Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

A GUI Model of Secured Fingerprint Authentication Using Image Fusion

Priyashree Firke[*1] and Nilesh Gupta[2]

[1]M.Tech Scholar,CSE Department, Chouksey Engineering College Lalkhadan Bilaspur(c.g).
[2]Assistant Professor ,CSE Department,Chouksey Engineering College LalkhadanBilaspur(c.g).

ABSTRACT

A fingerprint in its narrow sense is an impression left by the friction ridges of a human finger. The recovery of fingerprints from a crime scene is an important method of science.Fingerprint recognition is the most popular methods used for identification.This project explores the possibility of mixing two different fingerprints, pertaining to two different fingers, at the image level in order to generate a new fingerprint. 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, 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. This approach has following benefits: (a) it can be used to generate virtual identities from two different fingers (b) it can be used to obscure the information present in an individual's fingerprint image prior to storing it in a central database. In project stage 1, extraction of minutiae positions from one fingerprint is performed. So in stage 1, we propose a system for detecting minutiae positions from fingerprint images which can later be used for fingerprint protection.

KEY WORDS: Combination, biometrics, fingerprint, minutiae, privacy, protection.

[*]Corresponding Author

Priyashree Firke

Department of computer science and Engineering,

Chouksey Engineering College,

Bilaspur (C.G) india

E-mail: priyashree.firke@gmail.com

INTRODUCTION

Due to the event of computers and increased usage of web, leakage of personal information has become a heavy drawback. With the arrival of Electronic Banking, E-Commerce and smart cards and an increase emphasis on the privacy and security of information stored in various databases, Automatic Personal Identification has become a very important topic which is applied in a wide range of civilian applications involving the use of passports, cellular phones and ATMs. Traditionally, passwords (knowledge-based security) and ID cards (token-based security) have been used to restrict access to systems. However these approaches are not based on any inherent attributes of an individual to make a personal identification thus having number of disadvantages like tokens may be lost, stolen, forgotten, or misplaced; PIN may be forgotten or guessed by impostors. Given the inefficiency of PIN based systems, it has become increasingly important that a person be identified on the basis of some Bio-metric feature which is unique to him.

Bio-metrics is the measurement of a unique physical characteristics and acts as an ideal solution to the problem of digital identification. The advantages of Fingerprint Bio-metrics over other identification procedures are: Each of our ten fingerprints is unique, different from another and from those of every other person. Unlike passwords, PIN codes and smart cards that we depend upon today for identification our fingerprints are impossible to lose or forget, and they can never be stolen. We have ten fingerprints as oppose to two eyes, one face and one voice. Hence fingerprints have been used for centuries upon which one can make a claim on the uniqueness of each fingerprint.

In today's modern world authentication and security is of major concern. Finger print recognition is one of the most widely used biometric security system as it is easy to access and implement. The existing finger print technology does not provide much accuracy thus resulting into implementation of fusion techniques in the existing technology. Fusion at sample level finger print recognition also called as finger print recognition using hybrid technology provides high security at low cost.With the widespread applications of fingerprint techniques 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 beforethe 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.

PROPOSED SYSTEM

The motivation behind this project is protecting fingerprint privacy by combining two different fingerprints into a new identity. In this work, an input fingerprint image is mixed with another fingerprint (e.g., from a different finger), in order to produce a new mixed image that obscures the identity of the original fingerprint.

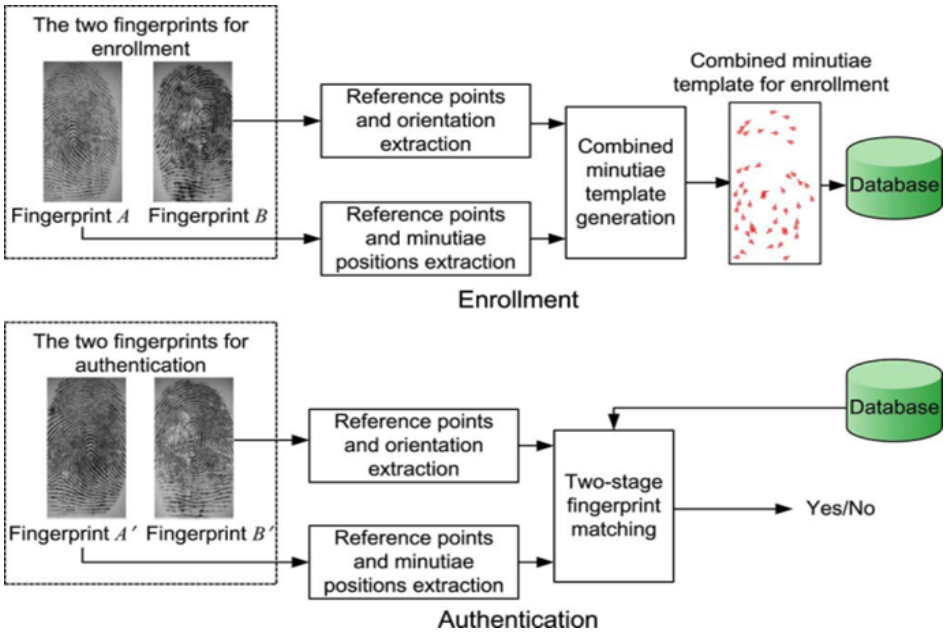

Figure 1: The block diagram of proposed system

Fig. 1 shows our proposed fingerprint privacy protection system. In the enrolment phase, the system captures two fingerprints from two different fingers. We extract the minutiae positions from 1st fingerprint, orientation from 2nd fingerprint and reference points from both fingerprints. Then, by using coding strategies, a combined minutiae template is generated 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. As what we have done in the enrolment, we extract the minutiae positions from the 1st fingerprint and the orientation from 2nd fingerprint. Reference points are detected from both queryfingerprints. This extracted information will be matched against the corresponding template stored in the database by using a two-stage fingerprint matching.

METHODOLOGY

In this segment, the proposed system in detail are clarified.

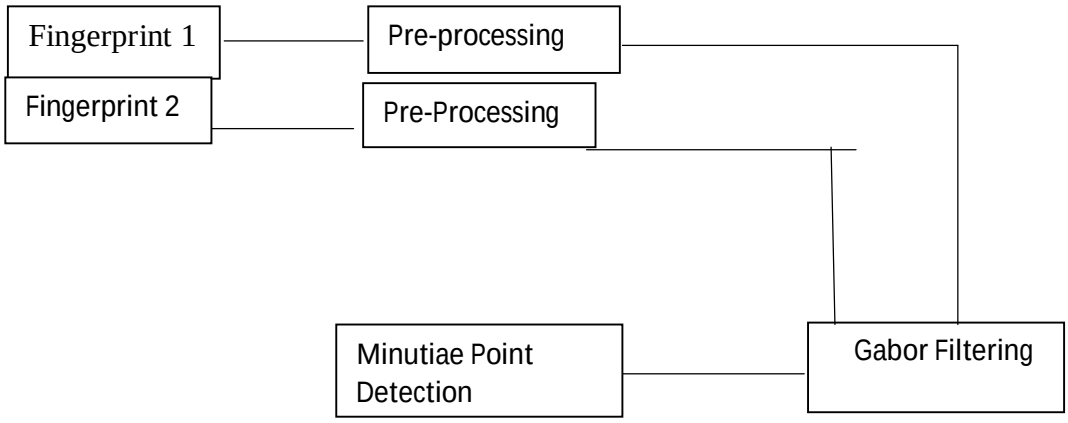

Figure 2: Work of Proposed System

The above figure shows thework (process) of proposed system. In this phenomenon firstly we have to input first fingerprint than second fingerprint after that pre-processing had been perform of the input fingerprints.

The pre-processing follows few steps which is required for the detection of minutiae.first the conversion of grey scale image had been performed of the original image.Then histogram representation had been done. That act as a graphical representation of the tonal distribution in a digital Image. After that morphological closing and opening of image had been performed.The closing operation can expand image and remove peak by background noise and the opening operation can shrink image and eliminate small cavities. Then the dilation had been performed, dilation add pixels to the boundaries of object in image.After that the histogram equalization had been done. The idea behind this is that the pixel should be distributed evenly over whole intensity range.

The next step is Gaborfiltering, which is named after, DennisGabor, and is used for the edge detection. At last we perform the minutiae points detection. Comparison of one finger with another can be made using minutiae.

GRAPHICAL USER INTERFACE FOR FINGERPRINT RECOGINTION AND AUTHENTICATION USING IMAGE FUSION WITH FOLLOWING ALGORTHIM

Step 1-Collection of Database.

Step 2- The main menu to enter name from database

Step 3- The authentication menu in which fingerprint of candidate enter

Step4- The firstfingerprint should be entered

Step 5- The first fingerprint converted to grayscale

Step 6- The first fingerprint is minutia extracted

Step 7- The second fingerprint should be entered

Step 8- The second fingerprint is minutia extracted

Step 9- The first and second fingerprint performGabor filtering

Step 9- The first and second fingerprint perform orientation image

Step 10- The first and second fingerprint perform template formation

Step 11- The first and second fingerprint perform feature extraction.

Step 12-The authentication of user found in database.

COMPARISON

In the traditional systems, finger prints are scanned single finger. The traditional pattern matching method for fingerprint verification verifies the identity of the patterns by directly comparing the objective fingerprint images with the registered image. Traditional encryption is not sufficient for fingerprint privacy protection because decryption is required before the fingerprint matching, which exposes the fingerprint to the attacker. To avoid thissituation, we propose here a system for protecting finger print privacy by combining two totally different fingerprints into a new identity.

RESULT AND DISCUSSION

.

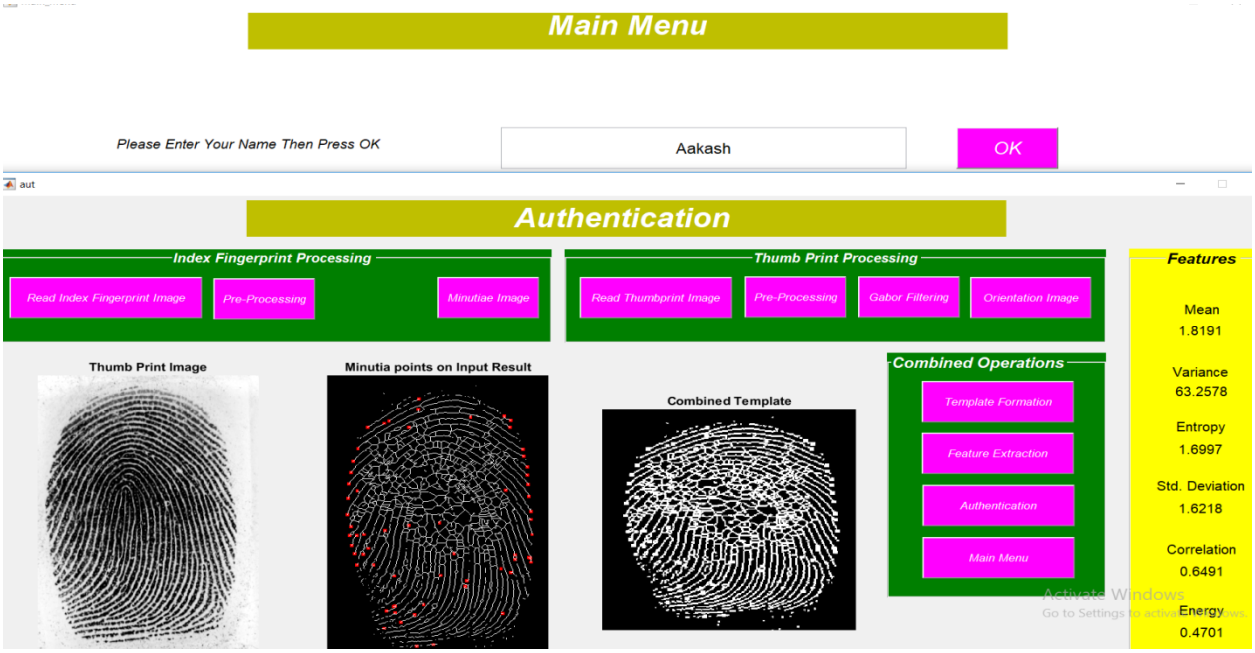

Figure 2: Result of Proposed System

The fingerprint minutia matching is implemented in MATLAB. The fingerprint of different person is collected in database in the form of image. The image is than converted to MATLAB code. The analysis are done on totally different collection of fingerprint image. These images are applied Gabor flitering method for better matching.

CONCLUSION

The above proposed methodology was really an effort to understand how the Fingerprint Recognition is used in many applications like biometric measurements, solving crime investigation and also in security system. From minutiae extraction to minutiae matching all stages are included in this proposed method which generates a match score. Various standard techniques are used in the intermediate stage of processing.

REFERENCES

1. F. Chen, J. Feng, A. K. Jain, J. Zhou, and J. Zhang, “Separatingoverlapped fingerprints,” *IEEE Trans. Inf. Foren. Secure* 2011*;* 76(10): .346–359.
2. J. Feng, Y. Shi, J. Zhou, “Robust and efficient algorithms for separating latent overlapped fingerprints”, IEEE Trans Inf Forensics Secure, 2012; 7(5): 1498–1510
3. Q. Zhao, A. Jain, “Model based separation of overlapping latent fingerprints”, IEEE Trans Inf Forensics Secure 2012; 7(3): 904–918,.
4. N. Zhang, Y. Zang, X. Yang, X. Jia, J. Tian, “Adaptive orientation model fitting for latent overlapped fingerprints separation”, IEEE Trans Inf Forensics Secure, 2014; 9(10):1547–1556
5. S. Jeyanthi, N.U. Maheswari and R. Venkatesh. "Neural network based automatic fingerprint recognition system for overlapped latent images." Journal of Intelligent & Fuzzy Systems, 2015; 28(6): 2889-2899.
6. Ross and A. Othman, “Visual cryptography for biometric privacy,” IEEE Trans. Inf. Forensics Security ,Mar 2011; 6(1): 70–81.