ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Privacy Protection of Fingerprint by Merging Two Fingerprints & Generate New Identity

Achut B. Gavhane [1], Ravindra P. Shelkikar [2]

PG Student, Department of Electronics and Telecommunication Engineering, TPCT's College of Engineering, Osmanabad (M.S.) India [1]

Associate Professor, Department of Electronics and Telecommunication Engineering, TPCT's College of Engineering, Osmanabad, (M.S.), India [2]

ABSTRACT: In this paper, we propose here a novel system for privacy protection of fingerprint by merging two fingerprints & generate new identity. In the enrollment phase, two fingerprints are taken from two different fingers of one person. From one fingerprint we extract the minutiae positions, from the other fingerprint we extract the orientations, and from both fingerprints we extract the reference points. From this extracted information and our coding strategies, we generate combined minutiae template and that generated combined minutiae template stored in a database. During authentication phase, the system requires two query fingerprints from the same two fingers of one person which are used during enrollment phase. A two-stage fingerprint matching system is used for matching the two query finger-prints from the same two fingers of one person against a combined minutiae template which is stored in database. By storing the combined minutiae template in the database, the complete minutiae positions of a single fingerprint will not be compromised when the database is stolen. Furthermore, because of the similarity in topology, it is very difficult for the attacker to differentiate a combined minutiae template from the original minutiae templates. With the help of an existing fingerprint reconstruction approach, we are able to reconstruct the combined minutiae template into a new virtual identity of merged fingerprints. Thus, a new virtual identity is generated from merging the two different fingerprints of one person, which can be matched using minutiae-based fingerprint matching algorithms. The experimental results shows that our system can achieve a very low error rate. Our work has the advantage in creating a better new identity when the two different fingerprints are randomly chosen as compared with the state-of-the-art technique.

KEYWORDS: biometrics, fingerprint, minutiae extraction, orientation.

I. INTRODUCTION

The main objective of this system is to prevent an attacker to compromise privacy of users or biometric data and not necessarily to the art by passing of the biometric authentication itself. The objective of this research is to develop a fingerprint combination & matching system using MATLAB. Beginning with input fingerprint images, the system processes the data and collects the minutiae positions, orientations & reference points from the fingerprint images. Fingerprints are the most widely used biometric characteristic. Fingerprint combination is a complex pattern recognition problem; designing algorithms capable of extracting salient features and matching them in a robust way is quite hard. With the widespread applications of fingerprint techniques in authentication phase, protecting the privacy of the fingerprint becomes an very important issue. Traditional encryption is insufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. Therefore, in recent years, significant efforts have been put into developing specific protection techniques for fingerprint. Most of the existing techniques make use of the key for the fingerprint privacy protection, which creates the inconvenience. They may also be vulnerable when both the key and the protected fingerprint are stolen. Teoh propose a bio-hashing approach by computing the inner products between the user's fingerprint features and a pseudorandom number (i.e., the key). The accuracy of this approach mainly depends on the key, which is assumed to be never stolen or shared. Some authors propose to generate cancellable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. The work shown to be vulnerable to intrusion and linkage attacks when both the key and the transformed template are stolen.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Some authors propose to implement fuzzy fault on the minutiae, which is vulnerable to the key-inversion attack. Our work imperceptibly hides the user identity on the thinned fingerprint using a key. The user identity may also be compromised when both the key and the protected thinned fingerprint are stolen. There are only a few schemes that are able to protect the privacy of the fingerprint without using a key. Ross and Othman propose to use visual cryptography for protecting the privacy of biometrics. The fingerprint image is decomposed by using a visual cryptography scheme to produce two noise-like images (termed as sheets) which are stored in two separate databases. During the authentication, the two sheets are overlaid to create a temporary fingerprint image for matching. The advantage of this system is that the identity of the biometrics is never exposed to the attacker in a single database. However, it requires two separate databases to work together, which is not practical in same applications. The works combine two different fingerprints into a single new identity either in the feature level or in the image level. In the concept of combining two different fingerprints into a new identity is first proposed, where the new identity is created by combining the minutiae positions extracted from the two fingerprints. The original minutiae positions of each fingerprint can be protected in the new identity. However, it is easy for the attacker to identify such a new identity because it contains many more minutiae positions than that of an original fingerprint. The experiment shows that the EER of matching the new identities is 2.1% when the original minutiae positions are marked manually from the original fingerprints. A similar scheme is proposed where the minutiae positions extracted from a fingerprint and the artificial points generated from the voice are combined to produce a new identity. In this work, the EER are shown to be fewer than 2% according to the experimental results. In the authors first propose 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. The identification of people by measuring some traits of individual anatomy, physiology or other behavioural characteristics has led to a specific research area called biometric recognition. Biometric technologies provide a strong mechanism for authentication and are still under continuous development. Their diffusion is mainly supported by governments, forensics and law enforcement agencies with the aim of improving the public security or in general a sense of security; in fact, the biometric identification does not directly improve the security but acts as deterrent to illegal activities.

II. RELATED WORK

In Existing system, contain only password authentication. So the hackers easily hack out password and communication to authentication server. So this system didn't provide fully supported security to users. The previous work on "Combining multiple biometrics to protect privacy," used to combine two different fingerprints into a single new identity in the feature level. Image level based fingerprint combination techniques proposed in "Mixing fingerprints for template security and privacy," and "Mixing fingerprints for generating virtual identities," are used to combine two different fingerprints in the image level. Teoh *et al.* [2] propose a biohashing approach by computing the inner products between the user's fingerprint features and a pseudorandom number (i.e., the key). The accuracy of this approach mainly depends on the key, which is assumed to be never stolen or shared. A. Kong *et al.* [3] propose the growing demand for accurate and reliable personal authentication, biometric recognition, a substitute for or complement to existing authentication technologies, have attracted considerable attention. It has recently been reported that, along with its variants, BioHashing, a new technique that combines biometric features and a tokenized (pseudo-) random number (TRN), has achieved perfect accuracy, having zero equal error rates (EER) for faces, fingerprints and palm prints. Ratha *et al.* [4] propose to generate cancellable fingerprint templates by applying noninvertible transforms on the minutiae. The noninvertible transform is guided by a key, which will usually lead to a reduction in matching accuracy. Demonstrate several methods to generate multiple cancellable identifiers from fingerprint images to overcome these problems. In essence, a user can be given as many biometric identifiers as needed by issuing a new transformation "key." The identifiers can be cancelled and replaced when compromised. It is also shown that the transforms are noninvertible by demonstrating that it is computationally as hard to recover the original biometric identifier from a transformed version as by randomly guessing.

III. PROPOSED METHODOLY

The following Block diagram shows enrollment & authentication phases for privacy protection of fingerprint by merging two fingerprints.

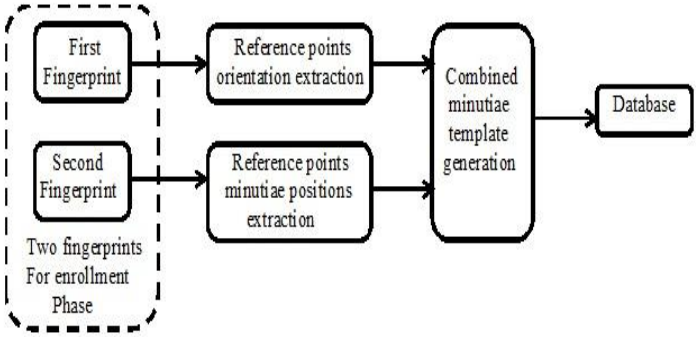
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

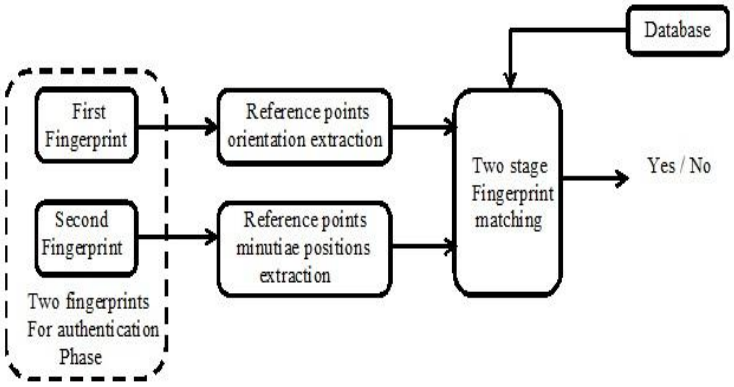
(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Fig. 3.1 shows our proposed privacy protection of fingerprint by merging two fingerprints. In the enrollment phase, the system captures two fingerprints from two different fingers, say fingerprints and from fingers and respectively.



Enrollment Phase



Authentication Phase

Fig.3.1 - Proposed system for privacy protection of fingerprint by merging two fingerprints.

We extract the minutiae positions from fingerprint and the orientation from fingerprint using some existing techniques. Then, by using our coding strategies, we generate combined minutiae template is 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. In the authentication phase, two query fingerprints are required from the same two fingers, say fingerprints and from fingers and. As what we have done in the enrollment, we extract the minutiae positions from fingerprint and the orientation from fingerprint. 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.

IV. MERGED FINGERPRINT GENERATION

In a combined minutiae template, the minutiae positions and directions (after modulo) are extracted from two different fingerprints separately. These minutiae positions and directions share a similar topology to those from an original fingerprint. Therefore, the combined minutiae template has a similar topology to an original minutiae template. Some existing works have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. By adopting one of these fingerprint reconstruction approaches, we are able to convert our combined minutiae template into a combined fingerprint image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

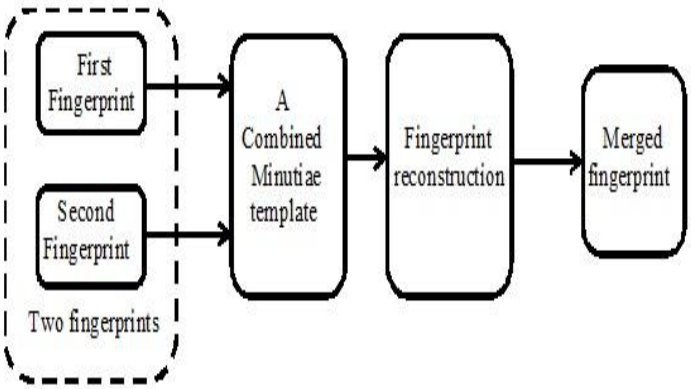


Fig. 4.1 Generating a merged fingerprint from two different fingerprints.

Fig. 4.1 shows our process to generate a combined fingerprint for two different fingerprints. Given any two different fingerprints as input, we first generate a combined minutiae template using our combined minutiae template generation algorithm. Then, a combined fingerprint is reconstructed from the combined minutiae template using one of the existing fingerprint reconstruction approaches. It should be noted that the combined minutiae template generated by adopting *Coding Strategy* 1 is not appropriate for generating a combined fingerprint. The reason is that we set as 0 or 1 randomly during the minutiae direction assignment, i.e., we add randomly for each minutiae direction in such a coding strategy. We need to perform a modulo operation for the minutiae directions during the fingerprint matching, so as to remove such randomness. Therefore, we will not be able to match the corresponding combined fingerprint by using a general fingerprint matching algorithm. While the purpose of generating a combined fingerprint is to issue a new virtual identity for two different fingerprints, which should be matched using general fingerprint matching algorithms. Among the existing fingerprint reconstruction approaches, our previous work achieves excellent performance. We here adopt this approach for generating a combined fingerprint from a combined minutiae template. However, the work does not incorporate a noising and rendering step to make the reconstructed fingerprint image real-look alike.

V. RESULT AND DISCUSSION

To create a real-look alike fingerprint image from a set of minutiae points, we further use GUI template in matlab. Here we create a one main GUI window for our project as illustrated in Fig. 5.1

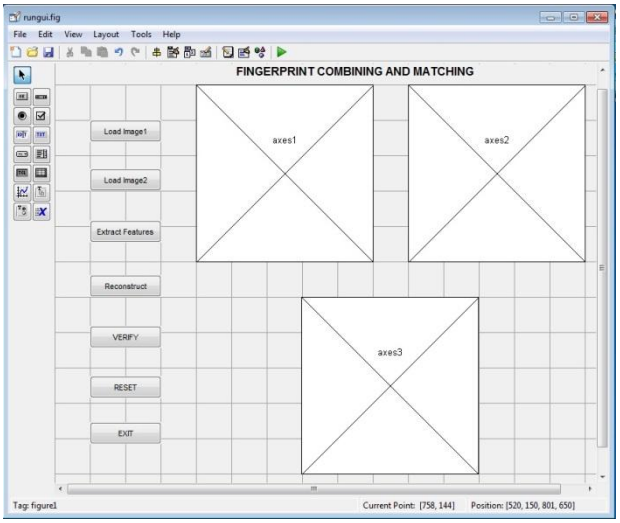


Fig. 5.1 Main GUI window.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

5.1 Steps for extraction of minutiae positions & orientation

1) Load first fingerprint through load image 1 button from the database.
2) Load second fingerprint through load image 2 button from the database.
3) Extract the minutiae points from first fingerprint, & extract the orientations from second fingerprint.
4) Extract reference points from both fingerprints & estimate an orientation field *O* from the set of minutiae points thus combined minutiae template is generated.
5) This generated template is stored in database for further verification process.
6) Reconstruct the image from these two fingerprints i.e new identity or merged fingerprint.
7) After reconstruction of image it verifies by two query fingerprints with template stored in database.
8) Thus results come out verified if it is verified otherwise not verified.

The experiment is conducted on the first two impressions stored in database, which contains 20 fingerprints from 10 fingers (with 2 impressions per finger). The VeriFinger6.3 is used for the minutiae positions extraction and the minutiae matching in FVC 2002 database.

5.2 Examples of privacy protection of fingerprint by merging two fingerprints

For this project we have taken 20 fingerprints of 10 peoples for implementation. Some of them explained here with enrollment, combined minutiae template, reconstruction of fingerprints i.e merged fingerprint & verification.

5.2.1 Example 1

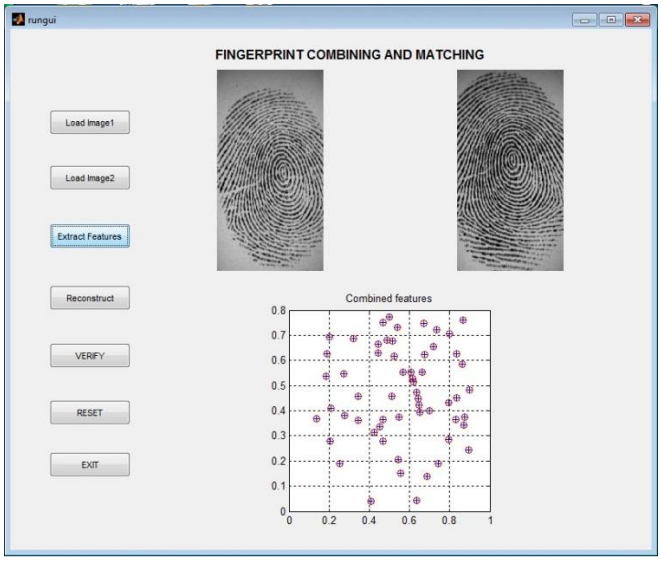


Fig. 5.2 Enrollment of two fingerprints to generate combined minutiae template & stored in database.

Here select two fingerprints for enrollment phase of user 1 as shown in following fig. 5.2

1) Load first fingerprint through load image 1 button from the database.
2) Load second fingerprint through load image 2 button from the database.

After giving two fingerprints as input follow the following steps & result is as shown in following fig. 5.2

3) Extract the minutiae points from first fingerprint, & extract the orientations from second fingerprint.
4) Extract reference points from both fingerprints & estimate an orientation field *O* from the set of minutiae points thus combined minutiae template is generated.
5) This generated template is stored in database for further verification process.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

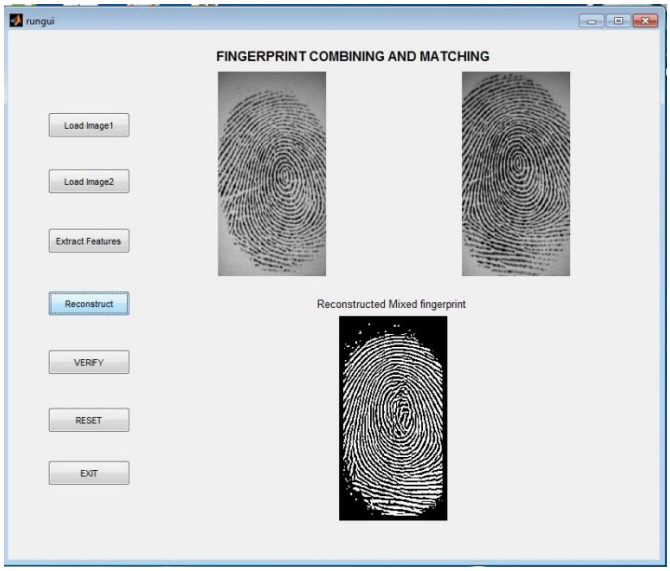


Fig. 5.3 Reconstruction of enrolled fingerprints stored in database.

After enrollment of fingerprints reconstruct the image from these two fingerprints i.e new identity or merged fingerprint as shown in following fig. 5.3
For each group of finger pairs, consider the same two cases for enrollment i.e.,
1) The first impressions of each finger pair are used to produce only one combined fingerprint for enrollment. The corresponding second impressions are used to generate a query combined fingerprint.
2) The first impressions of each finger pair are used to produce two combined fingerprints for enrollment. The corresponding second impressions are used to generate two query combined fingerprints.

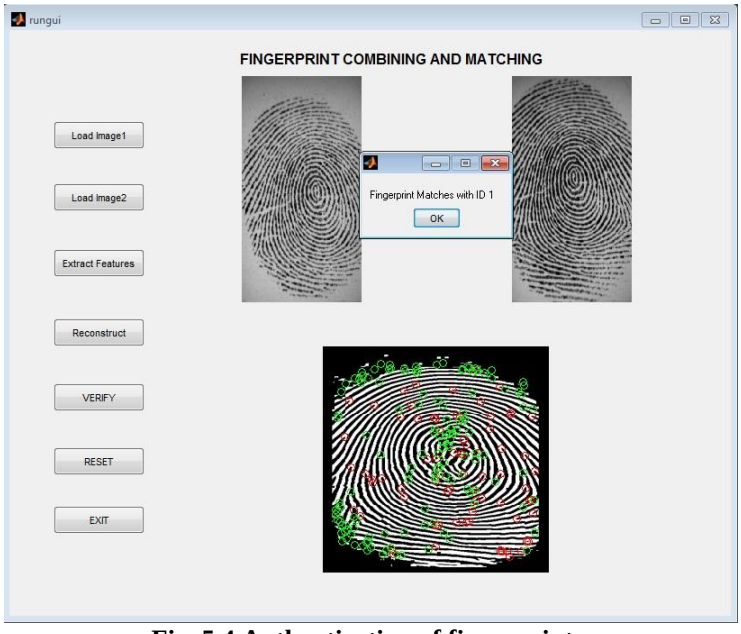


Fig. 5.4 Authentication of fingerprints.

1) After reconstruction of image it verifies by two query fingerprints with template stored in database.
2) Thus results come out verified if it is verified otherwise not verified as shown in following fig. 5.4

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

When results from identification or verification procedures are discussed, the following terms will be used in this report:

Success rate: The rate at which successful verifications or identifications are made compared to the total number of trials.

False rejection rate (FRR): The rate at which the system falsely rejects a registered user compared to the total number of trials.

False acceptance rate (FAR): The rate at which the system falsely accepts a nonregistered (or another registered) user as a registered one compared to the total number of trials. The FAR is in this report used in the identification version, as a contrast to verification procedures, where it measures if a user is accepted under a false claimed identity.

Equal error rate (EER): The common value of the FAR and FRR when the FAR equals the FRR. This is the value where both the FAR and FRR are kept as low as possible at the same time (see fig. 5.7). A low EER value indicates a high accuracy of the system.

VI. CONCLUSION

In this paper, we introduce a novel system for privacy protection of fingerprint by merging two different fingerprints into a new virtual identity. During enrollment phase, the system captures two fingerprints from two different fingers. Combined minutiae template generated based on minutiae feature, orientations feature & reference points of the two fingerprints will be generated and stored in a database. To make the combined minutiae template look real as an original minutiae template, three different coding strategies are introduced during the combined minutiae template generation process. During authentication process, two query fingerprints from the same two fingers of that person which we have taken in enrollment are required. A two-stage fingerprint matching system is proposed for matching the two query fingerprints against the enrolled template stored in database. Stored combined minutiae template has a similar topology to an original minutiae template. Therefore, we are able to combine two different fingerprints into a new virtual identity by reconstructing a real-look alike combined fingerprint from the combined minutiae template. The experimental result shows that our system can achieve a very low error rate with false rejection rate. Our work has the advantage in creating a better new identity when the two different fingerprints are randomly chosen as compared with the state-of-the-art technique.

REFERENCES

[1] Sheng. Li and Alex. C. Kot, "Fingerprint Combination for Privacy Protection," IEEE Trans. Inf. Forensics Security, vol. 8, no. 2, pp. 350-360, 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] 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.
[6] S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 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.