Iris and Fingerprint Fusion for Biometric Identification

Dipti.S.Randive
Department of Electronics and Telecommunication
Shri.Vithal Education and Research Institute's,
college of Engineering, Pandharpur, India.

Manasi.M.patil, Ph.D
Department of Electronics and Telecommunication
Shri.Vithal Education and Research Institute's,
college of Engineering, Pandharpur, India.

ABSTRACT
A biometric system which relies only on a single biometric identifier in making a personal identification is often not able to meet the desired performance requirement. The basic aim of a biometric identify system is to make distinction automatically between subjects in a reliable and dependable way, according to a specific-target application. Multimodal Biometric systems aim to fuse two or more physical or behavioral traits to provide optimal False Acceptance Rate (FAR) and False Rejection Rate (FRR), thus improving system accuracy and dependability. In an innovative multimodal biometric identify system based on Iris and fingerprint traits are proposed. Feature is extracted from preprocessed images of Iris and Fingerprint. These features of a query image are compared with those of a database image to obtain matching score and this score is fuse the final score is use to declare the person is accepted or rejected.

Keywords
Iris, Fingerprint, morphological operators, Haar wavelet, Hamming distance, Minutia matcher, Sum rule and Fusion.

1. INTRODUCTION
In a now a day's security systems take a more attention in public and private institute , organization which in security systems as visitor's identification, especially for building access control, suspect identification by police, driver's licenses, computer systems, laptops, cellular phones, ATMs and many other fields. In order to overcome the security problems biometric systems can be used. Pin numbers, email passwords, credit card numbers, and protected premises access numbers all have something in common. All of them are a key to your identity, and all of them can easily be stolen or guessed. Currently users have been encouraged to create strong passwords for every different domain. This leads to some logical problems. People tend to forget multiple, lengthy and varied passwords, therefore, they use one strong password for everything. This only allows the successful thief to gain access to all the protected information. The other option which follows is to carry a hard copy of each password which again can only be a reward for the quick pick-pocket. Technique for automated recognition or verification of identity of a person using unique physical or behavioral characteristics such as fingerprints, hand geometry, iris, voice, and signatures is required. Authentication procedures, based on the simple username as password approach, are insufficient to provide a suitable security level for the applications requiring a high level of protection for data and services. Biometric based identification systems represent a valid alternative approach to canonical approaches. Recent day some companies started use of unimodal biometric authentication to protect access to highly confidential information. You may be familiar with some of the physical characteristics used by biometric authentication program. Other biometric characteristics that can be measured include the voice, face, and the iris. However, this technology is very real and is currently being used in the private sector. Traditionally biometric identification systems, operating on a single biometric feature has many limitations, which are as given: 1) Trouble with data sensors, 2) Distinctiveness ability, 3) Lack of universality biometric features are universal, but due to the wide variety and complexity in the human body, not everybody is be gift with the same physical features. Due above limitation in single modal system, the recent approach become increase for multimode biometric system. These systems show significant improvements as compare to unimodal biometric systems, as higher accuracy and high capacity to resist spoofing. So here use two biometrics character iris and fingerprint. There is a sizeable amount of literature is available that details different approaches for multimodal biometric systems, which have been forth put in [5]–[8]. Multibiometrics data can be combined at different levels: fusion at data-sensor level, fusion at the feature extraction level, fusion at the matching level, and fusion at the decision level. As pointed out in [5], features-level fusion is easier to apply when the original characteristics are homogeneous because, in this way, a single resultant feature vector can be calculated. On the other hand, feature-level fusion is difficult to achieve because: 1) the relationship between the feature spaces could not be known; 2) the feature set of multiple modalities may be incompatible; and 3) the computational cost to process the resultant vector is too high.

In this paper, a template-level and matching score level using resulting in a unified biometric descriptor and integrating fingerprint and iris features is presented.

2. LITERATURE SURVEY
A fingerprint; face and speech based multimodal authentication system. They use minutiae based approach to detect fingerprint, Eigen face-based approach to detect faces and text dependent speaker recognition system using Hidden Markov Model (HMM) to detect Voice. The fusion is carried out in a parallel mode using rank level fusion at post-matching stage [1]. Conti *et al*. proposed a multimodal biometric system using two different fingerprint acquisitions. The matching module Integrates fuzzy-logic methods for matching-score fusion. Experimental trials using both decision-level fusion and matching-score-level fusion were performed. Experimental results have shown an improvement of using the matching score level fusion rather than a monomial authentication system [2]. Yang and Ma used fingerprint, palm print, and hand geometry to implement personal identity verification. Unlike other multimodal biometric systems, these three biometric features can be taken from the same image. They implemented matching score fusion at different levels to establish identity, performing a first fusion of the fingerprint and palm-print features, and successively, a matching-score fusion between the multimodal system and the palm-geometry unimodal system. The system was tested on a database containing the features self-constructed by 98 subjects [3]. Aguilar *et al.* proposed a multi biometric method using a combination of fast Fourier

transform (FFT) and Gabor filters to enhance fingerprint imaging. Successively, a novel stage for recognition using local features and statistical parameters is used. The proposed system uses the fingerprints of both thumbs. Each fingerprint is separately processed; successively, the unimodal results are compared in order to give the final fused result. The tests have been performed on a fingerprint database [4]. The proposed system uses the fingerprint, face, and hand geometry features of an individual for verification [5].Subbarayudu and Prasad presented experimental results of the unimodal iris system, unimodal palm print system, and multi biometric system (iris and palm print). The system fusion utilizes a matching scores feature in which each system provides a matching score indicating the similarity of the feature vector with the template vector. The experiment was conducted on the Hong Kong Polytechnic University Palm print database. A total of 600 images are collected from 100 different subjects [9]. A comparison between multiple fusion techniques at rank level by fusing face and iris to identify users and they also use an Eigen face-based approach to detect faces and employ an algorithm that characterizes local variations in iris for matching. The fusion techniques used for comparison include weighted sum, a Fisher discriminate analysis and neural network based classifier [10].The likelihood ratio (LR) test used in the Neyman-Pearson theorem directly maximizes the genuine accept rate (GAR) at any desired false accept rate (FAR) [11].Robert Hastings, Develop a method for enhancing the ridge pattern by using a process of oriented diffusion by adaptation of anisotropic diffusion to smooth the image in the direction parallel to the ridge flow. The image intensity varies smoothly as one traverse along the ridges or valleys by removing most of the small irregularities and breaks but with the identity of the individual ridges and valleys preserved [12].

3. MULTIMODEL BIOMETRIC SYSTEMS

Fusion strategies are divided into two main categories first is pre-mapping fusion i.e. before the matching phase, and second is post-mapping fusion i.e. after the matching phase. The first strategy deals with the feature-vector fusion level. Usually, these techniques are not used because they result in many practical problems. The second strategy is fusion at the decision level, based on some algorithms, which combine single decisions for each component of the system. Furthermore, the second strategy is also based on the matching-score level, which combines the matching scores of each component system. The biometric data can be combined at several different levels of the identification process. Input can be fused in the following levels (1)-(4).

1) Fusion at data-sensor level: Data coming from different sensors can be combined, so that the resulting information is in some sense better than single data. These sources of data were individually used for identification. The term better in case it gives more accurate, more complete and more dependable.

2) Fusion at feature-extraction level: The information extracted from sensors of different modalities is stored in vectors form on the basis of their classification. These feature vectors are then combined to create a joint feature vector, which is use for the matching and recognition process. One of the actually problems in this strategy is that, in some cases, a very high dimensional feature vector results from the fusion process are obtained. But, it is hard to generate homogeneous feature vectors from different biometrics in order to use a unified matching algorithm, as well as it required more memory to store data.

3) Fusion at decision level: With this approach, each biometric subsystem completes autonomously the processes of feature extraction, matching, and recognition. Decision strategies are usually of Boolean functions, where the recognition yields the majority decision among all present subsystems.

4) Fusion at template level: It is very difficult to obtain, since biometric features have different structures and distinctiveness. In this paper use two level fusion template level fusions and matching score level fusion. To generate a unified homogeneous template for fingerprint and iris features.

In this approach performs fingerprint matching using the segmented regions and minutia point on fingerprint On the other hand, iris preprocessing have aim to detect the circular region surrounding the iris as a result, adopted a Coarse to fine strategy equation, iris feature is extracted using haar wavelet, and obtaining a unified template. Successively, the HD and Minutia Matcher apply on the fused template for Iris and fingerprint respectively.

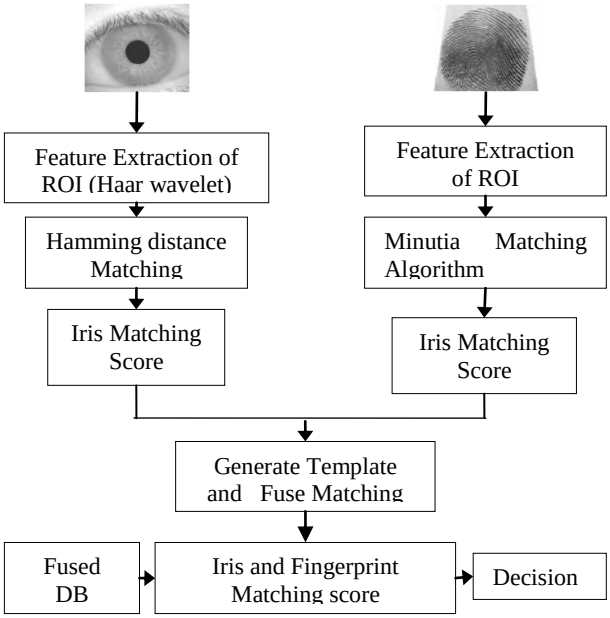

Fig:1 Multimodal system

Shown in Fig. 1, In this multimodal biometric system it having two main stages: the preprocessing stage and matching stage. Iris and fingerprint images are preprocessed to extract the region of interests, the iris region from eye and removing the eyelids and eyelashes which consider as disturbances in iris. The extracted features are used to generate iris code, and the classic minutiae-based approach is used to extract the features of fingerprint. The extracted region of interest is used as input for the matching stage. Two different matching algorithms is use for iris and fingerprint as HD matching algorithm, Minutia matching algorithm respectively. Then they are normalized, and obtain the matching score and fuse it using sum rule. If fused matching score is greater than the pre defined threshold then go for the decision. In this follows, each phase is briefly describe point.

3.1 Extraction of Iris

Iris is unique to each individual and remains constant over the life of a person. The iris is a thin circular diaphragm, which lies between the cornea and the lens of the human eye. The

iris is perforated close to its centre by a circular aperture known as the pupil. The pupil dilates when exposed to light and contracts in dark. Thus the size of pupil varies with respect to light it is exposed to. The iris is the annular ring between the sclera and pupil boundary and contains the flowery pattern unique to each individual. They are stable with age. Iris has extremely data rich physical structure having large number of features. It has inherent isolation and protection from the external environment. This texture information unique to each individual is extracted from rest of the eye image and is transformed into strip to apply pattern matching algorithm. Prior to implementation of steps mentioned above iris image has to be acquired which should be rich in texture because all subsequent stages depend upon the quality of image.

3.1.1 Image Acquisition

Image acquisition is considered the most critical step in this project since all subsequent stages depend highly on the image quality. In order to accomplish this used a CCD camera. The most compelling feature of iris camera is that have designed a circular NIR LED array, with suitable luminous flux for iris imaging. Iris camera can capture very clear iris images and set the resolution to 320*280, the type of the image to jpeg, and the mode to white and black for greater details. In this use CASIA database (Institute of Automation, Chinese Academy of Sciences, http://www.sinobiometrics.com/). CASIA-Iris-Interval (version4.0) database instead of capturing the eye images using camera. A fingerprint is the feature pattern of one finger. Each person has his own fingerprints with the permanent uniqueness. In this use CASIA fingerprint (version 5.0) database instead of capturing the fingerprint images using fingerprint sensor. The fingerprint images were captured using URU4000 fingerprint sensor in one session. All fingerprint images are 8 bit gray-level BMP files and the image resolution is 328×356.

3.1.2 Iris Localization

In Iris localization interest is detection of center coordinates and radius of pupil and Iris.

3.1.2.1 Pupil and Iris Detection

In pupil and iris detection eye images passing a minimum focus criterion were then resolve to find the iris, with clearly localization of its boundaries using a coarse-to-fine strategy terminating in single-pixel precision estimates of the center coordinates and radius iris and the pupil. Although the results of the iris search greatly constrain the pupil search, concentricity of these boundaries cannot be assumed. Very often the pupil center is nasal, and inferior, to the iris center. Its radius can range from 0.1 to 0.8 of the iris radius. Thus, all three parameters defining the pupillary circle must be estimated separately from those of the iris. A very effective integration differential operator for determining these parameters is:

$$\max(r, x_0, y_0) = \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right| \qquad (1)$$

Where I(x, y) is an image of eye. The operator searches over the image domain (x,y) for the maximum in the blurred partial derivative with respect to increasing radius r, of the normalized contour integral of I(x, y) along a circular arc ds of radius r and center coordinates (x_0, y_0). The symbol * denotes convolution and Gσ (r) is a smoothing function such as a Gaussian of scale σ. The complete operator behaves in effect as a circular edge detector, blurred at a scale set by σ, which searches iteratively for a maximum contour integral derivative with increasing radius at successively finer scales of analysis through the three parameter space of center coordinates and radius $(x_0;y_0;r)$ defining a path of contour integration. The results of the iris search greatly constrain (within close bounds) iris boundary is first detected and then pupil search, concentricity of these boundaries cannot be assumed. Very often the pupil center is shifted by up to 15% from center of the iris. Its radius can range from 0.1 to 0.8 of the iris radius. Thus, all three parameters defining the pupillary circle must be estimated separately from those of the iris. Figure 2 show both boundaries of pupil and iris boundaries.

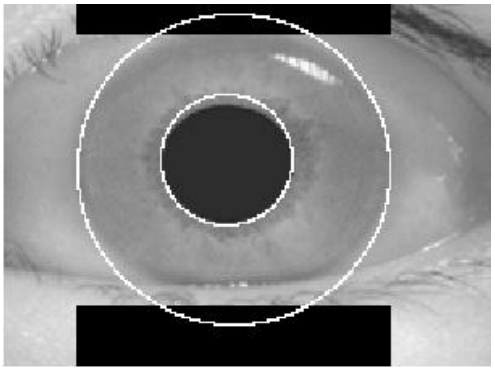

Fig: 2 Image with pupil and iris boundaries and Eyelids and eyelashes remove

3.1.2.2 Eyelids and eyelashes detection

Eyelids and eyelashes are considered to be "noise," and therefore, it seen to degrade the system performance. Eyelashes are of two types: separable eyelashes and multiple eyelashes. The eyelashes present in dataset belong to the separable type. Initially, the proposed method selects two search to detect upper and lower eyelids. The pupil centre, iris inner and outer boundaries are used as reference to select the two search regions. The search regions are confined within the inner and outer boundaries of the iris. The width of the two search regions is same with diameter of the Iris. The eyelid boundaries are normally occluded by the eyelashes. Eyelashes edge is detected using Canny detector. The next step, hysterisis thresholding, After finding the upper eyelids and lower eyelids, consider that as noise and remove it, as show in Figure 2.

3.1.2.3 Normalization of iris

When the iris image is proficiently localized, then the next step is to transform it into the rectangular sized fixed image format. The Daugman's Rubber Sheet Model is utilized for

the transformation process for Iris. Normalization process includes unwrapping the iris and transforming it into its polar equivalent form. It is performed utilizing Daugman's Rubber sheet model. The idea behind the dimensionless polar system is to assign an r and θ value to each coordinate in the iris that will remain invariant to the possible stretching and skewing of the image. The iris ring is mapped to a rectangular block in the anti-clockwise direction. Remapped image is called normalized image. The remapping of the iris image I (x, y) from raw Cartesian coordinate to polar coordinates I (r,θ) can be represented as,

$$I\,(x(r,\theta\,), y(r,\theta\,)) \rightarrow I\,(r,\theta\,) \qquad (1)$$

Where, r lies in the unit interval and θ is the angle between [0,2Π].Where x(r, θ) and y(r, θ) are defined as linear

combinations of both the set of papillary boundary points. The following formulas perform the transformation.

$$\left.\begin{aligned} X(r,\theta)&=(1-r)Xp\,(\theta)+\mathrm{Xi}\,(\theta) \\ Y(r,\theta)&=(1-r)Yp(\theta)+Yi(\theta) \end{aligned}\right\} \quad (2)$$

Where (Xp,Yp) and (Xi,Yi) are the coordinates on the pupil and limbus boundaries along the θ direction. Eye image unroll it (map it to Cartesian coordinates) .Normalization produces the image of unwrapped iris region of size 20×240.After normalization of unwrapped iris this is polar form of iris then find the value of polar which are not a number then that is average. It use for feature extraction.

3.1.3 Feature Extraction using Haar wavelet

Features are the attributes or values extracted to get the unique characteristics from the image. Features from the iris image are extracted using Haar Wavelet decomposition process [22].

In the wavelet decomposition the image is decomposed into four coefficient i.e., horizontal, diagonal, vertical and approximation, at 3rd, 4th or 5th level decomposition. Last level coefficients are converting information to form a vector. Here use only 3^{rd} level horizontal coefficient of vector size 3×30 pixel. The vector is binaries due to that the easy comparisons between the iris codes for database and query image is take pales, and it convert into binary code to generate Iris code as:

$$\left.\begin{aligned} &\text{If Coef (i) > 0 then Coef (i) = 1} \\ &\text{If Coef (i) < 0 then Coef (i) = 0} \end{aligned}\right\} \quad (3)$$

3.2 Fingerprint minutiae Extraction

Fingerprint is second main biometric traits which is use for fusion. Fingerprint is one of the most widely used biometric modality. The main reason behind the use of fingerprint biometric is that it is the most proven technique to identify the individual. The fingerprint is basically the combination of ridges and valleys on the surface of the finger. The use of minutiae feature for single fingerprint classification has been introduced in [23-24].

3.2.1 Image Enhancement

Fingerprint Image enhancement is to done to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality. For increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink are very useful for keep a higher accuracy to fingerprint recognition. Histogram Equalization and Fourier Transformer adopted in fingerprint enhancement. Histogram equalization is to expand the pixel value distribution of an image so as to increase the perceptional information, and Fourier transform divide the image into small processing blocks (32by 32 pixels) and In order to enhance a specific block by its dominant frequencies, multiply the FFT of the block by its magnitude a set of times and get Enhanced fingerprint image (Figure 3 (b)).

(a) Original image **(b) Enhanced Fingerprint**

Fig 3: Enhanced Fingerprint Image

3.2.2 Image Binarization

Enhanced fingerprint image is than binarized as In Fingerprint Image binarization is process to transform gray image into binary image in system it use for transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black color while furrows are white. A locally adaptive binarization method is performed to binaries the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block is 16x16 to which the pixel, then from the binarized image estimates the direction for fingerprint.

3.2.3 Image Segmentation

Image segmentation is useful to feature extraction to be recognized for each fingerprint image. The image area without effective ridges and furrows are first disposed since it can hold only background information. Then the bound of the remaining effective area is look out since the minutia in the bound region are confuse with those are counterfeit minutia that are generated when the ridges are out of the sensor. To extract the ROI, two-step methods are used. The first step is block direction appraisal and direction variety check [21], while the second is intrigued from some Morphological methods.

3.2.4 Minutiae Extraction

For minutia extraction stage, three thinning algorithms are tested and the Morphological thinning operation is finally given out with high efficiency and pretty good thinning quality. For this stage, a more rigorous algorithm is developed to remove false minutia based. Also a new co-ordinate representation for bifurcations in fingerprint is proposed to unify terminations and bifurcations.

3.2.4.1 Ridge Thinning

Ridge Thinning is to removes the redundant pixels of ridges till the ridges are just one pixel narrow. In each scan of the full fingerprint image, the algorithm marks down redundant pixels in each small image window (3x3 pixel). And finally removes all those marked pixels after several scans. In my testing, such an In this method select ridges has maximum gray intensity value. However, binariestion is implicitly strong that only pixels have maximum gray intensity value are remained. In the testing, the advancement of each selecting step has large number of complexity although it does not require the movement of pixel by pixel as in other thinning algorithms. Use morphological thinning function in MATLAB and thinned fingerprint image (Figure 4).

Fig 4: Thinned fingerprint image

3.2.4.2 Minutia Marking

After the fingerprint ridge thinning, marking minutia points is relatively easy. But it is still not a trivial task as most literatures declared because at least one special case evokes my caution during the minutia marking stage. Minutia marking stage where mark the ridged and bifurcation of fingerprint. Minutiae are extracted by scanning the 3x3 window across each ridge pixel which determines the CN value is use in many system in this it consider 8 neighbors, but in this system divide thinned image in 16×16 processing block and perform the scanning and it have a 3×3 window. Then interest in find the Neighbors Value. Neighbor value (NV) is calculated and then find the number of Neighbors (NN) as equations:

$$\left.\begin{array}{l} NV = \sum_{i=-1}^{1}\sum_{j=-1}^{1}(p_i, p_j) \\ \\ NV = NV - 1 \end{array}\right\} \quad (4)$$

This number of neighbor's value is determines a ridge pixel either to be an ending, bifurcation or non-minutiae point. The minutia marking, all thinned ridges in the fingerprint image are labeled with a unique ID for further operation. The labeling operation is realized by using the Morphological operation: BWLABEL.

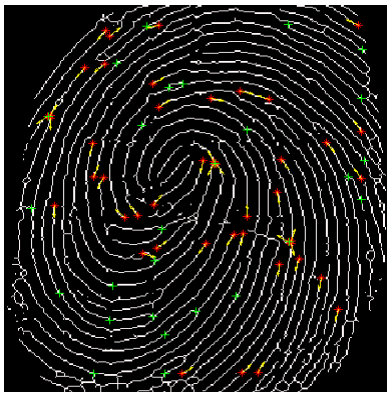

Fig 5: Marked Minutia

Extracted number of minutia as show in figure 5, it plot on fingerprint image by using plot function where red and green color represent end and branch respectively, minutia are occurred in fingerprint after minutia marking.

Each minutia is completely characterized by the following parameters at last: A) x-coordinate, B) y-coordinate, and C) orientation. So for it adopt the unification representation for both termination and bifurcation.

3.3 Matching Algorithm

3.3.1 Fusion

Fusion is performed by combining two feature vectors extracted from every pair of fingerprints and irises and stored in the mat file using append operation of mat lab. The homogenous biometric vector from fingerprint and iris data is composed of binary sequences representing the unimodal biometric templates. The proposed approach is based on a pair recognition of fingerprint and iris, and every part provides its own Matching score. Then Iris and Fingerprint Matching score is fused using simple sum rule. If the Fused matching score is larger than a pre-specified threshold, then the parson is accepted or rejected so it is clear that nobody can be accepted unless fused score of the results are greater than pre-specified threshold. Matching score for Iris is calculated through Hamming distance (HD) between two final fused templates.

$$\mathrm{HD} = \frac{1}{\mathrm{N}}\sum_{\mathrm{i}=1}^{\mathrm{N}} \mathrm{XOR}(\mathrm{X_A(i)}, \mathrm{Y_B(i)}) \quad (4)$$

Where, X_A and X_B are the coefficients of two iris images and N the size of the feature vector. For fingerprint minutia matcher is use it have two stages Alignment stage and Match stage. The matching algorithm for the aligned minutia patterns needs to be elastic since the strict match requiring that all parameters (x, y, θ) are the same for two identical minutia is impossible due to the slight deformations and in exact quantization of minutia.

$$MS = F_{iris} + F_{Fingerprint} > Threshold \quad (5)$$

The elastic matching of minutia is achieved by placing a bounding box around each template minutia. If the minutia to be matched is within the rectangle box and the direction discrepancy between them is very small, then the two minutia are regarded as a matched minutia pair. Each minutia in the template image either has no matched minutia or has only one corresponding minutia. The final match ratio for two fingerprints is the number of total matched pair over the number of minutia of the template fingerprint. The score is 100*ratio. Then matching score of fingerprint is fused with matching score of iris using sum rule.

4. EXPERIMENTAL RESULTS

The given multimodal biometric authentication system achieves interesting results on standard as well as commonly used databases. To show the effectiveness of approach, take test on different database, First test take on The CASIA-Iris-V1 database [22] and the FVC2004DB2A fingerprint database [22] have been used for fingerprints and irises, respectively. The obtained experimental results, in terms of recognition rates and execution times, are here outlined. The listed FAR and FRR indexes have been calculated following the FVC guidelines.

Second test the CASIA-Iris-Interval-V4 [23] and CASIA-Fingerprint-V5 database. The results are tested on iris and fingerprint images collected by the authors. The database consists of three iris images (60×2) and two fingerprint images (60×2) per person with total of 60 persons. The iris images are acquired using CCD camera, and that have designed a circular NIR LED array.

Iris camera capture very clear iris images and set the resolution to 320*280, the type of the image to jpeg, and the mode to white and black for greater details. That is CASIA-Iris-Interval-V4 database. However, the fingerprint images of CASIA-FingerprintV5 were captured using URU4000 fingerprint sensor.

Table: 1 Database composition for Test

Test set	Used Iris database	Used fingerprint database	User
DB[A]test1	CASIA Iris V1	FVC2004DB2A	55
DB[B]test2	CASIA Interval V4	CASIA Fingerprint V5	55

4.1 Recognition Analysis of the Multimodal System

The multimodal recognition system performance evaluation has been performed using the well-known FRR and FAR indexes. For an authentication system, the FAR is the number of times that an incorrectly accepted unauthorized access occurred, while the FRR is the number of times that an incorrectly rejected authorized access resulted. First iris and fingerprints algorithms are tested individually as unimodal. To evaluate and compare the performance of the proposed approach, several tests have been conducted. The first test has been conducted on the full FVC2002 DB2A database using unimodal minutiae-based recognition system. This approach has resulted in FAR= 3.33%and FRR=15.00%. The performance of the fingerprint unimodal recognition system using the previously described frequency-based approach on the same full CASIA-Fingerprint V5 database has also been evaluated. This approach has resulted in FAR = 3.30% and FRR =16.66%. Table 2 shows the achieved results of all models. Finally, following the items listed in Table 1, DB[A]test1 and DB[B]test2 datasets have been considered to further evaluate the proposed fusion strategy.

Table: 2 FAR and FRR of Proposed Multimodal Result Compared to Unimodal Databases Reduced to 55 Users

Biometric System	Database	FAR	FRR
Iris Unimodel (Haar wavelet)	CASIA Iris V1	0.066	0.133
Iris Unimodel (Haar wavelet)	CASIA Iris Interval V4	0.083	0.1
Fingerprint unimodel (Minutiae Matching)	FVC 2004 DB2A	0.033	0.15
Fingerprint unimodel (Minutiae Matching)	CASIA FP V5	0.033	0.166
Multimodel (Haar wavelet Minutiae)	DB[A]test1	0	0.09
Multimodel (Haar wavelet Minutiae)	DB[B]test2	0	0.054

Table 2 shows the achieved results in terms of FAR and FRR indexes. The results achieved by the two unimodal recognition systems on the same pertinent databases are also reported in Table 2.

An initial test has been conducted on the DBtest1 dataset using a proposed fusion approach at the matching-score level. obtained: FAR=0% and FRR=9.00%. as in Table 2. Table 2 shows the achieved results in terms of FAR and FRR indexes. As shown in Table 2, the conducted tests produce comparable results on the used datasets, underlying the presented approach robustness. Figure 4 shows the Receiver operating characteristic (ROC) curves for the systems dealing with the DBtest2 dataset.

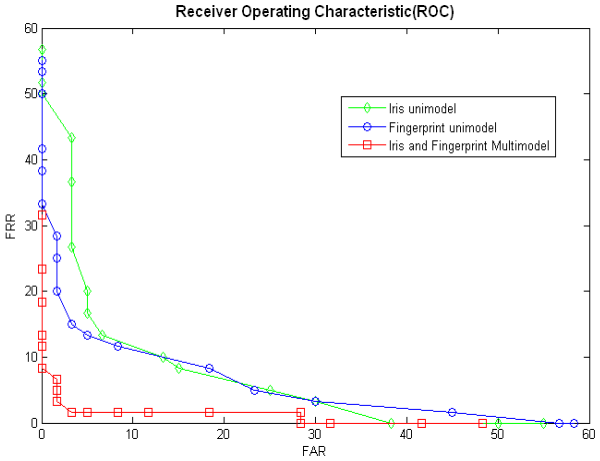

Fig 6: Receiver operating Characteristic (ROC) curves for the DB [B] test1 dataset

Analogous curves have been obtained with the remaining datasets. Proposed multimodel system give better result as compare to the unimodel, as shown in Table 2 test1 the overall performance of the system has increased showing an accuracy of 95.45% and test2 the FAR of 0% and FRR of 5.45% from the individual and combined system. The overall performance of the system has increased showing an accuracy of 97.27%

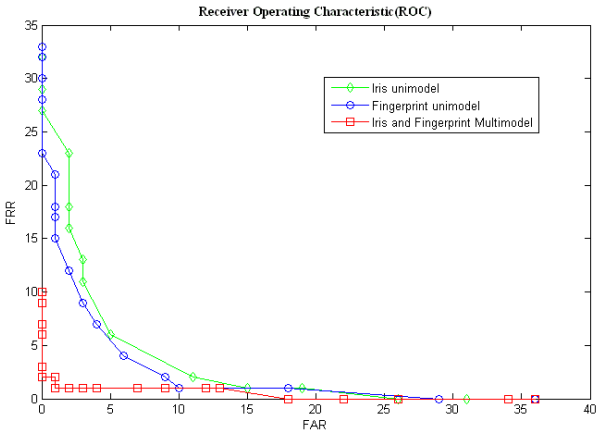

Fig 6 : Receiver operating Characteristic(ROC) curves for the DB[B]test2 dataset

4.2 Computational Time

The multimodal systems have been implemented using the MATLAB environment on a general-purpose Intel at 3.00GHz processor with 2-GB RAM memory. Table 3 shows the average software execution times for the preprocessing and matching stage. The fingerprint preprocessing time can change, since it depends on Minutia extraction detection.

Table: 3 Software Execution Time for system

Stage	Iris	Fingerprint
Pre-processing Stage	6.33 sec	5.11sec
Matching Stage	6.29 sec	

5. CONCLUSION

The paper proposes a biometric personal authentication system using a novel combination of iris and fingerprint. For system deployment the combination is found to be useful. One modality is used to overcome the limitations posed by the other. The experimental results show that the accuracy of system would increase on combining the traits. The system is giving an overall accuracy of DB [A] test1 is 95.45%, having the FAR is 0% and FRR is 9.00%. DB [B] test 2 with accuracy 97.3% and FAR, FRR of 0%, 5.40% respectively. As compare to unimodel FAR, The proposed Multimodel giving FAR is 0% The HD matching score for and Minutia based matching score are fused template has been used for the compare with predefined threshold. If Fused Matching score is greater than predefined threshold it decides the person is accepted or rejected.

6. REFERENCES

[1] Ross and A. Jain, "Information fusion in biometrics," *Pattern Recogn. Lett.*, vol. 24, pp. 2115–2125, 2003. DOI: 10.1016/S0167–8655(03)00079-5.

[2] F. Yang and B. Ma, "A new mixed-mode biometrics informationfusion based-on fingerprint, hand-geometry and palm-print," in*Proc. 4th Int. IEEE Conf. Image Graph.*, 2007, pp. 689–693. DOI:10.1109/ICIG.2007.39.

[3] J. Cui, J. P. Li, and X. J. Lu, "Study on multi-biometric feature fusion and recognition model," in *Proc. Int. IEEE Conf. Apperceiving Comput. Intell.Anal. (ICACIA)*, 2008, pp. 66–69. DOI: 10.1109/ICACIA.2008.4769972.

[4] S. K. Dahel and Q. Xiao, "Accuracy performance analysis of multimodal biometrics," in *Proc. IEEE Syst., Man Cybern. Soc., Inf. Assur. Workshop*,2003, pp. 170–173. DOI:10.1109/SMCSIA.2003.1232417.

[5] A.K. Jain, L.Hong, Y. Kulkarni, "A Multimodal Biometric System using Fingerprints, Face and Speech", 2nd Int'l Conference on Audio- and Video-based Biometric Person Authentication, Washington D.C., pp. 182-187,March 22-24, 1999.

[6] V. Conti, G. Milici, P. Ribino, S. Vitabile, and F. Sorbello, "Fuzzy fusion in multimodal biometric systems," in *Proc. 11th LNAI Int. Conf. Knowl.-Based Intell. Inf. Eng. Syst. (KES 2007/WIRN 2007)*, Part I LNAI 4692.B. Apolloni *et al.*, Eds. Berlin, Germany: Springer-Verlag, 2010,pp. 108–115.

[7] F. Yang and B. Ma, "A new mixed-mode biometrics information fusion based-on fingerprint, hand-geometry and palm-print," in *Proc. 4th Int. IEEE Conf. Image Graph.*, 2007, pp. 689–693. DOI:10.1109/ICIG.2007.39.

[8] G. Aguilar, G. Sanchez, K. Toscano, M. Nakano, and H. Perez, "Multimodal biometric system using fingerprint," in *Proc. Int. Conf. Intell. Adv. Syst. 2007*, pp. 145–150. DOI: 10.1109/ICIAS.2007.4658364.

[9] V. C. Subbarayudu and M. V. N. K. Prasad, "Multimodal biometric system,"in *Proc. 1st Int. IEEE Conf. Emerging Trends Eng. Technol.*, 2008, pp. 635–640. DOI 10.1109/ICETET.2008.93.

[10] Yunhong Wang, Tieniu Tan, and Anil K. Jain,"Combining Face and Iris Biometrics for Identity Verification". Systems, Proc. of Audio- and Video-based Biometric Person Authentication (AVBPA), Rye Brook, NY, 2005.

[11] S. C. Dass, K. Nandakumar, & A. K. Jain, A Principled Approach to Score Level Fusion in Multimodal Biometric

[12] 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).

[13] 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).

[14] L. Flom, & A. Safir, Iris Recognition System, U.S.Patent No. 4641394, 1987.

[15] A. E. Hassanien, & J M. Ali, An Iris Recognition System to Enhance E-security Environment Based on Wavelet Theory, *Advanced Modeling and Optimization Journal, 5*(2), 2003, 93-104.

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

[17] D. Maltoni, D. Maio, and A. Jain, S. Prabhakar, "4.3: Minutiaebased Methods' (extract) from Handbook of Fingerprint Recognition", Springer, New York, pp. 141-144, 2003.

[18] N. Ratha, S. Chen and A.K. Jain, "Adaptive Flow Orientation Based Feature Extraction in Fingerprint Images", Pattern Recognition, Vol. 28, pp. 1657-1672, November 1995.

[19] Image Systems Engineering Program, Stanford University. Student project By Thomas Yeo, Wee Peng Tay, Ying Yu Tai.

[20] L.C. Jain, U.Halici, I. Hayashi, S.B. Lee and S.Tsutsui. Intelligent biometric techniques in fingerprint and face recognition. 1999, the CRC Press.

[21] Lin Hong. "Automatic Personal Identification Using Fingerprints", Ph.D. Thesis, 1998.

[22] Fingerprint Verification Competition FVC2004. (2009, Nov.). [Online].Available: http://bias.csr.unibo.it/fvc2004/

[23] CASIA database (Institute of Automation, Chinese Academy of Sciences, http://www.sinobiometrics.com/).

[24] S. Prabhakar, A. K. Jain, and J.Wang, "Minutiae verification and classification,"presented at the Dept. Comput. Eng. Sci., Univ. Michigan State,East Lansing, MI, 1998.

[25] V. Conti, C. Militello, S. Vitabile, and F. Sorbello, "A multimodal technique for an embedded fingerprint recognizer in mobile payment systems,"*Int. J. Mobile Inf. Syst.*, vol. 5, no. 2, pp. 105–124, 2009.

.