Volume 2, Issue 10, October 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Feature Extraction Algorithm of Fingerprint Recognition

Prateek Verma*, Yogesh Bahendwar, Amrita Sahu, Maheedhar Dubey
Department of Electronics & Telecommunication
CSVTU
Chhattisgarh, India

Praveen Verma
Asst. Manager, NTPC
Chhattisgarh, India

Abstract- ***Most fingerprint matching algorithms are based on finding correspondences between minutiae in two fingerprints. In this paper we present a modification of minutiae matching method, which utilizes correlation scores between the local neighbourhood areas of corresponding minutiae pairs and the edges that connect neighbouring matched minutiae pairs. Minutiae based matching approach considers the overall minutiae distribution pattern between the two fingerprints. Neighbourhood correlation score represents the local similarity between the matched pair of minutiae. Edge correlation score gives the resemblance of areas that in between the two corresponding minutiae pairs. With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics-based verification, especially fingerprint-based identification, is receiving a lot of attention Biometrics deals with identifying individuals with help of their biological data. We match the finger prints, one that is already in the database of the sensor and second the fingerprint that we enrolled in the sensor currently by using the Boolean function X-ORING. We get the matching score and decide the result on the matching score basis, whether the fingerprint is matched or not. With the basis of that we will give it another application like attendance system.***

Keywords —Fingerprint, Biometrics, Artificial Intelligence, Sensors.

I. INTRODUCTION

The use of biometric systems is growing every day. Neighborhood correlation score represents the local similarity between the matched pair of minutiae. Edge correlation score gives the resemblance of areas that in between the two corresponding minutiae pairs. With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometrics-based verification, especially fingerprint-based identification, is receiving a lot of attention Biometrics deals with identifying individuals with help of their biological data. We match the finger prints, one that is already in the database of the sensor and second the fingerprint that we enrolled in the sensor currently by using the Boolean function X-ORING. We get the matching score and decide the result on the matching score basis, whether the fingerprint is matched or not.

A. *Need for Secured Identification System*

In order to protect users of computer systems and to secure network-based transactions, demand is increasing for improved user authentication process. The hacking of passwords and personal information is increasing day by day.

B. Existing Methods

Reliable user authentication is becoming an increasingly important task in the Web-enabled world. The consequences of an insecure authentication system in a corporate or enterprise environment can be catastrophic, and may include loss of confidential information, denial of service, and compromised data integrity. The value of reliable user authentication is not limited to just computer or network access. The prevailing techniques of user authentication, which involve the use of either passwords and user IDs (identifiers), or identification cards and PINS (personal identification numbers), suffer from several limitations. Passwords and PINS can be illicitly acquired by direct covert observation. Once an intruder acquires the user ID and the password, the intruder has total access to the user's resources. In addition, there is no way to positively link the usage of the system or service to the actual user, that is, there is no protection against repudiation by the user ID owner.

II. FINGERPRINT

A. What is a fingerprint?

Finger skin is made of friction ridges, with pores (sweat glands). Friction ridges are created during fetal live and only the general.Shape is genetically defined. Friction ridges remain the same all life long, only growing up to adult size. They reconductible the same if not too sévère injury.

Fig 1 Fingerprint details

- Minutie are the discontinuités of the ridges.
- Endings, the points at which a ridge stops.
- Bifurcations, the point at which one ridge divides into two.
- Dots, very small ridges.
- Ponds or lakes, empty spaces between two ridges.

B. Types of Fingerprint

Fig 2 Types of fingerprint

We have developed an algorithm to classify fingerprints into all the five classes, namely**,** *whorl, right loop, left loop, arch, and tented arch*.. This information is further quantized to generate a finger code which is used for classification. The classifier is tested on 4,000 images in the given nist-4 database. For the five-class problem, classification accuracy of more than 90% is achieved. By incorporating a reject option, the classification accuracy can further be increased to 96% for the five-class classification and to 97.8% for the four-class classification when 30.8% of the images are rejected.

C. Characteristic of Fingerprint

Personal characteristics often involved with horoscopes and similar non-scientifically proven prophesies. The two first are by far by the greatest areas. Fingerprint-based systems will be discussed. Enormous amounts of information are stored in a given fingerprint database. The same problem does not occur with these fingerprints.

According to the differences between image and text, recently there have been several innovative encryption techniques:

III. DESCRIPTION OF PAPER

In this paper we are just making a comparison between two of the image using X-oring of the pixels. first of all we saves a image in any memory location then the person whose fingerprint is to be matched is asked to place his finger in any of the sensor used, then the software using Matlab matches the image as follows:-

If the image is the RGB image then convert it into the gray scale image using the instruction rgb2gray.

Resize the image in the scale 512*512.

Enhance the image using histogram equalization for greater clarity and brightness.

Start the matching process using instruction X-or and the corresponding pixels are compared.

After comparing all the pixels the image is said to be matched if 90% of the pixels are matched**.**

A. Algorithm Level Design

Level 1:- If the image is the RGB image then convert it into the gray scale image using the instruction rgb2gray.
Level 2:- Resize the image in the scale 512*512.
Level 3:- Enhance the image using histogram equalization for greater clarity and brightness.
Level 4:- Convert the image into its equivalent the binary image using instruction im2bw in the matrix of 0s and 1s.
Level 5:- Start the matching process using instruction X-OR and the corresponding pixels are compared.
Level 6:- for the same pixel, counter is incremented by one.
Level 7:- After comparing all the pixels the image is said to be matched if 92% of the pixels are matched.

IV. SENSOR AND HISTOGRAM METHODOLOGIES

A. Optical Sensor

Firstly the fingerprint is placed in the optical sensor. The ridges are in contact with the sensor for the input image. The light is then illuminated and the reflection is seen so as to get the proper input of the image.

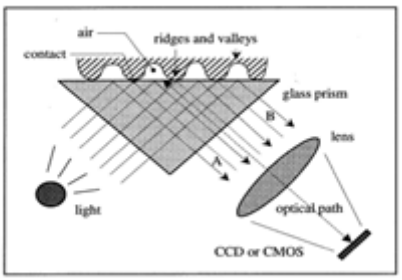

Fig 3 An FTIR-based Fingerprint Sensor

B. Fingerprint Image Preprocessing

B.I Fingerprint Image Enhancement

Fingerprint Image enhancement is to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, 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 for keep a higher accuracy to fingerprint recognition.
Two Methods are adopted in fingerprint recognition system: the first one is Histogram Equalization; the next one is Fourier Transform.

B.II Histogram Equalization:

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. The original histogram of a fingerprint image has the bimodal type [Figure 4.2.2(a)], the histogram after the histogram equalization occupies all the range from 0 to 255 and the visualization effect is enhanced [Figure 4.2.2(a)].

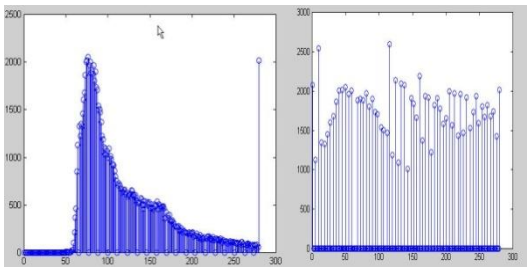

Fig. 4(a) the Original histogram of a fingerprint image (Left) Histogram after the Histogram Equalization (Right)

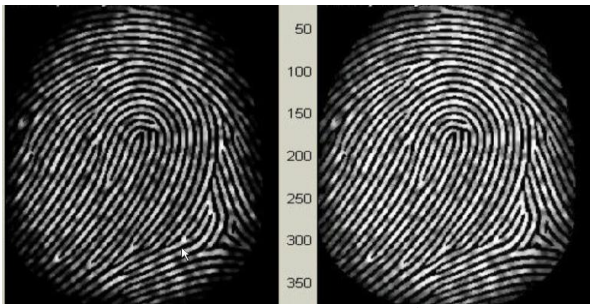

Fig. 4(b) Histogram Enhancement. Original Image (Left). Enhanced image (Right)

B.III Fingerprint Enhancement by Fourier Transform

$$F(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y) \times exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$$

For u = 0, 1, 2... 31 and v = 0, 1, 2... 31.

Where the magnitude of the given original FFT = abs(F(u,v)) = |F(u,v)|.

Get the enhanced block according to $g(x,y) = F^{-1}\{F(u,v) \times |F(u,v)|^{k}\}$ ... (2)

Where $F^{-1}(F(u,v))$ is done by

$$f(x,y) = \frac{1}{MN} \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} F(u,v) \times exp\left\{j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \dots\dots\dots\dots (3)$$

for x = 0, 1, 2... 31 and y = 0, 1, 2... 31.

Thus a termination might be a bifurcation. Fig. 4.2.3 presents the image after FFT enhancement.

V. EXPERIMENTAL RESULT

The method is showing the correct result if we are taking the 92% threshold value. There is scope for future betterment of

the algorithm by using Neural Network technique that can give better results as compared to this approach. With the help of neural network technique accuracy can be improved. Instead of having a constant threshold, it could be made adaptive, depending upon the conditions and the database available, so as to maximize the accuracy.

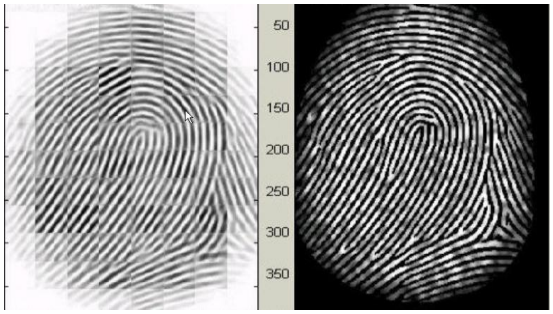

Fig 5 Fingerprint enhancement by FFT
Enhanced image (left), Original image (right)

VI. CONCLUSION & FUTURE SCOPE

In Biometrics-based authentication has many usability advantages over traditional systems such as passwords. Specifically, users can never lose their biometrics, and the biometric signal is difficult to steal or forge. We have shown that the intrinsic bit strength of a biometric signal can be quite good, especially for fingerprints, when compared to conventional passwords. Yet, any system, including a biometric system, is vulnerable when attacked by determined hackers. We have highlighted eight points of vulnerability in a generic biometric system and have discussed possible attacks. We suggested several ways to alleviate some of these security threats. Replay attacks have been addressed using data-hiding techniques to secretly embed a telltale mark directly in the compressed fingerprint image. A challenge/response method has been proposed to check the liveliness of the signal acquired from an intelligent sensor. Finally, we have touched on the often-neglected problems of privacy and revocation of biometrics. It is somewhat ironic that the greatest strength of biometrics, the fact that the biometrics does not change over time, is at the same time its greatest liability. Once a set of biometric data has been compromised, it is compromised forever.

.

A. Full system on a chip

Imagine having the sensor, processor, associated memory, and reference storage all together on the same chip. It would be practically impossible to crack the system by listening to transmission lines or PC connection, and breaking the security by mimicking the data traveling back and forth. This is *the* solution for most applications. Then, the only output is then a yes or no, ciphered with a proper code.

B. In FPUI system (Fingerprint user interfacing)

In this system a person can do the multitasking in which one can do a lot of tasks at a time by assigning different tasks to different fingers.
A table is prepared to match the pre assigned task and it will be performed instantly.

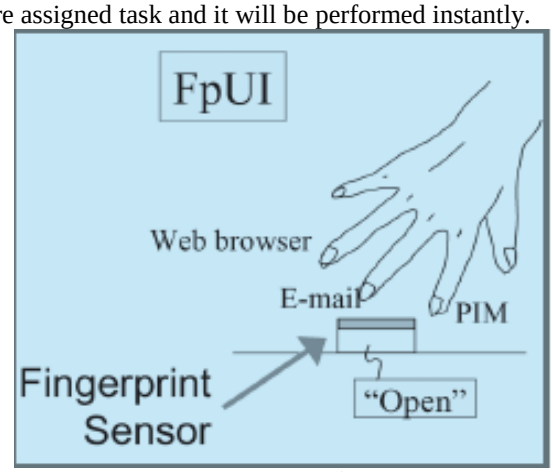

Fig 6 Fingerprint User Interfacing Systems

REFERENCES

[1]. Mazumdar, Subhra; Dhulipala, Venkata (2008). "Biometric Security Using Finger Print Recognition"
[2]. B. Miller, (1994), "Vital Signs of Identity," IEEE Spectrum 31, No. 2, 22–30.

[3]. L. O'Gorman, (2000) "Practical Systems for Personal Fingerprint Authentication," IEEE Computer 33, No. 2, 58–60.
[4]. R. Germain, A. Califano, and S. Colville,(2010) "Fingerprint Matching Using Transformation Parameter Clustering," IEEE Computational Science and Engineering 4, No. 4, 42–49 .
[5]. A. Jain, L. Hong, and S. Pankanti, (2000) "Biometrics Identification," Communications of the ACM 43, No. 2, 91–98.
[6]. B. Schneier, "The Uses and Abuses of Biometrics, (1999)" Communications of the ACM 42, No. 8, 136.
[7]. N. Memon and P. W. Wong, "Protecting Digital Media Content," Communications of the ACM 41, No. 7, 35–43 (1998).
[8]. A. Ross, S. C. Dass, and A. K. Jain, "Fingerprint warping using ridge curve correspondences," Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, no. 1, pp. 19–30, 2006, 0162-8828.
[9]. Z. Jianxin, O. Zongying, and W. Honglei, "Fingerprint matching using phase-only correlation and fourier-mellin transforms," in Sixth International Conference on Intelligent Systems Design and Applications
[10]. B. Schneier, (1996)Applied Cryptography, John Wiley & Sons, Inc., New York.

