INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 3 ISSUE 1 -JANUARY 2015 - ISSN: 2349 - 9303

Reduction of False Acceptance Rate Using Cross Validation for Fingerprint Recognition Biometric System

Arunprakash.k[1]
[1]Sona College of Technology
Department of CSE
prakasharun1991@gmail.com

Narayanan R.C[2]
[2]Sona College of Technology
Department of CSE
rc_narayanan@yahoo.co.in

Dr.Krishnamoorthy.K[3]
[3]Sudharshan Engineering College
Department of CSE
kkr_510@yahoo.co.in

Abstract— In the field of biometric modality fingerprint is considered to be one of the most widely used method for individual identity. The fingerprint authentication is used in most application for security purpose. In the biometric systems, the input images are binarized and feature is extraction. The Minutiae matching in fingerprint identification is done by identifying the minutiae point of interest and their relationship. The validation testing in the proposed system using the method of K- fold cross validation by using two , a training set and test set of images to find the appropriate image that matches the input image ,increase the accuracy of recognition by reducing the false acceptance rate of the system**.**

Index Terms— Minimum Biometric, Binarization, Minutiae, Cross validation, False Acceptance Rate.

1 INTRODUCTION

BIOMETRICS is the science that deals with measuring and analyzing biological data of human body. Biometric techniques are gaining importance for personal authentication and identification as compared to the traditional authentication methods by comparing the extracted features against the database set. Biometric templates include fingerprint, palm vein, palm print, hand geometry, DNA, iris recognition and retina. Fingerprint based authentication is one of the most reliable and mature biometric recognition techniques due to the distinctiveness and stability that fingerprints can provide compared to other biometrics. Fingerprints are the raised ridges of the skin on hands and feet. These portions remain unchanged throughout the lifetime. The methods used in fingerprint authentication systems can be roughly divided into following two categories as texture-based methods and minutiae-based methods. Among them, minutiae-based methods are more reliable and popular. In minutiae-based algorithms, a fingerprint image is represented by a set of labeled minutiae, which refer to ridge ending and bifurcation. Fingerprint matching with minutiae-based algorithms can be considered as point pattern matching. Although much attention has been given to minutiae-based matching in recent years, fingerprint matching is not an easy task due to fingerprint uncertainty caused by rotation, translation and nonlinear deformation at each fingerprint image acquisition.

Biometric recognition often makes use of a comparator module which can be carried out in two different modes, namely user verification and user identification. The verification is performed by authentication based on individual who has access to the system. This mainly involves a straight forward one to one comparison and result in the process of accept or rejects decision. The identifiers are usually in the form of user IDs or smartcards. The main aim of user identification is to find the closest matching identity, if any exists. Biometric identification is often carried out in many areas to prevent multiple users using the same identity and to avoid wrong usage of information. Also it ensures security than other verification method. The proposed k-fold cross-validation schemes are commonly used in the classification literature to analyze the expected performance of a classifier over a dataset. Also, when comparing classifiers, it is common to compare them according to their performances averaged over a number of iterations of cross-validation

This paper is organized as follows: In section I we discuss the features of fingerprint. In the next section we stated some of the relevant works. Section III describes various process of fingerprint recognition. In the next section features of the proposed system are defined. In the next section the performance evaluation is done. The last section draw a conclusion out of all discussion followed by the list of references.

1.1 Fingerprint

Fingerprints are the most important part of human finger. It is found that fingerprints are identical even for the twins. Fingerprints have remarkable permanency and uniqueness throughout the life time. The fingerprints have been used for the forensic application and identification for a long time. They provide more secure and reliable personal identification than passwords, id-cards or key can provide. A fingerprint is the composition of many ridges and furrows but cannot be distinguished by their ridges and furrows. It can be distinguished by abnormal points on the fingerprint ridges called as Minutia.

Minutia is divided into two parts such as: termination and bifurcation. Termination is the abrupt ending point of the ridge and bifurcation is the branch where a single ridge is divided into ridges. The minutia also consists of ridges and furrows. The fingerprints have two set of features .The local features which are unique and used for positive identification. The global features that can be seen through our naked eyes includes

- Basic Ridge Pattern
- Type Lines
- Pattern Area
- Core Point
- Delta
- Ridge Count

Pattern Area contains all global features, but it is found that some local features are present outside the area.

Core Point is the Centre approximation point of the fingerprint, used as the point of reference for reading/classifying the fingerprint.

Type Lines tend to surrounds the pattern area by two innermost ridges after starting in parallel and diverge.

Delta is the point of divergence of the two type lines on a friction ridge or a triangular area which denotes the radiation of ridges outwards in three directions.

Ridge Count is the total number of ridges that touch the imaginary line between the delta and core.

1.2 Global Ridge Pattern

A fingerprint is a combination of convex skin called ridges and concave skin called valleys with a spiral curve line shape based on the characteristics of global ridge pattern. The global fingerprint features are

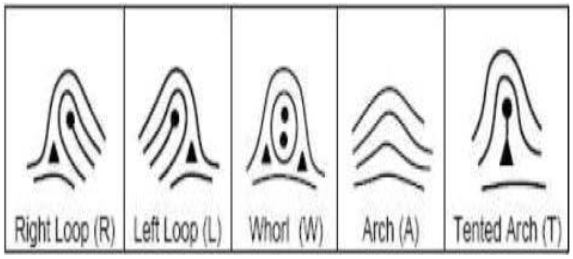

Fig 1.Fingerprint Ridge Pattern

2 Related Work

Ravi J, K. B. Raja, Venugopal K. R [2] stated that pre-processing the original fingerprint involves binarization of images, thinning of ridges and noise removal. Minutia Score Matching based fingerprint recognition uses Ridge pointing and Ridge bifurcation for matching of the minutia points. The proposed method gives better false minutiae removal values compared to the existing method. Sonam Shukla and Pradeep Mishra[3] proposed a new Automatic Fingerprint Identification System (AFIS) for extracting minutiae from poor quality fingerprint impressions arising from very dry fingers and fingers mutilated by scars, scratches due to accidents, injuries. The minutia based fingerprint recognition consists of Binarization, Thinning, Minutiae extraction and matching .Based on the matching score the minutiae matching is done. Fingerprints which undergo Thinning and Binarization process produce better results than other prints. Prathima Devi Sirivella and D.Raaga Vamsi [4] have proposed minutiae matching algorithm which explore the minutiae matching process and user authentication based on the elliptical curve generated for each fingerprint images. This provides better result for the database based attacks. Here Gabor filters are used to specify the angle of frequency-selective and angle-selective for the fingerprint ridges. Loris Nanni and Alessandra Lumini [5] state the functions of the existing fingerprint matchers and proposed a hybrid fingerprint matcher which uses the Gabor filters from the minutiae localizations and orientations to improve the performance. Based on the experimentation on a set of images, it is proved that an image-based matcher cannot be faked with the sole knowledge of the minutiae position and orientation. Umarani Jayaraman [6] proposed a geometric hashing along with indexing and searching using minutiae .It inserts each minutia along with the feature vector exactly once into a hash table. Since minutiae of all fingerprint images in the database are found to be well distributed into the hash table, no rehashing is required. This hashing may be used for the validation of fingerprint. Iwasokun G. B [7] et al proposed an Automatic fingerprint identification algorithm which performs the process of fingerprint feature detection, validation and extraction algorithm. It is found that using the proposed algorithm valid, true minutiae points were extracted from the images with greater speed and accuracy. Omar N. Faqhruldin [8] et al proposed a new method for the distributed generation based on the detection of islands and make use of the K-fold cross validation to test the accuracy of the detection process. Kambiz Frounchi [9] and his team perform analysis on the problem reported while using the manual image segmentation procedures and found that it is time consuming. They proposed an ISAO- Image Segmentation Automated oracle that uses a machine learning to construct an oracle, which acts as reference for the verification process.

Also the validation is done on the classified image by using the cross fold validation technique. Ron Kohavi [10] et al states that by using cross fold validation the accuracy can be increased by increasing the number of fold and it is found that tenfold validation method is used to increase the accuracy rate of the estimation. Jan C. van Gemert [11] et al stated that the cross validation along with SVM increases the classifier performance of the videos.

3 FINGERPRINT RECOGNITION

The fingerprint recognition is the process of identifying the individual fingerprint with that of the set of other that are available in the database. Fingerprint recognition technology extracts features from impressions made by the fingertip ridges. The fingerprints are either flat or rolled. A flat print captures the region of the central area between the fingertip and the first knuckle; a rolled print captures ridges on both sides of the finger. The fingerprint identification problem can be grouped into two sub-domains such as Fingerprint verification and identification.

3.1 Fingerprint verification

Use Fingerprint verification is the method where we compare a fingerprint database with an enrollee fingerprint and finds the matching between both the fingerprints. This method is mainly used to verify a person's authenticity. For verification a person need their fingerprint to be read into the fingerprint verification system which is saved in some format with the person's identity. Then it is applied to the fingerprint verification system so that the person's identity can be easily verified. Verification is also called as peer to peer matching.

Fig 2. Fingerprint Minutiae

3.2 Fingerprint Identification

The Fingerprint identification is mainly used to specify any person's identity by his fingerprint. Identification has been used for criminal fingerprint matching. Here the system matches the fingerprint of unknown individual against the other fingerprints present in the database to associate a crime with identity. This process is also called, one to many matching. Identification is traditionally used to solve crime and catch thieves. It also provides access to the authenticate user and ensures security.

The biometric system used now a day's perform the operations based on the identification and verification process may lead to FAR which may allow the unauthorized user to access to the information or system.

The fingerprints which are subject to several variations, mainly due to the presence of skin distortions and of different skin quality such as dry, moist, dirty skin or wet skin are the cause for the false acceptance. Due to this the identified accuracy is reduced.

4 PROPOSED METHOD

The proposed fingerprint recognition method consists of the following phases

4.1 Image Acquisition

Initially the images of the fingerprint are recorded with the help of the fingerprint sensors. The reading of the images is either static as well as dynamic. For the authentication based biometric system the fingerprint images of the authorized users are obtained and recorded in the form of database. The images are acquired as input to the system using the external sensors or from the database for the recognition purpose.

4.2 Preprocessing

The preprocessing module is used for the process of image enhancement before extracting the features from the image. It is done to extract the features accurately than earlier which can be done by the process of histogram equalization. The image binarization is used for preprocessing, by setting the threshold value for the image. The fingerprint image binarization is used to transform the gray fingerprint image to an image by changing the value for the ridges and the furrows based on the threshold values and pixels defined earlier. After this operation, the ridges in the fingerprint will be highlighted with black colour while furrows will be coloured with white, increasing the clarity of the image.

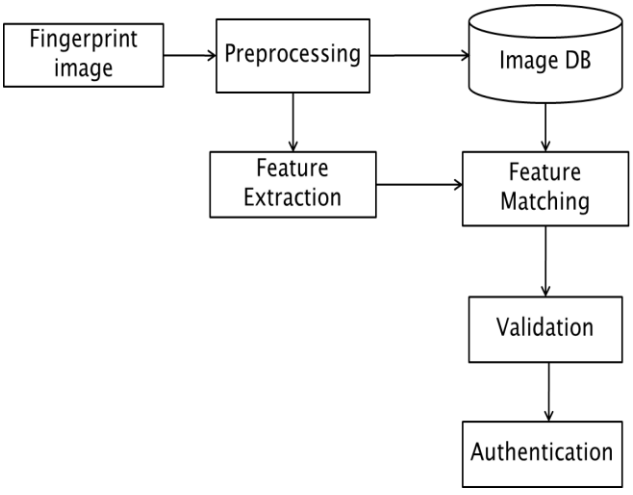

Fig 3. System Architecture

4.3 Feature Extraction

The Extraction of required features from an image is done by using a set of Gabor filters with varying frequencies. By tuning a Gabor filter to specific frequency and direction, the local frequency and orientation information can be obtained along with the texture information from images. Minutiae points are extracted for identifying of the identical fingerprints.

4.4 Feature Matching

The matching is a key operation of the fingerprint recognition system. Minutiae features extracted are matched by finding the alignment between the template and the input minutiae sets which result in the maximum paring of minutiae The similarity between the input and stored template are computed and matched features are obtained from minutiae based matching. Minutiae alignment is done by associating the ridges of each minutia by assigning the coordinates for the ridges. The similarity of correlating the two ridges is derived from (1).

$$S = \frac{\sum_{i=0}^{m} xi\ Xi}{\sqrt{\sum_{i=0}^{m} xi^2\ Xi^2}} \qquad (1)$$

Where, m is the minutiae points and x is the coordinate values.

Minutiae matching are done by computing the matching ratio of the each minutiae computed from (2). If the match score is greater than the threshold value then they are said to be matched.

$$Match\ score = \frac{Number\ of\ total\ minutiae\ pair}{Number\ of\ minutiae\ of\ template\ fingerprint} \qquad (2)$$

Based on the matching the fingerprints are classified. The classification outcome is used for accepting or rejecting the input image of the fingerprint recognition system.

4.5 Validation Testing

In the process of fingerprint recognition the accuracy of identification is a mandatory task. The minutiae matching provide appropriate outcome, but in order to increase the rate of accuracy we are validating the identified fingerprint. In this module the image recognised are compared with all other images by using the cross fold validation testing, taking the two a training set and the test set, increasing the identification rate.

5 EXPERIMENTAL RESULTS

5.1 Performance Evaluation

The performance is determined by two indexes, False Acceptance Rate (FAR) and False Rejection Rate (FRR) which is computed by matching each sample with that of the images in the database. The rate is determined by the match score obtained by matching the minutiae.

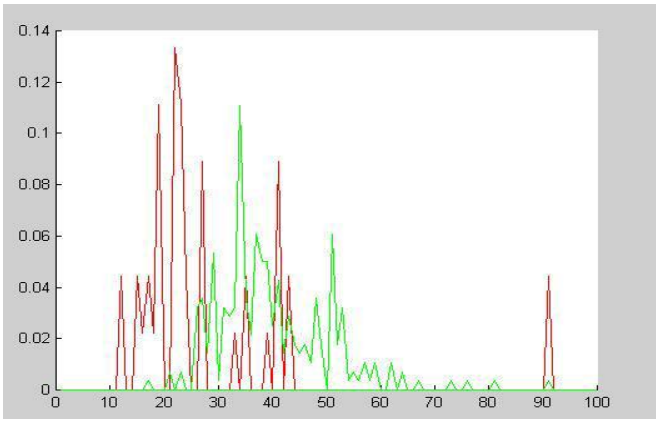

Fig 4. Distribution of incorrect and correct scores
Green line: Correct Score
Red line: Incorrect Score

The distribution curve gives the average matching score of the samples on the database chosen.

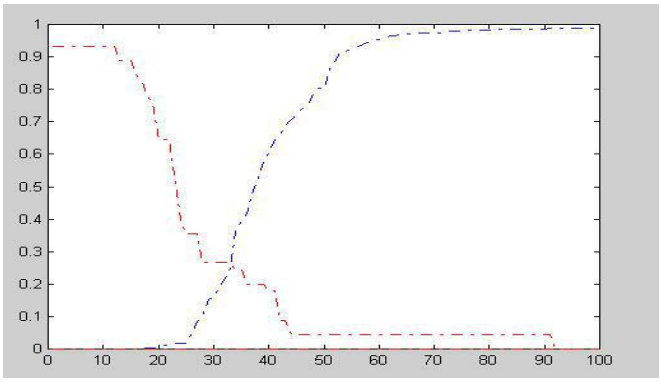

Fig 5.Curve of FAR and FRR
Red line: FAR
Blue line: FRR

6 CONCLUSION

The Fingerprint recognition is used in many applications like biometric measurements, solving crime investigation and also in security systems. They undergo various stages from preprocessing of the acquired image to minutiae matching by using various techniques to perform operation on each stage. They provide authenticity by matching the input image with that of the images in the database by using the minutiae points of each image. Though it is found that fingerprints are the excellent biometric, in some cases due to some external impact the fingerprints which are unauthorized are recognized increasing the false acceptance rate of the system. The increasing demand to ensure security and reducing error open many research opportunities. By validating the recognized image the accuracy of recognition is increased, but in future establishing the uniqueness of fingerprint remains challenging.

REFERENCES

[1] Handbook of Fingerprint Recognition by Davide Maltoni, Dario Maio, Anil K. Jain & Salil Prabhakar

[2] J.Ravi, K.B. Raja, K.R.Venugopal, "Fingerprint Recognition Using Minutia Score Matching", *In proceedings of the International Journal of Engineering Science and Technology* ,2009,Vol.1(2).

[3] Sonam Shukla, Pradeep Mishra, " Increasing The Accuracy Of An Existing Fingerprint Recognition System Using Adaptive Technique" , IJARCSSE'13: *In Proceedings of the International Journal of Advanced Research in Computer Science and Software Engineering* , June 2003.

[4] Prathima Devi Sirivella, D.Raaga Vamsi, "Fingerprint Validation and Outlier Detection Using Minutiae Approach in Network Security", IJCOT'12: *In Proceedings of the International Journal of Computer&OrganizationTrends*, October 2012

[5] Loris Nanni, Alessandra Lumini, " Descriptors for image-based fingerprint matchers,": *In Proceedings of the Expert Systems with Applications* ,Elesvier 2009.

[6] Umarani Jayaraman, Aman Kishore Gupta, Phalguni Gupta,"An efficient minutiae based geometric hashing for fingerprint database*": In Proceedings of Neurocomputing 137*, Elesvier 2013 .

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

[8] Omar N. Faqhruldin,, Ehab F. El-Saadany, Hatem H. Zeineldin, "A Universal Islanding Detection Technique for Distributed Generation Using Pattern Recognition": *In Proceedings of IEEE Transactions On Smart Grid*, Vol. 5, No. 4, July 2014

[9] Kambiz Frounchi, Lionel C. Briand, Leo Grady , Yvan Labiche , Rajesh Subramanyan "Automating image segmentation verification and validation by learning test oracles *": In Proceedings of the Information and software Technology 53*, Elesvier 2011.

[10] Ron Kohavi, "A Study of Cross Validation and Bootstrap for Accuracy Estimation and Model selection*": In the Proceedings of International Joint Conference on Artificial Intelligence (IJCAI),* 1995.

[11] Jan C. van Gemert, Cor J. Veenman and Jan-Mark Geusebroek," Episode-Constrained Cross-Validation in Video Concept Retrieval": *In the Proceedings of IEEE Transactions on Multimedia*.

[12] Uday Rajanna, Ali Erol, George Bebis evin," A comparative study on feature extraction for fingerprint classification and performance improvements using rank level fusion" : *In Proceedings of the Theoretical Advances*, Springer 2009 .

[13] Ravi Subban, Dattatreya P. Mankame," A Study of Biometric Approach Using Fingerprint Recognition": *In Proceedings of the Lecture Notes on Software Engineering*, May 2013.

[14] Loris Nanni, Alessandra Lumini, " Descriptors for image-based fingerprint matchers,": *In Proceedings of the Expert Systems with Applications* ,Elesvier 2009.

[15] Javier Galbally, Sebastien Marcel, "Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint and Face Recognition": *In Proceedings of the IEEE Transactions On Image Processing*, Vol. 23, No. 2, February 2014.

[16] Jose Garcia Moreno-Torres, Jose A.Saez, and Francisco Herrera," Study on the Impact of Partition-Induced Dataset Shift on k-fold Cross-Validation*": In Proceedings of IEEE Transactions On Neural Networks And Learning Systems*, Vol. 23, No. 8, August 2012

[17] Muhammad Umer Munir and Dr. Muhammad Younas Javed," Fingerprint Matching using Gabor Filters*": In Proceedings of National Conference on Emerging Technologies*, 2004.