Wavelet feature extraction and ANOVA based Multimodal Biometric Fusion System

Jatin Azad[1] Nidhi Mittal[2]
[1]M.Tech Scholar [2]Assistant Professor
[1,2]Department of Electronics and Communication Engineering
[1,2]DIET,Karnal, Haryana

Abstract— We live in a world today in which technology moves at a very rapid pace. Many of these technological advances can be used to make our everyday life easier and safer. One such technology which is very popular these days and is in extensive use is biometrics system. A biometric system attempts to confirm an individual's claimed identity by comparing a submitted sample to one or more previously enrolled templates. But there are few limitations associated with unimodal biometric system such as noise in sensed data, non-universality, spoof attacks etc. So it is possible to overcome these limitation which gives rise to multimodal biometric system. In this work, the biometrics traits under consideration are: human iris, fingerprint and face. The reviewed papers propose methods that employ PCA, fisher face projection, minutia extraction and LBP feature extraction on different biometric traits. However these techniques contribute to complexity and accuracy of the entire system has scope for improvement. With advances in digital image processing methods, pre-processing of each unimodal system sample and techniques such as wavelet based feature extraction and ANOVA deals with the existing system in a way making it more secure. It can be gauged by parameters such as FRR, EER, FAR. Thus, the complexity and accuracy gaps between the reviewed and proposed system becomes substantially smaller. This paper is about the effectiveness of multimodal biometric fusion system and presents tools employed to enhance it which is depicted by ROC curve.

Key words: unimodal, multimodal, ANOVA, wavelet feature extraction

I. Introduction

A biometric system presents automatic recognition of an individual based on some sort of unique feature or characteristic of the individual. Biometrics is the science of computerized recognition of persons based on one or more physiological or behavioural characteristics. Biometric system is based on fingerprints, facial features, voice, hand geometry, handwriting, the retina and iris. Biometrics is originated from Bio (means life) and Metrics (means system used for measurement)[1]. This means that biometrics means technology with the purpose of measuring and analyzing physiological or biological characteristics of living person for identification and verification purposes. Biometrics is widely used in many applications, such as access control to secure facilities, verification of financial activities such as transactions, welfare fraud protection, law enforcement, and immigration status checking when entering a country. The method of identification based on biometric characteristics is preferred over traditional passwords and PIN based methods for several reasons such as: The person to be identified is required to be physically present during the time of identification. Identification of individual based on biometric techniques obviates the need to remember a password or carry a token.

Performance Evaluation Parameters

= FRR (False Rejection Rate) - the frequency of rejections relative to people who should be correctly verified. When an authorized user is rejected he/she must represent his/her biometric characteristic to the system. Note that a false rejection does not mean necessarily an error of the system; for example, in the case of a fingerprint-based system, a incorrect positioning of the finger on the sensor or dirtiness can produce false rejections.

= FAR (False Acceptance Rate) - the frequency of fraudulent accesses due to impostors claiming a false identity.

II. Multimodal biometrics

In unimodal biometric systems, we face a variety of problems such as noisy data, intra-class variations, restricted degrees of freedom, non-universality, spoof attacks, and unacceptable error rates. The limitations imposed by unimodal biometric systems can be overcome by using multiple sources of information for establishing identity. Such systems are known as multimodal biometric systems[3]. These systems are more reliable due to the presence of multiple independent pieces of evidence. These systems are able to meet the performance requirements of various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. Spoofing is not possible in multimodal biometric system because it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. In other words,Multimodal biometric systems are those that utilize more than one physiological or behavioral characteristic for enrollment, verification, or identification. In applications such as border entry/exit, access control, civil identification, and network security, multi-modal biometric systems are looked to as a means of

1) Reducing false non-match and false match rates,
2) Providing a secondary means of enrollment, verification, and identification if sufficient data cannot be acquired from a given biometric sample, and
3) Combating attempts to fool biometric systems through fraudulent data sources such as fake fingers.

A multimodal biometric verification system can be considered as a classical information fusion problem i.e. can be thought to combine evidence provided by different biometrics to improve the overall decision accuracy. Generally, multiple evidences can be integrated at one of the following three levels.

– Abstract level: The output from each module is only a set of possible labels without any confidence value associated with the labels; in this case a simple majority rule may be used to reach a more reliable decision.

- Rank level: The output from each module is a set of possible labels ranked by decreasing confidence values, but the confidence values themselves are not specified.
- Measurement level: the output from each module is a set of possible labels with associated confidence values; in this case, more accurate decisions can be made by integrating different confidence values.

The reason to combine different modalities is to improve recognition rate. The aim of multi biometrics is to reduce one or more of the following:

- False accept rate (FAR)
- False reject rate (FRR)
- Failure to enroll rate (FTE)
- Susceptibility to artefacts or mimics

Multi modal biometric systems take input from single or multiple sensors measuring two or more different modalities of biometric characteristics. Multimodal system is a combination of two or more than two biometric traits of an individual for the identification purpose. Use of multimodal biometric system provides high security as compared to unimodal biometrics.

A. *Architecture of Multimodal Biometric System:*

Architecture of a multimodal biometric system refers to the sequence in which multiple cues are acquired and processed. There are two types : serial and parallel.

- Serial Architecture:In the serial or cascade architecture, the processing of modalities takes place sequentially and the outcome of one modality affects the processing of the subsequent modalities. Example, Bank ATMs.
- Parallel Architecture:In the parallel design, different modalities operate independently and their results are combined using an appropriate fusion scheme. Example, in military.

As multimodal biometric systems are better than unimodal biometric systems, we can use following three traits to form a multimodal biometric system.

III. FINGERPRINT RECOGNITION

Fingerprint recognition is one of the most popular and well-known biometrics. Because of their uniqueness, fingerprints have been used for recognition for over a century. Recently fingerprint recognition is becoming automated (i.e. a biometric) due to advancements in computing capabilities. Today fingerprint biometrics is one of the most popular, widespread, reliable and efficient biometric technology available. Due to versatility of fingerprint biometrics, these are applicable in almost all areas which require clear identification. Fingerprints are distinct to each person because of unique papillary features which are different even in twins. Fingerprint patterns remain unchanged throughout the entire adult life and that's why easily used for identification. In any case if a finger is damaged, other fingers that are previously enrolled into the system can also be used for identification. Fingerprint identification is based on two basic premises:

- Persistence: the basic characteristics of fingerprints do not change with time.
- Individuality: the fingerprint is unique to an individual.

IV. HUMAN IRIS

Due to many colors, iris is known as "Goddess of the Rainbow", which is a Greek word. The thin portion between the dark pupil and white sclera is iris. In human eye, iris is the colored part which is placed behind the cornea. Iris is protected by the eyelid and is responsible for controlling the diameter and size of the pupil. The major function of adjusting the size of the pupil is done by the iris sphincter and the dilator muscles. There is only one internal part of the human body which is normally externally visible that is iris. Iris is completely developed at the age of eight months or so and remains same for the whole life. The color of the iris is often referred to as "eye color" because it is responsible for the color of the eye. The iris of the eye has been described as the ideal part of the human body for biometric identification for several reasons:

It is an internal organ that is well protected against damage and wear by a highly transparent and sensitive membrane (the cornea). This distinguishes it from fingerprints, which can be difficult to recognize after years of certain types of manual labor.

The iris is mostly flat, and its geometric configuration is only controlled by two complementary muscles that control the diameter of the pupil. This makes the iris shape far more predictable than, for instance, that of the face.

V. FACE RECOGNTION

The least intrusive and fastest biometric technology is the face recognition. This technology works with the recognition of human face. Unlike other recognition system in which people need to place their hands on a reader or precisely position their eye in front of the scanner, face recognition system takes picture of people's face as they enter a defined area. This system works without any delay. Even in most cases the people are entirely unaware of this process.[6] Face recognition includes the position/size/shape of the eyes, nose, cheekbones and jaw line. There are few barriers to universality associated with this biometric such as hair, glasses ,age. Face images can be captured from a distance without touching the person being identified, and the identification does not require interacting with the person. In addition, face recognition serves the crime deterrent purpose because face images that have been recorded and archived can later help identify a person. Face scanning biometric tech is incredibly versatile and this is reflected in its wide range of potential applications.

However, there are few disadvantages associated with it. The main disadvantage of face recognition is similar to problem of photographs: people who look alike can fool the scanners. There are many ways in which people can significantly alter their appearance and slight changes in facial hair are one way to fool the device. Different poses do affect the entire process. Because pictures of the same person taken from different positions will be different. Also some systems have difficulty in maintaining high levels of performance as the database grows in size.

VI. FUSION IN MULTIMODAL BIOMETRIC SYSTEMS

In multimodal biometrics we use more than one biometric modality; we have more than one decision channels. We need to design a mechanism that can combine the classification results from each biometric channel; this is called as biometric fusion. Multimodal biometric fusion combines measurements from different biometric traits to enhance the strengths and diminish the weaknesses of the individual measurements.

VII. Fusion levels

Multimodal Biometrics with various levels of fusion: sensor level, feature level, matching score level and decision level.

A. *Sensor Level Fusion:*

In sensor Fusion we combine the biometric traits coming from sensors like Thumbprint scanner, Video Camera, Iris Scanner etc, to form a composite biometric trait and process.

B. *Feature Level Fusion:*

In feature level fusion signal coming from different biometric channels are first preprocessed, and feature vectors are extracted separately, using specific fusion algorithm we combine these feature vectors to form a composite feature vector. This composite feature vector is then used for classification process.

C. *Matching Score Level:*

Here, rather than combining the feature vector, we process them separately and individual matching score is found, then depending on the accuracy of each biometric channel we can fuse the matching level to find composite matching score which will be used for classification.

D. *Decision Level Fusion:*

Each modality is first pre-classified independently. The final classification is based on the fusion of the outputs of the different modalities.

Multimodal biometric system can implement any of these fusion strategies or combination of them to improve the performance of the system.

E. *Advantages of Multimodal Biometric Systems:*

1) Accuracy: Multi-modal biometric uses multiple modalities to identify a person which ensures higher accuracy.
2) Security: Multi-modal biometric systems increase the level of security by eliminating any chance of spoofing. It is unlikely that a person would be able to spoof multiple types of biometric traits at once.
3) Liveness Detection: Multi-modal biometric systems ask end users to submit multiple biometric traits randomly which ensures strong liveness detection to protect from spoofing or hackers.
4) Universality: A multimodal biometric system is universal in nature, even if a person is unable to provide a form of biometric due to disability or illness, the system can take other form of biometric for authentication.
5) Cost-effective: Multimodal biometric systems are cost effective by providing higher levels of security to lessen the risk of breaches or criminal attacks.

Though time taken in multimodal biometric systems is larger than the unimodal systems still it is used in place where security is the chief concern. By using appropriate normalization technique and fusion technique it is possible to achieve a high security multimodal biometric system.

VIII. Cognitive biometrics

Recently, a new trend has been developed that merges human perception to computer database in a brain-machine interface. This approach has been referred to as cognitive biometrics. Cognitive biometrics is based on specific responses of the brain to stimuli, which could be used to trigger a computer database search. Cognitive biometrics is a new authentication scheme that utilises the cognitive, emotional, and conative state of an individual as the basis of user authentication and/or identification.

IX. Social acceptance and privacy issues

Human factors dictate the success of a biometric based identification system to a large extent. The ease and comfort in interaction with a biometric system contribute to its acceptance. For example, if a biometric system is able to measure the characteristic of an individual without touching such as those using face, voice, or iris, it may be perceived to be more user friendly and hygienic. Additionally, biometric technologies requiring very little cooperation or participation from the users (e.g., face and face thermograms) may be perceived as being more convenient to users. On the other hand, biometric characteristics that do not require user participation can be captured without the knowledge of the user, and this is perceived as threat to privacy by many individuals. The very process of recognition leaves behind trails of private information. The issue of privacy becomes more serious with biometric based recognition systems because biometric characteristics may provide additional information about the background of an individual. For example, retinal patterns may provide medical information about diabetes or high blood pressure in an individual. A health insurance company may use this information in an unethical way for economic gains bt denying benefits to a person determined to be of high risk.

X. Literature review

Dinakardas CN et al(2013) [1]:proposed a multimodal system in which they use PCA (Principal component analysis), Fisher face projection, minutia extraction and LBP (Local Binary Pattern) for Face, Fingerprints and Iris traits. They use two different methods to compare the results. In first method PCA is used to extract the features of fingerprint and iris, and fisherface is used for the face image. In second method fisherface is used for face, minutiae extraction for fingerprints and LBP feature for iris image. The performance of the system was tested on real time database which consists of 500 images of iris, fingerprints and face. They compare PCA and PCA with Fisherface technique in terms of sensitivity and from there results it shows that PCA with Fisherface works more efficiently than PCA. The Receiver Operating Characteristics also shows that the proposed methods are superior compared to other techniques under study.

S.Anith et al(2013) [2]:presented a forensic face recognition which is robust to changes with age, pose, expression and illumination. It has a pre-processing stage in which all the background information including the hairy parts in the face is removed by thresholding. After preprocessing, the thresholded image is divided into macroblocks. The scale invariant feature points are extracted from all the blocks by means of Scale Invariant Feature

Transform. These extracted feature points are further refined by Taylor transformation technique and dominant orientation is assigned to every feature point.

Nadir Naurain Dawoud and Brahim Belhaouari Samir(2011) [3]:examined wavelets functions in order to choose the best wavelet for face classification process and for finding the optimal number of levels of decomposition. In this paper, seven wavelet functions namely Symelt, Daubechig, Coiflets, Mayer Discrete, Biorthogonal, Reverse Biorthogonal and Haar were tested with different number of decomposition levels and different number of biggest coefficients is selected to reduce the huge feature dimension, and for the classification purpose the Euclidean Distance Method (EDM) was used. Also a statistical method has been proposed to produce new metric of features coefficients, the experiments brought about 40% improvements in comparison to the method that accounts the biggest coefficients from the four levels of decompositions. The experiments have been performed on Olivetti Research Laboratory database (ORL) and Yale University database (YALE). The result showed the effect of wavelets proprieties on classification process and the Symelt wavelets were shown to be optimum wavelets for the face classification with four levels.

Le Hoang Thai and Ha Nhat Tam (2010) [4]: described the standardized fingerprint model which is used to synthesize the template of fingerprints. The synthesizing fingerprint model consists of four steps. These are, a) Preprocessing b) Finding and adjusting parameter sets c) Synthesizing fingerprints d) Post processing. They used FVC2004(DB4) fingerprint database for their research. They have done 800 synthesizing, 2800 matching between consistent and 79200 matching between inconsistent pairs to estimate the distribution of genuine and imposter matching respectively. The experiment results are compared to another results based on approach of Xiping Luo, 2000.FAR (fault acceptance ratio) of this model is very less as compares to Xiping luo's model.

Muhammed Razzak et. al(2010) [5]:presented the combination the face and finger veins in which multilevel score fusion is performed to increase the robustness of the authentication system. The score level fusion of client specific linear discriminant analysis (CSLDA) for fusion of face and finger veins result is performed. The score of face and finger veins are combined using weighted fuzzy fusion. This system is efficiency in reducing the FAR 0.05, FRR 0.23 and the accuracy of the system is 95%.

Nageshkumar.M, Mahesh.PK and M.N. Shanmukha Swamy(2009) [6]:proposed Biometrics based personal identification system which is usually regarded as an effective method for automatically recognizing, with a high confidence a person's identity. A multimodal biometric systems consolidate the evidence presented by multiple biometric sources and typically better recognition performance compare to system based on a single biometric modality. This paper proposes an authentication method for a multimodal biometric system identification using two traits i.e. face and palmprint. The proposed system is designed for application where the training data contains a face and palmprint. Integrating the palmprint and face features increases robustness of the person authentication. The final decision is made by fusion at matching score level architecture in which features vectors are created independently for query measures and are then compared to the enrolment template, which are stored during database preparation. Multimodal biometric system is developed through fusion of face and palmprint recognition.

Adams Kong et al(2009) [7]: described that palmprint recognition has been investigated over 10 years. During this period, many different problems related to palmprint recognition have been addressed. This paper proposed an overview of current palm- print research, describing in particular capture devices, preprocessing, verification algorithms, palmprint- related fusion, algorithms especially designed for real-time palmprint identification in large databases and measures for protecting palmprint systems and users' privacy. Finally, some suggestion is offered.

XI. Problem Defination

Dinakardas CN et.al proposed an multimodal recognition system that combined results from both PCA (principal component analysis), Fisher Face Projections, minutia extraction and LBP(Local Binary Pattern) feature extraction on different biometric traits. This identification system used the face, fingerprints and iris of a person for recognizing a person. They used two different methods for comparing the performance. The first model used principal component analysis to extract the features of the fingerprint and iris image, and fisherfaces for the face image. The second method used fisherface for face, minutiae extraction for fingerprint and LBP feature for iris image.

- The problem with the existing paper is that there is nothing mentioned about pre-processing of face, iris and fingerprint.
- There is approx. 95% accuracy in the existing system which can be improved.

XII. Objectives

In the proposed work, efforts will be made to achieve some improvements for example to improve recognition rate, standard deviation, confidence interval. Also to calculate new parameters like FAR (Fault acceptance rate) and FRR (Fault Rejection Rate). To achieve it, pre-processing of every unimodal system in proposed system shall be done separately.

1) To segment and normalize the iris before feature extraction.
2) To enhance and segment the fingerprint before feature encoding.
3) To do the pre-processing of biometric traits.
4) To improve the accuracy of the existing system.

XIII. Methodology

Implementation of the following preprocessing steps will be done before every unimodal system as depicted below:

- Separately pre-processing of every unimodal system, like for Iris recognition, segmentation and normalization processes shall be performed.
- For fingerprint recognition, Image enhancement and segmentation shall be performed and then feature encoding shall be done.
- For image recognition, Image enhancement and feature extraction is done and then fusion of the individual matrix for matching will be done.

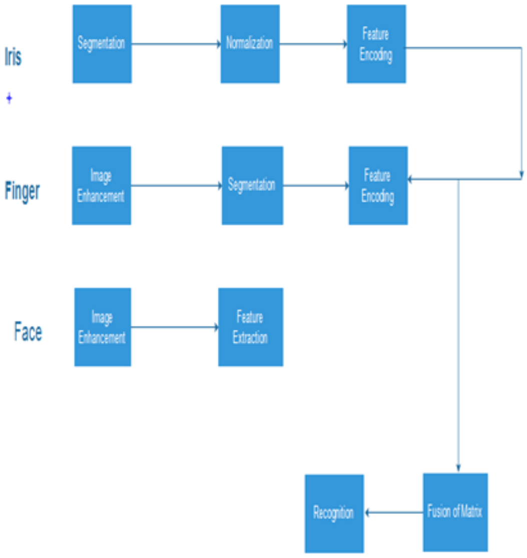

Fig. 1:

XIV. Implementation

A. *Human Iris:*

B. *Segmentation:*

Circular Hough transform based approach is used here for detecting the upper and the lower eyelids of the eye, and the iris and pupil boundaries. This procedure involves generation of an edge map, which is done through employing Canny edge detection technique. In this, gradients are biased in the vertical direction for the outer iris (sclera boundary), as recommended by Wildes et al. system. On the other hand, gradients were weighted equally both in horizontal and vertical directions for the inner iris (pupil boundary).

XV. Results

The automatic segmentation method was employed successfully on both the dataset and a high success rate was achieved with the help of first database (especially provided for research). Through the implementation of first database, wide separation in the intensity of iris and pupil was observed due to which it became easy to detect the iris and pupil boundaries. Out of 190 iris image, 185 iris images achieved proper segmentation, i.e. approx. a total of 97.36% iris are properly segmented. The 2.64% eye images failed to achieve proper segmentation Due to low intensity variation on iris and pupil region.

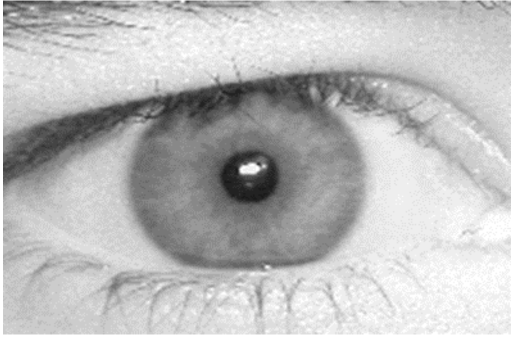

Fig. 2: input eye image

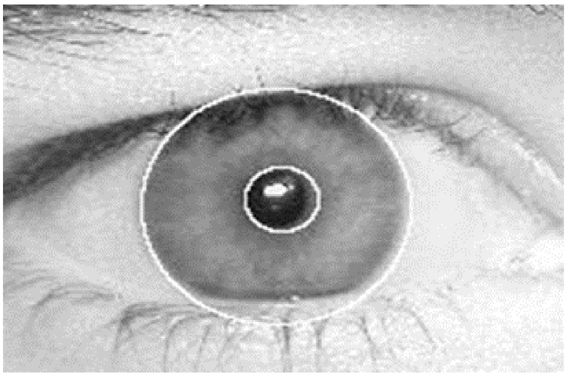

Fig. 3: Segmented eye image

Given below are some images where the segmentation failed due to the low intensity variation between the iris and the pupil regions.

So the figure depicted next shows improper segmentation

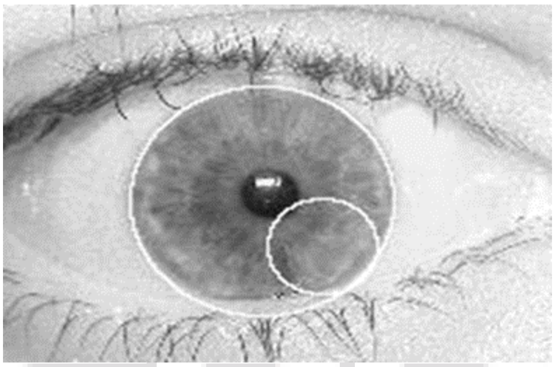

Fig. 4: Region of Improper Segmentation

XVI. Normalization and Enhancement

Daugman's rubber sheet model technique was employed to demonstrate the normalization of the iris regions. The reference point here refers to the centre of the pupil, and the radial vectors that are considered pass through the iris region. Along each radial line, a stable number of data points are selected which are referred to as the radial resolution and the angular resolution is defined as the total number of the radial lines that are available around the region of the iris. Since the pupil can sometimes be non-concentric to the region of the iris, therefore a remapping formula is employed to rescale the points depending upon the angle around the circle. This is given by:

$$r' = \sqrt{\alpha\beta} \pm \sqrt{\alpha\beta^2 - \alpha - r_1^2} \quad ..(1)$$

With $\alpha – o^2x + o^2y$

$\beta – \cos(\pi – \arctan(o_y / o_x) – \Theta)$

XVII. Fingerprint

A. *Pre-Processing:*

In pre-processing stage image enhancement and image binarization is performed.

B. *Image Enhancement:*

Fingerprint images need to be clear for easy processing, so for this image enhancement methods are used to make the images clear for advanced operations. As the images obtained from sensing devices like scanners are not considered of great quality that's why image enhancement methods are used to increase the contrast between valleys and ridges and is helpful for keeping the higher accuracy rate. For image enhancement we used two methods first is Histogram Equalization and second is Fourier Transform.

C. *Enhancement By Fourier Transform:*

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

$$F\,(u,v) = \sum_{x-0}^{M-1}\sum_{y-0}^{N-1} f\ (x,y)$$
$$\times \exp\left\{-j2\pi \times \left(\frac{ux}{M} + \frac{vy}{N}\right)\right\} \ldots.(2)$$

D. *Image Binarization:*

In binarization the information that is extracted from the print is in binary; valleys vs. ridges. This step is very important in ridge extraction as images taken are usually grayscale images. So, the purpose of binarization is to convert 256-level image into 2-level image that presents the same information. Usually in binarization pixels that belongs to an object are given a value of "1" while the other pixels which belongs to background are given a value of "0". The problem in performing binarization is that all fingerprint images have not same contrast characteristics, so we cannot use global thersholding. For this we use a locally adaptive method to binarize fingerprint images. In locally adaptive method we calculate the mean intensity value.

E. *Image Thinning:*

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

F. *Result:*

The fingerprint recognition system has been tested on FVC2002 DB1-B. An image is of size 560*296. Performance evaluation criteria used is false accept rate (FAR) and false reject rate (FAR). According to the results the obtained FRR is 3.17% at FAR 2.08%.

XVIII. FACE RECOGNITION

A. *Histogram Equalization:*

When Histogram equalization is applied to an image it expands the distribution of pixel values. It enhances the contrast between valleys and ridges. Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information. This method usually increases the global contrast of many images, especially when the usable data of the image is represented by close contrast values. Through this adjustment, the intensities can be better distributed on the histogram. This allows for areas of lower local contrast to gain a higher contrast. Histogram equalization accomplishes this by effectively spreading out the most frequent intensity values.

B. *Feature Extraction:*

Feature extraction methodologies analyse signals to extract the most prominent features that are representative of the various classes of signals. The main aim of feature extraction is to obtain the further information from the raw signal.

C. *Anova:*

Analysis of variance (ANOVA) is a collection of statistical models used to analyze the differences among group means and their associated procedures (such as "variation" among and between groups), developed by statistician and evolutionary biologist Ronald Fisher. In the ANOVA setting, the observed variance in a particular variable is partitioned into components attributable to different sources of variation. In its simplest form, ANOVA provides a statistical test of whether or not the means of several groups are equal, and therefore generalizes the t-test to more than two groups. ANOVAs are useful for comparing (testing) three or more means (groups or variables) for statistical significance. It is conceptually similar to multiple two-sample t-tests, but is less conservative (results in less type I error) and is therefore suited to a wide range of practical problems. ANOVAs assess the importance of one or more factors by comparing the response variable means at the different factor levels.

D. *Wavelet Feature Extraction:*

Wavelet transform forms a general mathematical tool for signal processing. Its basic use includes time-scale signal analysis, signal decomposition and signal compression. The set of wavelet functions is usually derived from the initial (mother) wavelet h(t). 2D wavelets for encoding the iris, face, fingerprint pattern data. The mother wavelet is defined as the second derivative of a smoothing function θ(x).

$$\psi(x) = \frac{d^2\theta(x)}{dx^2} \ldots\ldots\ldots\ldots\ldots.(3)$$

The zero crossings of dyadic scales of these filters are then used to encode features. The wavelet transform of a signal f(x) at scale s and position x is given by

$$w_s f(x) = f * \left(s^2 \frac{d^2\theta(x)}{dx^2}\right)(x)$$
$$= s^2 \frac{d^2}{dx^2}(f * \theta_s)(x)$$

E. *Matching:*

For the comparison of the two binarized fused matrix, the hamming distance algorithm is employed. Since the iris region contains features with very high degrees of freedom, and each iris produces a bit-pattern which is independent to that produced by another iris, whereas the codes produced by the same iris would be similar. If two bits patterns are completely independent, then the ideal Hamming distance between the two patterns will be equal to 0.5. It happens because independent bit pattern are completely random. Therefore, half of the bits will agree and half will disagree between the two patterns. The Hamming distance is the matching metric employed by Daugman, and calculation of the Hamming distance is taken only in bits that are generated from the actual iris region.

The Hamming distance will be defined as follows:

$$HD = \frac{1}{N}\sum_{j=1}^{N} X_j \oplus Y_j \ldots\ldots\ldots\ldots\ldots(4)$$

XIX. Results

To evaluate the performance of the proposed method, the proposed multimodal biometric system is implemented in MATLAB R2012a and the laptop of 1.85GHz processor and 1GB RAM is used to run our prototype model. The values of various parameters like FAR, FRR and EER are calculated and it is clear from the results that performance of the proposed system is improved as compared to the existing systems. The proposed system has values as FAR 0.005%, FRR as zero and EER as 0.0025%. ROC curve is plotted using true positive rate against false positive rate and the area under ROC curve is found to be 0.99% which makes the system much efficient than the existing systems.

Parameters	D. das[9]	Proposed method
Az	0.9620	0.99
S.D	0.0137	0.012
CI	0.9351	0.9901

Table 1: Comparison with existing research

Some additional parameters are also computed which are depicted in the table shown below:

Parameter	Value
FAR	0.005%
FRR	0
EER	0.0025

Table 2: Parameters calculated in proposed work

where the False Acceptance Rate (FAR) and the False Rejection Rate (FRR), defined as the accepting of a false person and rejecting of a genuine person for a given value of hamming distance respectively.

A threshold value is chosen that reaches EER where FAR=FRR. This is shown with the help ROC curve as:

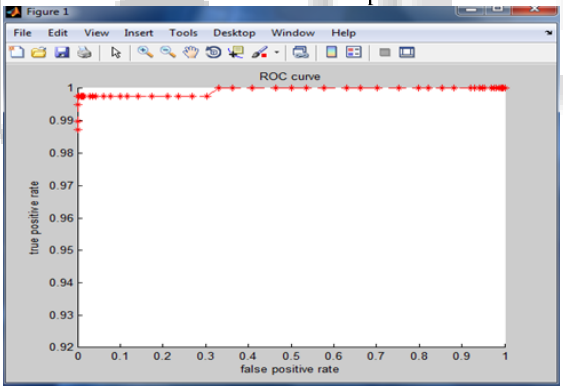

Fig. 5: Receiver operating characteristics curve

Receiver operating characteristics (ROC) curves are an accepted method for summarizing the performance of imperfect pattern matching systems. An ROC curve plots, parametrically as a function of decision threshold, the rate of “false positives” (i.e. impostor attempts accepted) on the x-axis, against the corresponding rate of “true positives” (i.e. genuine attempts accepted) on the y-axis.

Authors	FAR (%)	FRR (%)
Mohamad Abdolahi *et al*	2	2
Sheetal choudhary *et al*	2	2
HunnyMehrotra *et al*	1.58	6.34
Nageshkumar M *et al*	2.4	0.8
R. Gayathri *et al*	1.6	0.8
Le Hoang Thai *et al*	3.57	2.5
Proposed system	0.0005	0.1

Table 3: Comparison table of FAR and FRR

XX. Conclusion

With advancement of technology, and increasing frauds there is need of high security systems which have obviously high degree of accuracy, increased and reliable recognition, vulnerability and user acceptance. Such a system is multimodal biometric system and this is the reason to embark study in this domain. This paper comprises of introduction to biometrics system followed by multimodal biometric system emergence. After that the survey of various papers were conducted which depicts several techniques employed to fuse one or more biometric traits. Among these papers, the base paper taken takes into consideration the three biometric traits namely : fingerprint, iris and face. The methods employed for fusion yields results which gives optimum accuracy but there was still scope of improving accuracy by employing methods such as preprocessing of each unimodal system and employment of techniques such as wavelet feature extraction and ANOVA followed by metafusion, the accuracy of the system depicted a significant improvement .Thus, improved accuracy justifies the entire processing procedure of the proposed system which inturn reduces the complexity of the system.

XXI. Future scope

The proposed multimodal biometric system can be enhanced and extended with regard to various situations and conditions. Human Iris:If the person is wearing spectacles or any other individual who is wearing contact lenses. Another complexity arises from the fact that a person who has undergone cataract surgery (in which the natural lens of eye is replaced with an artificial lens) or surgery to get rid of spectacles (most commonly referred to as LASIK LASER). With taking above complexities under consideration, proposed system can be extended.

Fingerprint: The proposed system is limited if situations arises such as: there is oil applied on the fingers of a person or the fingers could be little damaged due to injury or skin rashes ,cuts, wounds, swelling due to certain reasons leading the proposed system realising its limitation. So by taking these limitations under consideration, the proposed system can be enhanced to accommodate certain features which take into account such situations.

Face Recognition: if a person is wearing intense make-up then layers of bases applied on skin may cause significant reduction of distances between eyes, nose, mouth and jaw edges. A lot of other facial features gets modified such as winged eye lashes, prosthetics, silicon implants, facial hairs. Moreover, limitations can possibly arise from the fact that a person if subjected to medical procedure may have scars and pimples or uneven surface, one such condition could be chicken pox or small pox.

References

[1] Dinakardas CN, Dr.S Perumal Sankar and Nisha George, “A Multimodal Performance Evaluation on Two Different Models Based on Face, Fingerprint and Iris Templates”,IEEEInternational Conference on Emerging Trends in VLSI, Embedded System,Nano Electronics and Telecommunication System(ICEVENT),pp1-6, Jan 2013.

[2] S.Anith, D.Vaithiyanathan, and R.Seshasayanan,“Face Recognition System Based on Feature Extraction”,IEEE International Conference onInformation Communication Embedded

[3] S.Nadir Nourain Dawoud and Brahim Belhaouari Samir, “Best Wavelet Function For Face Recognition Using Multi-level Decomposition”,International Conference onResearchand Innovation in Information System(ICRIIS), pp1-6,Nov.2011.ystem (ICICES),pp 660-664, Feb.2013.

[4] Le Hoang Thai and Ha Nhat Tam, “Fingerprint recognition using standardized fingerprint model,”International Journal of Computer Science Issues (IJCSI) vol. 7, pp. 11-17,May 2010.

[5] Muhammed Imran Razzak, Rubiyah Yuosf and Marzuki Khalid, “Multimodal face and finger veins biometric authentication”, Scientific Research and Essays, Vol.5, No.17, pp. 2529-2534, 2010.

[6] Nageshkumar, M., P. K. Mahesh, and MN Shanmukha Swamy. "An efficient secure multimodal biometric fusion using palmprint and face image." arXiv preprint arXiv:0909.2373 (2009).

[7] Kong, Adams, David Zhang, and Mohamed Kamel. "A survey of palmprint recognition." Pattern Recognition 42.7 (2009): 1408-1418.