Enhancing the Performance of Iris Recognition System using Matching Score Fusion Technique

Dr.S.R.Ganorkar, A.P.Ligade

Abstract— As biometrics, iris always a preferred trait because of its uniqueness of pattern contain by each eye and lifetime stability. The random distribution of features in an iris image texture allows performing iris based person authentication with high confidence. But use of single iris image indicator often has to contend with noisy sensor data, physiological defects, and unacceptable error rates. So this paper proposed an iris recognition algorithm in which an image of left iris and right iris are use as an input. DCT can be employed to extract unique iris pattern and encode it into binary template. Then allows comparison between current and stored template using hamming distance. This process is applied on left iris and right iris separately and corresponding distance scores are generated for each eye. This score are then combined using weighted average fusion rule to generate final score. This score is compared with threshold to decide the person is genuine or imposter. Simulation studies are made to test the validity of the proposed algorithm. The results obtained ensure the superior performance of this algorithm. This ensures the presence only alive person and increases recognition rate by eliminating the possible spoofing attacks.

Index Terms— Accuracy, authentication system, biometrics, DCT, fusion techniques, hamming distance, iris trait.

1 INTRODUCTION

Biometric recognition or biometrics refers to the automatic authentication of a person based on his/her physiological or behavioral characteristics. Biometric recognition offers many advantages over traditional PIN number or password and token-based (e.g., ID cards) approaches. A biometric trait cannot be easily transferred, forgotten or lost, the rightful owner of the biometric template can be easily identified, and it is difficult to duplicate a biometric trait. Some well-known examples of traits used in biometric recognition are fingerprint, iris, face, signature, voice, hand geometry, retina, and ear. Biometric technology has now become a viable and more reliable alternative to traditional authentication systems in many security applications including access control, forensic investigation, identity verification, information protection and security monitoring. Iris recognition has received increasing attention in recent years as it provides promising solution to security issues due to its uniqueness, stability and non-invasiveness. The human iris, a ring like structure sandwiched between the black colored central pupil region and white sclera region in the human eye, has a very complex fiber like structure which can be inscribed to formulate a biometric template. The human iris, evolved out of chaotic morphogenetic processes. It has also been shown to remain consistent over a lifetime of a human. Unlike fingerprints, typically, an iris image is captured using A non-contact imaging process and has shown potential of deployment in real time applications. Iris recognition process takes eye image as input and produces an output called iris code, which is the mathematical representation of the iris region in binary format. There are several requirements that need to be met by a particular biometric trait when being considered for use in an authentication system. These requirements are[1]: (i) universality, which means that each individual should possess the trait, (ii) distinctiveness, which means that the trait for two different persons should be sufficiently different to distinguish between them, (iii) permanence, which means that the trait characteristics should not change, or change minimally, over time. Biometric systems operating on a single biometric feature called unimodal system. It has many limitations. They are inherently varied because of the existence of background noise, signal distortion, biometric feature changes and environment variations. As a result recognition based on a single biometric trait may not be sufficiently robust and it has a limited ability to overcome spoofing attack.

Multimodal biometric systems are a recent approach developed[2] to overcome these problems. These systems demonstrate significant improvements over unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing. The key to multimodal biometric system is the fusion of various biometric modality data.

The paper is organized as follows: Section 2 present the review of literature. Section 3 gives information about different fusion techniques used in multimodal biometric authentication system. Section 4 describes the

- *Dr.S.R.Ganorkar is currently working in electronics and telecommunication engineering Dept. in Sinhgad college of engineering, University of Pune, India, PH-9422514726. srgomom@rediffmail.com*
- *A.P.Ligade is currently pursuing masters degree program in electronics and telecommunication in University of Pune,India, PH-9403076288. ashwiniligade5@gmail.com*

implementation biometric system. Finally some results and conclusions are reported in Section 5 and 6 resp.

2 LITERATURE SURVEY

Human iris possesses genetic independence and contains extremely information-rich physical structure and unique texture pattern which makes it highly complex enough to be used as a biometric signature. Statistical analysis reveals that the iris is the most mathematically unique feature of the human body because of the hundreds of degrees of freedom it gives with the ability to accurately measures its texture.

Daugman[4] made use of multiscale Gabor filters to demodulate texture phase structure information of the iris. Filtering an iris image with a family of filters resulted in 1024 complex-valued phasors which denote the phase structure of the iris at different scales. Each phasor was then quantized to one of the four quadrants in the complex plane. The resulting 2048-component iriscode was used to describe an iris. The difference between a pair of iriscodes was measured by their Hamming distance. Vatsa et al.[5] applied a set of selected quality local enhancement algorithms to generate a single high-quality iris image. A support-vector-machine-based learning algorithm selects locally enhanced regions from each globally enhanced image and combines these good-quality regions to create a single high-quality iris image. Two distinct features are extracted from the high-quality iris image. The global textural feature is extracted using the 1-D log polar Gabor transform, and the local topological feature is extracted using Euler numbers. An intelligent fusion algorithm combines the textural and topological matching scores. It gives accuracy (97.21%) with an average identification time of less than 2 s. Wildes et al. [6] represented the iris texture with a Laplacian pyramid constructed with four different resolution levels and used the normalized correlation to determine whether the input image and the model image are from the same class. Snelick et al. [7] used a directional filter bank to decompose an iris image into eight directional subband outputs and extracted the normalized directional energy as features. Iris matching was performed by computing Euclidean distance between the input and the template feature vectors.

Generally, unimodal biometric recognition systems present different drawbacks due its dependency on the unique biometric feature. For example, feature distinctiveness, feature acquisition, processing errors, and features that are temporally unavailable can all affect system accuracy. A multimodal biometric system should overcome the aforementioned limits by integrating two or more biometric features.

Ross and Jain [8] have presented an overview of Multimodal Biometrics and have proposed various levels of fusion, various possible scenarios, the different modes of operation, integration strategies and design issues. They have shown that combination approach performs better than some classification methods like decision tree and linear discriminant analysis. Apart from fusion of multi classifiers, much work has also been done to combine traits/modalities at various levels. Conti,et al.[9] proposed the fusion of iris and face modalities and reported that besides improving verification performance, the fusion of these two has several other advantages. Theoretical framework [10] for combining classifiers using sum rule, median rule, max and min rule are analyzed under the most restrictive assumptions and have observed that sum rule outperforms other classifiers combination schemes. The fusion methods include sum rule and product rule in rule-based fusion and support vector machines, multilayer perceptrons and binary decision trees in learning-based fusion. Besbes et al. [11] proposed a multimodal biometric system using fingerprint and iris features. They use a hybrid approach based on: 1) fingerprint minutiae extraction and 2) 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 considering the unimodal decision through an "AND" operator.

This section has discussed the literature survey of the existing techniques for iris recognition system in detail which shows many researcher is going on to improve system performance and to avoid intrusion attacks.

3 FUSION TECHNIQUES

Biometric systems that utilize more than one physiological or behavioral characteristics for identification are called multimodal biometric systems. Fusion produces a single image by combining information from a set of source image together. Fusion image contains greater information content than any one of the individual image. Biometric fusion is generally classified in terms of categories and levels[8]. Categories define what inputs or processes are being used for fusion and levels define how the fusion performed. Table 1 below illustrates the five multibiometric categories.

3.1 Categories of fusion

1. Multi-sensor: A single biometric trait is captured using multiple sensors.
2. Multi-algorithm: It processes the same biometric trait using multiple algorithms.
3. Multi-instance: Fusion of multiple instances of the same individual traits like image of left and right fingerprint.
4. Multi-sample: The same biometric trait can be acquired no of times by using single sensor.
5. Multi-modal: Fusion of multiple biometric traits. For e.g. fingerprint and face, iris and face, etc.

TABLE 1
COMPARISON BETWEEN THE FIVE MULTIBIOMETRIC CATEGORIES

Category	Modality	Algorithm	Biometric trait	Sensor
Multi-sensor	1	1	1	2 or more
Multi-algorithm	1	2 or more	1	1
Multi-instance	1	1	2 instance of 1 trait	1
Multi-sample	1	1	2 sample of 1trait	1
Multi-modal	2 or more	2 or more	2 or more	2 or more

3.2 Levels 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 over-all 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 matching score level.

4 AUTHENTICATION SYSTEM

In this section we explain the implementation of recognition system. A unique significant characteristic of the iris is that, no two irises are similar, even for identical twins, among the human population. To study the characteristics of the irises, we will only deal with samples of the grey-level profiles and use these to construct a representation. Input images are reprocessed to extract the portion containing the iris. The iris image contains not only abundant texture information, but also some useless parts, such as eyelid, pupil, etc. The iris portion is present between the pupil (inner boundary) and the sclera (outer boundary). Iris recognition can be used for verification (1:1 matching) as well as identification (1: N matching). The proposed multimodal biometric system is composed of two main stages as shown in fig 1:

1. Enrollment phase: The biometric templates are processed and stored into the database.
2. Verification phase: A new biometric template (called the query template) is extracted from the user who wants to be identified, and it is compared with the data already stored (reference template).

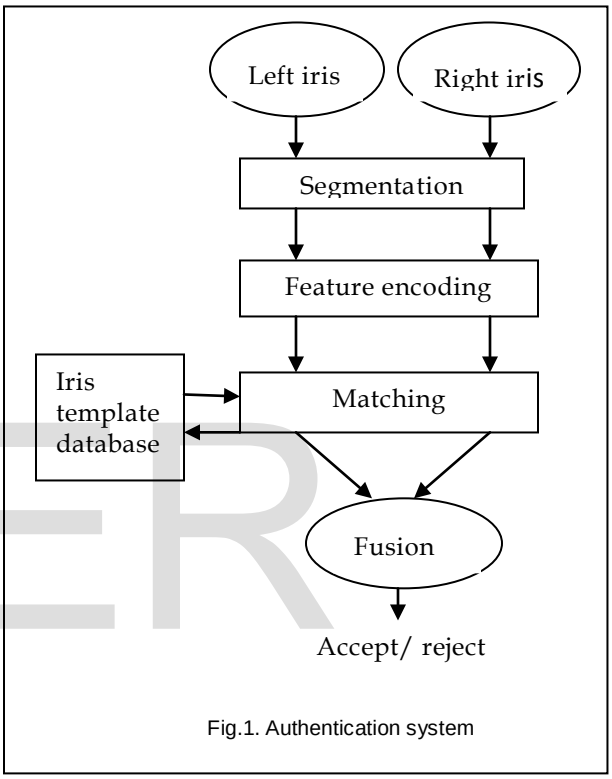

Fig.1. Authentication system

4.1 Implementation

1. Iris segmentation and normalization: It is a significant module in iris recognition. The iris image is first fed as input to the canny edge detection algorithm that produces the edge map of the iris image for boundary estimation. The exact boundary of pupil and iris is located from the detected edge map using the Hough transform.

$$(x-a)^2 + (y-b)^2 = r^2 \quad \text{.....(1)}$$

where a & b are the centre of the circle in the direction x and y respectively and r is the radius.

Daugman`s Rubber Sheet Model is utilized for the transformation process. It converts the circular iris image into rectangular format. This process is called as normalization.

2. Feature extraction: The normalized 2D form image is disintegrated up into 1D signal, and these signals are made use to convolve with 1D DCT transform.

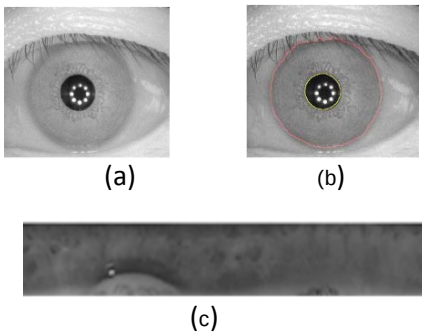

Fig.2. iris segmentation algorithm output a) original image b) final iris and pupil boundary c) normalized image

3. Matching: Matching is a process to determine whether two iris templates are from the same individual or not.

Hamming distance (HD): It is applied for bit-wise comparisons of images. Noise in the iris image is masked and only significant bits generated from the true iris region are used in the Hamming distance calculation between two iris templates.

$$HD = \frac{\|(codeA \times codeB) \cap (maskA \cap maskB)\|}{\|(maskA \cap maskB)\|} \quad \ldots\ldots\ldots\ldots\ldots\ldots(2)$$

where A and B are two normalized iris images, code A and code B are the bit-codes of A and B, mask A and mask B are respectively the masks of noise of A and B.

4. Fusion technique matching score level: Each system provides a matching score indicating the proximity of the feature vector with the template vector. These scores can be combined to assert the veracity of the claimed identity. Score level fusion is commonly preferred in multi-biometric systems because matching scores contain sufficient information to make genuine and impostor case distinguishable and they are relatively easy to obtain. matching scores for a pre-specified number of users can be generated even with no knowledge of the underlying feature extraction Therefore, combining information obtained from individual modalities using score level fusion seems both feasible and practical. Since the scores generated by a biometric system can be either similarity scores or distances scores.

Weighted average fusion rule: It is a very promising multimodal biometrics fusion approach. The simplest form of combination would be to take the weighted average of the scores from the multiple units. This strategy was applied to all possible combinations of the two iris units. Equal weights were assigned to each unit. Given the matching scores of left iris(Sl) and right iris(Sr), then the fused score is obtained by linearly combining the two scores as,

$$S = \frac{(1-\beta)\times Sl + \beta \times Sr}{2} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3)$$

where β is a combination weight that can be computed using training data or made dependent on the quality of input. The set of weights that minimizes the total error rate (sum of the false accept and false reject rates) at some specified threshold is chosen. If more than one set of weights minimize the total error rate, then the set of weights that assigns almost equal weights to all the modalities is chosen. The threshold is set to a common value for users.

5 Experimental Results

The reliability of the proposed multimodal biometric authentication system is described with the help of experimental results. The system has been tested using CASIA iris image database created by National Laboratory of pattern recognition, Institute of Automation, Chinese Academy of Science is used for obtaining iris images. From this dataset, 100 left and 100 right iris templates comparisons were made and the results were taken up for score level fusion later.

TABLE2
COMPARISON BETWEEN LEFT IRIS, RIGHT IRIS AND FUSION RULE

Threshold	Left eye		Right eye		Fusion by average rule	
	FRR	FAR	FRR	FAR	FRR	FAR
0.05	97.4	0.4	96.2	0	98.4	0
0.11	9.8	5.2	9.4	5.8	3.6	2.6
0.20	0	100	0	100	0	100
accuracy	90.23%		92.05%		96.40%	

The performance measures used in our analysis are False Acceptance Rate (FAR), False Rejection Rate (FAR). Table 2 shows the set of values obtained for different thresholds. Graphs are plotted for FAR and FRR by considering different threshold value as shown in Fig 3 and Fig 4.

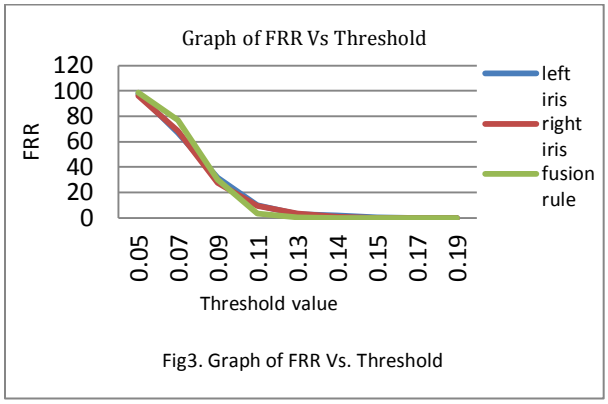

Fig3. Graph of FRR Vs. Threshold

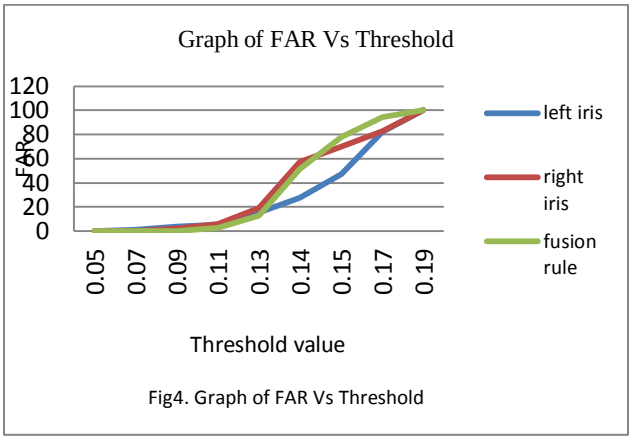

Fig4. Graph of FAR Vs Threshold

Thus the performance of multi-unit iris shows that there is a very good improvement in the recognition rate of multi unit system compared to the use of either left or right iris.

6 Conclusion

Unimodal biometric systems fail in case of lack of proper biometric data for a particular trait. It is robust to use multiple biometrics for providing authentication. This paper proposed an efficient algorithm which helps to improve the accuracy of recognition system. Feature encoding and matching are derived by DCT and HD respectively. Fusion of matching scores of left eye and right eye is used because matching scores contain sufficient information to make genuine and impostor case distinguishable. They are relatively easy to obtain. The performance analysis is made using the publicly available CASIA database and the recognition rates are found to be 90.23% and 92.05% for left and right iris respectively. In order to improve the accuracy, a score level fusion of distances obtained from left and right irises is performed using weighted average rule method. This shows a very good enhancement in the recognition rate to 96.4%, compared to the usage of left or right iris alone.

Acknowledgment

I am sincerely thankful to my guide Dr. 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.

References

[1] K. Nandakumar and A. K. Jain, "Multibiometric based on feature-level fusion," *in Proc. IEEE 2nd Int. Conf. on information, and Security*, vol.7, no.1, Feb.2012. (IEEE Transactions}

[2] Norman Poh, Josef Kittler "A Unified Framework for Biometric Expert Fusion Incorporating Quality Measures," *IEEE Transactions on pattern analysis and machine intelligence*, Vol. 34, no. 1, January 2012. (IEEE Transactions)

[3] Nagar, K. Nandakumar, and A. K. Jain, "Multibiometric cryptosystems "Department of Computer Science and Engineering, Michigan State University, Tech. Rep. MSU-CSE-11-4, 2011.

[4] J. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Trans. Pattern Analy. Machine Intell.*, vol. 15, pp. 1148–1161, Nov. 1993

[5] M. Vatsa, R. Singh, and A. Noore, "Improving iris recognition performance using segmentation, quality enhancement, match score fusion, and indexing," *IEEE Trans. Syst., Man, Cybern. B, Cybern.*, vol. 38, no. 4, pp. 1021–1035, Aug. 2008.

[6] R. Wildes, J. Asmuth, G. Green, S. Hsu, R. Kolczynski, J. Matey, and S. McBride, "A machine-vision system for iris recognition," *Machine. Vision .Application .*, vol. 9, pp. 1–8, 1996.

[7] R. Snelick, U. Uludag, A. Mink, M. Indovina, A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems", *IEEE Trans- actions on Pattern Analysis and Machine Intelligence* 27 (3) (2005) 450–455.

[8] Ross & A. K. Jain, "Information Fusion in Biometrics", *Pattern Recognition* Letters, 24 (13), pp. 2115-2125, 2003

[9] 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.

[10] J. Kittler, M. Hatef, R. P. W. Duin, & J. Mates, "On combining classifiers", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(3), pp. 226–239, 1998

[11] 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* (ICTTA2008), pp. 1–5. DOI: 10.1109/ICTTA. 2008. 4530129.

[12] Nagar, S. Rane, and A. Vetro, "Privacy and security of features extracted from minutiae aggregates," *in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, Dallas, TX, Mar. 2010, pp. 524–531.

[13] T. Ignatenko and F. M. J. Willems, "Biometric systems: Privacy and secrecy aspects," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 4, pp. 956–973, Dec. 2009.

[14] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney, "An adaptive multimodal biometric management algorithm," *IEEE Trans. Syst., ManCybern. C, Appl.* Rev., vol. 35, no. 3, pp. 344–356, Aug. 2005.

[15] K. Miyazawa, K. Ito, T. Aoki, K. Kobayashi, and H. Nakajima, "An effective approach for iris recognition using phase-based image matching," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 30, no. 10, pp. 1741–1756,Oct. 2008.

[16] W. W. Boles and B. Boashash, "A human identification technique using images of the iris and wavelet transform," *IEEE Trans. Signal Process.,vol.* 46, no. 4, pp. 1185–1188, Apr. 1998.

[17] Ross, K. Nandakumar, A. Jain, Score normalization in multimodal biometric systems, *Pattern Recognition* 38 (2005) 2270–2285.

[18] T.C. Sabareeswari, S. Lenty Stuwart "Identification of a Person using Multimodal Biometric System", *Internnational journal of computer application*(0975-8887)Vol.3-No.9,July 2010.