The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 12 || Pages || PP -01-06|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Fingerprint Recognition and Matching using Matlab

Aliyu Tukur
Department of Electrical Engineering, Hassan Usman Katsina Polytechnic, Katsina-Nigeria

ABSTRACT

Fingerprints are considered to be the best and fastest method for biometric identification. They are secure to use, unique for every person and do not change in one's lifetime. Human fingerprints are rich in details called minutiae, which can be used as identification marks for security purposes. This paper is a study and implementation of a fingerprint recognition using image processing tool in Matlab. The approach mainly involves extraction of minutiae points from sample fingerprint images and then performing matching based on the number of minutiae pairing among two fingerprints in question. For each task, some classical and up-to-date methods in literatures are analyzed. Based on the analysis, an integrated solution for fingerprint recognition is developed for demonstration. It finally generates a percentage score which tells whether two fingerprints match or not.

Keywords - *Edge detection; Minutiae; Fingerprint, prewitt,matlab.*

Date of Submission: 02 November 2015 Date of Accepted: 16 December 2015

I. INTRODUCTION

Fingerprint recognition refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Because of their uniqueness and consistency over time, fingerprints have been used for over a century, more recently becoming automated due to advancement in computing capabilities. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection and their established use and collection by law enforcement and immigration.

Digital image processing is a process of manipulating images in a digital computer. This processing can be achieved by development of a computer based algorithm in order to process these images. It is a technology widely used for digital image operations like feature extraction, pattern recognition, segmentation and morphology [1].

II. FINGERPRINT

A fingerprint is the feature pattern of one finger (figure 1.1). It is an imprints formed by the friction ridges of the skin and thumbs. They have long been used for identification because of their immutability and individuality. Immutability refers to the permanent and unchanging character of the pattern on each finger. Individuality refers to the uniqueness of ridge details across individuals; the uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as by features called minutiae, which are some abnormal points on the ridges (figure 1.1). However, shown by intensive research on fingerprint recognition, fingerprints are not distinguished by their ridges, but by the minutiae points.

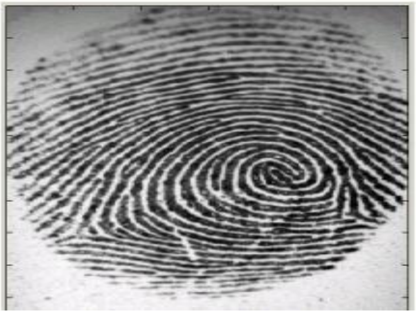

Fig. 1: A fingerprint image acquired by an optical sensor

III. FINGERPRINT RECOGNITION

Fingerprint recognition 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.

Fingerprint verification is to verify the authenticity of one person by his fingerprint. The user provides his fingerprint together with his identity information like his ID number. The fingerprint verification system retrieves the fingerprint template according to the ID number and matches the template with the real-time acquired fingerprint from the user. Usually it is the underlying design principle of AFAS (Automatic Fingerprint Authentication System).

Manual fingerprint verification is so tedious, time consuming and expensive that is incapable of meeting today's increasing performance requirements. An automatic Fingerprint identification system is widely adopted in many applications such as building or area security and ATM machines [1-3]. Also, it potentially prevents unauthorized admittance to access control systems, Time & Attendance Systems, cellular phones, smart cards, desktop PCs, Workstations, vehicles and computer networks. Biometric recognition systems offer greater security and convenience than traditional methods of personal recognition [6].

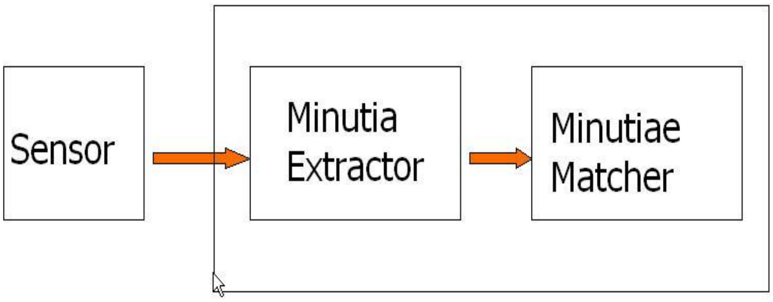

Fig. 2: Simplified fingerprint recognition system

Fingerprint identification is to specify one person's identity by his fingerprint(s) without knowledge of the person's identity, the fingerprint identification system tries to match his fingerprint(s) with those in the whole fingerprint database. It is especially useful for criminal investigation cases. And it is the design principle of AFIS (Automatic Fingerprint Identification System).

A number of methods are used to acquire fingerprints. Among them, the inked impression method remains the most popular one. Inkless fingerprint scanners are also present eliminating the intermediate digitization process. They have high efficiency and acceptable accuracy except for some cases that the user's finger is too dirty or dry.

Fingerprint quality is very important since it affects directly the minutiae extraction algorithm. Two types of degradation usually affect fingerprint images: 1) the ridge lines are not strictly continuous since they sometimes include small breaks (gaps); 2) parallel ridge lines are not always well separated due to the presence of cluttering noise. The resolution of the scanned fingerprints must be 500 dpi while the size is 300 x 300.

IV. MINUTIAE EXTRACTION TECHNIQUES

Extraction of appropriate features is one of the most important tasks for a recognition system. Typical fingerprint recognition method employ feature-based matching, where minutiae mostly ridge ending and ridge bifurcation are extracted from the registered fingerprint image and the input fingerprint image, and the number of corresponding minutiae pairs between the two images is used to recognize a valid fingerprint image.

Segmentation is a fundamental tool in image processing, particularly in the area of feature extraction which aims at identifying points in a fingerprint image at which the image brightness changes sharply or, more formally, has discontinuities. Thereafter the minutiae points are extracted in the final extraction step by ridge thinning, minutiae marking and removal of false minutiae processes.

V. FINGERPRINT MATCHING TECHNIQUES

Two representation forms for fingerprints separate the two approaches for fingerprint recognition. The first approach, which uses image-based methods [3] [4], tries to do matching based on the global features of a whole fingerprint image. It is an advanced and newly emerging method for fingerprint recognition. And it is useful to solve some intractable problems of the first approach.

The second approach, which is minutiae-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. Given two set of minutiae of two fingerprint images, the minutiae match algorithm determines whether the two minutiae sets are from the same finger or not.

No match is ever perfect in either verification or identification system, because every time a biometric is captured, the template is likely to be unique. Therefore, biometric systems can be configured to make a match or no match decision, based on a predefined number, referred to as a threshold, which establishes the acceptance degree of similarity between the trial template and the enrolled reference template. After the comparison, a score representing the degree of similarity is generated, and this score is compared to the threshold to make a match or no match decision.

VI. ALGORITHM IMPLEMENTATION

Implementation of the fingerprint verification system is broken down into four distinct stages as follows:

1. Image acquisition.
2. Edge detection.
3. Comparison of images.
4. Decision making.

A.Image Acquisition

The fingerprint images are captured using the inkless fingerprint sensor (scanner). The quality of the fingerprint images is very important since it affects directly the minutiae extraction algorithm. The resolution of the scanned images is within the acceptable values (500dpi), while the size is about 300×300 and is in JPG format.

B.Edge Detection

An edge is the boundary between two regions with relatively distinct gray level properties. The idea underlying most edge-detection techniques is on the computation of a local derivative operator such as ‘Roberts’, ‘Prewitt’ or ‘Sobel’ operators. In practice, the set of pixels obtained from the edge detection algorithm seldom characterizes a boundary completely because of noise, breaks in the boundary and other effects that introduce spurious intensity discontinuities [7]. Thus, edge detection algorithms typically are followed by linking and other boundary detection procedures designed to assemble edge pixels into meaningful boundaries.

Basic edge detection, which is said to be the detection of changes in intensities for the purpose of finding edges, can be achieved using First-order or Second-order derivatives. Edges are calculated by using the difference between corresponding pixel intensities of the image.

- First-order derivative- The First-order derivative is the gradient of a 2-D function. The gradient of a 2-D function (x, y), is defined as the vector [1]

$$\nabla f = \frac{g_x}{g_y} = \frac{\partial f}{\partial x,}\frac{\partial f}{\partial y} \qquad (1)$$

The gradient of this vector is

$$\nabla f = mag(\nabla f) = [g_x^2 + g_y^2] \qquad (2)$$

The angle at which this maximum rate of change occurs is [1]

$$\alpha(x, y) = \tan^{-1}\frac{g_x}{g_y} \qquad (3)$$

- Second-order derivative: The second-order derivative is normally used to computed the image using the laplacian of a 2-D function f (x,y).

$$\nabla^2 = f(x, y) = \frac{\partial f}{\partial x} + \frac{\partial f}{\partial y} \qquad (4)$$

Prewitt operator provides us two marks; one for detecting edges in horizontal direction and another for detecting edges in vertical direction. All the masks that are used for edge detection are also known as derivative masks.

$$Vertical \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}. \qquad Horizontal \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix}$$

C. Comparison of Images

Comparison of images is based on algorithm of matching black and white points that are present in the fingerprint image and hence compared using Matlab basic scripting to compare the black and white dots.

Fingerprint verification is the process of matching two fingerprints against each other to verify whether they belong to same person or not. When a fingerprint matches with the fingerprint of same individual, we call it true accept or if it doesn't, we call it false reject. In the same way if the fingerprint of different individuals match, we call it a false accept or if it rejects them, it is true reject. False Accept Rate (FAR) and False Reject Rate (FRR) are the error rates which are used to express matching trustability [3].

FAR is defined by the formula:

$$FAR = \frac{FA}{N} \times 100 \qquad (5)$$

FA = Number of False Accepts, N = Total number of verifications

FRR is defined by the formula :

$$FRR = \frac{FR}{N} \times 100 \qquad (6)$$

FR = Number of False Rejects.

Alignment process:

The ridge associated with each minutia is represented as a series of x-coordinates (x_1, $x_2 \ldots x_n$) of the points on the ridge. A point is sampled per ridge length L starting from the minutia point, where the L is the average inter-ridge length. And n is set to 10 unless the total ridge length is less than 10*L [3].

So the similarity of correlating the two ridges is derived from:

$S = \sum^{m}_{i=0} x_i X_i / [\ \sum^{m}_{i=0} x_i^2 X_i^2\ ]$^0.5,

where $(x_{i\sim}x_n)$ and $(X_{i\sim}X_N)$ are the set of minutia for each fingerprint image respectively. And m is minimal one of the n and N value. If the similarity score is larger than 0.8, then go to step 2, otherwise continue to match the next pair of ridges.

. For each fingerprint, translate and rotate all other minutia with respect to the reference minutia according to the following formula:

$$\begin{pmatrix} xi\_new \\ yi\_new \\ \theta\, i\_new \end{pmatrix} = TM * \begin{bmatrix} (xi - x) \\ (yi - y) \\ (\theta i - \theta) \end{bmatrix}, \qquad (7)$$

where (x, y, θ) is the parameters of the reference minutia, and TM is

$$TM = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

D. Decision Making

Decision making is done on the basis of the percentage of image matched, i.e. if more than 90% matched; images are matched. If less than 90% matched; images are different. Depending on the setting of the threshold in identification systems, sometimes several reference templates can be considered matches to the trial template, with the better scores corresponding to better matches. The final match ratio for two fingerprints is the number of total matched pairs divided by the number of minutiae 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 (typically 90%), the two fingerprints are from the same finger.

VII. EXPERIMENTAL RESULTS

The pictorial representations of the simulation results for the two fingerprints matching cases are shown in figures 1.3 to 1.6. Figure 1.3 shows the two sample fingerprints of the same image after applying edge detection algorithm. It can be clearly seen from the plots that both the vertical and horizontal edges of the ridges are more visible than the sample images shown in figure 1.5.

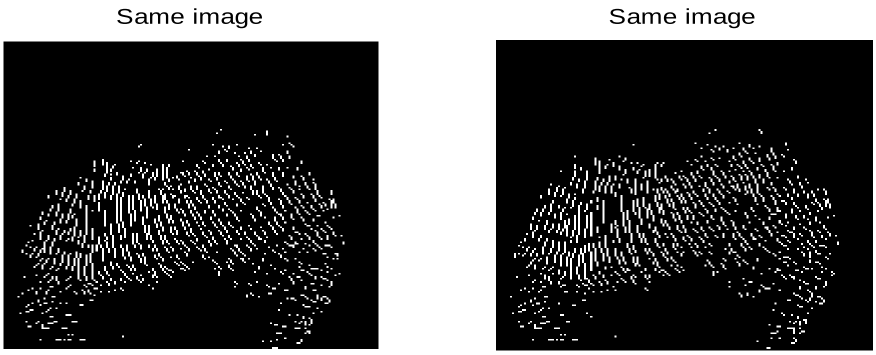

Fig. 3: Same Fingerprint images after applying edge detection

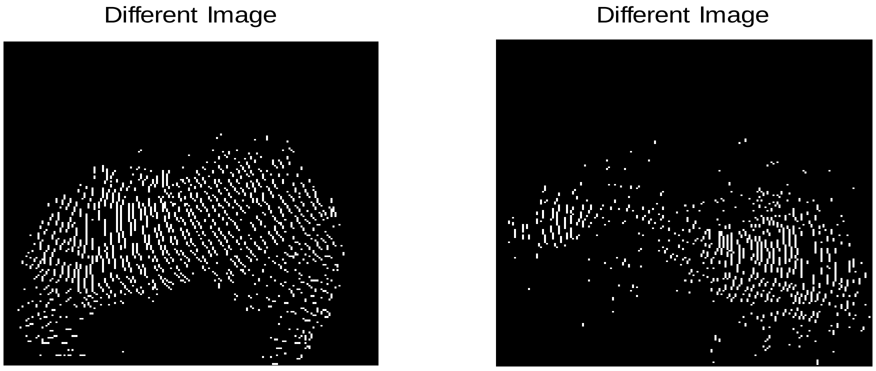

Fig. 4: Different Fingerprint images after applying edge detection

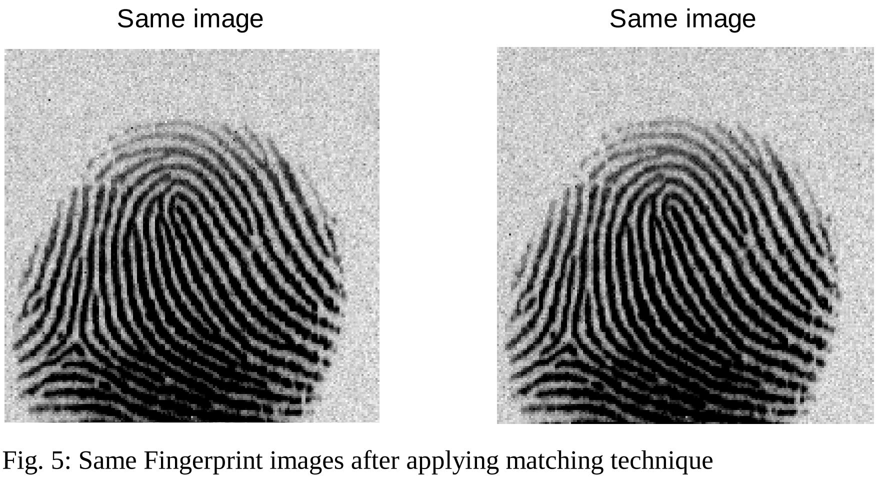

Fig. 5: Same Fingerprint images after applying matching technique

It can be seen from the combined plots in figure 1.5 that the two fingerprints are identical. The outcome of the result also indicates a total matched percentage of 100; hence the images have been matched. With different Fingerprints a total matched percentage of 7.5049 was indicated (less than 90%); hence the images have not been matched.

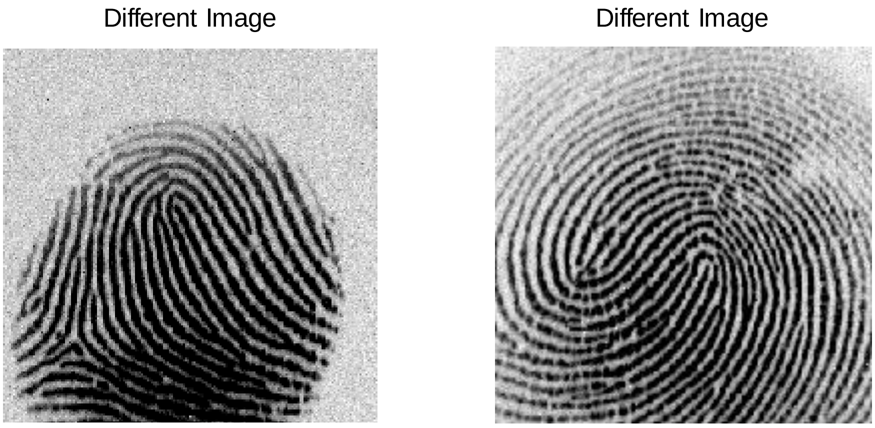

Fig. 6: Different Fingerprints after applying matching technique

VIII. CONCLUSION

The above implementation was an effort to study and understand how a Fingerprint verification system is used as a form of biometrics to recognize identities of human beings. It includes all the stages mentioned in the foregoing study. The outcome of the experiment shows that the proposed technique can be adopted on large databases such as that of a country like Nigeria.

The reliability of any automatic fingerprint verification 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 minutiae matching algorithm is capable of finding the correspondences between minutiae without resorting to exhaustive research. However, 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.

REFERENCES

[1] Amand, E., Anju, G., Simulink model Based Image Segmentation”, Intellectual Journal of Advanced Research In Computer Science and Software Engineering, Vol. 2, issue 6. (2012).

[2] Jain, A., Hong, L. and Boler, R., Online Fingerprint Verification, IEEE trans, PAMI-19, (4), pp. 302-314, (1997).

[3] Leung, W.F., Leung, S.H., Lau, W.H. and Luk, A, Fingerprint Recognition Using Neural Network, *proc. of the IEEE workshop Neural Network for Signal Processing*,(2000). pp. 226-235.

[4] Lee, C.J., and Wang, S.D. Fingerprint feature extraction using Gabor filter, Electroni. Lett. 35, (4), (1999), pp.288-290.

[5] Raymond, T. Fingerprint Image Enhancement and Minutiae Extraction,,Technical report, The University of Western Australi, (1991).

[6] Tico, M., Kuosmanen, P. and Saarinen, J. Wavelet domain features for fingerprint recognition, Electroni. Lett., 2001, 37, (1), (2001), pp.21-22.

[7] Yang S. and Verbauwhede I. A Secure Fingerprint Matching Technique, Wanda Lee, Hong kong, (2003).