Volume: 6 Issue: VI Month of publication: June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6220

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Face Spoof Detection System Based on Genetic Algorithm and Artificial Intelligence Technique

Diksha Anand[1], Kamal Gupta[2]
[1, 2]Computer Science and Engineering, GNIT Mullana

***Abstract**: A secure face spoof detection systems demands the capability to identify whether a face is from a real person or a spoofed image which is create by spoofer. Face spoofing induces deformation in the image and also degrades the image pattern quality. In this research work, analysis of distortion and the quality assessment of an image to identify spoof attack is the most important consideration. The existing methods in image distortion analysis, extracts the feature sets that capture the facial details but pattern of image is not in consideration. So, the designed spoof detection system utilizes a hybrid algorithm by combining the genetic algorithm and artificial neural network to create a unique feature sets according to the categories of database images. In addition, it also uses SIFT descriptor to extract the key points of face and identify the pattern of face in the ROI of image. Artificial Neural Network (ANN) classifier is used for the training of proposed spoof detection system. It is seen that the designed hybrid system face spoof detection achieves high performance than the existing system and execution time is also well. The proposed approach is evaluated using MATLAB simulator in image processing and computer vision toolbox.*

Keywords: Biometric, Face Spoofing, SIFT, GA, ANN

I. INTRODUCTION

Biometrics technology implies techniques for measuring and analyzing human characteristics. Biometrics will be divided into 2 categories, in particular physical features such as fingerprints, facial or iris patterns, and activity features such as speech, signature or walk patterns (steps) [1]. That's because it may be one of the most prominent major challenges in various biometric systems, namely the possibility of fraud. This is known as Spoofing attack. The pirated data will be effectively used and imitated by pirates to achieve unauthorized access to the biometric identification system, rather than the consent of the actual user. Efforts to check the identification of fraudulent attacks produce a completely different view. In a part of the work, a progressive deception recognition technology was given to the physiological properties to detect light-weight facial statistics [2]. In general, there are two types of masks: positive and negative. The positive category (also known as the real face) limits the change, but the negative category adds a bad face to the picture, virtual or recorded video.

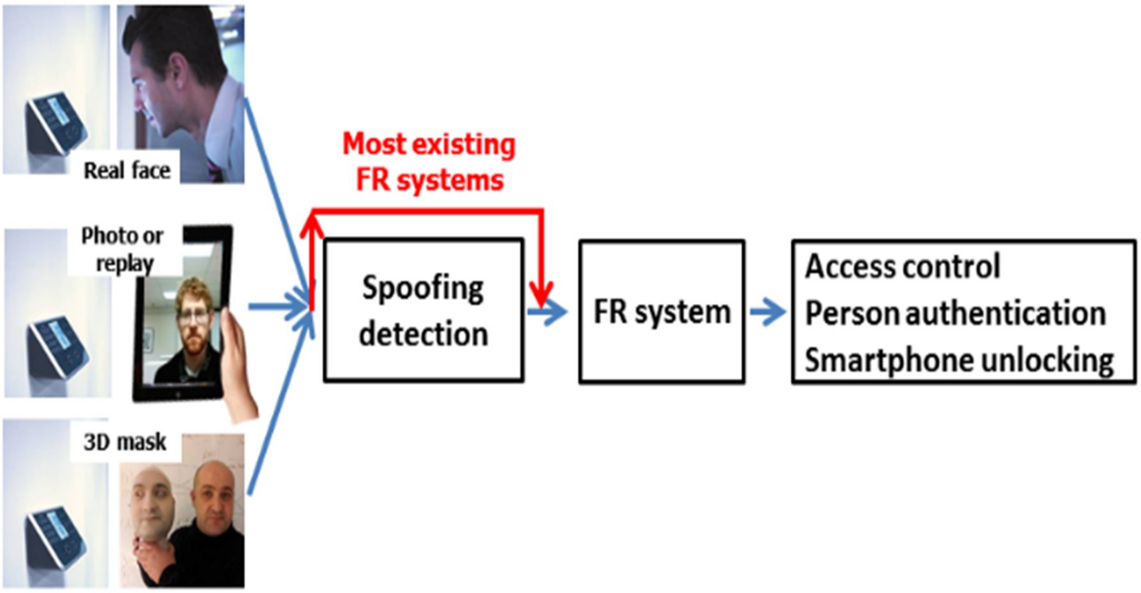


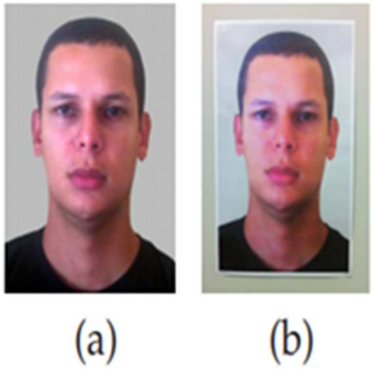
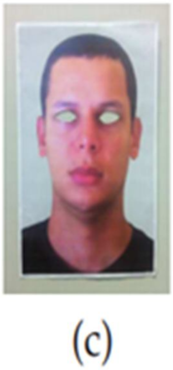
Fig. 1Face recognition system with spoofing detection module

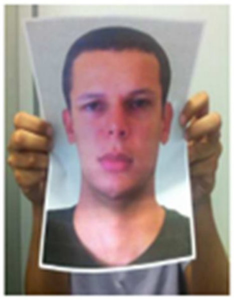
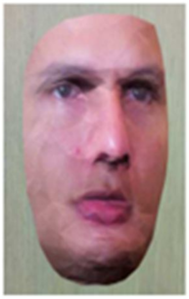
The popularity of face recognition has lifted up the issue of face-spoofing attacks (also referred to as biosensor rendering attacks) in which pictures or videos of authorized faces can be used to acquire facilities or services [3]. Although many face deception detection techniques have been proposed, their generalization capabilities have not yet been fully resolved.

With the approach of electronic medium, society is progressively reliant on PC for handling. With expanding innovation, man gets to be included with PC as the pioneer of this innovative age [4]. It has opened another age for humanity to go into world. A standout amongst the most imperative objectives of PC vision is to accomplish visual acknowledgment. Among numerous acknowledgment subjects, face spoofing detection has drawn significant interest and consideration from numerous analysts, for example, in the territories of reconnaissance, Closed Circuit Television (CCTV) control, client confirmation, HCI human PC interface, insightful robot et cetera. Various face spoofing strategies has been proposed for face detection, which is quick [5]. The proposed methodologies have focal points over the other face spoofing plots in its speed and effortlessness. We have proposed face spoofing detection scheme by using artificial intelligence. In the proposed work, face spoofing detection system using Artificial Neural Network has been proposed. In the case of ANN, first part is training and second is classification, and ANN has been trained by appropriate feature sets, so, in classification, they can easily classify test image with the help of trained structure. But problems may occur in case of feature optimization, if optimization technique is not used then training and testing will create problems. So, for the feature optimization in proposed work, genetic algorithm (GA) has been used. The main improvement in proposed work is the use of Genetic Algorithm to optimize the feature to increase the accuracy [6].

Face spoofing detection, counter measures for facial spoofing attacks, face liveness detection and face anti-spoofing are the types that are used interchangeably for denoting the techniques for identifying an imposter that tries to impersonate as an authentic user in face recognition system. These systems generally utilized following types of spoofing attacks [7].

TABLE 1 TYPES OF SPOOFING ATTACKS

Flat printed photo  	The utilization of flat printed photo is shown in figure 2(b) and is considered as the common one having the prospective to occur as number of people is there with facial pictures on the internet (social media) or the imposter could take the picture without permission or collaboration.
Eye cut photo attack  	In this, the regions of eye for the printed photo are cut off to show the blink deeds of the impostor as shown in figure 2(c).
Warped photo attacks	These are consisted in the bending of the printed photo in some direction for simulating the facial motions as depicted in figure 2 (d)

 (d)	
Video playback (e)	The attack occur because of video play back depicts the each behaviour as the real faces having the essential features of applicable user as shown in figure 2 (e). This kind of attack has the physiological signs of life which are not there in photos, viz. facial expressions, eye blinking, and head and mouth movements. It could be simply executed with the tablets or huge smart phones.
Mask attacks (f)  (g)	The mask attacks are of two types as shown in figure 2(f) and 2(g). These types of attacks are provided to anti-spoofing system which analyzes the 3-D face structures and is known as one of the composite attack for detection. The manufacturing of mask is more difficult and costly as compared to another attack with printing particular devices and 3-D scanning.

II. PLANNED FRAMEWORK

This work has dealt with the proposing a technique of efficient face spoofing technique with face images of any dimension. An appropriate face segmentation technique for the face recognition part to make feature extraction easy and best has been presented. The suitable and appropriate feature set form the face images SIFT feature are used. For achieving better accuracy in authentication systems, artificial neural network as a classifier has been proposed. The methodology of proposed work is given below:

Step 1: Design and develop a proper GUI for the proposed facial emotion recognition system.

Step 2: Upload the face images for Training and Testing of proposed facial spoofing detection system.

Step 3: Apply pre-processing on uploaded face images in both section. The proposed pre-processing algorithm is given as:

Algorithm 1st: Pre-Processing Algorithm

```
Upload Images
Apply pre-processing algorithm on uploaded image
For I = 1 to all sets
Resize_image = Resize (I)
Face_detection = Face_detector (I)
```

```
Thershlod = Threshold (Face_detection)
Gray_Face = Gray_conversion(Face_detection, Threshold)
ROI = Crop (Gray_Face, Region of Face)
End
```

Save all ROI data in as an input of SIFT feature extraction technique.

Step 4: Develop a code for the face spoofing detection from the pre-processed face images in training as well as testing section.

Step 5: Apply SIFT Descriptor for the feature extraction from the detected face. The SIFT algorithm is given as;

```
Algorithm 2nd: SIFT Algorithm
Load ROI data of face images
For I = 1 to all sets
detection= Gray_Face (I)
Keypoint_localization=Extrema_detection (I)
If localization need orientation
Orientation=Keypoint_localization (I)
end
Keypoint_descriptor=All best Feature
End
```

Save Keypoint_descriptor of proposed work for the next phase and we apply the Genetic Algorithm on the Keypoint_descriptor and fin the optimal solution of proposed work.

Step 6: Initialize Genetic Algorithm to optimize SIFT features and remove the unwanted feature sets using the novel objective function. Used algorithm of feature optimization is given as:

```
Algorithm 3rd: Genetic Algorithm
Define the population size of the GA (50)
Initialized the GA in Matlab
Set all initialization parameters
Load Keypoint_descriptor
For I = 1 to all Keypoint_descriptor
      For r=1 to all rows
      For c=1 to all columns
Define Ft (Threshold) = Average of Keypoint_descriptor
Define Fs = Keypoint_descriptor (r,c)
Call fitness function
                  $\text{Fitness Function} = \begin{cases} \text{True}, & \text{if Fs} > \text{Ft} \\ \text{False}, & \text{otherwise} \end{cases}$
         If fitness functions==True
           Consider as best solution as GA_data
         End
     End
     End
End
```

Save GA_data of proposed work and pass it as an input of ANN for training in training part and for classification in classification part.

Step 7: Apply Artificial Neural Network on optimized data to train the database and train the data using following steps:

Select optimized feature as an input of artificial neural network for training and testing data.Compute the total categories which are generated by the training of optimized data using artificial neural network.Step 8: After that in the classification section, the test data has been classified according to the trained artificial neural network structure. The ANN algorithm is given as:

```
Algorithm 4th: ANN Algorithm
Load GA_data
Training_data = GA_data
```

```
Initialize ANN
Generate group of data = group
Set iteration = 50
For I = 1 to iteration
    Weight = GA_data (i)
    Hidden_Neurons = [10] (tansig)
    Net_algo = trainlm
    Generat Net structure of ANN (net)
    Net = train (net, Training_data, group)
End
Save Net of proposed work as a structure and classify the test face on the basis of Net.
```

Step 9: At last of the module, the performance parameters of proposed spoof detection system like FAR, FRR, Execution time, Error rate and Accuracy are calculated.

III. RESULT AND DISCUSSION

Below figure described the structure of proposed spoof face detection system which is bassically developed using the concept of artificial intellegence techniques

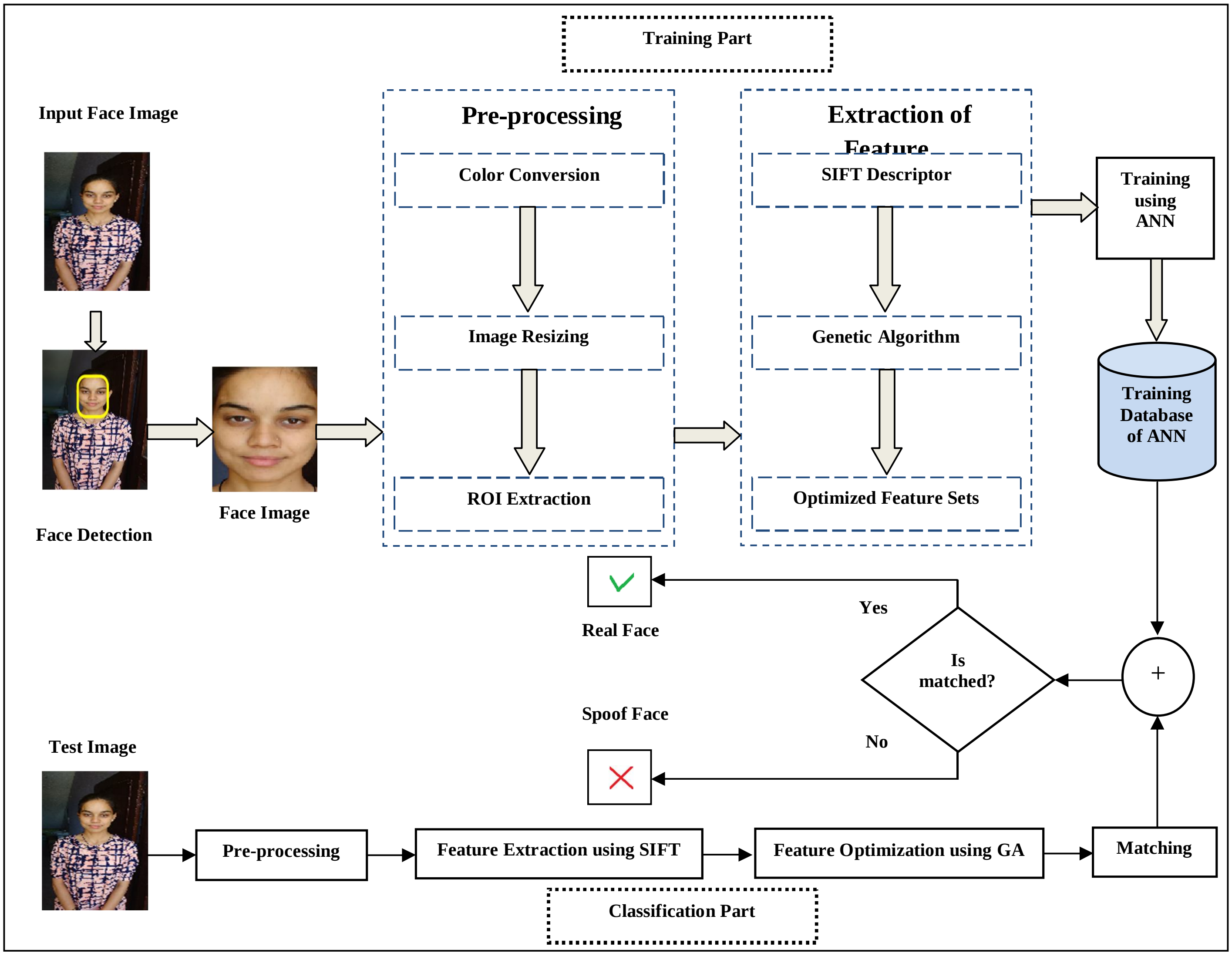


Fig. 2 Structure of proposed spoof face detection system

There are two section of proposed work, first is training and second is the classification of test face data. For the classification of proposed image we used images from the below described database.

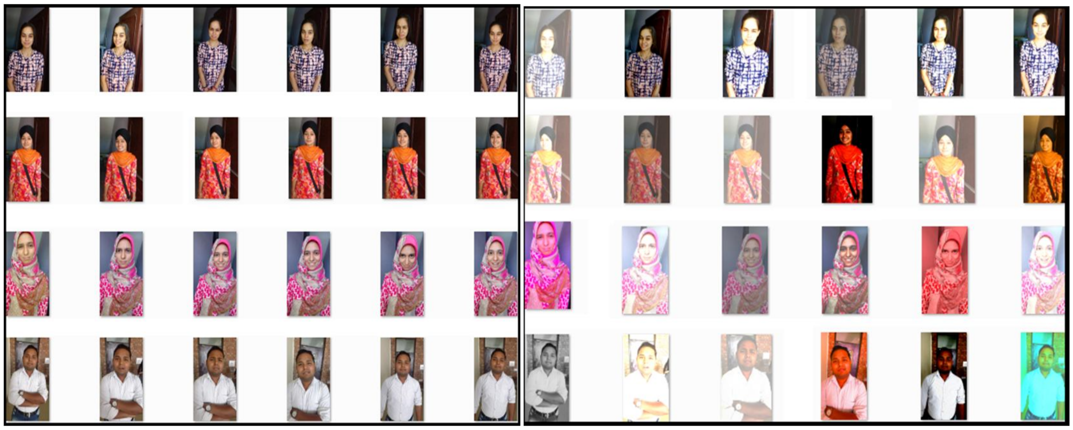
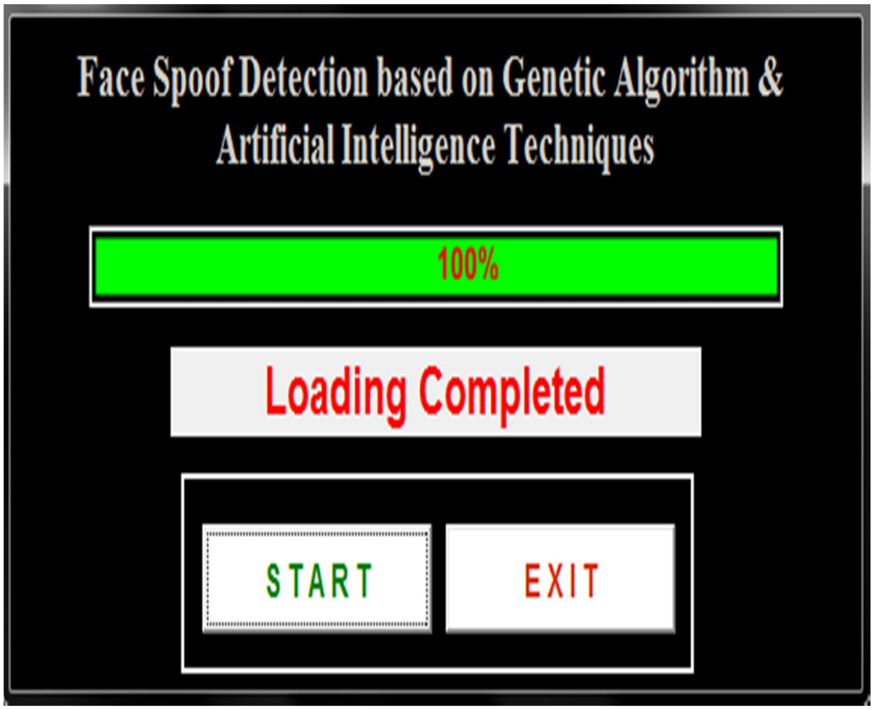


Fig. 3 (a) Original Images and (b) Database Images

Above figure represents the database of proposed work for detection of spoof image. A face spoof detection algorithm is based on SIFT along with genetic algorithm and artificial neural network is proposed, which is effective in grasping the intrinsic distortions of spoof face images with respect to the genuine face images. We has constructed a face spoof database using the cameras with non compression technique and the format of database images are ".JPEG". In the figure, (a) is the set of original image and (b) is the set of spoof images. The simulation results of proposed spoof detetcion system is described in the below section on the basis of database images.



Face Spoof Detection based on Genetic Algorithm & Artificial Intelligence Techniques

Loading Completed

Fig. 4 Title Window of Proposed Work

Title figure window of the proposed research work is shown in the above figure. The figure mainly comprises of two buttons named as START and EXIT button along with title window. In the title window, name given to the proposed work has been displayed and the status of simulation is also displayed in given window. After starting the title window, we have got the working figure window which is described in the below.

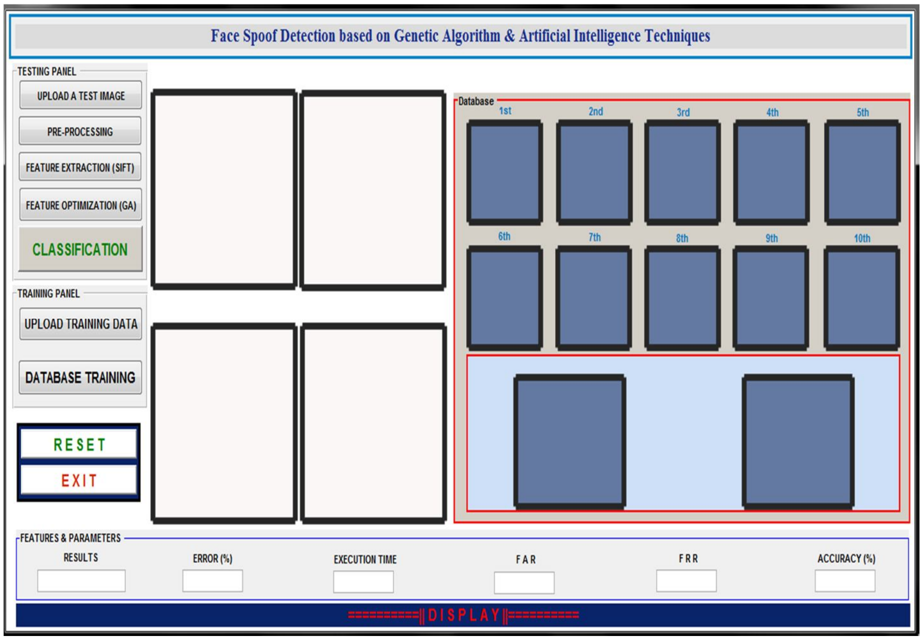
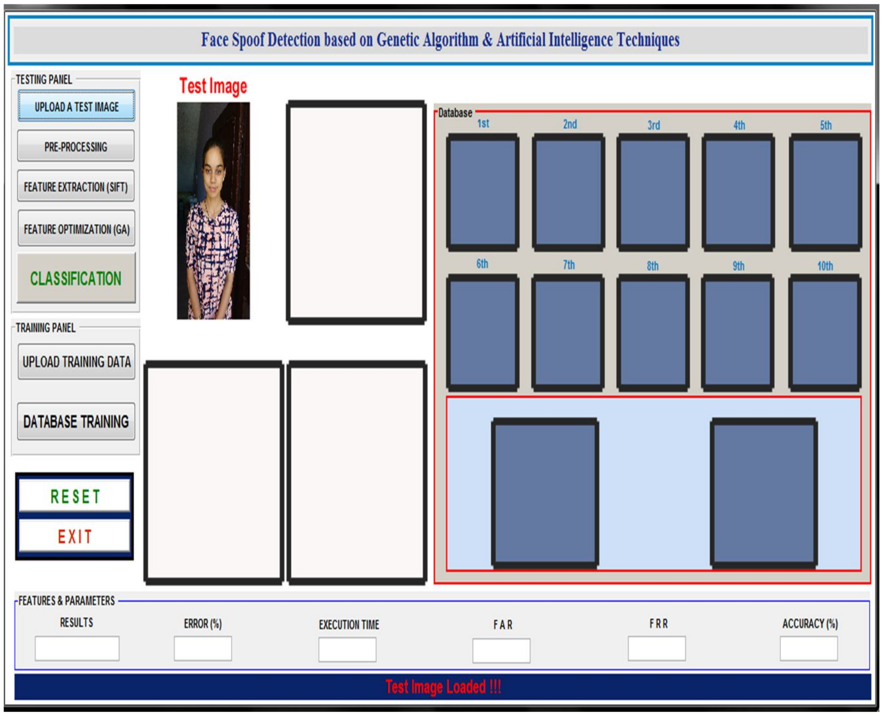


Fig. **Error! No text of specified style in document.** Working Window of Proposed Work

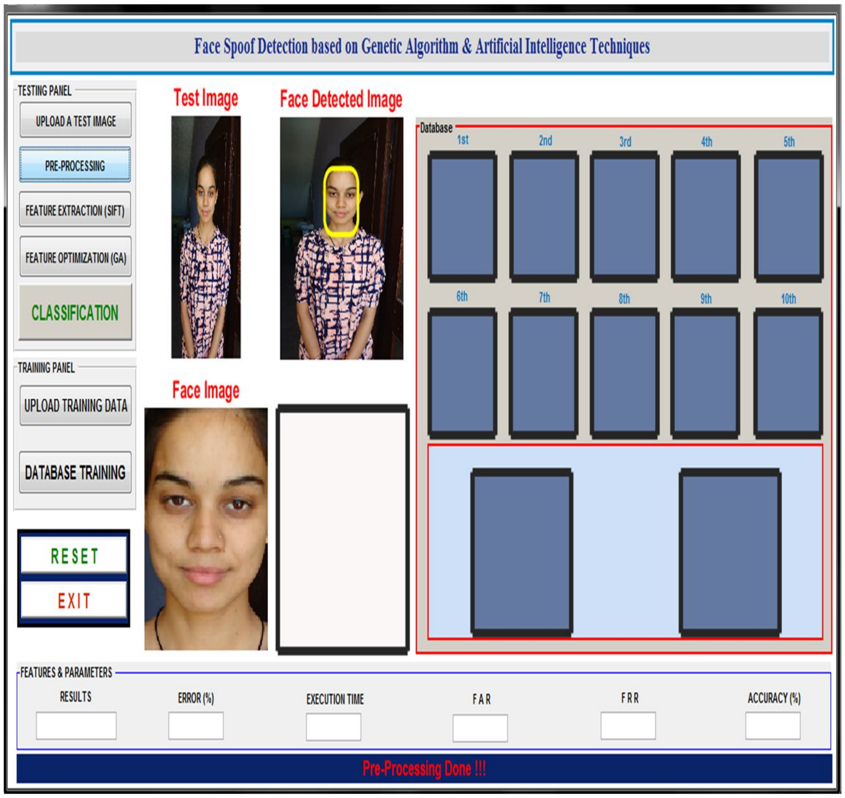
Working window of the proposed work comprises of two panels, testing panel and Training panel. In the training panel, database of face images is uploaded for training purpose. Training is done by using hybrid algorithms named as genetic algorithm (GA) and artificial neural network (ANN). ANN classifies the extracted features obtained from SIFT descriptor. Then, output of SIFT has been provided as input to the ANN classifier as input. By using two hybridization techniques, the accuracy of the system has been increased which is well described in the results section.



Test Image Loaded !!!

Fig. 6 Testing of Proposed Work

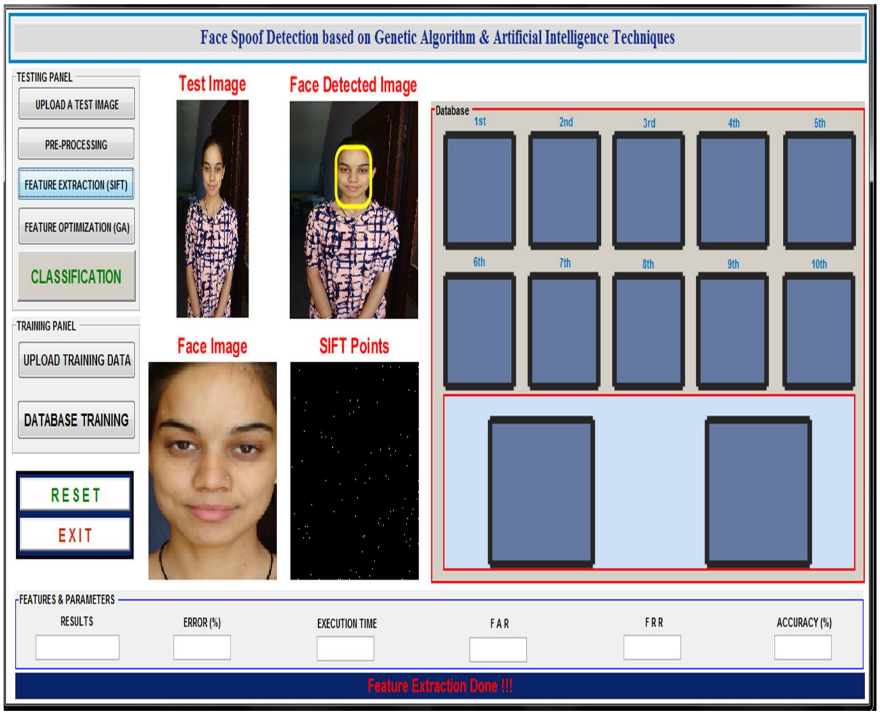
Under the testing panel, there is a button of upload test data, when we click on it, the test image has been uploaded as shown above. In testing panel, various processes have been carried out for detection of spoof face that is pre-processing, feature extraction, feature optimization and classification. All these techniques are explained one by one in methodology section as well as in below section.



Pre-Processing Done !!!

Fig. 7 Face detection in Proposed Work

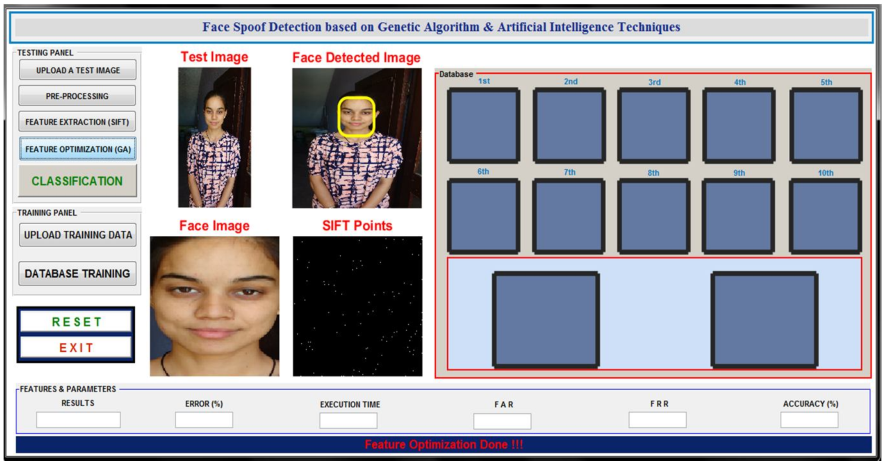
Above figure has shown the detected face region from the entire image. Detected face region is called as region of interest (ROI). Detected ROI is used as an input data of SIFT descriptor to extract the pattern of feature.



Feature Extraction Done !!!

Fig. 8 SIFT feature of Face Image

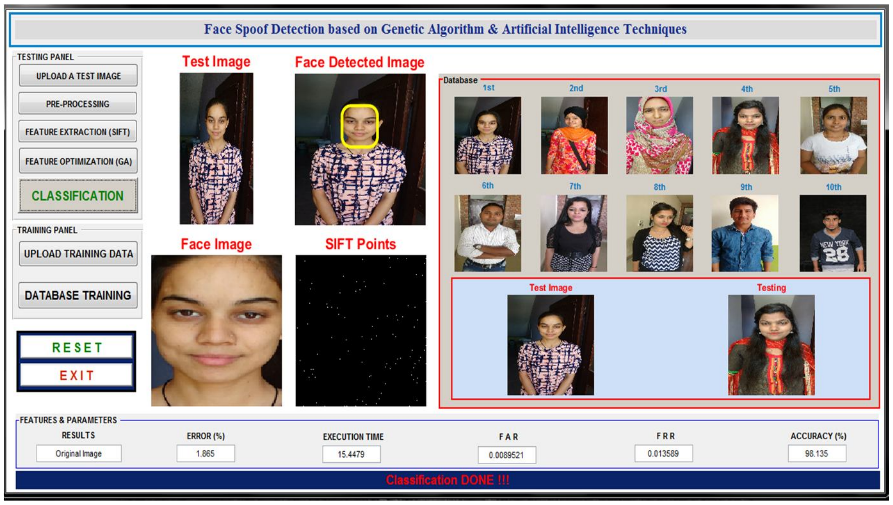
Extracted SIFT Features of the uploaded face image is shown above figure in the form of key points. In the feature extraction technique, SIFT descriptor is used for the extraction of key points and it is denoted by the white spots in the image of 'SIFT Points'.



Feature Optimization Done !!!

Fig. 9 Feature Optimization using Genetic Algorithm

After the feature extraction, we need to create a unique feature set according to the data categories. So, we have used genetic algorithm as an feature optimization technique to separate the unique feature and design a normalize feature set for each categories of face data.



RESULTS	ERROR (%)	EXECUTION TIME	F A R	F R R	ACCURACY (%)
Original Image	1.865	15.4479	0.0089521	0.013589	98.135

Classification DONE !!!

Fig. 10 Classification of Proposed Work

After the feature optimization, we have classified the test image on the basis of training of proposed spoof detection system. After the classification, we have calculated the performance parameters of proposed work in terms of FAR, FRR, Error rate, Execution time and Accuracy.

TABLE 2 PERFORMANCE PARAMETERS

S No.	FAR	FRR	Error (%)	Accuracy (%)	Execution Time (s)
1	89.52	53.58	1.87	98.13	15.45
2	91.36	29.83	1.66	98.34	12.78
3	83.26	45.82	2.08	97.92	14.76
4	87.36	67.27	1.28	98.72	12.74
5	93.27	38.74	2.72	97.28	11.87
6	74.72	34.79	2.28	97.72	09.34
7	78.37	67.62	1.73	98.27	17.38
8	84.28	72.42	3.62	96.38	16.88
9	87.82	55.53	2.92	97.08	13.73
10	82.73	67.34	1.19	98.81	12.48

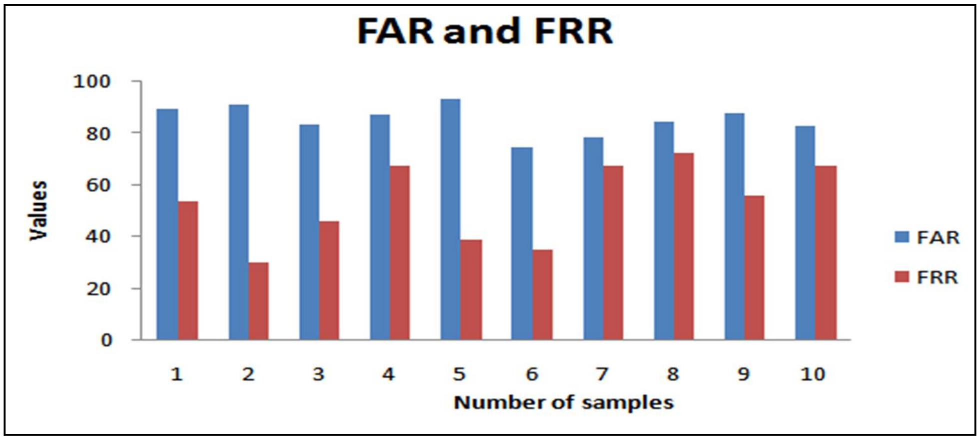


Fig. 11 FAR and FRR

Above figure describes the result of FAR and FRR after simulation. X-axis in the figure defines the number of samples and Y-axis defines the values obtained of FAR and FRR after simulation. Blue bar defines the result of FAR and red bar defines the result of FRR. The average value of FAR is 85.26 and the average value of FRR is 53.29.

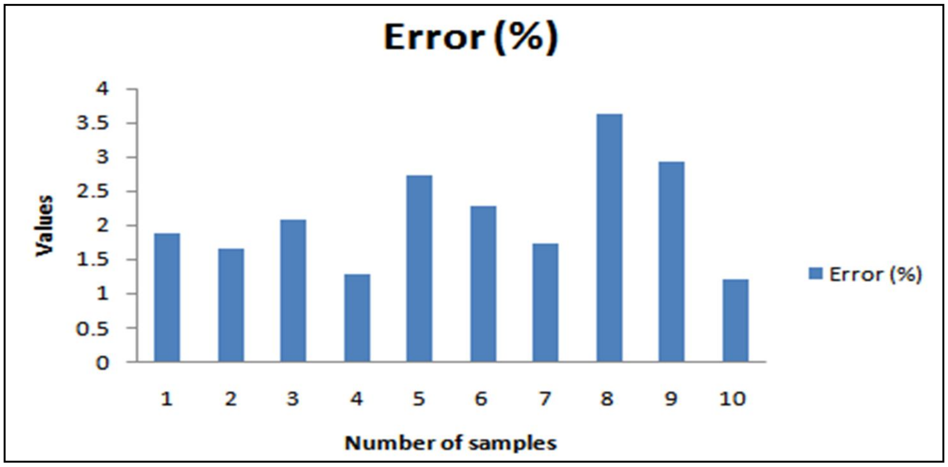


Fig. 12 Error

Above figure depicts the amount of errors in the proposed work X-axis in the figure defines the number of samples taken to execute the work and Y-axis defines the values obtained for Error. The presence of error in the work is 2.13% approximately.

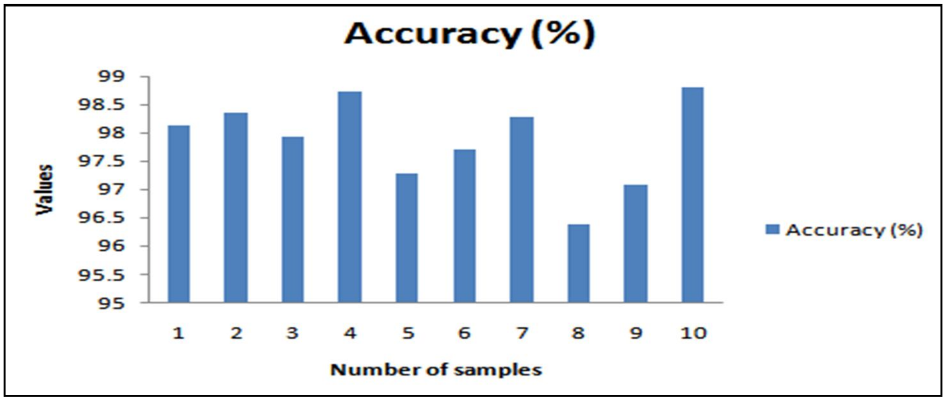


Fig. 13 Accuracy

Above figure describes the result of Accuracy after simulation. X-axis in the figure defines the number of samples and Y-axis defines the values obtained of FAR and FRR after simulation. The average value of accuracy is 97.86.

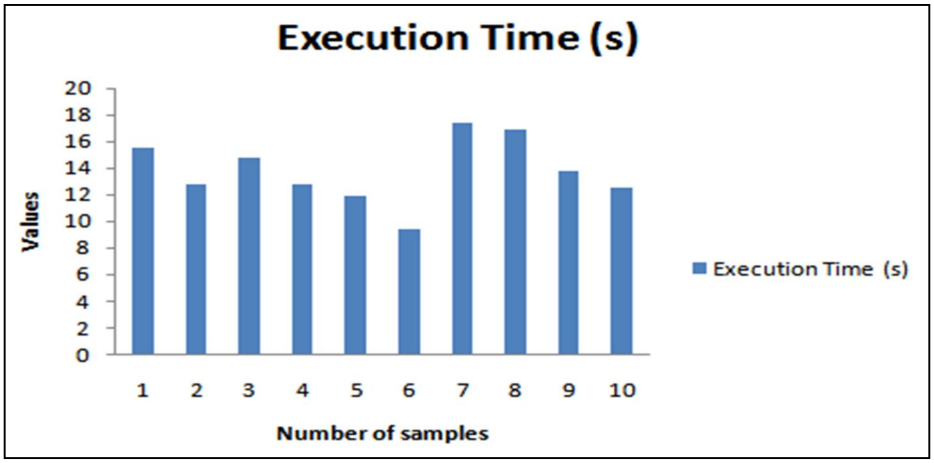


Fig. 14 Execution time

Above figure describes the result of execution time after simulation. X-axis in the figure defines the number of samples and Y-axis defines the values obtained for execution time after simulation. The average value of accuracy is 13.741 approximately.

IV. CONCLUSION

In this research, we have proposed a spoof detection system using genetic algorithm and artificial neural network. For the feature extractions SIFT descriptor is used and once the face images are translated into a proper feature space, there are some disparities between the original and spoofed images that may become evident. In this framework, it is assumed that spoofing induces some distortions in the image and the image quality properties of real accesses and fraudulent attacks will be different. Artificial neural network classifier consists of optimized key points that have been trained for different spoof face and real face. Proposed solution has suggested an effective and efficient method against spoof detection. The proposed approach has also shown increment in the detection rate as compared to the existing systems by using the concept of hybridization of genetic algorithm and artificial neural netw The future works include devising more novel techniques for attaining discriminative image patches and inclusion of temporal information in the proposed method for higher security applications in spoof detection system. It is possible by the using of some important pre-processing steps in the training and classification phases.

REFERENCES

[1] Kumar, S., Singh, S., & Kumar, J. (2017). A Comparative Study on Face Spoofing Attacks. In IEEE International Conference on Computing, Communication and Automation (ICCCA), 5th-6th May.
[2] Song, X., Zhao, X., & Lin, T. (2018). Face spoofing detection by fusing binocular depth and spatial pyramid coding micro-texture features. arXiv preprint arXiv:1803.04722.
[3] Farmanbar, M., & Toygar, Ö. (2017). Spoof detection on face and palmprint biometrics. Signal, Image and Video Processing, 11(7), 1253-1260.
[4] Kaur, R., & Mann, P. S. (2017). Techniques of Face Spoof Detection: A Review. International Journal of Computer Applications, 164(1).
[5] Bhattacharjee, S., Mohammadi, A., & Marcel, S. (2017). Spoofing Deep Face Recognition with Custom Flexible Masks(No. EPFL-REPORT-233563). Idiap.
[6] Dengale, R. R., Deshmukh, B. S., Mahangade, A. R., & Ujjainkar, S. V. (2017). A Face Recognition and Spoofing Detection Adapted to Visually-Impaired People. International Journal of Engineering Science, 6051.
[7] Bhat, K., Chauhan, S., Benure, G., Ambekar, P., & Salunke, S. (2017). Prevention of Spoofing Attacks in Face Recognition System Using Liveness Detection.
[8] Fourati, E., Elloumi, W., & Chetouani, A. (2017, August). Face anti-spoofing with image quality assessment. In Bio-engineering for Smart Technologies (BioSMART), 2017 2nd International Conference on (pp. 1-4). IEEE.
[9] Padma, p., & shivaji, r. (2017). Identification of face and spoofing for impaired people in the visualization. Ijitr, 5(6), 7451-7453.
[10] Zhang, B. (2017). Distributed SVM face recognition based on Hadoop. Cluster Computing, 1-8.
[11] Wang, M., & Deng, W. (2018). Deep Face Recognition: A Survey. arXiv preprint arXiv:1804.06655.
[12] Adejoke, E. J., & Samuel, I. T. (2017). Face Recognition Enabled Codded Eye-Blink Sign Communication for Triggering Security Alert. IJCSIS.
[13] Dhawanpatil, T., & Joglekar, B. (2018). A Review Spoof Face Recognition Using LBP Descriptor. In Proceedings of First International Conference on Smart System, Innovations and Computing (pp. 661-668). Springer, Singapore.
[14] Modak, S. K. S., & Jha, V. K. (2017). Feature level Fusion of Face and Hand for Multibiometric Based Personal Identification.
[15] Fatt, W. K., Kushsairy, A. K., Nasir, H., Safie, S. I., & Noor, N. M. (2017). Fingerprint and Face Recognition: Application to Multimodal Biometrics System. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(2-2), 81-85.