Fingerprint Matcher System

Ms. Archana S. Shinde, Prof. Santwana Gudadhe, Prof. Varsha Bendre

Abstract— Nowadays need of increased security in various domains of real life activities demands Automatic Authentication System with fast execution time and accuracy. There are different biometric technologies. But among all biometric technologies, Automatic Fingerprint Matcher System is widely used for person verification and identification. In the Fingerprint Matcher system, different matching methods and algorithms are available. Matching methods and algorithms based on minutiae are more robust and reliable. From last many decades, the research is going on to improve the Automatic Fingerprint Authentication System based on software solutions because it is not required to remember any pin or password using such automatic authentication system. This paper has proposed an Automatic Fingerprint Matcher System based on minutiae extraction and minutiae matching. Moreover, in this paper the techniques used for feature extraction and matching are also described. The experimental results shown in this paper describes the working of the system using FVC2000 database.

Index Terms— Authentication, Biometrics, Identification, Minutiae, Minutiae extraction, Minutiae matching, Verification.

1 Introduction

SECURITY is most important challenge in most of the usual applications like Forensics, Government and Commercial domains. In past forensic application have used forensic experts, government applications have used token system and commercial applications have used knowledge based (passwords) systems [1]. However the security was not robust due to the way of authentication to user. Automatic Identification system based on biometric features overcomes the drawback of manual authentication like loss and robbery of tokens or passwords [2], [3].

The word biometrics is derived from the Greek words bios means life and metron means measurement; so biometric identifiers are measurements from human body [1]. Biometric recognition uses different physiological (e.g. hand geometry, fingerprint, face, iris...) and behavioural (e.g. handwriting, gait, voiceprint…) human characteristics [4]. Biometrics is most important for personal authentication because they cannot be stolen or misplaced and they are the features of true user.

Among all these human characteristics, fingerprint is most widely used technique for personal authentication. Fingerprint biometric authentication system is stronger as compared to other biometric technologies due to its certain advantages like High accuracy, Low cost scanner, Medium universality, High uniqueness, High Permanence and High performance etc [1].

The earlier biometric systems were based upon software solutions includes general purpose programming languages and performed by the general purpose hardware like Microcontroller along with sensor and database memory [5], [6]. But from last few years research is going on reconfigurable architectures like FPGA or DSP with advancement in VLSI (Very Large Scale Integration).

- *Ms. Archana S. Shinde, Pune University, Pune, Maharashtra, India, E-mail : arcahan_bhamare123@yahoo.co.in*
- *Prof. Santwana Gudadhe, Pune University, Pune, Maharashatra, India E-mail: s.santwana20@gmail.com*
- *Prof. Varsha Bendre, Pune University, Pune, Maharashatra, India E-mail:* varshabendre22@gmail.com>

The Fingerprint Authentication System has two stages involved:

1) Enrollment Stage
2) Authentication Stage

During the first stage, user is enrolled into the system along with its other personal information whereas in the second stage, user is authenticated based on its enrolled information. In this authentication system, if user is the imposter, then system denies the access. Hence it provides a security to the resource to be accessed [4].

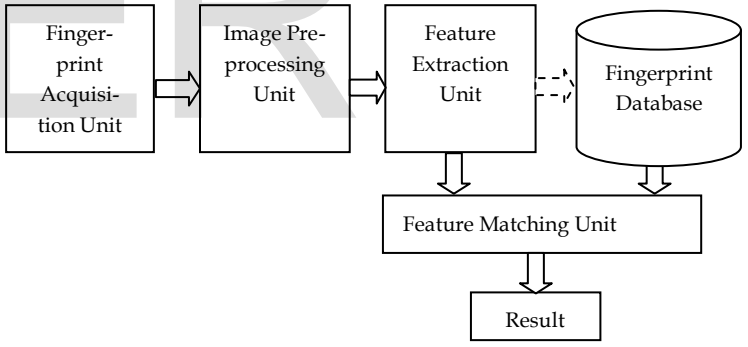


Fig. 1: Basic System Architecture

A basic system architecture of fingerprint recognition system consist of four main modules as shown in Fig. 1 depending upon the main tasks involved in the personal recognition process.

1.1 Fingerprint Image Acquisition Unit:

In the old days the ink and paper was used to perform fingerprint acquisition, nowadays electronic fingerprint sensors and capture methods have been developed in order to automate the acquisition process. As a result of this module, a digital grayscale image of the user's fingerprint is obtained [4].

1.2 Image Pre-processing Unit:

In this module, several pre-processing stages are applied to the original image to remove noisy regions and to adapt the image to the next processing steps. A quality filter can be

applied to the input images to reject low quality fingerprint impressions [4].

1.3 Feature Extraction Unit:

This module has several complex algorithms such as gradient map computation, image segmentation, brightness and contrast enhancement, orientation field calculation, bitmap binarization and ridge thinning can be applied to the image prior to feature extraction of the fingerprint. The ridge discontinuities of the fingerprint called minutiae are the features extracted in this step [4].

1.4 Feature Matching Unit:

The fourth module, matching recognition achieves result by comparison of features with stored features patterns. Various similarity measure criteria's are used for comparison. After comparison the query image is either accepted or rejected [4]. This module gives the confidence to check two fingerprints are from same user or not. Although the accuracy of the recognition system does depend on the reliability of every stage involved, fingerprint matching has special influence on the final system performance.

This paper describes a Fingerprint Matcher System based on minutiae extraction and matching. The main contribution of this paper is that the study of several techniques associated with implementations of fingerprint process. Moreover, this paper describes the approaches used at each level of implementation of fingerprint authentication system.

The paper is organized as follows: In Section 2, literature review of the fingerprint is described. In section 3, proposed system for fingerprint authentication system is covered. The experimental results are discussed in section 4. The conclusion is detailed in section 5. Finally, the challenges and future work is summarized in section 6.

2 Literature Review

A. Alilla, M. Faccio [5] has implemented an approach to fingerprint recognition problem using FPGA. Spatial binary filtering is used for feature extraction and Euclidean distance between features vectors is used for matching two fingerprint images. They have implemented fingerprint recognition on the Xilinx Virtex 4 Evaluation Board [5]. Furthermore, author also suggests the use of Xilinx Spartan family to reduce the hardware cost.

Qingqing Fu, Aiping Wu [6] has implemented a fingerprint identification system in FPGA. In this paper, Nios II processor is designed in FPGA using SOPC Builder. Author has selected Cyclone II series of Altera among all kinds of FPGA boards for Fingerprint Identification System. The fingerprint registration and identification are done with the help of custom commands and logic circuits. Hence, custom instructions improve the speed of fingerprint identification.

G. Danese, M. Giachero, F. Leporati, N. Nazzicari [7] has described architecture in which matching algorithm is based upon Band Limited Phase Only Spatial Correlation (BLPOC). It is developed by Stratix II family Altera FPGA. The enrollment phase is performed using floating point arithmetic during the perform evaluation.

G. Danese, M. Giachero, F. Leporati, G. Matrone, N. Nazzicarimhas [8] has developed FPGA based architecture that efficiently uses the core of a matching algorithm based on POC i.e. phase only spatial correlation. The FPGA used is Altera Stratix II FPGA (EPS2S180 model). The implemented matching algorithm decides whether the two images belong to the same finger or not. A pre-processing is done by Poincare Index based algorithm and then this point will be a reference point to align two images. A set of POC functions are computed with respect to the reference point in this system. C Program is used to test the performance of the system.

Mariano Fons, Francisco Fons, Enrique Canto [4] has discussed a novel system architecture using hardware-software co-design for a fingerprint authentication system. The system is implemented on FPSLIC (Field Programmable System Level Integrated Circuit) from Atmel. This paper describes the hardware software co-design importance for matching two fingerprint minutiae sets. Authors have used minutiae based local and global structures analysis to perform fingerprint alignment and matching.

Thus, in this section few papers are discussed based on their matching algorithms. Its purpose is to give an idea about the implementation Fingerprint Authentication System to the reader.

3 Proposed System

Depending upon the tasks involved in the Fingerprint Authentication System, the proposed system is divided into different units as shown in Fig. 2.

During the enrollment stage, the user's template is stored in the database and during the authentication stage, the query fingerprint image is processed by all the units and at the matching step the query fingerprint image features are compared with the user's template feature. Finally, it shows the result of feature matching. The details of each block are discussed as below:

3.1 Image Pre-processing Unit:

Image pre-processing is very necessary task in Fingerprint Authentication System. This task is consists of Image Enhancement and Image Binarization.

1) **Image Enhancement:** The Image enhancement is done by Histogram Equalization and Fourier Transform (FFT). Histogram Equalization is used to increase perceptional information and improves the visual effects. Furthermore, the image is enhanced using the Fourier Transform. It connects the some falsely broken points on ridge and to remove some spurious connections between ridges.

2) **Image Binarization:** Fingerprint Image Binarization is to transform 8 bit Grey Image to 1 bit Black & White Image. After the operation, the ridges become black and furrows becomes white.

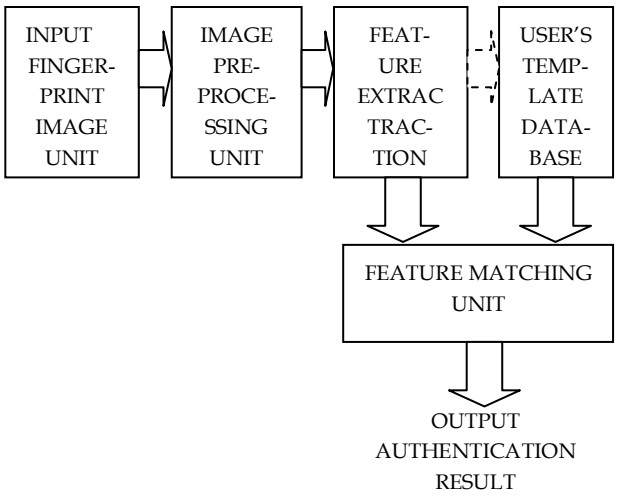


Fig. 2 : Proposed System

3.2 Minutiae Extraction:

1) **Estimation of Orientation Field:** In proposed system, a new implementation of Rao's algorithm is used [9]. Its steps are as below:
   a) Divide the input fingerprint image into blocks of size W x W, where W=16
   b) Compute the gradients G_x and G_y at each pixel in each block.
   c) Estimate the local orientation of each block using the following formula:

$$\theta_o = \frac{1}{2}\tan^{-1}\left(\frac{\sum_{i=1}^{W}\sum_{j=1}^{W} 2G_x(i,j)G_y(i,j)}{\sum_{i=1}^{W}\sum_{j=1}^{W}\left(G_x^2(i,j)-G_y^2(i,j)\right)}\right) \quad (1)$$

where W is the size of the block and Gx and Gy are the Gradients magnitudes in x and y directions, respectively.

   d) In order to improve the poor local orientation field following steps are carried out:

      i) Compute the consistency level of the orientation field in the local neighborhood of a block (i, j) with the following formula :

$$C_o = \frac{1}{N}\sqrt{\sum_{(i',j')\in D}\left|\theta(i',j')-\theta(i,j)\right|^2} \quad (2)$$

$$|\theta'-\theta| = \begin{cases} d & \text{if } \left(d=(\theta'-\theta+360)\bmod 360\right)<180 \\ d-180 & \text{otherwise} \end{cases} \quad (3)$$

ere D represents the local neighborhood around the block (i, j) (in our system, the size of D is 4x4); N is the number of blocks within D; $\theta(i, j)$ and $\theta(i',j')$ are local ridge orientations at blocks and (i, j) respectively [9]

      ii) If the consistency level is above certain threshold Tc, then local orientation around its region are reestimated until it is below a certain level [9].

2) **Ridge Detection:**
The next step in minutiae detection is ridge detection after the orientation field estimation. In Ridge detection a fingerprint image is first convolved with the two masks $h_t(x, y; u, v)$ and $h_b(x, y; u, v)$, of size L x H respectively [9]. These two masks are capable of accentuating the local maximum gray level values along the normal direction of the local ridge direction. If two grey level values at pixel (x, y) of the convolved images are larger than a certain threshold T_{ridge}, then pixel (x, y) is labeled as a ridge. The result of this step is Smooth Ridge Map.

3) **Minutiae Detection:**
At the start, Fingerprint Ridge Map is thinned to find minutiae in fingerprint image. The steps performed in this unit are as below [9]:-
   a) Assume Pixel(x, y) is on a thinned ridge map and N0, N1, N2,…, N7 are its 8 neighbors.
   b) A smoothing procedure is applied to remove H-breaks and spikes to eliminate the noisy region.
   c) Check for Ridge ending using $\left(\sum_{i=0}^{8} Ni\right)$ =1
   d) Check for Ridge Bifurcation using $\left(\sum_{i=0}^{8} Ni\right)$ >2
   e) Removal of false minutiae.
   f) After removal of false minutiae remaining minutiae are treated as true minutiae.
   g) Store true minutiae.

3.3 Minutiae Matching:

Basically Matching approaches are divided into following different categories [1], [10], [11], [12]:

- Correlation based matching
- Minutia based matching
- Ridge feature based matching
- Non-minutia based matching

- Hybrid Methods

Among all these techniques minutiae based matching algorithm is used in our proposed system. The proposed algorithm is referred from [11], [12]. In this system, local and global analysis of minutiae are applied to perform alignment and matching [4]. There are several steps performed for the fingerprint matching.

1) Minutia Description: Local Analysis

In this step a local structures of each minutiae is determined for two different fingerprint images. Each minutia is defined using triplets: Euclidean distance d, Angles ϕ and ridge direction γ. Thus each minutiae denoted by N triplets (d, ϕ, γ) and forms a W minutiae points is then forms W x N triplets (d, ϕ, γ) [4]. These triplets are given by following formulae:

$$d = \sqrt{(x_1 - x_0)^2 + (y_1 - y_0)^2} \quad (4)$$

$$\alpha = tg^{-1}\left(\frac{y_1 - y_0}{x_1 - x_0}\right) \quad (5)$$

$$\phi = \alpha - \beta_0 \quad (6)$$

$$\gamma = \beta_1 - \beta_0 \quad (7)$$

2) Minutia Comparison: Similarity Matrix

Once the minutiae set for user and query image is prepared, the similarity correspondence between two minutiae set is determined to find out the best minutiae pair in the local structures [4].

3) Central Feature Selection

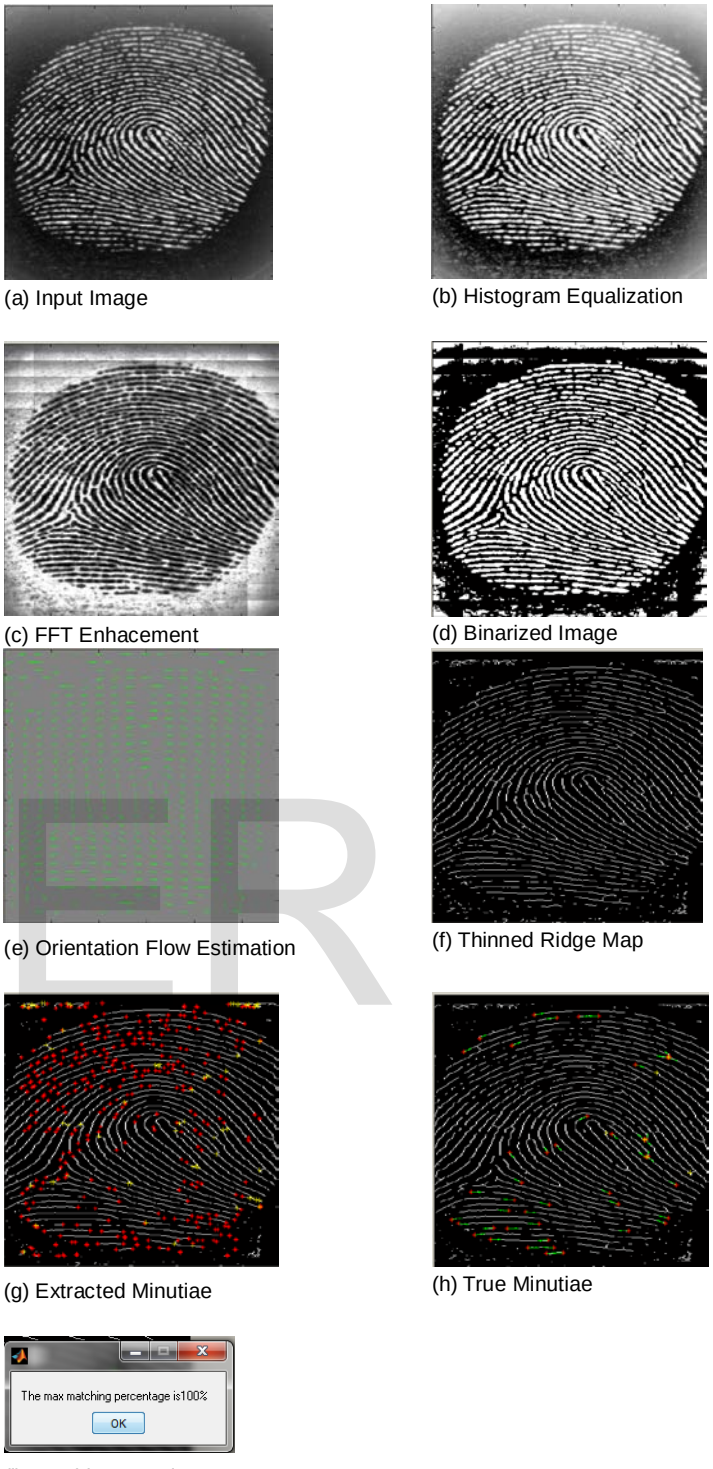
Once the best minutiae pair is determined depending upon the similarity matrix, the best matched minutiae pair will become center point to align two images.

4) Minutiae Description: Global Analysis

With reference to the central feature minutiae are defined for global structure. Now the minutiae set will have W-1 minutiae points and characterized by W-1 x N triplets (d, ϕ, γ) related to the central feature [4].

5) Decision Making: Match Result

The similarity score is determined for global structures of two images. This similarity score is compared with threshold value to decide that the query fingerprint is from the same user or not [4].



(a) Input Image (b) Histogram Equalization (c) FFT Enhacement (d) Binarized Image (e) Orientation Flow Estimation (f) Thinned Ridge Map (g) Extracted Minutiae (h) True Minutiae (i) Matching Result

Fig. 3: Results of Fingerprint Authentication System (a) Input Image, (b) After Histogram Equalization, (c) FFT enhanced image, (d) Binarized Image, (e) Orientation field superimposed on input image, (f) Thinned Ridge Map, (g) Extracted Minutiae, (h) True Minutiae Extraction, (i) Matching Result

4 Experimental Results

In this section, the Fingerprint Matcher System results are discussed and shown in Fig. 3.

The fingerprint authentication system is tested on MATLAB R2013a as platform running on general purpose hardware (Laptop with Intel Core I3 microprocessor, 1.40GHz clock frequency) and Windows 7 O.S. (Operating System).

Euclidean Distance algorithm is used for similarity measurement. The database used is FVC 2000 collected from FVC2000 Fingerprint Verification Competition [13].

A FVC2000 fingerprint database is used to test the experiment performance. Here are the results of fingerprint authentication system using 1:1 mapping approach. The observed results are discussed as follow:

1. The input image shown in Fig. 3(a) is from fingerprint database.
2. The input image enhancement is done by using Histogram equalization and FFT as shown in Fig. 3(b) & (c) respectively.
3. The binarization is performed on the enhanced image as shown in Fig. 3(d).
4. For minutiae detection, Estimation of orientation flow and Thinning is performed as mentioned in Fig. 3(e) & (f) respectively.
5. False minutiae are removed to get true minutiae as shown in Fig. 3(g) & (h) respectively.
6. Finally, True minutiae of two images are matched to get the similarity result as shown in Fig. 3(i).

5 Conclusion

The fingerprint images are matched with the database image with 1:1 mapping in simple way. From the result, it is observed that minutiae matching algorithm shows better result. After applying smoothing & enhancement techniques to input image help to increase the matching result. The proposed system architecture described in this work is implemented and tested in MATLAB R2013a. The feasibility to build a system for fingerprint recognition is demonstrated.

6 Challenges And Future Work

In this paper, the survey of fingerprint techniques encourages the reader for development of new techniques in this area as future work. Although, researchers are working in Fingerprint Recognition, there are some of the challenges with fingerprint systems. With the advancement in reconfigurable architectures, the future scope is to improve Accuracy and Speed of verification of the system using reconfigurable architecture at low cost.

References

[1] Maltoni, D. Maio, A. K. Jain, S. Prabhakar, Handbook of Fingerprint Recognition, Springer, 2003.

[2] A. K. Jain, L. Hong, S. Pankanti, R. Bolle, "An identity authentication system using fingerprints", Proceedings of the IEEE, vol. 85, no. 9, pp. 1365-1388, September 1997.

[3] Lopez, M.; Canto, E., "FPGA implementation of a minutiae extraction fingerprint algorithm," Industrial Electronics, 2008. ISIE 2008. IEEE International Symposium on , vol., no., pp.1920,1925, June 30 2008-July 2 2008

[4] Fons, M.; Fons, F.; Canto, E., "Design of an Embedded Fingerprint Matcher System", Consumer Electronics, 2006. ISCE '06. 2006 IEEE Tenth International Symposium on , vol., no., pp.1,6

[5] Alilla, A.; Faccio, M.; Vali, T.; Marotta, G.; DeSantis, L., "A new low cost fingerprint recognition system on FPGA", Industrial Technology (ICIT), 2013 IEEE International Conference on , vol., no., pp.988,993, 25-28 Feb. 2013

[6] Qingqing Fu; Aiping Wu; Yonghua Li, "Fingerprint Identification System Based on SOPC", Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th International Conference on , vol., no., pp.1,4, 23-25 Sept. 2011

[7] Danese, G.; Giachero, M.; Leporati, F.; Nazzicari, N., "A Multicore Embedded Processor fors Fingerprint Recognition", Digital System Design: Architectures, Methods and Tools (DSD), 2010 13th Euromicro Conference on , vol., no., pp.779,784, 1-3 Sept. 2010

[8] Danese, G.; Giachero, M.; Leporati, F.; Matrone, G.; Nazzicari, N., "An FPGA-Based Embedded System for Fingerprint Matching Using Phase-Only Correlation Algorithm", Digital System Design, Architectures, Methods and Tools, 2009. DSD '09. 12th Euromicro Conference on, vol., no., pp.672, 679, 27-29 Aug.2009

[9] Anil Jain, Lin Hong, and Ruud Bolle, "On-Line Fingerprint Verification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 19, no. 4, April 1997

[10] http://shodhganga.inflibnet.ac.in/bitstream/10603/6681/8/09_chapter2.pdf last referred on 1 Feb. 2014.

[11] Ross, A. K. Jain, and J. Reisman, "A Hybrid Fingerprint Matcher", Pattern Recognition, Vol. 36, No. 7, pp. 1661-1673, 2003

[12] X. Judong, W.-Y. Yau, "Fingerprint minutiae matching based on local and global structures", Proceedings of ICPR 2000, pp. 1038-1041, 2000.

[13] Fingerprint Verification Competition 2000 (FVC2000). Available: http://bias.csr.unibo.it/fvc2000/database.asp