ISSN 2229-5518

Fusion of Iris & Fingerprint Biometric for Security Purpose

P.U.Lahane, Prof. S.R.Ganorkar

Abstract— Basic aim of a biometric system is automatically discriminate between subjects as well as protect data. It also protects resources access from unauthorized users. We develop a biometric identification system that represents a valid alternative to conventional approaches. In biometric system physical or behavioral traits are used. A multimodal biometric identification system aims to fuse two or more physical or behavioral traits. Multimodal biometric system is used in order to improve the accuracy. Multimodal biometric identification system based on iris & fingerprint trait is proposed. Typically in a multimodal biometric system each biometric trait processes its information independently. The processed information is combined using an appropriate fusion scheme. Successively, the comparison of data base template and the input data is done with the help of Euclidean-distance matching algorithm. If the templates are matched we can allow the person to access the system. We are going to check FAR & FRR with different threshold level. Multimodal biometric system provides optimal False Acceptance Rate (FAR) & False Rejection Rate (FRR), thus improving system accuracy & reliability.

Index Terms— Biometrics, False Acceptance Rate (FAR), False Rejection Rate (FRR), Fingerprint trait, Fusion technique, Identification system, Iris trait, Multimodal.

1 INTRODUCTION

THE term biometrics is derived from the Greek words Bio & Metric. The term Biometrics relates to the measurement (metric) of characteristics of a living (Bio) thing in order to identify a person. Biometrics uses various physiological or behavioral characteristics. Common physiological biometric measurements include fingerprints, hand geometry, retina, iris, facial images etc. While common behavioral biometric measurements include signatures, voice recordings, keystroke rhythms etc.

With an increasing importance of security, there is a need to guaranty that only authenticated users have access to the system. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. However, even the best biometric traits till date are facing numerous problems some of them are inherent to the technology itself. Biometric authentication systems generally suffer from enrollment problems due to non-universal biometric traits, insufficient accuracy caused by noisy data acquisition in certain environments. Biometric measurements are inherently varied because of the existence of back-ground noise, signal distortion, biometric feature changes and environmental variations. Identification based on a single bio-metric trait may not be sufficiently robust and it has a limited ability to overcome spoofing.

One way to overcome these problems is the use of multi-biometrics. A multi biometric system uses multiple sensors for data acquisition. This allows capturing multiple samples of a single biometric trait and/or samples of multiple biometric traits. This approach is enables to provide significant improvement over unimodal biometric system in terms of higher accuracy.

- *P.U. Lahane is currently pursuing master degree program in communication network in Pune University, India, PH-9096396158. E-mail: prashlahane@gmail.com*
- *S.R. Ganorkar is currently working as associate professor in electronics & telecommunication dept. of SCOE in Pune University, India, PH-9422514726. E-mail:srgomom@rediffmail.com*

2 EXISTING APPROCHES

A variety of articles can be found which propose different approaches for traditional and multimodal biometric system.

S. Prabhakar, A. K. Jain, and J. Wang presented a unimodal fingerprint verification and classification system. The system is based on a feedback path for the feature-extraction stage, followed by a feature-refinement stage to improve the matching performance. This improvement is illustrated in the contest of a minutiae-based fingerprint verification system. The Gabor filter is applied to the input image to improve its quality [2]. N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish proposed a unimodal distortion-tolerant fingerprint authentication technique based on graph representation. Using the fingerprint minutiae features, a weighted graph of minutiae is constructed for both the query fingerprint and the reference fingerprint. The proposed algorithm has been tested on a large private database with the use of an optical sensor [3].

Y. Zhu, T. Tan, and Y. Wang proposed a system for person identification based on iris patterns. The algorithm for iris feature extraction is based on texture analysis using multi-channel Gabor filtering and wavelet transform [4]. L. Ma, Y. Wang and D. Zhang proposed Efficient Iris Recognition by Characterizing Key Local Variations. Multichannel and Gabor filters have been used to capture local texture information of the iris, which are used to construct a fixed-length feature vector [5]. V. Conti, G. Milici, P. Ribino, S. Vitabile and F. Sorbello proposed a multimodal biometric system using two different fingerprint acquisitions. The matching module integrates fuzzy-logic methods for matching-score fusion [6].

F. Yang and B. Ma proposed a mixed mode biometric information fusion based on fingerprint, palm print, and hand geometry. 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 [7]. F. Besbes, H. Trichili and B. Solaiman proposed a multimodal biometric system using finger-print and iris features. They use a hybrid approach based on fin-gerprint minutiae extraction and iris template encoding through a mathematical representation of the extracted iris region. This approach is based on two recognition modalities and every part provides its own decision. The final decision is taken by consid-ering the unimodal decision through an "AND" operator [8]. G. Aguilar and his colleagues proposed a system which uses the fingerprints of both thumbs. Each fingerprint is separately pro-cessed. Successively the unimodal results are compared in order to give the final fused result [9].Comparing the approaches found in literature and detailed earlier, we introduces an innovative idea to unify and homogenize the final biometric descriptor using two different strong features—the fingerprint and the iris. We are going to use the official fingerprint verification competition (FVC) 2002 DB2 fingerprint database [10] and UBIRIS database [11].

3 Multimodal Biometric System

Multimodal biometric identification system is a new approach. A unimodal biometric system consists of three major modules: sensor module, feature extraction module and matching module. The performance of a biometric system is largely affected by the reliability of the sensor used and the degrees of freedom offered by the features extracted from the sensed signal. Further, if the biometric trait being sensed or measured is noisy (for example a fingerprint with a scar or a voice altered by a cold), the resultant matching score computed by the matching module may not be reliable. This problem can be solved by installing multiple sensors that capture different biometric traits. Different biometric features are used by these systems. Biometric systems that utilize more than one physiological or behavioral characteristic for identification are called multimodal biometric systems. Multimodal biometric systems are expected to be more reliable due to the presence of multiple pieces of evidence.

Biometric fusion is generally classified in terms of both categories and levels. The categories define what inputs or processes are being used for fusion and the levels define how the fusion performed [12].

Categories of fusion:

1. Multi-sample: Fusion of multiple samples (images) acquired from the same source, such as multiple images of a single fingerprint, images of the same face.
2. Multi-instance: Fusion of multiple instances of the same type of biometric such as fingerprints from multiple fingers, or images of both irises.
3. Multi-modal: Fusion of multiple types of biometrics, such as a combination of a subject's fingerprints, face, irises and voice.
4. Multi-algorithm: Fusion of multiple methods of processing for each individual sample. In practice, this usually means the use of multiple matchers but can also apply to multiple methods of feature extraction.

Level of Fusion:

1. Data-sensor level: Data coming from different sensors can be combined so that the resulting information is in more accurate, more complete or more dependable form.
2. Feature-extraction level: The information extracted from sensors of different modalities is stored in vectors on the basis of their modality. These feature vectors are then combined to create a joint feature vector which is the basis for the matching and recognition process.
3. Matching-score level: This is based on the combination of matching scores. After separate feature extraction and comparison between stored data and test data for each subsystem is done. From the matching score of each subsystem, an overall matching score is generated using linear or nonlinear weighting.
4. Decision level: In this approach each biometric subsystem completes the processes of feature extraction, matching and recognition. Decisions are made by using Boolean functions. The recognition output is nothing but the majority decision among all present subsystems.

Multimodal biometric system can implement any of these fusion schemes to improve the performance of the system. We are going to do fusion at feature extraction level to generate a homogeneous template for fingerprint and iris feature.

4 Proposed Biometric System

A multimodal biometric system based on fingerprint and iris characteristic is proposed.

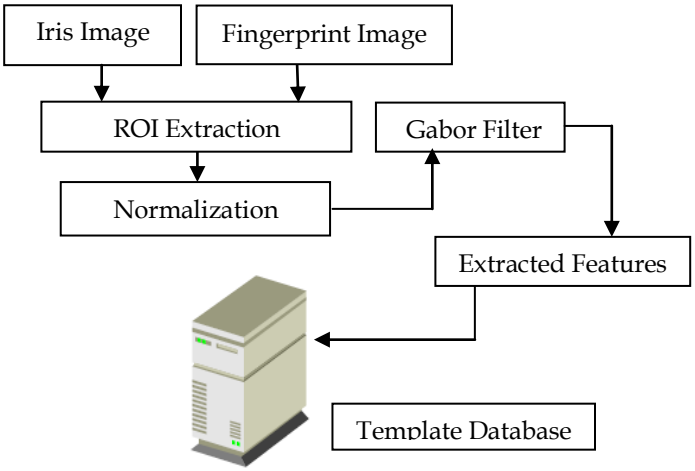

Fig.1. Enrollment Module

The proposed multimodal biometric system consists of two main modules Enrollment module & Identification module. The enrollement module is shown in above Fig.1. While enrollment module contain the preprocessing stage and identification module contains preprocessing stage as well as matching stage.

The identification module is shown in below Fig.2.

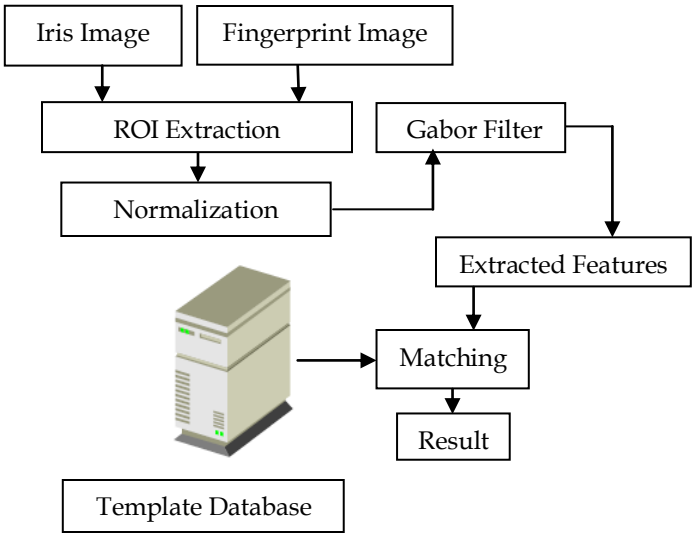

Fig.2. Identification Module

Iris and fingerprint images are preprocessed to extract the ROIs (Regions of Interest). Iris image preprocessing is performed by segmenting the iris region from eye and deleting the eyelids and eyelashes. Fingerprint image preprocessing is performed by segmenting the singularity region from fingerprint. The extracted ROIs are used as input for the normalization. Then normalized data is given to the Gabor filters. After that the extracted features are stored in template data base. While in identification module theses template data bases are match with input template to identify the person.

4.1 Preprocessing stage

To improve the image quality we are going to perform preprocessing on input image. In preprocessing the fingerprint singularity region extraction process and the iris region of interest extraction process are described. A region of interests is a selected part of an image used to perform particular task.

4.1.1 Iris Region of Interest Extraction:

This approach is used to detect the center, radius and circumference of the pupil and iris region even if the circumferences are usually not concentric [13]. First of all the center of the iris image is found. With reference to that image center we can find the pupil center with the help of threshold. From the centre of the pupil we can calculate the radius of the pupil.

The edge is detected using canny edge detector. It has very low error rate and there is almost zero response to nonedges when giving an appropriate threshold. This algorithm uses horizontal and vertical gradients in order to deduce edges in the image. After running the canny edge detection on the image a circle is clearly present along the pupil and iris boundary. In iris segmentation phase the iris boundary is detected. The radius of the pupil is subtracted from the radius of iris. After subtracting we get the exact iris region. The iris region is in the polar form, which we convert in to the rectangular form for further processing. Eyelids and eyelashes are considered to be "noise" which degrades the system performance. Initially the eyelids are isolated by fitting a line to the upper and lower eyelid using the linear Hough transform.

4.1.2 Fingerprint Singularity Region Extraction:

First we read the fingerprint image. A fingerprint image can be enhanced by remapping the intensity values using the histogram equalization. i. e. Histogram equalization is usually increases the global contrast of an image. Then we are going to extract the singularity region with help of threshold. Particular fingerprint zones surrounding singularity points namely the "core" and the "delta" is known as singularity region. After that we get the segmented fingerprint image.

4.1.3 Normalization:

A normalization operation must be performed after ROIs extraction. The fingerprint and iris images of different people may have different size. For a person biometric feature size may vary because of illumination changes during the iris acquisition phase or pressure variation during the fingerprint acquisition phase.

4.1.4 Gabor Filter:

A Gabor filter is obtained by modulating a sinusoid with a Gaussian. For the case of one dimensional (1D) signals, a (1D) sinusoid is modulated with a Gaussian. This filter will therefore respond to some frequency, but only in a localized part of the signal. For 2D signals such as images, a (2D) sinusoid is modu-lated with a Gaussian [14]. The Gabor filter can be defined as follows

$$\psi(x, y, \varpi, \theta) = \frac{1}{2\pi\sigma^2} e^{-\left(\frac{x'^2+y'^2}{2\sigma^2}\right)} [e^{i\varpi x'} - e^{-\frac{\varpi^2\sigma^2}{2}}]$$

$$x' = x\cos\theta + y\sin\theta, y' = -x\sin\theta + y\cos\theta$$

..(1)

where (x, y) is the pixel position in the spatial domain, ω is the radial center frequency, θ is the orientation of Gabor filter and σ is the standard deviation of the round Gaussian function along the x- axes and y-axes. In addition, the second term of the Gabor filter compensates for the DC value because the cosine component has nonzero mean while the sine component has zero mean. Gabor filter bank with five frequencies and eight orientations is used to extract the Gabor feature for iris & fingerprint representation [15]. The real part of the Gabor filters with five frequencies and eight orientations is shown in Fig.3.

The Gabor feature representation of an image I(x, y) is the convolution of the image with the Gabor filter bank $\psi(x, y, \omega_m, \theta_n)$ as given by:

$$O_{m,n}(x, y) = I(x, y) * \psi(x, y, \varpi_m, \theta_n) \quad \ldots\ldots (2)$$

Where * denotes the convolution operator. The homogenous biometric vectors from fingerprint and iris data are made. But we understand that the time require for Gabor feature extraction is somewhat more and the dimension of Gabor feature vector is large. Then from homogenous biometric vector we generate fused template.

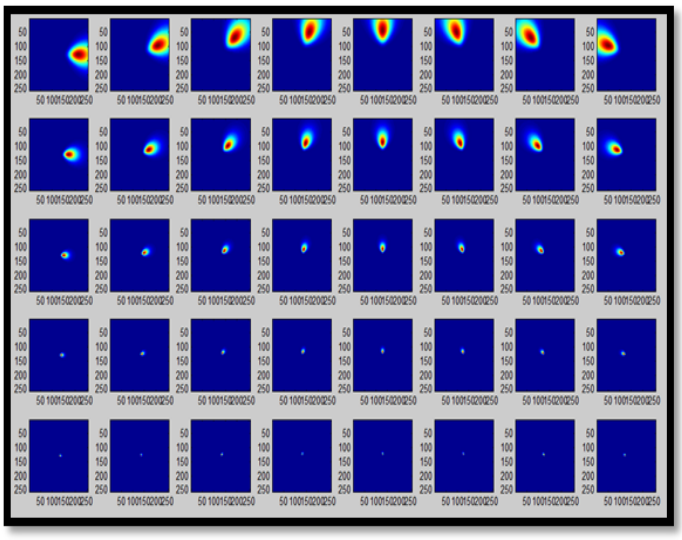

Fig.3. Real part of Gabor filters with five frequencies & eight orientations

4.2 Matching Stage

The region of interest (ROI) extracted from the original images are stored in different vectors. Successively, each vector is normalized in rectangular coordinates. The features are extracted using Gabor filter. Then fusion is performed by combining the biometric features extracted from pair of fingerprints and irises images. Finally Euclidean Distance is used for matching score computation.

4.2.1 Euclidean Distance Based Matching:

The matching score is calculated through the Euclidean Distance calculation between two final fused templates. The template obtained in the encoding process will need a corresponding matching metric that provides a measure of the similarity degree between the two templates. The result of the measurement is then compared with an experimental threshold to decide whether or not the two representations belong to the same user.

5 Result

In enrollment process we enroll the ten users with five iris image & five Fingerprint image of each person. After the processing of input images (feature extraction) in enrollment, we create the template database. In identification process we enter the third iris and third fingerprint image of second person, which is shown in Fig. 4 & Fig. 5 respectively. After processing we get the correct output that is enter person recognized correctly which is shown in Fig. 6. Same way if we enter the different iris & fingerprint images of different person from the database we get the output as Not Recognized. If we take the iris & fingerprint images which are not from the database then we get the output as Unknown Person. We have tested this system for different threshold which is shown in Table 1.

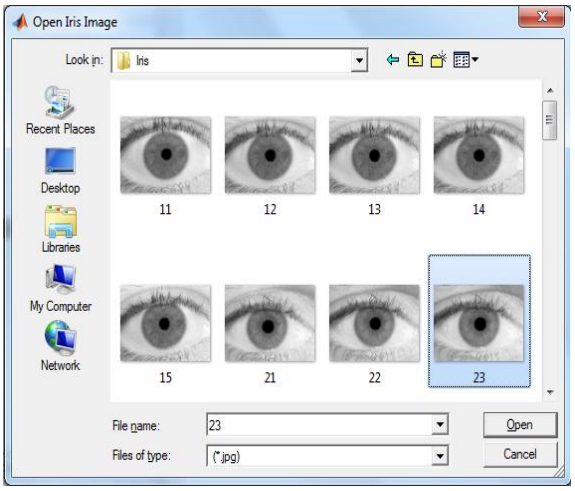

Fig.4.Input Iris Image (Second Person)

Fig.5. Input Fingerprint Image (Second Person)

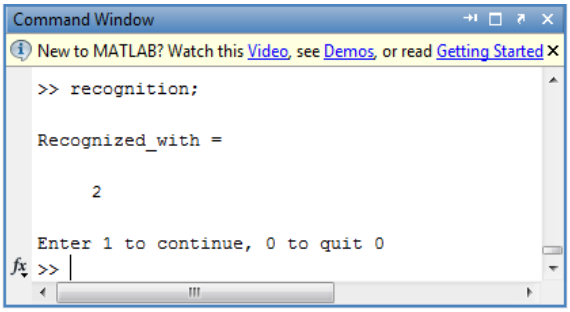

Fig.6. Correct Recognition of Person (Second Person)

TABLE 1
Recognition Rate of Proposed System for Different Threshold

Performance Measure	Multimodal (Iris + Fingerprint)		
	Thresholds		
	0.1	0.5	1
FAR	0.5%	0.4%	0.3%
FRR	0.9%	0.7%	0.5%
EER	1.80	1.75	1.66
Accuracy	99.1%	99.3%	99.5%

6 Conclusion

Efficient security system by using iris and fingerprint traits has been design.The accuracy of the multimodal system is 99.5% for threshold 1 compare to 99.1% and 99.3% for threshold 0.1 and 0.5 respectively. FAR, FRR and EER values are better for threshold 1 also.

7 Acknowedgement

I am sincerely thankful to my guide Prof. S. R. Ganorkar for his relevant help, encouragement and providing the necessary guidance. I am also proud to thank our HOD (E&TC Department) Dr. A. D. Jadhav and our Principal Dr. S. D. Lokhande for moral support. I am really thankful to all professors of SCOE for their guidance. Without their help it was tough job for me.

8 References

[1] Vincenzo Conti, Carmelo Militello, Filippo Sorbello & Salvatore Vitabile "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems" IEEE Transaction on systems, Man & Cybernetics—Part C: Applications & Reviews, VOL. 40, No. 4, JULY 2010.

[2] 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.

[3] N. K. Ratha, R. M. Bolle, V. D. Pandit, and V. Vaish, "Robust fingerprint authentication using local structural similarity," in Proc. 5th IEEE Workshop Appl. Comput. Vis., Dec. 4–6, 2000, pp. 29–34. DOI 10.1109/WACV.2000.895399.

[4] Y. Zhu, T. Tan, and Y. Wang, "Biometric personal identification on iris patterns," in Proc. 15th Int. Conf. Pattern Recogn. 2000, vol. 2, pp. 805–808.

[5] L. Ma, Y. Wang and D. Zhang, "Efficient iris recognition by characterizing key local variations" IEEE Trans. Image Process., vol. 13, no. 6, pp. 739–750, Jun. 2004.

[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 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.

[8] F. Besbes, H. Trichili, and B. Solaiman, "Multimodal biometric system based on fingerprint identification and Iris recognition," in Proc. 3rd Int.IEEE Conf. Inf. Commun. Technol.: From Theory to Applications (ICTTA 2008), pp. 1–5. DOI: 10.1109/ICTTA.2008.4530129.

[9] 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.

[10] Fingerprint Verification Competition FVC2002. (2009, Nov.). [Online].Available: http://bias.csr.unibo.it/fvc2002/

[11] UB Iris Database, University of Beira Interior, Portugal. Available: http://iris.di.ubi.pt/ubiris1.html

[12] Austin Hicklin, Brad Ulery, Craig Watson "A Brief Introduction to Biometric Fusion" 16 June 2006.

[13] M. L. Pospisil, "The human Iris structure and its usages," Acta Univ. Palacki Phisica, vol. 39, pp. 87–95, 2000.

[14] V. Shiv Naga Prasad, Justin Domke, "Gabor Filter Visualization".

[15] Hong-Bo Deng, Lian-Wen Jin, Li-Xin Zhen, Jian-Cheng Huang" A New Facial Expression Recognition Method Based on Local Gabor Filter Bank and PCA plus LDA", International Journal of Information Technology Vol. 11 No. 11 2005