ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

Combined Fingerprint Verification for Privacy Protection

D.Sriganesh[1], B.Baskar[2], K.Somasundaram[3], C.Janani[4]

B.Tech, Department of Electronic and Communication Engineering, Dr. S.J.S Paul Memorial College of Engineering and Technology, Pondicherry, India[1, 2, 3]

Assistant Professor, Department of Electronic and Communication Engineering, Dr. S.J.S Paul Memorial College of Engineering and Technology, Pondicherry, India[4]

ABSTRACT: In this paper we have proposed an innovative fingerprint recognition system by combining two different fingerprints into a new identity which contains minutiae position and minutiae orientation. In the enrollment phase, two fingerprints are obtained from two different fingers 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 enrollment. 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.

KEYWORDS: minutiae-based fingerprint matching algorithms, minutiae position, minutiae orientation minutiae orientation, combined template.

I.INTRODUCTION

We concentrate for using a biometric system is to provide non-cheatable authentication. 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. **(See Fig:-1)** .Therefore in this paper we propose a model of creating a combined minutiae template. By using the combined minutiae template, the complete minutiae feature of a single fingerprint will not be compromised when the database is stolen.

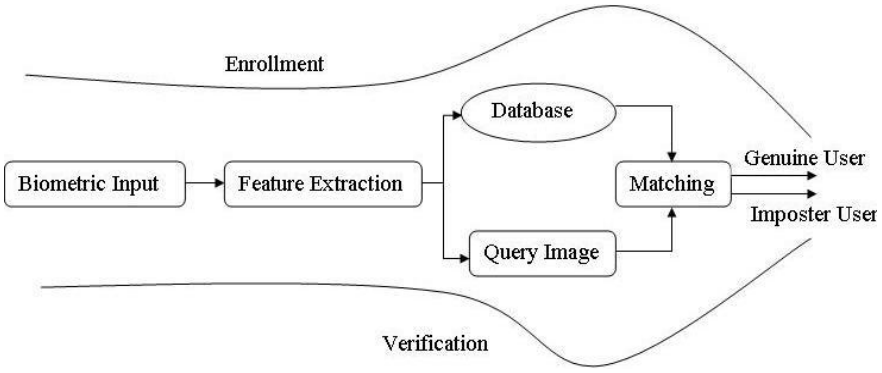

Fig: 1 BLOCK DIAGRAM OF BIOMATRICS SYSTEM

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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

"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. The previous work on "Generating cancelable fingerprint templates," proposed to generate cancellable fingerprint templates by applying noninvertible transforms on the minutiae.

II.RELATED WORD

"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 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. PROPOSED SYSTEM

Biometrics is gaining popularity; there is increased concern over the loss of privacy and potential misuse of biometric data held in central repositories. The association of Fingerprints with criminal raises further concerns. On the other hand, the alternative suggestion of keeping biometric data in smart cards does not solve the problem, since forgers can always claim that their card is broken to avoid biometric verification altogether. So it is important to generate a better and robust 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**. (See Fig: - 2)**

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

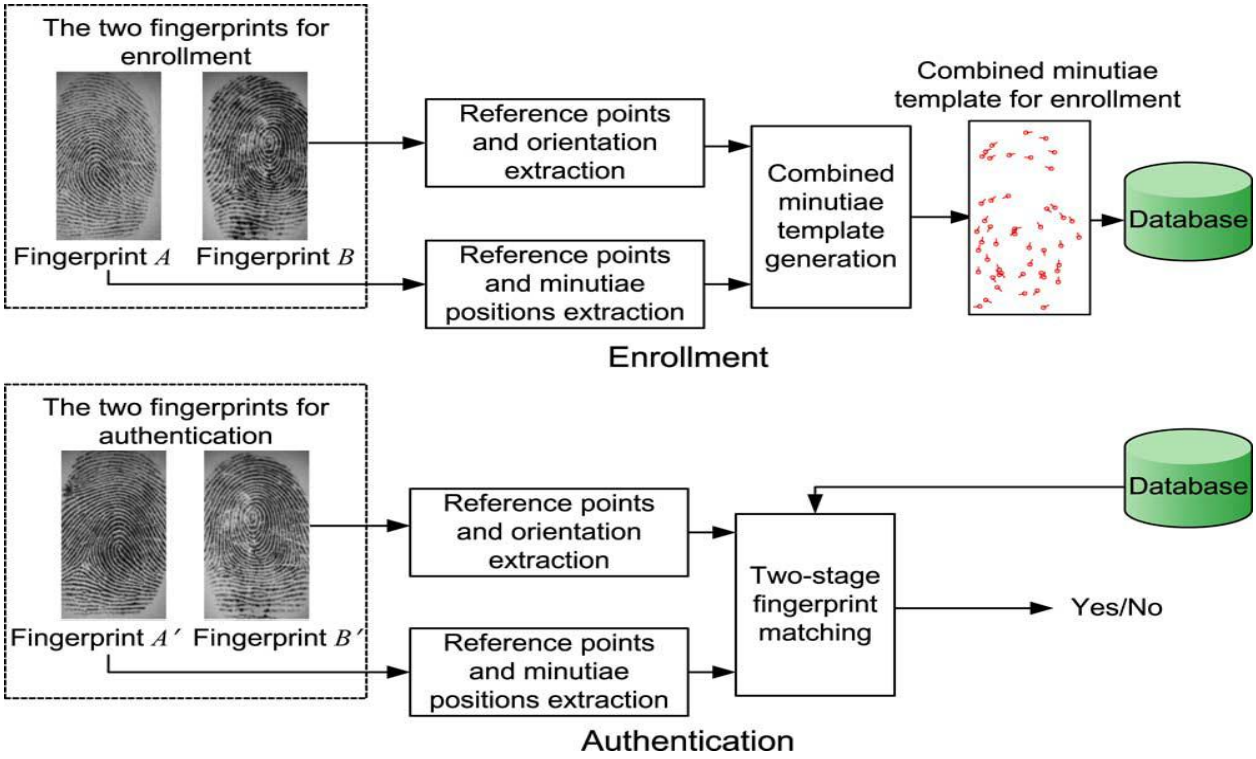

FIG: - 2 ENROLMENT AND AUTHENTICATION PHASE

FINGERPRINT BASICS:
Fingerprints are known to be unique to every individual. We can extract minutiae and orientation from a fingerprint.

MINUTIAE
A Minutia is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. **(See Fig: - 3)**

FIG: - 3 MINUTIAE POSITION IN FINGERPRINT

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

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 90^o and 270^o, since the ridges oriented at 90^o and the ridges oriented at 270^o in a local neighbourhood cannot be differentiated from each other. **(See Fig: - 4)**

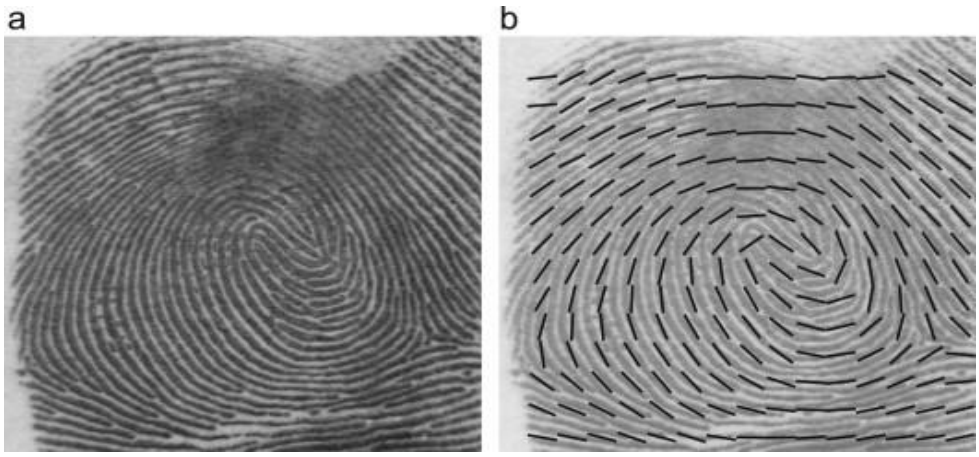

FIG -4: ORIENTATION FIELD IN FINGERPRINT

COMBINED MINUTIAE TEMPLATE GENERATION

Given a set of N minutiae positions $P_A = \{\mathbf{p}_{ia} = (x_{ia}, y_{ia}), 1 \le i \le N\}$, of fingerprintA, the orientation O_B of fingerprint B and a combined minutiae template M_C is generated by minutiae position alignment and minutiae direction assignment. **(See Fig: - 4)**

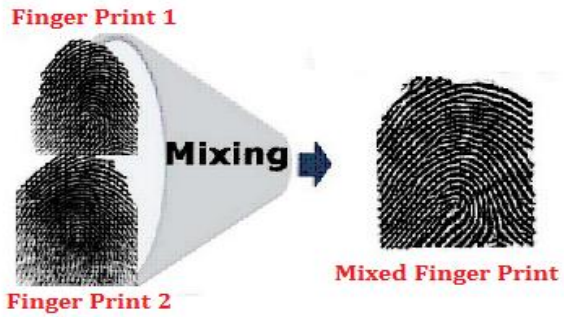

FIG:-4 COMBINED MINUTIAE TEMPLATE

IV.ALGORITHM

The algorithms used in the system are,

- Minutiae Points Detection Algorithm
- Orientation Estimation Algorithm
- Combined Minutiae Template Generation Algorithm

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

- Minutiae-Based Fingerprint Matching Algorithms

EXPERIMENTAL RESULT

Two different finger print image is given as an input for the system. Minutiae point detection algorithm and orientation estimation algorithm is used to obtain two different features.

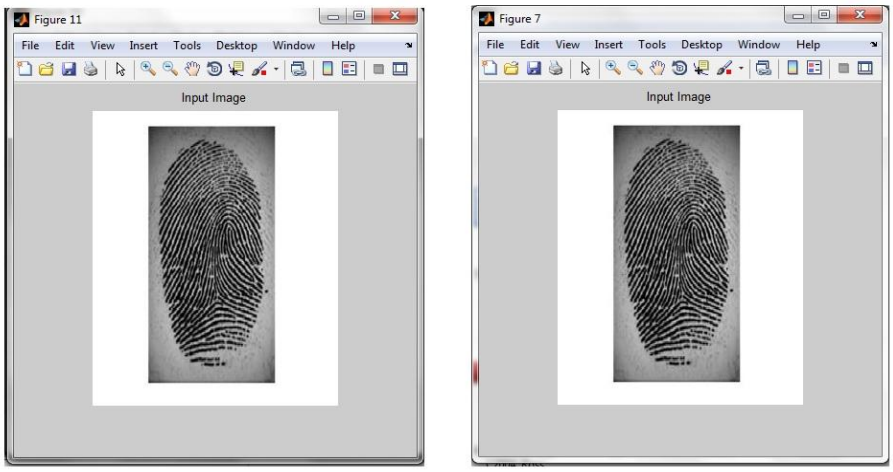

FIG:-5 INPUT FINGERPRINT IMAGE

Minutiae points Detection algorithm is applied to obtain the Minutiae position from first finger print and by using Orientation Estimation algorithm, Orientation field is obtained from second finger print.

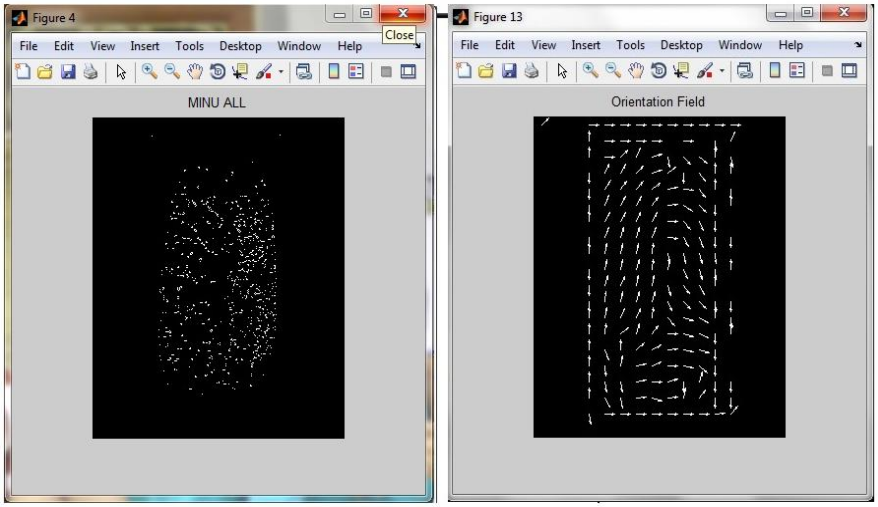

FIG:-6 MINUTIAE POSITION AND ORIENTATION FROM INPUT FINGERPRINT

By applying combined fingerprint generation algorithm a combined template is generated using minutiae position and orientation template.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

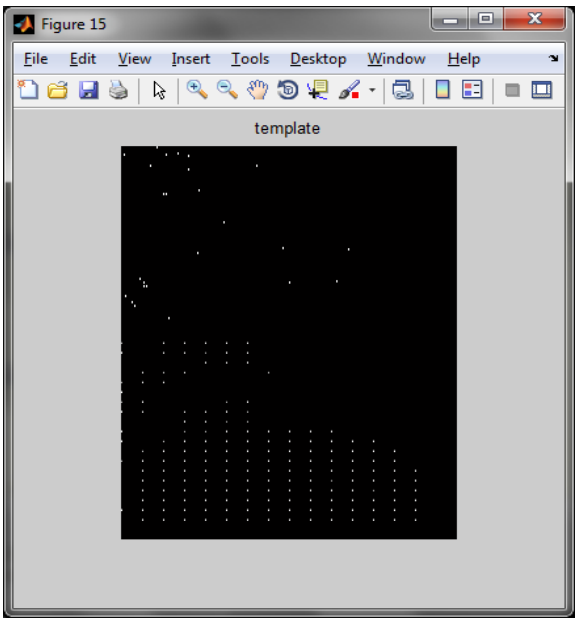

FIG:-7 COMBINED TEMPLATE

VI.CONCLUSION AND FUTURE WORK

In this paper, we introduce a novel system for fingerprint privacy protection by combining two fingerprints into a new identity. In the enrolment, 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 combined minutiae template. The experimental results show that our system achieves a very low error rate.

VII. ACKNOWLEDGMENTS

We thank our HOD Dr.T.Thirumurugan, Ph.D. (Department of Electronics and Communication Engineering) to help us for creating this paper with his sincere guidance and Technical Expertise in the field of communication. The help of our guide Ms. C.Janani, M.Tech, Department of ECE, Dr, SJS Paul College of Engineering and Technology is really immense and once again I thank her for her great motivation. I thank Dr. SJS Paul College of Engineering and Technology to provide me such a standard educational environment so that I am able to understand the minute concepts in the field of Engineering and Technology.

VIII. REFERENCE

[1] S. Li and A. C. Kot, "A novel system for fingerprint privacy protection," in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.
[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.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 2, February 2015

[5] A. Nagar, K. Nandakumar, and A. K. Jain, "Biometric template transformation: A security analysis," in Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose, Jan. 2010.
[6] 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.
[7] W. J. Scheirer and T. E. Boult, "Cracking fuzzy vaults and biometric encryption," in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.
[8] S. Li and A. C. Kot, "Privacy protection of fingerprint database," IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011.
[9] A. Ross and A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81,Mar. 2011.
[10] B. Yanikoglu and A. Kholmatov, "Combining multiple biometrics to protect privacy," in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.
[11] 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

IX.BIOGRAPHY

Ms. C.Janani is working as a Assistant Professor (Department of ECE) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. She has published two international journals. She is interested in Electro Magnetic wave theory, wave guides and antennas, Digital signal processing, signals and system.

Mr.Sriganesh is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in Electro Magnetic wave theory, wave guides and antennas, Digital signal processing, signals and system.

Mr.Baskar is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in Digital circuits, Digital signal processing, and Electronic circuits.

Mr.Somasundaram is a student who is pursuing B.Tech (Electronics and Communication Engineering) in Dr. S.J.S PAUL MEMORIAL COLLEGE OF ENGINEERING AND TECHNOLOGY. He is interested in VLSI design, Digital signal processing, and digital electronics.