Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.616 – 622

RESEARCH ARTICLE

Fingerprint Authentication System Using Minutiae Matching and Application

M.Sathiya Moorthy[1], R.Jayaraj[2], Dr. J. Jagadeesan[3]

[1]M.Tech Student, Department of Computer Science and Engineering, SRM University, India

[2]Asst. Prof (O.G)/ Dept. of Information Technology, SRM University, India

[3]HOD, Department of Computer Science and Engineering, SRM University, India

[1] msathya2010@gmail.com; [3] hod.cse@rmp.srmuniv.ac.in

Abstract—Fingerprints are the most widely used biometric feature for person identification and verification in the field of biometric identification. Fingerprints possess two main types of features that are used for automatic fingerprint identification and verification: (i) global ridge and furrow structure that forms a special pattern in the central region of the fingerprint and (ii) minutiae details associated with the local ridge and furrow structure. This paper presents the implementation of a minutiae based approach to fingerprint identification and verification and serves as a review of the different techniques used in various steps in the development of minutiae based Automatic Fingerprint Identification System (AFIS). The technique conferred in this paper is based on the extraction of minutiae from the thinned, binarized and segmented version of a fingerprint image.

Keywords— Fingerprint, Enhancement, Segmentation, Minutiae Extraction, Minutiae Matching

I. INTRODUCTION

With the recent advancement in information communication technology, the need for secure personal authentication methods has increased rapidly. Conventionally, IC cards and passwords are widely used and are popular in personal authentication. However, these methods have several drawbacks. The major disadvantage is that the IC cards could be stolen or faked, and in the case of passwords, they could become known to others by trial and error or other methods.

Fingerprints have been in use for biometric recognition since long because of their high acceptability, immutability and individuality. Immutability refers to the persistence of the fingerprints over time whereas individuality is related to the uniqueness of ridge details across individuals. Fingerprint authentication is one of the most important biometric technologies [4]. A fingerprint is the pattern of ridges and valleys (furrows) on the surface of the finger.

This paper focuses on fingerprints, which can provide personal authentication at high accuracies and low cost in a small-scale project. Firstly, Fingerprint image is obtained from sensor. And this image is enhanced because enhancement algorithm can improve the clarity of the ridge structures of input fingerprint images, then the enhancement image is binarized by fixing the threshold value. The binarization image is thinned using morphological operations. Then the output image is segmented for minutiae extraction. After minutiae extraction, false minutiae are removed by using Euclidean distance. After preprocessing, the existing data collection and template data collection are matched by using two steps (registration and verification).

II. RELATED WORK

Jinwei Gu, et at., [5] proposed a method for fingerprint verification which includes both minutiae and model based orientation field is used. It gives robust discriminatory information other than minutiae points. Fingerprint matching is done by combining the decisions of the matchers based on the orientation field and minutiae.

Manvjeet Kaur et al., [6] have introduced combined methods to build a minutia extractor and a minutia matcher. Segmentation with Morphological operations used to improve thinning, false minutiae removal, minutia marking. Haiping Lu et al., [3] proposed an effective and efficient algorithm for minutiae extraction to improve the overall performance of an automatic fingerprint identification system because it is very important to preserve true minutiae while removing spurious minutiae in post-processing.

The matching stage computes the Euclidean distance between the template finger code and the input finger code. The method gives good matching with high accuracy.

III. DESIGN AND IMPLEMENTATION SYSTEM

A. System Level Design

A fingerprint recognition system contributes of fingerprint acquire device for generating digital image of fingerprint, Minutiae Extractor and Minutiae Matcher as shown in Fig. 1.

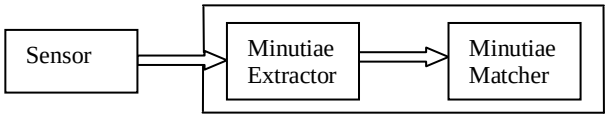

Figure 1. System Level Design

B. Procedures of Fingerprint Recognition System

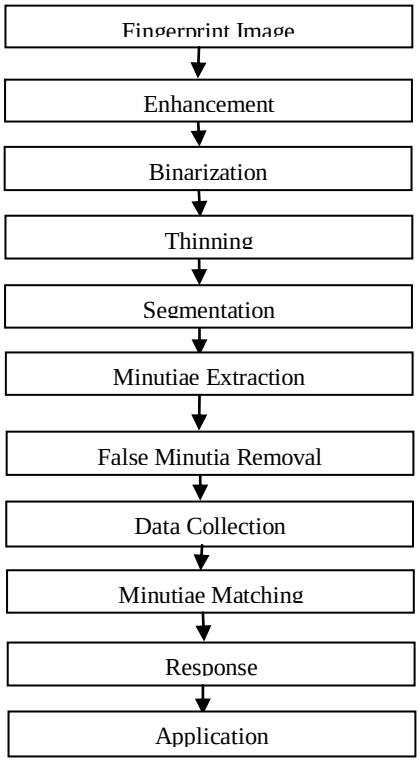

Figure 2. Procedures of Fingerprint Recognition System

C. Overall Diagram of Fingerprint Authentication and Application

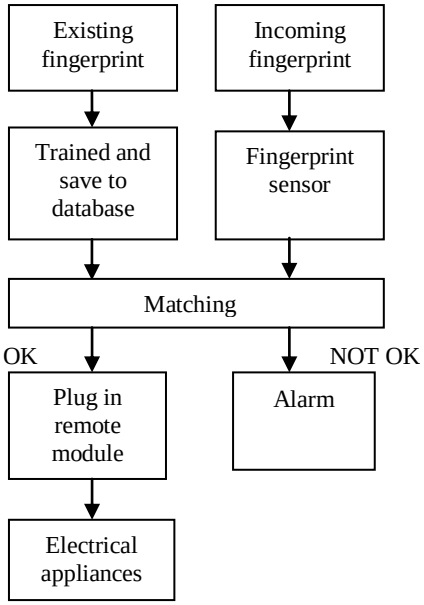

Figure 3. Overall Diagram of Fingerprint Authentication and Application

D. Fingerprint Image Processing

Following are the various steps during image Preprocessing stage. Fig. 4 shows selecting an image to preprocess.

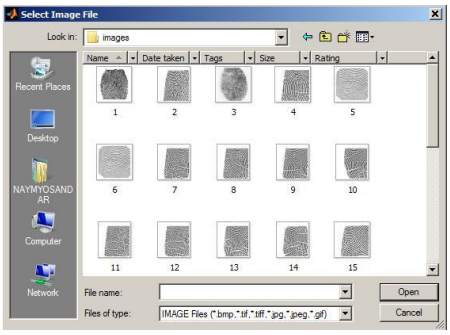

Figure 4. Selecting an Image to Preprocess

1. Enhancement

An enhancement algorithm which can improve the clarity of the ridge structures of input fingerprint images and can improve the performance of the minutiae extraction algorithm, and for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful to keep a higher accuracy to fingerprint recognition. Fig. 5(b) is shown the output of image enhancement

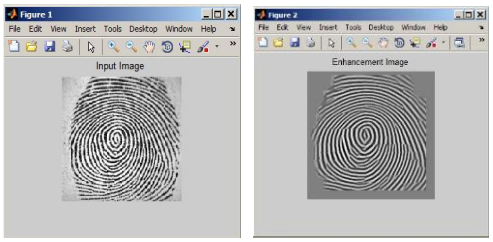

Figure 5. (a) Input Image (b) Enhanced Image

2. Binarization

Binarization is to convert gray scale image into binary image by fixing the threshold value. The pixel values above and below the threshold are set to '1' and '0' respectively. Binarized image can be seen in Fig. 6.

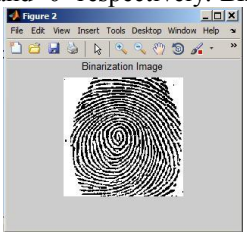

Figure 6. Binarized Image

3. Thinning

The binarized image is thinned to reduce the thickness of all ridge lines to a single pixel width no discontinuities. Each ridge should be thinned to its centre pixel. Noise and singular points should be eliminated. No further removal of pixels should be possible after completion of thinning process (Fig. 7).

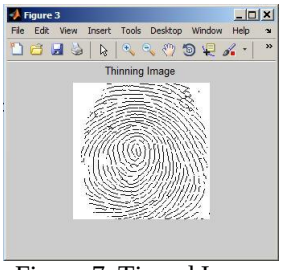

Figure 7. Tinned Image

4. Segmentation

Fingerprint segmentation (Fig. 8) is an important part of a fingerprint identification and verification system. In general, only a Region of Interest (ROI) is useful to be recognized for each fingerprint image. The image area without effective ridges and furrows is first discarded since it only holds background information.

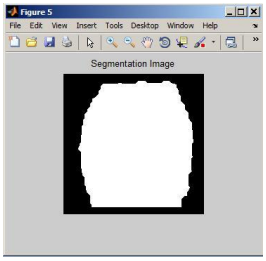

Figure 8. Segmented Image

5. Minutiae Extraction Technique

Minutiae extraction is just a trivial task of extracting singular points in a thinned ridge map. The performance of currently available minutiae extraction algorithms depends heavily on the quality of input fingerprint images.

The minutiae location and the minutiae angles are derived after minutiae extraction. The terminations which lie at the outer boundaries are not considered as minutiae points, and Crossing Number is used to locate the

minutiae points in fingerprint image Rutovitz's definition of crossing number for a pixel 'P' is defined as half the sum of the differences between pairs of adjacent pixels defining the 8-neighborhood of 'P'.
Mathematically,

$$C_{n=}\frac{1}{2}\sum_{i=1}^{8}|\text{val}\,(P_{\text{imod}8}) - \text{val}(P_{i-1})|$$

Where P_0 to P_7 are the pixels belonging to an ordered sequence of pixels defining the 8-neighborhood of P and val(P) is the pixel value.
Fig. 9 shows the extracted minutiae points. Red circle (ro) shape shows the position of termination and green circle (go) shape shows the position of bifurcation.

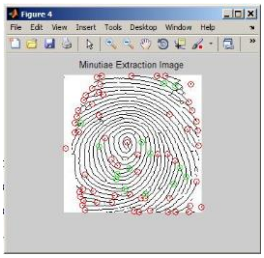

Figure 9. Minutiae Extraction Image

6. False Minutia Removal

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated [2].

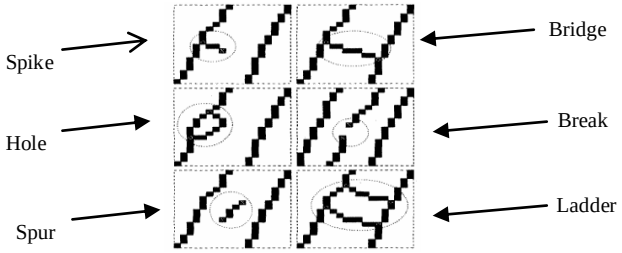

Figure 10. Types of False Minutiae

7. Minutiae Matching

Matching is the final stage of this study. It is needed to verify one that person must be registered before. So the steps are: 1. Registration, 2. Verification (Fig. 11).

1. Registration: In this process, the process takes the one's fingerprint as an image format and processed that image as few steps such as filtering, enhancing, lining and shaping. Then it requires selection of minutiae points as feature then generates a template and stores it. The authenticate template contains the total number of minutiae points limited by a bindings named limited region to improve the flexibility of verification, and then find out the co-relation among the features bounded by limited region.

Verification: To verify one, the process takes one's fingerprint as an image format through fingerprint acquisition hardware and processed that. Then it requires technique to detect minutiae points and selects features, and then to verify, load the templates and compare with the information gathered from verifying one. If it obtains any template matched with that of verifying one, it makes a decision that one was authenticated, or not.

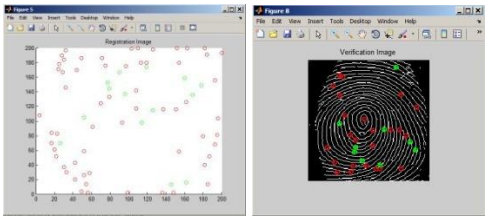

Figure 11. Minutiae Matching by Using Registration and Verification Steps

Figure 12. Message Box to Continue or Not.

If this fingerprint is from the same person it will show YES. Then it will drive an electronic hardware to open the gate etc. If it is not from the same person it will show NO and it will not open the gate.
The next step is to change if the unauthorized person to be the authorized person. For example, a person newly appointed at an office is an authorized person. So the office supretendent must allow him/her to go into the office. So the supretendent must register that newly appointed person and the software will allow him/her to enter the office. If the supretendent does not register, the software will not allow him/her to enter the office.
Applications can be used in Banks (Electronic Banking), Airports (Entry), Army Head Quarters (Entry), Ammunition Stores (Entry), Nuclear Power Plants (Entry), Research Departments (Entry), Government Offices (Attendance), Schools (Attendance), Universities (Attendance), Intelligent Offices (Entry and Attendance), Border Pass Areas (Pass), Quarantine Areas (Entry), Home Security (Entry), Rocket Launching (Switch), Opening Ceremonies (Switch) etc.

Algorithm: Matching

1. Take X and Y as two co-ordinates.
2. Take a minutiae point (I th), where 1<=I<=total minutiae points.
3. Now, take another minutiae point J th, Where 1<=J<=total minutiae points and I!=J.
4. if Y_I=Y_J then
DISTANCE: =X_J-X_I
if DISTANCE <0 then
DISTANCE:=DISTANCE×(-1);
else if (Y_I>Y_J) then
if (Y_I-Y_J:=1) or (Y_I-Y_J:=-1) then
DISTANCE:=0
else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2) then
DISTANCE:=Y_I-Y_J
else DISTANCE:=(Y_I-Y_J)-2
*DISTANCE:=(DISTANCE*WIDTH) +(WIDTH-X_J)+X_I*
else if (Y_I-Y_J):=1 or(Y_I-Y_J):=-1
then DISTANCE:=0
else if (Y_I-Y_J:=2) or (Y_I-Y_J:=-2)
then DISTANCE:=Y_J-Y_I
else DISTANCE:=(Y_J-Y_I)-2
*DISTANCE := (DISTANCE*WIDTH) +(WIDTH-X_I)+X_J*
5. Repeat step 1,2 & 3 for the verified image also.
6. Find the equality of minutiae points (M1 & M2), as EQ: = matched (M1, M2)/greater (M1, M2);
7. Calculate total number of correlated distances DISTANCE-of-both

IV. LIMITATION

There are some limitations in matching live-fingerprint from fingerprint sensor. Because some images from the sensor are not typical or standard images due to mal position, distortion, and not full images. So this may lead to mismatched results.
The performance of a fingerprint feature extraction and matching algorithm critically upon the quality of the input fingerprint image. It is very important to acquire good quality images but in practice a significant percentage of acquired images are of poor quality due to some environmental factors or user's body condition. While the 'quality' of a fingerprint image cannot be objectively measured, it roughly corresponds to the clarity of the ridge structure in the fingerprint image. Whereas a 'good' quality fingerprint image has high contrast and well-defined ridges and valleys, a 'poor' quality fingerprint is marked by low contrast and ill-defined boundaries between the ridges. There are several reasons that may degrade the quality of a fingerprint image.
(1) Presence of creases, bruises or wounds may cause ridge discontinuities.
(2) Excessively dry fingers lead to fragmented and low contrast ridges.
(3) Sweat on fingerprints leads to smudge marks and connects parallel ridges.

(4) Skin diseases such as dermatitis, psoarisis can produce poor fingerprint images.

It is estimated that roughly 10% of the fingerprint encountered during verification can be classified as 'poor' [1]. Poor quality fingerprints lead to generation of spurious minutiae. In smudgy regions, genuine minutiae may also be lost, the net effect of both leading to loss in accuracy of the matcher.

ACKNOWLEDGEMENT

First of all, the author would like to express her special thanks to His Excellency Dr T.R.Pachamuthu. The author would like to express her respectful gratitude to, Principal of SRM University for allowing to develop this research and giving her general guidance during period of her study.

Finally, the author is grateful to her parents who specifically offered strong moral and physical support, care and kindness.

REFERENCES

[1] D. Maio, D. Maltoni, A.K. Jain, S. Prabhakar, Handbood of Fingerprint Recognition, Springer, Berlin, 2003.

[2] L.C. Jain, U. Halici, I. Hayashi, S.B. Lee, and S. Tsutsui, "Intelligent biometric techniques in fingerprint and face recognition", The CRC Press, 1999.

[3] Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, "*Fingerprint Verification System using Minutiae Extraction Technique",* Proceedings of World Academy of Science, Engineering and Technology vol. 36, pp. 497-502, (2008).

[4] Newham, E.: The Biometric Report. SJB Services. New York (1995).

[5] Robert Hastings, "*Ridge Enhancement in Fingerprint Images Using Oriented Diffusion",* IEEE Computer Society on Digital Image Computing Techniques and Applications, pp. 245-252, (2007).

[6] Unsang Parh, Sharath Pankanti, and A. K. Jain, "*Fingerprint Verification using SIFT Features",* SPIE Defense and Security Sysmposium, (2008).

