iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** XII **Month of publication:** December 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Review Paper on Fingerprints for Privacy Protection

Ujma A. Mulla[1]
[1]PG Student of Electronics Department of, B.I.G.C.E., Solapur, Maharashtra, India

Abstract –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.
Keywords: fingerprint, minutiae extraction, orientation, privacy, protection.

I. INTRODUCTION

The Greek word “biometrics” is divided it into two roots: “bio” means life and “metrics” means to measure. Biometrics refers to technologies for measuring, and analyzing a person's physiological or behavioral characteristics. These unique characteristics are used to verify and identify to individuals. Fingerprints are most commonly represented by a set of points, called minutiae. At present many Fingerprint Authentication Systems are based on minutiae matching. Minutiae are generally indicated as the terminations and bifurcations of the ridge lines in a fingerprint image. The two most important local ridge characteristics of minutiae are the ridge ending and the ridge bifurcation unique. Ridge ending is termed as the point where the ridge ends abruptly. Ridge bifurcation is termed as the point where a ridge forks or diverges into branch ridges. A fingerprint authentication system can be generally divided into two parts namely

A. Enrollment

B. Identification or Verification

The enrollment part is responsible for registering individuals into the biometric system. In this enrollment phase, the characteristic of an individual is first scanned by a biometric reader to produce a raw digital representation of the characteristic. Fingerprint verification is to verify the authenticity of one person by his fingerprint.

A novel system is proposed for providing privacy to the fingerprint biometric system by combining two different fingerprints into a new identity. The system captures two fingerprints from two different fingers which may be from same person or from different person while registering. The combined minutiae template is generated based on three features. In such a combined template, the minutiae positions are extracted from one fingerprint, while the orientation from other fingerprint and reference points from both the fingerprints. The template will be stored in a database for authentication which requires two query fingerprints during verification.

II. RELATED WORK

"Combining Multiple Biometrics to Protect Privacy"- B. Yanikoglu and A. Kholmatov,-2004

In this work a biometric authentication framework which uses two separate biometric features, combined to obtain a non-unique identifier of the individual, in order to address privacy concerns. As a particular example, we demonstrate a fingerprint verification system that uses two separate fingerprints of the same individual. A combined biometric ID composed of two fingerprints is stored in the central database, and imprints from both fingers are required in the verification process, lowering the risk of misuse and

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

privacy loss. We demonstrate the performance of the proposed method on only a small fingerprint database.

"Mixing fingerprints for generating virtual identities,"- A. Othman and A. Ross,-2011

This work explores the possibility of mixing two different fingerprints at the image level in order to generate a new fingerprint. To mix two fingerprints, each fingerprint is decomposed into two different components, viz., the continuous and spiral components. After pre-aligning the components of each fingerprint, the continuous component of one fingerprint is combined with the spiral component of the other fingerprint image.

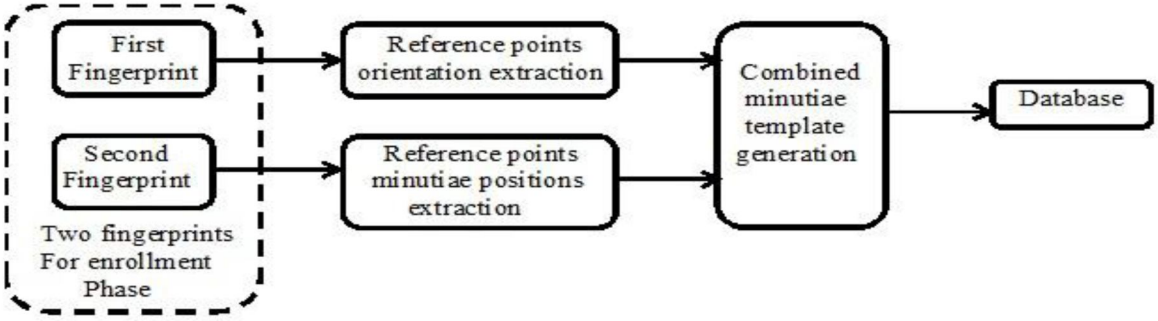
"Fingerprint image reconstruction from standard templates,"- R. Cappelli, A. Lumini, D. Maio, and D. Maltoni,-2007

A minutiae-based template is a very compact representation of a fingerprint image, and for a long time, it has been assumed that it did not contain enough information to allow the reconstruction of the original fingerprint. This work proposes a novel approach to reconstruct fingerprint images from standard templates and investigates to what extent the reconstructed images are similar to the original ones (that is, those the templates were extracted from). The efficacy of the reconstruction technique has been assessed by estimating the success chances of a masquerade attack against nine different fingerprint recognition algorithms.

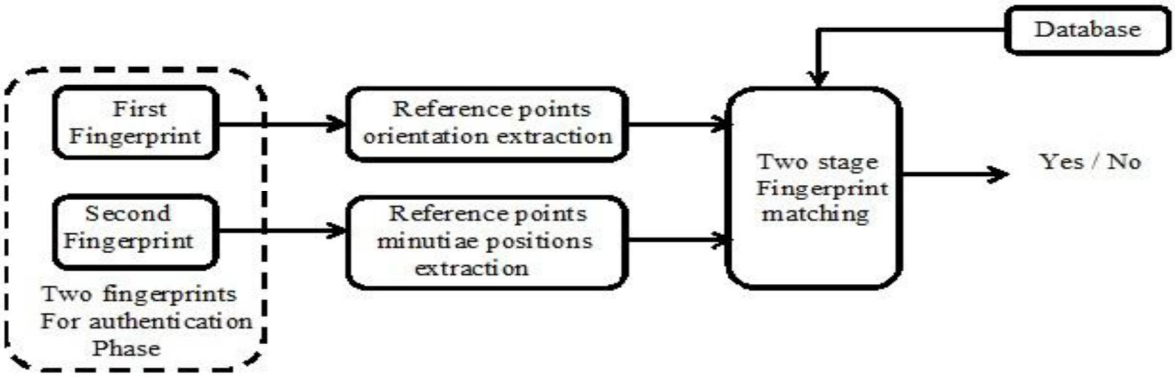
III. THE PROPOSED FINGERPRINT PRIVACY PROTECTION SYSTEM

Identification systems rely on three key elements: 1) attribute identifiers (e.g., Social Security Number, driver's license number, and account number), 2) biographical identifiers (e.g., address, profession, education, and marital status), and 3) biometric identifiers (e.g., fingerprint, iris, voice, and gait). It is rather easy for an individual to falsify attribute and biographical identifiers; however, biometric identifiers depend on intrinsic physiological characteristics that are difficult to falsify or alter.

This paper deals with combined fingerprint which requires two fingerprints used for verification and authentication and minutiae positions from one fingerprint, the orientation from the other fingerprint. Based on this extracted information, a combined template is generated and stored in database. In the verification phase, the system requires two query fingerprints from the fingers which are used in the enrolment. The fingerprint matching process is done by minutiae based fingerprint matching algorithms. By storing the combined template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.



Enrollment Phase



Authentication Phase

Fig.1 - Proposed system for privacy protection of fingerprint by merging two fingerprints.

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig.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.

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

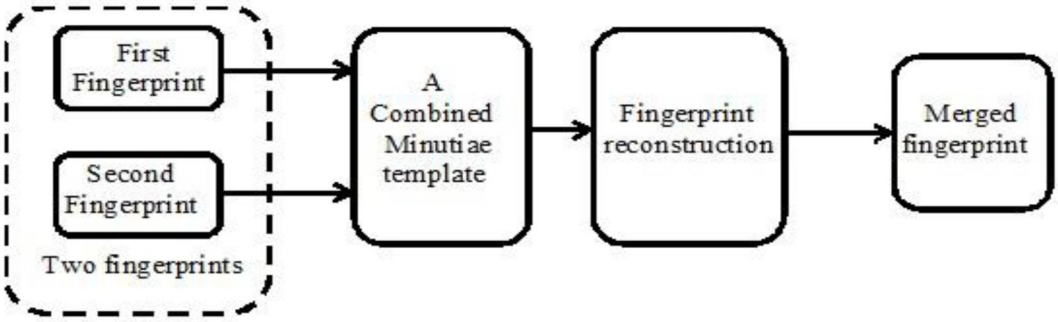


Fig.2 - Generating a merged fingerprint from two different fingerprints.

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.

V. ALGORITHM

The algorithms used in the system are,

A. Minutiae Points Detection Algorithm

A Minutia is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings.

Volume 4 Issue XII, December 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig.3 – Minutiae Position in fingerprint.

The proposed algorithm focuses on minutiae-based method. In particular, we are interested in the most important minutia features: ridge ending and bifurcation. When the curve of a ridge is traced, the radius R of curvature is equal to the distance w of the neighboring ridge. Every point of the current tracing ridge is continuously traced in turn.

B. Orientation Estimation Algorithm

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 90^o and 270^o, since the ridges oriented at $90^o$and the ridges oriented at 270^o in a local neighborhood cannot be differentiated from each other.

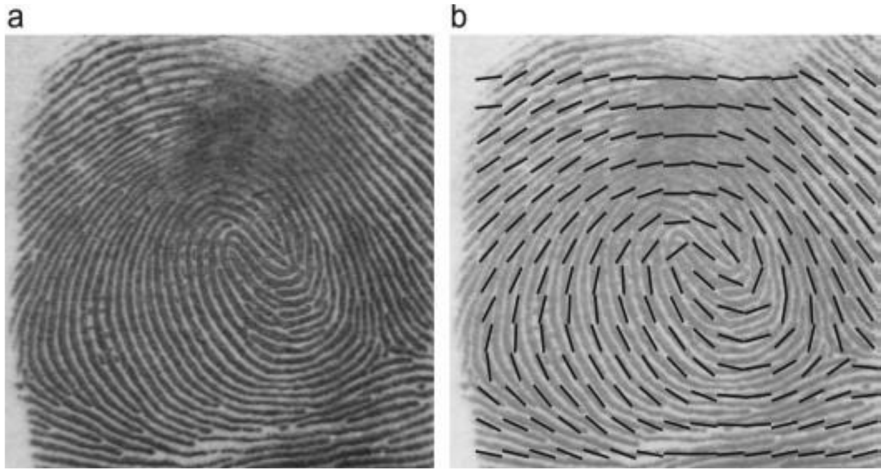


Fig.4 – Orientation field in fingerprint.

C. Combined Minutiae Template Generation Algorithm

Given a set of N minutiae positions PA = { **p**ia = xia ,yia , , 1 ≤ i ≤ N}, of fingerprint A, the orientation OB of fingerprint B and a combined minutiae template MC is generated by minutiae position alignment and minutiae direction assignment.

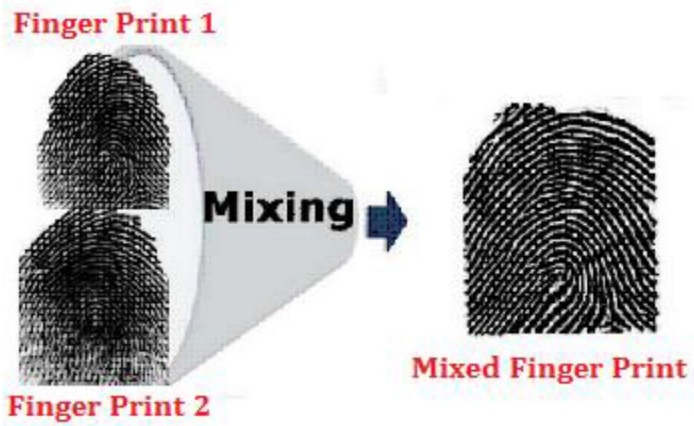


Fig.5 – Combined minutiae template.

D. Minutiae-Based Fingerprint Matching Algorithms

Two types of minutiae features are extracted, which are ridge endings and bifurcations. The minutiae are marked using a 3 x 3 pixels window to extract ridge ending and bifurcation.

Prior to the matching process, minutiae alignment is executed to improve the robustness of image rotation between the processed image and those available in the database for more accurate fingerprint matching. In order to match an input image to those in the database, the core points of both fingerprint images are chosen as reference point to align and rotate the minutiae position until a

match of a major minutiae point is achieved. Using the coordinate system calculation, when the similarity is larger than a set threshold, a new set of coordinates of the minutiae points is recalculated using the reference point as the origin, and the x-axis is set to coincide with the direction of the reference point. After aligning the minutiae points, the fingerprint image are matched to those in the database for either identification (one-to-many matching) or verification (one-to-one matching). Two matching scores are used, namely the percentage of similarity matching score and the Euclidean distance. Along with this score computation, the Euclidean distance between all minutiae features of those in the input image and those in the database is also computed. This method computes the shortest distance between fingerprint features from images in the database with those in the input image. The shortest distance computed is determined as the fingerprint match.

E. Comparison

TABLE I
PERFORMANCE COMPARISION BETWEEN OUR PROPOSED SYSTEM AND SOME EXISTING PRIACY PROTECTION SCHEMS

Techniques	Performance
Ratha et al.[4]	FRR(False Rejection Rate)= 16 % at FAR(False Acceptance Rate) = 0.01%
Nagar et al. [5]	FRR= 5% at FAR= 0.01%
Sheng Li et al [1]	FRR= 3% at FAR= 0.01%
The Proposed system	FRR= 0.1 % at FAR = 0.01%

VI. CONCLUSION

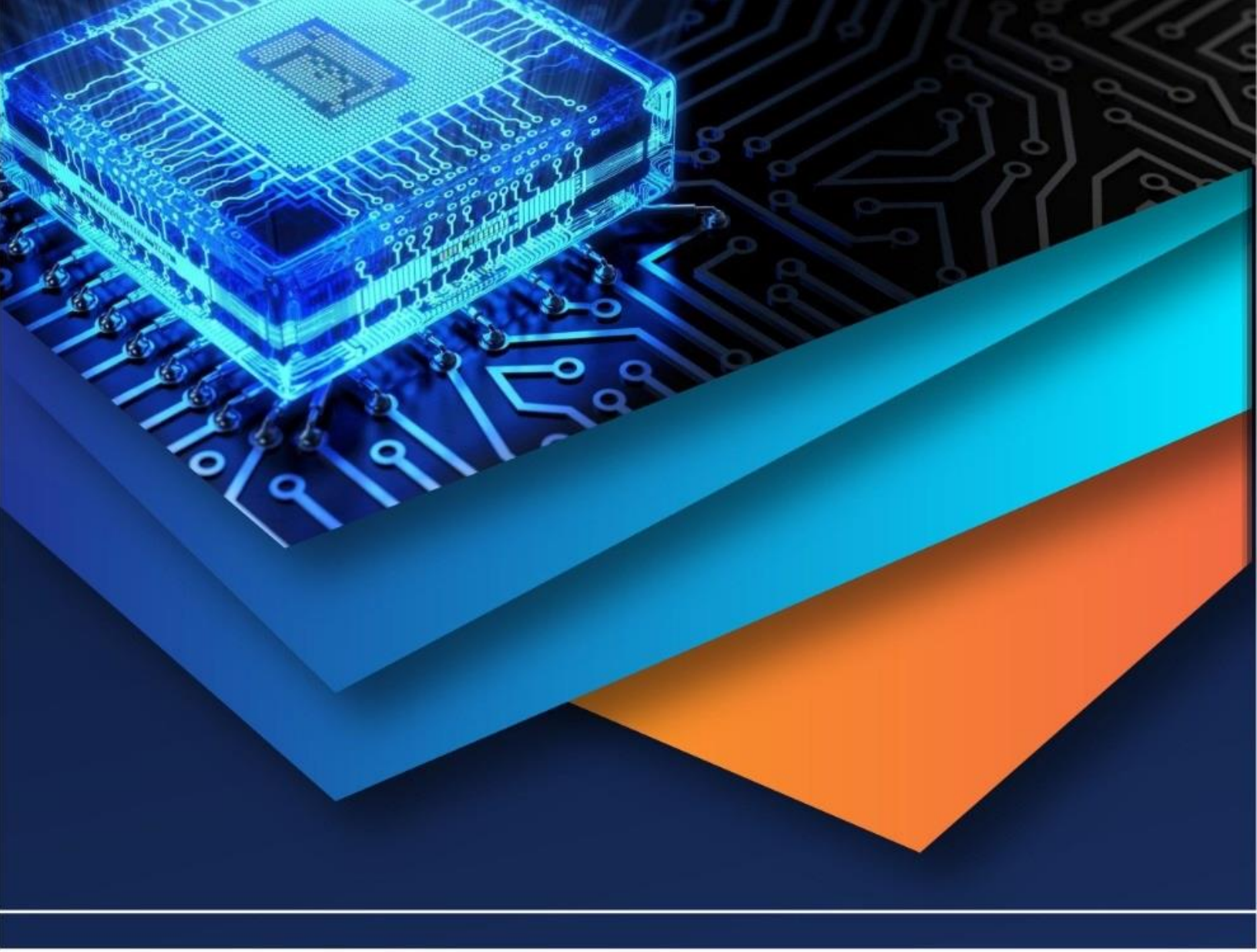
In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrollment, the system captures two fingerprints from two different fingers. A combined minutiae template containing only a partial minutiae feature of each of the two 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.

In the authentication process, two query fingerprints from the same two fingers are required. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against the enrolled template. Our 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.

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 tokenized 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,” PatternRecognit., 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.
[11] B. Yanikoglu and A. Kholmatov, “Combining multiple biometrics to protect privacy,” in Proc. ICPR-BCTP Workshop, Cambridge, U.K., Aug. 2004.
[12] Sheng Liand Alex C. Kot, “Fingerprint Combination for Privacy Protection” IEEE Trans on Info, Forensics and Security, Vol. 8, NO. 2, Feb 2013.
[13] N. Yager and A. Amin. Fingerprint alignment using a two stage optimization. PRL, 7(5):317–324, 2006.
[14] N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometrics-based authenticationsystems.IBM Systems Journal, 40(3):614–634, 2001.

[15] A. Ross, J. Shah, and A. Jain. From template to image: reconstructing fingerprints from minutiae points.PAMI, 29(4):544–560, 2007.
[16] Amengual J. C., Juan A., Prez J. C., Prat F., Sez S. and Vilar J. M. Real-time Minutiae Extraction in Fingerprint Images.Proc. of the6th Int. Conf. on Image Processing and its Applications, July 1997.
[17] 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.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY