ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department Of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Personal Authentication using Fingerprint Biometric System

V Prasathkumar[1], Mrs. V. Evelyn Brindha[2]

PG Scholar, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India[1]

Associate Professor, Department of CSE, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India[2]

ABSTRACT— A significant step in automatic fingerprint matching is to automatically and constantly extract minutiae from the input fingerprint images. However, the presentation of a minutiae extraction algorithm relies heavily on the excellence of the input fingerprint images. In order to make certain that the presentation of an automatic fingerprint identification/verification system will be strong with respect to the excellence of input fingerprint images, it is necessary to incorporate a fingerprint enhancement algorithm in the minutiae extraction module. We present a high-speed fingerprint authentication algorithm, which can adaptively improve the simplicity of ridge and valley structures of input fingerprint images based on the estimated local ridge orientation and frequency. We have evaluated the presentation of the image enhancement algorithm using the goodness index of the extracted minutiae and the exactness of an online fingerprint verification system. An experimental result shows that the verification algorithm improves both the goodness appearance and the verification accuracy.

KEYWORDS—Biometrics, fingerprint, minutiae, enhancement, Gabor filters, performance evaluation

I. INTRODUCTION

Biometrics (or biometric authentication) refers to the identification of humans by their characteristics or traits. Biometric identifiers are often categorized as physiological and behavioral characteristics. Physiological uniqueness is associated to the shape of their body. Examples are fingerprint, face recognition, DNA, Palm print, hand geometry, iris recognition, retina and so on. Behavioral uniqueness is associated to the pattern of proceedings of a person. Examples are typing rhythm, gait, and voice. Fingerprint identification is one of the most significant biometric technologies which have drawn a significant amount of consciousness recently. A fingerprint is the outline of ridges and valleys (also called furrows in the fingerprint literature) on the exterior of a fingertip. Each individual person has distinctive fingerprints. The uniqueness of a fingerprint is completely determined by the local ridge uniqueness and their associations. A total of 150 different local ridge uniqueness (islands, short ridges, enclosure, etc.) have been recognized. This local ridge uniqueness is not regularly distributed. Most of them depend seriously on sense conditions and excellence of fingerprints and are hardly ever experimental in fingerprints. The two most excellent local ridge uniqueness, called minutiae, are

1) Ridge ending and
2) Ridge bifurcation

A ridge ending is defined as the point where a ridge ends immediately. A ridge bifurcation is defined as the point where a ridge forks or diverges into branch ridges. A high-quality excellence fingerprint typically contains about 40–100 minutiae in each. Examples of minutiae are shown in Fig. 1.Automatic fingerprint matching depends on the comparison of these local ridge characteristics and their associations to make a personal recognition. A significant step in fingerprint matching is to repeatedly and constantly extract minutiae from the input fingerprint images, which is a tricky task.

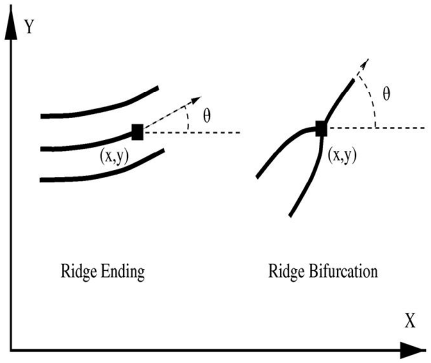


Fig. 1. Examples of minutiae. (a) A minutiae can be characterized by its position and its point of reference.

Fingerprint enrichment can be conducted on either binary ridge images or gray-level images.A binary ridge image is an image wherever all the ridge pixels are assigned a value one and non-ridge pixels are assigned a value zero. The binary image can be obtained by applying a ridge removal algorithm on gray level intensity fingerprint image. Since ridges and valleys in a fingerprint image blinking and run consequent to each other in a local neighborhood, a number of difficult heuristics can be used to differentiate the ridge understanding from true ridge understanding in a binary ridge image.

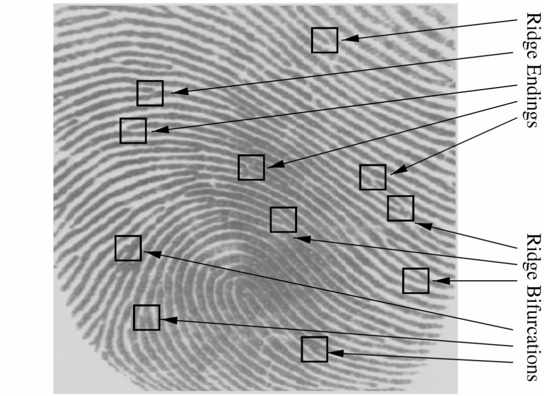


Fig. 1. Examples of minutiae (b) Minutiae overlaid on a fingerprint image.

In a gray-level fingerprint image, ridges and valleys in a local neighborhood form a sinusoidal shaped plane wave which has a clear frequency and orientation. A number of techniques that take benefit of this in order to propose enhance gray-level fingerprint images. However, they typically imagine that the local ridge orientations can be consistently predictable. In performance, this statement is not suitable for fingerprint images of reduced quality, which really restricts the applicability of these techniques.

In the following sections, we will explain in detail our fast fingerprint verification algorithm. Section 2 addresses the main steps of our algorithm. A goal-directed presentation assessment of the implemented fingerprint verification algorithm on fingerprint databases (Experimental Results) is described in Section 3. Section 4 contains the conclusion and discussion.

II. FINGERPRINT AUTHENTICATION

A fingerprint image authentication algorithm receives an input fingerprint image, applies a set of transitional steps on the input image, and to conclude output as a improved image. In order to initiate our fingerprint image authentication algorithm, a list of notations and some basic definitions are given below.

A. Notation

A gray-level fingerprint image is defined as an N x N matrix, where G(i, j) represents the intensity of the pixel at the ith row and jth column. We suppose that all the images are scanned at a declaration of 500 dots per inch (dpi), which the resolution is suggested by frequency based intensity. The mean and variance of a gray-level fingerprint images are defined as

$$\mathrm{M(I)}=\frac{1}{N^{2}}\sum_{I=0}^{N-1}\sum_{J=0}^{N-1} I(i,j) \qquad (1)$$

and

$$\mathrm{VAR(I)}=\frac{1}{N^{2}}\sum_{I=0}^{N-1} s \qquad (2)$$

respectively. An orientation image, O, is defined as an N x N image, where G(i, j) represents the local ridge orientation at pixel (i, j). Local ridge orientation is typically specified for a block rather than at every pixel. An image is divided into a set of w x w non overlapping blocks and a single local ridge orientation is defined for each block. and not as an independent document.

B. Algorithm

The flowchart of the fingerprint enhancement algorithm is shown in Fig. 2. The main step of the algorithm includes:

1) Binarization: An input fingerprint image is binarized so that it has a prespecified mean and variance.

2) Elimination of noise: The image noise can be eliminating by using the median filter.

3) Thinning: The fingerprint image is computed from the binarization input fingerprint image and the estimated thinning image.

4) Minutiae extraction: The region mask is obtained by classifying each block in the thinning input fingerprint image into a bifurcation and a ridge ending.

5) Minutiae matching: the minutiae points can be matched to other fingerprint. If fingerprint is recognized as authenticate one then to access it.

C. Binarization

Let G(i, j) denote the gray-level value at pixel (i, j), M and VAR denote the estimated mean and variance of **I**, respectively, and G(i, j) denote the gray-level value at pixel (i, j). The grayscale image is defined as above equation 1 and 2.An original image is divided into sub-blocks with the size 3x3 and the region of interest of the fingerprint image is obtained. The preferred mean and variance for the image binarizied are resolute according to possessions such as mean and variance of each block.

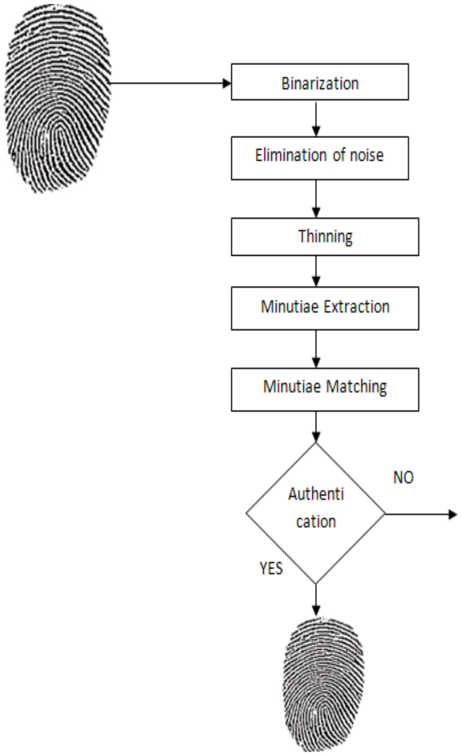


Fig. 2. A flowchart of the proposed fingerprint authentication algorithm.

D. Elimination of noise

Median filtering is similar to using an averaging filter, in that every output pixel is set to an normal of the pixel values in the neighborhood of the equivalent input pixel. However, with median filtering, the value of an output pixel value is determined by the *median* of the neighborhood pixels, pretty than the mean. The median is much less responsive than the mean to tremendous values (called *outliers)*. Median filtering is therefore enhanced able to remove these outliers without reducing the roughness of the image. The medfilt2 function is used to implement through median filtering.

E. Thinning

Thinning algorithm is a Morphological operation that is used to remove selected foreground pixels from binary images somewhat like erosion or opening. It preserves the topology (extent and connectivity) of the original region while throwing away most of the original foreground pixels. It can be used for several applications, but is frequently useful for skeletonization. In this mode it is commonly used to neat up the output of edge detectors by dropping all lines to single pixel thickness. Thinning is applied only for the binary images, and it generates new binary image as a sequence output image.

F. Minutiae Extraction

The next step after thinning of the image is the extraction of minutiae. The improved image is binarised in first . The framework of the image is next formed. The minutiae points are then extracted by the following scheme. The binary image is thinned as a result of which a ridge is only one pixel broad. The minutiae points are thus those which have a pixel value of one (ridge ending) as their neighbor or more than two ones (ridge bifurcations) in their region. This ends the process of extraction of minutiae points. The whole identification process is talented in the, biometric uniqueness of fingerprints are extracted (uniqueness denoted as *minutiae*, which symbolize basically the start, end or bifurcation of a ridge).

Minutiae are effectively terminations and bifurcations of the ridge lines that represent a fingerprint pattern. Regular minutiae recognition is an tremendously vital process, specially in low-quality fingerprints where noise and distinction lack can originate pixel configurations related to minutiae or cover real minutiae.

G. Minutiae Matching

Fingerprints will be matched with templates belonging to the test database. This is the most popular and widely used in commercial applications, because of its good presentation and low calculation time, particularly for good feature images. This method tries to arrange in a line the minutiae of the input image (query template) and stored templates (reference template) and find the number of corresponding minutiae. After alignment, two minutiae are measured in similar if the unusual distance and direction distinction among them are smaller that a given acceptance. A proper aligning of fingerprint is very important in order to make best use of the number of corresponding minutiae; this requires the computing of the transformation and rotation in sequence, as well as other geometrical transformations such as level and alteration.

III. EXPRIEMENTAL RESULTS

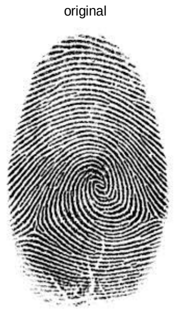


Fig. 3. (a)Input Fingerprint Image

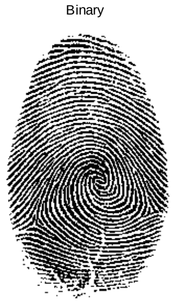


Fig. 3. (b)Binary Fingerprint Image

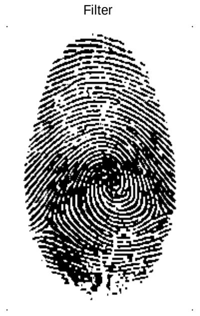


Fig. 3. (c)Elimination of noise in Fingerprint Image

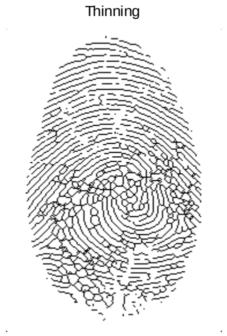
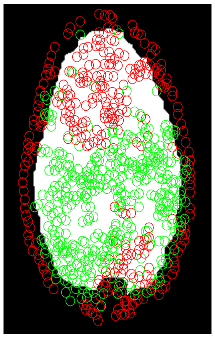


Fig. 3. (d)Thinning of Fingerprint Image



IV. CONCLUSION

The main benefit of this algorithm is its quick running speed. It improves the authentication performance. The algorithm identifies the unrecoverable degraded areas in the fingerprint and removes them from further processing. This is an important feature of the algorithm as the occurrence of these areas would prove to be particularly harmful for the extraction of minutiae points to match the fingerprint database. It helps in removing the spurious minutiae too which may also prove to be harmful in matching fingerprints correctly.

REFERENCES

[1]. L. Hong, A. Jain, S. Pankanti and R. Bolle, "Fingerprint Enhancement", Pattern Recognition, 202-207, 1996.

[2]. K. Jain, L. Hong, S. Pantanki and R. Bolle, "An Identity Authentication System Using Fingerprints", Proc of the IEEE, vol, 85, no.9,1365-1388,1997.

[3]. Y.AlNajjar , "Minutiae extraction for fingerprint recognition", Proceeding of the 5th International conference on signal processing, pp.1–5,2008.

[4]. F.Chen ,X. Huang, , & Zhou, J 2011, "Hierarchical Minutiae Matching for Fingerprint and Palmprint Identification", IEEE transactions, vol. 22, no. 2, pp. 350-360.

[5]. G. Chen, "An improved OPTA fingerprint thinning algorithm based on neighborhood searching", Proceeding of the IEEE International conference on Computer Science and Information Processing (CSIP), pp.637 – 640,2012.

[6]. P. Munshi,"A rough-set based binarization technique for fingerprint images", Proceeding of the IEEE International conference on Signal Processing, pp. 1 – 6,2012.