Multimodal Biometric Identification System: Fusion of Iris and Fingerprint

Sameer P Patil
UG Student, Dept. of E&TC
College of Engineering,
Pune, MH – 411005, India

Tushar N Raka
UG Student, Dept. of E&TC
College of Engineering,
Pune, MH – 411005, India

Shreyas O Sarode
UG Student, Dept. of E&TC
College of Engineering,
Pune, MH – 411005, India

ABSTRACT
This paper proposes a biometric person identification system based on fusion of Iris and Fingerprint images. This paper attempts to improve the performance of iris and fingerprint-based identification system by combining the individual features obtained by implementing Iris and Fingerprint identification system. There exist techniques to provide biometric identification systems based on one or other type of modalities. But usage of multiple modalities has resulted in higher accuracy and reliability as concluded by the experiments conducted.

General Terms
Image Processing, Pattern Recognition, Biometrics, Security, Personal Verification

Keywords
Multimodal Biometrics, Fusion, Iris, Fingerprint,

1. INTRODUCTION
An automated method which recognizes a person based on his/her physiological or behavioural characteristic is called biometrics. Biometric technologies include dynamic signature verification, iris scanning, face recognition, DNA recognition, voice recognition and fingerprint identification. Biometric identification is superior to lower technology identification methods in common use today - namely passwords, PIN numbers, key-cards and smart cards. PINs (personal identification numbers) were one of the first identifiers to offer automated recognition. However, this means recognition of the PIN, implies recognition of the PIN but not the person to whom they belong. Similar analogy can be extended to cards and other tokens. The token recognition is easy but is not 100% fake-proof. It carries a threat of being stolen and recreated. The primary use of physical objects or behaviours based on memory has a clear set of problems and limitations. Objects are often lost or stolen and a behaviour based on memory is easily forgotten. Identity cannot be guaranteed, privacy is not assumed and inappropriate use cannot be proven or denied. These limitations decrease trust and increase the possibility of fraud.

Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. Biometric-based techniques are able to provide for confidential financial transactions and personal data privacy. A biometric cannot be easily transferred between individuals. The scalability for integrating biometrics into a variety of processes can be extended if the verification procedures are made more user-friendly. The most basic definition of biometrics is that it is a pattern recognition system, which establishes and validates an individual's identity based on a specific and unique biological characteristic.

Biometric-based authentication applications include workplace, network, and entry access, single sign-on, application logon, data safeguarding, remote access to resources, transaction security and Web security. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than conventional methods (e.g. usage of Passwords or Personal Identification number). The reason being using biometric nullifies the need to carry or remember any password or PIN. Moreover, biometrics is something that are unique to one and only one person. The rising popularity and inexpensiveness of such methods make the technology more acceptable.

Biometric characteristics can be classified into two broad categories:

Physiological – based methods verify a person's identity by means of his or her physiological characteristics such as fingerprint, facial features, DNA, hand geometry, palm print, iris pattern.

Behavioural – based methods performs the authentication task by recognizing people's behavioural patterns such as typing rhythm and voice print.

2. PRIOR WORK
Vincenzo Conti, Carmelo Militello, Filippo Sorbello used a frequency based approach for features fusion in fingerprint and iris multimodal biometric identification systems[1].They have come up with an innovative multi-modal biometric identification system based on iris and fingerprint traits. The paper is itself benchmark in advancement of multi-biometrics, offering an innovative perspective on features fusion. Using frequency-based approach results in a homogeneous biometric vector that integrates iris and fingerprint data. Consecutively, a hamming-distance-based matching algorithm can be coupled with the unified homogenous biometric vector.

Asim Baig, Ahmed Bouridane, Fatih Kurugollu and Gang Qu used a single hamming distance matcher for fingerprint- iris fusion based identification system [2]. They proposed a framework for multimodal biometric identification system which provide smaller memory footprint and faster implementation than the conventional systems. This framework has been verified by developing a fingerprint and iris fusion system which utilizes a single Hamming Distance based matcher. Such systems provide higher accuracy than the individual uni-modal system.

Huny Meharotra, Ajita Rattani, Phalguni Gupta have done fusion of iris and fingerprint, at matching score level architecture using weighted sum of score technique in their

paper " Fusion of iris and fingerprint biometric for recognition" [3]. The pre-processed images of iris and fingerprint are used for extraction of features. For each query image, its features are compared with those database images to calculate matching scores. The individual scores generated after matching are used as input to the fusion module. This module consists of three stages i.e., normalization, generation of similarity score and then fusion of weighted scores. The final score is used as decision making score state whether the person is genuine or an impostor. The system was tested on database collected by the authors for 200 samples.

S. Hariprasath and S. Venkatsubramaniam have proposed an iris recognition system based on wavelet packet analysis in their paper "Iris feature extraction and recognition using wavelet analysis"[4]. They have proposed a multi-resolution approach based on Wavelet Packet Transform (WPT) for iris texture analysis and recognition. The motivation behind this concept was the observation that dominant frequencies of iris texture are located in the low and middle frequency channels. WPT sub images coefficients are quantized into 1, 0 as iris signature using an adaptive threshold. This signature represents the local information for different irises. The size of the iris signature of code attained was 1280 bits. The signature of the new incoming iris pattern is compared against the stored pattern after computing the signature of new iris. Recognition was performed by calculating the hamming distance.

Lenina Birgale and M. Kokare have proposed a method for improved iris recognition with reduced processing time, FAR and FRR in their paper, "Iris recognition without iris normalization"[5]. They have used different masks to filter out iris image from an eye. After performing comparative study of different masks, optimized mask was proposed. The experiment was carried using CASIA database which had 756 iris images of 108 persons. For each person, there were seven images of eye (108´7= 756) in the database. They proposed new method wherein: Normalization is avoided; Computational time was drastically reduced by 0.3342 sec; Iris signature size was reduced; Improved performance parameters. (These new proposed method achieved 99.4866% accuracy, 0.0069% FAR, 1.0198% FRR and proportionate increase in speed of the system).

Raida Hentati, Moncef Bousselmi, Mohamed Abid have proposed a system for Human Authentication based on iris texture analysis in their paper "An Embedded System for iris Recognition"[6]. They presented a Hardware/software implementation algorithm for detection and hence localisation of iris based on shape properties. This system has been implemented in a CYCLONE II DE2 Board using the NIOS II processor. This is characterized by its flexibility and programmability. The database used for testing was CASIA version 1.0.

Wang Yuan, Yao Lixiu nad Zhou Fugiang proposed a real time fingerprint recognition system in their paper "A Real Time Fingerprint Recognition System Based On Novel Fingerprint Matching Strategy"[7]. In this paper they have presented a new real time recognition system based on a novel fingerprint minutiae matching algorithm. The system is developed is currently in usage in today's embedded systems for fingerprint authentication. The system consist of modules like fingerprint enhancement, fingerprint feature extraction, fingerprint matching using a novel matching algorithm, quality control and networking capability for other identification system.

Hiew , Melaka Teoh and Pang proposed a touch less fingerprint recognition system in their paper, "Touch less fingerprint recognition system"[8].The system which used digital camera addressed the constraints of the fingerprint images such as the low contrast between the ridges and valleys in fingerprint images, lack of focus and motion blurriness. The system was made of pre-processing stage, feature extraction stage and matching stage. The proposed pre-processing stage exhibited promising results in regarding segmentation, enhancement and core point detection. Features were extracted using Gabor filter. The results were obtained with the Support Vector Machine.

3. IMPLEMENTATION

Typical phases of Biometric Identification would include Collection of data (biological characteristics), Extraction (of a template based on the data), Comparison(with another biological characteristic) and Matching. The exact design of biometric systems provides a degree of flexibility in how activities of enrolment, authentication, identification and long-term storage are arranged.

3.1 Image Acquisition and Database preparation

For Iris identification, experiment was performed on IIT Delhi Database. This iris image database mainly consists of the iris images collected from the students and staff at IIT Delhi, India. This database was originally collected by Biometrics Research Laboratory during January - July 2007 using JIRIS, JPC1000 using digital CMOS camera. The database of 2240 images is acquired from 224 different users and made available freely to the researchers. All these images were acquired in the indoor environment. The acquired database is saved in 224 folders, each corresponding to 224 subjects. First five iris images were acquired from the left eyes while the rest five images were acquired from Right eye.

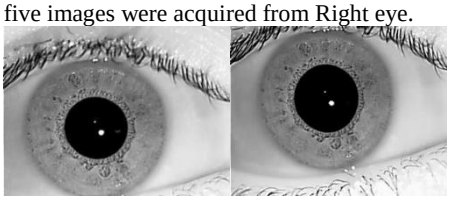


Fig 1: Sample of Right and left eye of same person IIT D Database

For Fingerprint, image database was created using Futronic FS80 Finger Print Scanner. Fingerprint scanning window size was set to 16x24mm. The resolution of acquired images is 480x320 pixel, 500 DPI. The Size of each raw fingerprint image file is 150K byte.

3.2 Feature Extraction

3.2.1.1 Pre-processing for Iris Images

In the pre-processing stage, IRIS images are transformed from RGB to gray level and from eight-bit to double precision thus facilitating the manipulation of the images in subsequent steps.

In this approach, Hough Transform was used to detect the centre of iris and pupil boundary. This involved first employing Canny edge detection to generate an edge map. The gradients thus generated were biased in the vertical direction for the outer iris/sclera boundary, as concluded by Wildes et al. [4]. Vertical and horizontal gradients were then weighted equally for the inner iris/pupil boundary. The Hough transform for the iris/sclera boundary was performed first in order to make the circle detection process more efficient and accurate, then it was repeated for the iris/pupil boundary within the iris region, instead of the whole eye. The reason

being the pupil is always within the iris region. After completion of this process, six parameters were stored, namely, the radius, and x and y centre coordinates for both the circles.

For segmentation of iris part from the image, a masked image is used which is shown in figure. The mask image is a ring which inner radius and outer radius is same as original iris image.

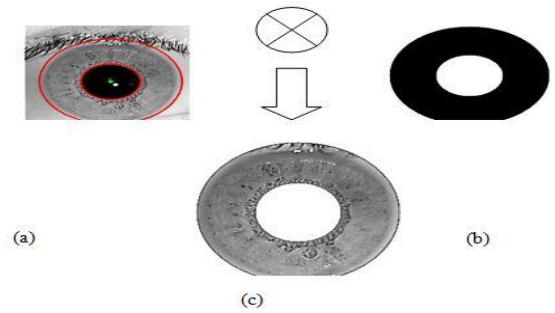


Fig 2 : (a) iris image, (b) Mask image, (c) Segmented Image

3.2.1.2 Normalization and Feature Extraction

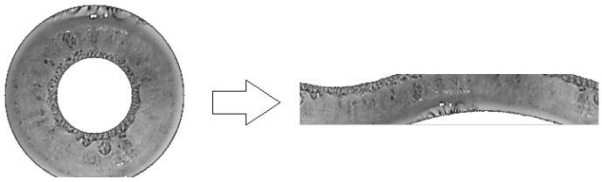


Fig 3 : Unwrapping of segmented iris image

After determining the limits of the iris in the previous stage, the iris should be isolated now and stored in a separate image. There is slight possibility of the pupil dilating and appearing of different size in different images. To overcome such scenarios, the coordinate system was modified by unwrapping the lower part of the iris and mapping all the points within the boundary of the iris into their polar equivalent. The size of the Mapped image is fixed which implies that an equal amount of points at every angle are taken. Therefore, if the pupil dilates the original points are considered and mapped again which enables mapping process to be stretch invariant.

3.2.1.3 Pre-processing for Fingerprint Images

The finger print images are divided small processing blocks (32 by 32 pixels) and perform Fourier transform according to:

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

for u = 0, 1, 2, ..., 31 and v = 0, 1, 2, ..., 31.

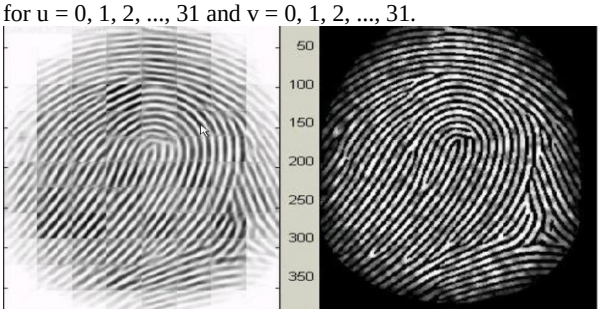


Fig 4: Enhanced image (left), Original image (right)

In order to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows, fingerprint Image is passed through Binarization module. After this operation, ridges in the fingerprint are highlighted with black colour while furrows in white. Hereafter, a locally adaptive binarization method is deployed to binarize the fingerprint image.

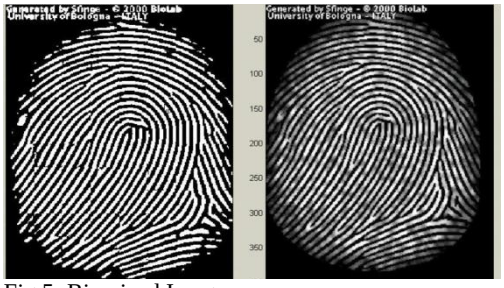


Fig 5: Binarized Image

The Region of Interest (ROI) is recognized using segmentation. The remaining area without effective ridges and furrows is then discarded. Then the bound of the remaining effective area is sketched out since the minutia in the bound region can be confusing with those spurious minutiae that are generated when the ridges are out of the sensor. A two-step method is employed for extracting ROI. The first step is block direction prediction and direction variety check while the second is realized from some Morphological methods

3.2.1.4 Feature Extraction and Matching

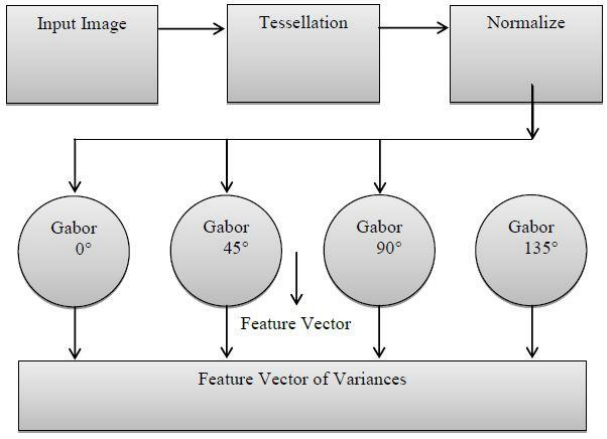


Fig 6 : Gabor Filter Extraction

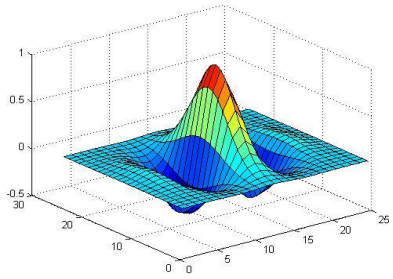
The block diagram of feature extraction of finger print images is shown above.

Therefore, it is becomes important to accurately represent the local vital information in a finger print. There are many techniques suggested in the literature for extracting unique and invariant features from the finger print image. But these techniques have used either texture- or appearance-based features. Gabor filter has been used.

General form of a 2D Gabor filter is defined by

$$\boldsymbol{h(x,y,\theta_k,f,\sigma_x,\sigma_y)} = \mathbf{exp}\left[-\frac{1}{2}\left(\frac{{x_{\theta_k}}^2}{{\sigma_x}^2} + \frac{{y_{\theta_k}}^2}{{\sigma_y}^2}\right)\right] \times \mathbf{exp}\left(i2\pi f x_{\theta_k}\right)$$

where $\boldsymbol{x_{\theta_k} = x\cos\theta_k + y\sin\theta_k}$ and $\boldsymbol{y_{\theta_k} = y\cos\theta_k - x\sin\theta_k}$, $\boldsymbol{f}$ is the frequency of the sinusoidal plane wave, $\boldsymbol{\theta_k}$ is the orientation of the Gabor filter, and $\boldsymbol{\sigma_x}$ and $\boldsymbol{\sigma_y}$ are the standard deviations of the Gaussian envelope along the $\boldsymbol{x}$ and $\boldsymbol{y}$ axes, respectively.



Since most local of the ridge structures of fingerprints come with well-defined local frequency and orientation, the reciprocal of the average inter ridge distance can be set as $\boldsymbol{f}$ and $\boldsymbol{m}$ shall be the number of orientations for calculating $\boldsymbol{\theta_k} = \frac{\boldsymbol{\pi(k-1)}}{\boldsymbol{m}}$, $\boldsymbol{k = 1, 2, \ldots \ldots, m}$.

For matching any two fingerprints, special representations for each fingerprints sample has to be created, which are then compared in the matching process. The Gabor filtered representations are not used for comparison directly for performance issues. Therefore, the Gabor filter responses have to be translated into a so-called feature map. There are two ways to create such a template: a circular or a rectangular tessellation, which will be put over the particular fingerprint.

The circular tessellation variant was selected because usually the prime focus areas of a fingerprint are around the reference point. By using circular tessellation with the reference point as center, these areas are represented in a higher resolution. In contrast, a rectangular feature map resolves every area in the fingerprint in the similar way. Moreover, the rectangular tessellation can be applied only on straightly aligned fingerprints to obtain resembling feature maps of two fingerprints, which are twisted to each other. The circular tessellation is able to handle twisted fingerprints as well.

The content of every sector si of the feature map is to represent how good the ridges in a sector correlate to the specific Gabor filter direction. The feature map is computed by calculating the average absolute deviation from the mean gray level for every sector.

Fig. 7: Gabor filtered fingerprint in direction $\boldsymbol{\theta_k} = \boldsymbol{0^\circ, 45^\circ, 90^\circ, 135^\circ}$ resp.

3.3 Fusion of Fingerprint and Iris

Any individual trait cannot provide 100% accuracy. Also problem may arises when iris image captured was taken in low light. Human eye being the most sensitive organ of human body, the problem becomes worse if the individual has some eye disease. In such cases an individual cannot be identified using the iris patterns and the existing biometric system becomes underachiever. Similarly, the challenge fingerprint recognition system face is the presence of scars and cuts. The scars distort the originality of the data by adding noise to the fingerprint image. This results in noisy input to the system which is not able to extract the minutiae points correctly and hence results in false identification. Thus to overcome the problems faced by conventional systems based on individual traits of iris and fingerprint, a new combination is proposed for the recognition system. This new integrated system makes it difficult for an intruder to spoof multiple biometric traits simultaneously, thus making the system anti spoof. The individual traits are used to generate scores which are combined at matching score level using weighted sum of score technique.

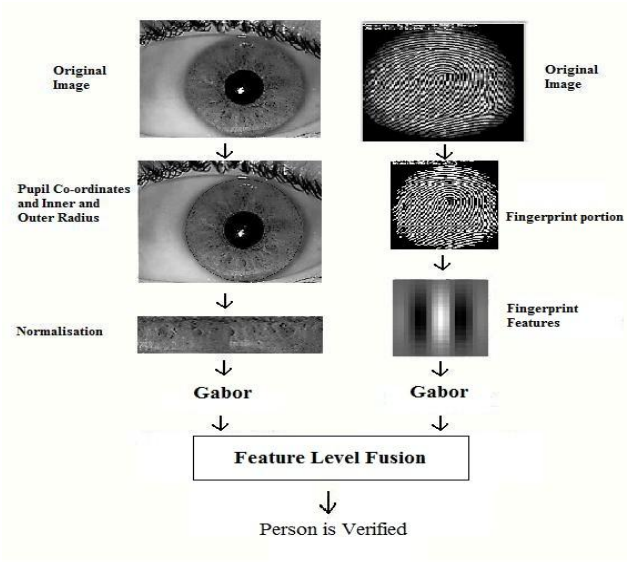


Fig 8: System Architecture and Algorithm

3.3.1 Decision level fusion

In this type of fusion method, the decision of person verification is taken based on thresholds obtained by both the modalities. Hence the sample given as input is accepted genuine person only it satisfies both the criteria.

3.3.2 Score level fusion

In this type of fusion the output scores obtained from the modalities are initially normalized and then combined by either of the following method: concatenation, addition or subtraction to get the resultant score. This obtained score can be used for verification.

3.4 Feature Normalization

Following techniques are used to normalize the features.

3.4.1 Min-Max normalization

The easiest normalization technique is the Min–max normalization. Min–max normalization can be applied when the bounds (maximum and minimum) of the scores calculated by a matcher are known. In such case, the minimum and maximum scores/features can be easily shifted to 0 and 1, respectively. If the known matching scores are not bounded, the minimum and maximum values for that set of matching scores/features can be estimated and then applied the min–max normalization. For given set of matching scores {sk }, k=1, 2, . . . , n, the normalized scores/features are given by

$$\frac{(s - \min(s))}{(\max(s) - \min(s))}$$

However, this method is not robust since the minimum and maximum values are estimated from the given set of matching scores(This method is more sensitive to outliers).This technique retains the original distribution of scores except for a scaling factor and transforms all the scores/features into a common range [0, 1].

3.4.2 Z-score normalization

The Z-score is calculated using the arithmetic mean and standard deviation of the given data. This method performs well if prior knowledge about the average and score variations of the matcher are available. The normalized scores are given by

$$\frac{s-\mu}{\sigma}$$

Where μ is the arithmetic mean and σ is the standard deviation for the given data. Z-score normalization cannot retain the input distribution at the output if the input scores/features are not Gaussian distributed. Since the mean and standard deviation are the optimal location and scale parameters only for a Gaussian distribution, Gaussian distribution results in retention of input scores/features. The arbitrary distribution results in mean and standard deviation which are reasonable estimates of location and scale, respectively, but are not exactly optimal.

3.5 Feature Matching

Scores generated from individual traits are combined at matching score level using weighted sum of score technique. Experiments were conducted for following permutations:

1. Matching of Iris features using Cityblock and Lorentzian distance
2. Matching of Fingerprint features using Lorentzian distance
3. Fusion of Iris and Fingerprint without normalization using Canberra distance
4. Fusion of Iris and Fingerprint with Z-score normalization for Lorentzian.
5. Fusion of Iris and Fingerprint with min-max normalization for Cityblock and Lorentzian distance
6. Fusion of Iris and Fingerprint with Z score normalization for Lorentzian (varying no of features)
7. Fusion of Iris and Fingerprint with Z score normalization for Lorentzian (varying distances and number of persons)

It was concluded that Z-score normalization using Lorentzian distance with total of 150 features (iris + fingerprint) provides maximum accuracy and performance.

4. RESULTS AND DISCUSSIONS

Ten Iris images and eight Fingerprint images for each of the subject were acquired. Out of this database, five Iris images and four fingerprint images were used for training and remaining for testing. Initially, the individual level scores are generated. The two scores are then fused using different distances and normalization levels. Total Minimum Error Rate (TMER) was deployed as a metric for system performance evaluation. When TMER is used as a criterion, the sum of FAR and FRR is taking into consideration. The threshold at which the sum is minimum is used as decision metric.

Table 1 shows FAR and FRR for Iris as per different distances

Types of Distances	FAR (%)	FRR(%)
Cityblock	6.5	7.83
Lorentzian	6.8	8.21

Table 2 shows FAR and FRR for Fingerprint as per different distances

Types of Distances	FAR (%)	FRR (%)
Canberra	2.5	3.13
Lorentzian	1.7	2.89

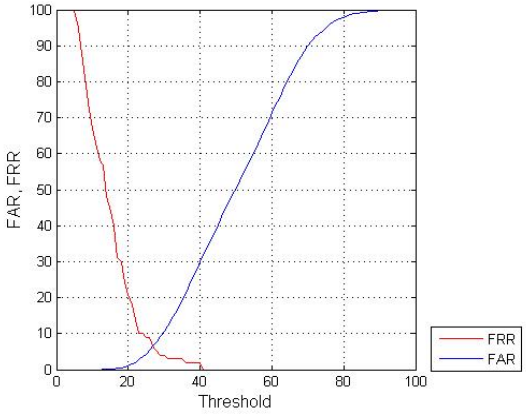


Fig. 9 a) Results for Iris features using z-score normalization using Cityblock distance

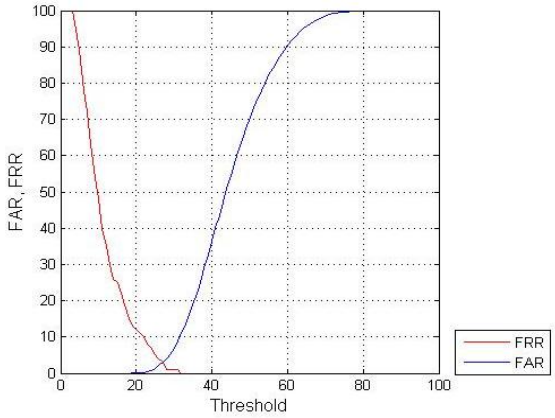


Fig. 9 b) Results for Fingerprint features using z-score normalization using Lorentzian distance

Table 3 shows describes FAR and FRR using z-score normalization by varying features

Table 3 shows FAR and FRR for Decision level fusion by varying no. of features

Types of Distances	FAR (%)	FRR (%)
Canberra	2.5	5.7
Lorentzian	1.7	4.89

Table 4 describes False Acceptance Rate (FAR) and False Rejection Rate (FRR) for score level fusion. Here all the features are combined at score level. For score level fusion, z-score normalization is done with different distances such as Lorentzian, CityBlock, Canberra and Hellinger. This

combined score is then used to evaluate the performance of system.

Table 4 shows FAR and FRR by varying distances for 100 persons

Types of Distances	FAR (%)	FRR (%)
Lorentzian	0.33	3.1
Cityblock	0.58	6.5
Canberra	1.0	4.8
Hellinger	7.46	4.2

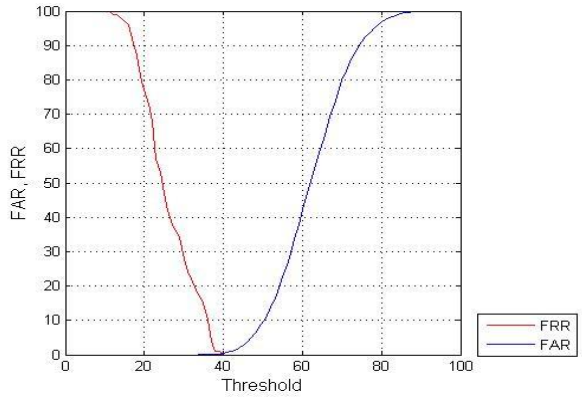


Fig. 10 a) Results for fusion of Iris and Fingerprint features using Lorentzian distance for 100 persons

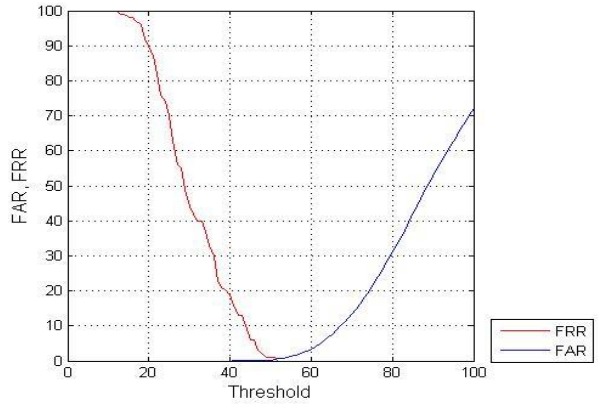


Fig. 10 a) Results for fusion of Iris and Fingerprint features using Cityblock distance for 100 persons

5. CONCLUSIONS

In this work a user verification system based Iris and Fingerprint has been developed. In this work different technique of fusion of the two types like Decision level fusion, score level fusions are compared. The algorithms used for extracting region of interest of Iris are less complex as against [4, 7]. Features extracted from individual modalities gave better results as compared to [2, 6]. Finally the features obtained from Iris and Fingerprint are fused at decision level, score level to increase recognition accuracy of the system. It is observed that by using Z-score normalization for Lorentzian distance, highest accuracy with FAR of 0.33% and FRR of 3.1% was achieved. It was also observed using Cityblock distance and by varying the number of persons, good FAR can be achieved but it also gives higher FRR of 6.5%. It underlines the fact that fusion of individual biometrics results in greater accuracy than individual iris or fingerprint recognition system. Z-score normalization using Lorentzian distance with total of 160 features (iris + fingerprint) provides maximum accuracy.

6. ACKNOWLEDGMENTS

Our special thanks to M.A. Joshi Mam, Ph.D, Professor at Dept. of E&TC, College of Engineering, Pune and Suhas Chate, former Graduate Research Assistant at Image Processing Lab, College of Engineering, Pune.

7. REFERENCES

[1] Vincenzo Conti, Carmelo Militello, Filippo Sorbello, "A Frequency-Based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE transactions on systems, man and cybernetics- Part C: Applications and Reviews, Vol. 40, No. 4, July 2010.

[2] Asim Biag, Ahmed Bouridane, Faith Kurugollu and Gang Qu, "Fimgerprint- Iris Fuion based Identification System using a Single Hamming Distance Matcher", 2009 Symposium on Bio-inspired Learning and Intelligent Systems for Security.

[3] Huny Meharotra, Ajita Rattani, Phalguni Gupta, "Fusion of iris and fingerprint biometric for recognition", Indian Institute of Technology, Kanpur.

[4] S. Hariprasath and S. Venkatsubramaniam, "Iris feature extraction and recognition using wavelet analysis", International Conference on Signal and Image Processing, 2010.

[5] Lenina Birgale and M. Kokare, "Iris recognition without iris normalization", Journal of Computer Science, Science Publications, 2010.

[6] Raida Hentati, Moncef Bousselmi, Mohamed Abid, "An Embedded System for iris Recognition", International conference on Design and technology of integrated systems in nanoscale era.

[7] Wang Yuan, Yao Lixiu nad Zhou Fugiang, "A Real Time Fingerprint Recognition System Based On Novel Fingerprint Matching Strategy", Electronic Measurement and Instruments, 2007. ICEMI '07. 8th International Conference, July 2007.

[8] Hiew , Melaka Teoh and Pang, "Touchless fingerprint recognition system", Automatic Identification Advanced Technologies, 2007 IEEE Workshop, June 2007

[9] Arun Ross, Anil Jain, " Information Fusion in Biometrics", Pattern recognition letters 24 (2003) 2115-2125.

[10] R. N. Kankrale, Prof. S. D. Sapkal, "Template level fusion of iris and fingerprint in multimodal biometric identification systems", National Conference on emerging trends in computer science and Information Technology (ETCSIT) 2011.

[11] Daugman J. "How iris recognition works", available at http://www.ncits.org/tc_home/m1htm/docsm1020044.pdf

[12] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric recognition", IEEE Transactions on circuits and systems for video technology, Vol. 14, No. 1, January 2004