

GA based Feature Selection for Multimodal Biometric Authentication

A. Saravana Priya

Research Scholar, Department of Computer Science & Engg.,
St. Peters Institute of Higher Education and Research, Chennai.

Dr. Rajeswari Mukesh

Professor, Department of Computer Science & Engg.,
Hindustan Institute of Technology & Science, Chennai.
rajeswarim@hindustanuniv.ac.in

Correspondence author: A. Saravana Priya, e-mail: saravanapriya@gmail.com

Abstract

Multi-modal biometric authentication effectively replaces uni-modal biometric authentication system towards addressing a wide range of technical glitches in identity management and authentication. Legitimacy is playing a vital role in banking, military, and healthcare sectors where highly secure, strategic and confidential data transmission is involved. By integrating many independent biometric systems, one can overcome the problems of spoofing. However, there is lack of a simple, efficient and sufficient biometric authentication. Hence, the present study focuses on designing and implementing a multi-modal biometric authentication using a Genetic Algorithm (GA) based feature extraction method. The proposed research focuses on extracting human Skeleton and Human face feature using 3D Imaging technology. This modelling technique is used to capture human joints including the depth data to improve the efficiency of the system. The proposed research is subdivided into three phases. These are, image preprocessing (MinMax method), feature extraction using Heuristic Optimization Techniques (HOT), and Personnel recognition via the Artificial Neural Network (ANN). The Performance of the proposed method is evaluated based on the measure of FAR, FRR and accuracy. Finally, the performance of proposed approach is compared with existing techniques like GA, Neural network, etc. Combined Biometric is done in an unobtrusive way whereas other human recognition needs physical contact.

Keywords: biometric authentication system, multi-modal, skeletal, feature extraction, artificial neural network.

1.0 Introduction

Recently, biometric based person identification system and security issues are emerging area of interest in research [8] [13] [24] [39]. Subsequently, the automatic detection of individual depends on their behavioral and physiological characteristics referred as “biometric” [37] [38]. Due to similarity among the individuals most of the studies in literature review are focused on fingerprint, face, palm print [27] and iris [7]. Particularly, the challenges in the face recognition includes appearance, age changes, beard and makeup. Ear images are affected less by change of appearance or makeup when compared with face images and the combination of face/ear recognition leads to disturbance less recognition and has the benefit of easy to understand with the combination of face and ear recognition [43]. The needs of few high security application do not meet up since there is no high enough accuracies in existing methods. The combination of palm print and iris is suitable for this type of application. In literature survey, Gaussian mixture model has been used as a biometric fusion approach in order to differentiate authentic from fake clients and it was considered to be powerful likelihood ratio-based classifier [27]. The paper [6] concentrates at the matching score level on the combination of iris and palm print, even though it didn't investigate the combination of GMM with Score Normalization. The iris code was built for iris as the template and in order to match the pattern of two palms for palm print [18]. Further, the fusion strategy was adopted which is a type of likelihood ratio-based scheme [27].

Unfortunately, some of these characteristics can be easily intercepted: the face is publicly available, and fingerprint may remain on a surface unwittingly. As a result, once biometric information is stolen, it's counterfeit can be produced and it becomes difficult to reliably prove one's identity [40]. Further, there are certain limitation such as reduced universality of the chosen noisy data, biometric trait and uniqueness affect the single biometric systems [32] [29]. Further, uni modal biometric systems also affected due to non-universality, lack of uniqueness and noisy data. Hence, achieving real world application's desired performance may not be possible. In order to highlight the limitation, recently multi biometric system was proposed [16] [20] [37].

Furthermore, to improve the accuracy and security, multi biometric methods are currently used. Particularly, soft and behavioral biometric data differs from person to person which is difficult to copy and change [36]. The user data are highly robust and performance of recognition also be higher, Recently, researchers

are increased to train the soft and behavioral biometrics with their features such as Gait^[8] full body analysis^[39], pose-based identification^[31]. The present study focuses on the multi-model system specifically face and Skeleton feature extraction using Heuristic Optimization Technique and Artificial Neural Network.

1.1 Problem statement

Multi-modal biometric authentication is preferred over uni-modal systems as the latter suffers problems due to poor captured sensor data, noisy data, user's physiological and physical conditions, intra-class variations such as incorrect interaction with the sensor, varying degree of distinctiveness, lack of universality and spoof attack^[22]. Therefore, before designing a versatile, efficient multi-modal biometric authentication system the following factors has to be considered. Growing international threat to security, development of robust biometric authentication using a combination of biometric technologies as each biometric technology has their own strengths and weaknesses and may not dominate every area of biometric industry.

1.2 Motivation

A multi-modal biometric authentication system using face and other biometrics is a most acceptable form of high-security biometric study as the face is the most acceptable and common method of recognition. Data acquisition problems with unimodal authentication systems based on fingerprint, voice, iris and DNA fingerprint can be overcome by combining any of these biometric with face biometric authentication system as obtaining face image is less technical and expensive.

1.3 Applications of Multimodal Biometrics

Multimodal biometrics is for a number of high-security requirements especially in defence and banking services. Intelligence and Defense agencies require high security as any vulnerability in it may result in a jeopardization of the nation's security. Other law enforcement agencies need this technology towards find criminals faster and prevent any unwanted incidents. Banking transactions need to adopt a multimodal method to prevent financial fraud and increase security to the money.

1.4 Organization

The present study has been organized as follows: The Section 2 discussed the previous studies related to unimodal and multi-modal biometric authentication system. In Section 3 presents a detailed description of proposed biometric authentication system along with its working principle. Subsequently, pseudo code, system model and working flow of whole implementation process have been discussed. The present the evaluation criteria towards validate the performance method. Section 4 discussed the input dataset and obtained simulation results. Section 5 present the findings and conclusion of proposed multimodal biometric authentication system.

2.0 Related work

Most of the researcher were done till date for human traits on basis of biometric identification system. Among those researchers only few highlighted multimode contemplation when considering the performance and classification accuracy as primary objective. Previous studies related to biometric authentication are discussed as follows:

A study by Galbally et al.^[11] proposed multiple biometric systems using fake detection technique for improving the security of biometric access system via having aliveness assessment in nonintrusive, fast and user friendly. Also, they detected the various types of fraudulent access attempts. By the simulation, the suggested methods have been evaluated and tested by publicly available datasets of iris, finger print and face.

Similarly, Bhardwaj and Gill^[2] developed a secure biometric system using matching level fusion approach with three biometric traits like face, Iris and fingerprint. Moreover, they applied Hough transformation on iris, ICA over face and fuzzy logic is utilized for fusion on these three biometric traits. By this technique, they proven the suggested approach is fast and highly secure to access information.

In order to overcome the problems of facial occlusion such as the application of thick cosmetics and noise due to poor quality images, Dandashi and Karam^[5] developed powerful algorithms to filter the images and detect facial marks such as prominent birthmarks and moles covered by thick cosmetics to detect the facial image. A study by Almayyan^[1] developed a multi-modal biometric recognition system using iris and fingerprint biometrics. The developed system used data from multiple sensors and multiple cues were integrated based on abstract, rank and measurement level. However, whole iris area, results in noise caused by eyelashes that mostly affect the upper part of the iris area^[28]. A research by Ganguly et al.^[13] proposed a new 3D face recognition scheme from 2D-3D hybrid face images using two supervised classifiers to handle expression and illumination variations. However, the study has few limitations such as extreme pose which can change x, y and z-axis of face images

was not taken into consideration. Also, this can be a time-consuming process, requiring adequate training to master.

Cuckoo Search is one of the preferred algorithms to work with genetic algorithms. Studies by Fan et al.^[9] indicate that cuckoo search has very good characteristics and has the ability to become the global optimization algorithm. Particle swarm optimization was also theoretically amazed in the same paper and it has been shown that its population diversity reduces very quickly, and all solutions get crowded close to a prevailing best solution in a tiny region^[42]. This can be detected by the multimodal operation, when the PSO algorithm converges quickly to the local optimum, while the cuckoo search is able to find a way to the global optimum. Cuckoo search also ensures that the population diversity is effectively maintained. It is also studied by Gandomi et al.^[12].

From the review it is understood that multi-modal biometric authentication systems are time-consuming, requires larger data storage and may require expensive technical equipment when compared to the unimodal biometric system⁽³⁵⁾. The performance evaluation of an effective multi-modal system requires a larger database⁽¹⁷⁾. Facial occlusions such as beard, small wrinkles around eyes or mouth, wearing glasses, thick cosmetics may increase the likelihood of false positives. Also, low-quality images, noises from extreme lighting conditions and facial expressions may affect the overall performance of the developed model. The extreme pose which can change x, y and z-axis of face images was not taken into consideration^[13].

3.0 Proposed Multi-modal biometric authentication system

The study presents, a novel framework for extracting human Skeleton and face feature using 3D Imaging technology. We superimpose skeleton biometric features having 25 skeleton points upon face data. This modelling technique used to capture human joints including the depth data as well as improve the system efficiency. A Genetic Algorithm was used for feature extraction as it is more advantageous compared to conventional optimization methods. The developed multi-modal biometric has four modules such as pre-processing, feature extraction, recognition and decision-making system. The pictorial representations of proposed multi-modal biometric authentication system (HOT-ANN) workflow are shown in Figure. 1 which summarizes the implementation way of each stage. First, a MinMax-based method was used to improve the contrast for the purpose of pre-processing an input image, we applied optimization technique and wavelet transform. Eventually, ANN is utilized for accurate recognition which enables the efficient multimodal biometric authentication.

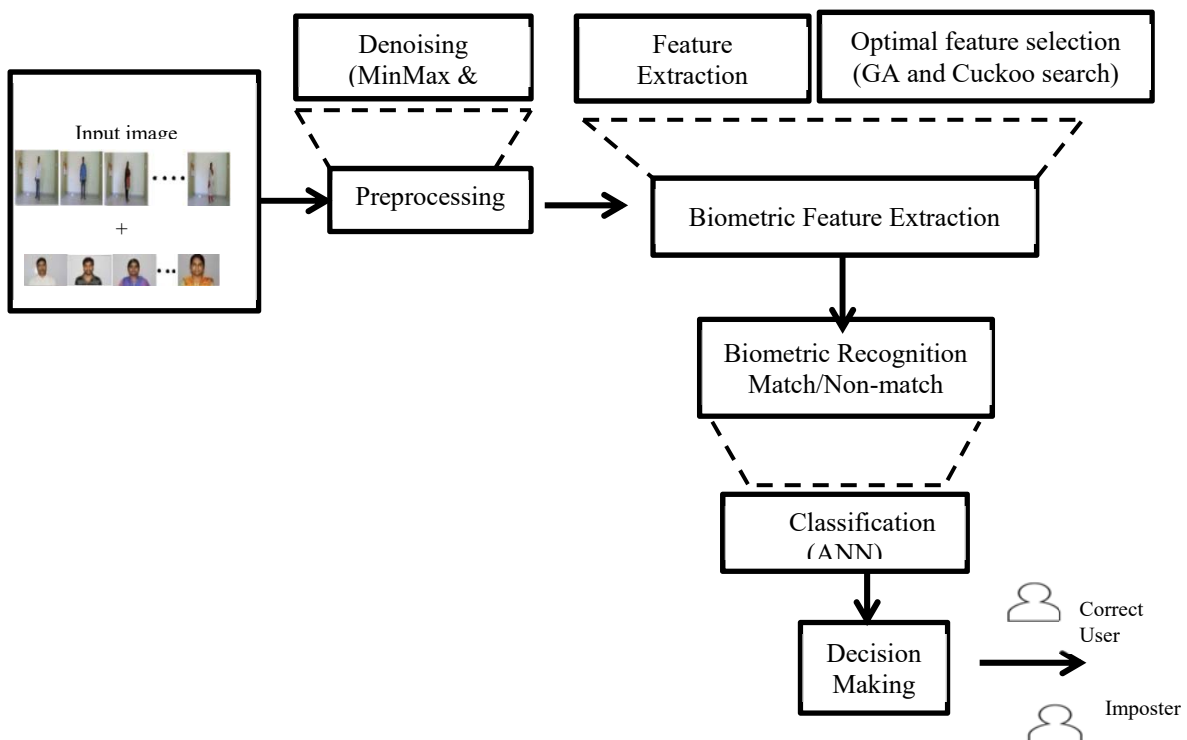


Figure 1: Proposed System Architecture

3.1 Image Preprocessing

3.1.1 Image enhancement

In this study, the image has been pre-processed using MIN-Max method and noise reduced via Gabor Filter. These filters have been used because they have frequency selective and orientation-selective properties. The frequency selection property allows the filter to access the ridges at a particular frequency and orientation in the biometric image. Hence, a Gabor filter that is properly tuned can reduce noise while still preserving the ridges.

Also, image normalization processes have been applied on the image to remove illumination variation. The performance of the recognition algorithms increased by decreasing the input data regarding non biometric features. During the pre-processing operations, the sampling point obtained from face were used.

3.1.2 Image Segmentation

This is done using Discrete Cosine Transform (DCT). It converts the biometric data from the spatial domain to frequency domain by segmenting the image into spectral sub-bands of varying importance.

3.2 Feature extraction

In this stage, to define a massive set of data in a exact way, the required amount of resources was simplified. Moreover, it represents the input image in its unique and compact form of matrix-vector or a single value. Here, the image features have been extracted in two ways: such as,

- Discrete Wavelet Transformation
- optimize features (GA with Cuckoo search)

3.2.1 Discrete Wavelet Transformation

By this transformation approach, can extract the characteristics from an input image which relies on different scales proceedings through low pass and high pass filtering process. Initially, the input image has been decomposed via DWT into N levels through decimation and filtering process towards attains approximation and transformation values known as wavelet coefficient. Then, features have been extracted from DWT coefficients. These extracted features are considered as useful features for classifiers on the basis of the efficient time-frequency representation of the image.

In the task of the input image identification and verification, the feature extraction plays a very leading part. The ultimate motive of the feature extraction is to scale down the original data set by evaluating certain properties or features which are capable of distinguishing an input pattern from the other. In our study, extracted the feature values by Discrete Wavelet Transform (DWT) based feature extraction, which is depicted in Figure. 2. A sensor was used to capture an image, but it generates some noises during capturing. MinMax image enhancement method was used to reduce the noise and to improve the contrast among the image sequences.

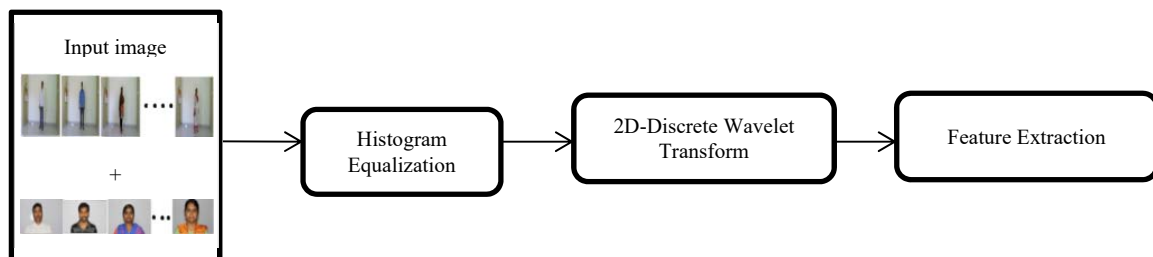


Figure 2: Feature Extraction Process Flow

During this process, initially the 2 rows and columns of zeros are added to the entire image. Then, the image has been separated into 3x3 matrices. Finally, central pixel depends on median of all the pixel values were evaluated. The noise has been removed from input image with Gabor filter. In order to improvise the visualization effect, histogram equalization was used to increase the size of the pixel. DWT is determined mathematically when the decomposition of the image into four different coefficients. Out of four, one is scaling function coefficient, and the other three are wavelet coefficients(horizontal, vertical and diagonal). Thus 2D-DWT is expressed as Feng et al.(10),

$$W_{\varphi}(j_0, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \varphi_{j_0, m, n}(x, y) \quad (1)$$

$$W_{\psi}^i(j, m, n) = \frac{1}{\sqrt{MN}} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x, y) \psi_{j, m, n}^i(x, y), \quad i = \{H, V, D\} \quad (2)$$

Where $f(x, y)$ - input image,

$W_{\phi}(j_0, m, n)$, $W_{\psi}(j, m, n)$ - coefficients of image approximation which offer horizontal, vertical and diagonal details of the image respectively.

In this, $W_{\psi}(j, m, n)$ is the wavelet function used to decompose the image into a number of levels. Thus multi-resolution features of the original image are extracted directly from the wavelet decomposition coefficients. These decomposed values are extracted and combined. All the combined coefficients will give the feature values of a particular image. The decomposition is done by decimating the given image into two levels as lower value components and higher value components using downsampling method through Haar transform and mathematically written as,

$$h_k(z) = h_{pq}(z) = \frac{1}{\sqrt{N}} \begin{cases} 2^{\frac{p}{2}} (q - 1) / 2^p \leq z \leq (q - 0.5) / 2^p \\ -2^{\frac{p}{2}} (q - 0.5) / 2^p \leq z \leq (q) / 2^p \\ 0 \text{ otherwise} \end{cases} \quad (3)$$

When calculating DWT value, the approximated value and level of decomposition are considered. In this paper, the level of decomposition as 2 is considered, which implies $J=2$, where $N=M=2J$, so $j=0, 1, 2, \dots, J-1$.

By comparing the pixel value of (x, y) with the neighbour pixel, have detected the local maxima and minima of the input image. In addition, it has been chosen once it is lower or higher than the neighbor pixel value. Later, eliminated the low contrast points along the edge of the image, texture based image analysis are used. After applying this method, stable key points are selected and located by eliminating the low-intensity pixel key points. The orientations of key points are assigned for the selected key points. The orientation of key points is assigned for the selected key points.

3.2.2 Optimize Features (GA with Cuckoo search)

In order to find the best optimal features from the large feature set, have applied genetic and cuckoo search algorithm. By the use of genetic approach can find best or optimal solutions for computational issues which maximize or minimizes a specific functionality. It works based on the genetic operators like selection, fitness, crossover, mutation, probability and obtains the best solution. Furthermore, the optimal features are selected via GA which searches for the finest feature subset which is equivalent to the efficient image retrieval process. By the experimental, the extracted features of face and Skeleton results are shown in figure 3.

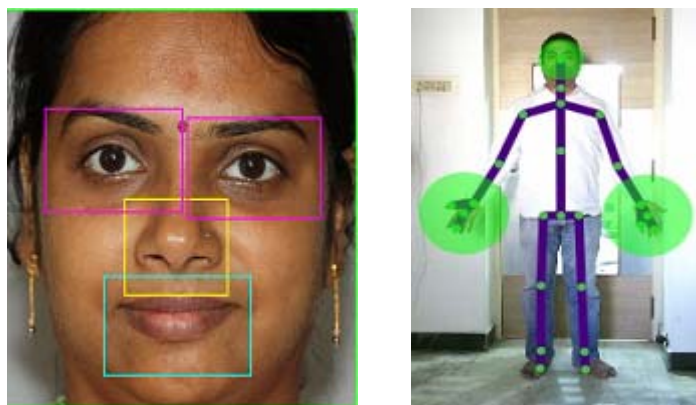


Figure: 3 (a) Face Feature Extraction

(b) Skeleton feature Extraction

Initial population: let us assume S is the number of features and the size of the population is N , In order to create random population S of N , is given as,

$$S = (s_1, s_2, s_3 \dots s_n) \quad (4)$$

Fitness function: The fitness of each pixel element (each row by column) has been measured through sum and average of whole intensity pixels of block region.

Selection: From the initial population have selected the two parents based on their finest fitness value that might be generated based on the new offspring.

Crossover and mutation: The term crossover is a process of taking more than one parent solutions and generating child solution from them. It includes interchange of elements from reproducing of two parent chromosomes to create one or more child chromosomes. Moreover, it's implemented through arbitrarily chosen a point, i.e. crossover point in the string as well as interchange the segments. Then, draw the crossover line wherein the lower part of the two images is swapped. By this process, able to increase the number of polynomials. Once completion of crossover performance, mutate the new offspring from a single parent. By this process able to reduces the local optimum value.

In addition, have applied cuckoo search towards obtaining enhanced image features with the optimal solution. The primary objective of using this approach provides improved results (i.e. cuckoos) towards exchange a not-so-good result in the nests. At a time, the entire cuckoo lays one egg then dumps its egg in a randomly selected nest. Further, will carry over to the next generation on the basis of best nests with high quality. Now the available host nests are constant manner. In the initialization process, each egg denotes a possible set of features which are chosen as well as utilized towards properly classifies the samples. Wherein the performance of classification system is measured through its classification accuracy. Subsequently, the crossover is utilized towards creating two eggs in the nest and selected the best one amongst them. With the help of above process, able to reduce the features dimensions and optimize the biases and weights of BPNN.

3.3 Recognition technique

Artificial Neural Network (backpropagation algorithm)

After extraction of image features, acquire training and testing feature matrix. In order to reduce the redundant features and improve the classification accuracy by optimization approach with back propagation network were employed. In addition, initial biases and weights of network have been optimized through hybrid optimization technique. Subsequently, a sequence of iterations, the best fitness and average fitness are progressively increased whereas set of input arguments are filtered. Also, reduced the dimensions of the feature set through hybrid optimization approach. The pictorial representation of recognition process is depicted in figure 4.

In order to recognize the human Skeleton and facial features, have determined the structure of ANN on the basis of a number of inputs, neurons, hidden layers and activation functions. Later, ANN is trained, using the input pattern and desired output. In addition, ANN is an efficient classification approach which is used for discrete, vector and real-valued functions. In specific, here we applied two-layer backpropagation approach for learning process. By this approach can reduce the error functions. Finally, validate the results validation of the trained ANN is done.

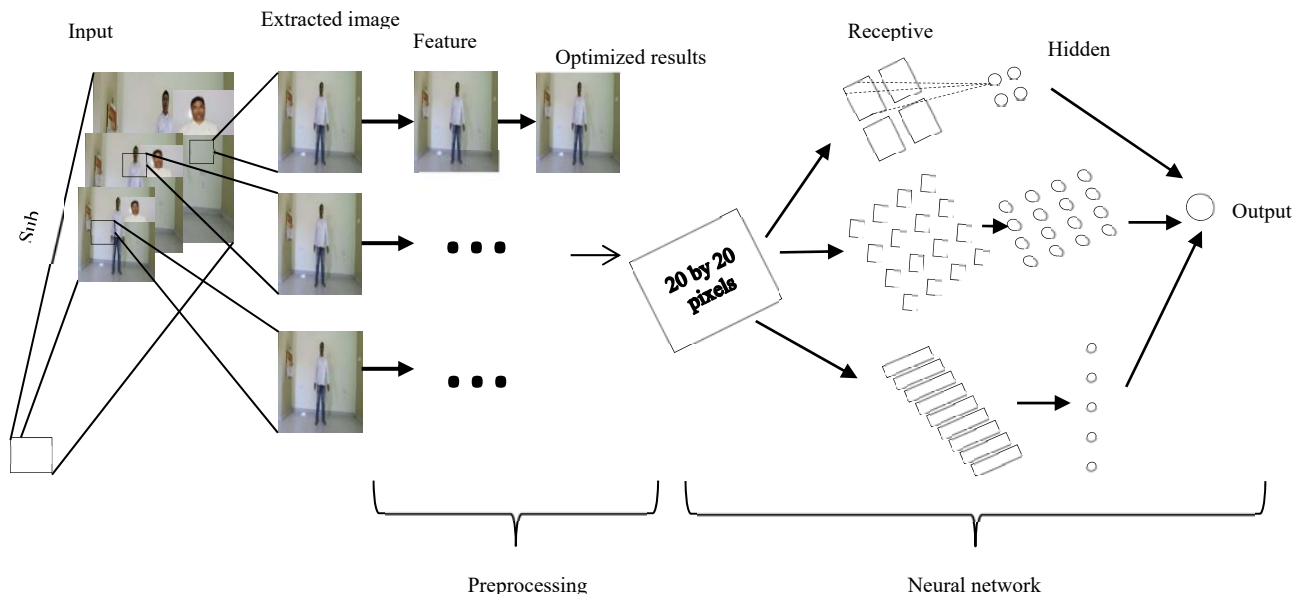


Figure 4: Pictorial representation of recognition process

In order to train the input image, have utilized the Back Propagation feed-forward ANN. The extracted image features (in the form of Eigenvalues) are fed into the NN. Based on the number of input images, the different number of NN has been taken. After initializing the parameters of NN are trained with Eigenvalues of input images through hidden, input and output layer. Furthermore, we have compared each distance of each image (based on eigenvalue) with the other. Here, the image of the same person is zero distance and output is taken is one or zero. Subsequently, the human has been recognized based on the output as one. Henceforth, NN has formed an Identity matrix for the different image set via outputs as 0's and 1's. The output layer error has been sent back to the earlier layer and updates the weights of this layer. This will minimize the error rate. Further, the learning process counts the update from earlier iterated and re-calculate the fresh, updated outcome. For each recognition process, the Eigenvalues are measured through optimized results. These tested results are related with the eigenvalues of trained NN for attaining better-recognized results. By the above, all process, the multimodal recognition system works with high accuracy results than the previous work. Also offers best success rate even for the noisy input image.

3.4 Human Recognition using GA and Cuckoo Search

3.4.1 Pseudo code for GA with cuckoo search/Algorithm for Human Recognition

Pseudo code for GA with cuckoo search/Algorithm for Human Recognition

Input: Skeleton and face image

Output: fitness, optimal solution and recognized image

Begin

Define obj. fun $f(s)$, $s=(s_1, s_2, s_3 \dots s_n)$

Initialize a random population of host nests $s_i(i=1, 2, \dots n)$

Define genetic and cuckoo search (dimension of search space, maximum generation, the total number of cuckoos) parameters

While ($t < \text{Max. generation}$)

Begin genetic

$i = 0$

evaluate fitness

while ($t < \text{max. generation}$); do

$i=i+1$;

calculate crossover and mutation parameter

evaluate fitness

Move cuckoo to the new nest with a step size

end while

rank the chromosome (find the current best)

end begin Genetic

```
for i=1:n
    Get a cuckoo and generate solution %% retrieve the optimal solution
    Measure the current best solution (nest)
    Pass the current best solutions to the next generation
    Based on the fitness, Rank the solutions
    Pick up the nest with the maximum fitness (egg)
End for
End while
```

The above algorithm briefly described by the following steps

3.4.2 Algorithm steps

```
Step 1: generate random initial population
Step 2: In the current population, evaluate the fitness function for each individual
Step 3: Move cuckoo to the new nest with a step size
Step 4: Worst solution is abandoned and new ones are built
Step 5: Measure the current best solution (nest)
Step 6: Based on the fitness, Rank the solutions
Step 7: Pick up the nest with the maximum fitness (egg)
Step 8: To perform mutation and crossover on the present population
Step 9: Repeat Steps 2 to 8 until reach the stopping criterion
```

3.5 System Model and Implementation procedure

Step 1: Firstly, design and developed a code for the loading the input image from the database using MATLAB software version 2016b. Subsequently, the face and human skeletal image value are stored in the workspace of the software.

Step 2: Apply to pre-process (normalization, image segmentation, and image enhancement) the uploaded input images in both section.

- **Normalization:** In this stage, the image has been divided into sub-blocks which is 11×11 pixels. In order to make the whole image in same brightness through subtracting the mean and the intensity value of each blocks. In addition, the scores has been normalized amongst 0 and 1 using min-max approach whereas α indicates acceptance ratio i.e presence of an imposter.
- Image segmentation – DCT
- Image Enhancement: A 3×3 Gaussian Filter / Gabor Filter

Step 3: After completion of pre-processing stage, we have created the code towards detect the face and skeleton feature on the basis of suggested technique.

Step 4: Apply Discrete Wavelet Transformation (DWT) for the feature extraction from the input image

Step 5: Initialized GA [Classifiers] with Cuckoo to optimize features. Then removed the unwanted feature sets using the objective function.

Step 6: Apply ANN (back-propagation algorithm) on optimized data to train and test the input image using following steps:

- Compute the total categories which are generated by the training of optimized data using ANN structure.

Step 7: After that, classified the test data according to the trained ANN structure.

Step 8: In the fusion part, have validated the recognition results on the basis of the matching number.

Step 9: At last of the module, calculated the different metrics of proposed biometric fusion system like False accept rate (FAR), false reject rate (FRR) and accuracy

Step 10: Compared the proposed GA based approach with another conventional algorithm like a neural network, convolutional neural network (CNN) and SVM.

3.6 Performance analysis

The Performance of proposed authentication system has been validated by measure of few metric named as True Accept Rate (TAR), False Reject Rate (FRR), Receiver Operating Characteristic (ROC) Curve and accuracy. It completely depends on the system error rates ^[25]. The basic definition of these metrics is discussed as follows:

The term TAR is measured by probability of correctly matched of genuine user to the consistent stored template value in the biometric authentication system. It's mathematically written as,

$$TAR = \frac{TA}{TA + FR} \quad (5)$$

Here TA- Correctly matched genuine user to the corresponding template stored in the system

FR- The genuine user is incorrectly rejected from the system.

The term FAR calculated by proportion of imposters that has been incorrectly matched to a genuine user's template stored biometric authentication system. It's also written as,

$$FAR = \frac{FA}{FA + TR} \quad (6)$$

Here FA- The imposter is incorrectly matched to a genuine user template stored in a system.

TR- The system correctly denies an imposter, where its data that not matching to any template within the system.

The term FRR is measured by the proportion of genuine users which is incorrectly rejected from a biometric authentication system. It also defined as,

$$FRR = \frac{FR}{TA + FR} \quad (7)$$

Receiver Operating Characteristic (ROC) Curve illustrate the trade-off amongst TAR(y-axis) and FAR(x-axis) in a single curve at different threshold values, where points are illustrated parametrically as a key function of the decision threshold (refer Figure. 7). In addition, FAR is equal to zero and TAR is equal to one.

Subsequently, the accuracy of proposed biometric authentication system has been evaluated by Ghoulmi et al.,^[15],

$$Accuracy = 100 - \frac{FRR + FAR}{2} \quad (8)$$

The receiver operator characteristic (ROC) curve is generated with the help of FAR and TAR. Its graphically shows the variation of genuine acceptance ratio(GAR) with variation in FAR. Whereas, the term genuine acceptance ratio is calculated by GAR=(100-FRR).

4.0 Experimental results

4.1 Dataset

In this study, have collected the input image from the 3D imaging sensor. This dataset consists of pictures of 500 people, 220 females and 280 males, under different poses, facial expressions and lighting conditions, taken with two different sessions between them using the Kinect camera. Within the scope of the study, the first 500 people in the dataset are used with the images of light on, natural and in closed environment.

4.2 Results & Discussion

In this study, have evaluated the performance of the proposed system use of the 3D imaging sensor dataset is considered. This dataset consists of a total of 500 images aged between 17 and 31 along with the different illumination condition, natural, smile. The performance evaluation is carried out using Matlab 2016b on an Intel i5 system.

S.No	Input Data	precision	Recall	F-measure	True Positive Rate	False Positive Rate
1	Image 1	0.896	1	0.952	100%	22%
2	Image 2	0.908	1	0.953	100%	22%
3	Image 3	0.913	1	0.951	100%	32%
4	Image 4	0.8806	0.69	0.759	66.6667%	14%
5	Image 5	0.863	0.914	0.9124	91.6667%	8.33333%

Table 1: Obtained results based on the proposed method

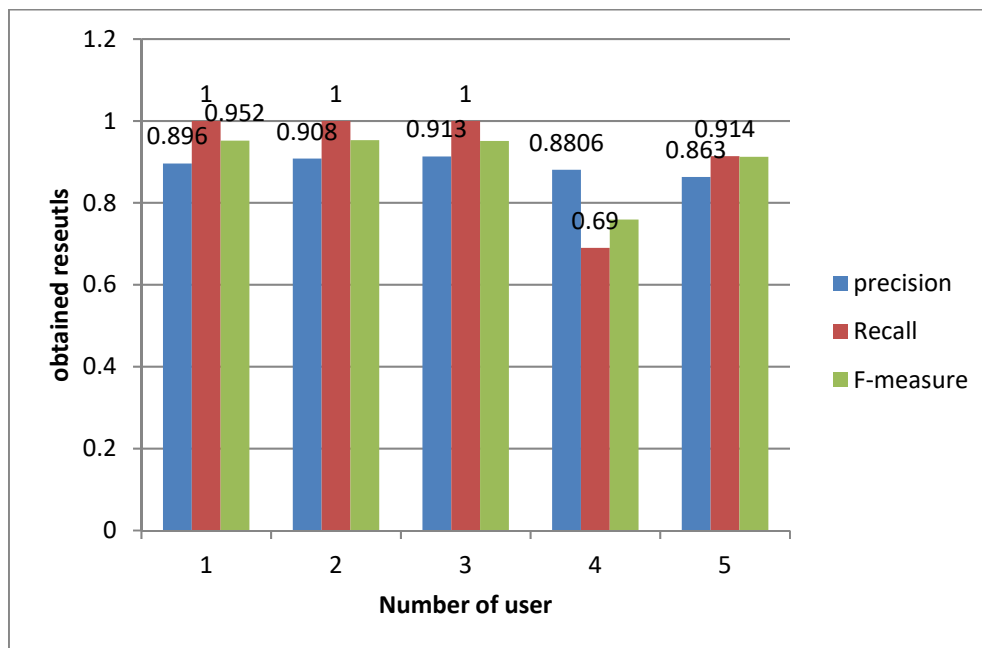


Figure 5: Pictorial representation of precision, recall and F-measure

The obtained results of true positive rate and true negative rate and listed in Table 2. Higher TPR is desirable as it indicates the authentication success rate; hence the proposed technique has a TPR of 1, which is the highest possible rate. TNR should be as low as possible as it is undesirable and compared to other methods; the proposed HOT-ANN method has a very low TNR of 0.09208.

Traits	TPR	TNR
Face ^[2] Bhardwaj and Gill	0.88	0.12
Fingerprint	0.86	0.14
Iris	0.90	0.10
Combined (Face + Iris+ Fingerprint)	0.92	0.8
Proposed Fusion (Body +face)	1	0.09208

Table 2: Evaluation measures for the classifier

It can be observed from table 2, unimodal bio- authentication system such as the face, fingerprint, iris, the average of obtained results of TPR and TNR is 0.88 and 0.12 respectively which is stated in 2. Further, they combined the face, fingerprint, iris and obtained the TPR and TNR is 0.92 and 0.8 respectively. Based on our proposed framework, the obtained result of TPR and TNR is 1 and 0.09208 respectively. When comparing with the existing approach, our proposed framework outperforms than the existing method.

S.No	Author	Methods	Multimodal system	FAR	FRR
1	Jagadeesan et al. ^[19]	Cryptographic Key Generation	Fingerprint	10%	22%
			Iris	2%	13%
			Fusion	0%	10%
2	Gawande et al. ^[14]	Feature Level Fusion	Fingerprint	6%	16%
			Iris	4%	12%
			Fusion	0%	8%
3	Author (2018)	HOT-ANN	Face+ Skeletal features	1%	4%

Table 3: Comparison of FAR & FRR

The equation 5 and 6 represents the false acceptance ratio (FAR) and false rejection ratio (FRR). Table 3 shows FAR, FRR values of fingerprint, Iris and fusion image. When comparing the FAR and FRR value with the existing method, the proposed work is lower when related to other method. Thus the performance of the method is better than the existing method. Biometric identification is more secure, quite flexible and easily scalable. From the result, the proposed method achieves a high level of recognition accuracy with biometrics systems for the kinetic image when compared to the existing method. The false acceptance and rejection rate of the suggested method is a minimum value when compared to the existing method.

S.No	Author	Multimodal system	Classifier	Accuracy
1	Shah ^[30]	Face	SVM	90%
2	Marak and Hambalik ^[26]	Fingerprint	Neural network	92%
3	Syafeeza et al. ^[34]	Face Recognition with Pose and Illumination Variation	CNN	85.71
4	Gawande et al. ^[14]	Fingerprint and IRIS Fusion	Radial Basis Function based neural network	92 %
5	Chaudhary and Nath ^[4]	Fusion of Palmprint, Fingerprint and Face	Fusion technique	87 %
6	Kundu and Sarker ^[23]	fingerprints, palm-prints, wrist-veins and handwriting	multi-classification based on template matching	96.67 %
7	Author (2018)	Face+ Skeletal features	Proposed method	98.3871%

Table 4: Comparative Study with the Accuracy of the Systems

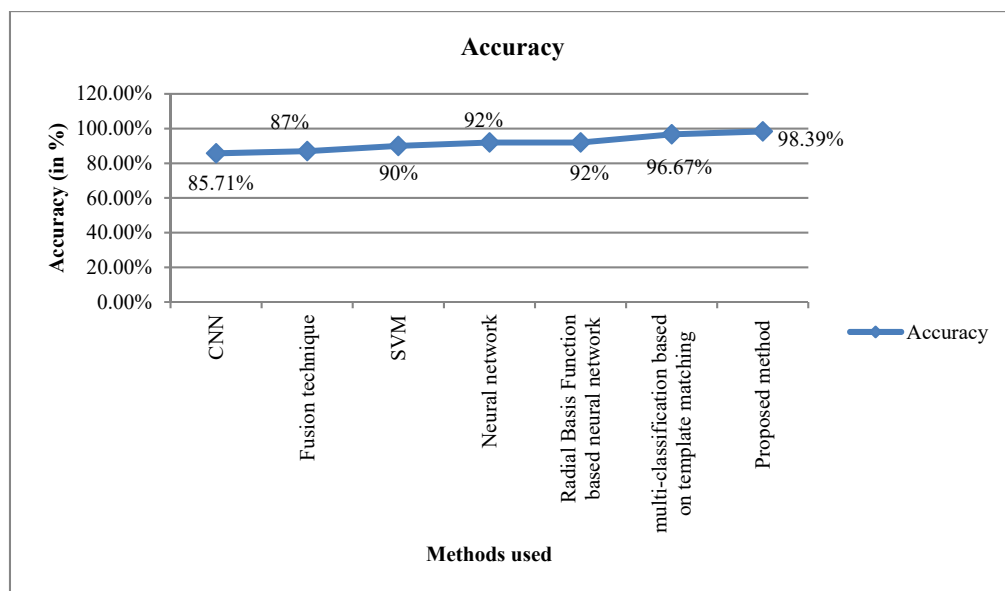


Figure 6: Pictorial representation of accuracy measurement

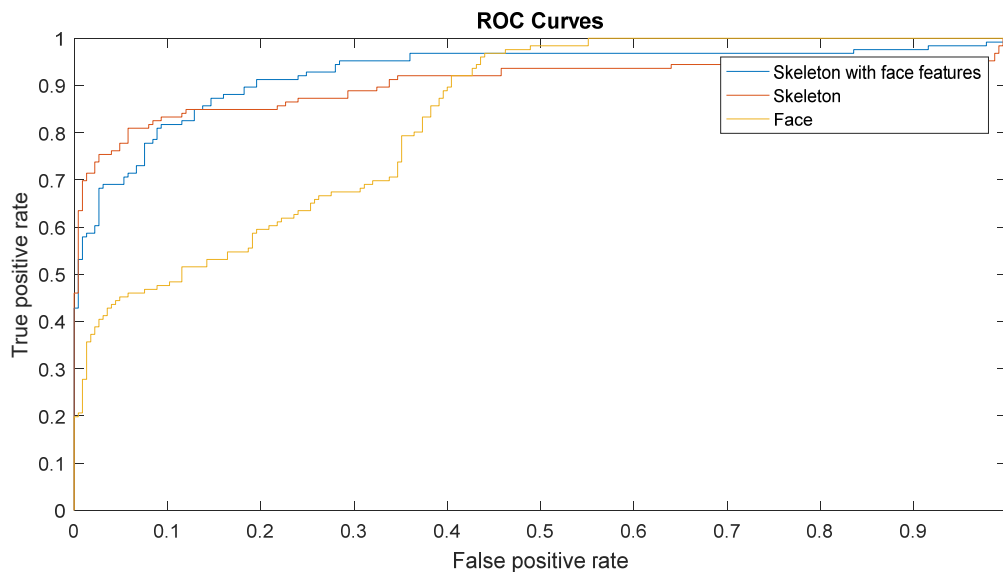


Figure 7: Performance of ROC curve

The examined ROC curve of proposed multimodal biometric authentication system is shown in figure 7. The performance has been compared with the unimodal as skeleton and face (alone) with the proposed system. The figure clearly shows the proposed method outperforms than the traditional technique.

Various multimodal systems such as the face, fingerprint, a fusion of fingerprint and iris, a fusion of palm print, fingerprint and face and fusion of palm print, wrist-veins, fingerprint and handwriting have been compared with the proposed HOT-ANN method. The proposed HOT-ANN Technique has been proven to give a better accuracy as shown in Table 4. Using the face and skeletal features of a person, the proposed technique has been able to give a high accuracy of 98.3871%. The accuracy data has been used to plot a chart as shown in Figure. 6. It can be seen that line grows linearly, and the proposed system has the highest accuracy while comparing to other shown methods.

5.0 Conclusion

In this paper, have presented the novel multi-model biometric authentication system by combining the face and Skeleton features. The novelties of the proposed system is utilized the sampling points in the face-tracking part and skeleton points has extracted based on the image textural feature analysis, which enables its real-time performance. Low error rates are achieved in both the face tracking and the Skeleton feature extraction based multi-model systems. This proposed method is robust to typical sources of errors like illumination changes, brightness and low-quality images. By the simulation, the proposed HOT-ANN method gives a better FAR, FRR, accuracy of 1%, 4% and 98.3871% respectively. The performance of proposed method has been compared and validated with the traditional appearance which includes Cryptographic Key generation, feature level fusion, support vector machine, neural network, cnn , fusion technique and multi-classification based on template matching. In addition, experimental results show that the suggested HOT-ANN method improves the performance dramatically than the traditional approach.

References

- [1] Almayyan W. Performance analysis of multimodal biometric fusion. *J Comput Sci.* 2012;9(3):290-296. <http://hdl.handle.net/2086/5998>.
- [2] Bhardwaj S, Gill SK. Recognition using Multimodal Biometric. *Int J Comput Appl.* 2016;146(8):24-29.
- [3] Cenys A, Gibavicius D, Goranin N, Marozas L. Genetic algorithm based palm recognition method for biometric authentication systems. *Elektron ir Elektrotechnika.* 2013;19(2):69-74. doi:10.5755/j01.eee.19.2.3473.
- [4] Chaudhary S, Nath R. A Multimodal Biometric Recognition System Based on Fusion of Palmprint, Fingerprint and Face. *2009 Int Conf Adv Recent Technol Commun Comput.* 2009;4(May):596-600. doi:10.1109/ARTCom.2009.224.
- [5] Dandashi A, Karam W. Biometrics security and experiments on face recognition algorithms. In: *2012 IEEE Symposium on Computational Intelligence for Security and Defence Applications.* IEEE; 2012:1-8. doi:10.1109/CISDA.2012.6291532.
- [6] Daugman J. How Iris Recognition Works. *IEEE Trans Circuits Syst Video Technol.* 2004;14(1):21-30. doi:10.1109/TCSVT.2003.818350.
- [7] Daugman JG. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans Pattern Anal Mach Intell.* 1993;15(11):1148-1161. doi:10.1109/34.244676.
- [8] Dikovski B, Madjarov G, Gjorgjevikj D. Evaluation of different feature sets for gait recognition using skeletal data from Kinect. In: *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO).* IEEE; 2014:1304-1308. doi:10.1109/MIPRO.2014.6859769.
- [9] Fan W, Xing-shi H, Yan W, Song-ming Y. Markov Model and Convergence Analysis Based on Cuckoo Search Algorithm. *Comput Eng.* 2012;38(1). <http://www.ecice06.com/EN/abstract/abstract23388.shtml>.

- [10] Feng T, Zhao X, Carbunar B, Shi W. Continuous Mobile Authentication Using Virtual Key Typing Biometrics. In: *2013 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE; 2013:1547-1552. doi:10.1109/TrustCom.2013.272
- [11] Galbally J, Marcel S, Fierrez J. Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition. *IEEE Trans Image Process*. 2014;23(2):710-724. doi:10.1109/TIP.2013.2292332.
- [12] Gandomi AH, Yang X-S, Alavi AH. Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. *Eng Comput*. 2013;29(1):17-35. doi:10.1007/s00366-011-0241-y.
- [13] Ganguly S, Bhattacharjee D, Nasipuri M. Hybridization of 2D-3D Images for Human Face Recognition. In: *Hybrid Soft Computing Approaches*. Europe; 2016:387-403. doi:10.1007/978-81-322-2544-7_13.
- [14] Gawande U, Zaveri M, Kapur A. Fingerprint and Iris Fusion Based Recognition Using RBF Neural Network. *J Signal Image Process*. 2013;4(1):142-148.
- [15] Ghoulami L, Draa A, Chikhi S. An ear biometric system based on artificial bees and the scale invariant feature transform. *Expert Syst Appl*. 2016;57:49-61. doi:10.1016/j.eswa.2016.03.004.
- [16] Ghouti L, Bahjat AA. Iris fusion for multibiometric systems. In: *2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. IEEE; 2009:248-253. doi:10.1109/ISSPIT.2009.5407577.
- [17] Goyal N. Multi-Biometric Recognition for Iris and Ear Images by using ICA, GA, Hamming Distance. *J Netw Commun Emerg Technol*. 2015;2(1):58-63. <http://www.jncet.org/Manuscripts/Volume-2/Issue-1/Vol-2-issue-1-M-11.pdf>.
- [18] Ito K, Aoki T, Nakajima H, Kobayashi K, Higuchi T. A Palmprint Recognition Algorithm using Phase-Based Image Matching. In: *2006 International Conference on Image Processing*. IEEE; 2006:2669-2672. doi:10.1109/ICIP.2006.313059
- [19] Jagadeesan A, Thillaikkarasi T, Duraiswamy K. Protected bio-cryptography key invention from multimodal modalities: Feature level fusion of fingerprint and Iris. *Eur J Sci Res*. 2011;49(4):484-502.
- [20] Jain AK, Ross A, Pankanti S. Biometrics: A Tool for Information Security. *IEEE Trans Inf Forensics Secur*. 2006;1(2):125-143. doi:10.1109/TIFS.2006.873653.
- [21] Jain AK, Ross A, Prabhakar S. An Introduction to Biometric Recognition. *IEEE Trans Circuits Syst Video Technol*. 2004;14(1):4-20. doi:10.1109/TCSVT.2003.818349.
- [22] Jiwnani G, Nisheeth S. Multi-modal Biometric Authentication using Fingerprint and Iris: a Review. *Int J Comput Sci Commun Networks*. 2011;5(2):115-119. <http://www.ijcsn.com/Documents/Volumes/vol5issue2/ijcsn2015050215.pdf>.
- [23] Kundu S, Sarker G. An Efficient Integrator based on Template Matching Technique for Person Authentication using Different Biometrics. *Indian J Sci Technol*. 2016;9(42):1-9. doi:10.17485/ijst/2016/v9i42/93805.
- [24] Kurban OC, Yildirim T, Bilgic A. A multi-biometric recognition system based on deep features of face and gesture energy image. In: *2017 IEEE International Conference on INnovations in Intelligent SysTems and Applications (INISTA)*. IEEE; 2017:361-364. doi:10.1109/INISTA.2017.8001186.
- [25] Mahfouz A, Mahmoud TM, Eldin AS. A survey on behavioral biometric authentication on smartphones. *J Inf Secur Appl*. 2017;37:28-37. doi:10.1016/j.jisa.2017.10.002.
- [26] Marak P, Hambalik A. Fingerprint Recognition System Using Artificial Neural Network as Feature Extractor: Design and Performance evaluation. *Tatra Mt Math Publ*. 2016;67(1):117-134. doi:10.1515/tmmp-2016-0035.
- [27] Nandakumar K, Yi Chen, Dass SC, Jain AK. Likelihood Ratio-Based Biometric Score Fusion. *IEEE Trans Pattern Anal Mach Intell*. 2008;30(2):342-347. doi:10.1109/TPAMI.2007.70796.
- [28] Omran SS. Design and Implementation of Multi-Model Biometric Identification System. *Int J Comput Appl*. 2014;99(15):14-21. <https://pdfs.semanticscholar.org/17c5/25ed8851efebc8db4136c150f79906db4a5d.pdf>.
- [29] Ross AA, Nandakumar K, Jain AK. *Handbook of Multibiometrics*. 1st ed. Germany: Springer; 2006.
- [30] Shah PM. Face Detection from Images Using Support Vector Machine. 2012. http://scholarworks.sjsu.edu/cgi/viewcontent.cgi?article=1322&context=etd_projects.
- [31] Sinha A, Chakravarty K. Pose Based Person Identification Using Kinect. In: *2013 IEEE International Conference on Systems, Man, and Cybernetics*. IEEE; 2013:497-503. doi:10.1109/SMC.2013.91.
- [32] Baveja M. An Analysis of the US-VISIT biometric program. 2007. <http://sci-hub.tw/10.1109/ISSPIT.2009.5407577>.
- [33] Subbarayudu VC, Prasad MVNK. Multimodal Biometric System. In: *2008 First International Conference on Emerging Trends in Engineering and Technology*. IEEE; 2008:635-640. doi:10.1109/ICETET.2008.93.
- [34] Syafeeza AR, Khalil-Hani M, Liew SS, Bakhteri R. Convolutional neural network for face recognition with pose and illumination variation. *Int J Eng Technol*. 2014;6(1):44-57. doi:10.1109/icpr.2010.371.
- [35] Thasiyabi VA, Koshy R, Satheesh S. Biometric fusion: Combining multimodal and multi algorithmic approach. In: *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPUS)*. Paralakhemundi: IEEE; 2016:618-620. doi:10.1109/SCOPES.2016.7955513.
- [36] Unar JA, Seng WC, Abbasi A. A review of biometric technology along with trends and prospects. *Pattern Recognit*. 2014;47(8):2673-2688. doi:10.1016/j.patcog.2014.01.016.
- [37] Vasuhi S, Vaidehi V, Babu NTN, Treasa TM. An efficient multi-modal biometric person authentication system using Fuzzy Logic. In: *ICOAC 2010*. IEEE; 2010:74-81. doi:10.1109/ICOAC.2010.5725365.
- [38] Wang J, Li Y, Ao X, Wang C, Zhou J. Multi-modal biometric authentication fusing iris and palmprint based on GMM. In: *2009 IEEE/SP 15th Workshop on Statistical Signal Processing*. IEEE; 2009:349-352. doi:10.1109/SSP.2009.5278568
- [39] Wu J, Ishwar P, Konrad J. Silhouettes versus skeletons in gesture-based authentication with Kinect. In: *2014 11th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*. IEEE; 2014:99-106. doi:10.1109/AVSS.2014.6918651.
- [40] Wu J, Konrad J, Ishwar P. Dynamic time warping for gesture-based user identification and authentication with Kinect. In: *2013 IEEE International Conference on Acoustics, Speech and Signal Processing*. IEEE; 2013:2371-2375. doi:10.1109/ICASSP.2013.6638079
- [41] Wu X, Zhang D, Wang K, Qi N. Fusion of Palmprint and Iris for Personal Authentication. In: *Advanced Data Mining and Applications*. Germany: Springer; 2007:466-475. doi:10.1007/978-3-540-73871-8_43.
- [42] Yang X-S, Deb S. Cuckoo search: recent advances and applications. *Neural Comput Appl*. 2014;24(1):169-174. doi:10.1007/s00521-013-1367-1.
- [43] Zhang Y-M, Ma L, Bo Li. Face and ear fusion recognition based on multi-agent. In: *2008 International Conference on Machine Learning and Cybernetics*. IEEE; 2008:46-51. doi:10.1109/ICMLC.2008.4620376