International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

Novel Biometric Fusion System using GA-PSO and ANN

Manpreet Kaur

Abstract*: Technology advancements have led to the emergence of biometrics as the most relevant future authentication technology. On practical grounds, unimodal biometric authentication systems have inevitable momentous limitations due to varied data quality and noise levels. The paper aims at investigating fusion of face and fingerprint biometric characteristics to achieve a high level personal authentication system. In the fusion strategy face features are extracted using Scale-Invariant Feature Transform (SIFT) algorithm and fingerprint features are extracted using minutiae feature extraction. These extracted features are optimized using nature inspired Genetic Algorithm (GA). The efficiency of the proposed fusion authentication system is enhanced by training and testing the data by applying Artificial Neural Network (ANN). The quality of the proposed design is evaluated against two nature inspired algorithms, namely, Particle Swarm Optimization (PSO)and Artificial Bee Colony (ABC) in terms of False Acceptance Rate (FAR), False Rejection Rate (FRR) and recognition accuracy. Simulation results over a range of image sample from 10 to 100 images have shown that the proposed biometric fusion strategy resulted in FARof 2.89, FAR 0.71and accuracy 97.72%.Experimental evaluation of the proposed system also outperformed the existing biometric fusion system.

Keywords*: Artificial Bee Colony (ABC), Artificial Neural Network (ANN), Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Scale-Invariant Feature Transform (SIFT).

I. INTRODUCTION

The rising incidents of security attacks and online thefts have raised the necessity of high level security systems to guard sensitive data from unauthenticated exploitation [1]. Among vivid security systems, biometric holds a significant position to deal with personal identification to offer privacy and security [2-4]. Various unimodal biometric authentication systems have been developed by numerous researchers that mainly deal with features of eye, face, fingerprint, palm geometry, etc [5-8]. In the development of a biometric authentication system several challenges are confronted that are majorly related to design and deployment cost, type of biometric used, acceptability and offered security level.

Revised Manuscript Received on February 28, 2020.
***** Correspondence Author
Dr. Manpreet Kaur*, Assistant Professor, Computer Science, Sri Guru Gobind Singh College, Chandigarh, India. Email: manpreet.sm@yahoo.com

The biometric aspects as shown in Fig. 1 forms the foundation of any biometric based recognition system and coordinating among them requires wiser considerations [9].These authentication systems fall in two categories.

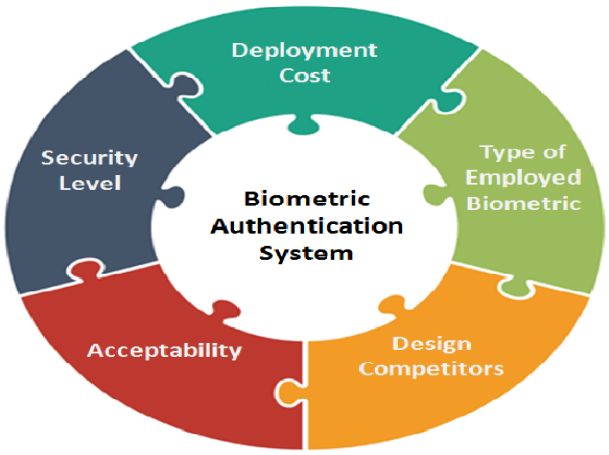

Fig .1. Aspects adjoining Biometric Systems

They are either a positive recognition systems that are employed to restrict unauthorised entry or are negative recognition systems that totally deny the access or entry of a specific individual. Out of the two, positive recognition systems are more popular than negative recognition systems [10]. Using single biometric trait may not reach the required security level. Hence, quality of unimodal biometrics systems can be enhanced with the combining features of individual unimodal biometrics [11]. The proposed research work comprises the fusion strategy that combines the strengths of individual face and fingerprint authentication systems in order to achieve the performance level which otherwise was unachievable with single biometrics. The major contributions in this research are listed below:

- Separate pre-processing steps are used to fingerprint and face data for better feature extraction from the data of fingerprint and face.
- The fingerprint features extraction is based on minutiae extraction algorithm where for face feature extraction, Scale-Invariant Feature Transform (SIFT) algorithm is used.
- Further, three optimization strategies namely, Genetic Algorithm (GA), Particle Swarm Optimization (PSO) and Artificial Bee Colony (ABC) are employed along with Artificial Neural Network (ANN) based training and classification to evaluate the quality of proposed recognition system in terms of False Acceptance Rate (FAR),

False Rejection Rate (FRR) and Recognition Accuracy.

The paper architecture is divided into 5 sections starting with introduction. In section 2 comprises of the related literature cited biometric work, section 3 discusses the proposed architecture design, section 4 evaluates the results and section 5 concludes the paper.

II. RELATED WORKS

In this section, various fusion systems have been discussed that were inspired by advantages of features exhibited by various biometric traits. It has been observed that most of the biometric recognition systems exploited face, fingerprint, iris and voice characteristics. In **2012, Muthukumar et al.** combined the features of fingerprint and iris to construct a multimodal biometrics authentication system. In the recognition evaluation was performed based on the similarity scores obtained in comparison to the defined threshold value. The paper incorporated Particle Swarm Optimization to deal with various security levels. The authors demonstrated that their proposed design successfully incorporated the features of biometric design in terms of security, legitimacy and flexibility [12]. **Aboshosha et al. (2015)** believed that with the combination of more than one feature could aid in the achievement of high level security system. In the light of their strong belief they proposed the biometric fusion system that combined the features of three biometric traits, namely, fingerprint, iris, and face. Their authentication system was based on scores that were that were subjected to minima-maxima based normalization. Following this, fusion was done based on the set of rules governing product, sum and weighted sum. The experimental evaluation demonstrated that the proposed multimodal score based biometric recognition system outperformed various unimodal biometric designs. Additionally, it was established that the weighed sum rule proved to be more effective as compared to sum and product rule based methods [11]. **Chaudhary and Nath (2016)** proposed a strong multimodal based biometric recognition design that was also based on score level fusion. The biometric design was based on the fusion of features of face, finger and iris features. In this study, scores were obtained while employing Support Vector Machines (SVM) approach in parallel fashion to order to successfully deal with the issues confronted due to missing biometric traits that may arise due to some inevitable conditions due to medical treatment or injury. The designed recognition system was evaluated against false acceptance rate and false rejection rate. It has been observed that the fusion of face and fingerprint features with the involvement of SVM achieved an accuracy of 97.653% [13]. **Yadav and Kumar (2016)** investigates the methods for fingerprint and face recognition. The face features examined with Euler-PCA to offer solution to deal with the visual variation in face categorization process and employed hamming distance for fingerprint minutiae features. The recognition was based on score level matching and the templates of both face and fingerprint were evaluated against a self created dataset. The simulation results in MATLAB 2015 a environment demonstrated false acceptance rate of 3.33% and false rejection rate of 3.27% [14]. **Mwaura et al. (2017)** proposed a score level face and fingerprint fusion biometric recognition system that was built using hamming distance approach and SIFT algorithmic design. The authors demonstrated that multimodal biometric system achieved a high recognition accuracy of 92.5% as compared to unimodal biometric systems, namely, fingerprint unimodal biometric system (82.5%) and face unimodal biometric system (90%) [15]. **Shivakumar and Patil (2018)** employed the use of fingerprint; iris and face features to construct a fusion based multimodal biometric system. In the proposed design, iris and face features were extracted using Bidirectional Empirical Mode Decomposition (BEMD) technique and fingerprint features were extracted using minutiae feature extraction technique. The authors proposed that the combination of BEMD, Grey Level Co-occurrence Matrix (GLCM) and minutiae feature extraction exhibited high recognition accuracy. In the process, multilevel Support Vector Machine (SVM) classifier was also involved. The results were evaluated in terms of sensitivity, accuracy, precision, recall, precision specificity, false acceptance and false rejection rate against existing works [16].**Gopal and Selvakumar (2018)** employed combination of Hybrid Bacterial Foraging and Particle Swarm Optimization to develop a multimodal face and fingerprint biometric recognition system. The face and fingerprint features were extracted using Principal Component Analysis (PCA) and Minutiae extraction, respectively. The system was evaluated using NIST BSSR1 database against 2068 fingerprint images and 1034 face images. The recognition system achieved an overall accuracy and ERR of 0.38 and 0.62, respectively [17]. **Singh et al. (2019)** presented a review that revolved around fusion strategies of biometric fusion systems. They covered the merits and criteria that decide what kind of feature, when and how specific features of a trait should be fused. Additionally information regarding developmental history of various biometric based recognition systems was also discussed. Hot topics integrating data quality, soft biometrics, approaches to enhance the accuracy of biometric recognition to prevent security attacks using cryptosystems were also discussed. Authors concluded their review while addressing the research challenges concerning biometric based fusion systems [18]. **Gunasekaran et al. (2019)** proposed a biometric recognition system that used Contour let Transform Model for pre-processing followed by Local Derivative Ternary Pattern model to improve recognition based on pre-processed features. Next, Weighted Rank Level Fusion was employed for the extraction of multimodal features to achieve score based fusion of face, fingerprint and iris modalities. A deep learning architecture was introduced to enhance the recognition rate of the proposed biometric system. It was demonstrated that fusion resulted in enhanced recognition rate of the proposed biometric recognition system [19]. **Viswanatham et al. (2019)** postulated a feature extraction design that could effectively extract features from low quality images. The proposed design was introduced as a variant of biometric fusion system. The design significantly lowered the requirement of large storage space along with minimizing the error rates of the recognition system.

Authors had implemented Morlet Wavelet Transform in order to decrease sensitivity of the system towards shape distortion while safeguarding local boundaries. The system achieved positive recognition when tested against 90% and 70% similar fingerprint and face images [20]. **Aleem et al. (2019)** proposed a face and fingerprint based biometric system to safeguard cyber-physical system. They employed Extended Local Boundary Pattern (ELBP) for facial features and alignment based elastic technique was used for fingerprint images. The system demonstrated high recognition accuracy when evaluated against images obtained from FVC 2000, ORL and YALE datasets [21].

III. PROPOSED DESIGN

In this section of paper, we discussed the implementation mechanism of proposed biometric fusion system using the two different biometric authentication systems such as fingerprint and face based unimodal. To evaluate the proposed model used the below discussed methodology step along with the databases.

A. Databases

In the proposed fusion biometrics authentication system two databases are used. The fingerprint images are obtained from Fingerprint Verification Competition (FVC) Database that provides high resolution fingerprint images available in gray scale [22]. Fingerprint images are available in *.tif format. Georgia Tech face database is used for face images that comprises of the image sized to square matrix of 150 pixels [23]. Face images are available in *.jpeg format.

B. Proposed Methodology

The fingerprint and face images are pre-processed to improve the quality of uploaded image followed by feature extraction. Fingerprint features are extracted using Minutiae based feature extraction and face features are expected using SIFT algorithm. The extracted features from image undergo feature optimization using GA. Further these optimized features are trained using ANN to construct a training dataset that is tested to evaluate the recognition efficiency of the proposed system in terms of false acceptance rate, false recognition rate and recognition accuracy of the fusion biometric system. The overview of the steps is summarized in the flow diagram shown in Fig. 2.

- Pre-processing

In this section, we apply the pre-processing steps on finger print as well as face image. In case of fingerprint, binarization and thinning is performed but in case of face part, face detection is performed by using the viola jones techniques is used with cascade process. The algorithm of pre-processing is written as:

Algorithm 1: Binarization of Fingerprint Data

Required Input: FP-Image←Fingerprint Image from Test Dataset

Obtained Output: BFP-Image← Binary Fingerprint Image

1 Start
2 Calculate the Size of FP-Image, [R, C] = size(FP-Image)
3 Find out the threshold pixel, Thresh = Average (FP-Image)
4 BFP-Image = null size of FP-Image
5 For m=1→R
6 For n=1→C
7 If FP-Image(m, n)> Thresh
8 BFP-Image (m, n) = 1
9 Else
10 BFP-Image (m, n) = 0
11 End – If
12 End – For
13 End – For
14 Return: BFP-Image as binary fingerprint image
15 End – Algorithm

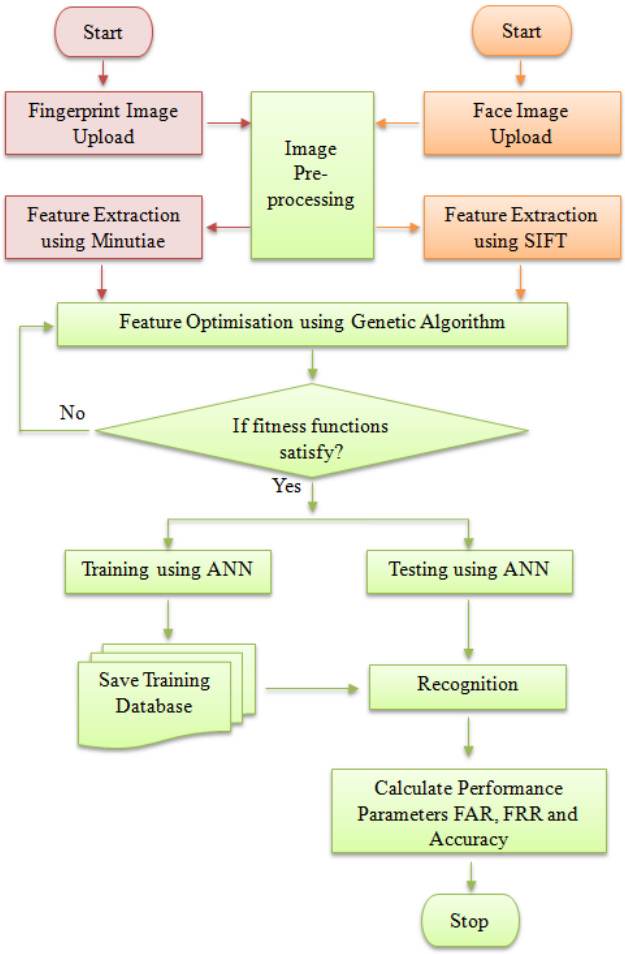

Fig. 2. Methodology flowchart of proposed biometric fusion system

Binarization is the process used to convert the image into black (0) and white (1) based on the threshold level of the pixel values which is exist in the image. Suppose, the threshold value of fingerprint image is calculated is 125 using the pixels of image. To convert the fingerprint image into binary image, if the pixel value is less than 125, then is considered as 0, whilst pixel value>= 125 are considered as using the given formula.

$$Binary\ Image, BTF - Image = \begin{cases} 0 & if\ pixel < Threshold \\ 1 & otherwise \end{cases}$$

According to the binarization algorithm and equation we convert the original fingerprint image into binary image which are shown in the Fig. 3 with original fingerprint image.

After the binarization, morphological operation is applied on the binary fingerprint image to convert image into thin image for better visualization of fingerprint ridges in terms of minutiae. The thinned fingerprint image is shown in the Fig. 3(c). Morphological operation is a collection of non-linear operations related to the shape or morphology of features in a fingerprint image. Apply Morphological operations on the binary image to find out the exact ridges within the binary image using the thinning operations and we got a thin fingerprint image (TFP-Image).

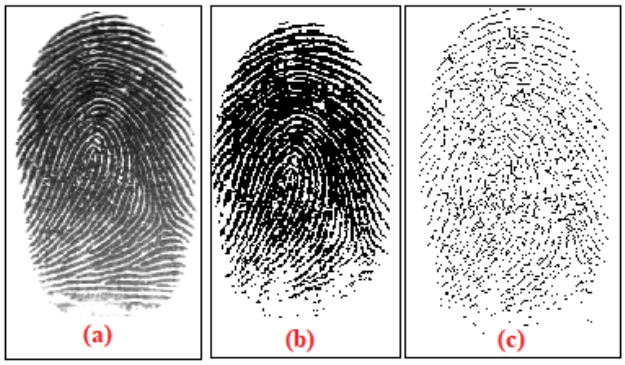

Fig. 3. Binary Images (a) Original Fingerprint Image, (b) Binary Image (0, 1) and (c) Thin Image

In case of face data, pre-processing is performed to detect the exact face region from the raw face data which is known as the region of face (ROF). To perform the pre-processing, we used the below mentioned algorithm.

Algorithm 2: Face Detector

Required Input: FC-Image← Face Image
Obtained Output: PFC-Image← Pre-processed Face Image

1 Start
2 Divide FC-Image in sub window for face region localization
3 Calculate the weights of each sub window
4 After that, normalization of weights is performing
5 Best weak classifier is selected using the concept of weighted error minimization
6 Based on the classifiers error, weights are updated
7 Repeat steps 3–6stepsfor each sub window
8 Apply Haar Wavelet for face pixel detection
9 Create a boundary of face region
10 Return: PFC-Image as a face boundary
11 End - Algorithm

In case of the face detection, the fundamental guideline of the Viola-Jones algorithm is to check a sub-window equipped for distinguishing faces over a given input face data. The methodology of non Viola-Jones algorithm is a time consuming due to the different size calculation and as opposed to the standard methodology of Viola-Jones algorithm using the concept of image rescaling. This algorithm uses a detector so it called integral image processing approach and the wavelet with the Haar family is applied. The concept of this algorithm is described in the algorithm steps. After the pre-processing we move towards the feature extraction process.

- Feature Extraction

In this step of methodology, we describe the process of feature extraction from fingerprint in terms of Minutiae Feature and from face data in terms of SIFT key points. The algorithm of Minutiae Feature Extractor is written as:

Algorithm 3: Minutiae Feature Extractor

Require Input: TFP-Image←Thin Fingerprint Image
Obtained Output: M-Points←Minutiae points of the TFP-Image

1 Start
2 Calculate the Size of TFP-Image, [R, C] = size (TFP-Image)
3 Count1 = 0 // initially termination is considered as 0
4 Count2 = 0 // initially bifurcation is considered as 0
5 For i=1→R
6 For j=1→C
7 Centriod of Ridge (i, j) = Properties (TFP-Image)
8 If Number of Centriod (i, j) ==1 // Represent the termination points
9 Termination (i, j) = Count1 +1
10 Else // Represent the bifurcation points
11 Bifurcation (i, j) = Count2 +1
12 End– If
13 End– For
14 End – For
15 M-Points = Concatenate[Termination + Bifurcation]
16 Return: M-Points as Minutiae points of the TFP-Image
17 End– Algorithm

Similar to minutiae extraction process in face-based biometric authentication system, SIFT feature is applied on the pre-processed ROF and the algorithm SIFT Descriptor is written as:

Algorithm 4: SIFT Descriptor

Required Input: PFC-Image←Pre-processed Face Image
Obtained Output: SIFT-Key points←SIFT feature of the PFC-Image

1 Start
2 Calculate the Size of PFC-Image, [R, C] = size(PFC-Image)
3 For m→1 to all R
4 For n→1 to all C
5 Scale Face Image=scaling (PFC-Image(m, n), Scale size)
6 L_Keypoints=Localization (Scale Face Image (m, n))
7 O_Keypoints=Orientation (L_ Keypoint (m, n), Angle)
8 SIFT-Key points=Filtering (O_Keypoint (m, n), Gaussian Filter)
9 End – For
10 End – For
11 Return: SIFT-Key points as SIFT feature of the TFC-Image
12 End

After the feature extraction in both cases fingerprint as well and in face recognition model, the achieved results is shown in the Fig.4.

It represents the extracted feature using the algorithm 3 and 4 for minutia extractor and SIFT descriptor respectively. Fig. 4 (a) represents the extracted minutia feature points of fingerprint image and 4 (b) represents the extracted SIFT key points of face image. After the feature extraction, we need to select a set of optimal or best feature set for training and testing of the proposed biometric fusion system.

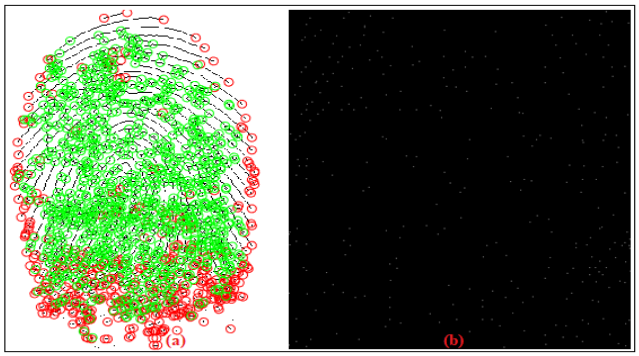

Fig. 4. Extracted Features (a) Minutiae Points, (b) SIFT Key points

▪ *Feature Optimization:* After the feature extraction step in both of biometric system, we need to create a unique feature sets which helps to increase the classification accuracy of biometric fusion system. So, Genetic Algorithm (GA) is used as a feature optimization technique and their algorithm is written as:

Algorithm 5: Feature Selection using GA

Required Input: M-Points←Minutiae points of the TFP-Image
SIFT-Key points← SIFT feature of the PFC-Image
EF=[M-Pointsor SIFT-Key points] ← Extracted Feature
Obtained Output: BSF← Best Selected Feature

1 Start
2 Initialize GA operators – Number of Iterations (T)
– Total Population Size (P)
– Crossover-function
– Mutation-function
– Objective/Fitness function
– Selection function (fs and ft)
3 Calculate the Size of EF, T = size(EF)
4 Fitness function: $f(fit) = \begin{cases} 1, (True) & fs \geq ft \\ 0, (False) & fs < ft \end{cases}$
5 For i= 1→ T
6 $fs = \sum_{i=1}^{P} f(i)$
7 $ft = \frac{\sum_{i=1}^{P} f(i)}{Lengt\ of\ total\ feature}$
8 f(fit) = fitness function which define above
9 No. of variables = 1
10 BSF = GA(f(fit), No. of variables, Initialized parameters)
11 End – For
12 Return: BSF as a Best Selected Feature
13 End – Algorithm

▪ *Training and classification:* After the feature selection using the GA as an optimization approach, ANN is used as classifier to train and classify the user based on their biometric traits using the concept of feature fusion. The Algorithm of ANN is written as:

Algorithm 5: ANN as a Classifier

Required Input: BSF ← Best Selected Feature as Training Data
G ←Target
N ←Neurons
Obtained Output: FS-Net←Trained Fusion System Network as a Structure

1 Start
2 Initialize the basic parameters of ANN– No. of Epochs (E) // as a repeating Iteration
– No. of Neurons (N) // as a carrier to carry input data
– Performance (MSE, Gradient, Mutation and Validation Point)
–Techniques of Training: Train-LM (Levenberg Marquardt)
– Data Division: Random
3 Calculate the Size of BSF, T = size(BSF)
4 For i = 1 → T
5 Group,G(i) = Categories of Training data
6 End – For
7 Initialized the ANN using Training data and Group
8 FS-Net = Newff (T,G,N)
9 Set the training parameters according to the requirements and train the system
10 FS-Net = Train (FS-Net, Training data, Group)
11 Return: FS-Net as Trained Fusion System Network as a Structure
12 End – Algorithm

IV. RESULTS

In this section of the research paper, we describe the experimental results of proposed biometric fusion system based on the simulation with different images. To evaluate the performance of the proposed model, we present a comparative analysis of fusion model with GA, PSO and ABC using the ANN as a classifier.

A. Evaluation Parameters

The proposed fusion design is evaluated in terms of Quality-of-Service (QoS) parameters. These parameters are defined as follows:

▪ *False Acceptance Rate (FAR):* In terms of biometric security, FAR is defined as the fraction that represents the number of times the designed system allowed an unauthorized access. FAR are also termed Type II error in statistical analysis.

$$FAR = \frac{Acceptance_{false}}{Total\ Matches_{Imposter}}$$

▪ *False Rejection Rate (FRR):* In biometric security, FRR defined as the fraction that represents the number of times the proposed design restricted an authorized access.

FRR can be understood as Type I error in statistical analysis and also termed as false non-Match errors.

$$FRR = \frac{Rejection_{false}}{Total\ Matches_{Genuine}}$$

FAR and FRR is a type of classification error and these errors could be overcome by wisely choosing the threshold of acceptance because high threshold will result in high FRR and low threshold will result in high FAR.

- *Classification Accuracy:* It defines the exactness of the match. It is the measurement criterion to determine the reliability of the designed biometric system. It is usually measured in terms of FAR and FRR exhibited by the system.

B. FAR Comparison

False acceptance rate observed with the proposed GA+ANN is compared against PSO+ANN and ABC+ANN. Table.1 summarizes the FAR observed while using GA, PSO and ABC when number of image samples is varied from 10 to 100.

Table-I: FAR comparison of GA, PSO and ABC

Number of Samples	GA	PSO	ABC
10	3.548	3.845	3.915
20	3.485	3.648	3.542
30	3.346	3.614	3.348
40	3.275	3.578	3.215
50	3.118	3.456	3.245
60	2.745	3.578	3.452
70	2.676	3.035	2.648
80	2.524	3.011	2.842
90	2.157	2.945	2.813
100	1.987	2.124	2.146

Comparative analysis of FAR values is shown in Fig. 5. The number of image samples ranging from 10 to 100 is plotted against parametric values observed for FAR using GA, PSO and ABC. The plot shows that GA exhibited lowest FAR values over all the image samples with the next higher FAR values observed with ABC followed by PSO. It has been observed that average FAR value with GA, PSO and ABC is 2.89, 3.29 and 3.12. This shows that GA achieved FAR value that is 0.4 and 0.23 lower when compared with PSO and ABC.

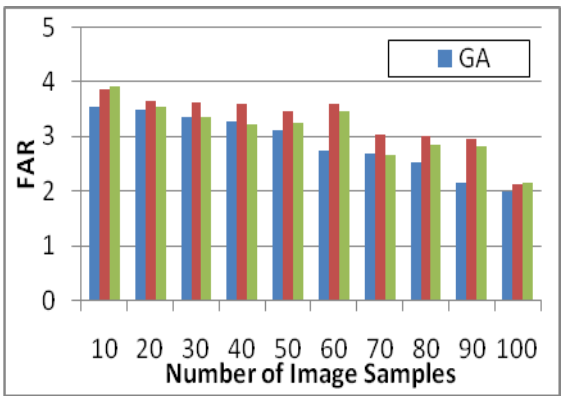

Fig .5. FAR comparison of GA, PSO and ABC

C. FAR Comparison

Similar to FAR, FRR values observed with GA are also compared against PSO and ABC. Table 2 shows the observed FRR values observed for GA in column 2 followed by PSO and ABC in column 3 and column 4 against experimental testing of 10 to 100 image samples.

Table-II: FRR comparison using GA, PSO and ABC

Number of Samples	GA	PSO	ABC
10	0.725	0.812	0.801
20	0.714	1.024	0.987
30	0.684	0.958	0.924
40	0.664	0.789	0.778
50	0.784	1.078	1.062
60	0.884	1.098	1.074
70	0.653	0.878	0.862
80	0.643	0.745	0.701
90	0.643	0.857	0.821
100	0.632	0.754	0.824

Fig.6 shows the comparison of FRR using GA, PSO and ABC approaches. It has been observed that over the range of 100 images lowest FRR have been observed in case of each image sample. In other words, GA approach exhibited a lowest average FRR of 0.71 as compared to average FRR of 0.9 and 0.89 exhibited by PSO and ABC. Hence, it can be concluded that average FRR value observed with GA is 0.19 and 0.18 lower than PSO and ABC.

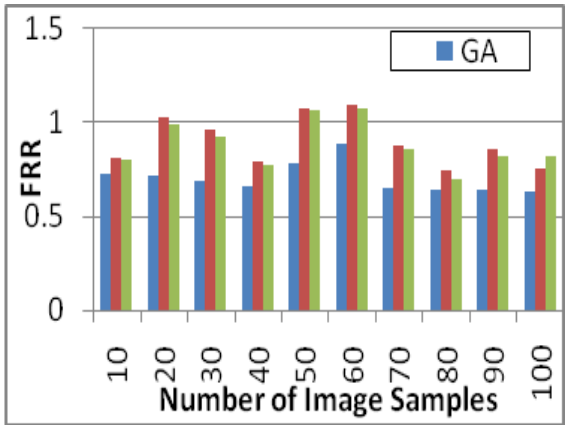

Fig .6. FRR comparison among GA,PSO and ABC

D. Accuracy Comparison

The recognition accuracy of the proposed architecture is also compared with the accuracy values observed while employing PSO and ABC. The accuracy values for the three cases, GA, PSO and ABC, in percentiles for the number of images samples from 10 to 100 are listed in Table .3.

Table-III: Accuracy comparison of GA, PSO and ABC

Number of Samples	GA	PSO	ABC
10	98.85	96.17	97.13
20	97.54	95.61	96.41
30	98.26	96.78	97.24
40	97.57	96.32	96.92
50	98.24	96.52	97.164
60	98.04	96.12	96.54
70	97.35	95.64	96.64
80	97.15	95.58	96.54
90	96.87	95.42	96.01
100	97.25	94.68	95.96

The accuracy values of the system are compared against the recognition accuracy of the system based on PSO and ABC as shown in Fig. 7. It has been observed that the biometric fusion system that is based on GA approach exhibited higher accuracy over all the image samples as compared to the systems that are based on PSO and ABC. GA based fusion system demonstrated an average accuracy of 97.72%, while the system based on PSO had an average accuracy of 95.89% and ABC had an average accuracy of 96.66%. This shows that GA approach had an enhanced accuracy of 1.83% and 1.06% over PSO and ABC based biometric fusion systems.

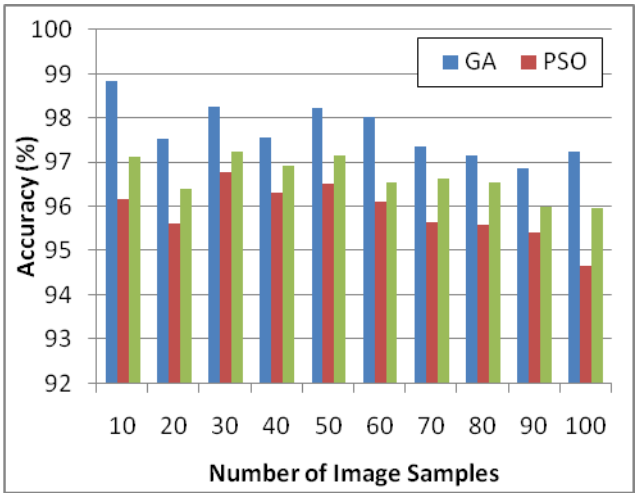

Fig. 7. Accuracy comparison of GA, PSO and ABC

E. Evaluation against existing work

The proposed system is also evaluated for FAR, FRR and accuracy values against the existing biometric fusion based recognition systems. FAR and FRR of the proposed work is compared against two existing works of Yadav and Kumar [14] and Mwaura et al. [15] is shown in Fig. 6. Yadav and Kumar's biometric fusion system employed the strengths of e-PCA (Euler Principal Component Analysis) and exhibited FAR of 3.33 and FRR of 3.27 while Mwaura et al.'s work was based on score level fusion and exhibited FAR of 3.75 and a very high FRR of 7.50. In contrast to these authors work, the proposed work outperformed the existing works with a lower FAR and FRR of 2.89 and 0.71, respectively.

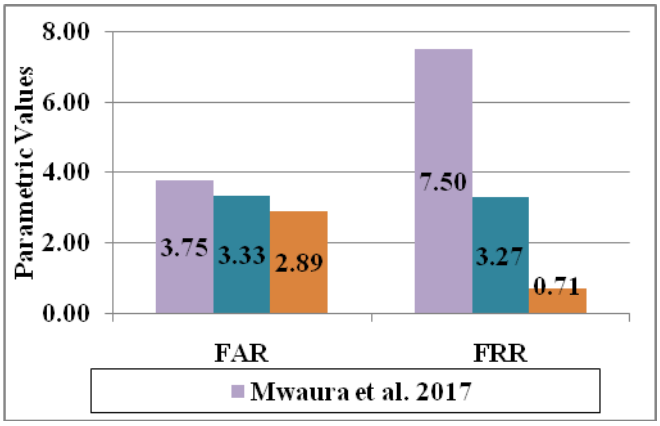

Fig . 8. FAR and FRR comparison of proposed work against existing work

Accuracy of recognition of the proposed biometric fusion system is also compared against existing of Chaudhary and Nath [13] and Mwaura et al. [15] as shown in Fig. 7. Chaudhary and Nath had designed the biometric fusion system that employed Support Vector Machine (SVM) to achieve a recognition accuracy of 97.65% while Mwaura el al. could only achieve an accuracy of 92.50% using score level fusion. In comparison to these systems, the proposed work using GA and ANN demonstrated an average accuracy of 97.72% which is 0.07% higher than Chaudhary and Nath's work and 5.22% higher than Mwaura et al.'s work.

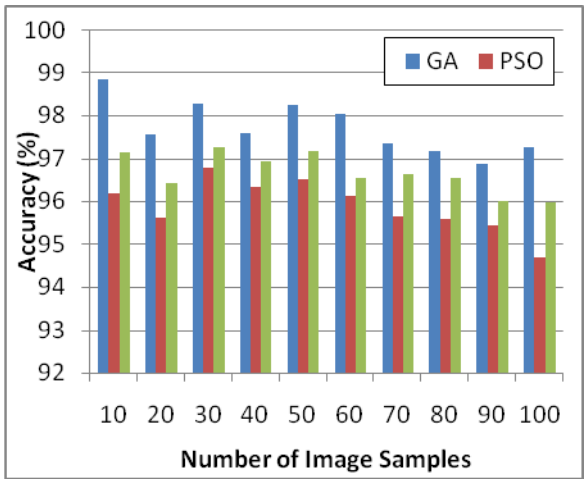

Fig. 9. Accuracy comparison of proposed work against existing work

V. CONCLUSION

The current work comprises the authentication system designed with the fusion of fingerprint and face features. Fingerprint and face features are extracted using minutia and SIFT based feature extraction approaches. Genetic algorithm was used to optimize the extracted features that are trained and classified using ANN to enhance the recognition accuracy and reduce FAR and FRR. The proposed system GA-ANN was evaluated against a combination of PSO-ANN and ABC-ANN.

It has been observed that GA, PSO and ABC achieved an average FAR value of 2.89, 3.29 and 3.12; average FRR value of 0.71, 0.9 and 0.89 and accuracy of 97.72%, 95.89% and 96.66%. These values demonstrated that the proposed GA-ANN combination outperformed the other two combinations, i.e., PSO-ANN and ABC-ANN. Moreover, the proposed recognition system also outperformed against the existing biometric fusion systems.

REFERENCES

1. Nareshkumar R. M., ApoorvaKamat, DnyaneshvariShinde "Smart Door Security Control System Using Raspberry Pi", International Journal of Innovations & Advancement in Computer Science, IJIACS, ISSN 2347-8616, Volume 6, Issue 11, November 2017
2. O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040.
3. Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. IEEE security & privacy, (2), 33-42.
4. Jain, A. K., Bolle, R., &Pankanti, S. (Eds.). (2006). Biometrics: personal identification in networked society (Vol. 479). Springer Science & Business Media.
5. Więcław, Ł. (2009). A minutiae-based matching algorithms in fingerprint recognition systems. Journal of medical informatics & technologies, 13.
6. Malhotra, P., & Kumar, D. (2017). An Optimized Face Recognition System Using Cuckoo Search. Journal of Intelligent Systems, 0(0). doi:10.1515/jisys-2017
7. Cao, K., & Jain, A. K. (2018). Automated latent fingerprint recognition. IEEE transactions on pattern analysis and machine intelligence, 41(4), 788-800.
8. Kalita, N., &Saikia, L. P. (2018). A Survey on Face Recognition based security system and its applications.
9. National Research Council, &Whither Biometrics Committee. (2010). Biometric recognition: challenges and opportunities. National Academies Press.
10. J. L. Wayman, "Fundamentals of Biometric Authentication Technologies", International Journal of Image and Graphics, Vol. 1, No. 1, pp. 93-113, 2001.
11. Aboshosha, A., El Dahshan, K. A., Karam, E. A., &Ebeid, E. A. (2015). Score level fusion for fingerprint, iris and face biometrics. International Journal of Computer Applications, 111(4).
12. Muthukumar, A., Kasthuri, C., & Kannan, S. (2012). Multimodal biometric authentication using particle swarm optimization algorithm with fingerprint and iris. ICTACT Journal on Image and video processing, 2(3).
13. Chaudhary, S., &Nath, R. (2016). A robust multimodal biometric system integrating iris, face and fingerprint using multiple SVMs. International Journal of Advanced Research in Computer Science, 7(2).
14. Yadav, N., & Kumar, V. (2016). A Novel Approach Based on Fingerprint Identification and Face Recognition. International Journal of Advanced Research in Computer Science, 7(3).
15. Mwaura, G. W., Mwangi, W., &Otieno, C. (2017). Multimodal Biometric System:-Fusion Of Face And Fingerprint Biometrics At Match Score Fusion Level. International Journal of Scientific & Technology Research, 6(4), 41-49.
16. Shivakumar, M., &Patil, C. M. (2018). Face, Finger Print and Iris Biological Characters Using Feature Level Fusion Based Multimodal Biometric Systems. Journal of Computational and Theoretical Nanoscience, 15(9-10), 2939-2948.
17. Gopal, N., &Selvakumar, R. K. (2018). A new approach for hybrid BF-pfPSO technique for face and fingerprint multimodal biometric system. International Journal of Applied Engineering Research, 13(6), 3512-3516.
18. Singh, M., Singh, R., & Ross, A. (2019). A comprehensive overview of biometric fusion. Information Fusion, 52, 187-205
19. Gunasekaran, K., Raja, J., &Pitchai, R. (2019). Deep multimodal biometric recognition using contourlet derivative weighted rank fusion with human face, fingerprint and iris images. Automatika, 1-13.
20. Viswanatham, P., Krishna, P. V., Saritha, V., &Obaidat, M. S. (2019). Multimodal Biometric Invariant Fusion Techniques. In *Biometric-Based Physical and Cybersecurity Systems* (pp. 321-336). Springer, Cham.
21. Aleem, S., Yang, P., Masood, S., Li, P., & Sheng, B. (2019). An accurate multi-modal biometric identification system for person identification via fusion of face and finger print. World Wide Web, 1-19.
22. FVC2004 database. Accessed URL http://bias.csr.unibo.it/fvc2004/databases.asp
23. Georgia Tech face database, Accessed URL http://www.anefian.com/research/face_reco.htm

AUTHORS PROFILE

Dr. Manpreet Kaur, Assistant professor in computer science in SGGS College, Chandigarh.