International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Two Levels Fusion Based Multimodal Biometric Authentication Using Iris and Fingerprint Modalities

Vedururu Sireesha[1]* **Sandhya Rani Kasi Reddy[2]**

[1] *Padmavathi mahila university, Tirupati, Andhra Pradesh, India*
[2] *Sri Padmavati Mahila Visvavidyalayam, Tirupati, Andhra Pradesh, India*
*Corresponding author's Email: vsireesha0480@gmail.com

Abstract: In the document, we are intending to present an innovative technique for the multimodal biometric authentication. Initially the input image is preprocessed then offered to feature extraction, where the modified local binary pattern is effectively utilized. Thereafter, the extracted features are furnished to the feature level and score level fusions. In feature level fusion, extracted features are offered to the GSO where the optimal features are shortlisted, and are furnished to the optimized neural network which effectively detects the iris and fingerprint image. In score level fusion, extracted features from the iris image are offered to the PSO and naive bayes classifier here one score value is achieved. After that, extracted features from the fingerprint image are applied to the AGFS and then one score value is attained. Finally, both the score values are combined. The evaluation tools utilized precision, FAR and FRR. The proposed method implemented in MATLAB platform.

Keywords: local binary pattern; group search optimizer; Bat algorithm; particle swarm optimization; naive bayes classifier; adaptive genetic fuzzy system.

1. Introduction with Problem Identification

Personal identity refers to a group of attributes that are linked with an individual such as name, social security number etc [1]. Biometric technology holds out the assurance of a trouble-free, safe technique to make exceedingly precise authentications of persons. It furnishes a secured method of recognition that cannot be stolen, misplaced or forgotten, which is being progressively more required in safety atmospheres and applications such as access control and electronic transactions [2]. Alternate symbols of distinctiveness like passwords and ID cards have the vulnerability of being easily misplaced, shared or stolen [3] and dictionary attacks [4] and offer negligible protection. As biometric techniques make it a precondition for the client to be physically present during validation, it serves as a deterrent against the possibility of clients emerging with bogus refutation claims at a later stage [4]. Biometrics throws open many an advantage over the conventional safety measures encompassing Non-repudiation, Accuracy, Screening and Security [5]. Biometric systems by design find out or confirm a person's identity based on his anatomical and behavioral features such as fingerprint, face, iris, voice and gait and these traits cannot be easily lost or forgotten or shared or forged [6]. A biometric scheme delivers automatic recognition of a person depending on some particular unique feature held by the individual [7].

The excellence of a biometric technique is assessed by means of its inherent competence in recognition, which is estimated using the bogus refutation and fake acceptance paces [7]. Biometric identification methods that make use of a single feature for identification are regularly affected by several practical problems like noisy sensor data, non-universality or lack of distinctiveness of the biometric trait, unacceptable error rates, and spoof attacks [8]. This is because of the fact that the accuracy of single biometric system is easily affected by the dependability of the sensor used [9]. These systems, commonly referred to as multimodal biometric systems, are estimated to be more

dependable because of presence of several, autonomous fragments of evidence. These methods are able to encounter the rigorous performance foods levied by numerous applications. They address the problem of non-universality, since multiple traits safeguard adequate population coverage [10]. Multimodal biometric systems overwhelm many of these limitations by combining the proofs obtained from various bases. Multimodal biometrics has produced better accuracy and population coverage, while decreasing susceptibility to spoofing [11].

Iris is the one of most reliable and accurate biometric feature among the present biometric features. Iris recognition is a largely recognized unmatched biometrics recognition technique in the world [6] considering its firmness, independence and non-invasiveness and it also has the potential for applications in widespread extents [12]. Iris is an externally visible, yet protected organ whose unique epigenetic pattern stays firm all over the adult life [13]. Image processing techniques can be used to obtain the unique iris pattern from a digitized image of the eye, and encrypt it into a biometric template, which can be stored in a database [14]. This biometric template comprises of an objective mathematical exemplification of the unique info stored in the iris, and permits evaluations to be done amongst the templates [13]. When a person desires to be recognized by iris recognition system, his/her eye is first photographed, and then a template is made for their iris region [10]. This template is then checked with the other templates which are stacked in a database until either a matching template is found and the subject is identified, or no match is found and the subject remains unidentified [15].

Generally, the fingerprint surface [16] is made up of a system of ridges and valleys that serve as friction surface when we are gripping the objects. The fingerprint images can be represented by both global as well as local features. The global features include the ridge orientation, ridge spacing and singular points such as core and delta. Minutiae are local features marked by ridge discontinuities. Commonly, fingerprint recognition [16] has the following advantages over other biometrics: (1) universality - the population that has legible fingerprints exceeds the population that possesses the passports; (2) high distinctiveness - even identical twins who share the same DNA have different fingerprints.

The birth of the multimodal biometrics is brought about by the synthesis of the diverse biometric mode data at the trait mining, match score, or decision level [17]. Score level blending is the most desirable factor in multimodal biometric systems in view of the fact that matching scores encompass ample data to distinguish between real and bogus cases and they are comparatively accessible at ease [9]. As the scores turned out by a biometric system can be either resemblance scores or remoteness scores, it becomes highly essential to one need to adapt these scores into an identical nature. Transformation-based score level fusion, classifier-based score level fusion and density-based score level fusion was few of the notable instances of amalgamation procedures [17]. The remainder of the paper is organized as follows: Section 2 provides an overview of related work in the field. Section 3 narrates the proposed model where the various module of the work is explored. Section 4 brings out the experimental results and discussions.

2. Literature Survey

There have been many works related to biometric recognition systems especially related to iris and finger print recognition. Some of these works are brief in this section.

Chen, Wei-Kuei, et al, [18] has attempted to detect shape information from the iris by analyzing local intensity variations of an iris image. The methodology involves extraction of iris features using bi-dimensional empirical mode decomposition (BEMD) and fractal dimension. After the preprocessing procedure, the normalized effective iris image was decomposed into 2D intrinsic mode function (IMF) components at different spatial frequencies by bi-dimensional empirical mode decomposition. Then the texture features of each intrinsic mode function image were obtained via the differential box-counting method. The efficacy of the proposed approach was evaluated using three different similarity measures used in recognition were adopted.

RaiHimanshu and AnamikaYadav, [19] have presented a novel and efficient approach for iris feature extraction and recognition was presented. The zigzag collarets area of the iris was selected for iris feature extraction because it captures the most important areas of iris complex pattern and higher recognition rate has been achieved. These extracted features were utilized for iris identification using the combined SVM and Hamming distance approach. The proposed approach also used parabola detection and trimmed median filter for the purpose of eyelid and eyelash detection. The recognition accuracy was compared with the previous reported approaches. The proposed method has better recognition rate than using SVM or Hamming distance alone. It is

also clear that the efficiency has been increased when we used separate feature extraction techniques for SVM and Hamming distance based classifier.

De Marsico, Maria, et al. [20], have described FIRME (Face and Iris Recognition for Mobile Engagement) as a biometric application based on a multimodal recognition of face and iris, which is designed to be embedded in mobile devices. The starting one handles image acquisition. From this point, different branches perform detection, segmentation, feature extraction, and matching for face and iris separately. As for face, an anti-spoofing step is also performed after segmentation. Finally, results from the two branches are fused. In order to address also security-critical applications, FIRME can perform continuous re-identification and best sample selection.

Yadav, Divakar et al, [21] have presented an in-depth analysis of the effect of contact lenses on iris recognition. Two databases, namely, the IIIT-D Iris Contact Lens database and the ND-Contact Lens database, are prepared to analyze the variations caused due to contact lenses. They also present a novel lens detection algorithm that can be used to reduce the effect of contact lenses. The proposed approach outperforms other lens detection algorithms on the two databases and shows improved iris recognition performance.

To deal with these difficulties, Kai Cao et al [22] proposed a regularized orientation diffusion model for fingerprint orientation extraction and a hierarchical classifier for fingerprint classification in this paper. The proposed classification algorithm is composed of five cascading stages. The first stage rapidly distinguishes a majority of Arch by using complex filter responses. The second stage distinguishes a majority of Whorl by using core points and ridge line flow classifier. In the third stage, K-NN classifier finds the top two categories by using orientation field and complex filter responses. In the fourth stage, ridge line flow classifier is used to distinguish Loop from other classes except Whorl. SVM is adopted to make the final classification in the last stage.

Ayman [23] suggested novel minutiae based fingerprint matching system. The paper presents a new thinning algorithm, a new features extraction and representation, and a novel feature distance matching algorithm. The proposed system is rotation and translation invariant and is suitable for complete or partial fingerprint matching. The proposed algorithms are optimized to be executed on low resource environments both in CPU power and memory space. The system was evaluated using a standard fingerprint dataset and good performance and accuracy were achieved under certain image quality requirements. In addition, the proposed system was compared favorably to that of the state of the art systems.

P. Lucena et al [24] has suggested the detection of explosive-contaminated human fingerprints technique, which constitutes an analytical challenge of high significance in security issues and in forensic sciences. The use of a laser-induced breakdown spectroscopy (LIBS) sensor working at 31 m distance to the target, fitted with 2D scanning capabilities and designed for capturing spectral information from laser-induced plasmas of fingerprints is presented. An effectiveness of 100% on fingerprints detection, regardless the substrate scanned, is reached. Environmental factors that affect the prevalence of the fingerprint LIBS response are discussed.

Jie et al [25] have proposed both the minutiae and orientation field feature are extracted and then fused to get a more comprehensive feature with scale and rotation invariability. Dealing with the second one, the pattern entropy is introduced to robustly measure the similarity of two incomplete fingerprints. Extensive experiments have been conducted on both those popular fingerprint databases and our extended databases containing more incomplete fingerprints. Meanwhile, thorough performance comparisons have been made with existing approaches. Experimental results show that our approach has more efficient ability especially in incomplete fingerprint recognition, and also performs well in both accuracy and efficiency.

3. Proposed Method

In the current investigation, an earnest effort is made to design an effective technique for the multimodal biometric recognition employing the Iris and Fingerprint. Initially, Iris recognition is carried out followed by the fingerprint recognition. Lastly, they are blended together to give shape to a novel multi-biometric so as to bring in superlative precision. Either of the two recognition procedures generally encompasses three diverse modules, such as the pre-processing, feature extraction and the recognition modules. In the first module viz. the preprocessing module, several methods are utilized which include the gray image conversion, histogram equalization, contrast enhancement to improve the image quality and adapt the image suitable for additional processing. Subsequently, the images are feature extracted by means of the modified LBP feature and Gabor based features in the feature extraction module. At last, the recognition is

performed with the help of the optimized Neural Network. The optimization function is executed by means of the sophisticated method namely the Bat Algorithm. After the recognition of the iris and fingerprint images, the images have to be blended. There are two levels of fusion performed such as the feature level fusion and score level fusion. In the feature level fusion, the Group Search Optimization algorithm is effectively employed. The correlation metrics are proficiently utilized for the purpose of the score level fusion, where the scores achieved from the diverse classifiers are integrated. The iris can easily be identified by means of the Naive bayes classifier together with the PSO whereas the Fingerprint image is detected with the help of the Adaptive Genetic Fuzzy System (AGFS). In the testing phase, the test images are furnished to the trained system for the purpose of identification. The comprehensive procedure of the novel technique is beautifully brought out in Figure.1 shown below.

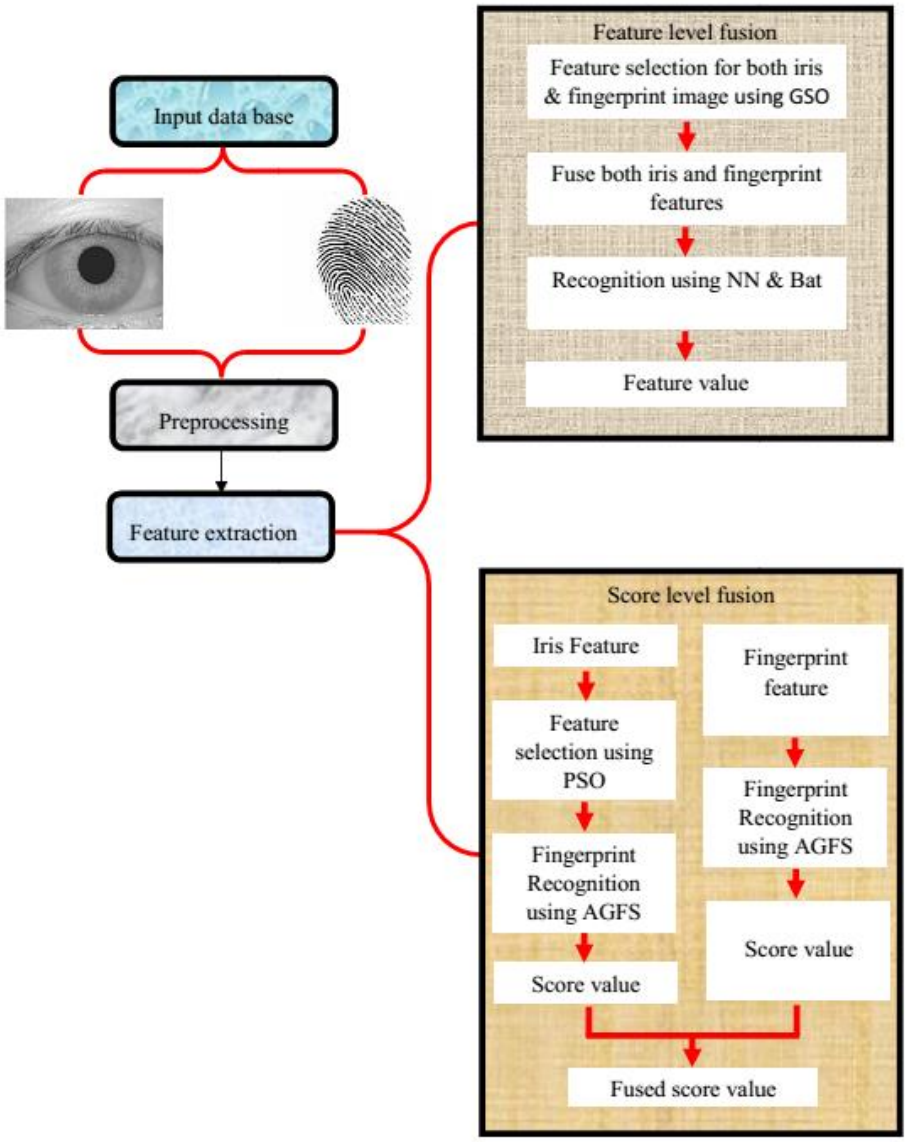


Figure.1 The block diagram for the proposed method

The innovative two-level fusions based multimodal biometric authentication technique navigates through the following three modules:

- The Preprocessing Module
- The Feature Extraction Module
- The Recognition Module

3.1. Module 1: Preprocessing

The fundamental target of the preprocessing module is dedicated for the enhancement of the

image quality to adapt it suitable for additional processing by getting rid of or scaling down the isolated and extra segments in the backdrop of the input images. Thus, it is highly essential to have the preprocessing task so as to perk up the quality of the input image. It effectively adapts the input image as ideal one for the succeeding two procedures such as the feature extraction and recognition. It is necessary to adapt the color image into gray image. With the intention of augmenting the image qualities, the histogram equalization is applied to the input image. Here, each and every pixel is substituted by integral of the histogram of the image in the corresponding pixel. The histogram equalization, in quintessence, represents a novel technique in the image processing of contrast modification by means of the image histogram. By means of this adaption, the intensities can be well distributed on the histogram. With the result, the regions having the lower local contrast achieves the superior contrast. The histogram equalization carries out this by effectively spreading out the most recurrent intensity values. Moreover, it is found to be advantageous in images with the backgrounds and foregrounds both of which are either bright or dark. Further, it is effectively employed to carry out the contrast adaption in such a way that the image anomalies become further transparent. Subsequent to the preprocessing function, the preprocessed image is furnished to the successive procedure.

3.2. Module 2: Feature extraction

Thereafter, the preprocessed images are feature extracted by means of the customized LBP feature in the feature extraction module. 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.

3.2.1. Modified LBP feature

The modified local binary pattern is evaluated by contrasting a center pixel of an image with its adjacent pixels. The resultant rigorously negative values are encoded with 0 and the others with 1. A binary number is achieved by concatenating the entire binary codes in a clockwise direction commencing from the top-left one and its resultant decimal value is employed for labeling. The achieved binary numbers are termed as the Local Binary Patterns or the LBP codes.

$$LBP(a,b)=\sum_{i=0}^{i-1}s(p_i-p_c)2^n \quad (1)$$

Where,
P_c - Gray value of the center pixel (a, b)
(a, b) – Pixel position
P_i - the grey values of the 8 surrounding pixels
n- Number of surrounding pixel
The function of $s(x)$ is given below,

$$S(x)=\begin{cases}1 & if \ \ x\geq 0\\ 0 & if \ \ x<0\end{cases} \quad (2)$$

Local Gabor XOR Pattern (LGXP)

The phase part of Gabor followed by LBP gives LGXP. In LGXP, descriptor phases are quantized into the diverse ranges. The number of phase ranges is generated so as to devise the patterns dynamic to the deviations of Gabor phase, and hence cannot be extremely elevated. Each and every phase value is quantized with the help of the quantization procedure. Subsequently, the LGXP operator is effectively utilized to the quantized phases of the central pixel and each of its neighbors. $LGXP_{\omega,v}^{k}=(k=1,2.....p)$ denotes the pattern determined between $\phi_{\omega,v}(l)$ and its neighbor H_k is evaluated as illustrated below.

$$LGXP_{\omega,v}^{k}=q(\varphi_{\omega,v}(H_{ph}) \ \ XOR \ \ q(\varphi_{\omega,v}(H_k)) \quad (3)$$

Here, $\varphi_{\omega,v}(H_{ph})$ denotes the phase and $q(\varphi_{\omega,v}(H_k))$ represents the quantized value of the phase and where $\phi_{\omega,v}(l)$ depicts the central pixel position in the Gabor phase map with scale w and orientation ω , p represents the dimension of neighborhood. At last, the consequential binary labels are concatenated jointly as the local pattern of the central pixel.

$$LGXP_{\omega,v}(H_{ph})=\sum_{k=1}^{p}2^{k-1}.LGXP_{\omega,v}^{k} \quad (4)$$

When the *LGXP* procedure comes to an end, an identical value is achieved and the relative task gets repeated for each and every block. Subsequent to the feature extraction procedure, the features are furnished to the fusion process.

3.3 Feature level fusion

In the feature level fusion, the extracted features from the Iris and fingerprint images are fed as the inputs for the feature level fusion. Now, the extracted features are furnished to the Group Search Optimization algorithm for choosing the optimal features. An extensive depiction of the GSO is

demonstrated below.

3.3.1 Group Search Optimization

The Group search optimization algorithm (GSO) is basically envisaged to optimize the extracted feature from the iris and fingerprint images. The members forming part of a group are of three diverse categories such as the producers, the scroungers and the rangers.

Producers: They are entrusted with the task of hunting for the food resources.

Scroungers: They effectively the resources, identified by the producers.

Rangers: They usually travel randomly and carry out the searching task in an orchestrated manner, in order to realize the effective identification of the food resources.

Initialize the search solution as well as the head angle

At first, the search solution is initialized and in the case of the novel technique, the solution characterizes the feature value from the iris and fingerprint image. In respect of each and every individual solution, the head angle can be expressed as shown in Equation (5).

$$\Psi_i^s = \left(\Psi_{i1}^s \ldots\ldots\ldots \Psi_{i(n-1)}^s\right) \tag{5}$$

The direction of search of the member is squarely dependent on the head angle which is illustrated in equation (6).

$$SD_i^s(\Psi_i^s) = \left(SD_{i1}^s \ldots\ldots\ldots SD_{i(n)}^s\right) \tag{6}$$

The Polar and Cartesian coordinate transformation is effectively deployed to appraise the direction of search based on the head angle.

$$SD_{i1}^s = \prod_{p=1}^{n-1} \cos(\Psi_{ip}^s) \tag{7}$$

$$SD_{ij}^s = \sin(\varphi)\ ;$$

$$where\ \ \varphi = \Psi_{i(j-1)}^s \prod_{p=j}^{n-1} \cos(\Psi_{ip}^s); \tag{8}$$

$$(j = 2 \ldots n-1)$$

$$SD_{in}^s = \sin(\Psi_{i(n-1)}^s) \tag{9}$$

Fitness function

The fitness function is evaluated as illustrated in Equation (10).

$$fitness = rand\ \ index \tag{10}$$

It is estimated for the initial solution sets. Subsequent to the assessment of the solutions, the producer of the group is found out.

Find the producer Z_p of the group

The member with the top fitness of Z_i is known as the producer and indicated as Z_p.

- Producer performance

In the course of the functioning of the GSO technique, the action of the producer Z_p at the "s^{th}" iteration may be described as given below.

(i) It carries out the scanning assignment at zero degree

$$Z_z = Z_p^s + \varepsilon_1 d_{\max} SD_p^s\left(\Psi^s\right) \tag{11}$$

Where, d_{max} denotes the maximum search distance.

(ii) It accomplishes the scanning function at the right hand side hypercube

$$Z_r = Z_p^s + \varepsilon_1 d_{\max} SD_p^s\left(\Psi^s + \varepsilon_2 \Phi_{\max}/2\right) \tag{12}$$

(iii) It executes the scanning task at the left hand side hypercube

$$Z_l = Z_p^s + \varepsilon_1 d_{\max} SD_p^s\left(\Psi^s - \varepsilon_2 \Phi_{\max}/2\right) \tag{13}$$

Where, ε_1 points to a normally distributed random number with zero mean and unity standard deviation and ε_2 stands for a uniformly distributed random sequence which has values within the range 0 and 1.

The maximum search angle Φ_{max} is effectively represented as:

$$\Phi_{\max} = \frac{\pi}{c^2} \tag{14}$$

Now, the constant *c* can be furnished as:

$$C = round(\sqrt{n+1}) \tag{15}$$

Here, n corresponds to the dimension of the search space.

$$\therefore \Phi_{\max} = \frac{\pi}{n+1} \tag{16}$$

The evaluation of maximum search distance d_{max} includes the ensuing equations.

$$d_{\max} = \left\| U_d - L_d \right\|$$

$$d_{\max} = \sqrt{\sum_{i=1}^{n} (U_{d_i} - L_{d_i})^2} \tag{17}$$

Here, d_{Ui} and d_{Li} represent the upper and lower limits of the *i*th dimension, correspondingly.

The best location consisting of the most

beneficial resource may be achieved by means of Equations (11), (12) and (13). The existing best location will give way for a new best location, if its existing resource is found to be inferior to that in the new location. Otherwise, the producer preserves its location and turns its head as per the head angle direction which is randomly produced by means of Equation (18).

$$\Psi^{s+1} = \Psi^{s} + \varepsilon_2 \tau_{\max} \tag{18}$$

Here, τ_{max} corresponds to the maximum turning angle which is evaluated with the help of the equation given below.

$$\tau_{\max} = \frac{\Phi_{\max}}{2} \tag{19}$$

When the producer is unable to identify a better position even after the completion of *m* iterations, its head would then assume its initial position as given in equation (20).

$$\Psi^{s+c} = \Psi^{s} \tag{20}$$

- Scrounger performance

In all the iterations, many members other than the producer are selected and they are termed as scroungers. During the *s*th iteration, the function of area copying which the *i*th scrounger carries out may be shaped as a movement to inch towards the producer in an intimate manner which is illustrated as:

$$Z^{s+1} = Z_i^{s} + \varepsilon_3 o(Z_p^{s} - Z_i^{s}) \tag{21}$$

Here, o specifies the Hadamard product which determines the product of the two vectors in an entry-wise manner and ε_3 denotes a uniform random sequence lying in the interval of (0, 1).

- Ranger performance

The rangers are the residual members of the group, which have been relocated from their current location. They are competent to efficiently locate the resources by carrying out arbitrary walks or by means of an orchestrated searching process. Both the head angle and the distance related to the ranger are created in an arbitrary manner.

$$d_i = c.\varepsilon_1.d_{\max} \tag{22}$$

The arbitrary walk to a novel point may be illustrated as:

$$Z^{s+1} = Z_i^{s} + d_i L_i^{s}\left(\Psi^{s+1}\right) \tag{23}$$

When the whole procedure comes to an end, the fitness of the modernized solution is estimated. The best solution is achieved, if the procedure is replicated for "s" number of iterations. In accordance with these, the extracted features are optimally chosen and are identified by means of the optimized neural network.

3.4 Module 3: Recognition

Optimized neural network

In the novel technique, the chosen features are identified with the help of the artificial neural network. The neural networks are logically organized in layers, composed of a number of interlinked 'nodes' having an 'activation function'. The patterns are furnished to the network by means of the 'input layer', which communicates to one or more 'hidden layers' where the actual processing is carried out by means of a system of weighted 'connections'. The hidden layers are next linked to an 'output layer'. Now the chosen feature values are offered as the input for neural networks. The structure of neural networks is beautifully pictured in Fig.2.

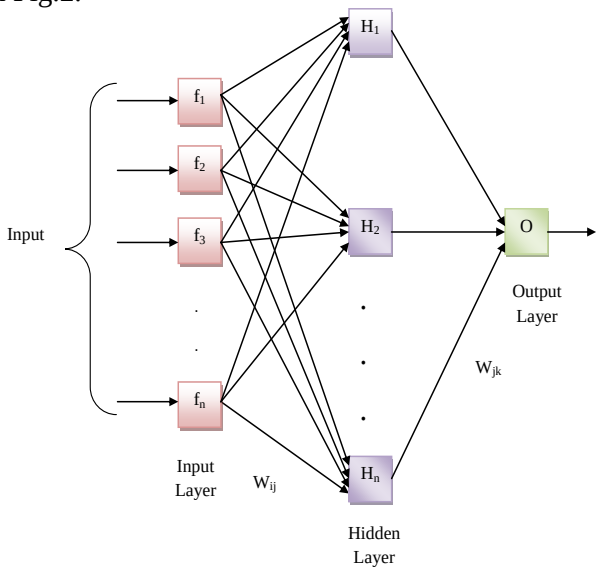


Figure.2 The structure of neural network

The major steps needed in the neural network are detailed as follows.

- The loads for each and every neuron are attached separately from the neurons in the input layer.
- The neural network is enlarged with the chosen feature value as the input units. Where, "H_n" as the Hidden units and "O" as the output unit.
- The recommended bias function is evaluated for the input layer as:

$$I = \sum_{i=1}^{n} w_n f_n \tag{24}$$

- The activation function for the output layer is estimated roughly as:

$$Active\,(I) = \frac{1}{1+e^{-I}} \quad (25)$$

In our proposed method we use three input layer, one hidden layer with twenty neurons and one output layers are used for recognize purpose. In the artificial neural network, the weights are optimized with the mighty assistance of the bat algorithm. With an eye on realizing the minimum error value the neural network weights are optimized, as illustrated in the following section.

3.4.1 Weight Optimization Using Bat algorithm

The innovative bat algorithm represents a meta-heuristic technique, stimulated by the echolocation conduct of the micro-bats. It is effectively employed to find the optimal weights for the neural network. Recounted below is a concise account of the novel bat algorithm.

Step by step procedure of bat algorithm

Step 1: Initially, the bat population S_i (where, $i=1, 2,\ldots,n$) is initialized. Here the population is represented as the weight.
Step 2: Thereafter, the pulse frequency (f) and velocity (v) are initialized which is followed by the initialization of the pulse rate (r) and loudness (L).
Step 3: At this junction, the fitness is estimated with the help of the following equation.

$$fitness = \sum_{1=1}^{n} MSE \quad (26)$$

Step 4: The new population is generated by adapting the frequency and modernizing the velocity by means of the following Relations.

$$\begin{aligned} f_i &= f_{\min} + (f_{\max} - f_{\min})\gamma \\ v_i^{\,x} &= v_i^{\,x-1} + (s_i^{\,x} - s_0) f_i \\ s_{new} &= s_{old} + EL^x \end{aligned} \quad (27)$$

Here $i= \{1,2,\ldots N\}$, where N denotes the number of bats. E and ϒ represent arbitrary numbers, E & ϒ ϵ [0, 1]. S_{old} symbolizes the existing global best location. $L^x = \langle L_i^x \rangle$ refers to the average of loudness.
Step 5: If the arbitrary number exceeds the pulse rate, the solution is selected from among the best and a local solution is created around the best solution by flying randomly. Now the fitness is determined.
Step 6: *If ($rand<L_i$ and $f(s_i)<f(s_n)$)*, new solution is accepted by stepping up the pulse rate and scaling down the loudness. Thus, the best location is found out. With the help of the above cited procedures, the optimal weights are found out, followed by the accomplishment of the neural network process.

- Now the learning error is located.

$$Error = \frac{(desired\ output - obtained\ \ output)^2}{2} \quad (28)$$

- The procedure is continued till the achievement of the minimum error.

In the long run, the target value is fixed and in accordance with the target value the images are identified. Then, the relative feature value is obtained. Finally, we got the feature value for both iris and fingerprint images. These values are fused based on the following procedure. Here we select the feature value position with the interval two bases and then we fuse the feature value. Based on these in our proposed work the feature values are fused.

3.5 Score level fusion

The score level fusion effectively matches scores output of the multiple biometric matchers by integrating them to produce a new match score. Here, the iris as well as fingerprint images are preprocessed and the features extracted. A comprehensive account of the preprocessing function and feature extraction has already been offered. Now, the extracted iris features are optimally chosen with the help of the particle swarm optimization technique and identified by means of the Naive bayes classifier and ultimately, the score value is attained. Thereafter, the extracted fingerprint features are detected by the Adaptive Genetic fuzzy system. Here, the rules are created by the fuzzy system and the optimal rules are chosen by means of the adaptive genetic algorithm. Now, the conventional genetic algorithm is improved with the assistance of the mutation function. The gradual process of the score level fusion for the iris and fingerprint images is beautifully pictured in the upcoming section.

3.5.1 Score level fusion using Iris image

Here the extracted features from the iris image are fed as the input for particle swarm optimization, which is elaborated in the following section,

Feature Selection Using PSO

The PSO is designed as per the social behavior of birds in a flock. Each particle flies in the search space with a velocity modified by its own flying remembrance and the flying experience of its companion in the PSO. Each particle possesses a key function value which is determined by a fitness

function. To choose the optimal features, the particle swarm optimization (IPSO) is effectively utilized.

Steps involved in Particle Swarm Optimization:

The diverse stages involved in the Particle Swarm Optimization are clearly spelt out below.

- **The Initialization:** At first, the particles are initialized randomly with position and velocity. Here, the particles characterize the extracted features.
- **The Fitness function:** In respect of each and every randomly created particle, the optimization fitness functions are ascertained.

$$fitness = rand\ index \quad (29)$$

- **The Gbest and Pbest initialization:** At the beginning, the fitness value is roughly determined for each and every particle. The optimal one is deemed as the Gbest and Pbest value among the fitness value. Subsequent to that iteration, the current optimal fitness value is selected as the Pbest and the overall best fitness value chosen as the Gbest.
- **The Velocity computation:** The velocity and the position of particle changed by means of Equation (30).

$$v_i(t+1) = v_i(t) + a_1 rand(Pbest(t) - s_i(t)) + a_2 rand(Gbest - s_i(t)) \quad (30)$$

$$s_i(t+1) = s_i(t) + v_i(t+1) \quad (31)$$

Where,

V_i is the particle velocity

S_i is the current particle

rand is a random number between (0,1)

a_1, a_2 are learning factor. Usually $a_1 = a_2 = 2$

- The procedure is continued until the achievement of the solution with superior fitness value.

After choosing the optimal features the features are detected by means of the Naïve bayes classifier. Here the optimal features are detected and the score value arrived at.

Naïve bayes classifier

The naive Bayes classifier represents an easy probabilistic classifier dependent on the famous Bayes theorem with strong presumption. This classifier is based on the configuration of a feature independent probability model. It presumes that the existence (or otherwise) of a specific feature of a class is not related to the existence (or otherwise) of any other feature, for a specified class variable. One of its outstanding merits is that it does not require a huge size of samples for effective training. The specified working procedure of the naive bayes classifiers is shown as follows. Let as assume *T* as the training sample set. Each sample (*S*) is characterized by a d dimensional vector and each vector describes n number of attributes (*A*).

(1) For a specified sample *S*, the naive bayes classifier forecasts the class dependent on the highest posterior probability. In other words, *S* is forecast to belong to the class C_x if and only if,

$$P(C_x \mid S) > P(C_y \mid S); for 1 \le y \le m, y \ne x \quad (32)$$

Thus we find the class that maximizes P(Cx|S). According to the bayes theorem,

$$P(C_x \mid S) = \frac{P(S \mid C_x)P(C_x)}{P(S)} \quad (33)$$

P(S) is identical for the entire classes, and hence it is necessary just to locate the largest *P (S|Cx) P (Cx)*. If the previous probability of class C_x is unidentified, it is generally presumed that the probability of these classes is the same. Thus *P (C1) = P (C2) = ...= P (Cm).*

(2) If the attributes of the dataset are high, the workload of evaluating $P(S|C_x)$ tends to very high. With a view to scale down the workload of $P(S|C_x)$, easy assumptions such that under certain situation attribute value is independent of each other

$$P(S \mid C_x) = \prod_{k=1}^{n} P(S_k \mid C_x) \quad (34)$$

(3) The Probability $P(S_1|C_x)$, $P(S_2|C_x)$, ..., $P(S_n|C_x)$ may be evaluated from the training set. Here S_k refers to the attribute A_k of sample *S.*

(4) For each and every class, $P(S|C_x)P(C_x)$ has to be evaluated. If and only if $P(S|C_x)P(C_x)$ is the maximum, the classifier forecast sample S belongs to class *Cx*.

Subsequent to the recognition of iris we attain the feature value from the naïve bayes classifier.

3.5.2 Score level fusion using fingerprint image

Here the extracted features from the fingerprint image are furnished the input to the adaptive genetic fuzzy system. It is effectively elaborated in the ensuing section.

Adaptive Genetic Fuzzy System

The adaptive genetic fuzzy system is effectively used to identify the fingerprint image. Firstly, the rules are created in accordance with the fuzzy system. Now, the input for the fuzzy system is the chosen features from the input of the fingerprint image. The output of the fuzzy system is the number of rules. At last, the optimal rules are chosen by means of the adaptive genetic algorithm. The general procedure by means of the gradual processes is beautifully pictured in the following section.

Fuzzy system

Here, a 360-degree view of the fuzzy system launched as the fingerprint recognition method. The most vital concepts underlying the fuzzy system employ the notion of the linguistic variables to take appropriate decisions dependent on the fuzzy rules and hence achieve a superior response in relation to a technique employing the crisp values.

1) Designing of fuzzy system

The design of the novel fuzzy technique is achieved through three vital steps such as the fuzzification, fuzzy inference engine and the defuzzification. *Fuzzification:* It effectively adapts the crisp input to a linguistic variable with the membership function gathered in the fuzzy knowledge base. *Fuzzy inference engine:* By means of the If-Then type fuzzy rules, it smartly adapts the fuzzy input into the fuzzy output. *Defuzzification:* It has the function of adapting the fuzzy output of the inference engine to the crisp with the help of the membership functions analogous to those employed by the fuzzifier. Thereafter, the crisp rules are fuzzified in the inference system by means of the triangular membership function in the current investigation work. The fuzzification is highly essential as a degree of membership function is specified for each member of set. The fuzzy system is capable of predicting the outcomes further accurately by means of the membership function.

Fuzzy Membership function: The membership function is achieved by choosing the proper membership function. Now, the triangular membership function is chosen to change over the data into the fuzzified value. The Triangular membership function is home to three vertices such as *a*, *b* and *c* in a fuzzy set (*a*: lower limit and *c*: upper limit where membership degree is zero, *b*: the centre where membership degree is one).

The formula employed to estimate the membership values is depicted as follows.

$$m(f)=\begin{cases} 0 & if\ f \le p \\ \dfrac{f-p}{q-a} & if\ p \le f \le q \\ \dfrac{r-f}{r-q} & if\ q \le f \le r \\ 0 & if\ f \ge r \end{cases} \qquad (35)$$

Now, it is crystal clear that at (*p*) and (*r*) the value is zero and it regularly achieves a maximum of value one at the centre point (*q*) between the (*p*) and (*r*). The triangular membership function is elegantly exhibited below.

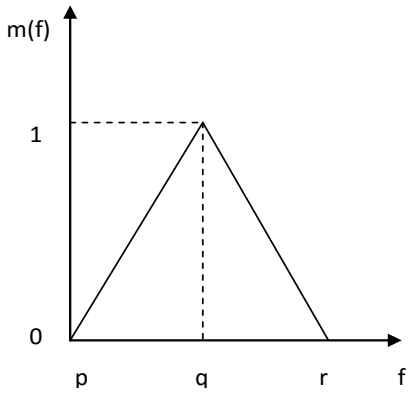


Figure.3Triangular membership function

Rule Base: The rule base encloses a set of fuzzy rule in the form of: If A and B then detect C. By employing the fuzzy system, the detection of fingerprint is carried out. The number of rule is equivalent to the number of features chosen from the input image. At last, the best rules are chosen by means of the adaptive genetic algorithm. Now, the conventional genetic algorithm is improved with the help of the mutation rate. In accordance with the AGA algorithm the optimal rules are chosen. The proposed method generates totally 260 rules. These rules are the input for the adaptive genetic algorithm. The detail explanation of adaptive genetic algorithm is given below,

Adaptive Genetic algorithm

In this method, the population is randomly created and subsequently two individuals are selected based on the fitness. Suppose A has fitness which is higher than that of B, then A is selected and B disregarded. The process goes on until an appropriate solution is obtained or a specific number of generations have passed, in phase with the needs of the user.

Generation of chromosomes

The initial solutions are randomly generated and each solution is called the gene. The individual genes are integrated as chromosomes and it is termed as the solution set. The numbers of genes are integrated with the chromosomes and the solution set for the population is created. The population of genetic algorithm encompasses the chromosomes and the population size is initialized as permanent. The numbers of solutions are initialized as per the typical genetic algorithm. Here, the initial solutions are called the number of rules.

Fitness function

The fitness function is evaluated by means of Formula 36 given below,

$$Fitness = \max accuracy \quad (36)$$

It is estimated for the initial solution sets of the chromosomes. After the evaluation of the solutions, the cross over and mutation function are applied on the chromosomes of the solutions sets.

Cross over

In the cross over, the two parent chromosomes are chosen with a view s to exchange their genes between them and perform the single point cross over.

Mutation

Subsequent to the crossover, the new chromosome is mutated for augmenting the efficiency of the solution. The optimal rules are achieved after the mutation function.

Updation

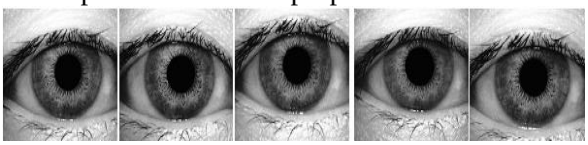
When the mutation function is completed, the new chromosomes are generated for the new solution sets. Later on, the fitness value is found out for the new solutions. The solution which furnishes the best value is selected and deemed as the optimal solution. Otherwise, steps cited above are repeated for the new solution sets.

The testing data with diminished attribute is specified to the fuzzy logic system, where the test data is adapted to the fuzzified value as per the fuzzy membership function. Subsequently, in accordance with the membership function, the fuzzified input is harmonized with the fuzzy rules defined in the rule base. Thereafter, the output is specified to the defuzzification, now the fuzzified value is converted to the crisp value and the evaluation is performed. The fuzzy score is created after the defuzzification procedure. At last we got the two score value based on the two score value we fused the iris and fingerprint image. Here we find the mean value of iris and fingerprint score value. Based on the mean value we fuse the iris and fingerprint image in score level fusion. The performance analysis of our proposed technique is shown in below section.

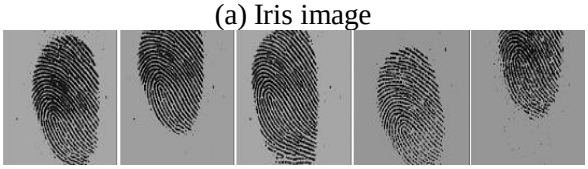
After the preprocessing stage the proposed method fed to the feature extraction process. Here modified LBP features are used to extract the features from the iris and fingerprint image. From the preprocessed image we have to find the number of features form both iris and fingerprint image using modified LBP feature. Table.1 shows the extracted feature value for both iris and fingerprint

4. Results and Discussion

The proposed fusion method is implemented in MATLAB platform. Here iris and fingerprint images are the input to this implementation. In our proposed method we are using CASIA database. Here we are taking 280 image for both iris and fingerprint images. Here 260 images for training and 20 images for testing. The following figure shows the sample iris and fingerprint images that are used as the input for the fusion purpose.



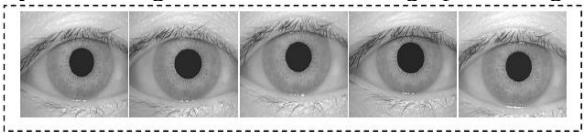
(a) Iris image



(b) Fingerprint image

Figure.4 Input sample image for both iris and fingerprint image

Initially the proposed implemented method is preprocessed here the input sample images are convert to gray scale image. Fig.5 shows that the gray scale image of both iris and fingerprint image.



(a) Iris image

(b) Fingerprint image

Figure.5 Grayscale image for both iris and fingerprint image

Then our proposed technique uses the contrast enhancement technique for each input gray scale image.

Table 1. Extracted features value for iris and fingerprint image

Image	**Feature value**									
Iris	956	345	530	319	1051	273	175	385	999	5025
Fingerprint	1879	385	350	126	340	912	140	162	607	11349

After the feature extraction, the feature value for both iris and fingerprint images are input for the optimization algorithm. Here the extracted features are optimized and select the optimal feature value. The optimal features values are tabulated in table.2. It is shown in below section,

Table 2. Optimal feature value

Image	Feature Value		
Iris	345	319	175
Fingerprint	385	126	140

Finally, the selected features are the input for the recognition module. In our proposed method two types of fusion technique is used here feature level fusion and score level fusion is employed based on these the iris and fingerprint images are recognized. In feature level fusion we find the feature value for both unimodal and multimodal approach. We find the recognition accuracy for iris and fingerprint image and also the fused image. Here the used image has high recognition accuracy value. The sensitivity, specificity and accuracy values are calculated using the expression given below,

Sensitivity

The proportion of actual positives which are correctly identified is the measure of the sensitivity. It relates to the ability of test to identify positive results.

$$Sensitivity = \frac{TP}{TP + FN} \quad (37)$$

Specificity

The proportion of negatives which are correctly identified is the measure of the specificity. It relates to the ability of test to identify negative results.

$$Specificity = \frac{TN}{FP + TN} \quad (38)$$

Accuracy

We can compute the measure of accuracy from the measures of sensitivity and specificity as specified below.

$$Accuracy = \frac{TP + TN}{TP + FN + FP + TN} \quad (39)$$

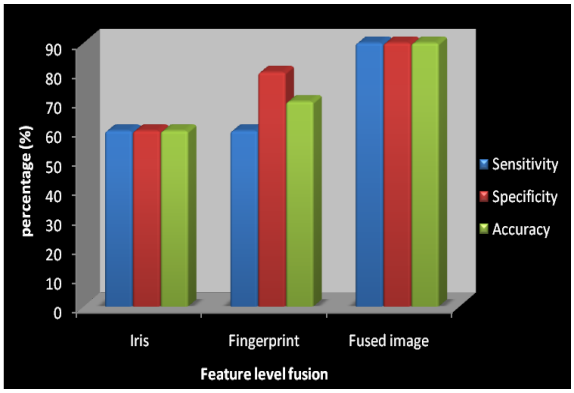


Figure.6 Performance value for feature level fusion

In our proposed feature level fusion method, the accuracy value for fused image achieves 90% accuracy value. Iris and fingerprint image achieves 60% and 70% recognition accuracy. The fig.6 shows the recognition accuracy, sensitivity and specificity value for feature level fusion.

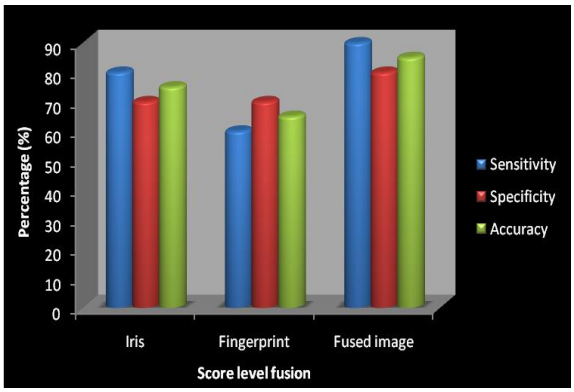


Figure.7 Performance value for score level fusion

Fig.7 represents the performance value for the score level fusion. In score level fusion, the iris and fingerprint feature values are the input. Here we find the score value for iris and fingerprint image separately and then fused the two score value. The recognition accuracy for the iris image achieves 75% accuracy value and the fingerprint image achieves 65% accuracy value. Finally, the fused score value from the iris and fingerprint image achieves 85% of accuracy value.

False Acceptance Rate (FAR)

It is ratio of number of false acceptance and number of identification attempts. It is indirectly proportional to the number of identification attempts.

$$FAR(\%) = \frac{No\ \ of\ \ false\ \ accep\tan ce}{No\ \ of\ \ identification\ attempts} \quad (37)$$

False Rejection Rate (FRR)

It is ratio of number of false rejection and

number of identification attempts. It is indirectly proportional to the number of identification attempts.

$$FRR(\%) = \frac{No\ \ of\ \ false\ \ rejec\tan ce}{No\ \ of\ \ identification\ attempts} \quad (38)$$

Equation 37 and 38 represents the false acceptance rate (FAR) and false rejection rate (FRR). Table.3 shows the FAR and FRR value for iris and fingerprint image and also for the fused image. In table.4 shows the FAR and FRR value for fused image is minimum when compared with the unimodal images. So our fused method is done efficiently and gets the better performance result.

Table 3. FAR and FRR value for different images

Level of fusion	**Image**	**FAR (%)**	**FRR (%)**
Feature level fusion	Iris	0.66	0.66
	Fingerprint	0.33	0.66
	Fused image	0.11	0.11
Score level fusion	Iris	0.375	0.25
	Fingerprint	0.5	0.66
	Fused image	0.22	0.11

The comparison of the proposed feature level fusion method and score level fusion method with existing method is shown in Table.4 and Table.5.

Table 4. Comparison of proposed feature level fusion method with existing method

Methods	Feature	FAR	FRR
Existing method [26]	Fused Image (iris and fingerprint)	2.3%	7.6%
Proposed Method	Fused Image (iris and fingerprint)	0.11%	0.11%

Table 5. Comparison of proposed score level fusion method with existing method

Methods	Feature	FAR	FRR
Existing method [27]	Fused Image (iris and fingerprint)	1.46%	6.87%
Proposed Method	Fused Image (iris and fingerprint)	0.22%	0.11%

From the above table.4 and table.5, it shows that the FAR rate of proposed feature level fusion method is 0.11% and FRR rate is 0.11%, which is lower than other existing feature level fusion method. And also the proposed score level fusion method achieve 0.22% FAR value and 0.11% for FRR value. When comparing the FAR and FRR value with existing method, the proposed work is lower when related with other method. Thus the performance of the method is better than existing method. Biometric identification is more secure, quite flexible and easily scalable. From the result, the proposed method achieves high level of recognition accuracy with biometrics systems for fused image when compared to the existing method. The false acceptance and rejection rate of the suggested method is minimum value when compared to the existing method for fused image.

5. Conclusion

The multimodal biometric authentication employing the iris and fingerprint images is elegantly launched in the document. The novel approach is performed in the MATLAB platform on a typical system and feat is assessed under benchmark datasets. The accomplishment of the novel technique is assessed in terms of evaluation tools such as the precision, accuracy, FAR and the FRR. The proposed feature level fusion method achieves 0.11% for FAR and 0.11% for FRR and the proposed score level method achieves 0.22% for FAR and 0.11% for FRR. The efficiency in performance of the new-fangled method is evaluated and contrasted with those of the parallel modern methods. The charismatic outcomes yielded by the epoch-making technique have appeared as ample credentials of par-excellence performance of proposed procedure especially in terms of superlative precision vis-à-vis those of the peer methods. In future work, the sensitivity specificity and accuracy value of recognition is improved using various optimization and classification techniques. And also evaluate various recognition metrics for the performance evaluation.

Reference

[1] D. V. Hiep, T. Q. Duc, and N. T. H. Lan, "A Multibiometric Encryption Key Algorithm Using Fuzzy Vault to Protect Private Key in BioPKI Based Security System", *Computing and Communication Technologies, Research, Innovation, and Vision for the Future (RIVF)*, pp. 1-6, Nov. 2010.

[2] R. Dhamija and J. D. Tygar, "The battle against phishing: Dynamic security skins", *In Proceedings of the Symposium on Usable Privacy and Security ACM Press*, pp. 77–88, 2005.

[3] K. D. Mitnick, W. L. Simon, and S.Wozniak, "The Art of Deception: Controlling the Human Element of Security", *John Wiley & Sons*, 2002.

[4] D. V. Klien, "A Survey of, and Improvements to Unix Password Security", *In Proceedings of the Second USENIX Workshop on Security*, pp. 5-14, 1990.

[5] S. Kadry and K. Smaili, "A Design and Implementation of a Wireless IRIS Recognition Attendance Management System", *Information Technology and Control*, Vol. 36, No. 3, pp. 323-329, 2007.

[6] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating Faces, Finger- prints and Soft Biometric Traits for User Recognition", *In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW), The Art of Deception: Controlling the Human Element of Security* Vol. 3087, pp.259-269, 2004.

[7] S. K. Mohanty and P. K. Pattnaik, "Authentication Based on Texture Analysis and SVM Classification", *International Journal of Instrumentation, Control and Automation (IJICA)*, Vol. 1, No. 1, pp. 61-66, 2011.

[8] Z. Yaghoubi, K. Faez, M. Eliasi and A. Eliasi, "Multimodal biometric recognition inspired by visual cortex and Support vector machine classifier", *International Conference onMultimedia Computing and Information Technology (MCIT)*, pp. 93-96, 2010.

[9] C. H. Chen and C. Chu, "Fusion of Face and Iris Feature for Multimodal Biometrics", *Lecture Notes in Computer Science*, Vol. 3832, pp. 571-580, 2005.

[10] A. Ross and A. K. Jain, "Multimodal Biometrics: An Overview", *in Proc. of 12th European Signal Processing Conference (EUSIPCO)*, pp. 1221-1224, September 2004.

[11] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 27, No. 3, pp. 250-255, March 2005.

[12] P. Paysan, R. Knothe, B. Amberg, S. Romdhani and T. Vetter, "Face Recognition Using 3-D Models: Pose and Illumination", *In proceedings of IEEE international conference on pattern recognition*, Vol. 94, No. 11, pp. 1977 - 1999, 2009.

[13] S. P. Narote, A. S. Narote and L. M. Waghmare, "Iris Based Recognition System using Wavelet Transform", *International Journal of Computer Science and Network Security*, Vol. 9, No. 11, pp. 101-104, November 2009.

[14] S. Gupta, V. Doshi, A. Jain and S. Iyer, "Iris Recognition System using Biometric Template Matching Technology", *International Journal of Computer Applications*, Vol. 1, No. 2, pp. 21-30, 2010.

[15] S. K. Devireddy, "An Accurate Human Identification through Iris recognition", *Georgian electronic scientific Journal in Computer Science and Telecommunication*, Vol. 6, No. 23, pp. 22-29, 2009.

[16] G. R. V. Sreenivasarao, P. Ramesh, and D. R. Kiran, "A Novel Approach for Human Identification through Fingerprints", *International Journal of Computer Applications*, Vol. 4, No. 3, pp. 35-42, July 2010.

[17] X. S. Yang, "A New Metaheuristic Bat-Inspired Algorithm", *Nature Inspired Cooperative Strategies for Optimization, Studies in Computational Intelligence, Springer*, Vol. 284, pp. 65-74, 2010.

[18] W. K. Chen, J. C. Lee, W. Y. Han, C. K. Shih, and K. C. Chang "Iris recognition based on bi-dimensional empirical mode decomposition and fractal dimension", *Information Sciences*, Vol. 221, pp. 439-451, 2013.

[19] R. Himanshu, and A. Yadav, "Iris recognition using combined support vector machine and Hamming distance approach", *Expert systems with applications*, Vol. 41, No. 2, pp. 588-593, 2014.

[20] M. D. Marsico, C. Galdi , M. Nappi, D. Riccio, "FIRME: face and iris recognition for mobile engagement and for mobile engagement", *Image and Vision Computing*, Vol. 32, No. 12, pp. 1161-1172, 2014.

[21] D. Yadav, J. S. Doyle, and M. Vatsa, "Unravelling the effect of textured contact lenses on iris recognition", *Information Forensics and Security, IEEE Transactions on Information Forensics and Security*, Vol. 9, No. 5, pp. 851-862, 2014.

[22] K. Cao, L. Pang, J. Liang, and J. Tian, "Fingerprint classification by a hierarchical classifier", *Pattern Recognition*, Vol. 46, No. 12, pp. 3186-3197, 2013.

[23] A. M. B. Eldin, "A medium resolution fingerprint matching system", *Ain Shams Engineering Journal*, Vol. 4, No. 3, pp. 393-408, 2013.

[24] P. Lucena, I. Gaona, J. Moros, J. J. Laserna, "Location and detection of explosive-contaminated human fingerprints on distant targets using standoff laser-induced breakdown spectroscopy", *Spectrochimica Acta Part B: Atomic Spectroscopy*, Vol. 85, No. 1, pp. 71-77, 2013.

[25] J. Zhang, X. Jing, N. Chen, J. Wang, "Incomplete fingerprint recognition based on feature fusion and pattern entropy", *The Journal of China Universities of Posts and Telecommunications*, Vol. 20, No. 3, pp. 121-128, 2013.

[26] M. Singh and T. S. Panag, "Heterogeneous Multimodal Biometric System with Fuzzy Vault Template Security", *International journal of advanced research in computer science and software engineering*, Vol. 4, No. 7, pp. 165-169, July 2014.

[27] U. Gawande, A. Sapre, A. Jain, S. Bhriegu and S. Sharma, "Fingerprint-Iris Fusion Based Multimodal Biometric System Using Single Hamming Distance

Matcher", *International journal of engineering Inventions*, Vol. 2, No. 4, pp. 54-61, Feb 2013.

[28] A. K. Jain, K. Nandakumar, X. Lu, and U. Park, "Integrating Faces, Finger- prints and Soft Biometric Traits for User Recognition", *In Proceedings of ECCV International Workshop on Biometric Authentication (BioAW)*, Vol. 3087, pp. 259-269, 2004.

[29] A. Ross and A. K. Jain, "Information Fusion in Biometrics", *Proc. of AVBPA, Halmstad, Sweden*, pp. 354-359, June 2001.

[30] M. T. Hagan and M. B. Menhaj, "Training Feed Forward Networks with the Marquardt Algorithm", *IEEE Transactions on Neural Networks*, Vol. 5, No. 6, pp. 989-994, 1994.