OPEN ACCESS
ISSN: 2249-6645

International
Journal
Of Modern Engineering Research (IJMER)

Combined Finger Print Template For Privacy And Security

Mallikarjun [1], Sai manohar [2] , veeranna [3]
*(Department of ECE, SBIT College/ JNTUH University, India) Email: mallikarjun.n20@gmail.com)
** (Department of ECE, SBIT College/ JNTUH University, India) Email: manoharsra1312@gmail.com)
***(Department of ECE, SBIT College/ JNTUH University, India) Email: dev.veer57@gmail..com)

Abstract : *Fingerprint recognition is an active research area nowadays. In many areas we are using fingerprint recognition for to improve the security and privacy. In finger print recognitions system the recognition can be done by fingerprint matching techniques. Fingerprint matching techniques are classified in two categories: Fingerprint verification and Fingerprint identification. In this project we are using the fingerprint verification. For this we propose here a novel system for protecting finger print privacy by combining two different fingerprints into a new identity. In the enrollment, two fingerprints are captured from two different fingers. We extract the minutiae positions from one fingerprint, the orientation from the other fingerprint, and the reference points from both fingerprints. Based on this extracted information and our proposed coding strategies, a combined minutiae template is generated and stored in a database. In the authentication, the system requires two query fingerprints from the same two fingers which are used in the enrollment. A two-stage fingerprint matching process is proposed for matching the two query fingerprints against a combined minutiae template. With the help of an existing fingerprint reconstruction approach, we are able to convert the combined minutiae template into a real-look alike combined fingerprint. Thus, a new virtual identity is created for the two different fingerprints, which can be matched using minutiae-based fingerprint matching technique.*

Keywords: *Fingerprint, minutiae*

I. INTRODUCTION

Fingerprint techniques have widespread of applications in authentication systems., protecting the privacy of the fingerprint becomes an important issue. Traditional encryption is not sufficient 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.

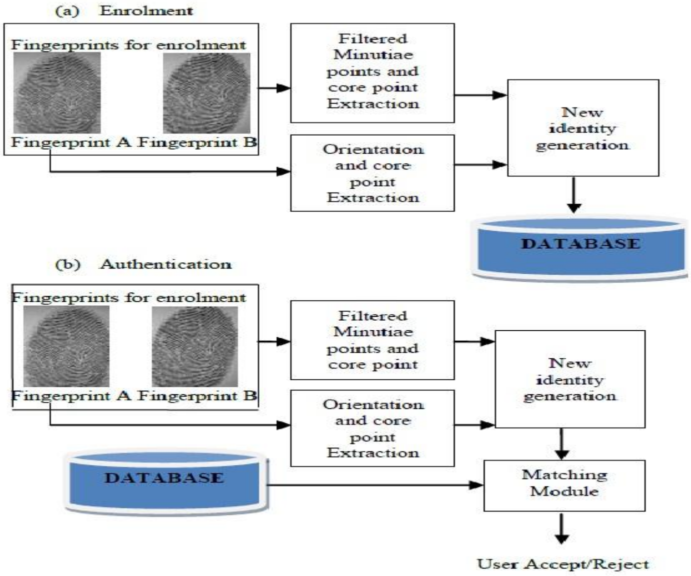
In this paper, i propose a novel system for protecting finger print privacy by combining two different fingerprints into a new identity. During the enrollment, the system captures two fingerprints from two different fingers. We propose a combined minutiae template generation algorithm to create a combined minutiae template from the two fingerprints. In such a template, the minutiae positions are extracted from one fingerprint, while the minutiae directions depend on the orientation of the other fingerprint and some coding strategies. The template will be stored in a database for the authentication which requires two query fingerprints. A two-stage fingerprint matching process is further proposed for matching the two query fingerprints against 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. In addition, the combined minutiae template share a similar topology to the original minutiae templates, it can be converted into a real-look alike combined fingerprint by using an existing fingerprint reconstruction approach. The combined fingerprint issues a new virtual identity for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms.

The advantages of our technique over the existing fingerprint combination techniques are as follows:

1) Our proposed system is able to achieve a very low error rate with FRR= 0.4 % when FAR = 0.1%.

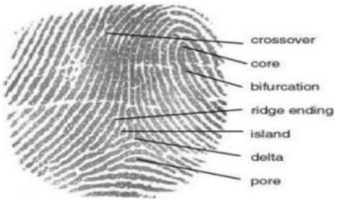
2) Compared with the feature level based technique, we are able to create a new identity (i.e., the combined minutiae template) which is difficult to be distinguished from the original minutiae templates.

II. DESIGN OF PROPOSED SYSTEM


(a) Enrolment
Fingerprints for enrolment
Fingerprint A Fingerprint B
Filtered Minutiae points and core point Extraction
Orientation and core point Extraction
New identity generation
DATABASE
(b) Authentication
Fingerprints for enrolment
Fingerprint A Fingerprint B
Filtered Minutiae points and core point
Orientation and core point Extraction
New identity generation
DATABASE
Matching Module
User Accept/Reject

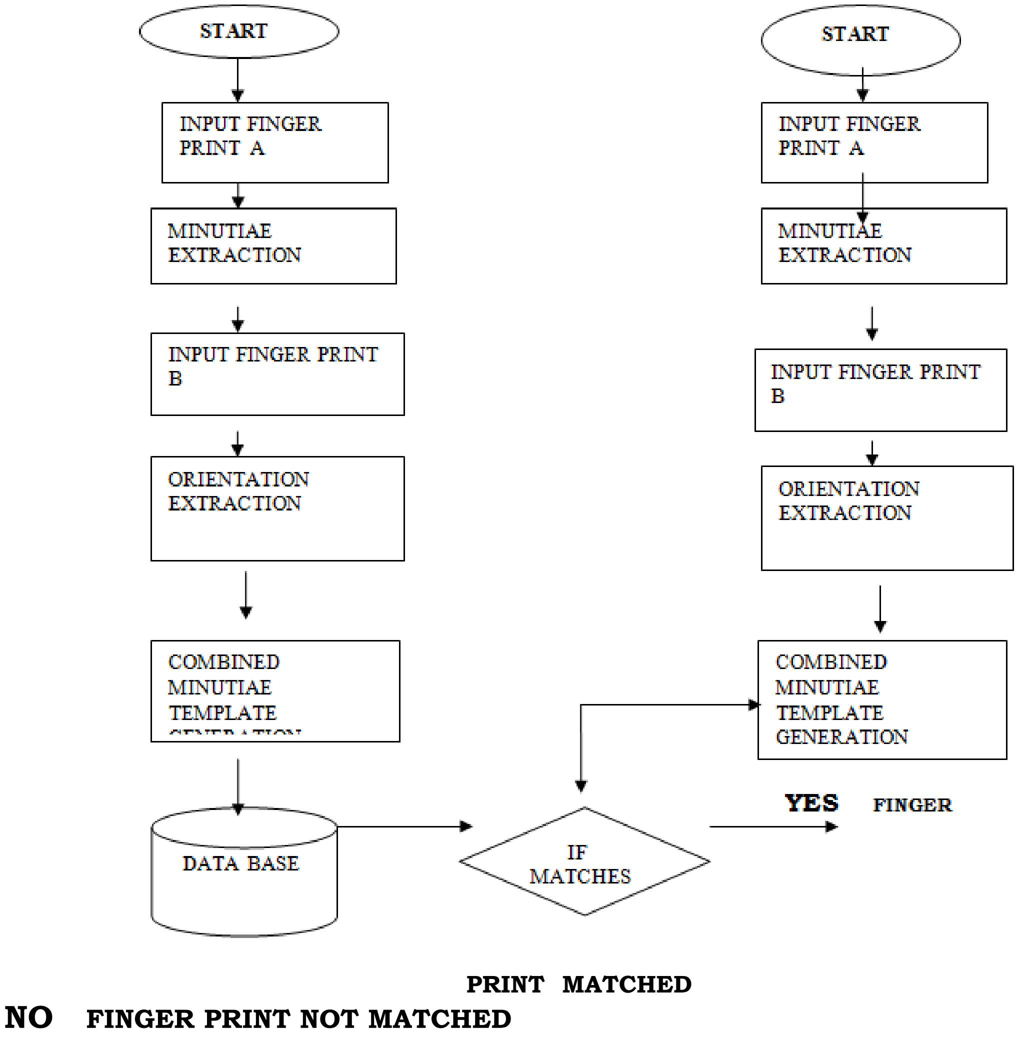
MINUTIAE:

A Minutia is defined as the points of interest in a fingerprint, such as bifurcations (a ridge splitting into two) and ridge endings. The most commonly used fingerprint features are minutiae. Minutiae are the discontinuities in local ridge structure. They are used by forensic experts to match two fingerprints. There are about 150 different types of minutiae . Among these minutiae types “ridge ending” and “ridge bifurcation” are the most commonly used as all the other types of minutiae are combinations of ridge endings and ridge bifurcations. A ridge ending is defined as the ridge point where a ridge ends abruptly . A ridge bifurcation is defined as the ridge point where a ridge forks or diverges into branch ridges . Some common types of minutiae are shown in fig.



III. MINUTIAE POINTS

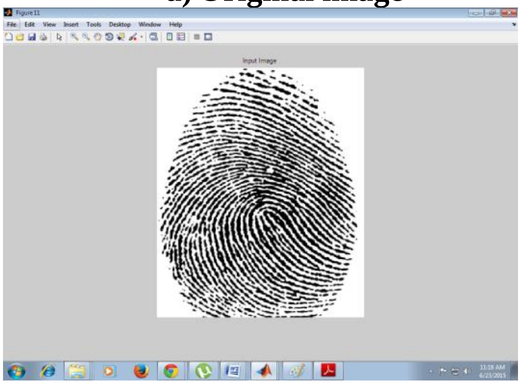
3. FLOW CHART:



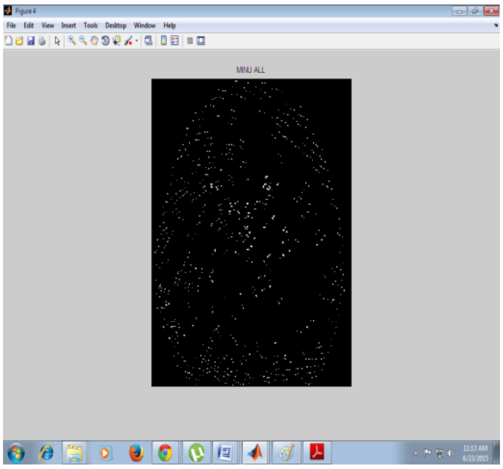
IV. RESULTS AND DISCUSSION

OUT PUT RESULTS:

a) Original image



b) false minutiae removal



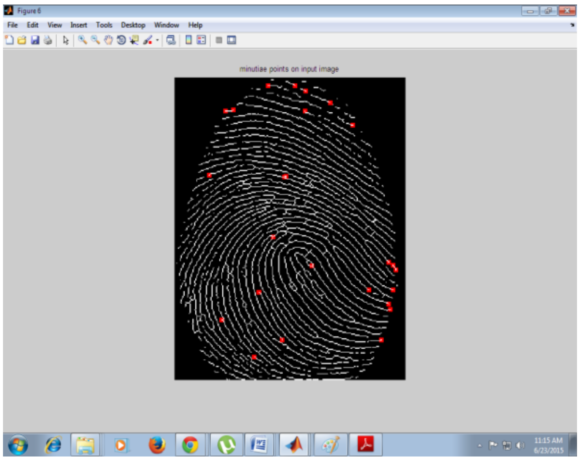
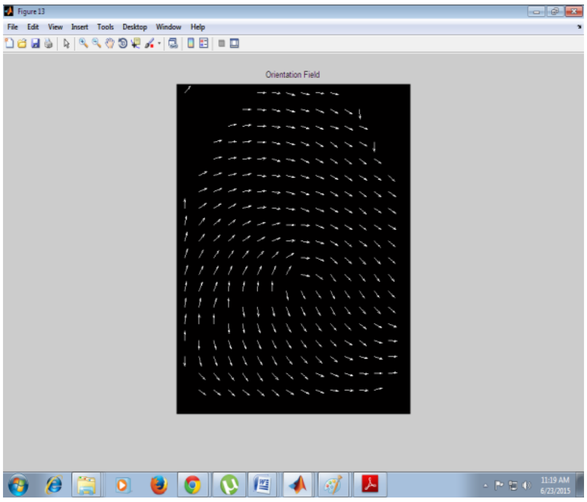
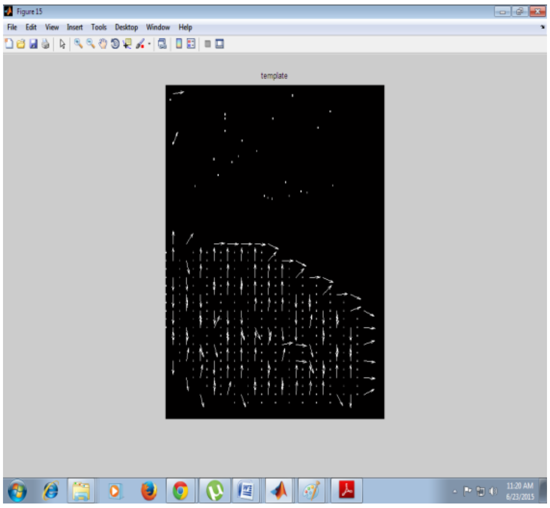


Figure 6
File Edit View Insert Tools Desktop Window Help
minutiae points on input image

b) Orientation field of finger print





***Evaluating Performance Of Proposed System Over Different Databases*:**

For evaluating the performance of proposed system the experiment is conducted on different fingerprint databases such as FVC2000, FVC2002 and FVC2004. We use the first two impressions in the FVC2002 DB2_A to evaluate system performance, which contains 200 fingerprints from 100 fingers as each finger has two impressions. Therefore, we have a 100 finger pairs the first two impressions of each fingerprint are combined to generate combine minutiae template during enrolment process. The algorithm Ratha 1995 and Sherlock 1994 are used for extracting features such as minutiae position and direction. The image processing algorithm convolution filter is used for fingerprint matching. To compute the False Rejection Rate (FRR), the second impressions of a finger pair are matched against the corresponding enrolled template, producing 100 genuine tests. To compute the False Acceptance Rate (FAR), the first impressions of a finger pair are matched against the other 99 enrolled templates, producing 100 99 imposter tests. Similarly our system performance evaluated for FVC2000 and FVC2004 Databases. The Table I shows the evaluated resultant value of FRR at various values of FAR. From table I we can see that, FRR of our system is 0.1% when FAR= 0.1%.

V. CONCLUSION

In this paper we introduced a novel system for privacy protection by combination of two fingerprints randomly chosen into a new template. During the enrollment stage, the system captures two fingerprint image from two different fingers. A combined template containing a partial minutiae feature of one finger and orientation field of another finger is created and stored in database for authentication. To make the combined minutiae template look real as an original template, three different techniques are introduced during the combined minutiae template generation process. In the authentication process, two input fingerprints are scanned. The fingerprint matching process is used to match the fingerprint images against the enrolled template. The combined minutiae template is similar to the original minutiae template. Therefore, we successfully combine the two different fingerprint image into a new template using watermark technique which is a real look-alike image of input fingerprints.

VI. ADVANTAGES

- Double level Security
- No Limited Privacy Protection
- System Can Achieve A Very Low Error Rate
- High Performance .

VII. APPLICATIONS

1. used in attendance systems, which are being increasingly used in various organisations to control employee timekeeping.
2. used in providing strong security at bank transactions.
3.used in for securing access to pc's and providing single logon facilities.
4.used in secure accessing of data .

VIII. REFERENCES

[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]. *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]. *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.*

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

[6]. *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.*

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

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

[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]. *Y. Wang and J. Hu, "Global ridge orientation modeling for partial fingerprint identification," IEEE Trans. Pattern Anal. Mach. Intell., vol. 33, no. 1, pp. 72–87, Jan. 2011.*

Mallikarjun Nuthanaganti was born on JULY 02, 1986 , India and got B.Tech in Electronics and Communication Engineering from JNTUH Hyderabad in the year of 2008. He completed his M.Tech in Embedded Systems branch from JNTUH university in the year of 2010. After completion of his M.Tech he joined as a Assistant Professor in ECE Department at SBIT- Khammam affiliated to JNTUH. His area of interest are Embedded system, image processing.

S.Sai manohar was born on MAY 15, 1986 , India and got B.Tech in Electronics and Communication Engineering from KU Warangal in the year of 2007. He completed his M.Tech in Embedded Systems branch from JNTUH university in the year of 2010. After completion of his M.Tech he joined as a Assistant Professor in ECE Department at SBIT-Khammam affiliated to JNTUH. His area of interest are Embedded system,VLSI.

D.Veeranna was born on MARCH 22, 1983 , India and got B.E ECE, from CBIT Hyderabad in the Year 2005, M.Tech. (VLSI SD) from NITW University, Warangal in the Year 2008. He has got 07 Years of Teaching Experience. Presently, he is working as Asst., Professor in Department of Electronics and communication Engineering in SBIT Engineering College Khammam. His area of interest are fault tolerance, image processing