STM JOURNALS

E - Commerce for Future & Trends

Volume 1, Issue 1
www.stmjournals.com

Personal Authentication-Based Fingerprint Recognition

Mokkapati Sanjana*, Penmetsa Sruthi, Palisetty Aruna Kumari, Ch Bindu Madhuri
Department of Computer Science and Engineering,
Jawaharlal Nehru Technical University, Kakinada Vizianagaram campus,
Vizianagaram, Andhra Pradesh, India

Abstract

As our society has become more and more electronically connected and more proxy representations of identity such as passwords cannot be trusted to establish a person's identity, biometrics offers a natural and reliable solution to certain aspects of identity management by utilizing fully automated or semi-automated schemes to recognize individuals based on their inherent physical and/or behavioral characteristics. Human fingerprints contain details called minutiae, which can be used as identification marks for fingerprint verification. The main goal is to develop a fingerprint verification system through extracting and matching minutiae. To extract good minutiae from fingerprints, preprocessing is applied in the form of image enhancement and binarization on fingerprints prior to their evaluation. Many techniques have been combined to build a minutia extractor and a minutia matcher. This system is capable of finding the correspondences between input pattern and the stored template pattern without resorting to exhaustive search. Evaluation of the developed system is done over a database with fingerprints from different people.

Keywords: *Biometrics, fingerprint recognition, authentication, minutia*

****Author for Correspondence*** E-mail: sanjana.mokkapati@gmail.com

INTRODUCTION

Biometric fingerprint technology is penetrating the market at an amazing rate. Biometric tradition offers many advantages over conventional pin number or password and token-based approaches [1]. Biometric-based personal authentication is aimed at determining the claimed identity based on user's physiological (e.g., fingerprint, iris, palm, etc.)/behavioral (e.g., voice, keystroke, etc.) traits. A biometric trait cannot be easily forgotten, exchanged or stolen; the rightful owner of the biometric template can be easily identified. It can be used to eliminate the inconvenience of barcodes, passwords, and PINs. A biometric system is simply a pattern recognition system that works by acquiring data from the sensor, extracting features from it and comparing them against those present in the database. Depending on the context of application, biometric systems operate either in [1] verification mode or identification mode.

- In the verification mode the system verifies the individual's identity by comparing the acquired biometric trait against the individual's own template stored in the database. Such a "one-to-one" search (1:1) is used for physical or computer access.
- In the identification mode, the system verifies the individual's identity by comparing the acquired biometric trait against all templates stored in the database. Such a "one-to-many" search (1: N) is used for identifying criminals.

Fingerprints are graphical flow of ridges and valleys on the human fingerprint surface [2]. But they are not distinguished by their ridges and valleys, but by minutia, which are some abnormal points on the ridges. Among the

variety of minutia types reported in literature, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive (Figure 1).

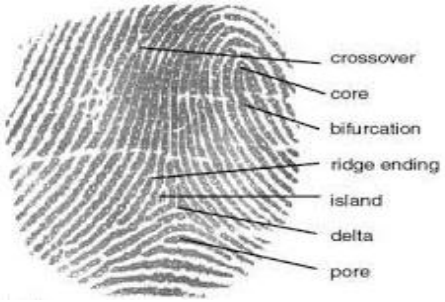

Fig. 1: *Different Minutia Present on the Human Finger Print* [3].

Advantages of fingerprint over other biometrics are:

- Fingerprint is the cheapest, fastest, most convenient and most reliable way to identify someone.
- Human fingerprints are unique.
- High level of accuracy.
- Ability to enroll multiple fingers; if there is some problem with one finger, the fingerprint technology still can be used with the other nine fingers.

RELATED WORK

Fingerprint recognition is one of the oldest and most reliable biometric techniques used for personal identification. Fingerprint recognition has been used for over 100 years now and has come a long way from tedious manual fingerprint matching. The former procedure of matching fingerprints manually was extremely cumbersome and time-consuming and required skilled personnel. But with the advent of technology it has been automated. Fingerprint matching techniques are generally of two types: minutia-based and correlation-based. Minutia-based approaches try to align the two sets of minutia and determine the total number of matched minutia. On the other hand, correlation-based techniques compare the global patterns of ridges and valleys to see if the ridges in the two fingerprints align. The performance of minutia-based techniques relies on the accurate detection and use of minutia points for matching, whereas the performance of correlation-based techniques [4] is affected by non-linear distortions and noise present in the image. Some techniques do not use image enhancement techniques which may lead to inaccurate minutia marking [5].

Gabor function for image enhancement, taking fingerprint ridge orientation and ridge frequencies as filtering parameters that yielded better results [6], presented a binarization-based model using Laplacian operator and dynamic threshold. Here many methods have been combined to build the fingerprint recognition system.

PROPOSED SYSTEM

The proposed fingerprint recognition system is minutia-based and constitutes fingerprint acquiring device, pre-processor, minutia extractor and minutia matcher. In the preprocessing stage, we are using an enhancement algorithm to enhance the ridge and valley patterns so that the extracted features are more accurate (Figure 2). Fingerprint images are rarely of perfect quality.

They may be degraded and corrupted with elements of noise due to many factors including variations in skin and impression conditions. This degradation can result in a significant number of false minutiae being created and genuine minutiae being ignored. A critical step in studying the statistics of fingerprint minutiae is to reliably extract minutiae from fingerprint images. Thus, it is necessary to make use of image-enhancement techniques prior to minutiae extraction to obtain a more reliable marking of minutiae locations.

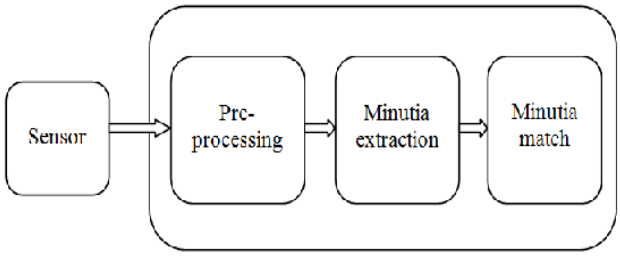

Fig. 2: *Block Diagram for Proposed Fingerprint Recognition System.*

METHODOLOGY

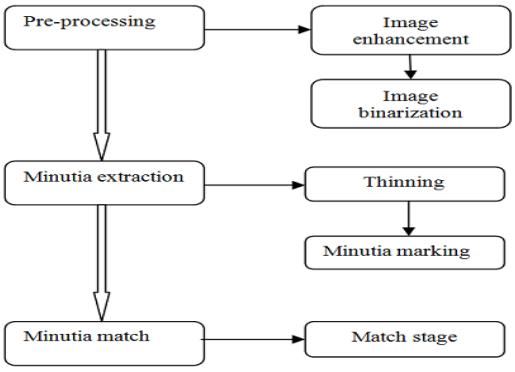

Fig. 3: *Flow Chart for Verification Process.*

The main modules of a fingerprint verification system are shown in the form of flow chart in Figure 3 :

- ***Fingerprint Sensing***, in which the fingerprint of an individual is acquired by a fingerprint scanner to produce a raw digital representation
- ***Preprocessing***, in which the input fingerprint is enhanced and adapted to simplify the task of feature extraction
- ***Feature Extraction***, in which the fingerprint is further processed to generate discriminative properties, also called feature vectors
- ***Matching***, in which the feature vector of the input fingerprint is compared against one or more existing templates

Preprocessing

In order to remove the number of spurious minutiae in the image due to misconnections and isolated regions, preprocessing is performed on the image before feature extraction. Preprocessing methods use a small neighborhood of a pixel in an input image to get a new brightness value in the output image. Different steps followed are *image enhancement* and *image binarization*

Fingerprint image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors are not assured with perfect quality, enhancement methods increase the contrast between ridges and valleys. Image binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white. These steps try to compensate for variations in lightening and contrast that occur during image acquisition.

Minutia Extraction

The reliability of any fingerprint recognition system strongly relies on the precision obtained in the minutia extraction process. A number of factors are detrimental to the correct location of minutia. The concept of crossing number (*CN)* [6] is used for extracting the minutiae**.** Before features are extracted from the image thinned has to be performed on it in order to eliminate the redundant pixels. An iterative, parallel thinning algorithm is used for thinning. After thinning, marking minutia points is relatively easy. Considering a 3×3 window, if the central pixel is 1 and has exactly 3 one-value neighbors, then the central pixel is a ridge branch. If the central pixel is 1 and has only 1 one-value neighbor, then the central pixel is a ridge ending

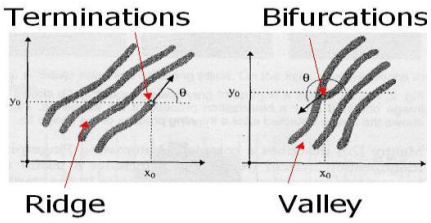

Fig. 4: *Ridge and Valley Patterns on the Human Finger* [8].

Termination is also called as ridge ending and bifurcation is also known as a branch.

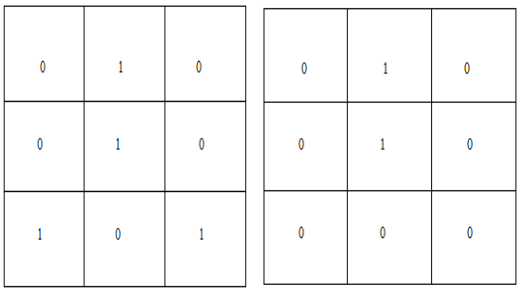

Fig. 5: *Illustration of Crossing Number Concept (a) Termination (Ridge Ending) (b) Bifurcation (Ridge Branch).*

After a successful extraction of minutiae, they are stored in a template, which may contain the minutia position (x, y), minutia type (bifurcation or termination), and in some cases the minutia quality may be considered. During enrollment, the extracted templates are stored in the database and are used in the matching process as reference template or database template. During verification or identification, the extracted minutia are also stored in a template and are used as query template during matching

Minutia Match

After we get two sets of minutia points, we count the matched minutia pairs by assuming that minutiae having nearly the same position and direction are identical. The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. The score is 100*ratio and ranges from 0 to 100. If the score is larger than a pre-specified threshold, the two fingerprints are from the same finger. The percent score shows whether the fingerprint is authorized or not.

EXPERIMENTAL RESULTS

The implantation of the work was done by using the MATLAB software.

Fig. 6: *Original Image Sensed from the Sensor.*

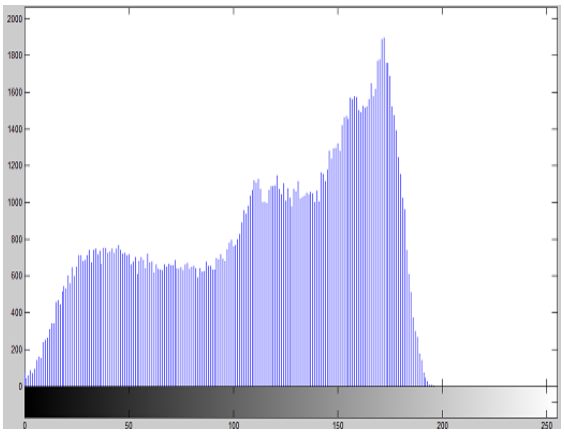

Fig. 7: *Histogram Equalization of the Original Image.*

Fig. 8: *Image Obtained after Enhancing the Original Image.*

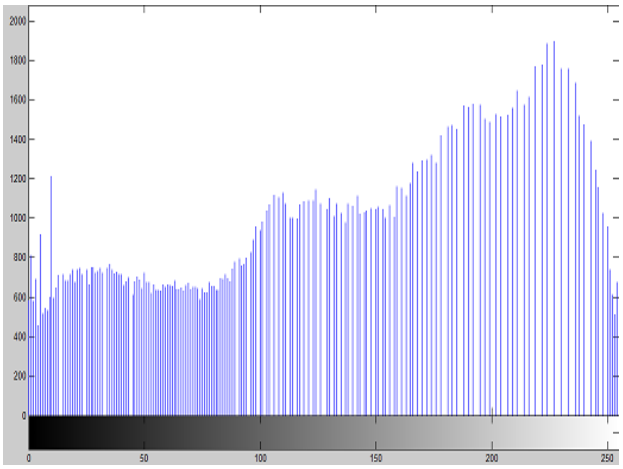

Fig. 9: *Histogram Equalization of the Enhanced Image.*

The matching performance of fingerprint verification systems is measured by two error measures known as false acceptance rate (FAR) and false rejection rate (FRR) [9]. The false acceptance rate (FAR) is the probability that the system outputs "match" for fingerprints that are not from the same finger. The false rejection rate (FRR) is the probability that the system outputs "non-match" for fingerprints that originate from the same finger.

Fig.10: *Image Obtained after Binarizing the Enhanced Image.*

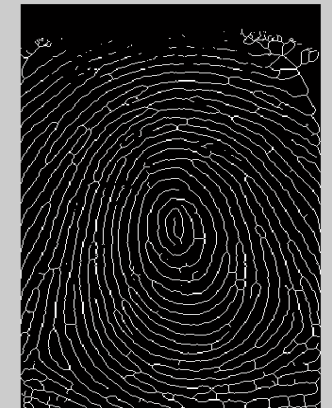

Fig.11: *Image Obtained after Thinning the Binarized Image.*

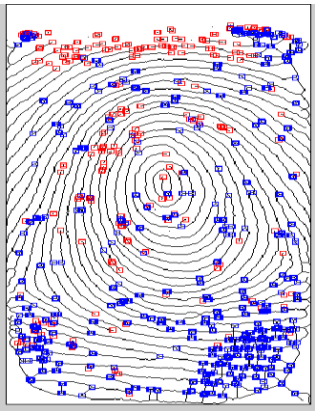

Fig.12: *Marking of Minutia for Template Generation.*

No. of persons accepted from out of database
FAR = ——————————————
Total no. of persons in database

No. of correct persons rejected
FRR = ——————————————
Total no. of persons in database

FAR	0.08
FRR	0.5

Fig. 13: *Table Showing the FAR and FRR over a Database.*

CONCLUSIONS

The authors have presented a model for personal identification based on fingerprint recognition. The future work will concentrate on improvement in terms of efficiency and accuracy which can be achieved by improving the image preprocessing techniques so that the input image to the thinning stage could be made better. This could improve the later stages and the final outcome.

REFERENCES

1. Abhishek Rawat. *Hierarical Fingerprint Matching System.* Thesis submitted to Department of Computer Science and Engineering, IIT Kanpur. 2009.
2. Raymond Thai. *Fingerprint Image Enhancement and Minutiae-Extraction.* Thesis submitted to School of Computer Science and Software Engineering, University of Western Australia.
3. Google images link- https://www.google.co.in/fingerprint
4. Roberge D, Soutar C, Vijayakumar B. High-speed fingerprint verification using optical correlator. In: *Proceeding SPIE*. 1998; 3386: 123–33p.
5. Hong L, Wan Y, Jain AK. Fingerprint image enhancement algorithm and performance evaluation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 1998; 20(8): 777–89p.
6. Moayer B, Fu KS. A tree system approach for fingerprint recognition. *IEEE Trans. Pattern Anal. Mach. Intell.* 1986; 8(3): 376–87p.
7. Rutovitz D. Pattern recognition. *J. Roy. Stat. Soc.* 1966; 129: 504–30p.
8. Singh Rohit, Shah Utkarsh, Gupta Vinay. *Thesis*, Department of Computer Science and Engineering, IIT Kanpur, 2009
9. Wikipedia-link http://en.wikipedia.org/wiki/Fingerprint_recognition