Fingerprint Image Recognition Using Bacterial Foraging Optimization Algorithm (BFOA)

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Information Security

Submitted By
Harpreet Singh Brar
(Roll No. 801233005)

Under the supervision of:
Dr. V.P. Singh
Assistant Professor

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR UNIVERSITY
PATIALA – 147004
July 2014

Certificate

I hereby certify that the work which is being presented in the thesis entitled, **"Fingerprint Image Recognition Using Bacterial Foraging Optimization Algorithm(BFOA)"**, in partial fulfillment of the requirements for the award of degree of Master of Engineering in **Information Security** submitted in Computer Science and Engineering Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of **Dr. V.P. Singh** and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

(Harpreet Singh Brar)

Roll No. 801233005

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

(Dr. V.P. Singh)
Assistant Professor
Thapar University
Patiala

Countersigned by

(Dr. Deepak Garg)
Head
Computer Science and Engineering Department
Thapar University

(Dr. S. K. Mohapatra)
Dean (Academic Affairs)
Thapar University
Patiala

Acknowlwdgement

The successful completion of any task would be incomplete without acknowledging the people who made it possible and whose constant guidance and encouragement secured the success.

First of all I wish to acknowledge the benevolence of omnipotent God who gave me strength and courage to overcome all obstacles and showed me the silver lining in the dark clouds. With the profound sense of gratitude and heartiest regard, I express my sincere feelings of indebtedness to my guide **Dr. V.P. Singh**, Assistant Professor, Computer Science and Engineering Department, Thapar University for her positive attitude, excellent guidance, constant encouragement, keen interest, invaluable co-operation, generous attitude and above all her blessings. He has been a source of inspiration for me.

I am grateful to **Dr. Deepak Garg**, Head of Department and **Dr. Maninder Singh** Associate professor, Computer Science and Engineering Department, Thapar University for the motivation and inspiration for the completion of this thesis.

I will be failing in my duty if I do not express my gratitude to **Dr. S. K. Mohapatra**, Senior Professor and Dean of Academics Affairs in the University, for making provisions of infrastructure such as library facilities, computer labs equipped with internet facility, immensely useful for the learners to equip themselves with latest in the field.

Last but not the least I would like to express my heartfelt thanks to my Parents and my friends **Herman, Baljeet, Onkar, Ankit, Rohit** who with their thought provoking views, veracity and whole hearted co-operation helped me in doing this thesis.

(**Harpreet Singh Brar**)
Roll No. 801233005

Abstract

Finger Print authentication system is one of the most common and often used bio metric analysis through which several organizations register the presence of their workers and employees. There are also some organizations in which verification of user is so critical that unauthorized access may harm the organization to a great level. It has been often seen that the matching procedure is difficult if the finger is tried with the some rotation angle or if the finger print has a little era of margin. Suppose a user whose data has been stored in the database gets a cut over his finger, a normal matching procedure would deny the access of the user till his finger is not perfectly cure and the matching scenario does not get a perfect scanned Centre. This might cause a problem for the organization or the organization might have to take external help to get the user verified through the system.

This work presents a unique verification system which is called finger print biometric authentication using Bacterial Foraging Optimization and the results of authentication has been compared with previously implemented algorithm Support Vector Machine (SVM). Bacterial Foraging Optimization (BFO) is artificial intelligence based optimization algorithm and helps in the selection of relevant features after feature selection so that matching will done with high accuracy rate. The mechanism has been tried with different set of rotation and matching score at the end the accuracy has been computed as 93% on an average with Bacterial Foraging Optimization (BFO) whereas the accuracy for Support Vector Machine (SVM) lies in 70 to 80%. Mat lab 7.11.0 version is used for implementation and moreover it is being used to compare the results.

Table of Contents

List of Figures

List of Tables

`

Chapter 1

Introduction

1.1 Authentication

Authentication is required when it is necessary to know if a person is who they claim to be. It is a procedure that involves a person making a claim about their identity, and then providing evidence to prove it. This study focuses on the initial authentication procedure that most computer users are accustomed to performing when they log onto a computer system. The initial authentication procedure is considered to be the first line of protection for computer systems. It therefore stands to reason that this procedure should be made as accurate and reliable as feasibly possible.

Authentication is an access control mechanism that is based on user identity. It comprises two processes:

- Identification: the naming or labelling of an identity, providing the means to distinguish that identity from among a set of similar identities. For example on a computer system, legitimate users are given a unique username by which the system differentiates them from other legitimate users of the system.
- Verification: the process of confirming the veracity of a claimed identity. For example on a computer system, a unique verification token (with direct correspondence to each username) is intended to verify the identity of a legitimate user. The verification process entails comparison of a stored or registered token, for a legitimate user, with a query token provided by the claimant during the authentication procedure.

1.2 Introduction to Biometrics

Biometrics refers a technology to authenticate individuals by automated means that rely on anatomical or behavioral human characteristics. Biometric systems have the potential to authenticate users with a high degree of assurance.

1.2.1 Characteristics of Biometrics

Any physical and/or behaviour characteristics of a human can be considered as a biometric different types of biometric recognition are shown below in figure 1.1 if it exhibits following characteristics:

- **Universality:** Each person accessing the biometric application should posses a valid biometric trait.
- **Uniqueness:** The given biometric trait should exhibits distinct features across individuals comprising the population.
- **Permanence:** The biometric characteristics should remain sufficient invariant over a period of time.

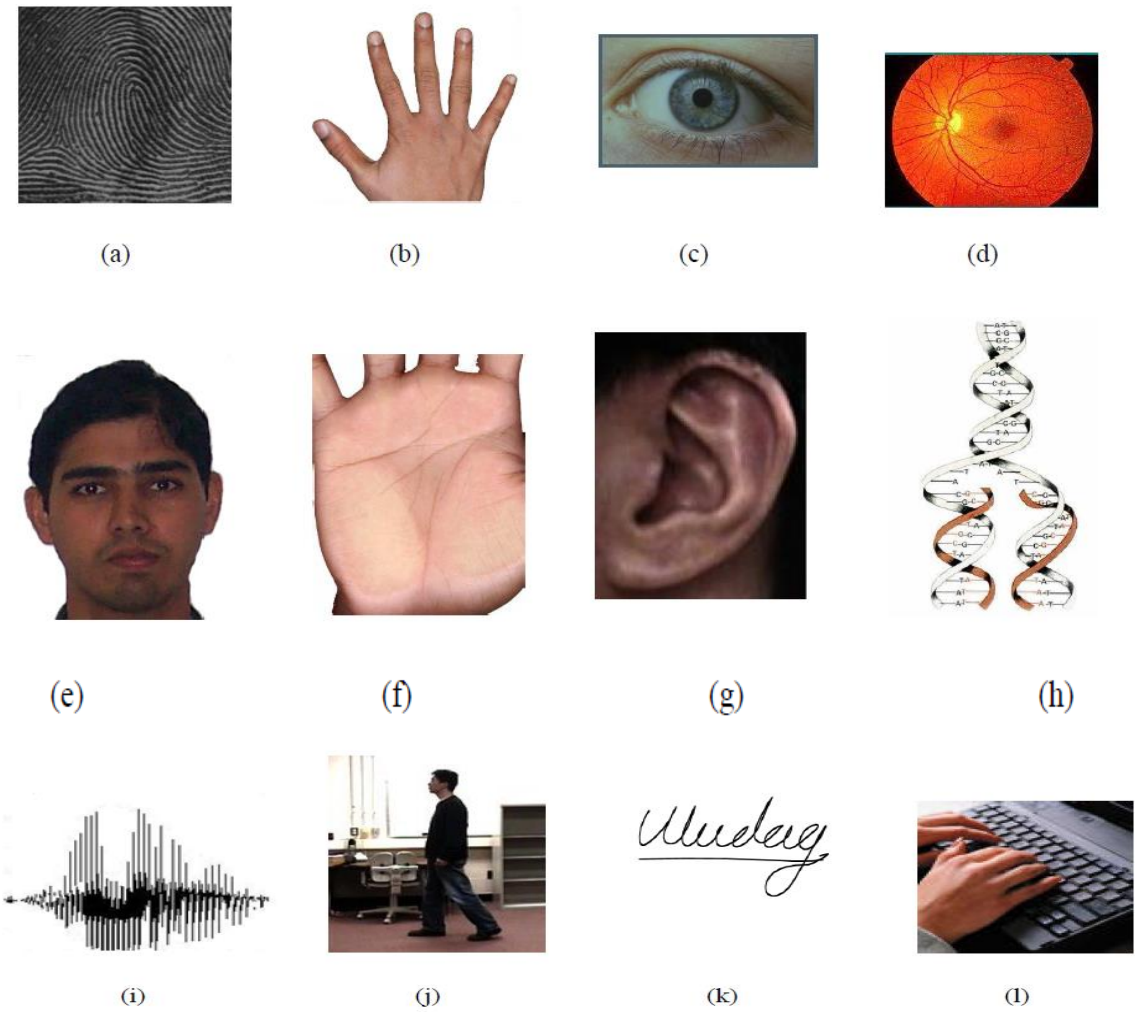


Figure 1.1 Different types of Biometric Recognition

- **Measurability:** The biometric characteristics can be quantitatively measured i.e. acquiring and processing of biometric trait should not cause inconvenience to the individual.
- **Performance:** The biometric trait should the required accuracy imposed by the application.
- **Acceptability:** The chosen biometric trait must be accepted by a target population that will utilize the application.
- **Circumvention:** This indicates how easily the chosen biometric trait can fooled using artefacts.

1.2.2 Advantages of Biometric

Biometrics eliminates fraud, enhances security, cannot be easily transferred, forgotten, lost or copied.

1.3 Application Fields for Biometrics Technology

Physical Access Control: - have an identity authentication process in which users are required to give physical characteristics. It's been used in locations like hospitals, military and police station. The access devices which are installed in computer or doors is one of the application of physical access control commonly used. It is an important and confidential application and is ensured with high level security. Human problems have been reduced by the physical access control. It also ensures to overcome the data loss in system. With the use of this system one can remove the process of finding complex and long codes with some different processes. It is not just efficient and effective but also secure profitable and safe in workplace.

Logical Access Control: - It is a process of scheme control over computer programs or data files. It contains information i.e. personal or private for many different users. It is been used by government and militaries to save their essential data by using a high security system i.e. biometric technology. The logical access controls is basically used for system access controls and computer networks which is the only difference between physical access control and logical access control. With this there is no need of a complex and long

passwords for users. For maintaining the private data in system it is one of the most effective and secure way. And it also gives an advantage by saving money and time.

1.4 Fingerprint Verification

1.4.1 What is a Fingerprint?

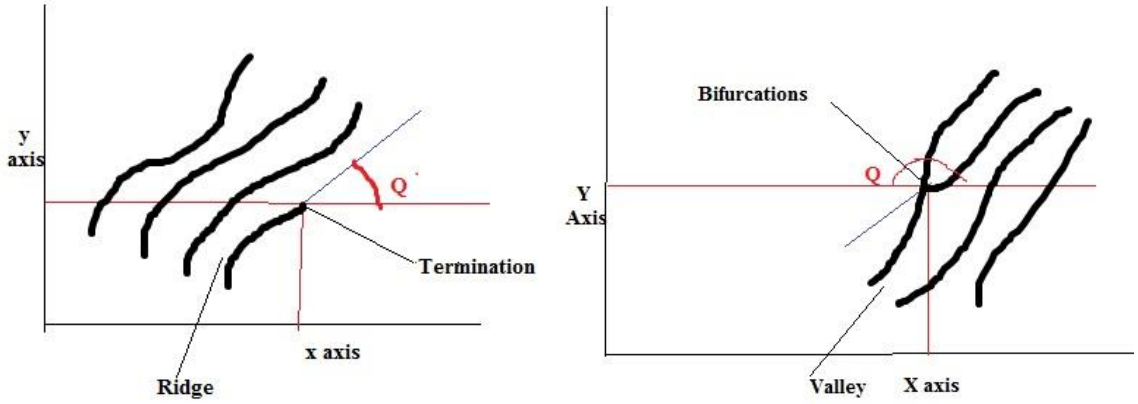
Feature pattern of one finger is known as fingerprint as shown in figure 1.2. There is no doubt in this that each fingerprint is unique. Every person has their own fingerprint with a complete uniqueness. So it is used in forensic investigation and for identification for quite some time now.

Figure 1.2: Fingerprint Image acquired by an Optical Sensor

The word biometrics is derived from the Greek words bios (meaning life) and metron (meaning measurement), biometric identifiers are measurements from living human body. [3]Anatomical and behavioral characters form all biometric identifiers, but these identifiers should not be placed into either behavioral or anatomical characteristics. For instance use of input devices is based on behavior of person but finger prints are anatomical. So, the input to this engine is a mixture of behavioral and anatomical characteristics

Fingerprints are the patterns formed on the epidermis of the fingertip. Fingerprints consists of series of ridges and valleys (known as furrows) appears on of the fingertip and have core around which pattern like swirls, loops or arches are curved to ensure that each print is unique [3**].**

Fingerprints consist of valleys and ridges. Fingers upper skin segment is Ridge and the lower segment Valley. Ridges further consist of: ridge endings and ridge bifurcations which are known as Minutiae points. In the former ridges end, in latter it divides into two. Different ridges furrows, minutiae points forms various combinations of finger-points are shown in figure 1.3. Fingerprints are made up five patterns: 1% -accidental whorls, 5% - arches like plain and tented, 34% - whorls, 60% - left and right loop.



(a) **(b)**

Figure 1.3: (a) Terminations and Ridges (b) Bifurcations and Valleys

Fingerprints can be detected by two algorithms: Pattern Matching and Minutiae Matching.

- Pattern Matching– instead of particular point, it covers entire area. It focuses more on density, thickness and curvature of figure. Figure image consist of areas with unusual ridge combination, around minutiae point or areas with low radius curvature.
- Minutiae Matching – it identifies the difference between fingerprints of one to others with the help of details from extract minutiae. When one uses the system they record direction and location of minutiae on figure surface, and when they use this system for recognition of finger prints, then the system compares the image provided at the time of access to minutiae image which comes up.

1.4.2 What is Fingerprint Recognition?

Problem of fingerprint recognition can be classified into two parts: one is fingerprint identification and other is fingerprint verification as shown in figure 1.4 .And also there is a different approach by experts for fingerprint identification, it is known as Automatic Fingerprint Recognition System (AFRS).

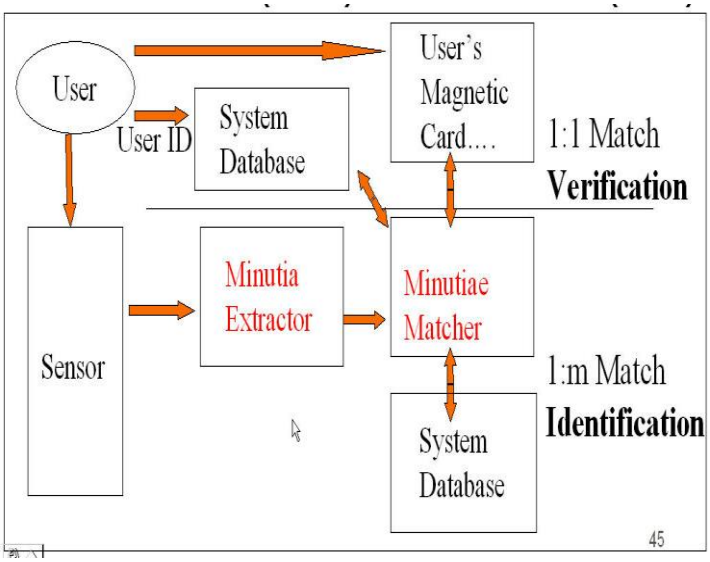


Figure 1.4: Verification vs. Identification

Fingerprint verification is to check person's authenticity by using his fingerprints. Along with identity information such as ID number user also gives his fingerprints. The fingerprint verification system gets the fingerprint for the user from his ID number and matches it with the present provided fingerprint by the user. It is basically the principle design of AFAS.

Fingerprint identification is basically to identify someone by using his fingerprint(s). If person's identity is unknown then fingerprint identification system checks the whole database and tries to find a match with the provided fingerprint by the user. This type of technique is really helpful in investigating criminal cases and it is based on AFIS design principle.

Still all the problem of fingerprint recognition either identification or verification basically based on properly defined representation of a fingerprint. Until and unless the

representation of fingerprints is simple and unique, the matching of fingerprint whether 1to1 or 1to m verification or identification case it is pretty simple and straightforward.

In below table 1 all factors are mention which effects the quality of fingerprint image. These factors do effect the accuracy in matching fingerprints

Table 1 Factors affecting the Quality of Fingerprint Image

Factors	Impact on Database
Manual work	Medium
Weather(dry or wet) conditions	Low
Placement(angle) of finger on senor	High
Dirty or oily fingers	Medium
Injury to fingers (cuts or bruises)	High

1.5 Objectives

This work encompasses a set of objectives that is connected with a set of objectives that is associated with target of this process. The objectives are mentioned below.

- To implement the Bacterial foraging optimization algorithm (BFO)classification method for the matching of finger print mechanism system evaluation
- To implement Support Vector Machine(SVM) for the for the matching of finger print mechanism system evaluation
- To test the accuracy of both discussed algorithm with rotated angles (triangle values)
- To compare the classification accuracy of SVM and BFO.

1.6 Significance of the Study

This learning is conceded out with the foremost objectives of fingerprint matching based on the results obtained, it is hoped that this is capable of achieve the following:

- To give disclosure on an additional capable technique of fingerprint matching that could suggest better results or at least identical performance at the existing techniques.
- To resolve the difficulty of fingerprint matching in areas of security regarding.

1.7 Thesis Outline

This report will mainly be divided into seven chapters.

First Chapter is an introduction and brief overview of the thesis including the objectives, scope of thesis, significance of the study and outline.

Second Chapter will discuss about the literature survey of finger recognition and classifier which used. Firstly we should survey about the basic of finger recognition like where basic need of finger recognition, which type of classifier we can apply and what already work done on finger recognition and classifier. The basic classifier is BFO.

Third Chapter will contain the problem statement i.e. what is the basis and need of this work research.

Fourth Chapter will describe the summary in detail of those classifiers which we will use for the implementation and next part of this chapter is about the proposed methodology that we follow to achieve our results.

In **Fifth Chapter** the snapshot will be shown that gives the step by step procedure to run the classifier and how to result. How image is represented in MATLAB platform and how it works. The results generated with classifier will identify better performance in comparison of existing technique.

Sixth Chapter includes the conclusion and future scope of the thesis.

Seventh Chapter will include references.

Chapter 2

Literature Review

Lie Wei [1] proposed a technique in which delta field Poincare index and a speedy arrangement algorithm is worn to categorize the fingerprint in to five classes on foundation of singularities. To get singularities a route of well-built alteration is used for probing by detection algorithm. Accuracy is enhanced when singularities perceived.

Hartwig Fronthaler, ***et al.*** **[2]** projected a process to perk up the matching performance and resourcefully computation in fingerprint recognition. In support of this operation directional filtering and image scale pyramid in spatial domain is done.

M. R. Girgisa, *et al*. [3] projected a fusion approach which used in facilitate of fingerprint matc+

hing on basis of line extraction and graph matching standard. Two phased existed one is genetic algorithm phase and other is a local search phase. Sturdiness of algorithm is established by results of implementation.

DuoqianMaio, *et al*. [4] proposed an auto fingerprint identification system which is based on foremost graph algorithm by keg that provides principal curves. As a result there were some minutiae point in fingerprint image; these points are extracted using an algorithm. He concluded that curves is generated by this proposed approach is extremely smoother as compared to thinning algorithm.

LupingJi and Zhang Yi [5] approximate a four direction oriented field method that completes its whole its procedure in subsequent four steps, i) pre-processing step is carried out first for image of fingerprint, ii) neuron pulse coupled neural network is worn to conclude primary ridge of fingerprint, iii) block direction is estimated by projective distance variance of a ridge, as an alternative of a full block, iv) in the ending step orientation field that is estimated initialized to correct process.

G. Sambasiva Rao, *et al*. [6] proposed a gray level watershed system for fingerprint recognition. It scanned fingerprints and locate out the ridges nearby on a fingerprint image.

JinweiGu, *et al*. [7] a fingerprint verification technique is anticipated that is based on purpose of minutiae and orientation field. Robust discriminatory information is provided by this that is other than minutiae points. Conclusion of matcher on orientation field and minutiae are combined to equivalent the Fingerprint.

V. VijayaKumari and N. Suriyanarayanan [8] proposed a manner which calculates performance in fingerprint by finding the edges of fingerprint images by five local operators i.e. LoG, Prewitt, Roberts, Sobel and Canny. Individual segments from image are take out from the edge detected image.

Raju Sonavane and B.S. Sawant [9] presented a technique for development in fingerprint by using a special domain in which the fingerprint image is decomposed into a class of filtered images following that we estimated orientation field. We need a mask for superiority purpose that differentiates among corrupted regions in the input image are generated. By means of the estimated orientation field, enhancement in fingerprint image is adaptively finished in the recoverable regions.

Eric P. Kukula, *et al*. [10] proposed a work on the examination of that five force levels that influence the performance, excellence of image and minutiae calculate between optical and capacitance fingerprint sensors. He chose three images from 75 participants that are indexed in sensing technology. Kruskal-Wallis conducted a test of nonparametric which found differences in counts of minutiae and quality scores of image based on the force level. The results concluded that there was no difference in minutiae count of images but the eminence of images has a great deal difference based on the force levels of the capacitance sensor. There were numerous factors that affect image quality score by force and sensor type, so far the subtraction of low quality images does not recover the system performance at every force level.

ManaTarjoman and ShaghayeghZarei [11] proposed a method that structural in type for fingerprint classifications. This method is using a directional image of fingerprint as an

alternative of singularities. Foremost directions of ridge lines are included in directional image.

SharathPankanti, *et al.* [12] proposed a practice for matching and demonstrating fingerprint is recognized as Scale Invariant Feature Transformation (SIFT). Amalgam approaches with combination of both SIFT and conventional minutiae are providing superior results than existing individual schemes.

BhupeshGour, *et al.* [13] have developed a scheme in which midpoint ridge curve depiction is used for extraction of minutiae in fingerprint images. At initialization of process segmentation process is performed one by one for foreground from background of fingerprint image. Size of area is 64x64 that is extracted from fingerprint image. 64 x 64 normalized windows are used in normalization distinction of the ridges for improved of filtering by appropriately tuned Gabor filter. Scanning of image is performed from left to right and top to bottom and transitions from white (background) to black (foreground) are detected. Calculation is done for curve length vector in all eight directions. Every element of contour is represented as a pixel on the contour, the x, y coordinates enclose field for pixel.

Haiping Lu, *et al.* [14] proposed an algorithm that is so effectual and proficient that improves the on the whole performance of fingerprint identification system that is automatic because it is very important to preserve true minutiae while removing imitation minutiae in post-processing. A large amount effort are used in projected novel fingerprint image post-processing algorithm to reliably differentiate between true ones and false one in minutiae by making use of ridge number information.

Ballan M [15] on the basis of singular point fingerprint smoothing, classification and identification are used for processing of a Directional Fingerprint. Fingerprint histogram that is directional by nature provides this. Lasso and Wirbel are considered as main categories of fingerprints. For finding the results some processes followed like formation of directional image with block representation, singular point detection and decision. Due to this method the errors for matching decision vectors are minimums, and method is simple and fast.

Prabhakar S, *et al*., [16] has developed a technique for fingerprint identification that is based on filter. Both characteristics local as well as global used for identification. Number of directions is available through which fingerprint image is filtered and a 640-dimensinal feature vector is extracted in the central region of the fingerprint. Only 640 bytes is required for compact feature vector. The amount of difference in distance between input finger code and template finger code for matching can be calculated by Euclidian distance formula. It is a very interesting approach. Lots of math work was involved in his study which was very useful in field of biometrics

Manvjeet Kaur, *et al*., [17] have proposed an approach that is used for the minutia extractor and a minutia matcher. False minutiae and improvement in thinning is done by Morphological operations with segmentation.

Alessandra Lumini and Loris Nanni [18] proposed a scheme of fingerprint that is based on minutiae based fingerprint and main problem of fingerprint is two - class pattern recognition. Support Vector Machine classifier is used for obtaining the minutiae matching. That matching is separated into authentic or pretender. That provided effect for performance upgrading.

Xifeng Tong, *et al*., [19] provided a resolution of trouble that is non-linear deformation using Local Relative Error Descriptor (LRLED). For achievement this process he conceded through three steps i) fingerprint alignment achieved by a pair wise arrangement method ii) to trim down non-matches a pair set is obtained with threshold value iii) the LRLED – based resemblance measure. Equivalent and different minutiae-pairs were differentiating by LRLED and works fine for fingerprint minutiae matching.

Mohamed, *et al*. [20] used FNN (Fuzzy Neural Network) to signify fingerprint recognition method. Some features of fingerprint like points of extraordinary positions and core direction and delta acquired from a binary form of fingerprint image. This effort gives most excellent results.

L. Lam, *et al.* [21] presented a method, a single pixel width beating can be generated by using thinning process that process is required to decrease the thickness of every line of patterns to just a single pixel width. Several basic need should be rewarded by a good with

respect to a fingerprint are i) there should be no discontinuities in single pixel width when image of fingerprint is thinned. ii) Each ridge should be thinned to its vital pixel. iii) Every singular pixel and noise should be eradicated. iv) After the whole process there should be no pixels offered that require all over again thinning process.

Ching-Tang Hsieh and Chia-Shing – Hu [22] proposed technique for Fingerprint recognition. At position of minutiae they wore ridge bifurcation and this algorithm leave out noise from image which is their planned work. The grades confirm that fingerprint recognition for humanoid is vigorous, reliable and brisk.

Asker M. Bazen, *et al.* [23] proposed a correlation-based fingerprint verification system. In this paper correlation based technique is used for verification of fingerprints. This correlation technique makes it different from traditional minutiae-based systems. The correlation-based fingerprint verification system first selects appropriate templates in the primary fingerprint, then it uses template matching to locate all of them in the secondary print, and then compares it with the template positions of both fingerprints.

David G. Lowe [24] presented an approach to distinctive image features from scale-invariant key points. This paper presents a method for extracting distinctive invariant features from images that can be used to perform reliable matching between different views of an object or scene.

Shunshan li, *et al.* [25] proposed the Image Enhancement Method for Fingerprint Recognition System. In this paper fingerprint image enhancement method, a refined Gabor filter, is presented which is very useful. This enhancement method do connect the ridge breaks, and it ensures the maximal gray values located at the ridge center and has the ability to compensate for the nonlinear deformations. It includes ridge orientation estimation, a Gabor filter processing and a refined Gabor filter processing. This algorithm also has the ability to compensate for the nonlinear deformations

Chapter 3

Problem Statement

3.1 Problem Formulation

A reliable identity management is a critical component in several applications that provide services to only legitimately enrolled users. Some of applications include physical access control to secure facility, access to computer networks, performing remote financial transactions etc. The primary task of identity management system is determination of individual's identity. The traditional method of establishing a person's identity include knowledge based like password or token based like ID cards, but these representations of the identity can easily be lost, stolen or shared. These methods are not sufficient for identity verification. In today's world with intermeshed societies developing identity is very important for a person. Queries like, "Is he in the governments watch list "or "Is he really who tell he is" are usually being put up in various situations for example while entering a country or getting a driver's license etc.

In this era of modern networking, communication, mobility and with the concerns of security user identification techniques are in very much demand**.** Biometrics refers a technology to authenticate individuals by automated means that rely on anatomical or behavioral human characteristics. Biometric systems have the potential to do the people authentication with a high degree of accuracy. Various aspects of human physiology, chemistry and human behaviors can be used in biometrics Perhaps all biometric identifiers are a combination of anatomical and behavioral characteristics and they should not be exclusively classified into either anatomical or behavioral characteristics. For example, fingerprints are anatomical in nature which means they do differ from person to person but the usage of the input device depends on the person's behavior. Thus, the input to the recognition engine is a combination of anatomical and behavioral characteristics.

3.2 Problem Statement

To develop an algorithm that can accurately recognize the fingerprints and then matching of fingerprints is done effectively. As Fingerprints consist of 80 minutiae, so it is very difficult to match the minutiae of one finger with other. There are many reasons which make the fingerprint matching a complex task like rotation angle of fingerprint, pressure applied on fingers, wet/dryness of fingers etc. These various reason are mentioned in table 1.1 .Matching of fingerprints is based on two assumptions 1. Fingerprints are unique and no two persons can have the same fingerprints 2. Background of fingerprints is free from all types of noise. To compare, the developed algorithm effectiveness with the existing algorithm. Then finally compare the performance of both the algorithms in term of two metrics FMR, FNMR.

FMR (false matching rate) = False matches / enrolled attempts

FNMR (false non-matching rate) = False non-matches / enrolled attempts

The current problem statement also involves the implementation of Bacterial Foraging optimization method for the classification of the finger print mechanism and comparison of BFO method with SVM classifier.

Chapter 4

Present Work

Recent studies have showed that most of the clients are using the biometrics technology for security concerns. Biometric technology is emerging rapidly as it reliable, easy to operate, robust, secure as well as free from memorize the passwords and pins as it is needed in earlier systems. There are different biometric technologies like ear, face recognition, fingerprints, finger geometry, iris recognition, retinal sketching, voice recognition, signature verification on the basis of which recognition of an individual is done. But our focus will be on the fingerprint biometrics only involving minutiae feature extraction method.

4.1 Basic Block Design

A biometric system constitutes of fingerprints image sample acquiring device for generating fingerprint samples. Simple system architecture is opted as shown in Figure4.1 where this stream of data using feature extraction and modelling tools are modelled independently. The feature vectors are fused using a proposed technique to extract Region of Interest (ROI) & obtain a new feature vector which can be stored in database. After storing all data, matcher can be used to match the new data with existing database & gives the results.

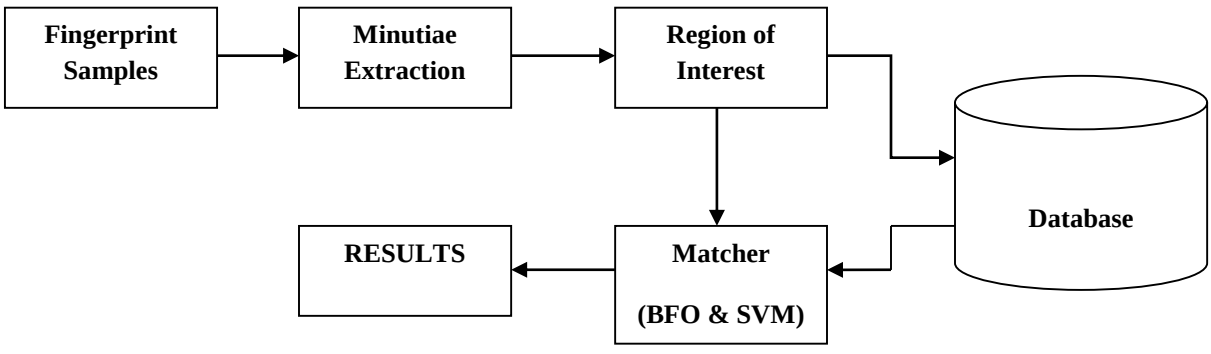


Figure 4.1: Basic Block Design

4.1.1 Minutiae Extraction

Researchers use a three - stage process to execute a minutia extractor. It is divided in two stages: post processing stage and preprocessing minutia. [fig 4.2]

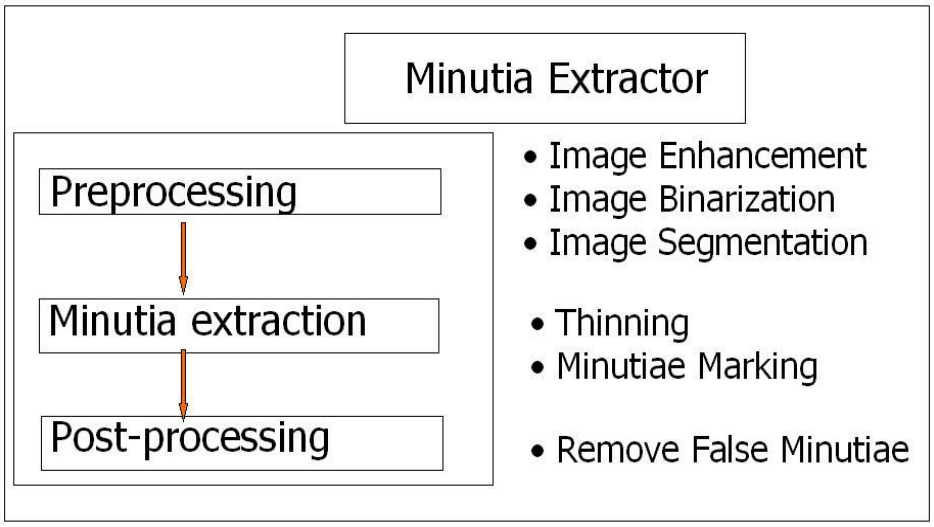


Figure 4.2 Minutia Extractor

For the fingerprint image preprocessing step threshold method which is locally adaptive is used to binarize a figure print [12]. A step approach is used to fulfill the image segmentation task: region of interest extraction by morphological approach, estimation by block direction, segmentation using direct intensity [4].In preprocessing stage the methods used are developed by different researchers but with combination of their researches the new results have been used in the project via error and trial. Image segmentation of fingerprints have been introduced with extraction ROI of morphological operations.

Three thinning algorithms [12] are examined at the step of minutia extraction and then finally operations of morphological thinning are bid out with good quality of thinning and high efficiency. Many literatures have reported minutia marking as easy task but however a case was detected while implementing and an extra correcting process was used to negate such oversight.

To eliminate false minutia, a more useful algorithm is processed for the post processing step [13].

4.1.2 Bacterial Foraging Optimization (BFO)

Bacterial Foraging Optimization Algorithm is an optimization algorithm which reduces the noise, features selected, unnecessary data and gives the high accuracy in case of fingerprint matching. Kelvin M Passino invented the BFO algorithm. It is basically a feature selection algorithm that led to following objectives:

- bound storage necessities, increase speed of processing
- Performance enhancement to achieve high correctness
- Exploitation of full resources.
- Improving identification rate

The BFO process can be divided into mainly three parts a. chemotaxis b. reproduction and c. elimination and dispersal.

a) **Chemotaxi**s: It is the behavior of the bacteria in which it tries to avoid the deadly substance and then move forward to search nutrients by hiking towards high nutrient area [26]. So it involves two steps 1. Unidirectional movement 2. Topple

In the unidirectional movement it moves only in one direction whereas in topple step it moves in other direction rather than unidirectional direction. There is a limit in number of steps to survey entire search space. Suppose Q_0 (p,q,r) be the position of o^{th} bacterium at p^{th} chemotactic, q^{th} reproductive and r^{th} elimination. Then chemotactic movement is represented as:

Z(o) is the size of the step.

Δ(o) indicates a vector in the uninformed path.

Δ(o) remains unaffected; or else,

Δ(o) is a arbitrary vector whose rudiments lie in [-1, 1]

p: Dimension of the search space,

j: Total number of bacteria in the population,

S: The number of chemotactic steps,

Ns: The swimming length.

M_8: The number of reproduction steps,

M_{ed}: The number of elimination-dispersal events,

P_{ed}: Elimination-dispersal probability,

Z(i): The size of the step taken in the random direction specified by the tumble.

Fitness function, denoted as P (o, p, q, r), will be evaluated for each step of run or topple in the chemotactic procedure.

b) **Reproduction:** The fitness of every bacterium is calculated as the computation of the step fitness throughout its time, namely,

$$P^o \text{ (Fitness)} = \sum^{m+1} P \text{ (o, p, q, r)}$$

Where m is amount of chemotactic steps.

c) **Elimination and dispersion:** Only Reproduction and chemotactic are not enough for universal optima exploration. Elimination and dispersion of reproductive steps are also required to move to another direction.

BFO Algorithm

Step-1 Initialize parameters j, S, M, M_8, M_{ed}, P_{ed}, Z(o) (o=1,. . . ,S), Θ_o

Step-2 Elimination-dispersal loop: q=q+1

Step-3 Reproduction loop: r=r+1

Step-4 Chemotaxis loop: p=p+1

For o =1,. . . ,S take a chemotactic step for bacterium o as follows.

Compute fitness function, P (o, p, q, r):

$P(o, p, q, r) = P(o, p, q, r) + P(\Theta_o (p, q, r), T(p, q, r))$

Let

$P_{last} = P(o, p, q, r)$

Compute P (o, p+1,q,r) and

let $P(o, p, q, r) = P(o, p, q, r) + P(\Theta_o (p, q, r), Z(p, q, r))$

Swim

Let n=0 (offset for swim length).

While n < M (if have not climbed down too long)

1. Let

   n = n + 1
2. If $P(o,p+1,q,r)<P_{last}$(if doing better), let $P_{last} = P(o, p + 1, q, r)$
3. Else, let this is the end of the while statement.

Step-5 If p < M, go to step 4. In this case keep on chemotaxis because the life of the bacteria is not ended.

Step-6 Reproduction

P^o (Fitness)= $\sum^{m+1} P(o, p, q, r)$

Step-7 If q < M, go to step 3

Step-8 Elimination-dispersal: For o= 1 , . . . , S with probability P_{ed}

4.1.3 Support Vector Machine (SVM)

Support vector machine is a feature classification scheme that has the skill to divide feature space into two modules by the use of optimal hyper plane. All over, the SVM takes as input fingerprint picture data that consist of optimistic and pessimistic samples and the difficulty of untying a set of training vectors belonging to two separate classes is solved by SVM algorithm.

SVM Algorithm

The mapping Q (•) is represented in the SVM classifier by a kernel function S (•,•) which defines the inner product in ‘K as shown :

S (a,b) = Q(a) • Q(b) and the decision function is written as:

$$\mathbf{G(y) = \sum^{l} C_y X_y S(\, y_y, \, y)}$$

Where, *l* is the number of data points and $x_y \varepsilon \{-1,1\}$

4.2 System Level Design

Fingerprint matching algorithm flowchart is shown below in the figure 4.3. In the first stage image acquisition of fingerprint image is done, in the second stage binarisation of fingerprints is done binarisation of image is must to perform various operations, in the third stage thinning of the fingerprint image is done, in the fourth step minutiae extraction is done to get the features, in the fifth stage removal of false minutiae is done which helps in improving accuracy percentage, after removing false minutiae in the sixth stage implementation of SVM and BFO is done. And verification using both algorithms is done with matching accuracy this process is repeated to record data.

In the final stage we collect our recorded data and comparison of accuracy of both algorithms is done. In this stage matching accuracy is compared for images on which same type of operations are performed and then on these images both algorithms are applied.

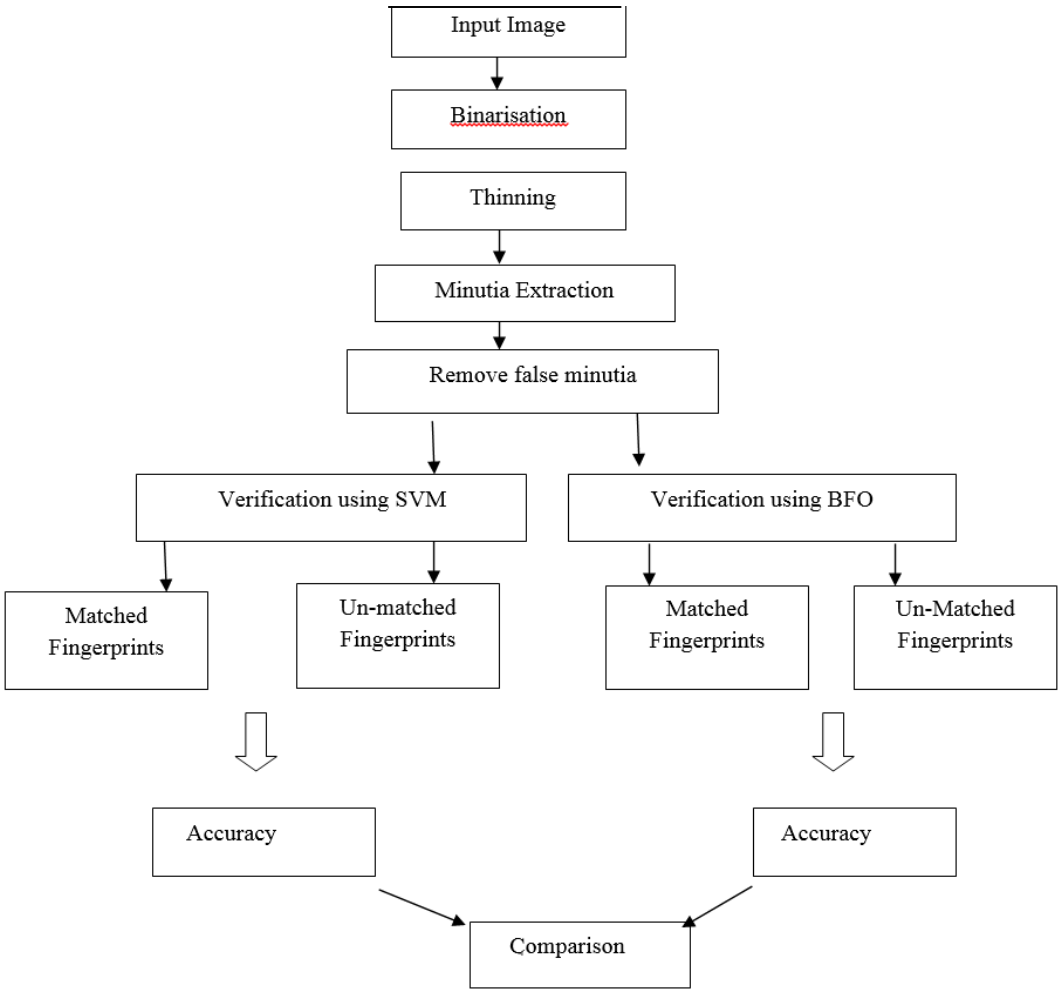


Figure 4.3: Flowchart of Fingerprint Matching Algorithm

4.2.1 Fingerprint Image Acquisition

Image acquisition or data collection is usually done with sensors. We have used images which are collected from two types of sensors solid state sensor and optical sensors.

4.2.2 Binarization of Fingerprint Image

Convergence to 1-bit gray image from 8 bit gray fingerprint image with 1-value for furrows and 0-value for ridges is called binarization of fingerprint image. After the command, furrows are presented in white, while ridges are presented in black color.

Fingerprint image is binarized by the method of binarization which is a locally adaptive method. A method like this is derived from the process of converting a pixel value to 1

only if the value is greater current block (16x16) mean intensity value to which the pixel belongs.

4.2.3 Thinning Morphological Operation

Thinning is the thickness reducing process which effectively thins the fingerprint. Thinning reduces the size of blueprint till the breadth of stroke becomes single pixel. When thinning is applied to a fingerprint image then some precautions has to be taken such as:

- thinning of ridges should be done to its innermost pixel
- No discontinuity should be done after thinning
- Noise removal has been done effectively

The process of removing the over plus pixels of ridges to a point where they are just 1 pixel wide is ridge thinning. Repetitive parallel thinning algorithm is used [12]. In every small window image (3x3) the over plus pixels are marked down by the algorithm in all the full scans of fingerprint image. In the testing such a repetitive, thinning parallel algorithm has poor efficiency though after enough scans it can get a perfect thinned ridge map. [2] To obtain directly from gray level fingerprint images of thinned ridges a one in all method is used. Ridges with utmost gray intensity value are tracked by this method. Now since pixels with only utmost gray intensity value are left binarization method is enforced implicitly. In the testing still huge computation complexity is seen in each trace step advancement but like other thinning algorithms it does not require pixel to pixel movement. Thus the morphological thinning function set up in MATLAB is bid out in third method.

4.2.4 Minutia Marking

Marking minutia points after thinning fingerprint ridge becomes comparatively simple. Many literatures said it not being a trivial job because at the time of minutia marking step at the least a single special case arouses caution**.**

If pixel in Centre is 1 and has neighbors of exactly 3 one –value for every 3x3 window then ridge branch is the pixel in the Centre. [Figure 4.4 (a), (b), (c)] now if pixel is in centre 1

and has neighbors of 1 one-value then the ridge ending is the pixel in the center. [Figure 4.4 (a), (b), (c)].

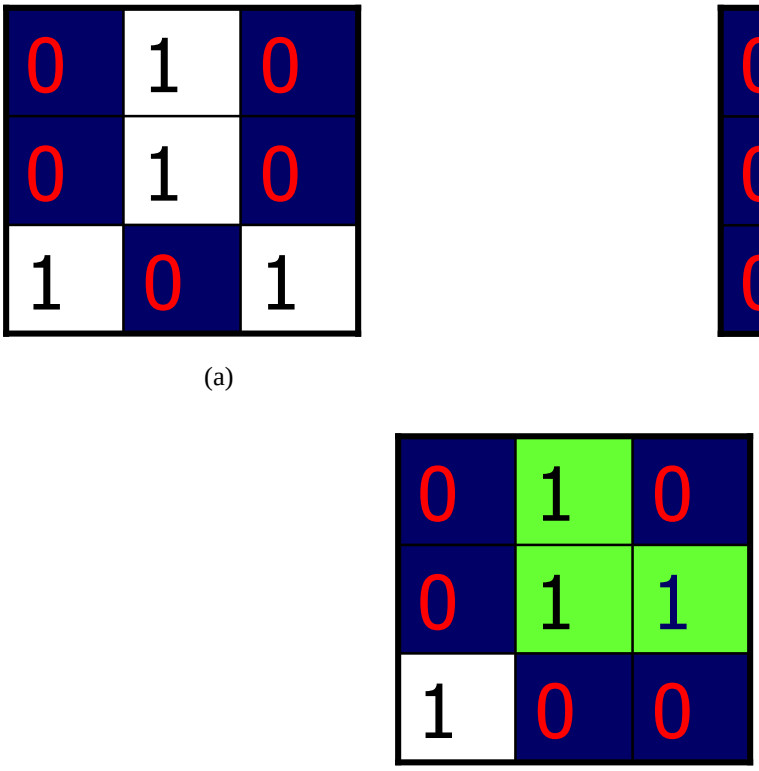


Figure 4.4: (a) Bifurcation, (b) Termination, (c) Triple Counting Branch

Triple counted branch, a special case is illustrated in figure 4.4. Two pixels will be highlighted as branches too if the rightmost pixel with 1 value and two uppermost pixel together with 1 value have outside the 3x3 window another neighbor.

At this stage estimation of average inter –ridge with D is done .Difference between the average of two inter ridge distance is called as average inter –ridge width**.** The process of approximating the value D is easy. In the row, pixels whose value is one are summed up and a row of thinned ridge image is scanned. Then to obtain an inter–ridge width the above summation is divided by row length. For further appropriateness, row scan of such a kind is done on various other rows and column scans, then finally to get the value of D average of every inter–ridge width is done.

For later work a specific ID is marked on every thinned ridges in a fingerprint image along with the minutia marking. Morphological operation: BWLABEL is used to realize labeling operation.

4.2.5 Remove False Minutia

The fingerprint image is not totally corrected at preprocessing stage**.** For instance, ridge cross-connections are not totally eliminated because of over inking and because of inappropriate ink false ridge breaks. Actually some artifacts are introduced sometimes by all the early stages which afterwards trace to spurious minutia**.** Accuracy of the matching will be affected if false minutia are called as genuine minutia. So for the fingerprint check system to be useful, some process of false minutia removing are required.

Removing of false minutia is a very important step of the pre-processing. Presence of large number of false minutia will led to the wrong fingerprint matching. False minutia removal has been taken place distinctively if following order to get the accuracy.

Steps for removing false minutia are as follows:

- If the same ridge has two minutia and the distance between one termination and one bifurcation is less than D then both of them are to be removed. Average distance between two neighbor ridges which are parallel is represented by D which is the inter-ridge width in average.
- Two bifurcations are eliminated if they are in the same ridge and the distance between them is less than D.
- Two terminations are called as false minutia obtained from a broken ridge and are eliminated if they follow the condition that no other termination is between the two terminations and if two terminations fall within a distance D and if directions of small angle variation is coincided by their directions.
- Two terminations are eliminated if their length is smaller than D and are located in a short ridge.

False minutia elimination procedure has two advantages. First - to decrease the computation complexity the order eliminating procedure is considered well. Second-minutia are distinguished using ridge ID and false minutia of seven types are defined by

comparing with other methods which are loosely defined. It outstrips the way used by [12] which does not use false minutia type relations.

Figure 4.5: (a) Original Image, (b) Enhanced Image, (c) Binarized Image, (d) Thinned Image

4.2.6 Orientation Field

Find the value of orientation angle that varies from 40 to -40 degree.

4.2.7 Implementation of BFO

Feature Extraction: generated the eigenvectors as the feature vector set will be input to the BFO.

Feature Selection: Apply the BFO algorithm on the feature vector set as stated in above division. Select the location of bacteria X with max (A) value. This location represents the finest feature subset of the features defined in feature extraction task.

Classification: compute the difference involving the feature subset (obtained through feature selection) of each fingerprint picture and the test image. Obtain the matched and non-matched fingerprints values on the basis of metrics.

4.2.8 Implementation of SVM

Feature Extraction: generate the feature vector values of the fingerprint samples and that will be the input to the SVM.

Classification: compute the difference involving the feature subset (obtained through feature extraction process) of each fingerprint sample and the test image. Obtain the matched and non-matched fingerprints values on the basis of metrics.

4.3Algorithm Level Design

The whole process is divided into two phases:

- Training Phase
- Testing Phase

The step wise algorithm for both of the phases is defined below:

4.3.1 Training Phase Algorithm:

1. Start
2. Upload an image for training
3. Provide angle if required

   Follow following steps

   - Binarization
   - Thinning
   - Minutiae
4. Save to database.
5. Choose image to be matched
6. Repeat the same steps for image 2
7. Save reduced value to db2
8. Store

4.3.2 Testing Phase Algorithm

1. Upload the image and rotate its angle if required
2. Follow these steps
   - Binarisation
   - Thinning minutiae
3. Save image as uploaded image fit

4. Convert image to double
5. Let x=doubled image
    - Fit function sqrt(x(counterno,1x))+ (counterno,2)
6. Process with fitness function.
7. Final optimised value
    - Db=$\sum_{i=1}^{n} org_{img} + x\_fit$
8. Matching

    If (db1-db2)<=threshold

    {

    Matched

    }

    Else

    {

    Rejected or not matched

    }

4.4 Implementation

This work considers different experiments to evaluate the results and to find out the accuracy of the recognition system. The whole fingerprint verification system use both SVM and new proposed BFO based classifiers to test the system efficiency.

4.4.1 Database Used

The database has been collected from different users. There are about 15-20 samples has been tested using both classifiers that is BFO & SVM. Samples used in this work are around 10-20 KB.

4.4.2 Working of the System

This work is implemented using MATLAB 7.11.0. A GUI design is prepared in MATLAB for easy access or usage of system. The basic design prepared in MATLAB is as shown in figure 4.6.

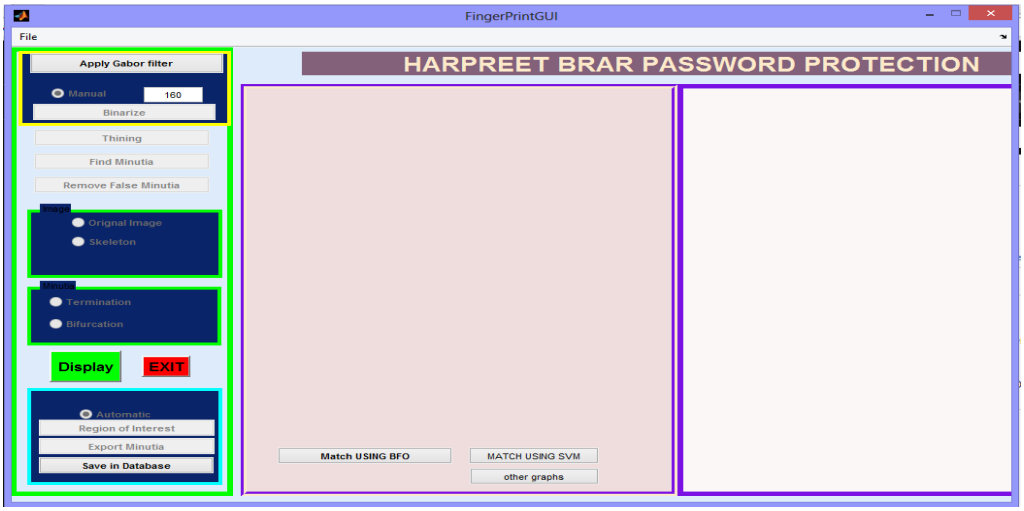


Figure 4.6: Basic Design of the System (MATLAB GUI)

Step 1: Upload Sample:

First Step of to work with this system is uploading an image file of fingerprint sample as shown in figure 4.7.

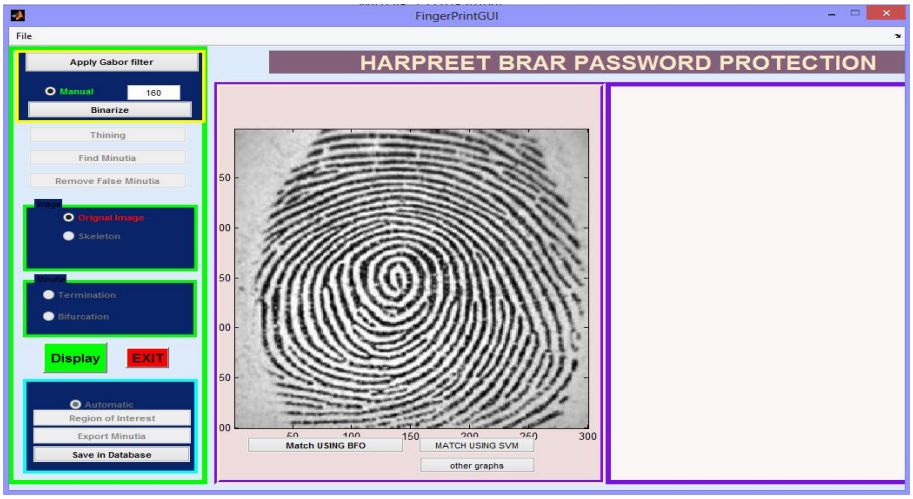


Figure 4.7: Upload Sample

Step 2: Set Angle of Rotation

After uploading samples, rotate the image to particular angle if required as shown in Figure 4.8 or to test system accuracy while image get rotate to different angle.

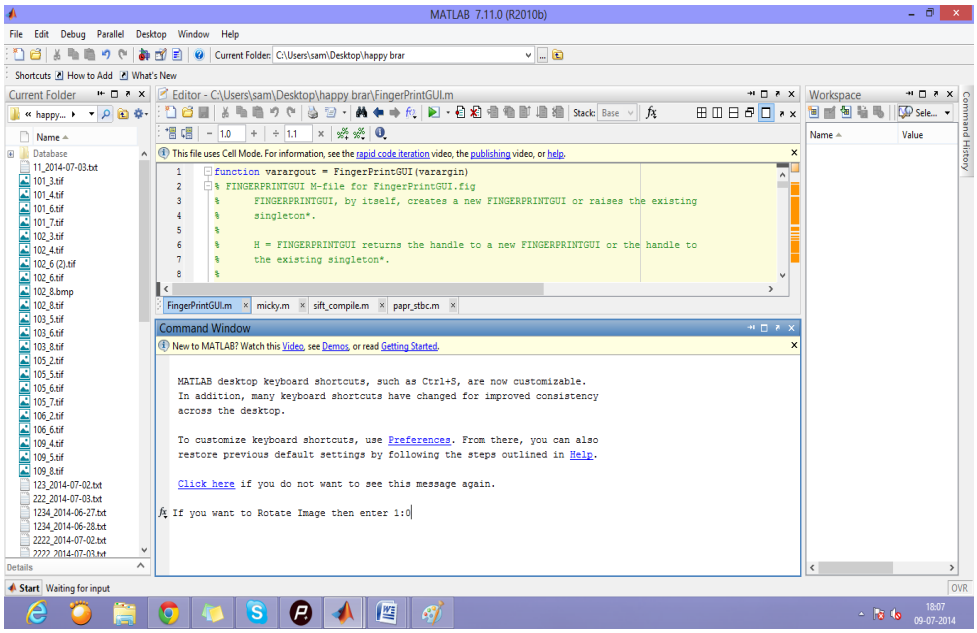


Figure 4.8: Angle Setup in Command Window

Step 3: Binarization

This process is used to binarize the base image so that the properties can be extracted in an efficient manner. To binarize an image in MATLAB 2010 im2bw command is supported. Morphological operations are also suitable for the same purpose. The binarized image is as shown in Figure 4.9.

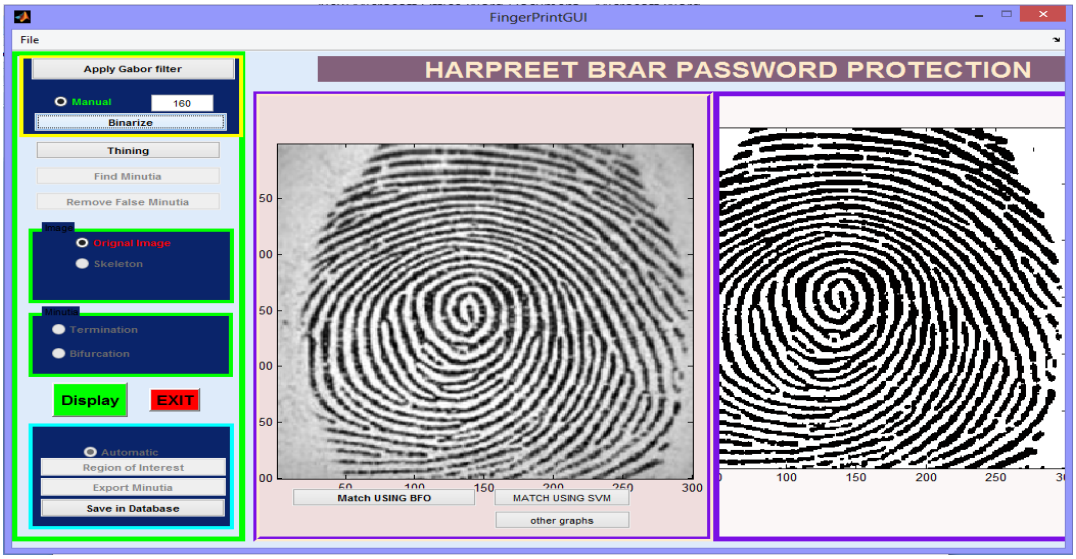


Figure 4.9: Binarization

Step 4: Thinning

The binarized image is then passed for the thinning process as the binary image might contain hard boundaries and they would result into false minutiae formation. The thinning process finds the relevant edges of the system so that minutiae extraction can become an easy process as shown in Figure 4.10.

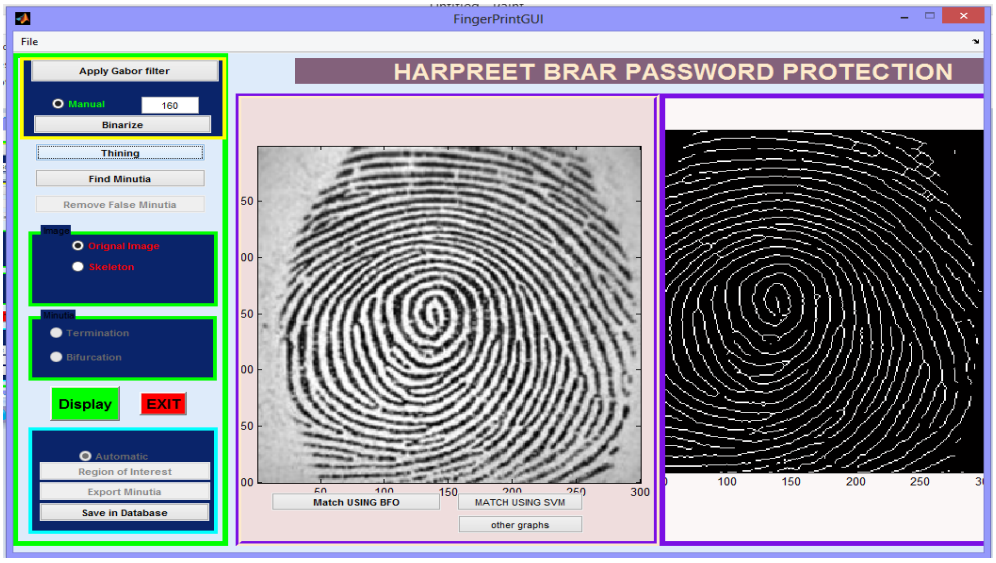


Figure 4.10: Thinning

Step 5: Minutiae Extraction

Minutiae extraction is an important procedural part in this proposed work. The minutiae points are carried out on the basis of the key point localization algorithm or surf detection algorithm which has been applied in the program while the development of the system. The surf points extract the exact points of the regions of the thinned image. It is quite possible that the system might detect some wrong minutiae points; hence removal of false minutiae has been applied once the minutiae part is done. The removal of false minutiae is done on the basis of the Centroid of the collected minutiae regions as shown in Figure 4.11.

Figure 4.11: Minutiae Extraction

Step 6: Region of Interest (ROI) Extraction

The region of intereset part in the system extract those part of the finger print where the probablity of the extraction is maximum as shown in figure 4.12. Further more the munitia values are saved through the export munita system. The export munita saves the entire munita region in a text file named after the wish of the user and for the same an image in the data base folder is saved. The database folder will consists of the original image uploaded by the user and the roated munita extrated points.

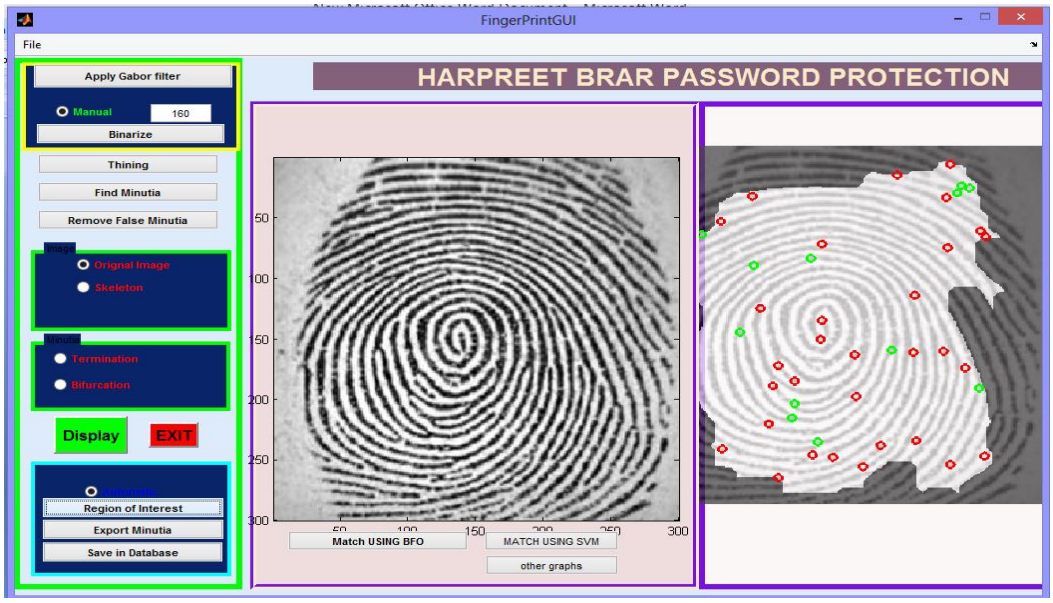


Figure 4.12: Region of Interest (ROI) Extraction

Chapter 5

Result and Discussion

Verification and Identification are two different modes in which a biometric recognition system can work. The process of finding out the identity of a person by viewing a pattern which is biometric is calculated using biometric features of an individual.

In cases of identification, system is accustomed with several persons pattern. In this stage of training calculation of biometric template is done for each person. For all the known template a pattern that is to be identified is matched, producing either a distance about the similarity. The system allots the individual the most identical biometric template. To protect against the patterns that are imposter (like the ones not known to the system) to be identified correctly, similarity has to surpass certain level, and rejection of the pattern occurs if the level is not procured

Identity of the person is claimed to be priority in the case of verification. Only the verified pattern is compared with the template of individual person. Like the case of identification the similarity between template and pattern is checked that weather it is sufficient to provide access of secured area and system

Biometric systems performance is measured by their appropriateness in identification. As discussed, the entire system is based on the finger print roation mechanism explained in the problem statement also. Further more the results are passed to two classifiers namely BFO (BACTERIAL FORGING OPTIMIZATION) & SVM (SUPPORT VECTOR MACHINE) which defines the system accuracy. The following table and graph shown in figure 5.1 describes the recognition rate of the system while tested by both algorithms i.e. BFO & SVM for an image sample by rotating them on different angles.

Table 2: Recognition rate using BFO & SVM

S. No.	Angle of rotation (In Degrees)	Accuracy (BFO)	Accuracy (SVM)
1	0	95	76
2	5	93	78
3	10	94	75
4	15	94	79
5	20	93	75
6	25	95	77
7	30	94	78
8	35	95	80
9	40	95	81
10	0	93	79
11	-5	95	78
12	-10	94	75
13	-15	93	78
14	-20	94	75
15	-25	93	79
16	-30	95	75
17	-35	94	81
18	-40	93	80

In this system minutiae feature extraction & ROI Extraction techniques are used in SVM and BFO to check the accuracy by the angle from 0 degrees to 40 degrees and from5 degrees to -40 degrees. The accuracy of BFO came out to be 93% to 95% and of SVM is from 75% to 81%.The current research work has proposed a mechanism based on the minutia points. So from the figure 5.1 it is crystal clear that SVM performs efficiently in comparison to BFO.

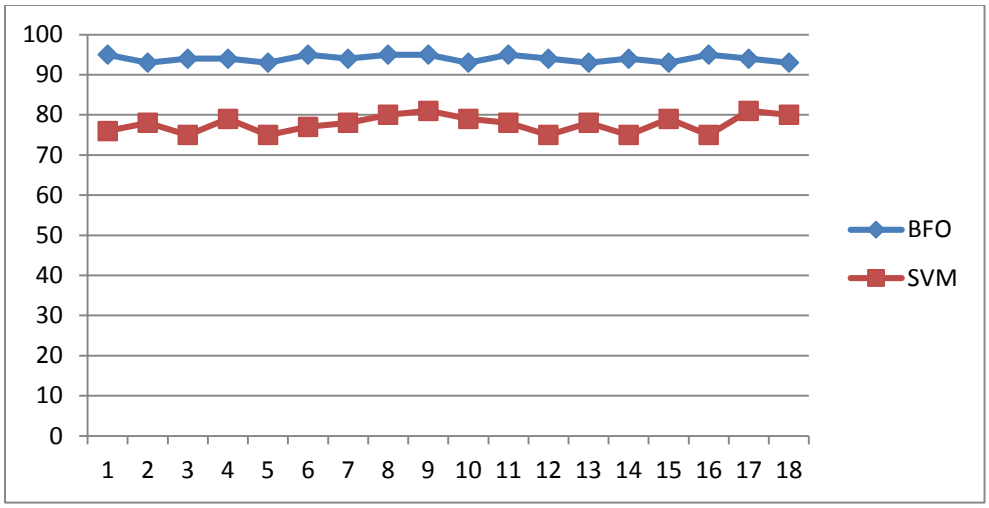


Figure 5.1: Recognition rate by using SVM & BFO

The comparison between Support Vector Machine and BFO is represented through graph where it is clearly visible line showing BFO is always above line showing SVM at different angles.

Chapter 6

Conclusion & Future Work

6.1Conclusion

This work is to enhance the recognition rate of the fingerprint verification system. Feature Extraction can be done by using Minutiae-extractions and various morphological operations. Two algorithms are used to test this system i.e. BFO and SVM. The consequence of Bacterial forging optimization algorithm is consecutively better than that of Support Vector Machines. BFO method matches the extracted minutiae point on the basis of epochs provided to the classifier. The classifier works with the hidden layers. Suppose there are 10 number of hidden layer's provided, then the system would be evaluated for 200 times with the epoch count as 20. In each and every iteration, the value of threshold to be applied is reduced to a level to check the accuracy of the classification. On the other hand SVM only takes the inputs in the binary format and its group train mechanism has been found to be not sufficient enough to enhance the classification accuracy above 85 percent.

The BFO classifier is one of the most suitable algorithms to check the finger print matching with angle variations. The system has been tested with several angles like -20, -40, 50, 70, 90 degrees of rotation. With every angle of rotation, BFO has shown a signification improvement in the classification accuracy in comparison to the SVM, hence it can be concluded that BFO works more efficiently in rough conditions.

6.2Future Work

The current research work has proposed a mechanism based on the minutia points. The future aspects of this research work may include more feature extraction techniques like Scale-Invariant Feature Transform (SIFT) in combination with the Bacterial foraging optimization (BFO)optimization method and also testing of this system using some noisy samples and forgeries

References

[1]. Liu Wei, "Fingerprint Classification using Singularities Detection", *International Journal of Mathematics and Computers in Simulation*, issue 2, vol. 2, pp. 158-162, (2008).

[2]. Hartwing Fronthaler, Klaus kollreider, and Josef Bigun, "Local Features for Enhancement and Minutiae Extraction in Fingerprints", *IEEE Transactions on Image Processing*, vol. 17, no, 3, pp. 354- 363, (2008).

[3]. M. R. Girgisa, A. A. Sewisyb and R. F. Mansourc, "Employing Generic Algorithms for Precise Fingerprint Matching Based on Line Extraction", *Graphics, Vision and Image Procession Journal*, vol. 7, pp. 51-59, (2007).

[4]. Duresuoquian Miao, Qingshi Tang, and Wenjie Fu, "Fingerprint Minutiae Extraction Based on Principal Cures", *the Journal of the Pattern Recognition Letters*, vol. 28, pp. 2184-2189, (2007).

[5]. Luping Ji and Zhang Yi, "Fingerprint Orientation field Estimation using Ridge Protection", *The Journal of the Pattern Recognition*, vol. 41, pp. 1491-1503, (2008).

[6]. G.Sambasiva Rao, C. NagaRaju, L. S. S. Reddy and E. V. Prasad, "A Novel Fingerprints Identification System Based on the Edge Detection", *International Journal of Computer Science and Network Security*, vol. 8, pp. 394-397, (2008).

[7]. Jinwei Gu, Jie Zhou, and Chunyu Yang, "Fingerprint Recognition by Combining Global Structure and Local Cues", *IEEE Transactions on Image Processing*, vol. 15, no. 7, pp. 1952 – 1964, (2006).

[8]. V. Vijaya Kumari and N. Suriyanarayanan, "Performance Measure of Local Operators in Fingerprint Detection", *Academic Open Internet Journal*, vol. 23, pp. 1-7, (2008).

[9]. Raju Sonavane and B. S. Sawant, "Noisy Fingerprint Image Enhancement Technique for Image Analysis: A Structure Similarity Measure Approach", *Journal of Computer Science and Network Security*, vol. 7 no. 9, pp. 225-230, (2007).

[10]. Eric P. Kukula, Christine R. Blomeke, Shimon K. Modi, and Tephen J. Elliott, "Effect of Human Interaction on Fingerprint Matching Performance, Image Quality, and Minutiae Count", *International Conference on Information Technology and Applications*, pp. 771-776, (2008).

[11]. Mana Tarjoman, and Shaghayegh Zarei, "Automatic Fingerprint Classification using Graph Theory", *Proceedings of World Academy of Science, Engineering and Technology*, vol. 30, pp. 831-835, (2008).

[12]. Unsang Park, Sharath Pankanti, A. K. Jain, "Fingerprint Verification Using SIFT Features", *SPIE Defense and Security Symposium*, Orlando, Florida, 2008.

[13]. Bhupesh Gour, T. K. Bandopadhyaya and Sudhir Sharma, "Fingerprint Feature Extraction using Midpoint Ridge Contour Method and Neural Network", *International Journal of Computer Science and Network Security*, vol. 8, no, 7, pp. 99-109, (2008).

[14]. Haiping Lu, Xudong Jiang and Wei-Yun Yau, "Effective and Efficient Fingerprint Image Post processing", *International Conference on Control, Automation, Robotics and Vision*, vol. 2, pp. 985- 989, (2002).

[15]. M. Ballan, AFIS Archives Preparing and Methods of Directional Image Senior Project, Electrical Engineering Dept.,Yildiz Technical Univ., 80750 Istanbul, Turkey, Feb. 1997.

[16]. Prabhakar, S, Jain, A.K, Jianguo Wang and Pankanti S, Bolle, "Minutia Verification and Classification for Fingerprint Matching", *International Conference on Pattern Recognition*, vol. 1, pp. 25-29, (2002).

[17]. Manvjeet Kaur, Mukhwinder Singh, Akshay Girdhar, and Parvinder S. Sandhu, "Fingerprint Verification System using Minutiae Extraction Technique", *Proceedings of World Academy of Science, Engineering and Technology*, vol. 36, pp. 497-502, (2008).

[18]. Alessandra Lumini, and Loris Nann, "Advanced Methods for Two-Class Pattern Recognition Problem Formulation for Minutiae-Based Fingerprint Verification", the Journal of the Pattern Recognition Letters, vol. 29, pp. 142-148, (2008).

[19]. Xifeng Tong, Songbo Liu, Jianhua Huang, and Xianglong Tang, "Local Relative Location Error Descriptior-Based Fingerprint Minutiae Matching", *the Journal of the Pattern Recognition Letters*, vol. 29, pp. 286-294, (2008).

[20]. Mohamed. S. M and Nyongesa.H, "Automatic Fingerprint Classification System using Fuzzy Neural techniques", *IEEE International Conference on Artificial Neural Networks*, vol. 1, pp. 358-362, (2002).

[21]. L. Lam S W Lee, and C Y Suen, "Thinning Methodologies-A Comprehensive Survey", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 14, pp. 869-885, (1992).

[22]. Ching-Tang Hsieh and Chia-Shing –", "humanoid fingerprint recognition based on Fuzzy neural network" *International Conference on Circuit, Systems, Signal and Telecommunications*, pp. 85-90, (2007).

[23]. Asker M. Bazen, Gerben T.B. Verwaaijen, Sabih H. Gerez, "A correlation-based fingerprint verification system." Workshops on Circuits,Systems and Signal processing, veldhoven, The Netherlands,(2000).

[24]. David G. Lowe, "Distinctive Image features from scale invariant key points." *International journal of computer vision*, Vol. 60, No. 2, pp. 91-100, (2004).

[25]. Shunshan li, Min Wei, Haiying Tang, Tiange Zhuang and Michael H. Buonocore, "Image Enhancement method for Fingerprint Recognition System." ,*In Proceedings of the 2005 IEEE,Engineering in Medicine and Biology 27th annual conference*, Shanghai, China, September1-4, pp.3386-3389,(2005).

[26]. D. DeRosier, "The turn of the screw: The bacterial flagellar motor," *Cell*, Vol 93, No. 1, pp. 17-20, (1998).

List of Publication

Harpreet Singh Brar, V.P. Singh, "Fingerprint Image Recognition Using Bacterial Foraging Optimization Algorithm", *International Conference on Advances in Computing Communication and Informatics,* IEEE, Noida, Uttar Pradesh,2014