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, Special Issue 1, March 2015

National Conference on Recent Advances in Electrical & Electronics Engineering (NCREEE 2015)

Organized by

Dept. of EEE, Mar Baselios Institute of Technology & Science (MBITS), Kothamangalam, Kerala-686693, India
On 26th & 27th March 2015

Biometric System for Voter Identification

Maria Antony[1], Elbin Eldo Benny[2], Aavani Mohan[3], Lakshmi R[4], Shajimon K John[5]

B.Tech Student, Dept. of ECE, SAINTGITS College of Engineering, Kottayam, Kerala, India [1,2,3,4]

Professor, Dept. of ECE, SAINTGITS College of Engineering, Kottayam, Kerala, India [5]

ABSTRACT: In this paper we proposes a biometric system for voter identification. Election is the real participation of people in democracy, where the people participate in direct way to form in government. But we know that nowadays the fairness of election is lost. So people are uninterested and disengaged with elections. We are even less likely to vote and lack of belief in the election. The main problem faced during election is the bogus votes. In order to prevent such cases, we proposed a system for voter identification. As fingerprint is the most widely used biometric for the identification purposes, we used the combination of fingerprints for the verification. Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between human fingerprints. With the widespread applications of fingerprint techniques in authentication systems, protecting the privacy of the fingerprint becomes an important issue. The proposed novel system for voter identification combines two different fingerprints into a new identity. In the enrolment, two fingerprints are captured from two different fingers. We can use the same fingerprint image that we have already collected during the enrolment phase of Aadhaar ID. Minutiae positions and orientations are extracted from two different fingerprints. Based on this extracted information and the 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 enrolment. 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 algorithm, the proposed system is 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 algorithms

KEYWORDS: Biometric, Authentication, Enrolment, Minutiae.

I.INTRODUCTION

Personal identification is to associate a particular individual with an identity. It plays a critical role in our society, in which questions related to identity of an individual such as “Is this the person who he or she claims to be?”, “Has this applicant been here before?”, “Should this individual be given access to our system?” “Does this employee have authorization to perform this transaction?” etc are asked millions of times every day by hundreds of thousands of organizations in financial services, health care, electronic commerce, telecommunication, government, etc. With the rapid evolution of information technology, people are becoming even more and more electronically connected. As a result, the ability to achieve highly accurate automatic personal identification is becoming more critical.

A wide variety of systems require reliable personal authentication schemes to either confirm or determine the identity of individuals requesting their services. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) [1, 2] have been used to restrict access to systems. The major advantages of this traditional personal identification are that
(i) They are very simple
(ii) They can be easily integrated into different systems with a low cost.
Therefore they are unable to satisfy the security requirements of our electronically interconnected information society. The emergence of biometrics has addressed the problems that plague traditional verification.

Biometrics means life measurement but the term is usually associated with the use of unique physiological characteristics to identify an individual. The application which most people associate with biometrics is security. Among all biometric traits, fingerprints have one of the highest levels of reliability and have been extensively used by forensic experts in criminal investigations. A fingerprint refers to the flow of ridge patterns in the tip of the finger. Fig

1 shows the ridge flow exhibits anomalies in local regions of the fingertip and it is the position and orientation of these anomalies that are used to represent and match fingerprints.

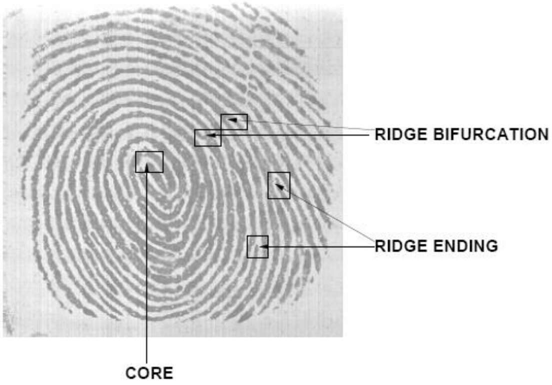

Fig 1 Fingerprint Template

An image of the fingerprint is captured by a scanner, enhanced, and converted into a template. Scanner technologies can be optical, silicon, or ultrasound technologies.

The uniqueness of a fingerprint is determined by the topographic relief of its ridge structure and the presence of certain ridge anomalies termed as minutiae points. Typically, the global configuration defined by the ridge structure is used to determine the class of the fingerprint, while the distribution of minutiae points is used to match and establish the similarity between two fingerprints

II.PROPOSED SYSTEM

The proposed system is for protecting fingerprint privacy by combining two different fingerprints into a new identity. There are two phases in the proposed system.

a. Enrolment
b. Authentication

During the enrolment, the system captures two fingerprints from two different fingers say fingerprints ‘A’ and ‘B’ from fingers ‘A’ and ‘B’, respectively. We extract the minutiae positions from fingerprint ‘A’ and the orientation from fingerprint ‘B’ using some existing techniques [3]. A combined minutiae template generation algorithm is 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. 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 [2, 5] for two different fingerprints, which can be matched using minutiae based fingerprint matching algorithms. Fig 2 shows the fingerprint privacy protection system:

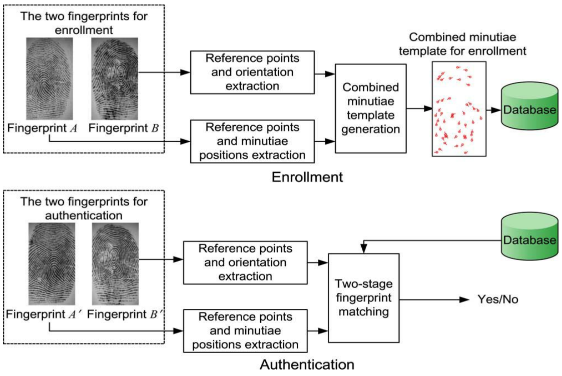
The two fingerprints for enrollment
Fingerprint A
Fingerprint B
Reference points and orientation extraction
Reference points and minutiae positions extraction
Combined minutiae template generation
Combined minutiae template for enrollment
Database
Enrollment
The two fingerprints for authentication
Fingerprint A′
Fingerprint B′
Reference points and orientation extraction
Reference points and minutiae positions extraction
Two-stage fingerprint matching
Database
Yes/No
Authentication

Fig 2.Fingerprint Privacy Protection System

The requirements are as follows:

a) PRE-PROCESSING

Fingerprint images acquired with various sensors will have different levels of the dynamic range altering the image contrast. Therefore a pre-processing operation in form of contrast enhancement should be performed before extracting the minutiae from the fingerprint. The contrast enhancement can be performed with various methods. For example histogram equalization can increase the contest of the image. Quality of the image can also be increased by using the filters. Low pass filter lowers the noise from the image. Band pass filter can lower undesired noise from orientations which helps to preserve true ridges. Image enhancement can also be performed using Fourier transform method. Fig 3 shows the changes after the pre processing stage.

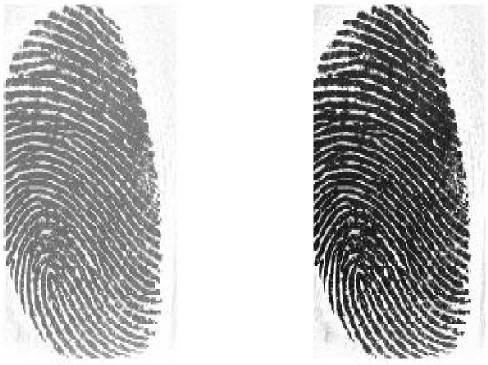

Fig 3 Fingerprint Obtained After Pre-Processing (1) Original Image (2) Enhanced Image

b) MINUTIAE EXTRACTION

After a fingerprint image has been enhanced, the next step is to extract the minutiae from the enhanced image. Following the extraction of minutiae, a final image post processing stage is performed to eliminate false minutiae. This chapter provides discussion on the methodology and implementation of techniques for minutiae extraction and fingerprint image post processing. The first section contains a review of existing literature in the field of minutiae extraction and post processing. The next section discusses the methodology for implementing each of these two techniques. The last section presents the results from the experiments conducted using the implemented techniques.

c) REFERENCE POINTS DETECTION

The reference point's detection process is motivated by Nilsson [6], who first proposes to use complex filters for singular point detection. For the alignment of two fingerprints certain landmark points are needed. These should be automatically extracted with low misidentification rate. As landmarks it suggests the prominent symmetry points (singular points, SPs) in the fingerprints. It can identify an SP by its symmetry properties. SPs are extracted from the complex orientation field estimated from the global structure of the fingerprint, i.e. the overall pattern of the ridges and valleys. Complex filters, applied to the orientation field in multiple resolution scales, are used to detect the symmetry and the type of symmetry. Locate a reference point satisfying the two criterions:

(i) The amplitude of the point (hereinafter termed as the certainty value for simplicity) is a local maximum.
(ii) The local maximum should be over a fixed threshold T.
Certainty map of reference point

$C_{ref} = Z * \overline{T_{ref}}$ ------------------------------- (1)

$Z = cos\,(2O) + jsin\,(2O)$------------------- (2)
Where Z is orientation.

$T_{ref\,=}$ (x + iy) $\times \frac{1}{2\pi\sigma^2} \times \exp(-\frac{x^2+y^2}{2\sigma^2})$--------(3) kernel for the reference point detection.

d) COMBINED MINUTIAE TEMPLATE GENERATION

Given a set of minutiae positions of fingerprint, the orientation of fingerprint and the reference points of fingerprints and, a combined minutiae template is generated by minutiae position alignment and minutiae direction assignment. Fig 4 shows the combined minutiae template generation process.

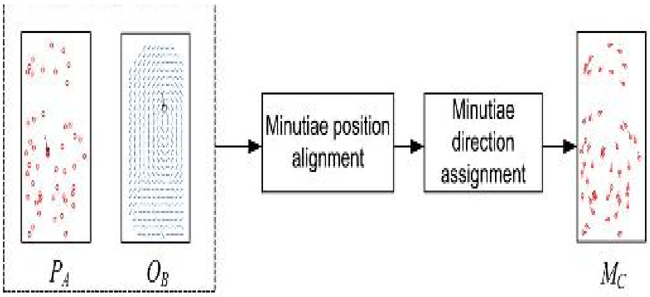

Fig 4 Combined Minutiae Template Generation

e) COMBINED FINGERPRINT GENERATION

In a combined minutiae template, the minutiae positions and directions (after modulo π) 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 [1]. Existing works [2, 3, 4] have shown that it is possible to reconstruct a full fingerprint image from a minutiae template. Adopting one of these fingerprint reconstruction approaches, it is able to convert our combined minutiae template into a combined fingerprint image. Given any two different fingerprints as input, then 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. Fig 5 shows the combined fingerprint template generation process.

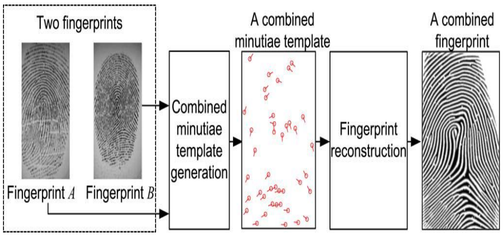
Two fingerprints
Fingerprint A
Fingerprint B
Combined minutiae template generation
A combined minutiae template
Fingerprint reconstruction
A combined fingerprint

Fig 5 Combined Fingerprint Generation

User can give the fingerprint input image into the system, that image may be colour image or gray scale image. If the image is colour image, then the system will automatically convert that into gray scale image. Then the system will do all other steps for generating combined form and authentication. After all these steps system will generate the output and stored in database and test the matching using two stage matching algorithm. Authentication will be successful if the matching score is over a predefined threshold. Thus the result of privacy protection enabled for the user.

III.TWO STAGE FINGERPRINT MATCHING

Depending upon the minutiae positions of fingerprint, the orientation of fingerprint and the reference points of the two query fingerprints are used for the matching process. In order to match the fingerprint stored in the Database, a two-stage fingerprint matching process including query minutiae determination and matching score calculation is done. Fig 6 shows the block diagram of fingerprint matching process.

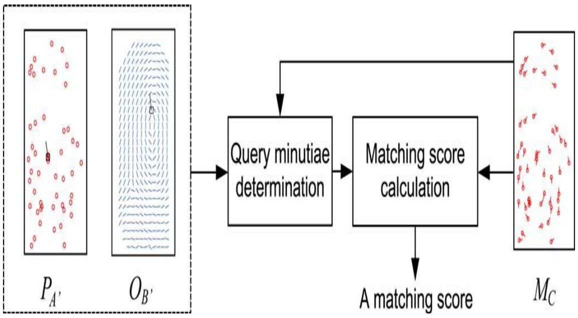

Fig 6 Two-Stage Fingerprint Matching

IV.ENROLMENT

The system captures two fingerprints from two different fingers. A combined minutiae template generation algorithm is used 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.

V.AUTHENTICATION

Reference points are detected from both query fingerprints. Then check 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.

VI.CONCLUSION

The main goal of this paper is to propose a combined biometric system which preserves privacy and increases accuracy. Privacy is preserved by fusing biometric information from two fingerprints at template level in the minutiae space. Since fingerprint minutiae and orientation fields generated are combined in the users' templates, privacy concerns are diminished by hiding the nature of the points in the templates.

In this paper a combined minutiae template generated, the minutiae positions and orientation are extracted from two fingerprints separately. If it is stolen, the complete minutiae features of each fingerprint are not compromised. Another preferable property is that these minutiae positions and orientation share a similar topology of those from an original fingerprint. Therefore, it would be difficult to distinguish a combined minutiae template from the minutiae of an original fingerprint. Such property would be able to further protect the privacy of the use's fingerprints because the attacker may treat our template as a minutiae template of a single original fingerprint. In this paper, only two fingerprints are used as template, there is a scope of using more than two fingerprints.

REFERENCES

[1] S. Li and A. C. Kot, ― Fingerprint Combination for Privacy Protection,‖ in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.

[2] 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.

[3] L. Hong, Y. F. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal Machine Intell* ., vol. 20, no. 8, pp. 777–789, 1998.

[4] 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.

[5] S. Li and A. C. Kot, "Attack using reconstructed fingerprint," in *Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS)*, Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

[6] 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.