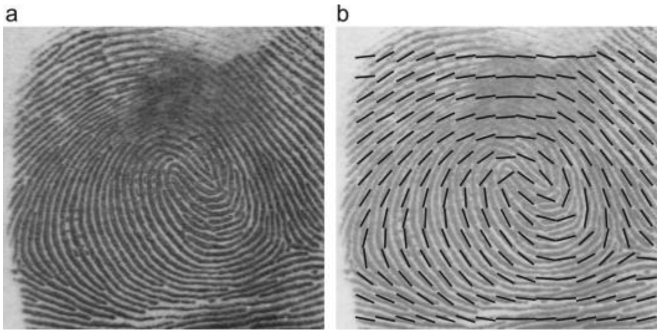

Figure 2: Orientation Field in Fingerprint

3.3 Block Diagram

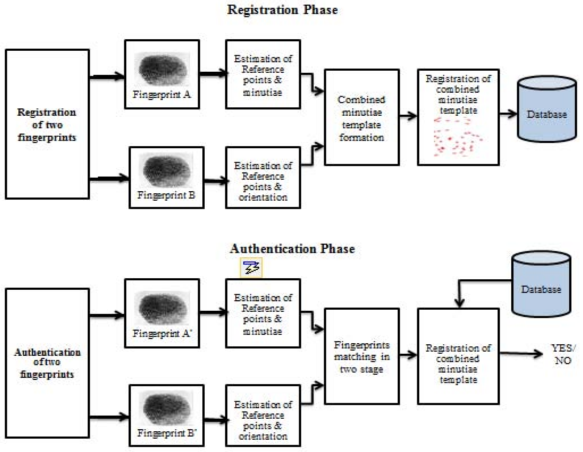
Registration Phase
Registration of two fingerprints
Fingerprint A
Fingerprint B
Estimation of Reference points & minutiae
Estimation of Reference points & orientation
Combined minutiae template formation
Registration of combined minutiae template
Database
Authentication Phase
Authentication of two fingerprints
Fingerprint A'
Fingerprint B'
Estimation of Reference points & minutiae
Estimation of Reference points & orientation
Fingerprints matching in two stage
Registration of combined minutiae template
Database
YES/ NO

Figure 3: Illustration of Registration and Authentication Process

1) Registration Phase:

This system demonstrates our proposed fingerprint security insurance framework. In the registration stage, the framework catches two fingerprints from two unique fingers, say fingerprints A and B. We separate the minutiae positions from fingerprint A and the orientation from B utilizing some current systems[11][12].At that point, by utilizing our proposed coding methodologies, a mixed minutiae template is produced taking into account the minutiae, the orientation and the reference points identified from both fingerprints. At long last, combined minutiae template is put away in a database.

2) Authentication Phase

In the validation stage, two query fingerprints are needed from the same two fingers, say fingerprints A' and B' from fingers A and B. As what we have done in the registration, we separate the minutiae points from A' and orientation from B'. Reference points are recognized from both quiry fingerprints. These extracted data will be coordinated against the comparing format put away in the database by utilizing a two-stage fingerprint matching. The verification will be effective if the matching score is over a predefined edge.

Design Considerations:

The system modules include following processes,

- Reference Points Detection In Registration Phase.
- Mixed Minutiae Template Formation.
- Reference Points Detection For Authentication Process.
- Two stage Fingerprint Verification.

A.Reference Points Detection In Registration Phase:

Input image is converted into grayscale image and normalization process is used to change the range of pixel intensity values i.e. Contrast stretching. Followed by following processes.

1) *Orientation Estimation Algorithm-* Orientation of fingerprint is computed from normalized image.
2) *Reference Points Detection*-Finally reference points are fetched from fingerprint [13].

B.Mixed Minutiae Template Formation-

The mixed minutiae template is formed by using extracted information from both fingerprints and by taking alignments of minutiae position and minutiae direction.

1) Alignment of Minutiae position-

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

2) Alignment of Minutiae Direction -

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

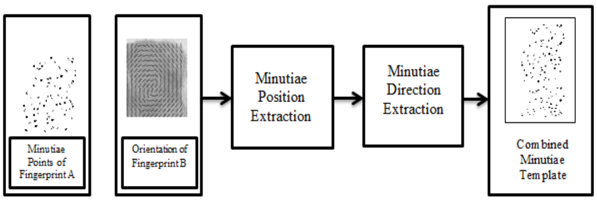
Minutiae Points of Fingerprint A
Orientation of Fingerprint B
Minutiae Position Extraction
Minutiae Direction Extraction
Combined Minutiae Template

Figure 4: Mixed Minutiae Template Formation

C.Reference Points Detection For Authentication Process

Here reference points are extracted from two query fingerprints for authentication purpose.

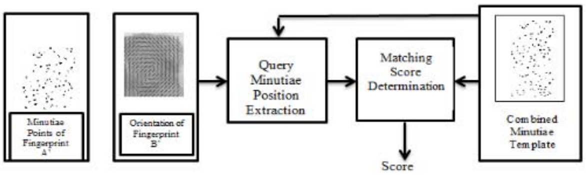
Minutiae Points of Fingerprint A'
Orientation of Fingerprint B'
Query Minutiae Position Extraction
Matching Score Determination
Combined Minutiae Template
Score

Figure 4: Two-Stage Fingerprint Matching Process

- *Query Minutiae Points Detection:* Extracting local minutiae points of query fingerprints this verification is started. The feature extraction is carried out using work proposed in [14].
- *Matching Rating Calculation*: Minutiae matching process is used to rate minutiae matching of minutiae points stored as combined template in database against minutiae points of query fingerprints.

D.Two stage Fingerprint Verification

Two stage fingerprint matching process of minutiae stored against query minutiae points is carried out.

4. Conclusion

In this paper combination of two fingerprints is carried out for privacy protection. During registration process two fingerprints of two different fingers are taken. From which some minutiae and reference points are taken from each finger and one mixed template is formed which look like an original minutiae template.

During authentication process two fingerprints of same two fingers are taken. These fingerprints are combined to form a template of minutiae and this template is used to compare with database. As the mixed minutiae template is matching with original database minutiae template so that we can use combination of fingerprints as a new identity for privacy protection.

References

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

[2] 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.

[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. Forensic Security*, vol. 2, no. 4, pp. 744–57, Dec. 2007.

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

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

[7] 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.

[8] K. G. Larkin and P. A. Fletcher, "A coherent framework for fingerprint analysis: Are fingerprints holograms?, " *Opt. Express*, vol. 15, pp. 8667–8677, 2007.

[9] VeriFinger 6.3. [Online]. Available: http://www.neurotechnology.com

[10] 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.

[11] K. Nilsson and J. Bigun, "Localization of corresponding points in fingerprints by complex filtering, " *Pattern Recognit. Lett.*, vol. 24, no. 13, pp. 2135–2144, 2003.

[12] X. Jiang and W.Yau, "Fingerprint minutiae matching based on the local and global structures," in *Proc. 15th Int. Conf. Pattern Recognition*, 2000, vol. 2, pp. 1038–1041.