Development of a Multimodal Biometric Identification and Verification System using Two Fingerprints

Neha Jain
M.Tech (CSE) scholar
Mewar University
Gangrar, Chittorgarh

S.K.Sharma,Ph.D
Director and Professor
Computer Engineering
Pacific Institute of Engineering,
Udaipur (Rajasthan)

B.L.Pal
Associate Professor & head
Computer Science Engineering
Mewar University
Gangrar, chittorgarh

ABSTRACT

Fingerprint recognition is one of the research hotspots of biometrics techniques. Fingerprints are the most widely used biometric feature for identification and verification in the field of biometrics. [1]. The traditional fingerprint recognition systems have such disadvantages as high computation complexity, low speed, low recognition rate to uncompleted or defiled fingerprints, and not robust[2]. In this paper, we propose a multimodel fingerprint identification and verification method based on pattern recognition, which emphasizes global features of fingerprint. With lots of artificial fingerprint samples, the results show that the proposed method is effective, fast, robust and shows the Improvement in rate of false acceptance and false rejections. Experimental results are analyzed and a fingerprint recognition system is introduced.

General Terms

Pattern Recognition, Fingerprint classification and verification

Keywords

Fingerprint classification, Fingerprint identification **techniques**, Minutiae extraction, image enhancement

1. INTRODUCTION

Biometrics means “The statistical analysis of biological observations and phenomena”.

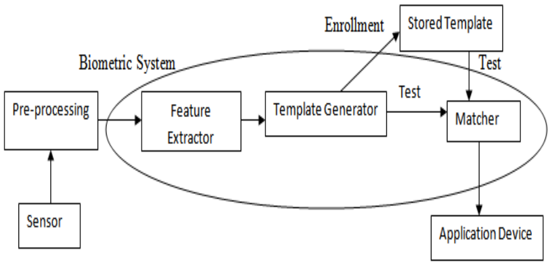


Figure 1.1: General block diagram of a biometric system

Biometric based identification relies on “something that you are”, or “something that you do”, and hence it differentiates between an authorized person and an impostor.[3]

Enrollment and authentication are the two primary processes involved in a biometric security system. During enrollment, biometric measurements are captured from a subject and related information from the raw measurements is gleaned by the feature extractor, and this information is stored on the database[4]. During authentication, biometric information is detected and compared against the database through pattern recognition techniques that involve a feature extractor and a biometric matcher working in cascade[5].

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image[6]. Digital image processing is concerned primarily with extracting useful information from images. Ideally, this is done by computers, with little or no human intervention. Image processing algorithms may be placed at three levels. At the lowest level are those techniques which deal directly with the raw, possibly noisy pixel values, with denoising and edge detection being good examples. In the middle are algorithms which utilize low level results for further means, such as segmentation and edge linking. At the highest level are those methods which attempt to extract semantic meaning from the information provided by the lower levels, for example, handwriting recognition[7].

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprint identification is popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and their established use and collections by law enforcement and immigration. Fingerprint recognition (sometimes referred to as dactyloscopy) or palm print identification is the process of comparing questioned and known friction skin ridge impressions from fingers or palms or even toes to determine if the impressions are from the same finger or palm. The flexibility of friction ridge skin means that no two finger or palm prints are ever exactly alike (never identical in every detail), even two impressions recorded immediately after each other[8]. Fingerprint identification (also referred to as individualization) occurs when an expert(or an expert computer system operating under threshold scoring rules) determines that two friction ridge impressions originated from the same finger or palm (or toe, sole) to the exclusion of all others[9]. The accuracy of a fingerprint matching algorithm is measured by:

FAR : It stands for false acceptance rate. It is defined as the ratio of the number of impostor images considered as authentic by the algorithm to the total number of impostor images.

FRR : It stands for false rejection rate. It is defined as the ratio of the number of authentic images not considered qualified by the algorithm to the total number of authentic images. When FAR and FRR are equal, we call it equal error rate (ERR). The performance of an algorithm is generally measured in terms of **ERR :** The uniqueness of fingerprint is determined by global features like valleys and ridges ,and by local features like ridge endings and ridge bifurcations , which are called minutiae[10,11].

2. LITERATURE REVIEW

Ballan and Ayhan Sakarya's Classification technique finds the directional images by checking the orientations of individual pixels, computes directional histograms using overlapping blocks in the directional image, and classifies the fingerprint into the Wirbel classes (whorl and twin loop) or the Lasso classes (arch, tented arch, right loop, or left loop). However, it takes much time for classification[12]. Hong et al., reported fingerprint enhancement based on the estimated local ridge orientation and frequency clarification of ridge and valley structures of input[13]. Surachai Panich suggested a method of Fingerprint Identification in order to match two fingerprints taken from database using Minutiae Matching [9]. Avinash Pokhriyal et. al. proposed a new way of thinning a fingerprint image is proposed. This method is called MERIT (Minutiae Extraction using Rotation Invariant Thinning), as it thins a fingerprint image irrespective of the fingerprint's position and then extracts minutiae points from a fingerprint image.[14]
Iwasokun G. B., Akinyokun O. C., Alese B. K. & Olabode O. compared each of the features of a template fingerprint image with each of the features in the feature sets in the reference database to determine whether the template and each of the reference images are from the same source. Comparison is done on the basis of preset parameters such as feature type, location, orientation and so on. The results obtained show that with the modified algorithm, valid and true minutiae points were extracted from the images with greater speed and accuracy[15]. Le Hoang Thai 1 and Ha Nhat Tam discusses on the standardized fingerprint model which is used to synthesize the template of fingerprints. In this model, after pre-processing step, we find the transformation between templates, adjust parameters, synthesize fingerprint, and reduce noises.[7]

In this research , we have proposed a method for improvement in rate of false acceptance and false rejections using two fingerprints as multimodality.

3. MULTIMODAL SYSTEM DESIGN

A fingerprint recognition system constitutes of fingerprint acquiring device, minutia extractor and minutiae matcher.

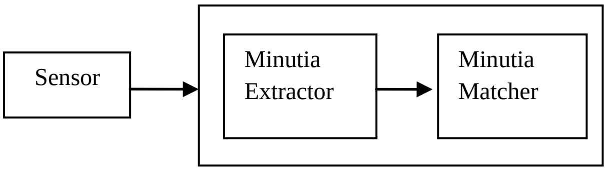


Figure 2 : Simplified Fingerprint Recognition System

For fingerprint acquisition, optical or semi-conduct sensors are widely used. They have high efficiency and acceptable accuracy except for some cases that the user’s finger is too dirty or dry. However, the testing database for my project is done from the available fingerprints provided by FVC2002 (Fingerprint Verification Competition 2002). So no acquisition stage is implemented.
This research work will be carried out to design a fingerprint identification technique which is expected to give better performance in terms of accuracy and acceptance rate etc.
This work is proposed to have a method for fingerprint matching based on minutiae matching. However, unlike conventional minutiae matching algorithms our algorithm also takes into account region and line structures that exist between minutiae pairs. This allows for more structural information of the fingerprint to be accounted for thus resulting in stronger certainty of matching minutiae. Also, since most of the region analysis is preprocessed it does not make the algorithm slower. Evidence from the testing of the preprocessed images gives stronger assurance that using such data could lead to faster and stronger matches[16].
The main objective of this research is improvement in the rate of false acceptance and false rejections which is implemented by a multimodel fingerprint system.

ALGORITHM

Input : Two different gray – scale fingerprint images A1 and A2.

Output: Verified fingerprint image with matching score.

Step 1 : Perform Histogram equalization on each fingerprint separately.

Step 2 : Enhancement of fingerprint images using FFT.

Step 3 : Apply Binarization on fingerprint images.

Step 4 : Perform Ridge detection and take out ROI.

Step 5 : Thinning on images and remove H-Breaks to obtain Minutiae points.

Step 6 : Remove spurious Minutiae to extract true minutiae and save it .

Step 7 : Combine true minutiae of both fingerprints and save it as a template.

This is the enrollment phase. To match the fingerprints, first perform all the above steps and then match them and goto step 8.

Step 8 : if match template>=Match score, then fingerprints are accepted otherwise rejected.

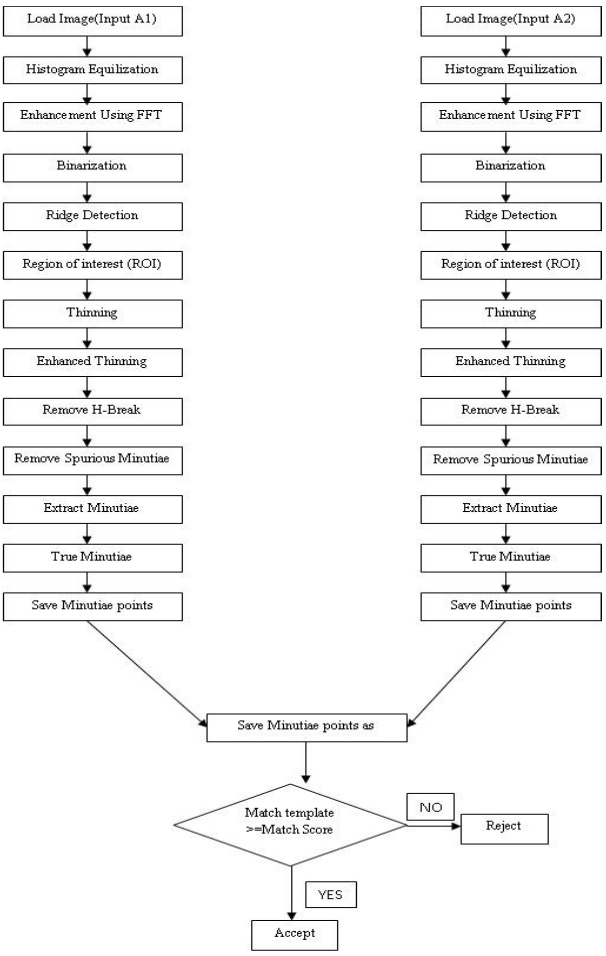


Figure 3 : A flowchart for Identification and Matching Phase

As shown in figure below, for fingerprint identification we will first input the fingerprint then all preprocessing will carried out on that input, then we input second fingerprint of the same person and all preprocessing carried out on that too, and minutia points of both the fingerprint are store into the database. This phase is known enrollment phase. Thus that fingerprint will be taken as authenticated one. Whenever we get another fingerprint as an input we will process it, apply matching algorithm on that input print and check the match score. If it matched then only we will accept the fingerprint.

Briefing of the pre-processing of the design phase

3.1 Fingerprint Image enhancement : It is to make the image clearer for easy further operations.
The enhancement may be useful for the following cases :

- connect broken ridges (generally produced by dry fingerprint or cuts, creases, bruises).

- eliminate noises between the ridges.

- improving the ridge contrast.

Two Methods are adopted in my fingerprint recognition system as :

3.1.1 Histogram Equalization

3.1.2 Fourier Transform.

Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information.

Fourier transform is to divide the image into small processing blocks (32 by 32 pixels) and perform the following operation according to the equation F(u,v)=

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

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

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times where the magnitude of the original FFT = abs (F (u, v)) = |F (u, v) |[17].

3.2 Fingerprint Image Binarization : It is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows[17].

3.3 Fingerprint Image Segmentation : In this, the gray scale image is converted to a binary image through the process of simple thresholding or some form of adaptive binarization[17].

3.4 Region of Interest (ROI) : It is a portion of an image that you want to filter or perform some other operation on. You define an ROI by creating a binary mask, which is a binary image that is the same size as the image you want to process with pixels that define the ROI set to 1 and all other pixels set to 0[17,18].

3.5 Minutia Extraction : It includes the following two processes :

3.5.1 Thinning

3.5.2 Minutia Marking

Thinning is a Technique to eliminate the redundant pixels of ridges till the ridges are just one pixel wide.
Minutia Marking

3.6 Minutiae Post Processing

3.6.1 False Minutiae Removal
3.6.2 Unification of minutia points

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 minutia. So some mechanisms of **removing false minutia** are essential to keep the fingerprint verification system effective[10,11].
Since various data acquisition conditions such as impression pressure can easily change one type of minutia into the other, most researchers adopt the **unification** representation for both termination and bifurcation. So each minutia is completely characterized by the following parameters at last:

1) x-coordinate
2) y-coordinate, and
3) Orientation.

3.7 Generation of mixed minutia templates : The two separate fingerprints undergone some pre-processing and then they are combined and saved as a template.

3.8 Minutia Match : Given two set of minutia of two fingerprint images, the minutias match algorithm determines whether the two minutia sets are from the same finger or not.

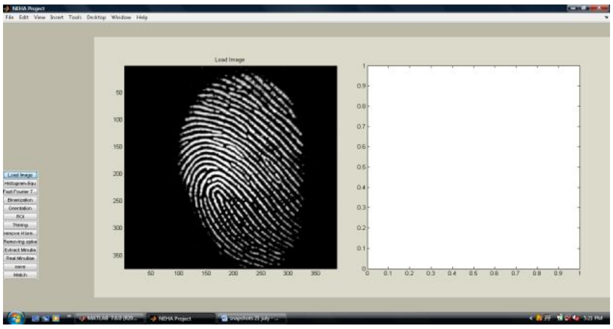
4. CONCLUSION & RESULTS

The reliability of any fingerprint system strongly relies on the precision obtained in the minutia extraction process. A number of factors are detrimental to the correct location of minutia. Among them, poor image quality is the most serious one. In this project, we have combined many methods to build a minutia extractor and a minutia matcher in order to improve the rate of false acceptance and false rejections.

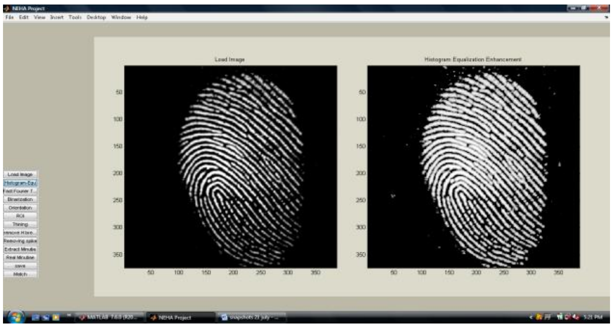
A fingerprint is believed to be unique to each person (and each finger). Fingerprints of even identical twins are different. Fingerprints are one of the most mature biometric technologies and are considered legitimate proofs of evidence in courts of law all over the world. Fingerprints are, therefore, used in forensic divisions worldwide for criminal investigations. More recently, an increasing number of civilian and commercial applications are either using or actively considering using fingerprint-based identification because of a better understanding of fingerprints as well as demonstrated matching performance than any other existing biometric technology.

Experimental Results

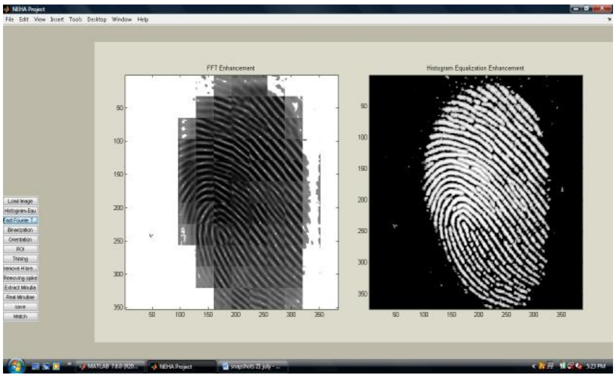
ORIGINAL IMAGE



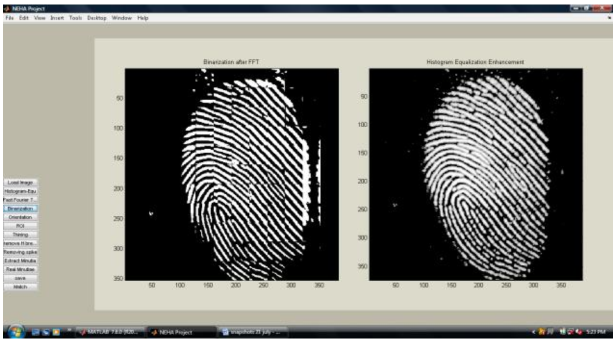
AFTER HISTOGRAM EQUALIZATION



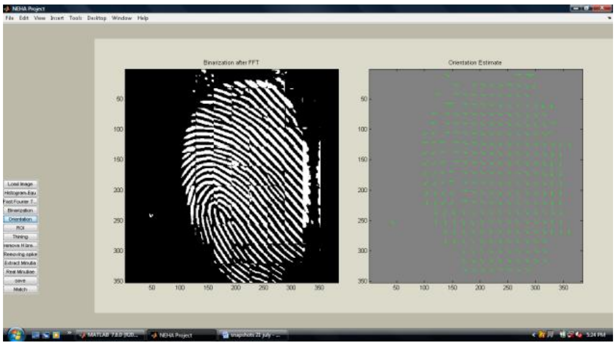
ENHANCED IMAGE USING FFT



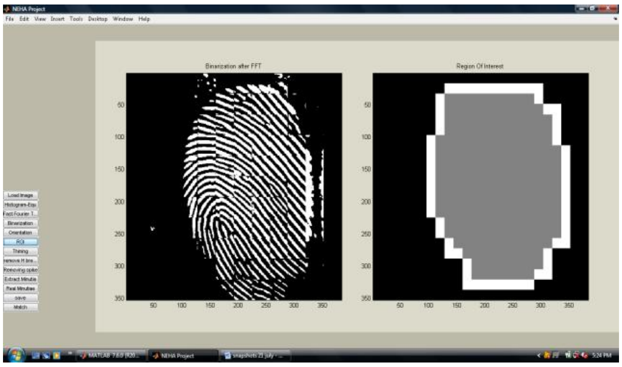
BINARIZED IMAGE



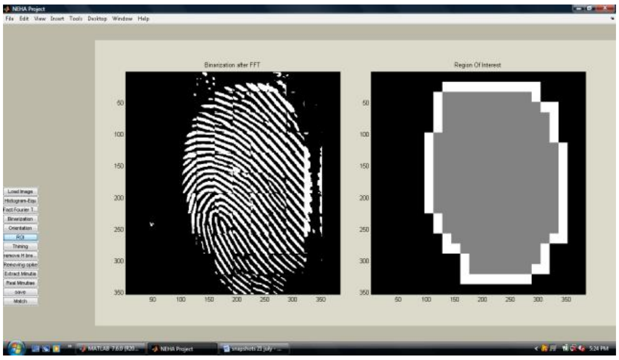
AFTER RIDGE DETECTION



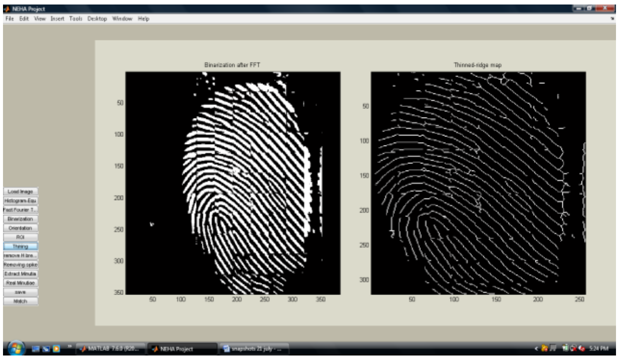
AFTER ROI



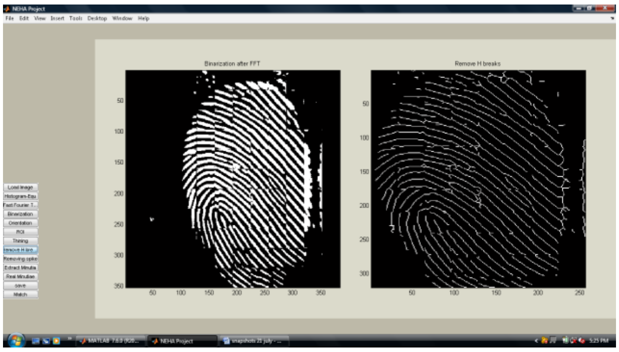
AFTER ROI



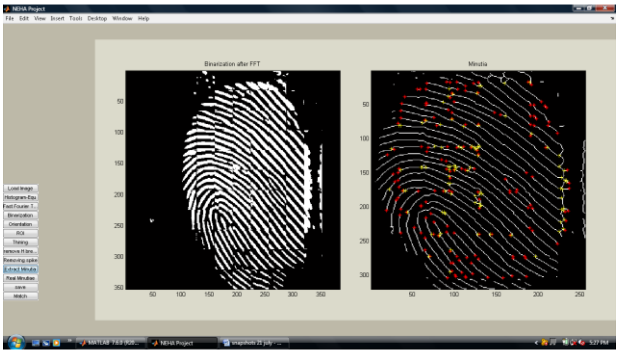
AFTER THINNING



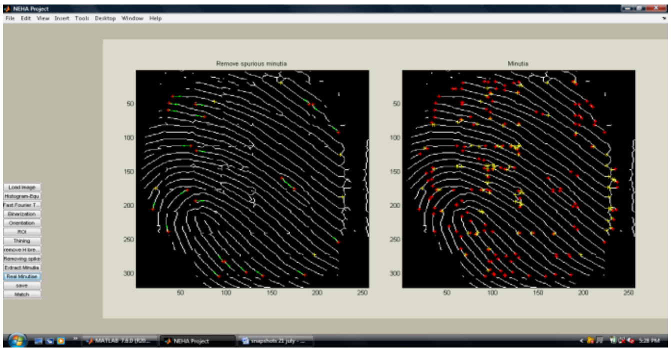
AFTER REMOVING H-BREAKS



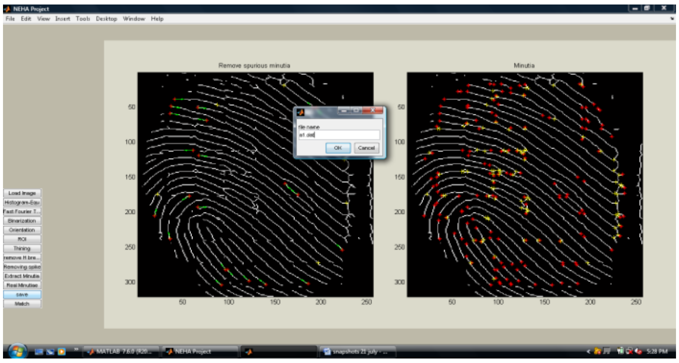
AFTER GETTING MINITIAE POINTS



AFTER REMOVING SPURIOUS MINITIAE POINTS



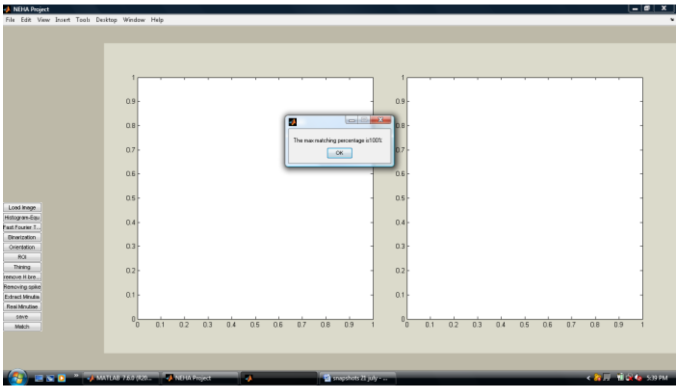
AFTER SAVING MINITIAE POINTS



file name
s1.dat

OK Cancel

AFTER MATCHING



The max matching percentage is100%

OK

FUTURE SCOPE

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 which could improve the future stages and the final outcome.

The additional suggestions which can further improve or extent the system:

- The Binarization process can be improved by automating the filter customization. This enables adaptation of the filter to better suit each fingerprint that is being processed.
- Extension with “enrolment failed” due to the bad quality of the input fingerprint (to dry, wet, small area, etc.. . .).
- Expansion to the fully identification system is possible by adding an algorithm that speeds up the

searching time through the database. This is the only difference between the verification and identification.

- Because the fingerprint verification system is implemented in Matlab, it executes quite slow. By importing the system to the C or assembler language its run time can be speeded up.
- Algorithm can be improved by encrypting the template with some key.
- Other formats of images like jpeg, gif can be used.
- Combination of two different biometrics can be used.

5. ACKNOWLEDGMENT

We would like to express our gratitude for our family, friends and relatives who always encouraged and supported us in all our good and bad times.

6. REFERENCES

[1] W. Sheng and G. Howells and M. C. Fairhurst and F. Deravi, "A Memetic Fingerprint Matching Algorithm", IEEE Trans. I nformation Forensics and Security, 2 (3). pp. 402-412, 2007.

[2] Dr. N. Bhargava, Dr. Bhargava, P. Narooka, and M. Cotia, "Fingerprint Recognition Using Minutia Matching", Volume 3 Issue 4, pp 641-643, 2012.

[3] https://en.wikipedia.org/wiki/Biometrics

[4] Roli Bansal, Priti Sehgal and Punam Bedi, "Minutiae Extraction from Fingerprint Images - a Review", IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 5, No 3, ISSN (Online) : 1694 - 0814, pp 74 - 85, September 2011.

[5] T. C. Clancy, N. Kiyavash, D. J. Lin, "Secure Smartcard Based Fingerprint Authentication".

[6] http://en.wikipedia.org/wiki/Image_processing

[7] Le Hoang Thai and Ha Nhat Tam, "Fingerprint recognition using standardized fingerprint model", IJCSI International Journal of Computer Science Issues, Vol.7, Issue 3, No 7, ISSN (Online) : 1694-0784, ISSN (Print):1694-0814, pp 11-17, May 2010.

[8] Fingerprint Classification and Matching by Anil Jain (Dept. of Computer Science & Engg, Michigan State University) & Sharath Pankanti (Exploratory Computer Vision Grp. IBM T. J. Watson Research Centre)

[9] Surachai Panich, "Method of Fingerprint Identification", Journal of Computer Science 6 (10) : 1062 -1064, ISSN 1549-3636, pp 1062-1064, 2010.

[10] ftp:// ftp.loks.lv/ SYRIS/ UserGuideManual/ Application /About%20FAR_FRR_EER.pdf

[11] Raju Rajkumar, K. Hemachandran, "A Secondary Fingerprint Enhancement and Minutiae Extraction", (SIPIJ) Vol.3, No.2, pp 185 196, April 2012.

[12] J.Ramakrishnan, R. malaisamy, "Performance Measurement and Method Analysis (PMMA) for Fingerprint Reconstruction" , IJCSI International Journal of Computer Science Issues, ISSN : 1694-0814, Vol. 9, Issue 3, No 2,pp 59-62, May 2012

[13]http://www.academia.edu/2537762/Fingerprint_Matching _using_RidgeEnd_and_Bifurcation_Points

[14] A. Pokhriyal, S. Lehri, "MERIT: Minutiae Extraction using Rotation Invariant Thinning", International Journal of Engineering Science and Technology Vol. 2(7), ISSN: 0975-5462, pp 3225-3235, 2010.

[15] Iwasokun G. B., Akinyokun O. C., Alese B. K. & Olabode O., "Adaptive and Faster Approach to Fingerprint Minutiae Extraction and Validation" International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (4) : 2011

[16] R. N. Verma, D.S.Chauhan, "Effect of Pressure Variation On the Fingerprint Minutiae Based Feature Vector Matching", World of Computer Science and Information Technology Journal (WCSIT) Vol. 1, No. 9, ISSN: 2221-0741, pp 376-379, 2011.

[17] S. M Rajbhoj, P. B. Mane, " An Improved binarization based algorithm using minutiae approach for Fingerprint Identification", International Journal of Engineering and Advanced Technology (IJEAT), Volume - 1, Issue-6, ISSN : 2249 – 8958, pp 219-222, August 2012.

[18] Bolle R, and Connell J, "Guide to Biometrics", Springer, 2003.

[19]Hugh Wimberly, Lorie M. Liebrock, 1081 - 6011/11 2011 I EEE D

Authentication to Reduce System Security : An Empirical Study"