JOURNAL OF INFORMATION, KNOWLEDGE AND RESEARCH IN COMPUTER SCIENCE AND APPLICATIONS

PERFORMANCE IMPACT OF THE USER ATTEMPTS ON FINGERPRINT RECOGNITION SYSTEM (FRS)

[1]DR. NEERAJBHARGAVA, [2]DR. RITUBHARGAVA, [3]MANISH MATHURIA, [4]MINAXI COTIA

[1]Associate Professor, Department of Computer Science, School of Engineering & Systems Sciences, MDS University Ajmer, Rajasthan, India
[2]Lecturer, Department of MCA, Government Woman's Engineering College Ajmer, Rajasthan, India
[3]Department of Computer Engineering & Information Technology, Government Engineering College Ajmer, Rajasthan, India
[4]Department of Computer Science, School of Engineering & Systems Sciences, MDS University Ajmer, Rajasthan, India

[1]drneerajbhargava@yahoo.co.in,[2]drritubhargava@yahoo.com, [3]manishmathuria@outlook.com, [4]minaxi.cotia @gmail.com

ABSTRACT : *The Fingerprint images are used to identify the person uniquely. The special system known as Fingerprint Recognition System (FRS) is used to match Fingerprints. The overall matching and recognition should be accurate, so that it can be used in the restricted areas. It is very important to consider the performance of the Fingerprint Recognition System (FRS). Today's world has a common question i.e. 'Why Fingerprints are not commonly used?' The answer of this question is the inefficient FRS method. User identification and verification techniques are designed in such a way that only authorized users are allowed to access. So, it is require studying the functional approaches by analyzing the problems regarding verification. This research paper experimentally present the performance evaluation of Minutia Matching based FRS by using of false acceptance rate (FAR) and false rejection rate (FRR). The result of user attempts evaluates by calculating Hough Transformation.*

Keywords: Fingerprint Matching System, System Accuracy, False Acceptance Rate, False Rejection Rate, Genuine User, Imposter User, and Hough Transformation.

1. INTRODUCTION

Person identification is information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context. In the industrial revolution, migration to the cities creates a need of person identification.

Commonly, password and ID cards are used for person recognition in restricted areas for access systems but these methods can be easily violated. Biometrics, which refers to study of measurable biometrics characteristics, biometrics has the capability to reliably distinguish between an authorized or genuine person and an imposter. In biometrics, identity of a person can be determined in two ways: verification and identification. Verification refers to verify authenticity of a person and identification refers to specify person identity.

Concernment of any biometric recognition system is based on its performance, here performance means to be detect genuine and imposter users. In many biometric applications, the performances of system are evaluated by False Acceptance Rate and False Rejection Rate. Fingerprint based recognition method used for its universality, permanence, uniqueness, acceptability, accuracy and low cost. The actual reason of using fingerprint for person identification is the ridges arrangement on every finger of every person is different. Basically, FAR represent the analysis of fingerprint matching techniques by comparing fingerprint images and generates imposter score and FRR represent the matching two fingerprint images of two different fingers and generate genuine score. One powerful approach is Hough transformation, which is a computationally procedure for detecting lines in images. It can be used to detect lines, circles and other parametric curves. The motive is to find location of lines in image and robust detection under noise and partial obstacle.

2. SYSTEM ACCURACY

This is world of smart devices where smart people require efficient results. The system should be such that the users can faith on the device. Human behavior is analyzed and implement as a software system. Artificial Intelligence is one of latest subject which only research to develop a machine program; this machine program provides capability to any device to take independent action.

Previously, most of the government department and computer systems are based on demographic data such as name, date-of-birth, address and other information derived from alphabets and number. For example, to search for a record, one would enter a name or id to operate data. The success of the system is dependent on the accuracy of the data which is entering Fingerprint recognition system is based on the data which is extracted from image. Success of the fingerprint matching depends on the image quality i.e. the correspondence between them. The latent fingerprint consists of fragmentary portion of single finger which exceed the problem to find out correspondence in the image record. The amount of information present in the image is usually affected with the background interference. Naturally, the better the latent image, the higher the chances of success. Inversely, the chance of missing identification is because of the image degraded by 75%. This percentage is calculated in research of Kenneth R. Moses titled as "Automated Fingerprint Identification System (AFIS)" [1].

3. FINGERPRINT MATCHING SYSTEM

Fingerprint Matching is the basis of any Fingerprint Recognition System, which may of different type such as: Minutia-Matching, Pattern-Matching, and Correlation-Matching. In this research paper, minutia based matching is used to determine whether or not the fingerprint represented the same identity (user).

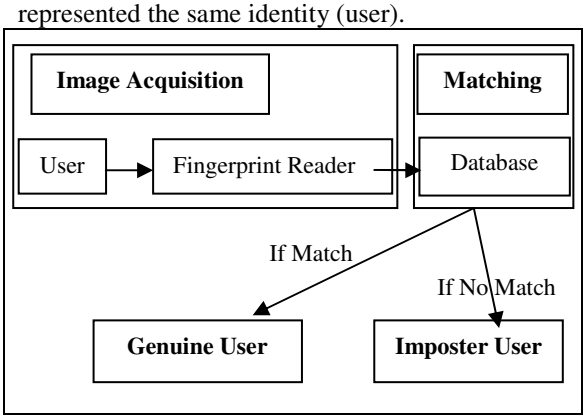

Fig.1 Fingerprint Matching System

In the minutiae based fingerprint matching algorithm examines input fingerprint image with the template or specimen fingerprint image stored in the database. The algorithm uses various standard preprocessing steps and it includes all the stages to extract the minutiae [2].

4. PERFORMANCE ANALYSIS

In this paper the performance of fingerprint matching system is measured with the help of FAR and FRR. Sometimes fingerprint matching techniques erroneously accepted invalid fingerprints due to lacking of complicated matching policies and also sometimes fingerprint matching technique erroneously rejected valid fingerprint due to lacking of identification policies.

A perfect fingerprint matching technique requires the FAR (False Acceptance Rate) and FRR (False Rejection Rate) to be zero (0).

4.1Image Quality

Quality of an image is essential feature of fingerprint authentication system. Basically image quality refers as clarity. Image quality is a characteristic of an image that tends to exclude potentially image degrading obstacles such as noise, fog, blurriness and imperfect image. Parameters of image quality are:

1) Geometric image accuracy—geometric image accuracy is the ability of the scanner to keep relative distances between points on an object (e.g., two minutiae) the same relative distances apart in the output image.

2) Modulation transfer function (MTF)—Modulation transfer function is used to approximate the ability of the scanning device to capture both low-frequency (ridges themselves) and high-frequency (ridge edge details) information in a fingerprint at minimum standards.

3) Signal-to-noise ratio—Signal-to-noise ratio is the ability of the scanning device to digitize the information without introducing too much electronic noise (that is, with the pure white image parts appearing pure white and the totally black image parts appearing totally black).

4) Gray-scale range of image data—This Parameter is used to avoiding excessively low-contrast images by ensuring that the image data are spread across a minimal number of shades of gray.

5) Gray-scale linearity—As the level of gray changes in a fingerprint capture, the digital image reflects a corresponding ratio of gray level across all shades of gray.

6) Output gray-level uniformity—It is the ability of the scanning device to create an image with a continuous gray scale across an area on the input image (tested using a special test image) that has a single gray level.

5. PERFORMANCE PARAMETERS

For determine the performance of a fingerprint matching system we can consider two main parameters that is false acceptance rate (FAR) and false rejection rate (FRR).

1) False Acceptance Rate (FAR):

The false acceptance rate (FAR) is a ratio of the probability that the fingerprint recognition system will decide to allow access to an imposter user.

$$\text{FAR} = \frac{\text{Total number of accepted invalid fingerprints attempts}}{\text{Total number of imposter attempts}}$$

2) False Rejection Rate (FRR):

The false rejection rate (FRR) is a ratio of the probability that the fingerprint recognition system denies access to an approved or genuine user. [3]

$$FRR = \frac{\text{Total number of rejected valid fingerprints attempts}}{\text{Total number of genuine attempts}}$$

Here is another term called as Equal Error Rate (ERR). If false acceptance rate and false rejected rate are equal is known as equal error rate.

3) Genuine attempt:

A "genuine" attempt is a valid attempt by a user to match his or her fingerprint which is stored as a template in the database.

4) Impostor attempt:

An "impostor" attempt is an invalid attempt by a person who is unknown to the system, and matches his or her fingerprint to the stored template.

5) Hough Transformation:

The Hough Transformation is used to detect straight lines present in any Digital Image and maps the line to a point. The equation $R=cos\ \theta + \sin\theta$ is used for mapping. The range of theta is -90 to +90 with the step of 10 degree. All the computed R is stored in a rectangular matrix T, known a Hough Transform matrix. Finally, plot all rows of the rectangular matrix against the same predefined theta variations of theta.

6. PREVIOUS WORK

The fingerprint image recognition is a very old technique, since the concept of digital image based security came into existence. Many researches were based on development of new approach to recognize fingerprint from the images. However, some research was based on evaluation of fingerprint recognition method. This research paper includes the concept of some recent researches on evaluation of FRS. The research paper on "Performance Evaluation of Fingerprint Verification Systems" discusses about data collection and testing protocols, and includes a detailed analysis of the results [4].

Another reviewed paper on "A Review of Schemes for Fingerprint Image Quality Computation" presents how the fingerprint image quality affects the performance of Fingerprint Recognition System. The most important fact is to understand the requirement of most efficient and effective method to improve performance of Fingerprint based Verification System [5].

Anil K Jain had analyzed the performance of fingerprint verification system by user habituation, combination of multiple fingers and combination of multiple impression of the same finger [6]. The latest research was based on Fingerprint Recognition with identical twin fingerprint. They have investigated the ability of the fingerprint verification matcher to discriminate between identical twins [7]. Minutiae based fingerprint matching is most powerful and effective fingerprint matching process. Our previous paper is based on minutiae matching technique. Minutiae points are the unique points which are created by series of ridges and valleys in fingerprints. In minutiae-based techniques first of all find minutiae points, and then generate data matrix for fingerprint to get the position, orientation and types of minutiae.

As shown in fig.2 minutiae based fingerprint recognition consists of Binarization, thinning, minutiae extraction, minutiae matching and computing matching score. Due to matching unique points it is very difficult for imposter user to cheat the system. FRS easily detects Genuine and imposter using minutiae based fingerprint matching technique [8].

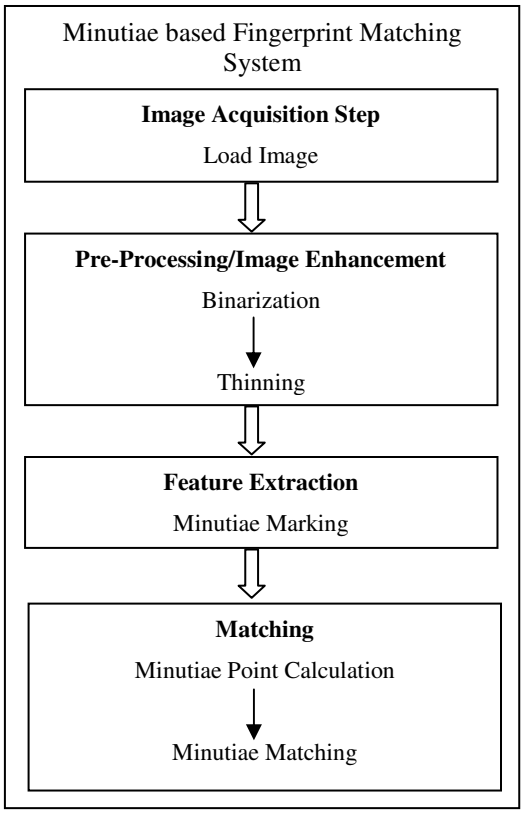

Fig.2 Minutiae Matching Algorithm

7. METHODOLOGY

1. Initially, we have two types of user one is genuine user and other one is imposter user.
2. In the first step, enroll one or more genuine fingerprint images into the database of the system with person name and other identity information.

3. Next step is the evaluation process of Fingerprint Recognition System (FRS). User A (Genuine user) and B (Imposter user) will individually try to login in the system. The following algorithm describes the further process.

Algorithm:
Input: Take Fingerprint images from fingerprint reader.
Output: Generate matching score of fingerprints and produce performance of fingerprint recognition system.
Step 1: Receive fingerprint images from fingerprint reader and image will supply to FRS as input.
Step 2: Apply basic preprocessing steps like Binarization and Thinning for image enhancement.
Step 3: Mark minutiae points (Ridges-end point and bifurcation point) and extract all the information about fingerprint image.
Step 4: Finally fingerprint matching Step occur. In this we have two conditions:
(a) First condition: where Imposter user will apply to the system, when the fingerprint isaccepted or not then the information is updated in FAR table.
(b) Second condition: where genuine user will apply, then if the fingerprint is rejected or accepted then information goes in FRR.

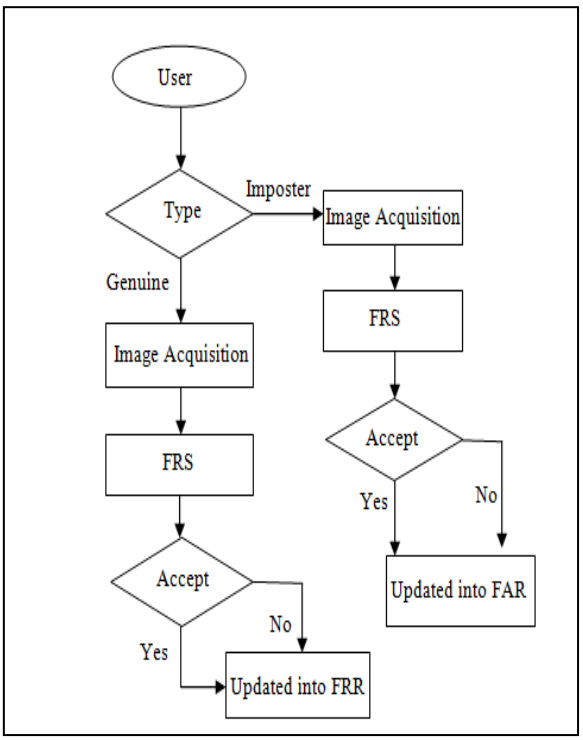

Fig.3 FRS Evaluation

8. RESULT

In the following result, User A and B i.e. a genuine and imposter user will apply to the FRS 4 times, separately. By obtain the values in the table, now, FAR and FRR can be calculated.

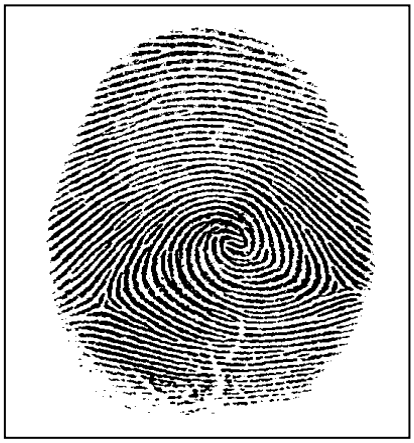

Fig.4. Image stored in the database of the user.

Fig.4. shows the fingerprint image which is initially stored in the database of the genuine user.

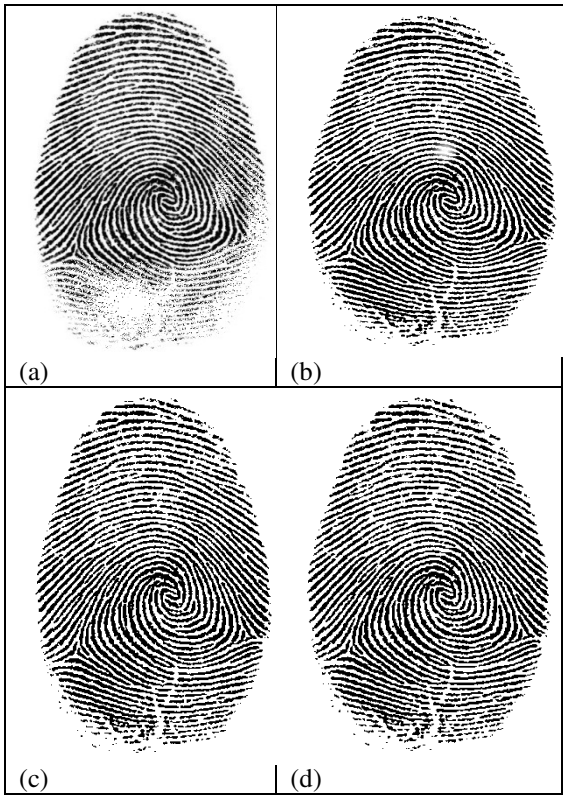

Fig.5. Genuine User Attempts

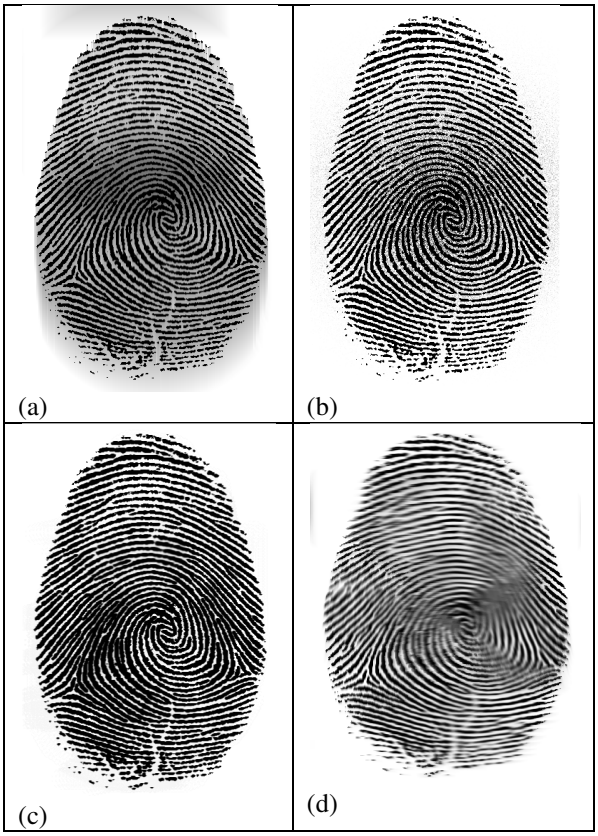

Fig.6. Imposter User Attempts

In the above result Fig.4 shows the total attempts of the genuine user (user A), in which attempts (a) and (b) are rejected due to improper fingerprint capture, sweat respectively and attempts (c) and (d) are accepted.

Fig.5 shows the total attempts of the imposter user (user B), which is trying to become valid user. In this all the attempts are rejected in fingerprint recognition system. This shows that our fingerprint recognition system cannot accept any kind of imposter activities.

The advantage of using Hough transformation is it's conceptually simple and implemented easily. Generalized Hough Transform can be used where a simple analytic description of feature is not possible. Results of Hough Transformation for user attempts:

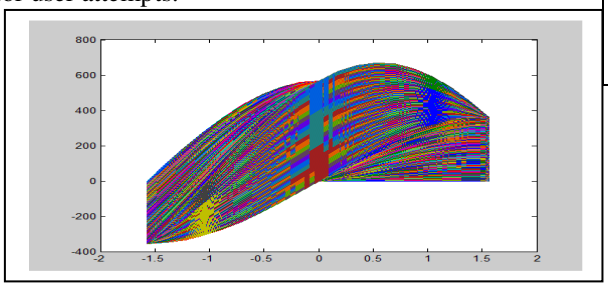

Fig.7. Hough Transformation of the Original FingerprintImage (Genuine User Fingerprint Image) stored in the database

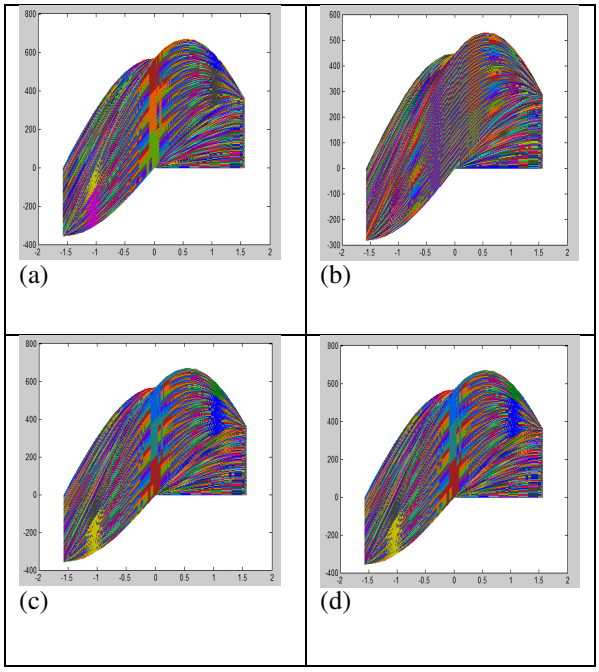

Fig.8. Hough Transformation result for Genuine User

Figures .8 demonstrate the Hough transformation result of all genuine user attempts. These figures show different color combinations and variations of genuine user attempts with slight changes.

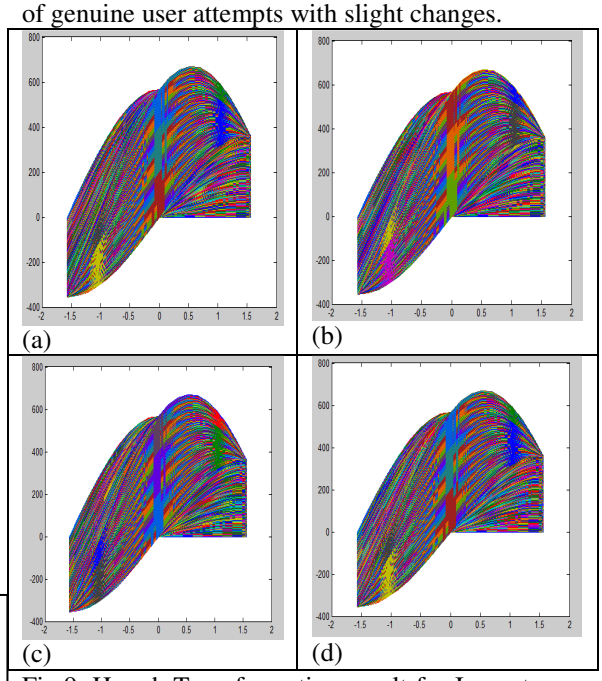

Fig.9. Hough Transformation result for Imposter User

Figure.9 displays totally different Hough transformation graph of imposter user in comparison of genuine user.

The Hough Transform is used for image analysis. This technique finds the imperfect instances of the object. By using Hough Transform, one can easily detect the changes between stored fingerprint and the applied fingerprint image. As the output of the Hough Transform the graphs are plotted between the

distance from the origin (mm) and the angle (radians).

TABLE I
FALSE REJECTION RATE TABLE

User	Attempt	Result
A	1	Reject
A	2	Reject
A	3	Accept
A	4	Accept

Table I explain, user A (Genuine user) are trying to login the system, but due to some reasons (like. Sweat, cut etc) attempts 1 and 2 are not accepted. Attempts 3 and 4 are accepted because these are in proper form

TABLE II
FALSE ACCEPTANCE RATE TABLE

User	Attempt	Result
B	1	Reject
B	2	Reject
B	3	Reject
B	4	Reject

Table II explain, user B (Imposter user) are trying to login the system, but our fingerprint recognition system do not allow to access the system and the FAR will be zero.

8. CONCLUSION

This research paper introduces the factors which actually affect the performance of FRS. Two types of users i.e. Imposter and Genuine are used to study the failure problems regarding authentication attempts. The results for different conditions are stored in the tables for both types of user. After the analysis of Minutia based Fingerprint Recognition System, it is very clear that Minutia based FRS is best to face Imposter attempts, but it has bad result regarding genuine user attempts. The analyzed reason is the minutia based recognition is performed by matching location of minutia point, so if a single point mismatches in the whole image then the failure occurs, because it matches the location of each Minutia Point. It is require improving the image acquisition to ignore authentication problem regarding genuine user. This research study also produce good understanding about the Hough Transformation and its uses.

9. REFERENCES

[1]. *Kenneth R. Moses, Peter Higgins, Michael McCabe, SalilPrabhakar, Scott Swann, "Automated Fingerpring Identification System".*

[2]. *Rohit Singh (Y6400), Utkarsh Shah (Y6510), Vinay Gupta (Y6534), "Fingerprint Recognition", Department Of Computer Science & Engineering Indian Institute Of Technology, Kanpur. Computer Vision And Image. Processing (Cs676) .*

[3]. *Lawrence O'Gorman, Veridicom Inc., Chatam,NJ,"FINGERPRINT VERIFICATION".*

[4].*RaffaeleCappelli, Dario Maio, Member, Ieee, DavideMaltoni, Member, Ieee, James L. Wayman, And Anil K. Jain, Fellow, Ieee "Performance Evaluation Of Fingerprint Verification Systems" Ieee Transactions On Pattern Analysis And Machine Intelligence, Vol. 28, No. 1, January 2006.*

[5]. *Fernando Alonso-Fernandez, Julian Fierrez-Aguilar, Javier Ortega-Garcia "A Review Of Schemes For Fingerprint Image Quality Computation".*

[6] *Anil k Jain, SahilPrabhakar , and Arun Ross "Fingerprint Matching: Data Acquisition And Performance Evaluation" Department of Computer Science and Engineering Michigan State University, East Lansing, MI 48824.*

[7] *Xunqiang Tao1., Xinjian Chen2., Xin Yang1, Jie Tian1,3* "Fingerprint Recognition with Identical Twin Fingerprints" PLoS ONE 7(4): e35704. doi:10.1371/ journal.pone.0035704.*

[8] *Dr. NeerajBhargava, Dr. RituBhargava, Manish Mathuria, MinaxiCotia "Fingerprint Matching Using Ridges-end And Bifurcation Point" International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in International Journal of Computer Applications® (IJCA) (0975 – 8887).*