International Journal of Innovation and Scientific Research
ISSN 2351-8014 Vol. 10 No. 2 Oct. 2014, pp. 458-465
© 2014 Innovative Space of Scientific Research Journals
http://www.ijisr.issr-journals.org/

Touchless Fingerprint recognition using MATLAB

Anju Mohan[1] and Prof. Shilpa P. Kodgire[2]

[1]Electronics & Communication Department,
M.I.T College, Aurangabad, BAMU,
Maharashtra, India

[2]Associate professor, Electronics & Communication Department,
M.I.T College, Aurangabad, BAMU,
Maharashtra, India

Copyright © 2014 ISSR Journals. This is an open access article distributed under the ***Creative Commons Attribution License***, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ABSTRACT: Fingerprint recognition is the reliable and oldest biometrics used for personal identification. Many sensors were developed for fingerprint recognition systems in which the user's finger print is placed on a sensor. Due to this contact the input fingerprint from the same finger can be different and there can be fingerprint issues which can lead to forgery and hygienic problem. For this reason touchless fingerprint recognition has been developed in which the fingerprint is acquired using a high resolution webcam. The acquired images are subjected to pre-processing steps and the region of interest is extracted. Minutia features are extracted from the fingerprint image and matching is based on the number of minutia pairings among two fingerprints to be matched. The project is coded in Matlab.

KEYWORDS: Biometric, Fingerprint, Minutia, Crossing Number, FAR, FRR.

1 INTRODUCTION

Human beings possess psychological and behavioural characteristics. The measure of these characteristics is called Biometrics. Biometrics is used for personal identification and verification. Voice, lip movements, hand geometry, face, odour, gait, iris, retina, fingerprint are the most commonly used authentication methods. Biometrics is actively growing area of research. The driving force of the progress in this field is, above all, the growing role of the Internet and electronic transfers in modern society. The biometrics has a significant advantage over traditional authentication techniques namely passwords, PIN numbers, smartcards etc. due to the fact that biometric characteristics of the individual are not easily transferable, are unique of every person, and cannot be lost, stolen or broken. The choice of Biometrics depends on accuracy, user acceptance, cost and implementation time and level of security required.

Of all the biometric based recognition systems, fingerprint based recognition systems is one of the oldest and most reliable biometric used for personal identification. A fingerprint is the pattern of friction ridges on a human finger, which provides increased friction for gripping. A fingerprint consists of ridges and valleys. Fingerprints are not distinguished by ridges and furrows but by minutia which are abnormal points on the ridges. Among the variety type of minutia, two are mostly significant and in heavy usage: one is called termination, which is the immediate ending of a ridge; the other is called bifurcation, which is the point on the ridge from which two branches derive. The characteristics of fingerprint are:

i. A fingerprint is an individual characteristic: No two persons, even identical twins does not have similar fingerprint pattern. The probability of two fingers being same is 1 in 1.9×10^{15} [1, 2, and 3].
ii. Fingerprints remains unchanged during a lifetime. Only a very deep cut would result in changes in a fingerprint.
iii. Fingerprint has general ridge patterns that permit them to be classified.

Current fingerprint verification techniques can be broadly classified as Minutiae-based, ridge feature-based, correlation-based and gradient-based. Fingerprint images that are acquired using web camera consist of certain constraints such as low contrast between the ridges and the valleys, defocus and motion blurriness. The paper is organized as follows. In next section we discuss the system development followed by performance analysis and results.

2 SYSTEM DEVELOPMENT

A Touchless fingerprint verification system comprising of hardware and software elements is proposed. An Xpro 20 Mpixel webcam was used to capture fingerprint. This is the main input device for data acquisition. The software architecture of the system involves the use of MATLAB version 11.0. MATLAB was used to perform the pre-processing, feature extraction and verification processes.

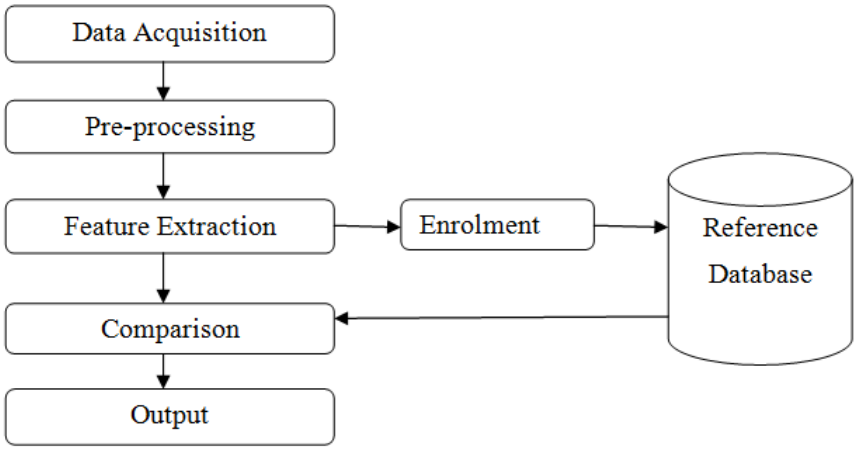

Figure1. Block Diagram of system

2.1 IMAGE ACQUISITION

The fingerprints are acquired using webcam. Then the raw data are sent to a microcomputer through an USB port. An XPRO night vision 20Mp webcam with crystal clear motion and special effects is used as data acquisition device. Data acquisition process is a process where the real time inputs of fingerprint from the webcam are read into the CPU for processing and to store the fingerprint in the database which is called fingerprint database.

2.2 FINGERPRINT PRE-PROCESSING

The images acquired for touchless fingerprint recognition may have problems like low contrast between ridges and valleys, noise, etc. These problems can be removed with the help of pre-processing. The purpose of fingerprint pre-processing step is to make fingerprint images standard and ready for feature extraction. Preprocessing is a necessary step to improve the accuracy of Feature extraction and Verification.

Figure2: Original Fingerprint Image

Pre-processing algorithm used in this work includes steps like image enhancement, binarization and segmentation.

2.2.1 IMAGE ENHANCEMENT

Image enhancement is done to improve the image quality for further operations. It increases the contrast between ridges and valleys. In our work, we have done the enhancement by histogram equalization and FFT. Histogram equalization improves the global contrast of image by adjusting the intensity distribution on a histogram.

Figure3: Enhanced mage after histogram equalization

Enhancement of image after FFT can connect falsely broken points on ridges and remove spurious connections between ridges. In FFT the image is divided into small processing blocks of 32x32 pixels and then perform the fourier transform according to the equation.

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

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

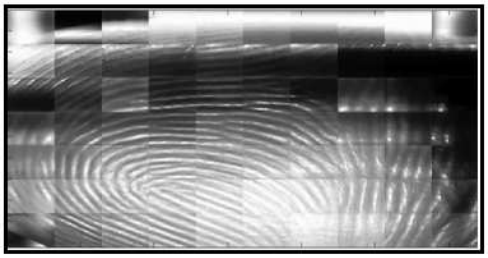

Figure 4: Enhanced image after FFT

2.2.2 IMAGE BINARIZATION

Fingerprint image binarization is to transform the 8-bit gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for valleys. A locally adaptive binarization method is performed to binarize the fingerprint image.

Figure5: Binarized image

2.2.3 IMAGE SEGMENTATION

The region of interest is useful for fingerprint image. The area without effective ridges and valleys is discarded as it is background information. For extracting region of interest, two steps are used. The first one is block direction estimation and the second is based on morphological methods in which morphological operations called OPEN and CLOSE are adopted. Open operation can expand images and remove peaks because of background noise. Close operation can shrink images and eliminate small cavities.

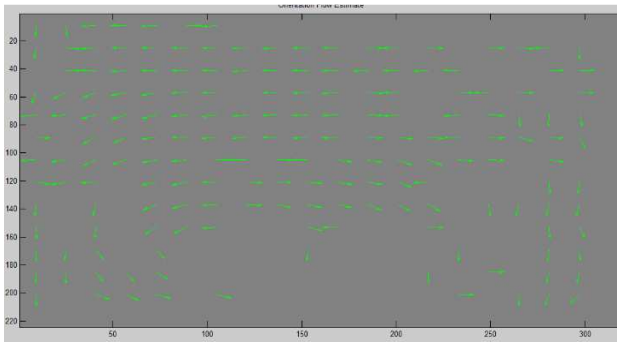

Figure6: Block Direction Estimation

Figure7: Region of interest+Bound

2.3 FEATURE EXTRACTION

Minutia features are extracted from the fingerprint image in our work. For minutia extractions, following process are done.

i. Ridge Thinning: Ridge Thinning is to eliminate the redundant pixels of ridges till the ridges are just one pixel wide [4,5]

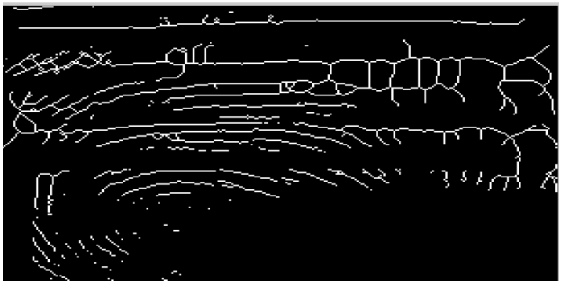

Figure8: Ridge Thinned image

ii. Minutia Marking: Minutia Features are extracted by the concept of Crossing Number(CN). Rutovitz's definition of crossing number for a pixel P is given by equation (2)

$$C_n(P) = \left(\frac{1}{2}\right)\sum_{i=1}^{8}|P_i - P_{i\neq 1}| \quad (2)$$

where Pi is the binary pixel value in the neighborhood of P with Pi = (0 or 1) and P1 = P9.

If $C_n(P) = = 1$ it's a ridge end and if $C_n(P) = = 3$ it's a ridge bifurcation point. There is no need to consider $C_n(P) > 3$ because it's a crossing point.

2.4 MINUTIA MATCHING

Minutia Matching Algorithm determines whether the two minutia sets are from the same fingerprint image or not. Alignment based match algorithm derived from [6] is used for matching of fingerprints. It includes two consecutive stages: one is alignment stage and second is match stage.

i. Alignment stage: If two fingerprints are to be matched choose any one minutia from each image; calculate the similarity of the two ridges associated with the two referenced minutia points. If the similarity is larger than a threshold, then transform each set of minutia to a new coordination system whose origin is at the referenced point and whose x-axis is coincident with the direction of the referenced point.

ii. Match stage: After the set of transformed minutia points is derived, the elastic match algorithm is used to count the matched minutia pairs by assuming two minutia having nearly the same position and direction are identical.

3 PERFORMANCE ANALYSIS AND RESULTS

For performance analysis, we considered fingerprint database consisting of 77 images. The performance of a fingerprint verification system is measured in certain standard terms. These are False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). FAR is the ratio of number of unauthorized user's attempts accepted by the biometric system to the total number of verification attempts made. FRR is the ratio of number of authorized user's attempts rejected by the biometric system to the total number of verification attempts made. EER is a point where FAR and FRR are same. MATLAB version used is MATLAB 7.10.0.499 (R2011a).

False Acceptance Rate: When a fingerprint of an individual matches with the different fingerprint individual than it is called as false acceptance rate.

False Rejecton Rate: When a fingerprint is not completely matches with the different fingerprint individual than it is called as false rejection rate.

Threshold - It is a value at which true or false will be considered. If value of matching equals to or greater than threshold then accepted otherwise rejected. I have set threshold as 600 for fingerprint matching.

Table 1: False Acceptance Rate Vs Threshold variance

Sr. No.	Threshold variance	Number of forged signatures Accepted (out of 100)	FAR (%)
1	100	3	3
2	200	5	5
3	300	6	6
4	400	8	8
5	500	12	12
6	600	15	15
7	700	18	18
8	800	20	20
9	900	27	27
10	1000	35	35

Following graph gives false acceptance rate against threshold variance for proposed fingerprint recognition systems.

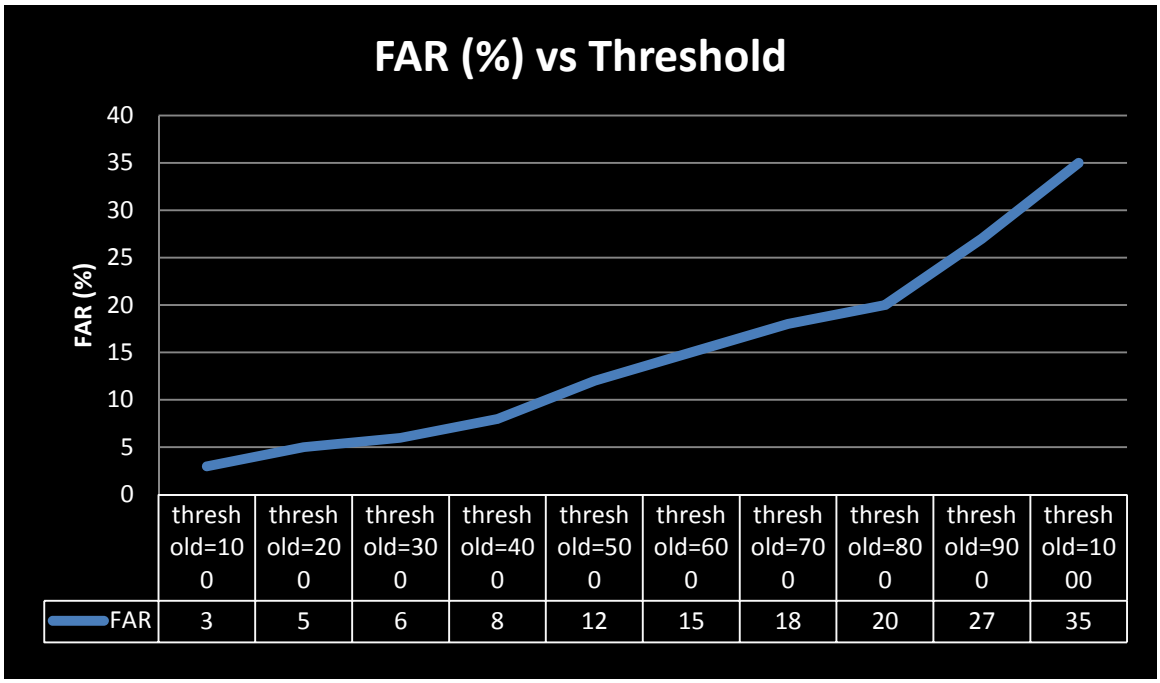

Figure 9: False acceptance rate Vs Threshold variance

Following table gives false rejection rate against threshold variance for proposed fingerprint recognition system.

Table 2: False Rejection Rate Vs Threshold variance

Sr. No.	Threshold Variance	Number of genuine signatures Rejected(out of 100)	FRR (%)
1	100	40	40
2	200	35	35
3	300	32	32
4	400	30	30
5	500	25	25
6	600	20	20
7	700	18	18
8	800	12	12
9	900	10	10
10	1000	5	5

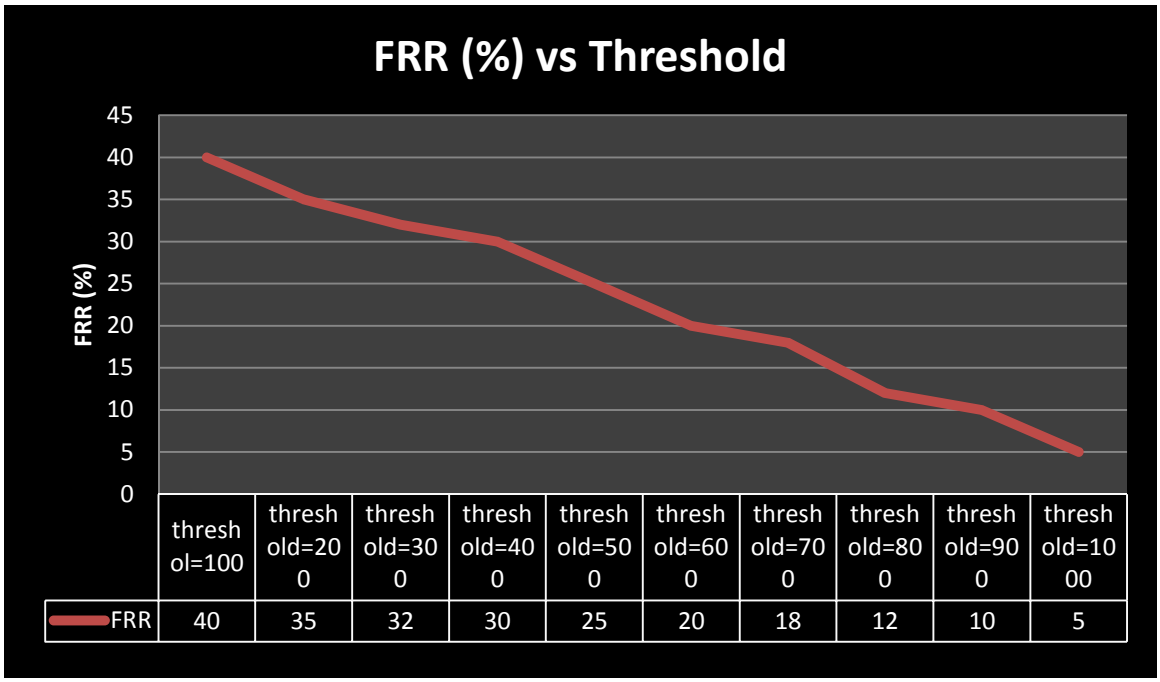

Figure 10 : False rejection rate Vs Threshold variance

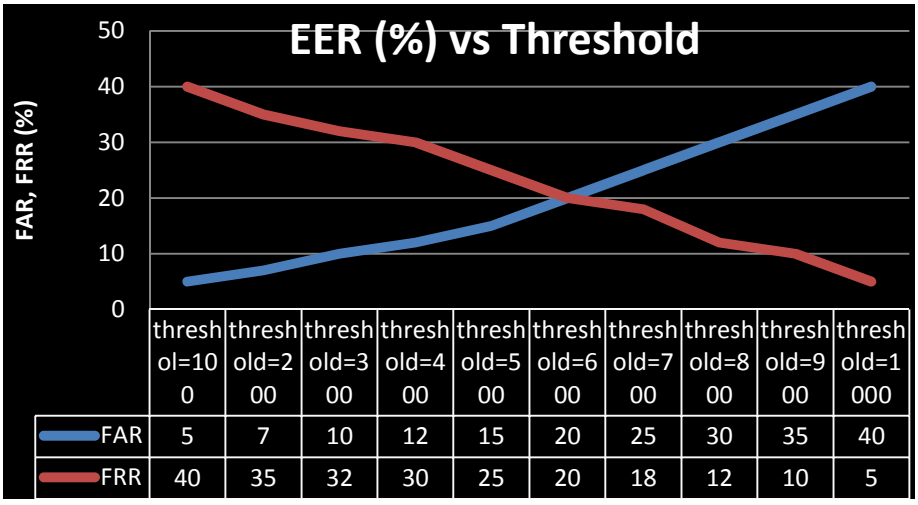

Figure 11: Equal Error Rate Vs Threshold variance

Generally fingerprint verification system shall have an acceptable trade-off between a low FAR and a low FRR. EER is a point at which false acceptance rate and false rejection rate is same. Following graph shows that equal error rate occurs at threshold variance = 600 at which FAR is 20% and FRR 20%.

4 CONCLUSIONS AND FUTURE WORK

Of all biometric technologies, whether biological or non-biological, proposed fingerprint verification offers most potential in terms of adaptability and implementation. This holds true from a number of perspectives i.e. ease of use, low implementation cost and the ease of embedding the system in an organization, without excessively affecting existing operations. . Our project can be used in any Employee Management Attendance System.There is a scope of further improvement in terms of efficiency and accuracy which can be achieved by improving the hardware (biometric) to capture the image.

REFERENCES

[1] Krithika Venkataramani, Vaibhav Kumar Singh. Fingerprint Identification: A brief literary review
[2] B.Y. Hiew, Andrew B.J. Teoh, Member, IEEE and Y.H.Pang, "Digital Camera based Fingerprint Recognition" IEEE International Conference on Telecommunications and MalaysiaInternational Conference on Communications, 2007, Penang, Malaysia
[3] S. Mil'shtein, M. Baier, C. Granz and P.Bustos, Mobile System for Fingerprinting and Mapping of Blood -Vessels across a Finger, IEEE Intern. Conf. on Technologies forHomeland Security, ISBN 978-1-4244-4179-2, page.No.30-34, 2009
[4] E. Hastings, "A Survey of Thinning Methodologies", Pattern analysis and Machine Intelligence, IEEE Transactions, vol. 4, Issue 9, pp. 869- 885, 1992.
[5] L. Lam, S. W. Lee, and C. Y. Suen, "Thinning Methodologies-A Comprehensive Survey", IEEE Transactions on Pattern analysis and machine intelligence, vol. 14, no. 9, 1992..
[6] L. Hong, "Automatic Personal Identification Using Fingerprints", Ph.D.Thesis, 1998.