

TO ENHANCE THE QUALITY OF BIOMETRIC IDENTIFICATION SYSTEMS

*Dissertation submitted in partial fulfillment of the requirements for the
Degree of*

MASTER OF TECHNOLOGY in COMPUTER SCIENCE AND ENGINEERING

**By
NAVNEET KAUR SANDHU**

Registration No-11500999

Supervisor
Ms. RUPINDER KAUR



School of Computer Science and Engineering

Lovely Professional University

Phagwara, Punjab (India)

April 2017

TABLE OF CONTENTS

PAC FORM.....	ii
ABSTRACT.....	iii
DECLARATION.....	iv
SUPERVISOR'S CERTIFICATE.....	v
ACKNOWLEDGMENT.....	vi
LIST OF TABLES.....	vii
LIST OF FIGURES.....	viii
LIST OF EQUATIONS.....	ix
INTRODUCTION.....	1
1.1 OVERVIEW:.....	1
1.2 BIOMETRIC MULTIMODAL SYSTEM.....	4
1.3 ADVANTAGES OF BIOMETRICS.....	5
1.4 APPLICATION OF BIOMETRIC.....	5
1.5 ERRORS IN BIOMETRIC SYSTEM.....	6
1.6 LATENT FINGERPRINT.....	11
1.7 FINGERPRINT RECOGNITION TECHNIQUE.....	14
CHAPTER 2.....	18
REVIEW OF LITERATURE.....	18
CHAPTER 3.....	29
PRESENT WORK.....	29
3.1 PROBLEM FORMULATION.....	29
3.2 OBJECTIVES OF THE STUDY.....	30
3.3 RESEARCH METHODOLOGY.....	25
CHAPTER 4.....	38
RESULT AND DISCUSSION.....	32

4.1 EXPERIMENTAL RESULTS:-	32
4.2DISCUSSION	42
CHAPTER 5	44
CONCLUSION AND FUTURE SCOPE.....	44
5.1 CONCLUSION.....	44
5.2 FUTURE SCOPE.....	44
REFERENCES	45
PUBLICATIONS	47

LIST OF TABLES

Table 1.1:- Different types of biometrics.....	13
Table 1.2:- Compares Different Biometric on the basis of accuracy, cost and social adaptability.....	15
Table 1.4:- Various stages during recognition of latent fingerprints	18
Table 1.3:- Differentiate Between Latent fingerprints and Exemplar Fingerprints	19
Table 1.5:- Principle categories of minutia are	21

LIST OF FIGURES

Figure 1.1:- A sample flow chart of biometric.....	2
Figure 1.2:- Verification Process.....	3
Figure 1.3:- Identification Process.....	4
Figure1. 4:- Whorl Fingerprint.....	16
Figure1. 5:- Loop Fingerprint.....	15
Figure1. 5: Arch Fingerprint.....	16
Figure 1.7:- Steps of latent fingerprint recognition.....	11
Figure 1.8 :- Fingerprint, Fingerprint with Minutiae, Minutiae.....	15
Figure 1.8:- Local Correlation Based Algorithm.....	16
Figure 3.1:- General fingerprints recognition steps.....	26
Figure 3.2:- Flow Chart of Proposed technique.....	27
Figure 4.1:- Image read.....	34
Figure 4.2:- Image Enhancement using Histogram.....	35
Figure 4.3:- Original Image for binarization.....	36
Figure 4.4:- Binarized Image.....	37
Figure 4.5:- Input image, Output image, Input -Output image.....	38
Figure 4.6:- Thinned image.....	39
Figure 4.7:- Marked Minutia.....	40
Figure 4.8:- Similarity Score.....	41
Figure 4.9:- Comparison of similarity score for brightness preserving dynamic fuzzy equalization and kernel approach.....	43
Figure 4.10:- Error rate.....	44

LIST OF EQUATIONS

Equation.1.....35

Equation 2.....35

INTRODUCTION

1.1 OVERVIEW:-In the computer security world, the term biometric is defined as "Individual's automated recognition based on physiological, behavioral and biological characteristics". Every person has distinct attributes which can be used for identification; these attributes include the retina, iris, fingerprint, voice and many more[1]. During enrollment phase biometric characteristics are acquired by applying different sensors and features are then extracted to make a biometric template. Feature extraction depends on the vendor's proprietary algorithm. After enrollment, the next step is verification in this process an individual offers a biometric input, the algorithm captures this input and produce a trial template, this trial biometric template is compared with the reference template of the individual, which was stored during the enrollment phase. Based on this comparison, the system yields rejection or acceptance.

Fingerprint traits are considered more reliable and are extensively used for authentication purposes. On the tip of the finger the ridge patterns are referred as a fingerprint. Every individual is thought to have a unique fingerprint[1]. Fingerprint uniqueness is based on its ridge structure and on certain ridge eccentricities known as the minutiae points. The comparisons between two fingerprints are done using the minutiae points. In many commercial fingerprint matching systems minutiae-based matching algorithms are used. Minutiae-based matching depends on the detection of delta and core for pre-alignment and on accurate minutiae extraction. Errors can be introduced by missing or spurious minutiae's.

Fingerprint recognition technique is using in the various field to identify the individual. A fingerprint is an impact left by the friction ridges of a person's finger, ready to be used to distinctive people from the distinctive pattern of whorls and features of the fingertips. There are different types of fingerprint pattern whorl, loop, and arch.

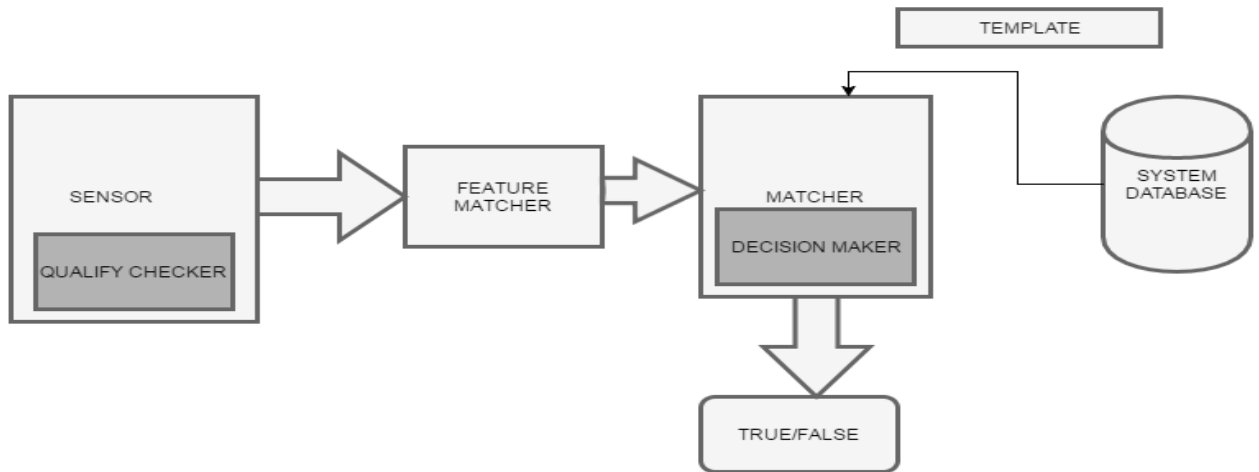


Figure 1.1:-A sample flow chart of biometric

Biometrics system identifies the individuals based on the corresponding features thereby providing the authentication whenever needed with better security mechanisms. In addition to this it is used to distinguish the people in a large gathering who are under observation. The biometric techniques are used to measure and analyze the personal characteristics. These characteristics includes both physiological and behavioral[1][2].

a. Physiological

- i. Face
- ii. Fingerprint
- iii. Hand
- iv. Iris

b. Behavioral

- i.
- ii. Keystroke
- iii. Signature
- iv. Voice

In the biometric system there are two main processes. One is validation and another is verification. In the validation process, the input claimed the identity and check with the

stored values. But in the verification process, the input matched with the large data and gets the similar images.

Validation of a person which is based upon biometric check is turning out to be progressively well-known in different applications like managing an account, aeronautics, monetary exchanges and so on. There are two functions used by a biometric system, one is identification and the other is verification. Verification system relies on comparing the presented biometric with a biometric reference that is already stored in the system which generates result much faster and accurate than the conventional identification systems, even with the increase in the size of the database.

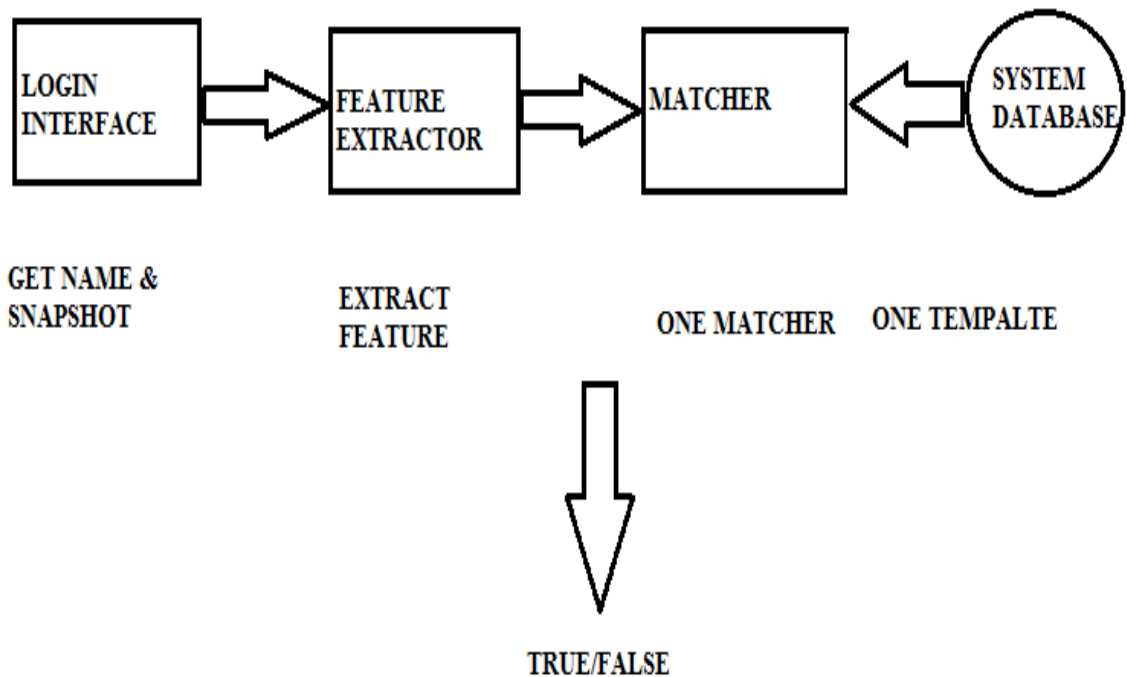


Figure 1.2:-Verification Process

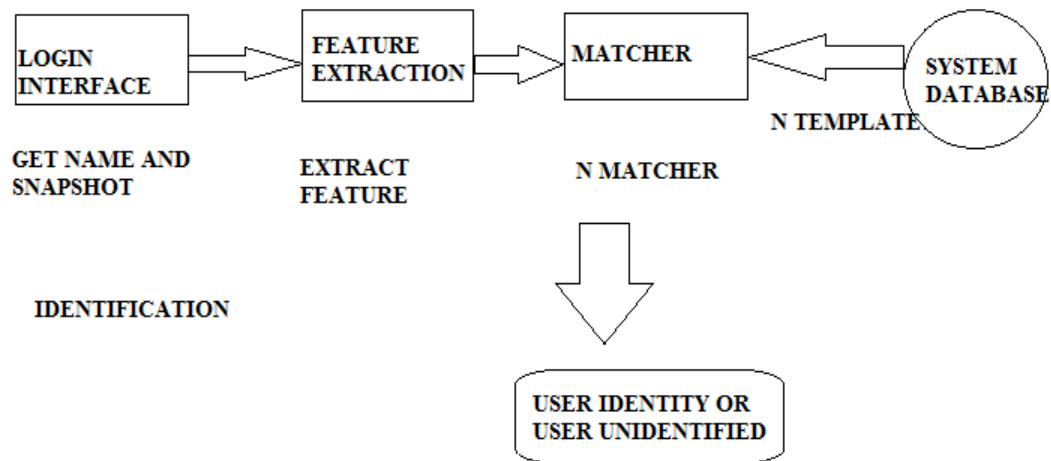


Figure 1. 3:-Identification Process

1.2 BIOMETRIC MULTIMODAL SYSTEM

Biometric multimodal systems use different more than one sensor to overcome the boundaries of biometric unimodal systems[3]. Biometric unimodal systems are restricted by the reliability of their identifier, it is doubtful that many unimodal systems will undergo from identical limitations. Biometric multimodal systems can take group of information from the same information from different biometrics. Biometric multimodal systems can mingle these unimodal systems concurrently. Biometric fusion information can happen at different stages of a recognition system.

Different stages of biometric fusion information:-

- At stage of feature level fusion extracted the feature from multiple biometrics are mingled.
- Score level matching fusion develops the scores generated by more than one classifiers pertaining to different modalities.
- At the last stage of decision level fusion the final results of more than one classifiers is combined via different techniques. Feature level fusion is more valuable than the other levels of fusion because the feature group contain good information about the input biometric data than the score matching level of the output decision. Fusion at

the feature level is probably to offer better identification results than the other stages of the level.

1.3 ADVANTAGES OF BIOMETRICS

Security: One of the major advantages of this framework is that they cannot be presumed or stolen. The issues regarding effective watchword frameworks are such that frequently there exists grouping of letters, numbers, images, which makes it hard to recollect every time. The difficulty with these token is they could be effortlessly stolen or missed where both of these expected strategies include the risk of data being shared. However that would not be the situation with the biometric attributes, and does not need to handle the risk of sharing, replication, and misrepresentation.

Accurate Identification Process: The traditional security frameworks are based on passwords, radiant cards; it can accomplish an irregular state of precision with biometrics frameworks. On the off chance when effectively set up the framework, that can make use of natural attributes such as filters for fingerprints and iris, which offers one of a kind and accurate strategies of recognizable proof. These elements cannot be easily and effortlessly copied that provides safety and security by just approving an authorized individual to get access.

Ease of use and safety: The privileged thing about the utilization of biometrics for identification is advanced frameworks are assembled and developed to be simple and more over to safe to use. The innovation in biometrics yields accurate results with negligible obtrusiveness as a straightforward output or a photo that is generally required. In addition the product as well as the equipment can be utilized effortlessly and anybody can implement with no requirement of advance preparation.

1.4 APPLICATION OF BIOMETRIC

- Entry control
- Logical Access control
- Attendance and time
- Surveillance
- Physical Access Control


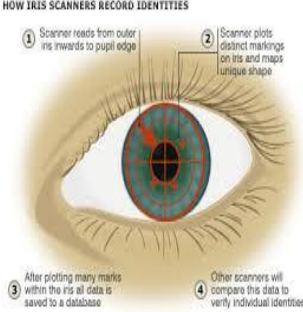
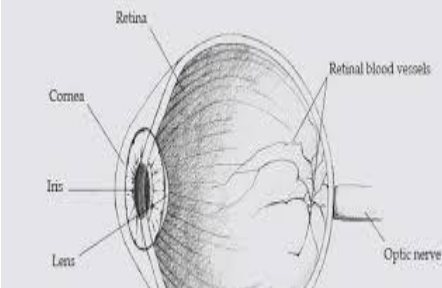

- Law enforcement
- Cross border security
- Adhaar card
- Financial transaction system
- Identification system.


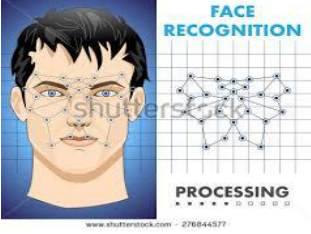
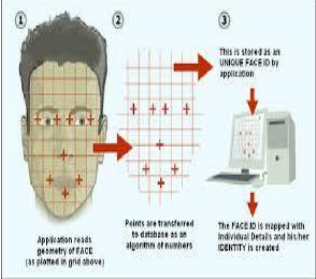

1.5 ERRORS IN BIOMETRIC SYSTEM

Types of errors:-

- **False genuine:** The probability that incorrectly matches the input pattern to a non-matching data in the database. A false match error in biometric system is the one which wrongly declares a correct match among the input pattern and the existing stored template pattern.
- **False imposter error:** It describes the situation where the biometric system wrongly declares as a failure between input pattern and stored template pattern. A false rejection error occurs when a matching pair of biometric data is wrongly rejected by the system.
- **Failure to capture error:** - When the input device is unable to capture biometric information. This kind of error is human dependent error.
- **Failure to enroll error:** - The system is unable to extract the information from the biometric system. It is strongly dependent the human factor and device.
- **Ranking error:** - This error is depending on the prefixed integer value.

Table 1.1:-Different types of biometrics

Name	Type of biometric	Description	Example
DNA	Chemical	The identification of an individual pattern using the analysis of segment from DNA.	 <p>Examples of DNA Fingerprints!</p>
Eye-Iris Recognition	Visual	The feature that found in iris is used to identify an individual.	 <p>HOW IRIS SCANNERS RECORD IDENTITIES</p> <ol style="list-style-type: none"> 1 Scanner reads from outer iris inwards to pupil edge 2 Scanner plots distinct markings on iris and maps unique shape 3 After plotting many marks within the iris all data is saved to a database 4 Other scanners will compare this data to verify individual identities
Eye-Retina Recognition	Visual	A pattern of veins in the back of the eye is used to accomplish recognition.	 <p>Retina Cornea Iris Lens Retinal blood vessels Optic nerve</p>
Ear	Visual	Using the shape of the ear define the identification of an individual.	 <p>Helix Superior crus of antihelix Antihelix Concha Antitragus Ascending helix Fosseta Inferior crus of antihelix Crus of helix Tragus Incisura Lobe</p>

Signature Recognition[4]	Visual/Behavioral	There are two key types of digital handwritten signature authentication, Static and Dynamic. It defines the individuality of the person.	
Face Recognition	Visual	Face gives the individuality to the person with the different facial features.	
Face Geometry	Visual	It define the shape of the face in the form of matrices and then it check by the sensor.	
Finger Recognition[5]	Visual	The use of the valleys and ridges on the top of the fingerprint identify an individual.	

+

The table 1.2 compares the different fingerprint from the point of view of cost, accuracy, social adaptability.

Table 1.2:-Compares Different Biometric on the basis of accuracy, cost and social adaptability

Biometric technology	Device used	Cost	Social stability	Accuracy
Hand geometry	Scanner	Low	High	Medium-low
Retina scan	Camera	High	Low	High
Fingerprint	Scanner	Medium	Medium	High
Voice recognition	Microphone, telephone	Medium	High	Medium
Signature recognition	Optic pen, touch panel	Medium	High	Low
Facial recognition	Camera	Medium	High	Medium-low
Iris recognition	Camera	High	Medium-low	High

Fingerprints: - A fingerprint is an impact left by the friction ridges of a person's finger, ready to be used to distinctive people from the distinctive pattern of whorls and features of the fingertips[6].

Types of fingerprints:-

- **Whorl:-** Any patterns with a minimum of 2 deltas and one re arching ridge which can be a spiral any variation of a circle is named a whorl loop.



Figure1. 4:- Whorl Fingerprint

- **Loop: -** A loop is a blueprint where the ridges enter from one side and make curve and tend to exit from the same side where they enter. Types of loops:-Plain loop, Ulnar loop,Radial loop.



Figure1. 5:-Loop Fingerprint

- **Arch: -** An arch is the pattern where the ridges enter from one side and rise from the center and exit from the other side. The arch is of two types: - Plain arch and Tented arch.



Figure1. 6: - Arch Fingerprint

1.6 LATENT FINGERPRINT:-Latent fingerprint has been used as proof in the court of law for over 100 years. Researchers found some important challenge in latent fingerprint recognition like background noise, low information content. Latent fingerprints are deposited when amino acids, proteins and sweat other natural secretions present in the surface of the skin come in contact with an external surface. These fingerprints are usually not seen by eyes of human directly[7]. It can be lifted and photographed in order to be used as proof in court proceedings. There are some stages or steps which are going to used in recognition of latent fingerprints. The steps are as follows:-

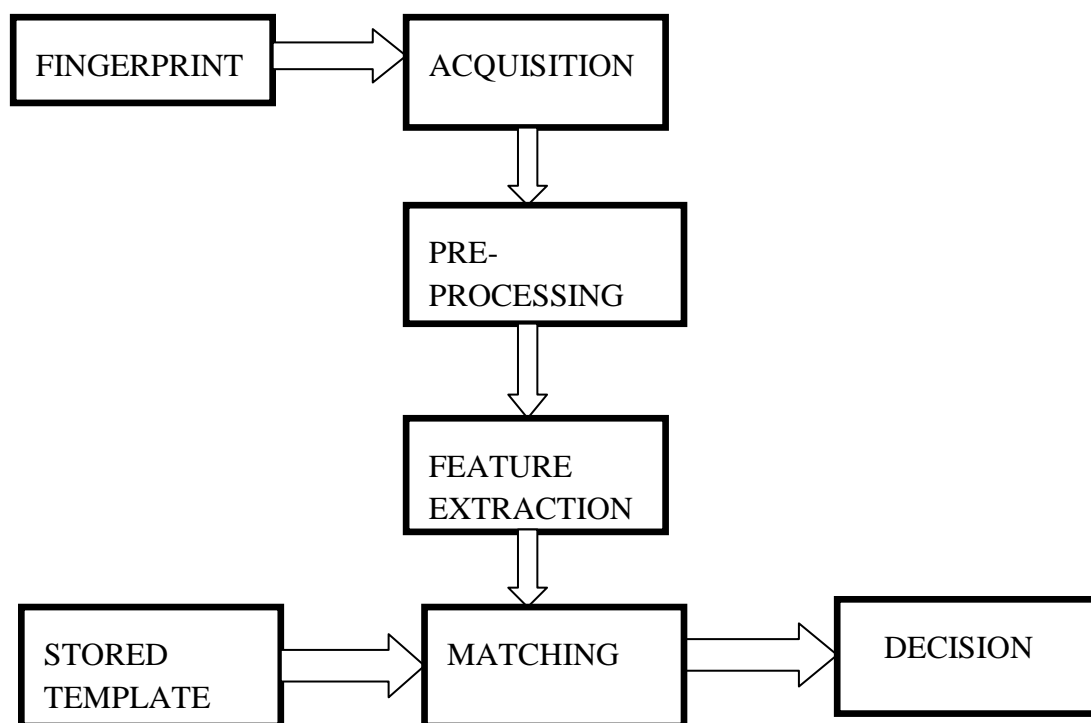




Figure 1.7:- Steps of latent fingerprint recognition.

Table 1.3:-Various stages during recognition of latent fingerprints

Stages	Process
Image Acquisition	Read Image
Preprocessing	FFT Image enhancement/Fuzzy Histogram Equalization
Feature extraction	Minutia extract
Matching	Redundancy removal

Table 1.4:-Differentiate Between Latent fingerprints and Exemplar Fingerprints

Latent fingerprints[8]	Exemplar Fingerprints
Latent fingerprint is that the likelihood recording of friction ridges deposited on the surface of an object or a wall.	Exemplar prints is one taken intentionally from individually for keeping purpose
It is low in quality	It is good in quality
It has less number of minutia points	It has as compare to latent more points of minutia
Latent fingerprint is partial, distorted and having background noise.	Exemplar fingerprint is smooth in nature.
<p>Latent fingerprints are not easily recognized. It cannot see by naked eye.</p> 	<p>It is easily recognized</p> 

1.7 FINGERPRINT RECOGNITION TECHNIQUE: Fingerprint is commercially successful biometric modality use for recognition. Fingerprint has been used in the forensic and law enforcement to identify the criminals. It has a long history as a means of identify individuals. Based on the uniqueness and persistence of fingerprints, fingerprint recognition become more popular in many application like forensic, law of enforcement, border control etc. There are different types of fingerprints. A fingerprint comprises of pattern of ridges and valleys upon the surface of finger of a person. A ridge can be defined as a single curved segment, whereas the region between two adjacent ridges forms a valley.

TECHNIQUES FOR FINGERPRINT RECOGNITION

Fingerprint recognition technique is the most commonly used and established biometric method and is the simplest to use for a higher security level. Even it is easy to install and it consumes less time and effort in acquiring one's fingerprint. It is a very secure technique in each and every field where security of data is demanded.

Minutiae Based Technique: This is the best fingerprint recognition technique. The process of scanning minutiae needs to work on gathering specific points in a finger image. Minutiae's are extracted from the two fingerprints and that they can store as cluster of points within the two-dimensional manner[9]. These minutia points define the unique of the fingerprints. A detail primarily based matching consists of finding the alignment between the template and therefore the input trivia sets that result in most variety of trivia pairings. Additionally there are two major specifications, ridges and bifurcation. Minutia mean little points of interest, and this to the conduct of the edges discontinuities, for example, end, bifurcation and trifurcation or different elements, for example, pores (little openings inside the edges), lake (two shut bifurcations), spot (short edges), and so forth. Most frameworks use just the end and bifurcations. With the goal of coordinating the fingerprints we have to extricate the unique finger impression elements, for example, details and peculiarity focuses[10][11].



Figure 1.7:- Fingerprint, Fingerprint with minutiae, minutiae

Table 1.5:-Principle categories of minutia are

Name	Represents
Ridge ending	end of a ridge
Ridge bifurcation	single ridge that divides into two ridges
Short or independent ridge	a ridge that begins, travels a small distance and then it ends
Island	a single small ridge within a short ridge or a ridge ending which is not connected to the remaining ridges
Ridge enclosure	A ridge that bifurcates and then reunites later to continue as one ridge
Spur	Denotes a bifurcation that has a short ridge branching off a bigger ridge
Crossover or bridge	A short ridge which runs along parallel ridges

Delta	It is a Y-shaped ridge meeting
Core	It is a U-shaped ridge pattern

Correlation-based Technique: To deal with some of the issues of minutiae-based methodology, one should have to choose an alternative methodology[12]. Correlation-based approach makes use of the gray-level data that is extracted from the fingerprint image. This is a promising approach to fingerprint matching where the new generations of fingerprint sensors are being used. The main limitation of this method is its high complexity of computation as well as low tolerance to nonlinear distortion and contrast variation. Hence there should have been another alternative proposals which are able to compute the correlation locally rather than computing it globally, in which only the regions of interest (for example, minutiae and regions of singularity) are to be selected and matched. Such kind of algorithms uses simple approaches for alignment of two images of fingerprints and subtract the input image from the template image to check whether the ridges corresponds[13][10].



Figure 1.8:-Local Correlation Based Algorithm

Image Based Matching/Pattern Based Matching: - Image-based matching technique compares two different images. These two images are aligned in the same orientation. The image matching finds the middle points in the image. In the image-based matching the technique the template contains the type size and the pattern orientation within the image. Image is compared with the template to recognize the degree[14].

CHAPTER 2

REVIEW OF LITERATURE

Anil K. Jain and Karthik Nandakumar (2004)[13] proposed Local Correlation based on Fingerprint Matching. This paper describes a correlation-based fingerprint matching which utilizes correlation of regions locally around the minutiae to identify the degree of matching between more than one fingerprint images. The minutia extraction algorithm is used to remove query images, templates, ridges points. They have displayed a local correlation based fingerprint impression matcher which uses local correlation of regions to determine the degree of the match between the two different fingerprints This strategy utilizes an outstanding calculation for details extraction and utilizations Procrustes analysis of corresponding ridge curve with the template to align. The two pictures are upgraded utilizing Gabor filter banks and the standardized cross-connection is utilized as the nature of the details coordinate

Mukvinder Singh ,Manvjeet Kaur and Parvinder S. Sindhu (2008)[9] presented a Minutiae Extraction Technique in fingerprint Verification System. This system introduced both methods to build a minutia extractor and a minutia matcher using two techniques one is FFT and the other one is histogram equalization for fingerprint image enhancement and the other is Crossing Number Perception for Minutiae Extraction. For improving thinning process, removal of false minutiae, and for marking of minutia, they used Segmentation with Morphological operations. In this they explain how to segment the image. In the morphological there are two operations one is open and the other one is close. The open expand the images by introducing the background noise, the close operation is used to shrink the image. Minutia-based fingerprint recognition techniques signify the fingerprint by its bifurcations local features, and like terminations.

Hrushikesh Garud, Debdoot Sheet *et.al.* (2010)[15] proposed a novel modification of the brightness conserving dynamic bar graph(histogram) equalization technique to reinforce its brightness conserving and distinction sweetening skills whereas reducing its machine complexity. Within the projected technique referred to the technique which is used to enhance the image the technique as brightness conserving dynamic fuzzy bar graph equalization (BPDFHE), uses fuzzy statistics of digital photos for his or her illustration and method. Illustration and method of images at intervals the fuzzy domain allows the technique to handle the quality of gray level values in an exceedingly very higher methodology, resulting in improved performance. Execution time depends on image size and nature of the bar graph, however experimental results show it to be faster as compared to the techniques compared here. The performance analysis of the BPDFHE at the side of that for BPDHE has been given for comparative analysis.

Mayank Vasta, Anush Sankaran *et.al.* (2014)[10] the researchers survey the latent fingerprints. Latent fingerprints has used as proof in the court of law. They have identified many challenges that are very important for recognition of latent fingerprint. Some of these challenges are:-background noise, partially, distorted, low information content. In this paper they explain the different level of the feature extraction. There are three levels. In level 1 the overall flow of ridge pattern contains. The ridge pattern basically smooth in nature but which are not smooth in nature that comes in the singular point. Fingerprints can be classified in loop, arch and whorl. To capture the singular points and determine the ridge pattern the images should be captured at least 300 PPI resolutions. In level 2 the minutia points constitutes. The minutia points are the local fingerprints features and discontinuity in the flow of ridges.

Jie Zhou, Jianjiang Feng, Xiao Yang (2014)[16] presented the dictionary based orientation field estimation approach. Lexicon based introduction field estimation approach has indicated promising execution for inert fingerprints. In this paper, they look to misuse more grounded earlier learning of fingerprints with a specific end goal to additionally enhance the execution. Understanding that edge introductions at various areas of fingerprints have distinctive qualities, they propose a limited word references based

introduction field estimation calculation, in which loud orientation patch at an area yield by a nearby estimation approach is replaced by genuine orientation patch in the neighborhood word reference at a similar area. The precondition of applying confined word references is that the stance of the idle unique mark should be assessed. They propose a Hough change based unique mark posture estimation calculation, in which the forecasts about unique finger impression posture made by all introduction fixes in the inactive unique mark are amassed. Trial comes about on testing inactive unique finger impression datasets demonstrate the proposed strategy beats past ones especially.

Anush Sankaran *et.al.*(2014)[10] described latent fingerprints identification is of basic significance in criminal examination. FBI's Next Generation Identification program requests latent fingerprints to be performed in lights-out mode, with next to no or no human negotiation. In any case, the execution of a mechanized still unique mark distinguishing proof is restricted because of uncertain robotized include extraction, particularly due to noisy ridge edge and presence of background noise.. In this paper, they proposed a novel descriptor based details identification calculation for dormant fingerprints. Minutia and non-minutia descriptors are learned from an extensive number of tenprint unique mark patches utilizing stacked denoising meager auto-encoders. Latent fingerprints details extraction is then acted like a parallel arrangement issue to order fixes as minutia or non-minutia fix. Tests performed on the NIST SD-27 database demonstrates promising outcomes on latent finger impression coordinating.

Shuiwang Li *et.al.* (2015)[17] presented the concept of minutiae distribution on the fingerprint. It plays a very important role in the study of different fingerprint recognition techniques such as fingerprint uniqueness for powering the scientific validity of fingerprint proof and generating synthetic fingerprints for high scale system evaluation. Fingerprint minutiae are not homogeneously distributed as once understood. Spatial inhomogeneity has been found in minutiae distribution. Spatial inhomogeneity is generally observed in fingerprint minutiae pattern.

Guoqiang Li, Bian Yang, and Christoph Busch(2015) [3]explained the Biometrics identification systems containing on a large-scale database have been gaining increasing attention. In order to speed up searching in a large-scale fingerprint database, fingerprint indexing algorithm has been studied and introduced into biometric identification system. One critical component of a fingerprint indexing algorithm is the feature extraction method.

Benjamin Tams, Preda Mihăilescu and Axel Munk(2015) [18] they described the theory of the fuzzy vault scheme. The scheme is a cryptographic primitive which can used to protect fingerprint pattern where they saved. This is analysis for the implementation for brute force security only in the account. They redecorate a minutiae based fuzzy vault implementation securing an adversary from running attacks via record diversity. They proposed a way or tool for robust absolute fingerprint pre-alignment. In the combination they obtain a fingerprint-based fuzzy vault that resist known record diversity attacks and that doesn't lost or leak information about the protected fingerprints from auxiliary alignment data.

D. Binu and P. Malathi (2015) [19]proposed a Multi-Model based Biometric Image Retrieval for Enhancing Security. In this work they introduced the multimodal biometric authentication which recognizes the human being with the consideration of four models fingerprint, face, palm, and iris improve the accuracy.

Ezhilmaran D, Adhiyaman M (2015)[20] explained that fingerprint matching is one of the amongst and the foremost necessary problems in Automatic Fingerprint Identification System (AFIS). It has emerged as a good tool for human recognition as a result of its singularity, generality and invariability. The importance of this work is to observe the matching and similarity for two or more fingerprint pictures at the same time. This planned algorithm has been developed supported minutiae points that examine n range of pictures.

Zhanpeng Jin, and Sarah Laszlo , Maria V. Ruiz-Blondet (2016)[21] described the work on brain biometric. The big mass of existing work on brain biometrics has been

done on the ongoing electroencephalogram (EEG). They disagree that the averaged Event-Related Potential (ERP) may provide the latent for more accurate biometric identification rules and regulations. They describe the Cognitive Event Related Biometric Recognition (CEREBRE) Protocol. An ERP biometric protocol designed to extract individually unique responses from multiple functional brain systems.

Sachin Kumar and R. Leela. Velusamy (2016)[8] described the work on the latent finger. In this research they compared the exemplar finger with the latent finger. Exemplar finger has good image quality and latent finger has some background noise and low image quality. In their they found the similarity between the exemplar finger and latent finger using kernel approach. To find the similarity between the images is not an easy task. Latent finger is partial, distorted and has some background noise. The main aim of this research is to design an intellectual procedure comparable to human perception in matching the exemplar fingerprint to latent fingerprint. Latent fingerprint is poor image quality and non-linear distorted, due to these reasons the similarity check is not easy and also matching is one of the risky concept.

Ajay Kumar Singh et.al (2016)[7] presented in this paper that the online fingerprints by biometric system is not wide used currently a days and there's less scope as user is friendly with the system. This paper represents a framework and applying the latent fingerprints obtained from the crime scene. These prints would be matched with our information and determine the criminal. For this method have to induce the fingerprints of all the voters. This technique might scale back the crime to an oversized extent. Latent prints area unit completely different from the patent prints. These fingerprints area unit found at the time of crime and these fingerprints area unit left accidentally. By this approach we have a tendency to collect these fingerprints by chemicals, powder, lasers and other physical means that. Sometimes, fingerprints have a broken curve and it's not thus clear owing to air mass. They apply the M_join rule to affix the curve to attain better results. Thus, their projected approach eliminates the pseudo trivialities and joins the broken curves in fingerprints.

3.1 PROBLEM FORMULATION

Fingerprint identification and others system like iris, DNA, speech recognition, palm etc are more reliable and are extensively used for authentication purposes. In the fingerprint recognition on the tip of the finger the ridge patterns are referred as a fingerprint. Every individual is thought to have a unique fingerprint. Fingerprint uniqueness is based on its ridge structure and on certain ridge eccentricities known as the minutiae points. The comparison between two fingerprints is done using the minutiae points. In many commercial fingerprint matching systems minutiae-based matching algorithms are used. Minutiae-based matching is very depends on the detection of delta and core for pre-alignment and on accurate minutiae extraction. Errors can be introduced by missing or spurious minutiae's.

The performance of automatic identification and verification algorithms depends on the quality of input fingerprint image. Many researchers have proposed a number of techniques for the fingerprint identification till now. Each one used some different technique to find or improve the different parameters like accuracy, performance, similarity, reduce error rate. There is a need of minutiae removal step to improve the accuracy and similarity of the existing fingerprint recognition techniques. In the current research work, the brightness preserving dynamic fuzzy histogram equalization algorithm and fast Fourier transformation is used to remove the redundancy from the minutia points and enhance the image for similarity measure and improve the error rate.

3.2 OBJECTIVES OF THE STUDY

Objectives of the study are:- The objective of the study is to improve the quality of the fingerprint recognition technique. With the use of different technique reduced the false minutia removal and improve the similarity and reduce the error rate.

1. To study and analyze various fingerprint recognition techniques and work towards their improvement.
2. To preprocess the latent fingerprint using Brightness Preserving Dynamic Fuzzy Histogram Equalization on Kernel approach for similarity measure.
3. To extract the minutiae points and mark them using morphological operation and cross number respectively.
4. To remove the noise and match the original image with its different impressions.
5. To validate the improved quality of the present work by comparing it with already existing Kernel approach

3.3 RESEARCH METHODOLOGY

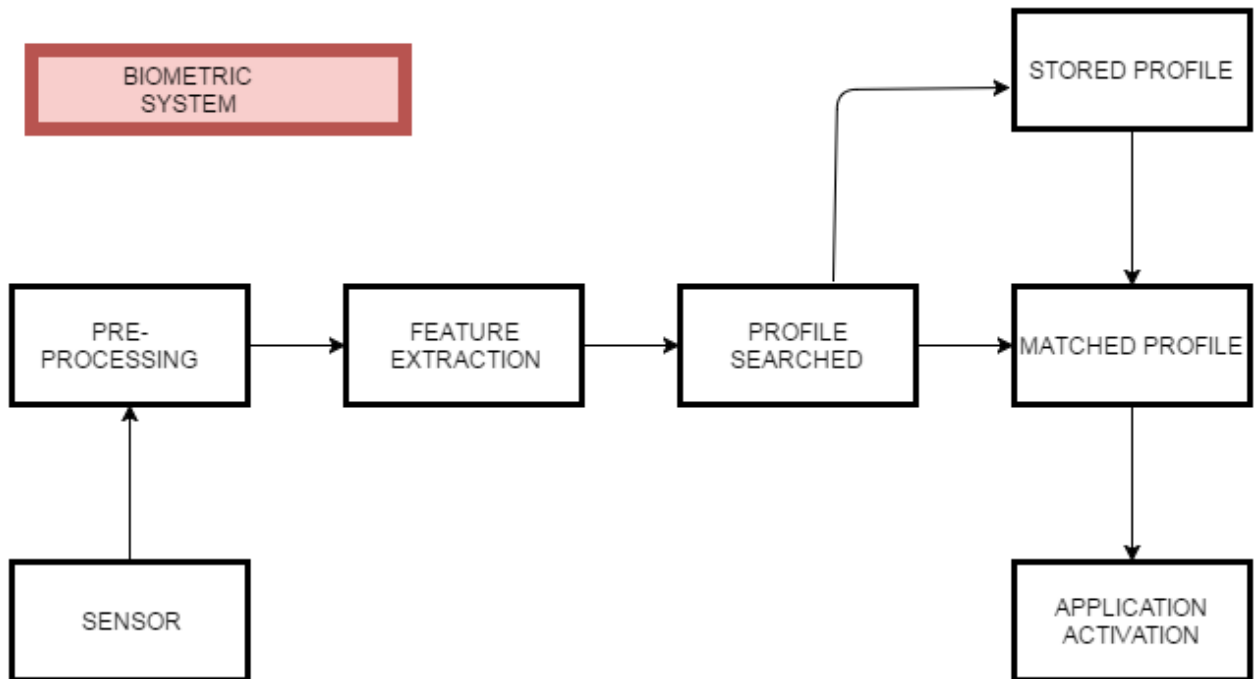


Figure 3.1: - General Flowchart of Fingerprint Recognition

Biometrics security system plays indispensable role in everyone's life. Fingerprint recognition technology and facial recognition technique are its main application. With these technologies, we can recognize any person in a group; therefore, we can verify their identification. Matching is the important step to verify whether fingerprints are genuine or false[4].

The main steps in the methodology are first to read the image using different sensor like digital camera. And after acquisition of image the preprocessing is done with the two techniques: one is FFT enhancement and the other is Brightness Preserving Dynamic Fuzzy Equalization [10]. After this step the minutia feature is extracted and last the matching is done. The given capture image is match with the already stored database.

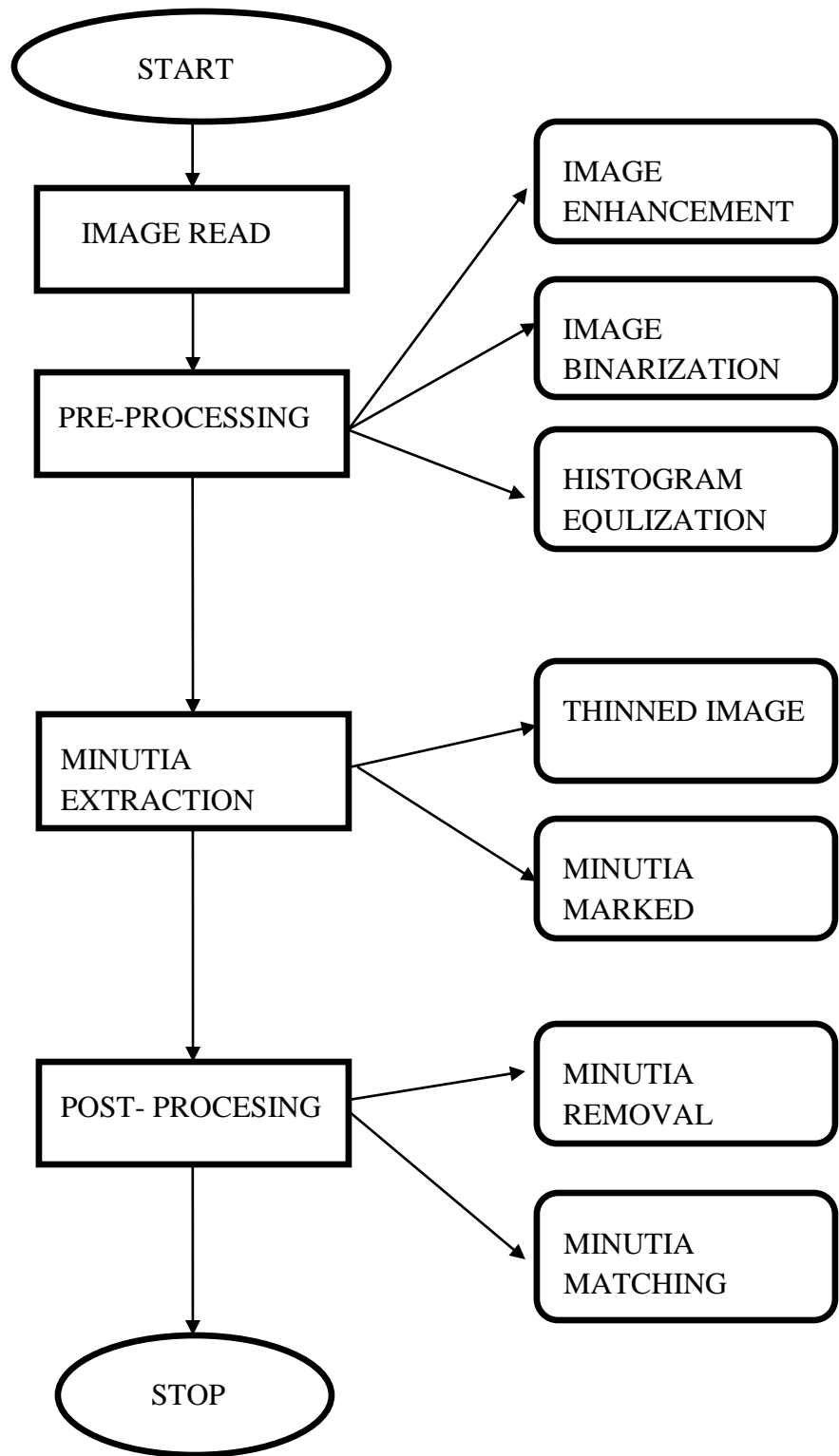


Figure 3.2:- Flowchart of Proposed Work

STEPS

1 Image Read: - First step is to read image by different sensors. In this step, the fingerprint image is loaded by using the MATLAB 2014 built-in function.

```
>>i=imread('101.tif');  
>>imshow(i);
```

2 Pre-Processing:-In preprocessing step, image enhancement [9]and image binarization are performed. An image enhancement technique improves noise and sharpens the edges. Image binarization is the process to converts a grayscale image into a binary image. A threshold is chosen and pixels values above threshold are classified as white and below threshold as black.

2.1 Image Enhancement:- Fingerprint images need to be clear for easy processing, so for this enhancement methods for image are used to make the images clear for advanced operations[22][8]. As the images obtained from sensing devices like scanners are not considered of great quality that's why image enhancement methods are used to improve the contrast between valleys and ridges and is helpful for keeping the higher accuracy rate. For image enhancement we used two methods first is Histogram Equalization and second is Fourier Transform. Some useful method which is used for image enhancement:-

- Histogram Equalization.
- Noise removal using wiener filter.
- Linear contrast adjustment.
- Filtering using Morphological operators.

```
i=imread('101.tif');  
imshow(i);  
imhist(i);
```

Imhist() function is used to enhance the image.

2.2 Image Binarization:- Image binarization converts a picture of up to 256 grey levels to a black and white image. Frequently, binarization is employed as a pre-processor before OCR. In fact, most OCR packages on the market work solely on bi-level (black & white) pictures. The simplest way to use image binarization is to settle on a threshold worth, and classify all pixels with values higher than this threshold as white, and every one different pixels as black. the matter then is a way to choose the right threshold. In several cases, finding one threshold compatible to the complete image is incredibly tough, and in several cases even not possible. Therefore, adaptation image binarization is required wherever best threshold is chosen for every image space.

```
bw = im2bw(X,map,0.5);  
imshow(bw),title('Output of im2bw')
```

2.3 Brightness Preserving Dynamic Fuzzy Histogram equalization:-It improves brightness, contrast enhancement while reducing computational complexity [28]. This technique uses fuzzy statistics of digital images for representation and processing as well as technique handles the ambiguity of gray level values in effective way which results in improved performance. Fuzzy histogram computed with a suitable member functions which does not provide random fluctuations or missing intensity levels hence making it smooth.

```
inputImage = imread('202.eft');  
outputImage = fcnBPDFHE(inputImage);  
figure, subplot 131, imshow(inputImage),title('Input Image');  
subplot 132,imshow(outputImage),title('output Image') ;  
subplot 133, imshow(inputImage-outputImage,[]),title('Input/output Image');
```

2.4 Enhancement by Fourier Transform:- To enhance the fingerprint image by Fourier Transform, an image is firstly divided into small blocks and then Fourier Transform is applied to each processing block. Fourier Transform is given by:

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

To enhance a particular block by the dominant frequency, we multiply the block's FFT (Fast Fourier Transform) by its magnitude multiple times. The magnitude of the original FFT is given by $FFT = \text{abs}(F(u, v)) = |F(u, v)|$

After this we get an enhanced block by

$$g(x, y) = F^{-1}\{F(u, v) \times |F(u, v)|^K\} \dots \dots \dots \text{Equation 2}$$

For $x = 0, 1, 2, 3, \dots, 31$ and $my = 0, 1, 2, 3, \dots, 31$

After applying FFT the enhanced images discards the false connection among ridges and improve broken points.

1 if the intensity value of the pixel is greater than the mean intensity value of the current block.

3 Minutiae Extraction:

A ridge bifurcation is outlined because the purpose wherever a ridge forks or diverges into branch ridges. Collectively, these features are called minutiae. In minutiae extraction stage image thinning is applied and minutiae's are detected.

3.1 Image Thinning:

After binarization ridge thinning is applied to remove the extra pixels of the ridges till the ridges remain one line. In each scan the thinning algorithm marks the extra pixels in (3*3) image window and then removes them after the number of scans. On this thinned map further morphological operations are applied to discard spikes and single points in the image. These spikes and single points are considered processed noise.

3.2 Minutiae Marking:

Fingerprint thinning process makes minutiae marking easy. For minutiae marking and extraction Cross Number (CN) is commonly used. Generally in 3*3 pixel windows if 1 is center pixel and there are three neighbors with value 1 then the center pixel with value 1 is called a **ridge branch**. If in 3*3 window center pixel is 1 and there is only one neighbor with value 1 then center pixel is **ridge ending**. For pixel values P, if $C_n(P) == 3$ then the point is ridge bifurcation and if $C_n(P) == 1$ then the point is ridge end.

4 Post-processing:

In post-processing step false minutiae's are removed.

4.1 Minutiae Removal:

Fingerprint images are usually not get fully fixed in the preprocessing stage, like spurious ridge breaks are not fully discarded. In general all the earlier stages introduce some processing noise which then introduces the false minutiae. If these spurious minutiae's are considered genuine then this will affect the system accuracy. So to make the system effective a mechanism is needed for the removal of false minutiae's. Following are the steps to remove false minutiae:

Distance

Similarity and distance are the concept that combined work to induce a similarity score. Matching is more positively when the distance is measured by Euclidian. It satisfies formula based on the spatial and angular measurement with some threshold value. If the given threshold value is less than the similarity score, it means it improve and finger is identical.

Step 1- The distance between one termination and one bifurcation should be greater than D, if distance is less than D and both minutiae's are on the same ridge then discard both of them. Where D is the average distance among two neighboring ridges.

Step 2- If two bifurcations are on the same ridge and the distance between them is less than D then discard both of them.

Step 3- If there are two terminations on the same ridge and distance and the length of the ridge is less than D then discard both terminations.

4.2 Minutiae Match[23][24]: -The minutiae match algorithm determines, given two sets of minutiae's whether they belong to same finger or not. The elastic match algorithm is used to count the pair of minutiae and then consider the minutiae's to be identical if two minutiae's have nearly same direction and position. The number of total pairs of minutiae's divided by the number of minutiae present on the template fingerprint is the final match ratio of two fingerprints. The matching score is actually ratio * 100. If the matching score is greater than the specified threshold, then the fingerprints are identical.

Matching Algorithm[27]

Step 1:-Elastic Matching algorithm is used to estimates the non-linear transformation in the different two stages

Step 2:- In the first stage it determines which minutiae is probably matching with the given data on the base on local similarity.

Step 3:- Second stage uses the possible correspondences to estimate a global ridge transformation.

This matching algorithm is used to count the pair of minutiae and consider to be identical if two minutiae's have nearly same direction.

CHAPTER 4

RESULT AND DISCUSSION

4.1 EXPERIMENTAL RESULTS:-In this framework, the similarity measure of the latent fingerprints is checked using Brightness Preserving Fuzzy Histogram Equalization approach. The proposed work implemented in MATLAB 2014a and verified on FVC2002 DB1-B and NIST SD27 low-quality fingerprint dataset. In the below table describes the analysis of low-quality fingerprints on the base of similarity. Figure 4.8 states that the average similarity score of proposed brightness preserving dynamic fuzzy is 0.2% more than kernel approach. Both approaches work on the same datasets FVC 2002 and NIST SD27. In these datasets stored low-quality image. Low-quality images are those images which have background noise, distorted and partial in nature. In my research work, I have worked on both the datasets.

MATLAB 2014a is used to implement proposed work. In this work, the input image is added which is captured by different sensors and is displayed on the screen. There are different sensors like digital camera, XRAY,MRI to capture the image and using MATLAB function image is read and shown on the screen. Here `imread()` is the function used to read the function and `imshow()` is the function used to show that image on the screen.

Image Read:- In the first step read the image using MATLAB

```
>>i=imread('1.tif');
```

```
>>imshow(i);
```

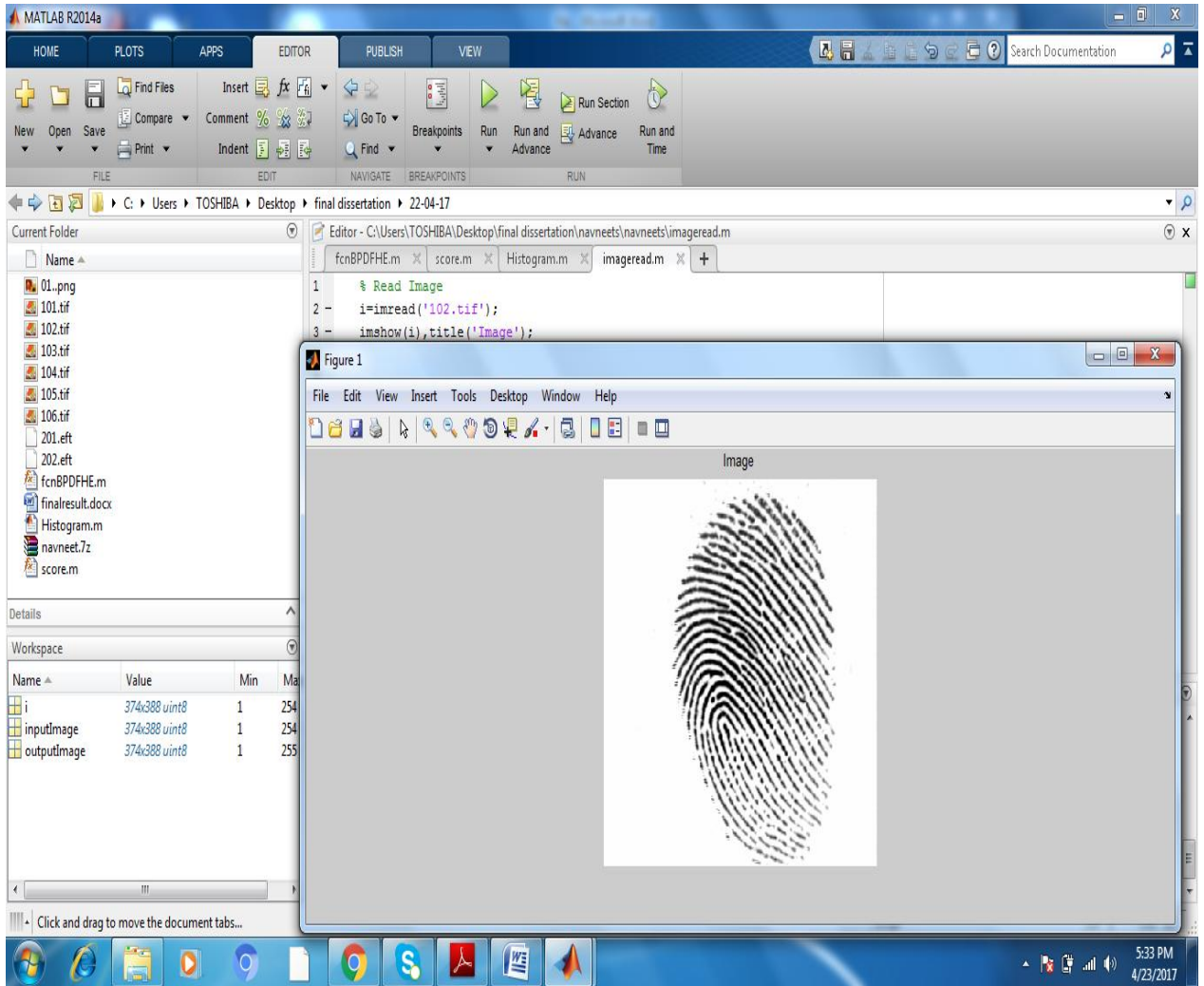


Figure 4.1: -Image read

In the second step the preprocessing will be done using the different methods. In the preprocessing first to enhance the image and binarized that image using different MATLAB function. After these I took brightness image preserving fuzzy equalization to improve contrast enhancement, brightness while reducing computational complexity.

Image Enhancement using histogram

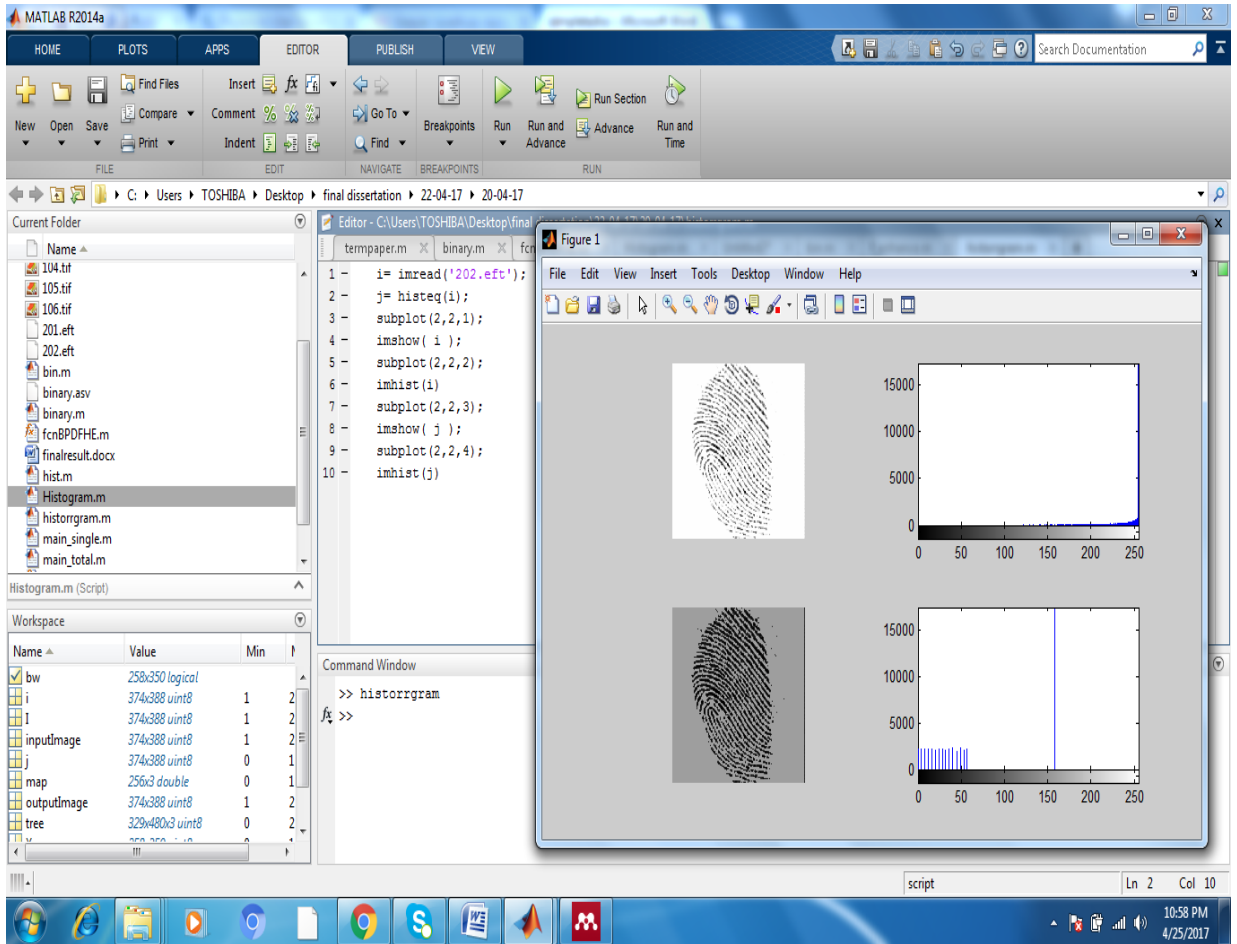


Figure 4.2: - Image Enhancement using Histogram

Image Binarization:- Image binarization means to convert the color image into black and white or in binary form.

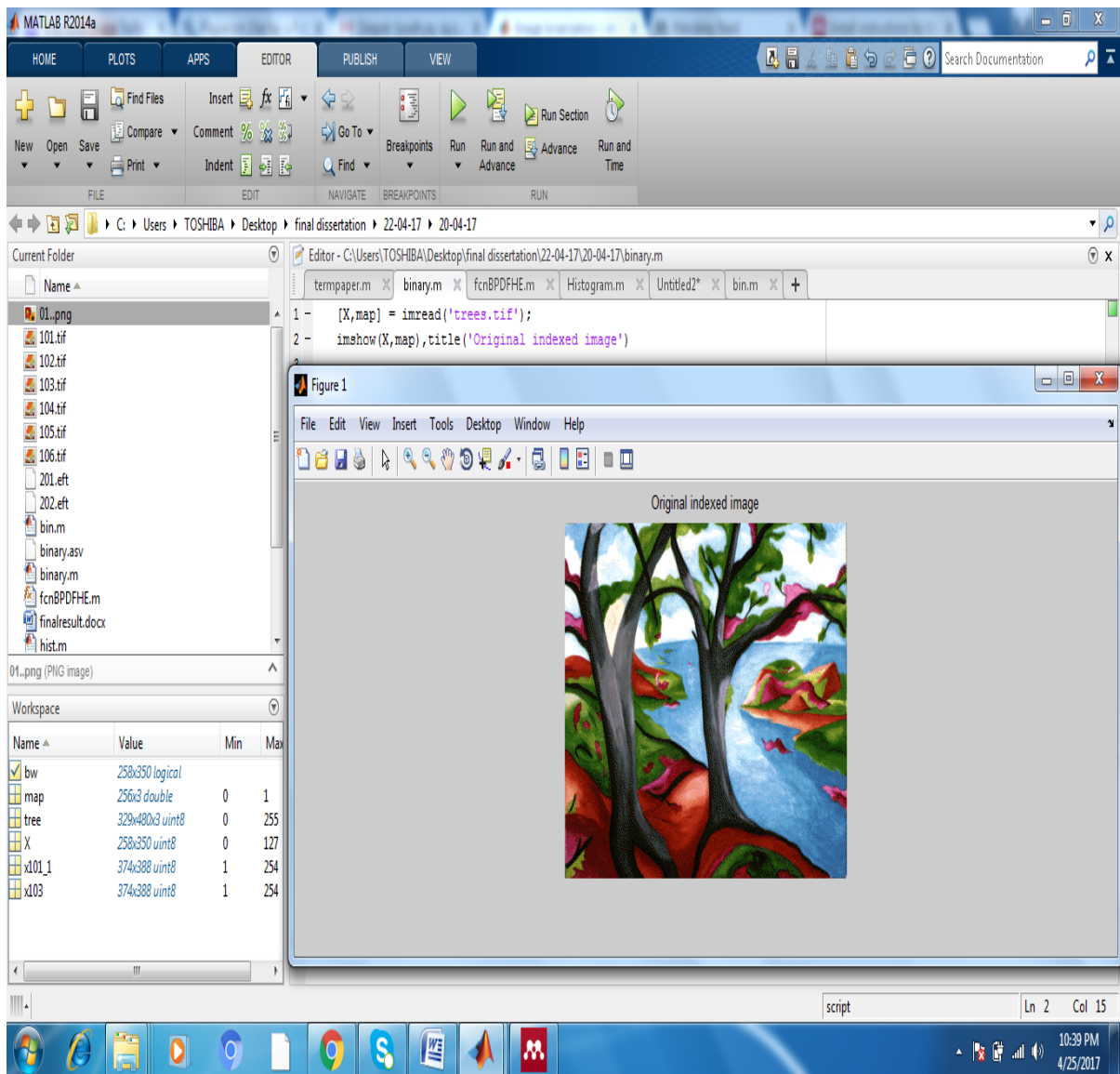


Figure 4.3: - Original Image

Image after conversion:- Figure 4.4 shows binary image

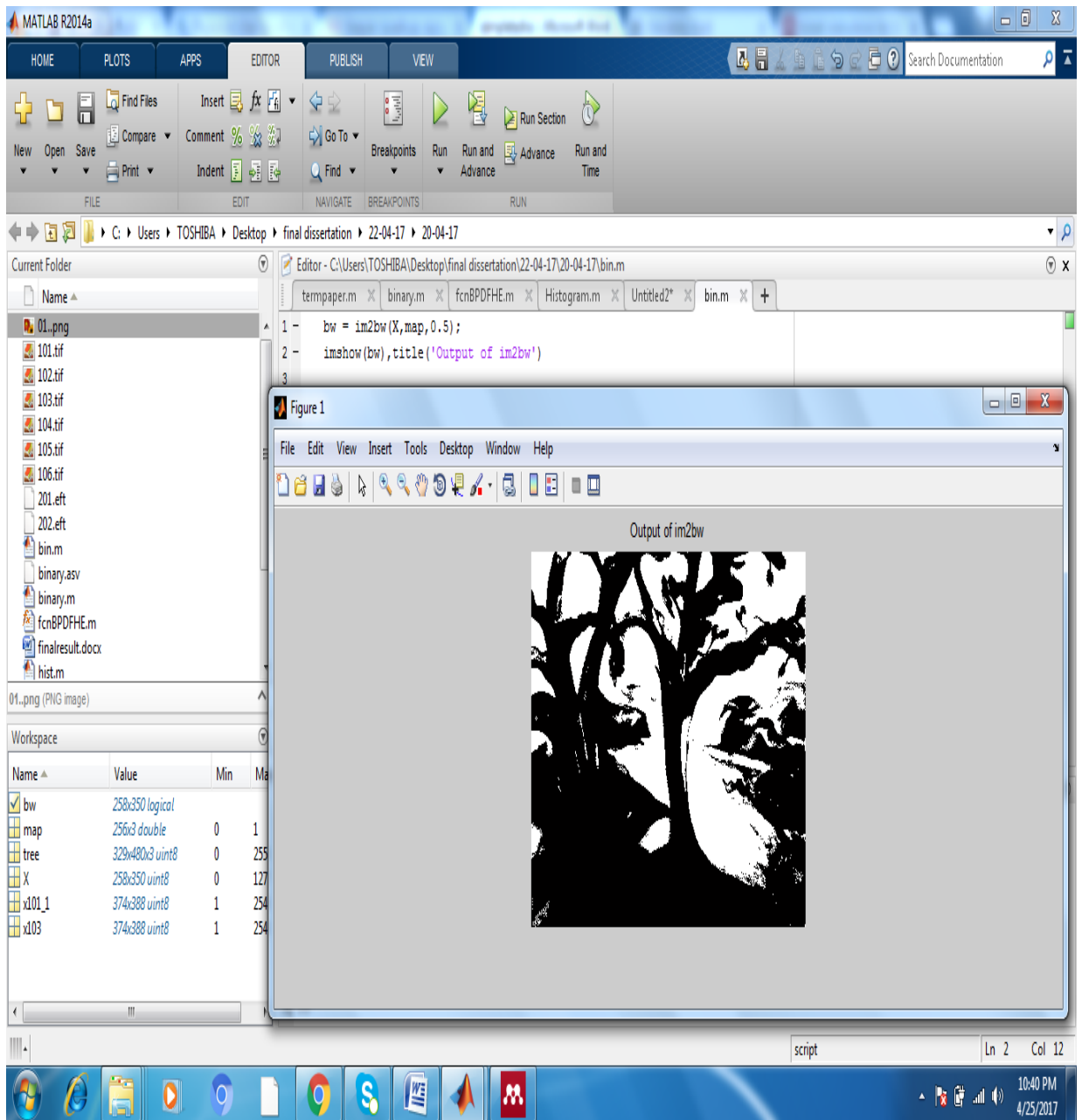


Figure 4.4: - Binarized Image

Brightness Preserving Dynamic Fuzzy Histogram Equalization (BPDFHE) used

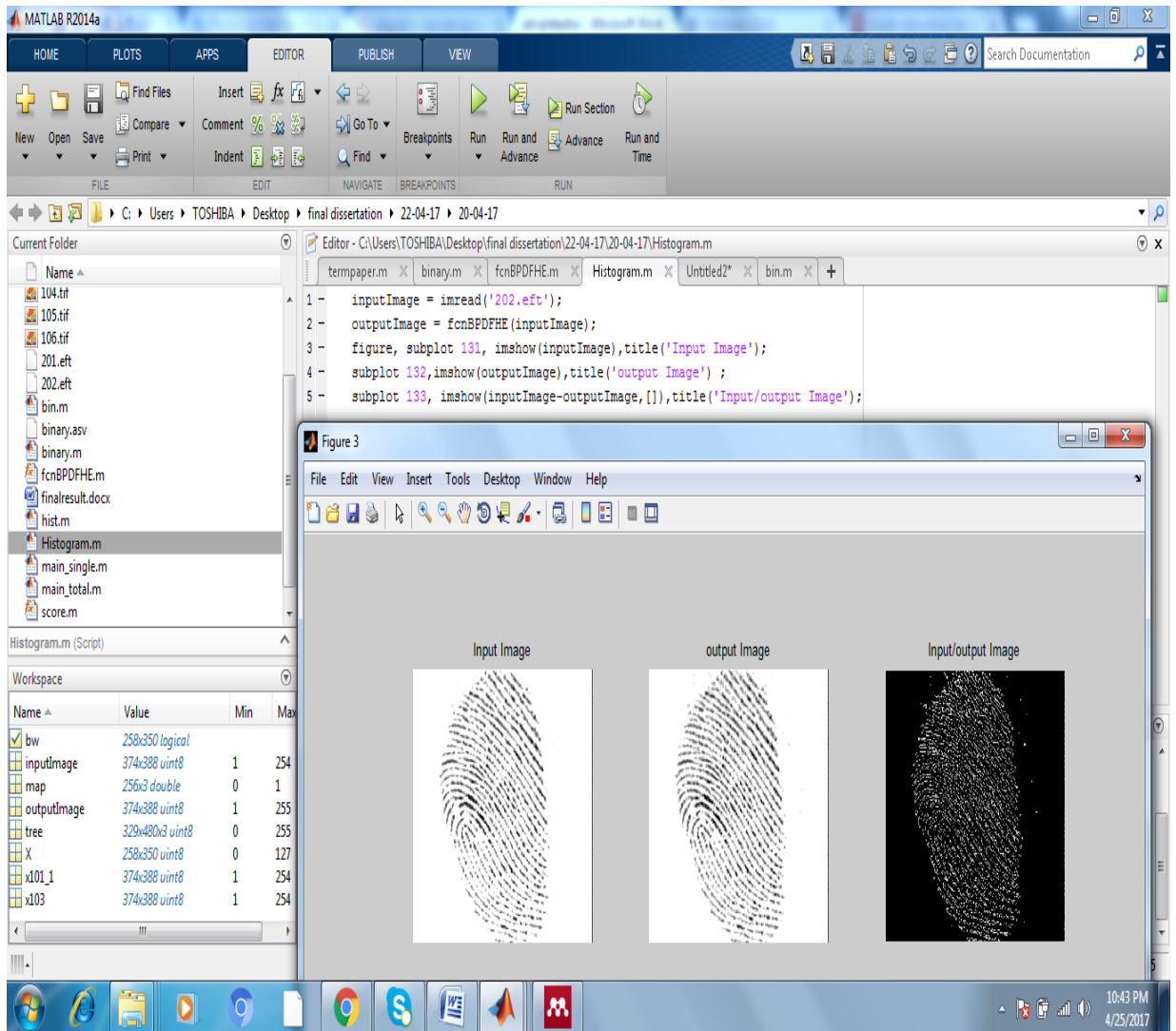


Figure 4.5 :- Input Image, Output Image, Input-Output Image

Figure 4.5 shows the input image and output image and the combination input output image.

Minutia Extraction:- In this step we have to used some MATLAB function to extract the minutia points.

Image Thinning



Figure 4.6: - Thinned Image

Figure 4.6 shows the thinning image using morphological operations

Minutiae Marked:- Minutiae marked means to mark the minutiae points.

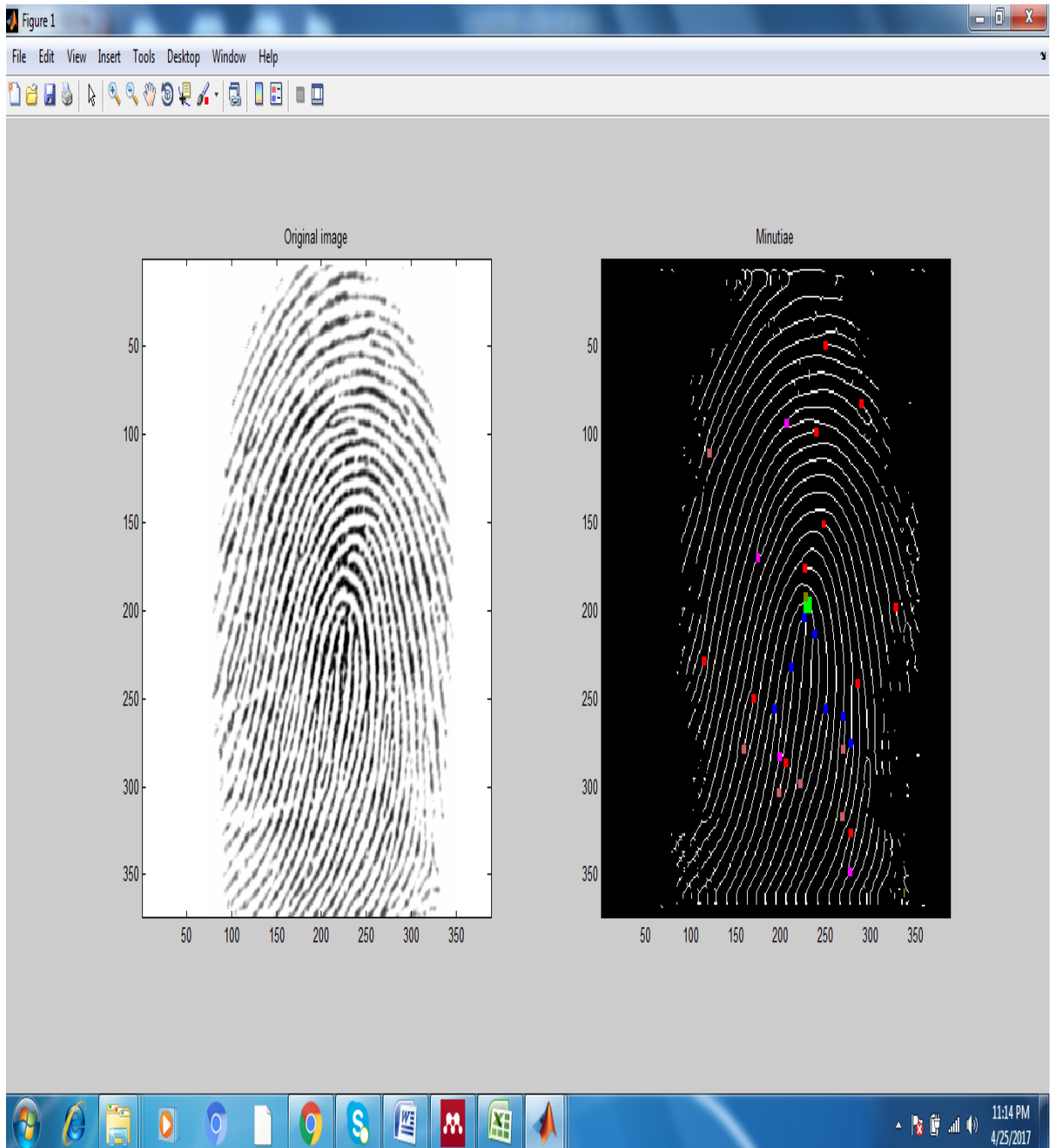


Figure 4.7:- Marked Minutia

Post Processing :- In this step false minutiae removal and match done. This figure 4.8 shows the the input image output image and the similarity score.

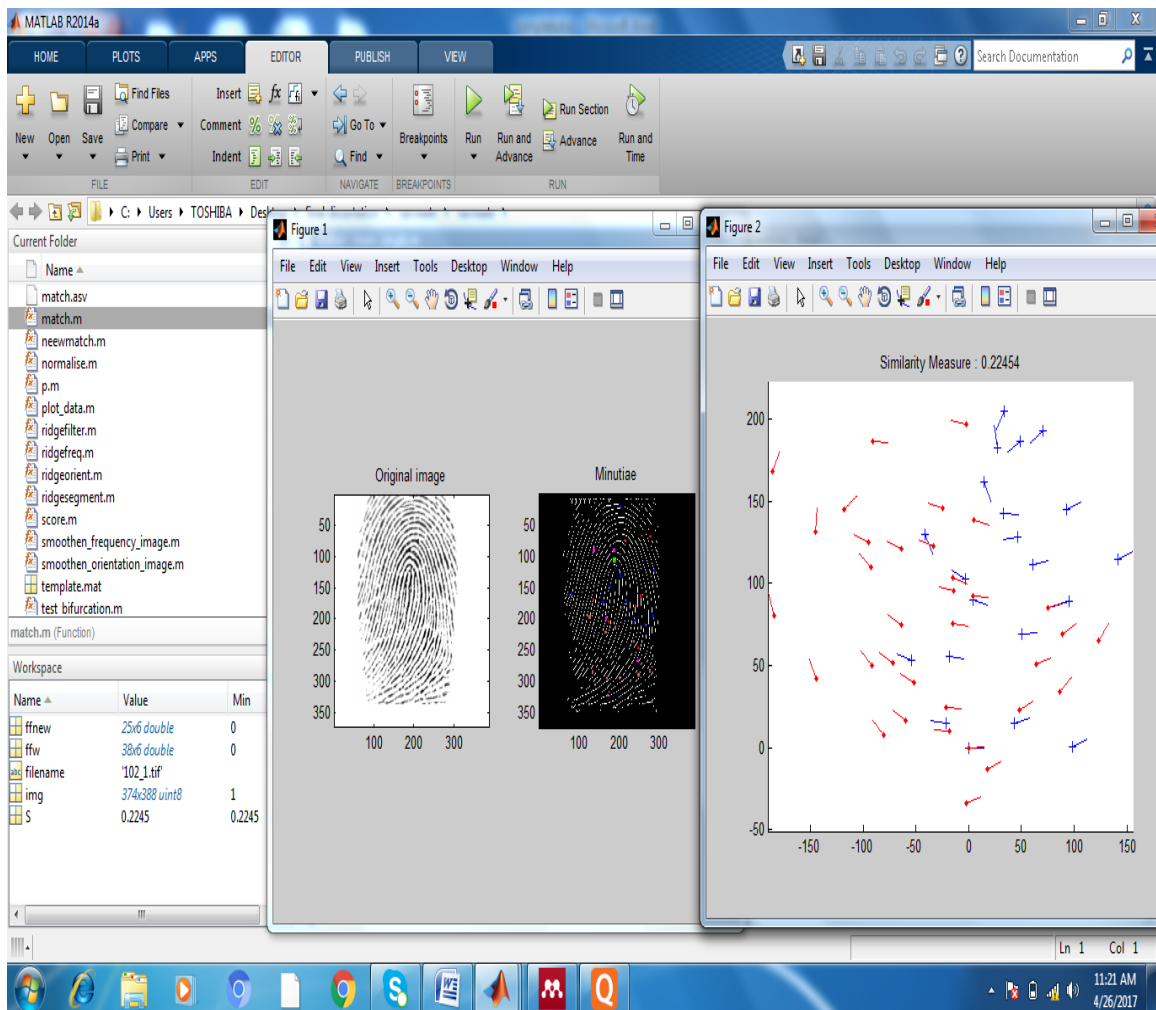


Figure 4.8:-Similarity Measure

In the above figure show the final result of the matching technique. In this there is original image, minutiae image and the similarity score. Similarity score shows the similarity between the original image and its fingerprint impression.

4.2 DISCUSSION

Table 4.1:-Analysis of Similarity Score for the Proposed and Kernel Approach On NIST SD27 And FVC2002

Sr. No	Brightness preserving dynamic fuzzy equalization	Kernel Approach[8]	Increase	% Change
1	1	1	0	0
2	0.78881	0.7883	0.005	0.5
3	0.77067	0.6934	0.07727	7.727
4	0.6932	0.6853	0.00799	0.799
5	0.7233	0.7223	0.001	0.1
6	0.6324	0.5836	0.0488	4.88
7	0.71082	0.6423	0.06852	6.852
8	0.6532	0.6423	0.0109	1.09
9	0.6324	0.6313	0.0011	0.11

The below figure represent the similarity of the latent image using two different approaches in the form of graph:-

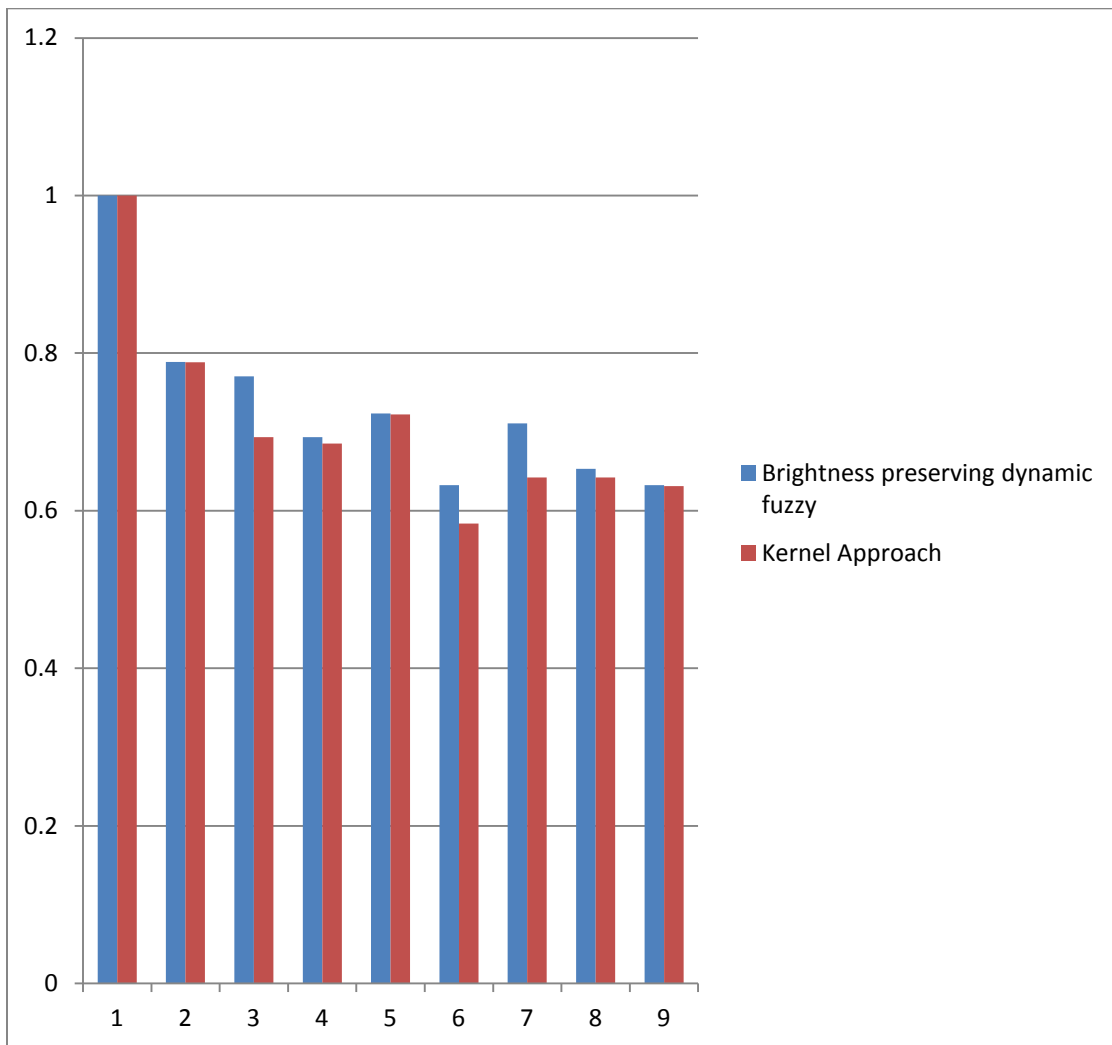


Figure 4.9:-Comparison of similarity score for brightness preserving dynamic fuzzy equalization and kernel approach.

The figure 4.10 shows the error rate of the BPDFHE technique. The error rate reduced when the similarity score improve.

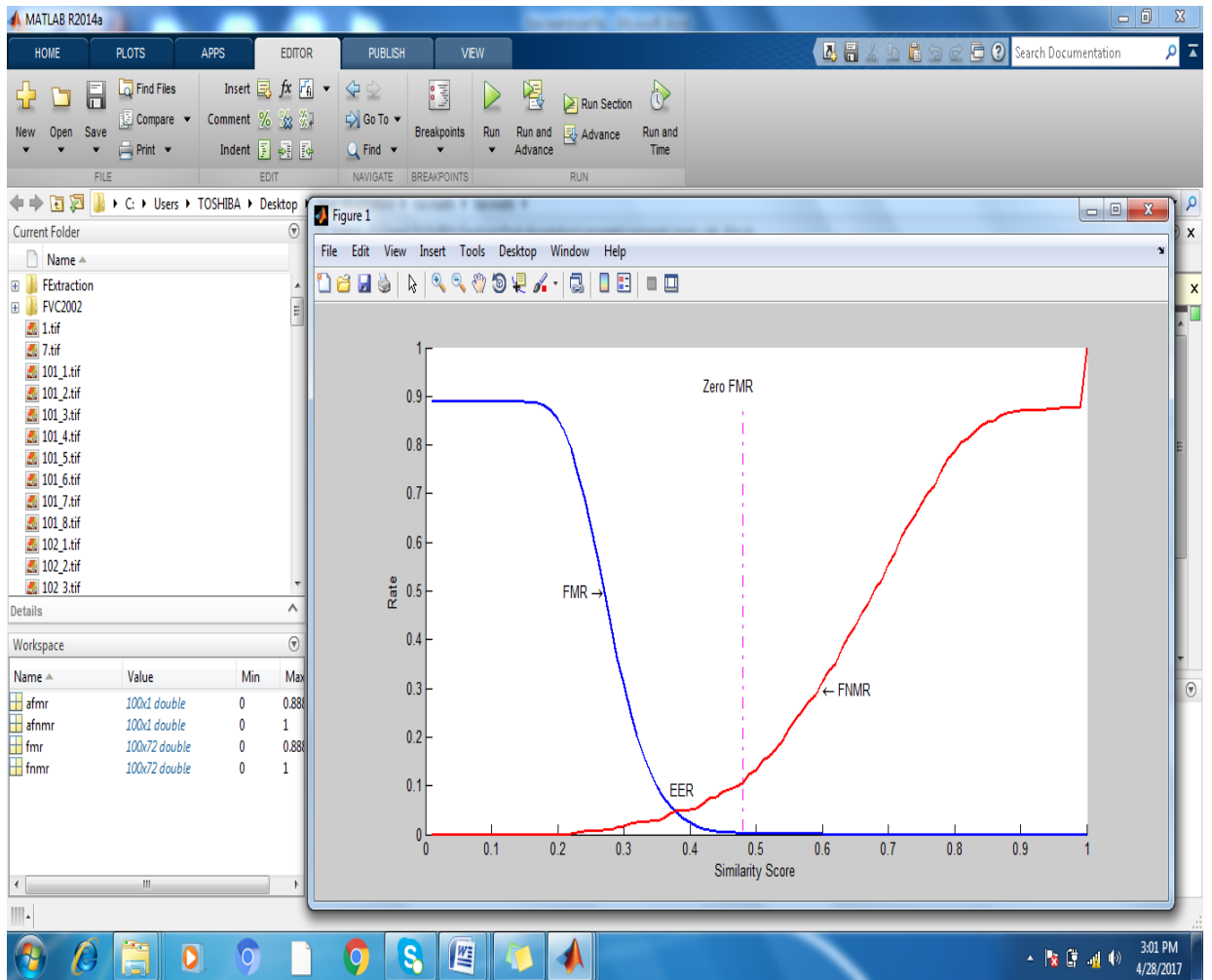


Figure 4.10:- Error rate

CHAPTER 5

CONCLUSION AND FUTURE SCOPE

5.1 CONCLUSION: - This research work strives to improve the similarity score (matching score) of multiple impressions of a finger. The Brightness Preserving Dynamic Fuzzy Histogram Equalization (BPDFHE) is used with the kernel approach to improve the similarity score on latent fingerprints. Histogram is used to enhance the image. Image enhancement in terms of similarity measure reduced the redundancy of the minutiae points. In the other words this technique removes the background noise of the given fingerprint. The result given in section IV proves that the similarity score is improved by using the Brightness Preserving Dynamic Fuzzy Histogram Equalization. As a result, it can be concluded that the similarity is improved by 0.2%.

5.2 FUTURE SCOPE: -The future work can be done on the patent fingerprints and on live images. Testing of the proposed work can be done on different datasets and more challenging surroundings like patent fingerprints and live videos.

REFERENCES

- [1] A. K. Jain, R. Bolle, S. Pankanti, A. A. Ross, and K. Nandakumar, "Introduction to biometrics," *Springer-Verlag Berlin Heidelb.*, pp. 1–20, 2011.
- [2] S. Id, W. Count, and C. E. R. Count, "by Navneet Sandhu," 2016.
- [3] D. Binu and P. Malathi, "Multi model based biometric image retrieval for enhancing security," *Indian J. Sci. Technol.*, vol. 8, no. 35, pp. 1–10, 2015.
- [4] F. Orság and M. Dražanský, "Biometric Security Systems : Fingerprint and Speech Technology Design of Biometric Security System."
- [5] M. M. H. Ali, "Overview of Fingerprint Recognition System," pp. 1334–1338, 2016.
- [6] A. V. V. M. S. P. College, T. Nadu, and P. Arch, "FINGERPRINT CLASSIFICATION BASED ON RECURSIVE NEURAL NETWORK WITH SUPPORT VECTOR MACHINE Contributions : Recursive Neural Networks and support Vector Machines : Related Work :", vol. 6956, no. January, pp. 163–168, 2011.
- [7] R. S. Prasad and S. M. Nejres, "An Efficient Approach for Fingerprint Recognition An Efficient Approach for Fingerprint Recognition," vol. 2, no. April 2015, pp. 3–8, 2016.
- [8] S. Yoon, J. Feng, and A. ~K. Jain, "On latent fingerprint enhancement," *Biometric Technol. Hum. Identif. VII*, vol. 7667, no. c, p. 766707, 2010.
- [9] R. Mathew, B. Thomas, and J. J. Kizhakkethottam, "Review on latent fingerprint matching techniques," *Proc. IEEE Int. Conf. Soft-Computing Netw. Secur. ICSNS 2015*, no. i, pp. 25–28, 2015.
- [10] S. Kumar and R. L. Velusamy, "Kernel approach for similarity measure in latent fingerprint recognition," *Int. Conf. Emerg. Trends Electr. Electron. Sustain. Energy Syst. ICETEESES 2016*, pp. 368–373, 2016.
- [11] K. Manvjeet, S. Mukhwinder, G. Akshay, and S. S. Parvinder, "Fingerprint Verification System using Minutiae Extraction Technique," *World Acad. Sci. Eng. Technol. Int. J. Comput. Electr. Autom. Control Inf. Eng.*, vol. Vol.2, no. No.10, pp. 3405–3410, 2008.
- [12] A. Sankaran, M. Vatsa, and R. Singh, "A Survey on Latent Fingerprint Matching Techniques," *IEEE Access*, vol. 2, pp. 982–1004, 2014.
- [13] P. Parra, "Fingerprint minutiae extraction and matching for identification procedure," *Engineering*.
- [14] A. Lindoso, L. Entrena, J. Liu-Jimenez, and E. San Millan, "Increasing security with correlation-based fingerprint matching," *Proc. - Int. Carnahan Conf. Secur. Technol.*, pp. 37–43, 2007.

- [15] K. Nandakumar and A. K. Jain, "Local Correlation-based Fingerprint Matching," *Indian Conf. Comput. Vision, Graph. Image Process.*, no. December, pp. 503–508, 2004.
- [16] S. Mousmi and T. Meyappan, "Automatic fingerprint Identification Using Minutiae Matching," vol. 4, no. 5, pp. 1407–1413, 2013.
- [17] S. Pawar, "A Survey of Minutiae Extraction from Various Fingerprint Images," vol. 6, no. 6, pp. 169–173, 2016.
- [18] W. Kabir, M. O. Ahmad, and M. N. S. Swamy, "A Novel Normalization Technique for Multimodal Biometric Systems," no. Mm.
- [19] X. Yang, S. Member, J. Feng, J. Zhou, and S. Member, "Localized Dictionaries Based Orientation Field Estimation for Latent Fingerprints," vol. 36, no. 5, pp. 955–969, 2014.
- [20] S. Li, Y. Wang, Q. Zhao, and Y. Zhang, "On the spatial inhomogeneity of fingerprint minutiae: A regression approach," *Proc. 2015 Int. Conf. Biometrics, ICB 2015*, pp. 379–385, 2015.
- [21] B. Tams, P. Mihăilescu, and A. Munk, "Security considerations in minutiae-based fuzzy vaults," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 5, pp. 985–998, 2015.
- [22] D. Binu and P. Malathi, "Multi Model based Biometric Image Retrieval for Enhancing Security," vol. 8, no. December, pp. 1–10, 2015.
- [23] M. Adhiyaman and D. Ezhilmaran, "Fingerprint matching and similarity checking system using minutiae based technique," *ICETECH 2015 - 2015 IEEE Int. Conf. Eng. Technol.*, no. March, pp. 4–7, 2015.
- [24] M. V. Ruiz Blondet, S. Laszlo, and Z. Jin, "Assessment of permanence of non-volitional EEG brainwaves as a biometric," *2015 IEEE Int. Conf. Identity, Secur. Behav. Anal. ISBA 2015*, 2015.
- [25] E. K. Sharma and V. K. Banga, "Biometric Security Issues : A Review," vol. 1, no. 3, pp. 1–8, 2013.
- [26] Y. He, J. Tian, X. Luo, and T. Zhang, "Image enhancement and minutiae matching in fingerprint verification," *Pattern Recognit. Lett.*, vol. 24, no. 9–10, pp. 1349–1360, 2003.
- [27] W. Zafar, T. Ahmad, and M. Hassan, "Minutiae based fingerprint matching techniques," *17th IEEE Int. Multi Top. Conf. Collab. Sustain. Dev. Technol. IEEE INMIC 2014 - Proc.*, pp. 411–416, 2015.
- [28] "Brightness Preserving Dynamic Fuzzy Histogram Equalization" Debdoot Sheet, *Graduate Student Member, IEEE*, Hrushikesh Garud, *Graduate Student Member, IEEE*, Amit Suveer, Manjunatha Mahadevappa, *Member, IEEE*, and Jyotirmoy Chatterjee, *Member, IEEE*

PUBLICATIONS

- [1] N. K. Sandhu and R. Kaur, "Biometric Security Technique: A Review" Indian Journal of Science and Technology, *Vol 9(47)*, DOI:10.17485/ijst/2016/v9i47/106905, December 2016

