Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4145785, 11 pages
https://doi.org/10.1155/2022/4145785

Research Article

Performance Improvement of Multibiometric Authentication System Using Score Level Fusion with Ant Colony Optimization

E. Balraj[1] **and T. Abirami**[2]

[1]*Department of Information Technology, M.Kumarasamy College of Engineering, Karur, India*
[2]*Department of Information Technology, Kongu Engineering College, Perundurai, India*

Correspondence should be addressed to E. Balraj; balraje.cse@gmail.com

Received 6 April 2022; Revised 13 October 2022; Accepted 18 October 2022; Published 13 December 2022

Academic Editor: Petros Nicopolitidis

Biometric systems are widely used by many organisations to protect the data from anomaly users. Unimodal biometric systems have many problems like noisy data, nonversatility, and nonuniversality. To avoid these problems, multibiometric system is the most suitable approach where we can integrate more than two individual modalities. Our proposed framework is utilised to minimize the rate of error while working on the exhibition by utilising the methodology of Ant Colony Optimization in view of Score Level Fusion strategies. The proposed work will extract the highlights from two distinct modalities of individual people like iris and face. The proposed frameworks employ ACO as an optimization technique to choose the fusion parameters called weight to apply the fusion rule for different biometric matcher used for Score Level Fusion mechanism. The matching scores will be calculated based on the fusion methods like sum, tanh, mean, median, min, max, and product. Our proposed system implements and analyzes four different types of fusion mechanisms.

1. Introduction

Biometric authentication is a technique commonly used to determine an individual person by manipulating their physical or behavioural traits of person. It can be fingerprint, iris, palm print, or nail print. It is more secure than our traditional methods like passwords and ID cards, which can be easily stolen or modified by others. But, it has issues like variation in intraclass sensor data with noise, spoofing attacks, and nonuniversality. So, it is not possible for a unibiometric system to solve all the above properties. It drives the research to develop a multibiometric authentication system that combines information from multiple biometric evidence sources. Combining multiple biometric features will increase the accuracy and decrease the number of anomaly attacks [1]. By using a multimodel biometric authentication system, the information can be integrated with various levels such as Feature Extraction Fusion, Score Level Fusion, and Decision Tree Level Fusion methods. Using the Feature Extraction Fusion, it will combine multiple biometric features of the same person in the authentication process. By deploying Score Level Fusion, individual scores with multibiometric recognition are matched for the purpose of determining the multimodal score. In the Decision Tree Level Fusion, some of the logical operations will be performed on multimodal systems to obtain the final solution [2]. The Score Level Fusion system will be comprised of two stages, called the normalization process and fusion activity. The normalization process will be used to compare the scores of different traits of the same person with the specified range. By using this step, we can eliminate the contribution of lower-range biometric traits [3]. Ant Colony Optimization is one of the evolutionary approaches that play a major role in multibiometrics. It is used for acquiring the optimum solution over a large population. It is achieved through the searching and updating of the past history of the particle system [4].

Authentication equipment with biometrics comprises some physical features like fingerprints, facial-like patterns, and patterns that include retinal type patterns for verifying the identity of the user. Biometric authentication is becoming widespread for several functions, as well as network logon. A biometry template or symbol (an instance sample noted by a user having a license) should hold on during information on the device to match with a brand new sample given throughout the logon method. Biometry is typically employed underneath the sensible cards on great-security platforms. The most widespread kinds of biometry devices are the following:

(1) Fingerprint scanner: these devices are available from different vendors for computers and portable devices. It can be connected through a USB cable or a PCMCIA card. It is used to scan fingerprints

(2) Face recognizer: it is also widely used by all modern authentication system to recognise the face images. It uses digital photographic technology to recognise the facial images

(3) Hand geometric recognition device: it is similar to a face recognition system, but instead of face recognition, hand geometrics will be recognized. A mix of prisms and lightweight, the images of the hands are captured in raw format. Nonetheless, every side of the hand is considered, as well as a few sides such as the palm, front, and back. Whenever the images in raw format are considered, the hand with a 3D picture is created. For catching the better raw pictures potentially, 5 directing stakes are settled essentially at a lower place, along with a camera for guiding the person into appropriately situating their hand. A genuine blemish with this strategy is that the photos of those stakes are likewise caught. Subsequently, an extra time stretch is expected to base them out from the raw images

(4) Iris scanner: the recognition scanners for iris work by enlightening the iris with infrared radiation that is invisible for selecting the distinctive patterns provided, they are not observable to the eye. Iris scanners discover and never include some features like eyelids, eyelashes, and mirror-like reflections, which generally restrict the iris components

For the past few decades, the most accurate and reliable biometric authentication has been required for all modern applications. Any recognition system must satisfy the two important factors called security and performance [5]. To obtain a good result, we need a biometric system that will provide template protection and performance to achieve robustness. To protect our original biometric templates, a new concept was introduced with the following requirements "cancellable biometric."

(1) Diversity: it is the derivation of a new template from the original template

(2) Revocability: it denotes that a replacement model should be issued if a hold on protected model gets compromised

(3) Noninevitability: it states that the initial biometric guide must not be recovered from the protected one

To confirm the privacy of any user and to stop any risk of security thieving to boost performance, biometric fusion has been adopted in recent years, which mixes information from several biometric modals.

2. Existing System

Many researchers have demonstrated their work on multibiometric authentication systems with various fusion parameters. Some of the work is demonstrated here.

Kittler et al. proposed the theoretical framework for combining classifiers of various fusion parameters such as the front side of the face, its profile, including voice. The proposed module verification is done with the help of the M2VTS database. This database is comprised of speech with five minutes and eight seconds of video data covering 37 clients, normally belonging to a month. In the experiment, they used some of the classifier techniques, including product, sum, min, median, and voting with majority classifiers [6].

Dalila et al. proposed a hybrid model based on the GA-PSO approach, which can be used to combine biometric modalities at the score level. They used three publicly available multibiometric databases from NIST, XM2VT, and BANCA to validate the fusion level techniques they were used with a normalization scheme to perform score modalities. The results were analysed for EER accuracies and ROC curves [7].

Latha and Thangasamy. proposed a multibiometric system that combines the score of palm print and iris of an individual person. The threshold value is compared with the resulting score for taking the decision to accept or reject the person. This system uses ant colony optimization to select the optimal threshold value of the person employed. Results are obtained using CASIA iris and palm print databases, which give lower error rates and higher recognition systems. It is one of the best models which apply the ant colony optimization to improve the accuracy of biometric authentication systems [1].

Alford et al. proposed an optimal layout integrating multiple modalities of score matching, deploying the ratio including likelihood with common densities. The main reason for generalised density is that some ranges of scores can be discrete [8]. So, they presented two approaches for combining the evidence of generalised density. (i) The sum rule is used to assess the independence of individual traits. (ii) The copula rule is used to assess dependence between multiple traits. The experiments are done with the help of MSU and NIST databases [9].

Table 1 gives the summary of various score normalization techniques from the existing work. It has been analysed and summarised based on the three important features, such as distribution retainment, outlier sensitiveness, and common range mapping [10]. The best score normalization algorithm can be chosen based on the following 3 parameters: (1) Less susceptible to outliers (2). Scores should be within a reasonable range. (3) Preservation of original distribution [11].

Table 1: Comparison of various Score normalization algorithm.

Sl. No	Fusion rule	Distribution retainment	Outlier sensitiveness	Common range mapping
1	Min fusion	Yes	Yes	Yes
2	Max fusion	Yes	Yes	Yes
3	Mean fusion	No	Yes	No
4	Median fusion	No	No	No
5	Sum fusion	Yes	Yes	Yes
6	Tanh fusion	No	No	No
7	Product fusion	No	No	Yes

2.1. Popular Optimization Techniques

(1) Hunger game search [12] is population based optimization technique, which is specifically designed to solve both constrained and unconstrained problems. It is designed based on the animals hunger driven activities. It is conceived on the basis of the instructions of the logical calculation rules that will be calculated on the basis of the hunger of the animals associated with an adaptive weight

(2) Runge-Kutta method [13] is a stochastic component-based swarm intelligent technique to solve optimization problems. The RUN builds a set of guidelines for the development of a population set in accordance with the logic of the swarm-based optimization algorithm by using the computed slope as a searching logic to explore the promising area in the search space

(3) The Harris hawks optimizer [14] is a revolutionary population-based, nature-inspired optimization methodology (HHO).The cooperative attitude and surprise pounce pursuing technique of Harris' hawks in nature serve as the major sources of inspiration for HHO. Many hawks work together to attack on a victim from various angles in an effort to surprise it. Based on the dynamic nature of situations and the prey's fleeing movements, Harris hawks can exhibit a variety of pursuit strategies. In order to create an optimization method, this study mathematically duplicates such dynamic patterns and behaviours

Even though all the above techniques mentioned in Section 2.1 have given good results, it is also having certain demerits such as requires more computation time [14], hidden complexity [12], and less global optimization cost for multi model systems [13]. To address all this above points, our proposed work designed with ACO with Score Level Fusion to combine biometric features of iris and face using highly exploitation and exploration mechanism.

3. Why Ant Colony Optimization

Ant Colony Optimization (ACO)-Marco Dorigo was the originator of ACO in 1992. It is one of the best techniques to obtain an optimal solution based on the behaviour of an ant. In the initial stage, every ant has the same amount of pheromone level, which has been compared to each other's resources and similarity based on their position to get the best outcome in further iteration. The major important factors in ACO are called evaporation factor and Q-pheromone constant (these values are always less than 1). The initial value of every ant is chosen randomly from the available possible range of value [15].

An ant is a social insect which lives in colonies. The main goal of an ant is to search for food. When it is searching for food, it will look after the neighbouring colonies. An ant moves from one place to another in search of food. When it is moving from one place to another, it leaves a small organic component called pheromone. Ants communicate with one another through pheromone trails. When a certain amount of prey is found, it conveys up to the extent limit. The pheromone is stored while returning the way in light of the amount and its nature. The prey is observed by the ant. Thus, the remaining ants observe and follow the same path. The way is picked depending upon the level of pheromone and its likelihood, and all the maximum ants follow the same way. In the meantime, the quantity of pheromone deposited increases in a specific way.

The mechanism used by ACO is "exploitation and exploration." [16]Exploitation is a mechanism used to obtain the best solution among all the possible solutions and make other ants follow the best solution. Exploration is a mechanism that is used to identify the most promising path in a given workspace.

These are the steps that will be followed in ACO.

(1) Ants travel randomly from nest to destination by leaving the pheromone trails along the path and returning to the nest after taking the food. In this process, shorter paths will be identified by leaving more pheromone trails

(2) Ants normally follow the shortest path possible from all possible directions

(3) After evaporation of pheromone trails and updation of the shortest path, the longest path will not be available for the ants to travel. This evaporation process will help all the ant members follow the shortest path rather than the longest path by leading with one ant. This is done with the help of pheromone trails

3.1. Algorithm for Pheromone Updation of Every Ant. For every ant, objective function will be calculated based on the pheromone updation.

p is the evaporation factor, Q is the pheromone constant, E is the error calculated, $\tau_i\,(t)$ is the i^{th} solution pheromone level

If i^{th} solution is selected in i^{th} iteration

$$\tau_{\mathrm{i}}\,(t+1)=\rho^{*}\tau_{\mathrm{i}}\,(t)+\left(\frac{Q}{E}\right), \tag{1}$$

$$\tau_{\mathrm{i}}\,(t+1)=\rho^{*}\tau_{\mathrm{i}}\,(t). \tag{2}$$

The objective function $\mathrm{G}=\mathrm{CFA}^{*}\mathrm{FAR}\,(\alpha)+\mathrm{CFR}^{*}\mathrm{FRR}\,(\alpha)$ where $\mathrm{CFR}+\mathrm{CFA}=2$.

3.2. ACO Based Proposed Model. The population of ant is initialized in the D-dimensional space. Every ant can be represented as $X_{\mathrm{md}}=(x_{\mathrm{m1}},x_{\mathrm{m2}},\cdot\cdots x_{\mathrm{mD}})$ in which m represents the m^{th} solution and dimension D. Due to Score Level Fusion, every ant has "$N+2$" dimensions in which 2 represents the number of modalities used in the proposed work. Every ant can be represented with four factors.

$$X\mathrm{md}=\{W1,W2,\alpha,F\}. \tag{3}$$

$W1$ is the weight of modality 1, $W2$ is the weight of modality 2, α is the threshold value, and F is any one of the fusion method described in Equations (4)–(10).

3.3. Contribution of ACO. The primary augmentation of the proposed research deals with ACO for the premier choice of the authentication parameters needed for the fusion of multimodal biometrics. For the discrete area requirements, it is also a well-described and probabilistic approach [17]. It is easy to put into force and is less afflicted by the local minimum paradigm when compared with PSO. The subsequent motion for every ant relies upon the pheromone quantity deposited in the direction, and the better awareness is that it drives the ants to search for that route. But, the ACO algorithm does no longer provide the popularity of a path. Subsequently, there may be a necessity to introduce the update mechanisms in order to diagnose the local and global answers. They will have provisions for the ACO with local and global updates. With this approach, the idea of global and local updates is borrowed from PSO and applied for updating the possibilities for selecting each direction. The selection of each best path is chosen between lower and upper values of probabilities [18]. Due to these added advantages, ACO-based technique may operate with noticeably lower error rates than the commonly used PSO and especially score level fusion produces better performance with a lower error rate than other fusion mechanism.

4. Fusion Methods Adopted in Our System

There are different varieties of fusion mechanisms available under the umbrellas of serial, parallel fusion. Selecting the best fusion mechanism gives the better performance in multibiometric authentication system. There are lot of score level mechanisms have been proposed in later research. But, the majority of these mechanisms are focuses to improve the accuracy of the fusion mechanism. All those mechanisms are not directly comparable, which are proposed for different purposes. There are lots of factors that are existing to compare directly those mechanisms such as size of the dataset and quality. But, all these factors directly impact the performance of the system [19]. In this manner, it is hard for one to pick the best fusion strategy. We should not consider only the accuracy of fusion mechanism to choose the best mechanism. So, when we are selecting the fusion mechanism, the following factors need to consider for the better performance of our proposed system [20].

(i) Resource availability

(ii) Merits of the approach

(iii) Security system requirements

Based on the above three factors, Score Level Fusion is one of the most suitable techniques for the proposed multibiometric authentication system. Because our matching score contains enough information to obtain genuine case of a person, so combining information from individual modalities is easier in Score Level Fusion method [21]. There are three types of Score Level Fusion technique. (i) Transformation-based Score Level Fusion. (ii) Classifier-based Score Level Fusion. (iii) Density-based score level fusion [22].

4.1. Mean Fusion. It is a method which combines the face and iris score by taking their mean value. The final score of mean fusion ($\mathrm{SF}_{\mathrm{Final}}$) is given by

$$\mathrm{SF}_{\mathrm{Final}}=\frac{(x*S_{\mathrm{IRIS}-R}+y*S_{\mathrm{FACE}}+z*S_{\mathrm{IRIS}-L})}{3}, \tag{4}$$

where S_{IRIS-R} is the score of right iris, S_{FACE} is the score of face, S_{IRIS-L} is the score of left iris, and x, y, z are the weights associated with various traits. The Final score ($\mathrm{SF}_{\mathrm{Final}}$) is compared against with the threshold value. Based on the result, it authenticated the person is genuine or not.

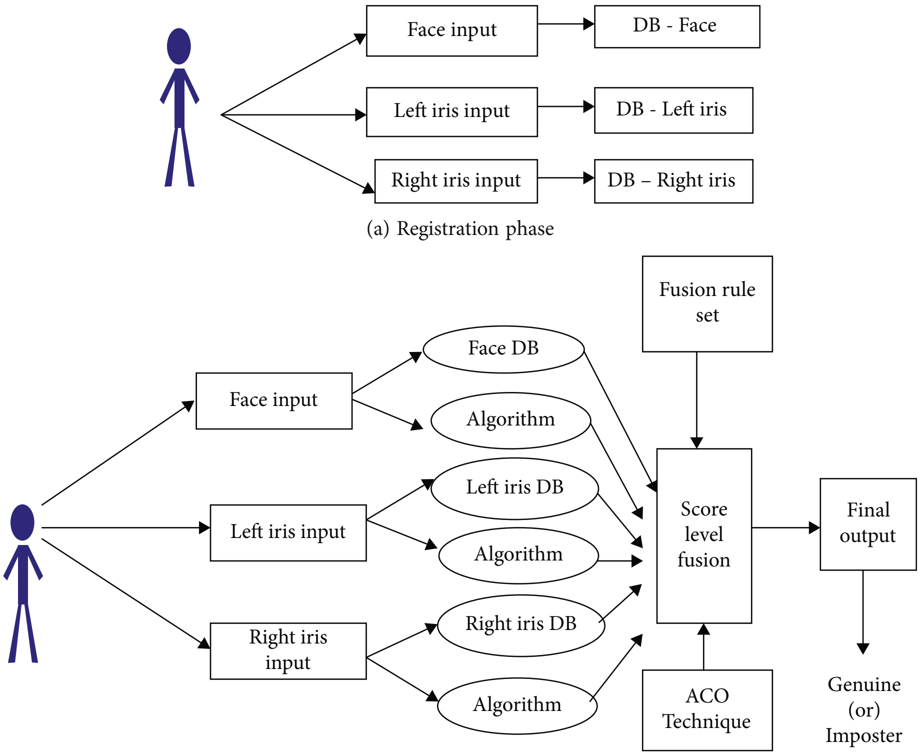
4.2. Min Fusion. This method is used to obtain the minimum score of the unimodel trait scores in the multimodal score value.

$$\mathrm{SF}_{\mathrm{Final}}=\min\,(S_{\mathrm{IRIS}-R},S_{\mathrm{FACE}},S_{\mathrm{IRIS}-L}). \tag{5}$$

4.3. Max Fusion. This method is used to obtain the maximum score of the unimodel trait scores in the multimodal score value.

$$\mathrm{SF}_{\mathrm{Final}}=\max\,(S_{\mathrm{IRIS}-R},S_{\mathrm{FACE}},S_{\mathrm{IRIS}-L}). \tag{6}$$

4.4. Sum Fusion. If there is a more noise which leads to ambiguity, so the individual classifiers posterior probabilities need to be computed such way that should not deviate from



(a) Registration phase

(b) Authentication phase

Figure 1: Architecture of multimodel biometric authentication system.

prior probabilities. The sum of those matching scores is given by

$$SF_{\text{Final}} = S_{\text{IRIS}-R} + S_{\text{FACE}} + S_{\text{IRIS}-L}. \tag{7}$$

4.5. Product Fusion. When there is different biometric trait that is mutually independent, the independence assumption of the multibiometric model can be measured by production fusion rule.The product of those matching scores is given by

$$SF_{\text{Final}} = S_{\text{IRIS}-R} * S_{\text{FACE}} * S_{\text{IRIS}-L}. \tag{8}$$

4.6. Tanh Fusion. The individual traits of the multibiometric model are combined by tanh hyperbolic sum of the score.

$$SF_{\text{Final}} = \tanh\left(S_{\text{IRIS}-R}\right) + \tanh\left(S_{\text{FACE}}\right) + \tanh\left(S_{\text{IRIS}-L}\right). \tag{9}$$

4.7. Median Fusion. This method is used to obtain the median score of the unimodel trait scores in the multimodal score value.

$$SF_{\text{Final}} = \text{median}\left(S_{\text{IRIS}-R}, S_{\text{FACE}}, S_{\text{IRIS}-L}\right). \tag{10}$$

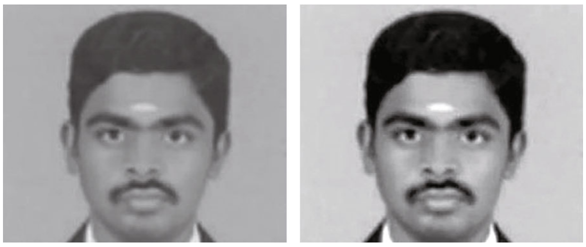


Figure 2: Comparison of original image and histogram equalized image.

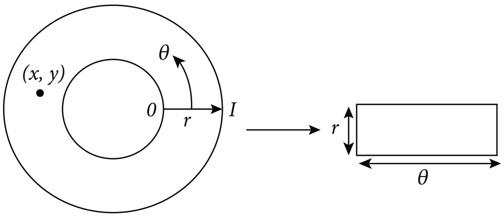


Figure 3: Rubber sheet model.

5. Proposed System

Our proposed system was an ACO-based multibiometric authentication system which improves the overall performance by using a Score Level Fusion technique. It extracts the two features of the individual person called the iris, face. The proposed system contains two phases. The first phase is called the registration phase—which is collecting the images of the face and iris of the individual person and storing them in the respective database. The second phase is called the authentication phase—the face and iris features extracted from the person are compared with existing scores of face and iris stored in the database, which is called SIRIS-R,

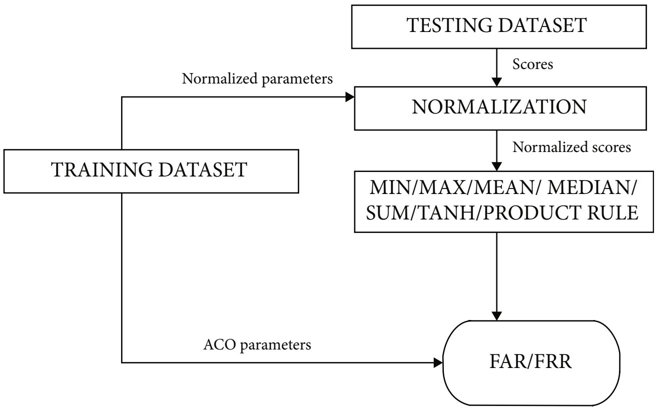


Figure 4: Execution flow of working model.

SFACE, and SIRIS-L. In this work, ACO is used as an optimization technique to select the fusion parameters SIRIS-R, SFACE, and SIRIS-L. The fusion rule is used to score level fusion. If the result is above the threshold value, then the user is considered genuine; otherwise, the user is an imposter. Figure 1 shows the architecture of proposed system.

5.1. Face Extraction. There are 3 phases in face feature extraction. First phase is called preprocessing, which is used to detect the facial images and identify the centre position location of the right and left iris of eyes. It is also used to measure the angle of our facial images (which is very helpful to adjust the head position of the image during authentication). Second phase is called image enhancement, which is used to improve the quality of the image. Third phase is called feature extraction; the facial images are transformed with the image size of 40 × 80 by using the mean variance normalization method or histogram equalization method, which is mainly used to remove the noise present in the image. Finally, by using the Manhattan distance formula to match scores calculated [23].

5.1.1. Histogram Equalization Method. It is one of the efficient image processing techniques, which are used to enhance the contrast of an image based on histogram [22]. To improve the contrast of an image, the most frequently pixel density values spread to entire image. By using this approach, the lower density pixels area of an image adjusted to higher density pixels. Because of this, the contrast of an image enhanced. Effectiveness of histogram equalization is shown in Figure 2.

5.2. Iris Extraction. There are 3 phases in iris feature recognition. First phase is called segmentation, it is used to separate the image of both the eyes from the whole image by using inner boundary and outer boundary method. There are 2 types of algorithms for iris segmentation which was proposed by Daugman and Wildes.

Daugman proposed segmentation method using integro-differential operators. It uses circular edge detectors to detect the outer and an inner boundary of the image. It is also used to detect the upper and lower boundaries of eyelids [24]. It is mathematically represented in the following form:

$$\max\,(r, x0, y0)\left|G\alpha(r)^{*}\left(\frac{\delta}{\delta r}\right)\int_{(r,x0,y0)}\frac{I(x,y)}{2\pi r}\,\mathrm{ds}\right|, \tag{11}$$

where r is the radius, (x_0, y_0) is the centre coordinates of eyelids, $_{\alpha}(r)$ is the Gaussian smoothing function, and $I(x, y)$ is the eye image.

Wildes proposed segmentation method using image intensity gradient and Hough transform [25]. Hough transform is a technique which is used to detect the parameters of any geometrical objects. Normally, for iris extraction, circular Hough transform is used to detect the centre position of iris regions [26].

$$h\left(x_j, y_j, x_c, y_{c,}r\right) = \begin{cases} 0 & \text{if } g\left(x_j, y_j, x_c, y_{c,}r\right) = 0, \\ 1 & \text{otherwise } g\left(x_j, y_j, x_c, y_{c,}r\right) = \left(x_j - y_j\right)^2 - \left(x_c - y_{jc}\right)^2 - r^2. \end{cases} \tag{12}$$

Second phase is called normalization. It is used to generate fixed dimension features of the image. Daugman proposed a model called rubber sheet model which is used to map the each points in the (x, y) region to any polar coordinates (r, θ). It is used to convert the images into fixed rectangular images. It was shown in Figure 3.

Third phase is called feature extraction. It is similar to face extraction.

Table 2: Fusion of face, left iris.

Th	FAR (%)	FRR (%)
0.8	0.2	23.95
0.9	0.4	21.25
1.0	1.3	18.11
1.1	2.8	15.74
1.2	4.3	13.16
1.3	6.4	11.02
1.4	9.8	7.19
1.5	11.7	4.83
1.6	14.0	3.14
1.7	16.1	1.46
1.8	18.9	0.44
1.9	21.3	0.22

Table 3: Fusion of face, right iris.

Th	FAR (%)	FRR (%)
0.8	0.19	22.27
0.9	0.5	18.67
1.0	0.8	16.19
1.1	2.8	14.51
1.2	4.3	12.26
1.3	6.4	10.79
1.4	9.6	7.19
1.5	10.9	4.83
1.6	12.9	3.14
1.7	14.4	0.89
1.8	16.6	0.56
1.9	19.8	0.11

Figure 4 represents the execution flow of our proposed system.

6. Experimental Results

Cost Factor Analysis (CFA) is used to determine the fusion parameters in ACO algorithm. It makes the algorithm to run faster [27]. Fusion parameters are calculated for every numeric value of CFA, which starts 1 and decreases 0.005 in every step to obtain the optimal solution. All the experiments are done in the range (0.005, 0.01) and finally we found that 0.01 is acceptable parameter. There are 15 ants involved to converge the solution for the algorithm with 50 iterations. The proposed framework is exhibited with by using "CASIA-IRIS-DISTANCE" database. It consists of 2639 images under 249 subjects (iris and face). The average size of extracted iris is 320 × 280.

The performance of our proposed system was measured with two parameters called False Acceptance Rate (FAR) and False Rejection Rate (FRR). It was represented in simple curve called ROC (Receiver Operating Characteristic) which plots the two parameters called FAR-probability and FRR-probability. FAR determines the numbers of invalid inputs that are incorrectly accepted by system. FRR determines the numbers of valid inputs that are rejected by the system.

$$\text{FAR}\,(\%) = \frac{\text{No of invalid inputs are incorrectly accepted}}{\text{No of samples}} \times 100,$$
$$\text{FRR}\,(\%) = \frac{\text{No of valid inputs are incorrectly rejected}}{\text{No of samples}} \times 100. \tag{13}$$

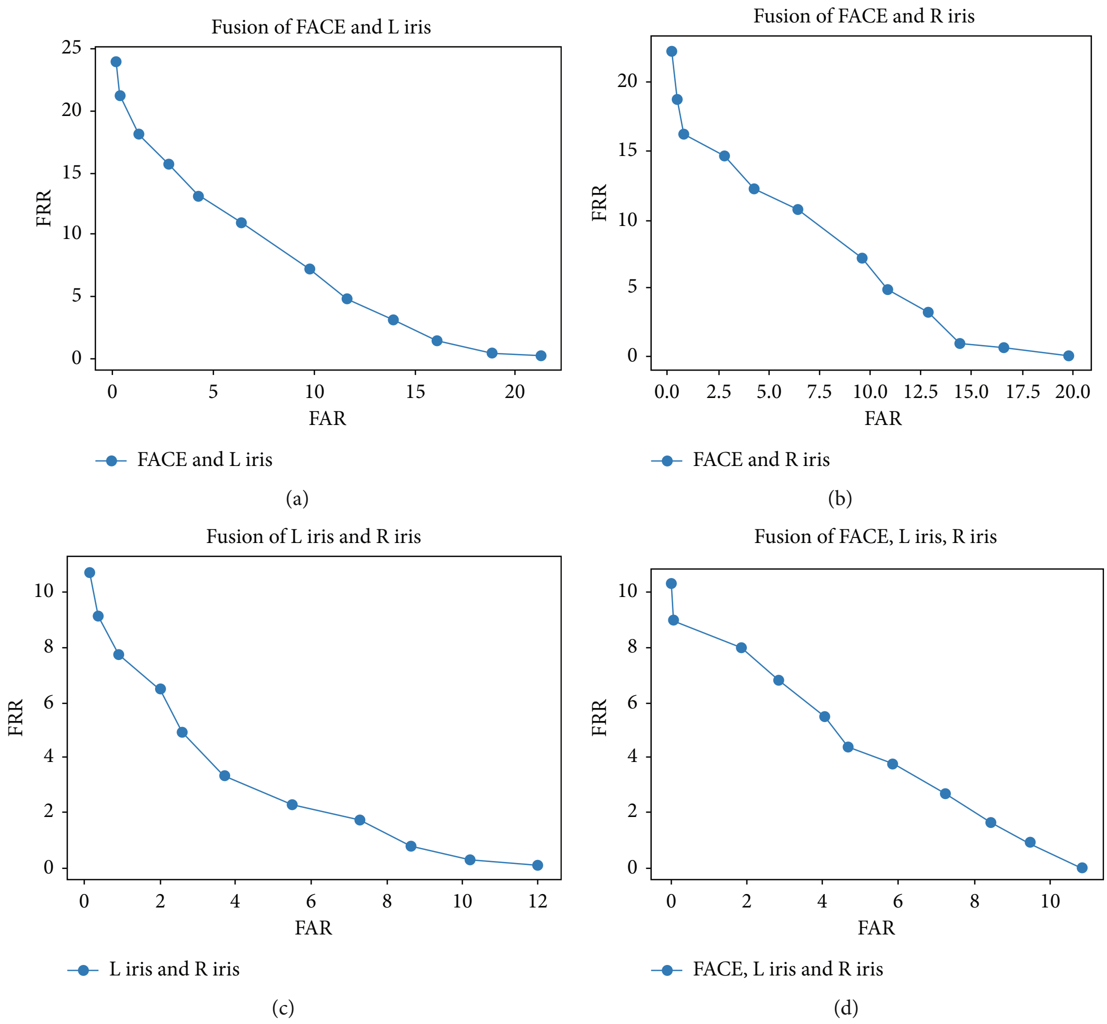
Table 4: Fusion of left iris, right iris.

Th	FAR (%)	FRR (%)
0.40	12.03	0.1
0.41	10.23	0.3
0.42	8.66	0.8
0.43	7.31	1.7
0.44	5.51	2.3
0.45	3.71	3.3
0.46	2.58	4.9
0.47	1.99	6.5
0.48	0.89	7.7
0.49	0.33	9.1
0.5	0.11	10.7

Table 5: Fusion of left iris, right iris, and face.

Th	FAR (%)	FRR (%)
0.40	10.86	0.1
0.41	9.47	0.9
0.42	8.43	1.7
0.43	7.24	2.7
0.44	5.85	3.8
0.45	4.68	4.4
0.46	4.04	5.5
0.47	2.87	6.8
0.48	1.81	7.9
0.49	0.09	8.9
0.5	0.01	10.2

To evaluate the effectiveness of our proposed work, two individual biometric traits of same person have been used in our system. Score Level Fusion is used to improve the security level. It has been done with the help of normalized scores of iris and face which are combined by using simple sum rule to carry out the fusion. There are 4 types of fusions done in our proposed work. Table 2 shows the experimental results of multimodel fusion of left iris and face. Table 3 shows the experimental results of multimodel fusion of right iris and face. Table 4 shows the experimental results of multimodel fusion of left iris and right iris. Table 5 shows the experimental results of multimodel fusion of left iris, right iris, and face.



(a)

(b)

(c)

(d)

Figure 5: ROC Curves of various fusion methods. (a) ROC curve shows the fusion of face and left iris with EER 8.36%. (b) ROC curve shows the fusion of face and right iris with EER 8.62%. (c) ROC curve shows the fusion of left iris and right iris with EER 3.51%. (d) ROC curve shows the fusion of face, left iris, and right iris with EER 4.54%. The lower Equal Error Rate gives more accuracy in the biometric system, as per figures, (d) which gives lower EER compare to remaining three fusion methods. So, fusion of left iris and right iris based on multimodel biometric system which gives the higher accuracy rather than any other fusion methods.

Table 6: Comparative study about various multimodel systems with Score Level Fusion mechanism.

Reference no	Author	Modality	Classification technique	Accuracy
[28]	Dhameliya and Chaudri	Fingerprint + palm print	Score level fusion	87%
[29]	Andersson and Araujo	Skeletal joints and gait	KNN	88%
[30]	Ankit et al.	Ear + face	FDA	90%
[31]	Le	Face	ANN	91%
[32]	Sheetal et al.	Face + iris + voice	Score level fusion	92%
[33]	Ujwalla et al.	Fingerprint + iris	Polynomial Kernal	94%
[34]	Hesham et al.	Face expressions	KNN	95.80%
[35]	Razzak et al.	Face, finger vein	Score level fusion	95%
[36]	Cui and Yang	Fingerprint, finger vein	Score level fusion	95%
**	Author	Left iris + right iris	Score level fusion	96.42%

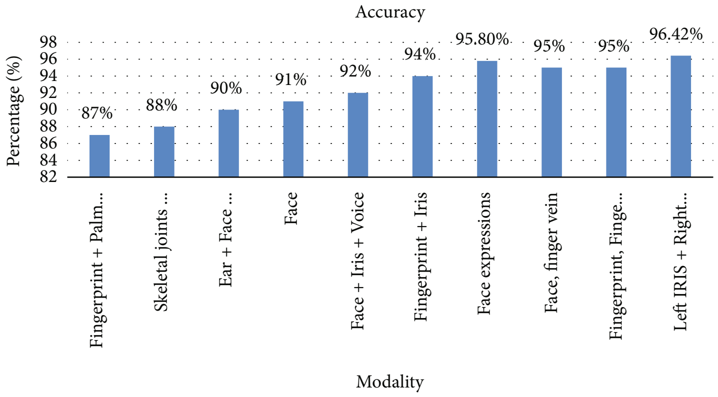


Figure 6: Comparison of proposed system accuracy with existing works.

The following table shows the results of Fusion of face with left iris. The accuracy results of this mechanism are represented as ROC curve in Figure 5(a).

The following table shows the results of fusion of face with right iris. The accuracy results of this mechanism are represented as ROC curve in Figure 5(b).

The following table shows the results of fusion of left iris with right iris. The accuracy results of this mechanism are represented as ROC curve in Figure 5(c).

The following table shows the results of fusion of left iris, right iris, and face. The accuracy results of this mechanism are represented as ROC curve in Figure 5(d).

Receiver Operating Characteristic (ROC) graph is one of the very efficient mechanism to showcase the performance of biometric authentication system. This graph gives the visual representation of series of FAR and FRR with different threshold values. In our proposed system, ROC curves are used to measure the EER. EER (Equal Error Rate) is where the FAR and FRR are equal in the curve. Biometric authentication system always expect FAR should be 0%. So, closer point of equality FAR and FRR in ROC curve gives the better performance.

The existing works mainly focused on palm print, fingerprint, skeletal joints, and gait, ear, face, voice, face expressions, and finger vein. But, our proposed system is analysed with various samples of iris and image. Any biometric system which will produce less error rate gives the better performance. In general, EER is used to measure the enhanced performance of biometric authentication system. Fusion of left iris and right iris given the less error rate compare to remaining other three fusion. So, EER of our proposed system is 3.51% with fusion of left iris and right iris. The accuracy of the proposed system is 96.42%. It is one of the very effective model which gives higher accuracy compared to the existing models. The various works related to the proposed system is demonstrated in Table 6. Figure 6 shows the comparison of our proposed system with existing models.

7. Conclusion

This paper proposed a multimodel biometric authentication system which combines the more than one trait of the same person to identify the person is genuine or imposter. Our proposed system uses two individual traits called face and iris which was combined by using Score Level Fusion mechanism to identify the matching scores. For combining more than one model, we have proposed extended ant colony optimization algorithm to normalize our results. The matching scores was calculated using sum rule of fusion level mechanism which gives better result rather than any other methods with of my best knowledge. There are 4 types of fusion mechanism applied to our proposed system. The experimental results show that fusion of left iris and right iris gives higher accuracy than remaining three fusion mechanisms. The proposed system significantly having advantages like reliability, increase the security and secrecy of information, accurate, high global optimization cost, and avoids intraclass variations. It is also having certain limitation such as integration issue (combining both metric). It takes little bit extra time to combine both biometric features from ACO using score level fusion.

8. Future Research

All the researchers are focusing on developing a model that combines only two biometrics of an individual's trait for authentication systems. Instead of that, a multimodal system can be developed with all the biometric traits of a person, such as the face, iris, palm vein, and fingerprint. Even if one biometric trait fails, the authentication can be done with other biometric traits of the person easily, and the accuracy of the system will be high. There are many optimization algorithms that have significant advantages with special features, especially algorithms like monarch butterfly optimization (MBO), slime mould algorithm (SMA), moth search algorithm (MSA), hunger games search (HGS), Runge-Kutta method (RUN), and Harris hawks optimization (HHO). All these algorithms have only minor disadvantages, such as less global optimization and integration with multimodel systems. With the help of modern deep learning algorithms, we can sort out this issue. By combining all these approaches, a full-fledged hybrid multimodel can be easily developed.

Data Availability

The datasets used for experimental analysis are CASIA-IRIS-DISTANCE dataset which is publicly available.

Conflicts of Interest

The authors have no conflicts of interest to declare.

References

[1] L. Latha and S. Thangasamy, "On improving the performance of multimodal biometric authentication through ant colony optimization," *WSEAS Transactions on Information Science and Applications*, vol. 8, pp. 453–463, 2011.

[2] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," in *Proc-IEEE Workshop on Automatic Identification Advanced Technologies*, pp. 59–64, NJ, USA, 1999.

[3] A. K. Jain and A. Ross, "Information fusion in biometrics," *Pattern Recognition Letters*, vol. 24, no. 13, pp. 2115–2125, 2003.

[4] M. Sandip Kumar and J. V. Kumar, "Enhancing performance of multibiometric system using ant colony optimization based on score level fusion," *International Journal of Computer Applications*, vol. 170, p. 6975, 2017.

[5] E. Balraj and T. Abirami, "A multibiometric authentication system using fusion level techniques," *International Journal of Scientific & Technology Research*, vol. 9, no. 1, pp. 3332–3335, 2020.

[6] J. Kittler, M. Hatef, R. P. W. Duin, and J. Matas, "On combining classifiers," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 3, pp. 226–239, 1998.

[7] C. Dalila, H. Imane, and N. A. Amine, "Multimodal score-level fusion using hybrid GA-PSO for multibiometric system," *Informatica*, vol. 39, no. 2, 2019.

[8] A. Alford, C. Hansen, G. Dozier et al., "GEC-based multibiometric fusion," in *2011 IEEE Congress of Evolutionary Computation (CEC)*, pp. 2071–2074, New Orleans, LA, USA, 2011.

[9] S. C. Dass, K. Nandakumar, and A. K. Jain, "A principled approach to score level fusion in multimodal biometric systems," in *Audio- and Video-Based Biometric Person Authentication. AVBPA 2005*, T. Kanade, A. Jain, and N. K. Ratha, Eds., vol. 3546 of Lecture Notes in Computer Science, pp. 1049–1058, Springer, Berlin, Heidelberg, 2005.

[10] T. M. Divyakanth and C. K. Kumbharana, "Comparative study of different fusion techniques in multimodal biometric authentication," *International Journal of Computer Applications*, vol. 66, p. 16, 2013.

[11] C. P. Chia, "Multimodal biometrics score level fusion using non-confidence information," Nottingham Trent University for the degree of Doctor of Philosophy, 2011.

[12] L. Sun, S. Chen, J. Xu, and Y. Tian, "Improved monarch butterfly optimization algorithm based on opposition-based learning and random local perturbation," *Complexity*, vol. 2019, Article ID 4182148, 20 pages, 2019.

[13] I. Ahmadianfara, A. A. Heidari, A. H. Gandomidm, X. Chue, and H. Chen, "RUN beyond the metaphor: an efficient optimization algorithm based on Runge Kutta method," *Expert Systems with Applications*, vol. 181, article 115079, 2021.

[14] B. K. Tripathy, P. K. R. Maddikunta, Q.-V. Pham et al., "Harris hawk optimization: a survey onvariants and applications," *Computational Intelligence and Neuroscience*, vol. 2022, Article ID 2218594, 20 pages, 2022.

[15] N. Pandey, O. Verma, and A. Kumar, "A hand-based biometric verification system using ant colony optimization," *Journal of Information Sciences and Computing Technologies*, vol. 7, no. 2, pp. 693–717, 2018.

[16] K. Veeramachaneni, L. A. Osadciw, and P. K. Varshney, "An adaptive multimodal biometric management algorithm," *IEEE Transactions on Systems, Man and Cybernetics, Part C (Applications and Reviews)*, vol. 35, no. 3, pp. 344–356, 2005.

[17] A. Kumar, V. Kanhangad, and D. Zhang, "A new framework for adaptive multimodal biometrics management," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 1, pp. 92–102, 2010.

[18] S. D. Patil, R. Raut, R. H. Jhaveri et al., "Robust authentication system with privacy preservation of biometrics," *Security and Communication Networks*, vol. 2022, Article ID 7857975, 14 pages, 2022.

[19] N. Srinivas, K. Veeramachaneni, and L. A. Osadciw, "Fusing correlated data from multiple classifiers for improved biometric verification," in *2009 12th International Conference on Information Fusion*, pp. 1504–1511, Seattle, WA, USA, 2009.

[20] R. Raghavendra, B. Dorizzi, A. Rao, and G. H. Kumar, "Particle swarm optimization based fusion of near infrared and visible images for improved face verification," *Pattern Recognition*, vol. 44, no. 2, pp. 401–411, 2011.

[21] A. Kumar and A. Kumar, "Adaptive management of multimodal biometrics fusion using ant colony optimization," *Information Fusion*, vol. 32, pp. 49–63, 2016.

[22] A. Kumar, M. Hanmandlu, and H. M. Gupta, "Ant colony optimization based fuzzy binary decision tree for bimodal hand knuckle verification system," *Expert Systems with Applications*, vol. 40, no. 2, pp. 439–449, 2012.

[23] A. Vora, C. N. Paunwala, and M. Paunwala, "Improved weight assignment approach for multimodal fusion," in *International Conference on Circuits, Systems, Communication and Information Technology Applications (CSCITA)*, pp. 70–74, Mumbai, India, 2014.

[24] J. G. Daugman, "High confidence visual recognition of persons by a test of statistical independence," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 15, no. 11, pp. 1148–1161, 1993.

[25] Z. Zainal Abidin, M. Manaf, A. S. Shibghatullah, S. H. A. Mohd Yunos, S. Anawar, and Z. Ayop, "Iris segmentation analysis using integro-differential operator and Hough transform in biometric system," *Journal of Telecommunication, Electronic and Computer Engineering*, vol. 4, pp. 41–48, 2015.

[26] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1348–1363, 1997.

[27] C. Chia, N. Sherkat, and L. Nolle, "Confidence partition and hybrid fusion in multimodal biometric verification system," in *International Conference on Biometrics ID Management and Multimodal Communication (BioID_Multi Comm' 09)*, vol. 5707, pp. 212–219, Madrid, Spain, 2009.

[28] M. D. Dhameliya and J. P. Chaudri, "A multimodal biometric recognition system based on fusion of palm print and fingerprint," *International Journal of Engineering Trends*, vol. 4, no. 5, pp. 1–4, 2014.

[29] V. Andersson and R. Araujo, "Person identification using anthropometric and gait data from kinect sensor," *Proc-Twenty-Ninth AAAI Conference on Artificial Intelligence*, vol. 29, pp. 425–471, 2015.

[30] G. Ankit, K. Abhishek, K. Nikit, and N. Lokesh, "A review on biometric recognition systems using ear and face," *International Journal of Science Technology & Engineering*, vol. 3, no. 6, p. 2349, 2016.

[31] T. H. Le, "Applying artificial neural networks for face recognition," *Advances in Artificial Neural Systems*, vol. 2011, Article ID 673016, 16 pages, 2011.

[32] C. Sheetal and R. Nath, "A new multimodal biometric recognition system integrating iris, face and voice," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 4, pp. 145–150, 2015.

[33] G. Ujwalla, Z. Mukesh, and K. Avichal, "A novel algorithm for feature level fusion using SVM classifier for multibiometrics-based person identification," *Applied Computational Intelligence and Soft Computing*, vol. 2013, Article ID 515918, 11 pages, 2023.

[34] A. Hesham, H. Galil, and M. Belal, "Benchmarking of convolutional neural networks for facial expressions recognition," *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 18, pp. 3104–3115, 2020.

[35] M. I. Razzak, R. Yuosf, and M. Khalid, "Multimodal face and finger veins biometric authentication," *Scientific Research and Essays*, vol. 5, no. 17, pp. 2529–2534, 2010.

[36] F. Cui and G. Yang, "Score level fusion of fingerprint and finger vein recognition," *Journal of Computer Information's Systems*, vol. 16, no. 1, pp. 5723–5773, 2014.