

# Multi Biometric System by Iris and Fingerprint

Chowdhury Md. Mizan, Sudeep Ghosh, Tridib Chakroborty, Moumita Das, Swarnava Sengupta,

Sandip Mondal, Suman Dey, Swarup Mondal, Biswarup Nayak

Department of Information Technology, Guru Nanak Institute of technology, Kolkata, India

**Abstract**—In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance. The reason to combine different modalities is to improve recognition rate.

The aim of multi biometrics is to reduce one or more of the following: FAR (False Acceptance Rate): It is a measure of the percent of invalid inputs that are incorrectly accepted.

**Keywords**—component, biometric, iris, verify, accept

## 1. Introduction

Biometrics refers to identity verification of persons according to their physical or behavioral characteristics. Many physical body parts and personal features have been used for biometric systems: fingers, hands, feet, faces, irises, retinas, ears, teeth, veins, voices, signatures, typing styles, gaits, doors, and DNA. Person verification based on biometric features has attracted more attention in designing security systems [1]. However, no single biometrical feature can meet all the performance requirements in practical systems [2]. Most of biometric systems are far from satisfactory in terms of user confidence and user friendliness and have a high false rejection rate FRR. There is a need for development of novel paradigms and protocols and improved algorithms for human recognition. Unimodal biometric systems use one biometric trait to recognize individuals. Multimodal biometric systems use multiple modalities to overcome the limitations that arise when using single biometric trait to recognize individuals. Multiple biometric systems perform better than unimodal biometric systems. The use of only one biometric trait susceptible to noise, bad capture, and other inherent problems makes the unimodal biometric system unsuited for all applications. Many works in the literature have demonstrated that the drawbacks of the unimodal biometric systems are mainly genuine and imposters identification failure due to the intraclass variations and the interclass similarities, while the drawbacks associated with multimodal biometrics are increased complicity of the system with two or more sensors [2–6] and thus higher cost, as well as inconvenience of using several biometrics. So, identification of person with high accuracy and less complexity of the system is becoming critical in a number of security issues in our society. Iris and fingerprint biometrics are more simple, accurate, and reliable as compared to other available traits. These properties make their fusion particularly promising solution to the authentication problems today. Moreover, fusion of iris and fingerprint is more reliable than fusion of each one with another biometric like face [7]. However, iris biometric has more features and stability and resistance to attacks than fingerprint biometric; despite this, the conventional fusion

methods still use the same weight in fusion for each single biometric, and this is the reason for why their best error rates are far from perfect. False accept rate identifies the number of times an imposter is classified as a genuine user by the system and false reject rate pertains to misidentification of a genuine user as an imposter. Although ideally both FAR and FRR should be as close to zero as possible in real systems, however, this is not the case [8]. For an ideal authentication system, FAR and FRR indexes are equal to 0. To increase the related security level, system parameters are then fixed in order to achieve the FAR = 0% point and a corresponding FRR point [9]. In this paper a novel combination of iris and fingerprint biometrics is presented in order to achieve best compromise between a zero FAR and its corresponding FRR; in our approach, iris trait has more weight in fusion with fingerprint and the system decision is made to have more intermediate values between bad and good recognition; the weight is simply an appreciation we assign to the matching distance for each single biometric set by fuzzy membership function and we use major concepts of fuzzy logic introduced by Zadeh [10] which are fuzzy sets, fuzzy membership function, and fuzzy inference system. The fuzzy inference system mimics our human thinking and this is mainly the reason we get enhanced results.

## 2. Aim/Objective

As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent. In recent years, biometrics authentication has seen considerable improvements in reliability and accuracy, with some of the traits offering good performance.

The reason to combine different modalities is to improve recognition rate.

The aim of multi biometrics is to reduce one or more of the following: FAR (False Acceptance Rate): It is a measure of the percent of invalid inputs that are incorrectly accepted. FRR (False Reject Rate): It is a measure of the percent of valid inputs that are incorrectly rejected.

CER (Crossover Error Rate): The rate at which both the accept and reject errors are equal, a lower value of the CER is more accurate for Biometric System.

### 1. Future Scope of The Project

Biometric technologies are rapidly becoming a part of the daily life of people around the world. Through integration with mobile devices, many of us interact with some form of

biometric authentication daily. The future of biometric trends is medicine, banking services, marketing research, and many other industries in which personal identification is required.

The Future of Biometric Security

Secure Data Storage

Business Applications

Mobile Payment

Online Banking

Immigration Services

Covering Government Needs

Staff Management etc.

#### 4. State of the Art of Multi Biometric

In this section we summarize the main ideas and principals involved in the area of multimodal biometric recognition.

##### 4.1. Fusion in Biometry

In order to join two or more biometric traits, a method called “fusion” is used [12]. Fusion in biometry refers to the process of combining two or more biometric modalities. In this section we present the different scenarios of fusion used by multimodal biometric systems. It is worth noting that the multimodality does not involve the use of multiple biometric modalities in the strict sense of the term (such as combining iris and fingerprint), but its meaning is broader as defined in the following by the various scenarios of fusion (see Figure 1).

Figure 1.

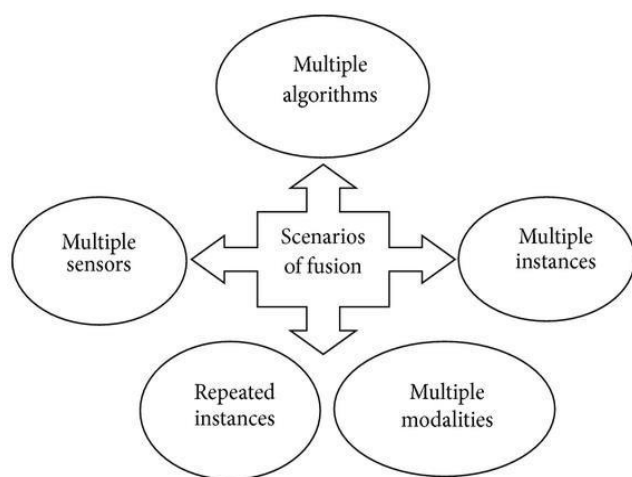


Figure 1

Fusion scenarios of multimodal systems.

##### 4.1.1. Level of Fusion

Five levels of fusion in multimodal systems were introduced in the literature [4, 12] which are the following.

(1) *Sensor Level*. Multisensorial biometric systems sample the same instance of a biometric trait with two or more distinctly different sensors [14]. Processing of the multiple samples can be done with one algorithm or combination of algorithms. Example face recognition application could use both a visible light camera and an infrared camera coupled with specific frequency.

(2) *Feature Level*. The feature level fusion is useful in classification [14]. Different feature vectors are combined,

obtained either with different sensors or by applying different feature extraction algorithms to the same raw data [21].

(3) *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 [9].

(4) *Rank Level*. Instead of using the entire template, partitions of the template are used. Ranks from template partitions are consolidated to estimate the fusion rank for the classification [18]. Rank level fusion involves combining identification ranks obtained from multiple unimodal biometrics. It consolidates a rank that is used for making final decision [19].

(5) *Score Level*. It refers to the combination of matching scores provided by the different systems. The score level fusion techniques are divided into two main sets: fixed rules (AND, OR, majority, maximum, minimum, sum, product and arithmetic rules) and trained rules (weighted sum, weighted product, fisher linear discriminate, quadratic discriminate, logistic regression, support vector machine, multilayer perceptions, and Bayesian classifier) [22].

Figure 2 shows the five levels of biometric fusion.

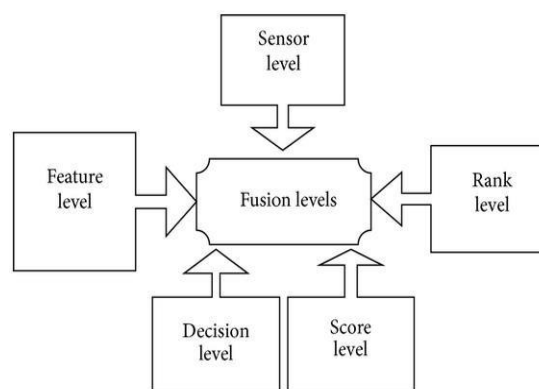


Figure 2

Levels of fusion in multimodal biometric systems.

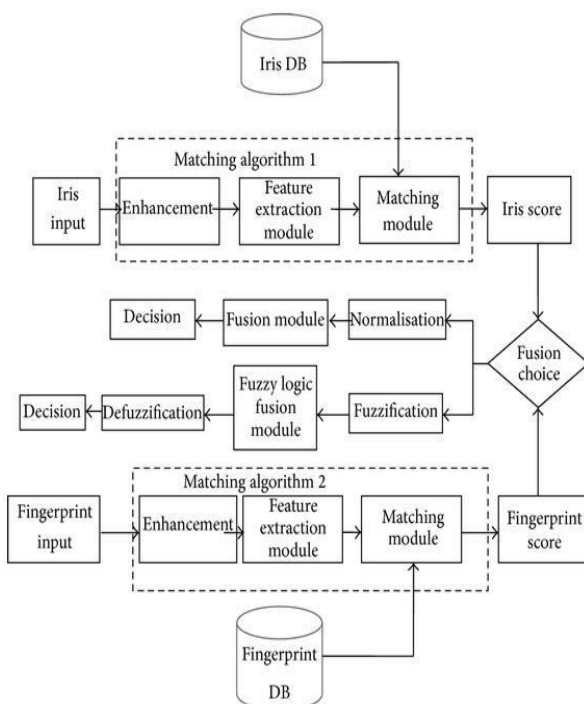
##### 4.1.2. Normalization

Score normalization brings both matching scores between 0 and 1 [23]. The normalization of both scores by the min-max rule are given by where and are the matching scores obtained from iris and fingerprint modalities, respectively, and are the minimum and maximum scores for iris recognition and are the corresponding values obtained from fingerprint trait. Other normalization algorithms also exist, like-score, Tan H and Sigmoid which gave very good results. Tan H method gave the best result but it involved a lot of parameters. Z-score and min-max are simple but they are insensitive to the presence of outliers [17].

#### 5. Proposed Scheme:

Figure 3 shows the different stages included in our multimodal recognition system and the overall system design shows the following.(i)The level at which the biometric information of the iris and fingerprint are fused is

indicated (here two levels are used: the score level fusion is used for the classical fusion and the decision level fusion is used for the fusion with fuzzy logic). (ii) The fusion approach used is the approach by combining scores when the method of fusion is classic. (iii) The other fusion approach used is fusion of decisions when the method of fusion is fuzzy. (iv) The normalization of scores is required prior to the fusion only for the classical fusion (which is explained by the use of the approach by combining scores for both classical sum rule matching and matching by the linear weighted sum rule). (v) Fusion by fuzzy logic does not require normalization of scores and only decisions are used by the fuzzy inference system. (vi) Three matching algorithms are used: the classical sum rule matching, the weighted sum rule matching, and our proposed matching with fuzzy logic.



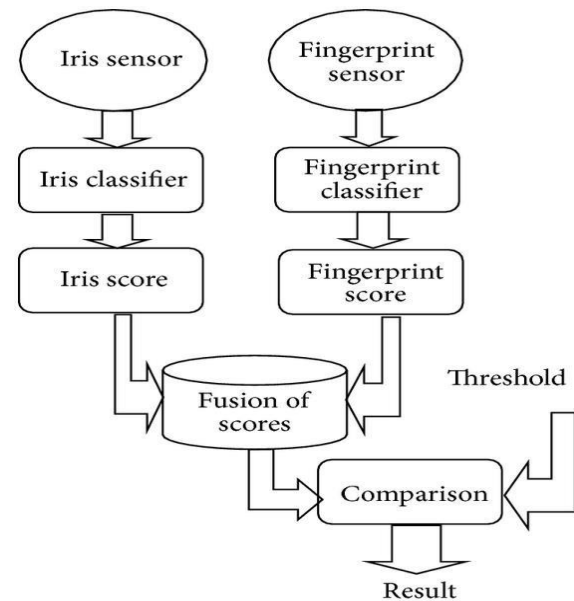
**Figure 3**

Flow chart of the application showing the main modules of the multimodal biometric recognition system.

The conventional fusion methods [2–4, 9, 11–17] use the same weight for each single biometric trait, but some biometric traits are more precise than the other ones; they have more stability and resistance to attacks. So in our approach, iris trait has more weight in fusion with fingerprint. Weight here is not a number assigned to the matching score, but a decision with intermediate values related to the matching distance.

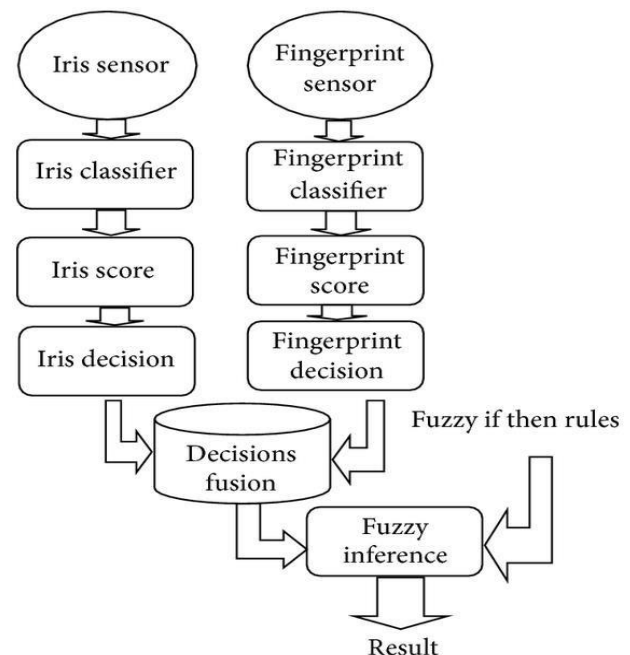
In this work, we have implemented two different architectures of the combined iris and fingerprint biometric recognition system in order to compare the recognition results (in terms of time, accuracy, and error rates) of both system architectures and conclude the best one. The first system architecture (see Figure 4) is based on the classical fusion of scores. The second system architecture (see Figure

5) is based on our proposed fuzzy logic matching using iris and fingerprint decisions.



**Figure 4**

Score level fusion using iris and fingerprint biometric modalities.



**Figure 5**

Decision level fusion using iris and fingerprint biometric modalities.

## 5.1. Classical Matching Strategies

### 5.1.1. Hamming Distance Based Matching

For the iris modality we use the hamming distance-based matching:

The hamming distance HD is calculated using formula (3), where  $a$  and  $b$  are the models to compare bit by bit, and  $n$  is the

noise masks for and, and is the number of bits represented by each model. For the fingerprint modality we use the Euclidian distance-based matching (see formula (4) where  $\mu_1$  and  $\mu_2$  are the models to compare.

### 5.1.2. The Sum Rule Based Matching

After the normalization of both iris and fingerprint scores, the score of fusion is calculated as presented by formula (5) where  $S_f$  is the score of fusion and  $S_i$  is the number of the scores, here.

### 5.1.3. The Weighted Sum Rule Based Matching

After the normalization of fingerprint and iris scores, the score of fusion is calculated as presented by formula (6) where  $S_f$  is the score of fusion,  $S_i$  and  $S_j$  are respectively, the scores of the biometric modalities to be combined, and  $S_k$  is the weight assigned to each modality.

In our experimentation we set to 0.8 for the iris modality and for the fingerprint modality.

### 5.2. Fuzzy Logic Based Matching

Our proposed fuzzy matching algorithm assigns a specific appreciation to each decision according to the best threshold minimizing both FRR and FAR. The fuzzy if-then rules produce decisions according to the matching distance calculated for each modality.

For that, (i) we define two fuzzy variables for the input: "finger" for the fingerprint trait and "iris" for the iris trait, (ii) we define the output fuzzy variable: "fusion," (iii) each variable is represented by a trapezoidal fuzzy set, (iv) for the inputs, we define three fuzzy sets according to the matching distance: bad, medium, and good, (v) the output is fuzzy: either very bad or bad or medium or good or very good, or excellent.

As shown by Figure 6,  $[a, b]$  is the interval of thresholds belonging to the fuzzy set "good,"  $[c, d]$  is the interval of thresholds belonging to the fuzzy set "medium,"  $[e, f]$  is the interval of thresholds belonging to the fuzzy set "bad."

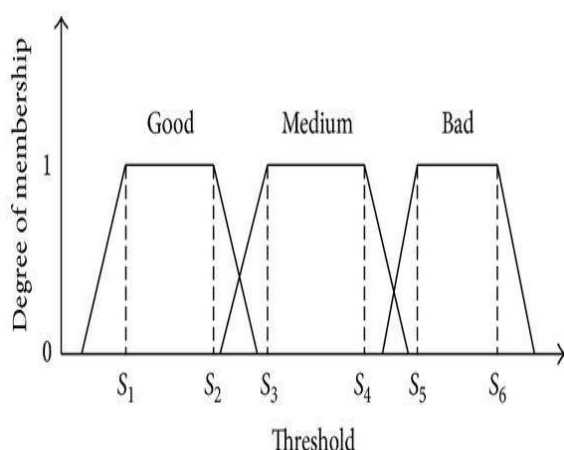


Figure 6

Fuzzy sets of the proposed entries and their trapezoidal membership functions.

The fuzzy if-then rules: combining decisions from iris and fingerprint modalities respect the following fuzzy rules: If(finger is bad) and (iris is bad) then (fusion is very bad) If(finger is bad) and (iris is medium) then (fusion is medium) If(finger is bad) and (iris is good) then (fusion is good) If(finger is medium) and (iris is bad) then (fusion is bad) If(finger is medium) and (iris is medium) then (fusion is

good) If(finger is medium) and (iris is good) then (fusion is very good) If(finger is good) and (iris is bad) then (fusion is medium) If(finger is good) and (iris is medium) then (fusion is very good) If(finger is good) and (iris is good) then (fusion is excellent).

We have set the if-then rules according to the following criteria: (i) the iris decision is more reliable than the fingerprint decision, so we give more weight to the iris decision in fusion with the fingerprint decision, (ii) the fusion decision is one of the following sets: very bad, bad, medium, good, very good, excellent, (iii) in the cases where the iris decision is "bad," the fusion decision should be either "bad" or "very bad" or "medium" even if the fingerprint decision is good, (iv) in the cases where the iris decision is "good," the fusion decision should be either "good" or "excellent" even if the fingerprint decision is "bad."

## 6. System Implementation

The programming language used to implement our system is MATLAB 7.10.0(R2010a). MATLAB as well as its interactive environment is a high-level language that allows the execution of tasks requiring high computing power and whose implementation will be much easier and faster than with traditional programming languages such as C, C++. It has several toolkits in particular image processing "Image Processing Toolbox" which proposes a set of algorithms and graphical reference tools for the processing, analysis, visualization, and image processing algorithm development. Our application is implemented on a laptop (HP630) Intel CORE I3 CUP M370 with 2 Giga byte of RAM and 320 Giga byte hard drive disk HDD and has a 2.40 GHz speed. The minimum required material characteristics for the application are 512 Megabyte of RAM and 80 Giga byte hard drive. To perform tests with our application, we use four databases which are as follows. (i) CASIA-Iris V1 [24], CASIA V1, contains 756 images from 108 eyes. For each eye, 7 images are captured in two sessions with a homemade iris camera, where three samples are collected in the first session and four in the second session. All images are stored as BMP format with resolution 320 \* 280. (ii) CASIA-Iris V2 [25] contains 2400 images from 120 eyes. For each eye, 10 images are captured using two different instruments (OKI and Pattek). All images are stored in BMP format with resolution 640\*480. CASIA-Iris V2 contains blurry images with different illuminations and wearing glasses is authorized. The database is available for free on demand. (iii) FVC 2004 [26] contains four sets DB1\_A, DB2\_A, DB3\_A, and DB4\_A. Each of these databases contains 800 fingerprints equivalent of one hundred (100) individuals each having eight (08) impressions. FVC 2004 database is characterized by different fingerprint image qualities. The database is purchased upon request. (iv) Our proposed database of combined irises and fingerprints made from an equivalent number of irises from CASIA-Iris V2 database and fingerprints from FVC2004 database (50 subjects 10 images).

For a given database if represents number of classes and represents total number of images per class, then intraclass combinations are calculated as  $(C_n^k)$  and interclass



combinations are calculated as  $(7 - 1) \times (7/2) \times 108$  and inter-class combinations are worked out as  $(108 \times 107 \times 7 \times 7)$ .

For the database CASIA-V2, the intra-class combinations are worked out as  $(20 \times (20/2) \times 120) = 22800$  and interclass are worked out as class combinations  $(120 \times 119 \times 20 \times 20) = 5,712,000$ .

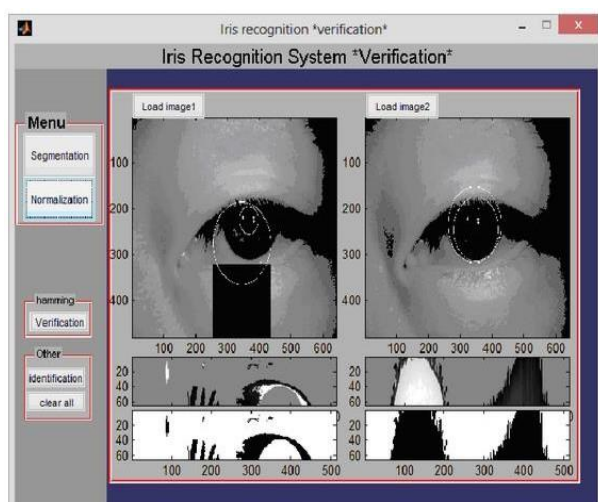
For database FVC 2004, intra-class combinations are worked out as  $(800 \times (800/2) \times 4) = 1,278,400$  and inter-class combinations are worked out as  $(4 \times 3 \times 800 \times 800) = 7680000$ .

## 7. Results

The application is divided mainly into three modules.

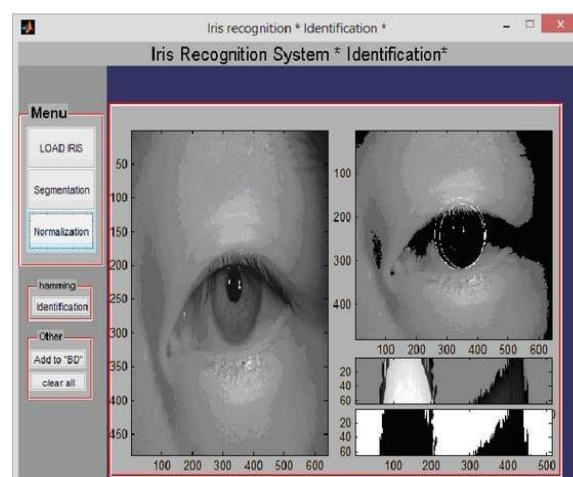
### 7.1. Iris Recognition Module

Both verification and identification processes are implemented. Figures below present the graphical user interfaces GUIs allowing the user to load an iris image from a database and to do segmentation, feature extraction, and either verification (see Figure 7) (the user has to upload another iris image) or identification (see Figure 8) (the system searches similar code in database).



**Figure 7**

GUI of the verification process in the iris monomodal recognition system.

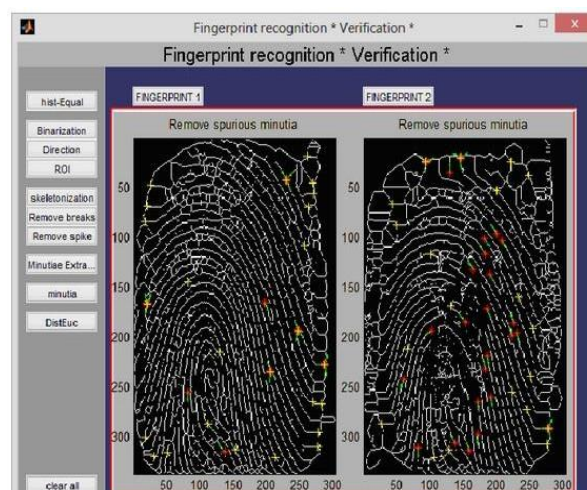


**Figure 8**

GUI of the identification process in the iris monomodal recognition system.

### 7.2. Fingerprint Recognition Module

Like the iris recognition module, both verification and identification processes are implemented. Figure 9 shows the GUI allowing the user to load two fingerprint images and then visualize the results of each step of the fingerprint recognition algorithm (binarization, region of interest and the orientation field localisation, the process of image thinning also called skeletonization, the extraction of minutia, the elimination of false minutia, and finally the matching by the Euclidian distance).



**Figure 9**

GUI of the verification process in the fingerprint monomodal recognition system.

The identification process in the fingerprint monomodal recognition system consists of matching the generated code from the input image with all codes stored in databases; if the identification failed, the user is asked either to add or not the nonidentified image to a chosen database (see Figure 10).

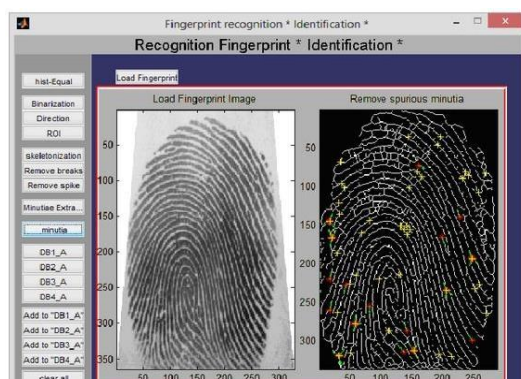


Figure 10

GUI of the identification process in the fingerprint monomodal recognition system.

### 7.3. Combined Iris and Fingerprint Recognition Module

Three matching algorithms are implemented; first is the matching using the fusion of iris and fingerprint by the sum rule, second is the matching of both modalities by the weighted sum rule, and the final is the matching using the fusion by the fuzzy logic if-then rules and the fuzzy inference system.

Figure 11 shows the GUI allowing the user to see the verification result of iris and fingerprint combined biometric traits.

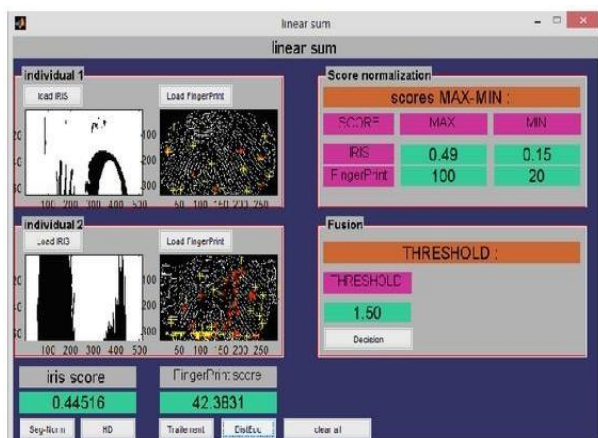


Figure 11

GUI showing the matching using the fusion by the sum rule

### 7.4 Performance Evaluation and Comparison

In order to test our proposed schemes for monomodal and multimodal biometric recognition systems and proceed with their evaluation and comparison, we do the following experiments.

**Experiment 1.** Both verification and identification processes are implemented within a monomodal iris recognition system. We use the public code of Masek and Koveski [28] for the verification and we extend it to perform the identification. The feature extractor employed for Iris modality is based on Doughman's approach [29] and was implemented by Masek and Koveski [28]. An Iris code comprising bit streams called Iris code by Doughman is generated. The hamming distance-based matcher provides the matching score. The experiment uses CASIA-V1 iris database.

**Experiment 2.** Both verification and identification processes are implemented within a monomodal iris recognition system. Like Experiment 1, we use the public code of Masek and Koveski [28] for the verification and we extend it to perform the identification. The experiment uses CASIA-V2 iris database.

**Experiment 3.** Both verification and identification processes are implemented within a monomodal fingerprint recognition system and we propose a minutia based fingerprint recognition system using the algorithm of Jayadevan et al. [16] to localize the region of interest and the orientation field, and the algorithm of Jain et al. [30] for the extraction of minutiae and posttreatment. Matching is based on Euclidian distance. The experiment uses FVC2004 fingerprint database.

**Experiment 4.** Only verification process is implemented within a multimodal biometric recognition system of combined iris and fingerprint using the sum rule-based matching. The experiment uses an equivalent number of images from CASIA Iris-V2 and FVC2004 fingerprint databases (5 from each modality 50 subjects).

**Experiment 5.** Only verification process is implemented within a multimodal biometric recognition system of combined iris and fingerprint using the weighted sum rule-based matching. The experiment uses an equivalent number of images from CASIA Iris-V2 and FVC2004 fingerprint databases (5 from each modality 50 subjects).

**Experiment 6.** Only verification process is implemented within a multimodal biometric recognition system of combined iris and fingerprint using our proposed fuzzy logic-based matching. The experiment uses an equivalent number of images from CASIA Iris-V2 and FVC2004 fingerprint databases (5 from each modality 50 subjects). For all the tests, we use the FVC2004 testing protocol [26] for the fingerprint and iris recognition modules.

The fingerprint testing protocol is described as) Genuine recognition attempts: the template of each impression is matched against the remaining impressions of the same individual, but avoiding symmetric matches. (ii) Impostor recognition attempts: the template of the first impression is matched against the first impression of the remaining individuals, but avoiding symmetric matches.

The iris testing protocol is described as follows. (i) First the database is divided into two parts: 40% of the database is reserved to enrolment in order to estimate the classifier parameters, and 60% of the database is used to test and validate the classifier. (ii) Genuine recognition attempts: the template of each iris is matched against the remaining irises of the same individual, but avoiding symmetric matches. (iii) Impostor recognition attempts: the template of the first iris is matched against the first iris of the remaining individuals, but avoiding symmetric matches. For experiments using fusion module, tests are conducted on a set of images belonging to 50 subjects having five fingerprint images from FVC 2004 fingerprint database and five iris images from CASIA-Iris V2 database.

#### 7.4.1. Time Execution Comparison

The values presented in Table 1 are results of execution time using CASIA V1, CASIA V2, and FVC 2004 databases and MATLAB 7.10.0(R2010a) programming tool.

Table 1

Matching time comparison.

We note that the fastest system in terms of matching recognition time is the monomodal fingerprint recognition system and this is mainly due to the use of the Euclidean distance in the matching phase (see Table 1).

Our experimental results shows that the fuzzy logic method for the matching scores combinations at the decision level is the best in terms of matching time followed by the classical weighted sum rule and the classical sum rule in order.

#### 7.4.2. Results in Terms of Error Rates FRR, FAR, and EER

The false reject rate (FRR), also known as type I error, measures the probability of an enrolled individual not being identified by the system. The false accept rate (FAR), also known as type II error, measures the probability of an individual being wrongly identified as another individual [28]. According to the statistical analysis in which we have calculated the inter-class and the intra-class thresholds using the above experiments, whose values minimize the rates of false acceptance and false rejection, we have estimated the best thresholds for minimal error rates for each experiment. See Tables 2, 3, 4, 5, and 6 (values in bold are best FAR and FRR for corresponding threshold).

**Table 2**

Best FAR, FRR, and corresponding threshold for Experiment 1.

**Table 3**

Best FAR, FRR, and corresponding threshold for Experiment 2.

**Table 4**

Best FAR, FRR, and corresponding threshold using Experiment 3.

**Table 5**

Best FAR, FRR, and corresponding threshold for Experiment 4.

**Table 6**

Best FAR, FRR, and corresponding threshold for Experiment 5.

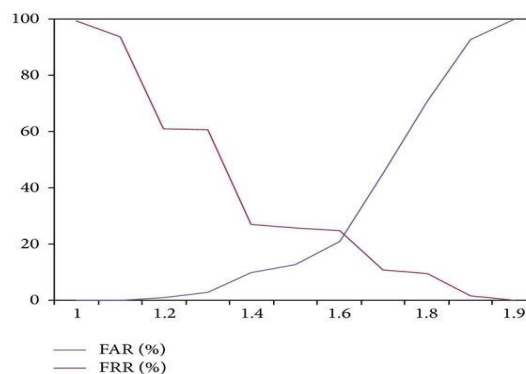
Unlike Experiments 1–5, we have no thresholds in Experiment 6 using our proposed fuzzy matching fusion algorithm, but we have decisions. Table 7 shows an example of its intra-class and inter-class distributions.

**Table 7**

Example of intraclass and interclass distributions using Experiment 6 (our proposed fuzzy matching fusion). According to our proposed fusion by fuzzy matching scheme based on if-then rules explained earlier, the results are either excellent or very good, or good or medium, or bad or very bad. The decision “medium” means that (i) either the fingerprint recognition result is “bad” and the iris recognition result is “medium”, (ii) or the fingerprint recognition result is “good” and the iris recognition result is “bad.” If we accept the decision “medium” as being genuine recognition of the individual so we achieve FAR = 0.16 and FRR = 0.0. If we reject the decisions “medium” as being imposter attempts so we achieve FAR = 0.0 and FRR = 0.05.

Experimental results show that the equal error rate calculated by Experiment 6 (our proposed fuzzy matching fusion) is EER = 0.038.

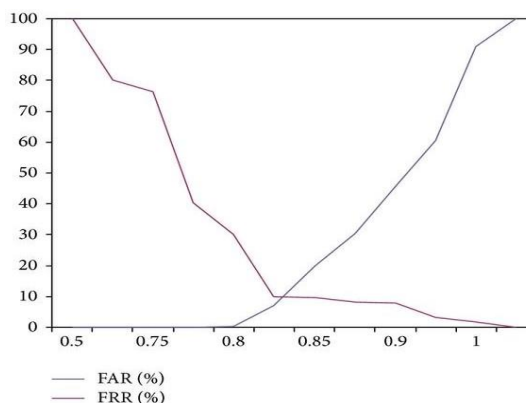
Figure 14 represents the plot of FAR and FRR using Experiment 4 (iris and fingerprint fusion based sum rule matching).



**Figure 14**

FAR and FRR using Experiment 4 (iris and fingerprint fusion-based sum rule matching).

As mentioned by Figure 14, the equal error rate for Experiment 4 is 1.55. Figure 15 represents the plot of FAR and FRR using Experiment 5 (iris and fingerprint fusion based weighted sum rule matching).



**Figure 15**

FAR and FRR using Experiment 5 (iris and fingerprint fusion based weighted sum rule matching).

Experimental results show that Experiment 5 achieves an equal error rate of 0.83. Here we compare the equal error rates of all the experiments we have carried out (see Table 8).

**Table 8**

Equal error rate comparison.

Table 8 presents an equal error rate comparison of the different recognition methods we have implemented; we see that Experiment 6 performing iris and fingerprint fusion by our proposed fuzzy logic matching method is the best followed by the weighted sum rule fusion based matching and finally the sum rule fusion based matching.

#### 7.3. Results in Terms of Accuracy

Table 9 presents accuracy comparison of all the experiments we have conducted.

**Table 9**

Accuracy comparison of all the implemented systems. In biometry, the system accuracy is calculated as follows: According to the results presented in Table 9, we conclude that the accuracy of the method of the fusion of decisions by fuzzy logic is better than that of the other techniques. This comparison is done to illustrate the fact that the proposed system provides improved results as compared to the results



from the individual unimodal systems and the results from the implemented multimodal systems using traditional matching.

#### 7.4. Comparison with Related Works in the Current Literature

Table 10 presents a comparison of the different recognition methods proposed and implemented in the current literature; we see that Experiment 6 performing iris and fingerprint fusion by our proposed fuzzy logic matching method is the better in terms of error rates than the other presented systems, and the matching time is comparable to that of Gawande et al.'s [20] system.

**Table 10**

Performance comparison with related systems.

#### 8. Conclusion

The objective of this research is the introduction of a novel matching approach for multimodal biometric recognition based on fuzzy logic. The biometric traits used in our work are iris and fingerprint.

In this paper a novel combination of iris and fingerprint biometrics is presented in order to achieve best compromise between a zero FAR and its corresponding FRR; in our approach, iris trait has more weight in fusion with fingerprint and the system decision is made to have more intermediate values between bad and good recognition and the weight is simply an appreciation we assign to the matching distance for each single biometric set by fuzzy membership function; the fuzzy inference system mimics our human thinking and this is mainly the reason we get enhanced results.

#### 9. References

1. R. Raghavendra, R. Ashok, and G. H. Kumar, "Multimodal biometric score fusion using gaussian mixture model and Monte Carlo method," *Journal of Computer Science and Technology*, vol. 25, no. 4, pp. 771–782, 2010. View at: [Publisher Site](#) | [Google Scholar](#)
2. J. Zhou, G. Su, C. Jiang, Y. Deng, and C. Li, "A face and fingerprint identity authentication system based on multi-route detection," *Neurocomputing*, vol. 70, no. 4–6, pp. 922–931, 2007. View at: [Publisher Site](#) | [Google Scholar](#)
3. A. Ross and A. K. Jain, "multimodal biometrics: an overview," in *Proceedings of the 12th European Signal Processing Conference (EUSIPCO '04)*, pp. 1221–1224, Vienna, Austria, September 2004. View at: [Google Scholar](#)
4. H. Ailisto, E. Vildjiounaite, M. Lindholm, S.-M. Mäkelä, and J. Peltola, "Soft biometrics-combining body weight and fat measurements with fingerprint biometrics," *Pattern Recognition Letters*, vol. 27, no. 5, pp. 325–334, 2006. View at: [Publisher Site](#) | [Google Scholar](#)
5. Google, Wikipedia