Robust LFP-Living Finger Pattern Technique for Authentication

K. Abirami[1], Mrs. G. Jayanthi[2]
[1, 2] Department of ECE
[1, 2] Parisutham Institute of Technology & Science, Thanjavur.

Abstract- *It is a security based concept in the fields where we are using our finger prints. The proposed concept holds two techniques. Using a heartbeat sensor to find the presence of heartbeat in a human body is the initial step followed by creating a pattern for any three fingers in one's hand and analysis the same order of given three finger known only by the person.In MATLABthe approach mainly involves extraction of minutiae points from the sample fingerprint images and then performing fingerprint matching based on the number of minutiae pairings among three fingerprints. Thus no one can access the data of a person whose system holds this security system as that particular person only knows the correct order of the finger pattern for authentication purpose.*

Keywords- Image enhancement, making mask, finding minutiae.

I. INTRODUCTION

Biometric is an automated methodology to uniquely identify human based on their physiological and behavioural characteristics. A lot of biometric characteristics have been proposed for authentication purpose. Traditionally, the biometric method can be categorized into two types: behavioural-based method and physiological based method.

In behavioural based method perform task of authentication based on their behavioural characteristics, such as, keyboard typing, signature, gait and voice. the main problem with behavioural based method they all have large variation, can't cope with and can be difficult to measure because of influences such as illness or stress. The Implementation of behavioural based method less cost.

Physiological-based method perform authentication by means of his and her physiological characteristics such as, face, fingerprint, hand geometry, iris or DNA.

Biometric Technology	Accuracy	Cost	Device Required	Social Acceptability
DNA	HIGH	HIGH	TEST EQUIPMENT	LOW
IRIS RECOGNITION	HIGH	HIGH	CAMERA	MEDIUM - LOW
RETINA SCAN	HIGH	HIGH	CAMERA	LOW
FACIAL RECOGNITION	MEDIUM - LOW	MEDIUM	CAMERA	HIGH
VOICE RECOGNITION	MEDIUM	MEDIUM	MICROPHONE	HIGH
HAND GEOMETRY	HIGH	LOW	SCANNER	HIGH
FINGERPRINT	HIGH	MEDIUM	SCANNER	MEDIUM

Table 1.1 Biometric technology

Fingerprints have been scientifically studied for many years in our society. The characteristics of fingerprints were studied as early as 1600s. Meanwhile, using fingerprints as a means of identification first occurred in the mid-1800s. Sir William Herschel, in 1859, discovered that fingerprints do not change over time and that each pattern is unique to an individual.

FINGERPRINT& HEARTBEAT SENSOR

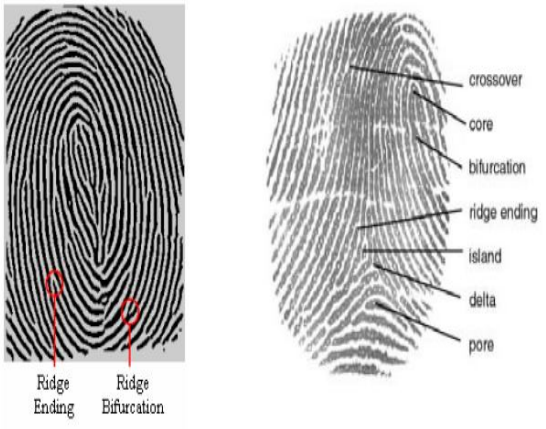
A fingerprint is the feature pattern of one finger. It is an impression of the friction ridges and furrows on all parts of a finger. These ridges and furrows present good similarities in each small local window, like parallelism and average width.

Figure 1.1: Fingerprint image from a sensor

However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges and furrows, but by features called Minutia, which are some abnormal points on the ridges (Figure 1.2). Among the variety

of minutia types reported in literatures, two are mostly significant and in heavy usage:

- Ridge ending - the abrupt end of a ridge
- Ridge bifurcation - a single ridge that divides into two ridges



(a) (b)

Figure 1.2:(a) Two important minutia features
(b) Other minutiae features

PRINCIPLE OF HEARTBEAT SENSOR

The heartbeat sensor is based on the principle of photo phlethysmography. It measures the change in volume of blood through any organ of the body which causes a change in the light intensity through that organ (a vascular region).

In case of applications where heart pulse rate is to be monitored, the timing of the pulses is more important. The flow of blood volume is decided by the rate of heart pulses and since light is absorbed by blood, the signal pulses are equivalent to the heart beat pulses.

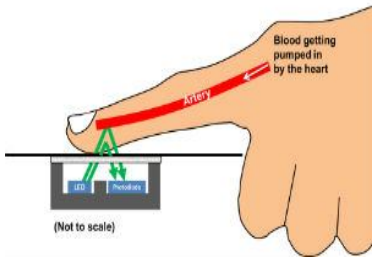


Figure 1.3: Heartbeat sensor

II. AFINGERPRINT RECOGNITION

Fingerprint recognition (sometimes referred to as dactyloscopy) is the process of comparing questioned and known fingerprint against another fingerprint to determine if the impressions are from the same finger or palm. It includes two sub-domains: one is fingerprint verification and the other is fingerprint identification. In addition, different from the manual approach for fingerprint recognition by experts, the fingerprint recognition here is referred as AFRS (Automatic Fingerprint Recognition System), which is program-based.

However, in all fingerprint recognition problems, either verification(one to one matching) or identification(one to many matching), the underlining principles of well-defined representation of a fingerprint and matching remains the same.

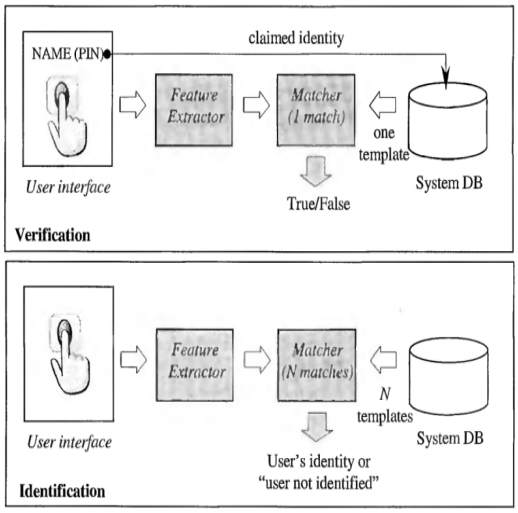


Figure 2.1 Verification vs. Identification

FINGERPRINT MATCHING TECHNIQUES:

The large number of approaches to fingerprint matching can be coarsely classified and they are.

- **Fingerprint Image Enhancement**

Fingerprint Image enhancement is used to make the image clearer for easy further operations. Since the fingerprint images acquired from scanner or any other media are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and valleys 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.

Originally, the enhancement step was supposed to be done using the canny edge detector. But after trial, it turns out that the result of an edge detector is an image with the borders of the ridges highlighted. Using edge detection would require the use of an extra step to fill out the shapes which would consume more processing time and would increase thecomplexity of the code

Figure 2.2Image Enhancement

Enhancement by Fourier Transform

We divide the image into small processing blocks (32 by 32 pixels) and perform the Fourier transform according to

$$F(u,v) = \sum_{X=0}^{M-1}\sum_{Y=0}^{N-1} f(x,y).exp\left\{-2j2\frac{\pi}{1}.\left(\frac{ux}{M} + \frac{vy}{N}\right)\right\}$$

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

Minutia Marking

After the fingerprint ridge thinning, marking minutia points is relatively easy. The concept of Crossing Number (CN) is widely used for extracting the minutiae.

In general, for each 3x3 window, if the central pixel is 1 and has exactly 3 one-value neighbour, 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 i.e., for a pixel P, if Cn(P) = = 1 it's a ridge end and if Cn(P) = = 3 it's a ridge bifurcation point.

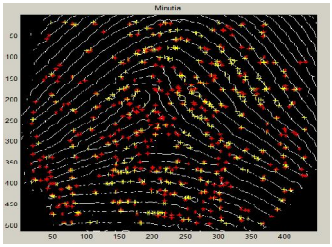


Figure 2.3:Minutia Marking

False Minutia Removal

The pre-processing stage does not usually fix the fingerprint image in total. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutia. These false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutiae. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

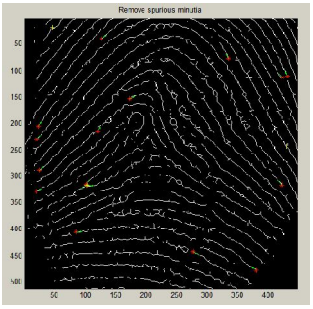
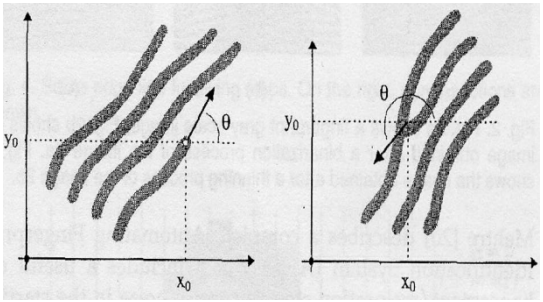


Figure 2.4False Minutia Removals

III. OUR IMPLEMENTATION

We have concentrated our implementation on Minutiae based method. In particular we are interested only in two of the most important minutia features i.e. Ridge Ending and Ridge bifurcation.



(a) (b)

Figure 3.1(a) Ridge Ending, (b)RidgeBifurcation

The outline of our approach can be broadly classified into 2 stages - Minutiae Extraction and Minutiae matching. Figure 3.2 illustrates the flow diagram of the same.

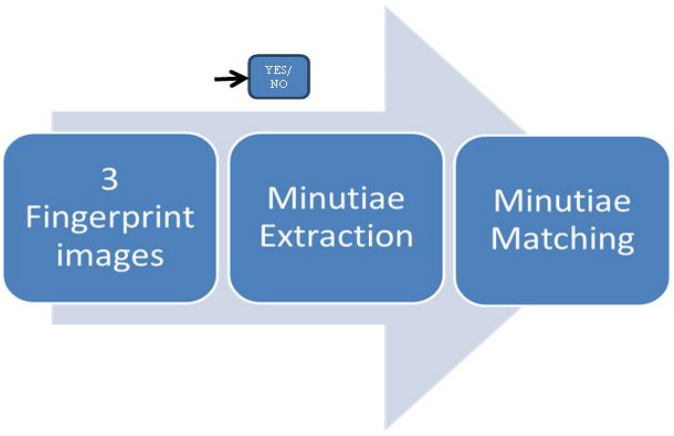


Figure 3.2 System Flow Diagram

Minutia extraction includes Image Enhancement, Image Segmentation and Final Extraction processes while Minutiae matching include Minutiae Alignment and Match processes.

IV. MINUTIAE EXTRACTION

As described earlier the Minutiae extraction process includes image enhancement, image segmentation and final Minutiae extraction.

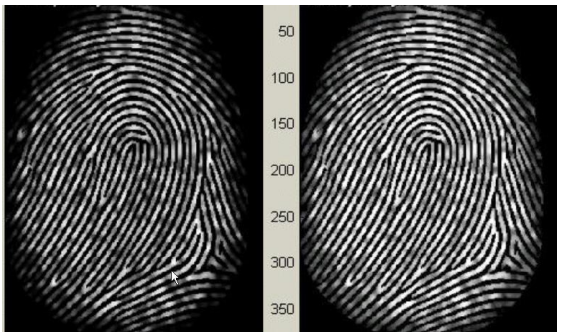


Figure 4.1(a) Original Image, (b) Enhanced Image after histogram equalization

I. Calculate the gradient values along x-direction (g_x) and y-direction (g_y) for each pixel of the block. Two Sobel filters are used to fulfill the task.

II. For each block, use following formula to get the Least Square approximation of the block direction.

$$tan2ß = \frac{2\sum\sum(g_x * g_y)}{\sum\sum(g_x{}^2 - g_y{}^2)}$$

for all the pixels in each block.

The formula is easy to understand by regarding gradient values along x-direction and y-direction as cosine value and sine value. So the tangent value of the block direction is estimated nearly the same as the way illustrated by the following formula.

$$tan2\theta = \frac{2sin\theta cos\theta}{cos^2\theta - sin^2\theta}$$

After finished with the estimation of each block direction, those blocks without significant information on ridges and furrows are discarded based on the following formulas:

$$E = \frac{2\sum\sum(g_x * g_y) + \sum\sum(g_x{}^2 - g_y{}^2)}{W * W * \sum\sum(g_x{}^2 + g_y{}^2)}$$

4.1 Image Binarization

Image Binarization is a process which transforms the 8-bit Gray 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.

A locally adaptive binarization method is performed to binarize the fingerprint image. In this method image is divided into blocks of 16 x 16 pixels. A pixel value is then set to 1 if its value is larger than the mean intensity value of the current block to which the pixel belongs

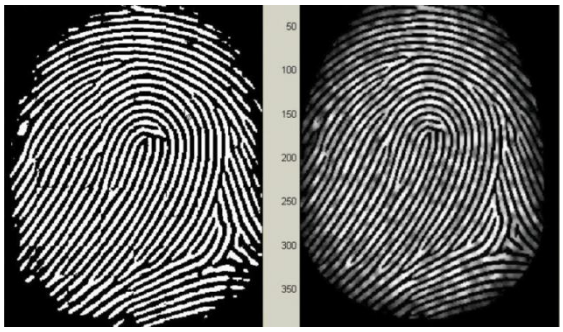


Figure 4.2(a) Binarized Image after, (b) Image before binarization

4.2 Minutiae Representation

Finally after extracting valid minutia points from the fingerprint they need to be stored in some form of representation common for both ridge ending and bifurcation.

So each minutia is completely characterized by the following parameters 1) x-coordinate, 2) y-coordinate, 3) orientation and 4) ridge associated with it (Figure 3.14)

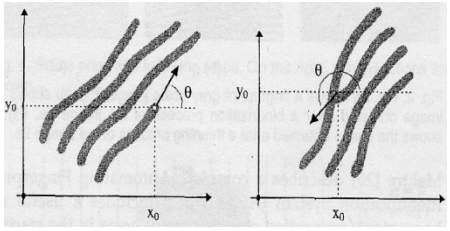


Figure 4.3 Minutia Representation

Actually a bifurcation can be broken down to three terminations each having their own x-y coordinates (pixel adjacent to the bifurcating pixel), orientation and an associated ridge.

The orientation of each termination (tx, ty) is estimated by following method. Track a ridge segment whose

starting point is the termination and length is D. Sum up all x-coordinates of points in the ridge segment. Divide above summation with D to get sx. Then get sy using the same way.

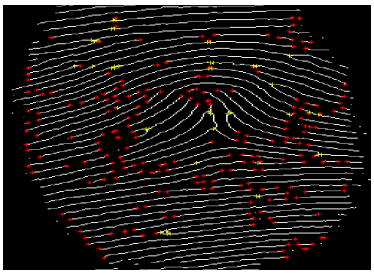


Figure 4.4 Minutiae after marking

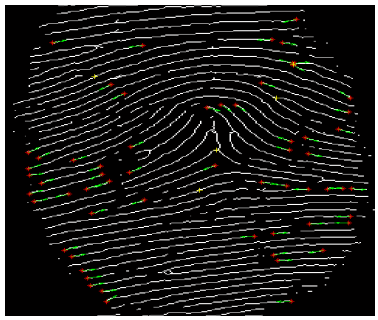


Figure 4.5 Real Minutiae after false removal

V. SIMULATION RESULTS

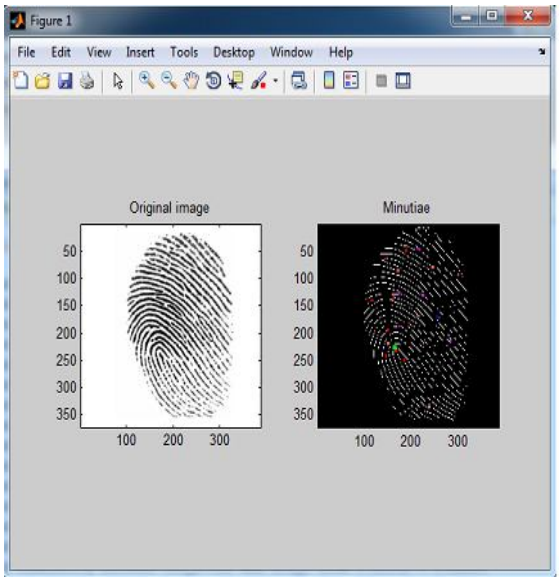


Figure 5.1 First finger output

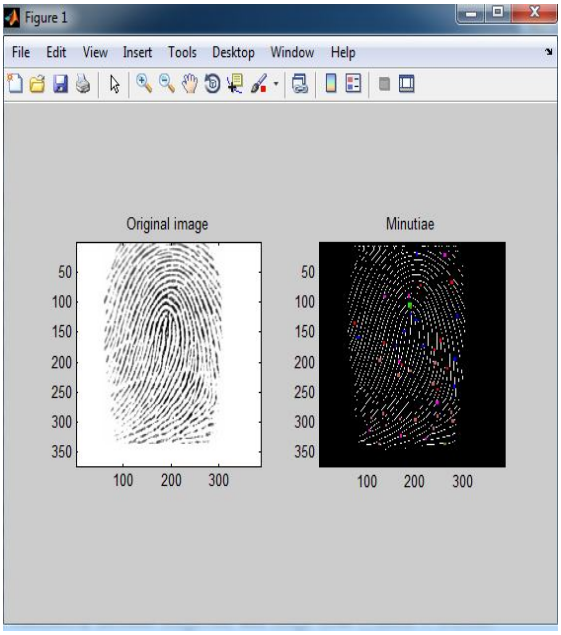


Figure 5.2 second finger output

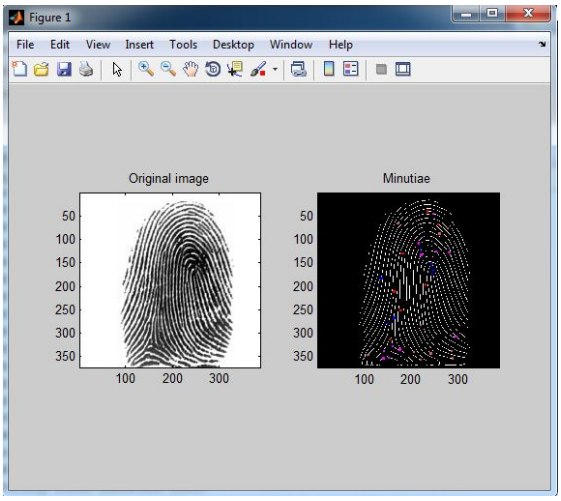


Figure 5.3 Third finger output

As we can see in the graph shown below, when eliminating a step from the whole process or changing some of the parameters, the matching process is affected.

Observations:

1. When altering in such an important step such as the image enhancement part, the performance quality of the system drops rapidly as the noise in the image is increased. Because when working with a biometric identification system, obtaining clear and noise free images is a really hard thing, so this step is usually needed.

2. If we try to remove the H-breaks step, the system wouldn't be greatly affected and the matching process wouldn't become harder, but it's considered a pre-

processing step and it doesn't add much complexity to the system, so no harm in keeping the accuracy higher.

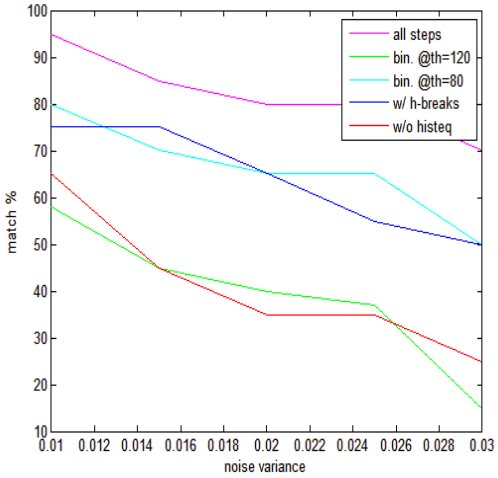


Figure 5.4 match percentage vs. noise variance

VI. CONCLUSION

The above implementation was an effort to understand how Fingerprint Recognition is used as a form of biometric to recognize identities of human beings. It includes heartbeat recognition to check the whether the person is alive or not and followed by all the stages from minutiae extraction from fingerprints to minutiae matching which generates a match score. Various standard techniques are used in the intermediate stages of processing.

The reliability of any automatic fingerprint system strongly relies on the precision obtained in the minutia extraction process. A number of factors damage the correct location of minutia. Among them, poor image quality is the one with most influence.

The proposed alignment-based elastic matching algorithm is capable of finding the correspondences between minutiae without resorting to exhaustive research.

There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware to capture the image or by improving the image enhancement techniques. So that the input image to the thinning stage could be made better, this could improve the future stages and the final outcome.

REFERENCES

[1] A. T. Abdel-Hamid, S. Tahar, and M. Aboulhamid, "A survey on IP watermarking techniques," Design Autom. Embed. Syst., vol. 9, pp. 211–227, 2004.

[2] M. Agrawal, S. Karmakar, D. Saha, and D. Mukhopadhyay, "Scan based side channel attacks on stream ciphers and their counter-measures," in Proc. Int. Conf. Cryptology in India (INDOCRYPT), 2008, pp. 226–238.

[3] Altera, "Anti-tamper capabilities in FPGA designs," [Online]. Available: http://www.altera.com/literature/wp/wp-01066-anti-tamper-capabilities-fpga.pdf/

[4] T. M. Austin, "DIVA: A reliable substrate for deep submicron micro architecture design," in Proc. Annu. Int. Symp. Micro architecture (MICRO), 1999, pp. 196–207.

[5] D. Bernick, B. Bruckert, P. D. Vigna, D. Garcia, R. Jardine, J. Klecka, and J. Smullen, "NonStop advanced architecture," in Proc. Int. Conf. Dependable Systems and Networks (DSN), 2005, pp. 12–21.

[6] E. Biham and A. Shamir, "Differential fault analysis of secret key cryptosystems," inProc. Annu. Int. Cryptography Conf. Advances in Cryptography, 1997, pp. 513–527.

[7] A. Bogdanov, L. R. Knudsen, G. Le, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," Cryptograph.Hardw. Embed. Syst., pp. 450–466, 2007.

[8] D. Boneh, R. A. Demillo, and R. J. Lipton, "On the importance of checking cryptographic protocols for faults," in Proc. Int. Conf. Theory and Application of Cryptographic Techniques (Eurocrypt), 1997, pp.37–51.

[9] Computer science/International Journal of Image Processing (IJIP)/Dec.2010 (CSCjournals.org)

[10] Interpol's public records/History of fingerprints (http://www.interpol.int/Public/Forensic/fingerprints/History/BriefHistoricOutline.pdf)

[11] Course notes from the Swiss Federal Institute of Technology/speech processing and biometric group (http://scgwww.epfl.ch/)