Normalized Feature Extraction and Selection Procedure for Facial Anti-Spoofing Detection

Sheetal sharma[1], Rasneet kaur[2]
[1]*Research Scholar,* [2]*Assistant professor*
[12]*Department of Computer Science Engineering,*
[12]*Shaheed udham Singh college of engineering and technology*

Abstract- Spoofing is the method of the Face detection of the various attacks. In the face recognition system, vulnerabilities to face spoof attacks create a major impact in the systems. In the typical spoofing the biometric conditions include face, fingerprint, iris, and voice and pattern recognition. The number of the approaches has been recognised in the face recognition and face spoofing. The information is evaluated in the spoofing detection in extraction and distortion of the data. The wide applications used in the face spoofing are biometric, mobile services, authentication solutions, fingerprints and patterns. However, the recognition of face spoofing is still a challenging issue due to the problems in judgment of the discriminative and computationally inexpensive features. It is necessary to develop a robust and an efficient method which can be detected the spoofing in a well general manner with specific imaging conditions. In these existing studies, the different applications used are both the spatial and temporal data for the detection of the face spoofing. The other techniques used in this research are generalisation methods where difference distances are reduced using the various domains. In the proposed work, various algorithms are developed which are categorised as SIFT (Scale Variant Feature Transform), PSO (Particle Swarm Optimisation) and BPNN (Back Propagation Neural Network). Implementation work, extract the features which is unique properties and selection of feature based on nature inspiring algorithm. After that classification methods implement to classify the selected and extracted features in knowledge base and validate the performance metrics. In the experimental tool used for research is MATLAB 2016a and compute parameters like accuracy and error rate. In research work, to enhance the accuracy rate achieved value is 98% with PSO and BPNN and minimizes the EER value is 0.6339.

Keywords- Face detection, spoofing, recognition phase, BPNN, PSOA and SIFT feature transformation.

I. INTRODUCTION

Spoofing is unauthorised access to system of a user by pretending it to be in use. A spoofing attack is an attempt to use privileges of other user by using a photo, video for authorised face of a person. Along with face recognition, texture plays vital role in detection of face spoofing. In anti-spoofing technique the texture features extracted from images in order to detect the fake face. The local binary pattern is used to detect the texture image [1]. Anti-spoofing is method used to distinguish between authentic user and fake trait. The measures against spoofing can be classified into several categories such as texture based analysis and reflectance based analysis [2]. Face Spoofing is the method of the detection of the various attacks. In the face recognition system, vulnerabilities to face spoof attacks create a major impact in the systems [3]. The spoofing detection based on the different methods recognized through the biometric systems [4]. With the developing fame of using face recognition for access control, the face spoofing has become a common method of the face recognition. The figure describes the classification of the face spoofing. The face spoofing based on the various categories which are 2D image spoofing and 3D image spoofing such as Photo attack, Video Attack and Mask Attacks.

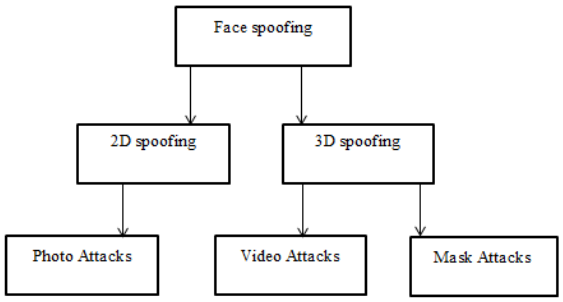

Fig.1: Classification in Face Spoofing Attacks [4]

In existing research work, uses the ordinary LBP feature descriptor along with CNN classifier, which can be further improved by using the improved LBP feature descriptor. The improved LBP feature descriptor option can be Diamond sampling structure based Local Adaptive Binary Pattern (DLABP) model, learned from another scheme designed to recognize the texture for the texture classification. Also, the performance of face spoofing detection models using CNN is observed lower for the CASIA dataset in comparison with NUAA dataset in another study. The CASIA face spoofing dataset contains the higher order to variability than NUAA dataset, which challenges the face spoofing detection schemes. Hence, the focus of this research can be kept on to the CASIA dataset along with NUAA dataset.

In research proposed method has implemented using SIFT, BPNN and PSOA methods. **Feature Extraction:**The SIFT method effectively recognizes scale-space extrema paying little mind to examining issues [7]. This requires the extension of the technique to take into consideration varieties in the

majority of its parameters, to change it into a careful strategy. In that way it ends up conceivable to look at the definite technique (all the more unequivocally a firmly oversampled scale-space adaptation) to the first one, and to assess the culmination and security of the distinguished key points. The SIFT calculation has ended up being adequately scale-invariant to be utilized in various applications [9]. By and by, nonetheless, scale invariance might be debilitated by different wellsprings of mistake characteristic to the SIFT method influencing recognitions dependability and precision. The thickness of the examining of the Gaussian scale-space and the dimension of haze in the information picture are two of these sources [8]. **Feature Selection:**PSO is utilised to invent the flocking of the birds flying sequence and unexpected route modifications. The swarm associate is called as particle that acquire best outcome through normal intelligence method. Though, every particle moves along already existed location [11]. Particle Swarm Optimization is an evolutionary technique determine about the behaviour of the nature of strategies, programming, evolutionary algorithms and genetic programming. PSO is sociological process associated with bird flocking. PSO is evolutionary based algorithm with population of random solutions. The population of each particle represents a potential solution to an optimization problem is PSO algorithm. The random velocity and potential solutions for the evolutionary algorithm called as particles. The particles flow out through the problem space [5, 6].**Detection Phase:**The classification process using Back Propagation method is generally based on the learning approach. It is expensive and powerful kind of approach in form of the calculation required for the training purpose. The network with unique group of the hidden layer consists of the processing components which can classify the regular functional data to some degree of the exactness having required amount of the components in the hidden layer. Back propagation approach is the method of supervised learning approach used in multilayer neural network and is also called as generalised method rule [10].

Section I: define about the introduction using Face spoofing, classification methods and attacks. Existing issues define in face spoofing detection and proposed method used to resolve the issues comes under the face spoofing detection and improve the performance metrics and compared it. Section II describes literature review with various methods. Section III and IV define research proposal and Result analysis and V section shows conclusion and future work.

II. RELATED WORK

Komulainen, J., Hadid, A and Pietikäinen, M. et al., 2012[12] presented a monitoring behaviour of the utilisation of the texture for the detection of face spoofing. The three dimensional masks , real face were required instead of the facial muscles that leads to temporary deformed facial characteristics like as eyes, lips and so forth. The main goal of the research was organisation and appearances of the actual face of face micro-texture that determines the real face. However, they introduced a new method of face spoofing detection using dynamic structure with local binary method. Experimental analysis was done using required dataset which contains various fake face threats of different features under different circumstances.**Mei, L., Yang, D., Feng, Z and Lai, J et al., 2015[13]** proposed research on different algorithms that depends on different on picture descriptors which were applied for the detection of the face against face spoofing threats like as LBP and LBP-TOP. Hence, picture descriptors were not robust to spoofing threats. In this research, they proposed robust and influential energy descriptor known as WLD-TOP. It links temporal and spatial data into single descriptor with multiple resolution method. Experimental analysis was done using CASIA and SYSU-MFSD dataset which describes that the descriptor can attain better liveness detection in both internal and cross dataset as compared to state ofart method that depends on descriptors.**Y.Binny Reeba et al., 2015 [14]**implemented face spoofing detection system for the detection of the facial masks. The algorithm utilised for standard face detection algorithm was dependent on the functions of the face detection and anti-spoofing. A detection technique was demonstrated for recognition of the two dimensional pictures using SURF features of the picture. The real face and the mask is differentiated where anti spoofing is analysed through extraction of the LBP features. In addition , histogram of LBP features were trained through support vector machine to recognise of internal data will be retrieved or not. The classification was done using support vector machine to improve the accuracy rate.This research was determined by detecting modified faces due to surgery and the detection of the face masks. **Qi, W. S., Ding, H. M., Wang, Y. B and Xie, Z. F. et al., 2018[15]**evaluated the intra test (training and testing dataset) using convolutional neural network.Inappropriately, when method fails to detect the unidentified threats training was done on one dataset and evaluation on other dataset. The main concern about the face anti spoofing was mainly unnoticed. Experimental analysis was done using face spoofing database, CASIA and replay threats, and described the version capability for convolution neural network from one database to other database. The visualisation of the implicit consideration of CNN and they found scene dependent features removed by CNN that effects the methods abilities. To remove this issue, they proposed a new outcome that depends on relating scene independent structuresdemonstration.**Yadav, M. and Gupta, K et al., 2018[16]** classified the spoofed as well as non-spoofed pictures and proposed a face spoofing detection method. The textual features was analysed in the test picture using DWT approach. The classification of support vector machine was used to classify features of spoofed and non-spoofed face. Hence, proposed method enhanced the accuracy to improve the spoofed face. The proposed method analysed the comparison between planned and existing method in form of the accuracy and time of execution.

III. RESEARCH PROPOSAL

This research work consists of a set of objectives that is associated with milestone of this process. The main objectives

are; (i) Collect the dataset from the UCI Machine Learning sites (NUAA Dataset) in Face Spoofing and development methods. (ii) Develop a pre-processing steps and extract the features of the dataset using SIFT algorithm. (iii) Implement a nature inspiring with BPNN algorithm to detect the spoofing face in the given datasets.

Initial Phase to create Knowledge based which is called as training set. Upload the image from the dataset. Uploaded image is a color image and converts the RGB to Gray scale format. The grayscale method to reduce the image dimensionality size wise. To identification method used to noise detection in the uploaded images. After that filtration method has implemented to remove the noisy information in the facial image. Filter image has implemented using SIFT algorithm. SIFT algorithm extracts the features in the form of KPD (Key Point Descriptor). SIFT [17] algorithm extracts the unique properties in the facial image. Selection phase has implemented a PSO [18] algorithm to select the feature based on the fitness function. In FFn calculates the best solution values in the face images. Classification phase has applied in the face images and detect the spoof face images based on the BPNN method. In BPNN methods are three layers such as;

(i) Input Layer
(ii) Hidden Layer and
(iii) Output Layer

Input layer process the input features accordingly to the layer division. Hidden layer process the features and in-built feature validate and output layer to check and validate the spoofed face properties based on the activation function. After that detection phase, evaluate the performance metrics such as accuracy rate and reduce the error rate and compared with the existing methods.

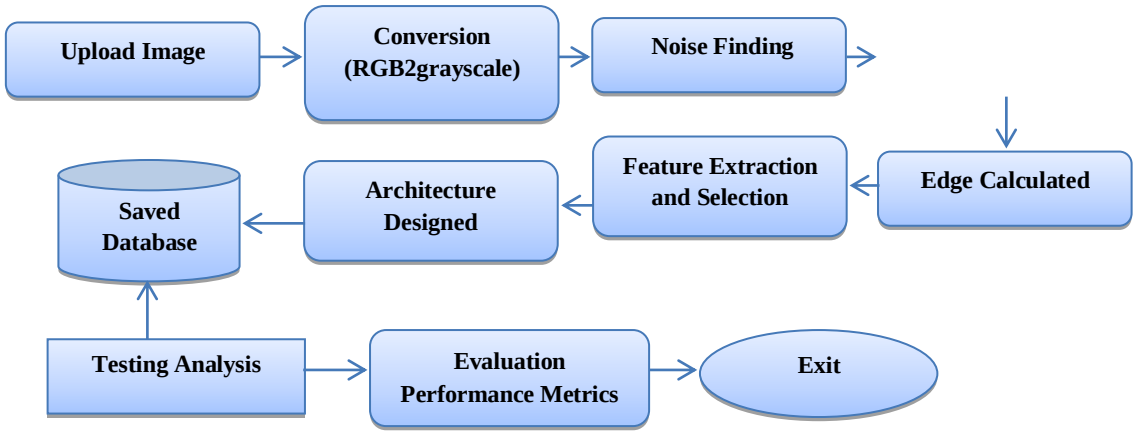

Fig.2: Research Proposal Work

IV. RESULT ANALYSIS

The image NUAA dataset is gathered by various web cameras from electric market. The dataset is gathered from three methods in interval of two weeks among two sessions and situation of every session is varied. Every session catches the picture of both live subject and images that is numbered from 1to 15 subjects. The sample pictures from three sessions of the dataset. The real human data placed at left and images are placed at right. There will be modifications in the appearance of the detection system. Every picture in the dataset is colored image with similar pixels. Every session use web camera for catching sequence of the data pictures. Every subject sees neutral expressions during picture capturing. In this manner human looks like an image [18].

Fig.3: (i) Real facial Images and (ii) Fake facial Images [19]

The graphical user interface which is considered by MATLAB 2016a used and supports the GUI. In this phase create the knowledge based on real images and duplicate images. Knowledge based learn the unique properties and understand, all features which is extracting by SIFT feature extraction and architecture procedure the layers by BPNN method. BPNN method to search the face classes real and duplicate or fake images in the internal machine.

1. Upload face image
2. Conversion
3. Noise checking
4. Filtration
5. Feature Extraction and Selection

6. Classification and detection
7. Performance metrics
8. Comparative Analysis
9. Stop.

Fig.4: (i) Test Facial Image (ii) Gray scale Image (iii) Noise test Image (iv) Filter Image and (v) Edge Detection Image

Here figure 4(i) shows upload the test image from the test database which is color image. Figure 4 (ii) gray scale image means converts the color image to gray scale image and reduce the size of the image. Fig 4(iii) shows the noisy data check in the grayscale image. Fig 4 (iv) shows the noise free image using 2D- Transformation method and Fig 4 (v) defines the edge detection methods to extract the region points and edges in the smooth image.

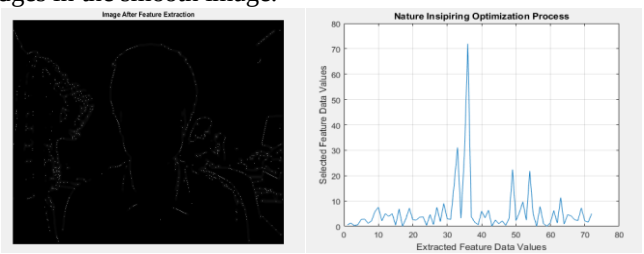

Fig.5: (i) Feature Extraction (SIFT) and (ii) Feature Selection (PSOA)

Here fig 5(i) shows the feature extraction in the form of Keypoints. SIFT method effectively recognizes scale-space extrema paying little mind to examining issues. This requires the extension of the technique to take into consideration varieties in the majority of its parameters, to change it into a careful strategy. In that way it ends up conceivable to look at the definite technique (all the more unequivocally a firmly oversampled scale-space adaptation) to the first one, and to assess the culmination and security of the distinguished key points. Fig 5(ii) defines the feature extraction using particle swarm optimization. It selects the value of the features in the face spoofing in the digital images.

Fig.6: (i) Neural Network

Here figure 6 shows the BPNN architecture performs the training and testing phase. In this architecture shows the feature data into different layers. All features are divided into different-2 layer passed. Defines the number of iterations 7 processed out of 100 iterations. It calculates the time; performance based on error rate, gradient, mutation and validation checks.

Table 1: Performance Parameters

Parameters	**Values**
Accuracy Rate	98%
EER	0.6113
FAR	0.0058
FRR	0.0061
HTER	0.3887

Here Table 1 show the performance based BPNN with PSOA method. This is a proposed module it is designing to detect the face such as two categories real or Fake. In this proposed method performance is accuracy rate is high 98 %, Error Rate value is reduces 0.6113.

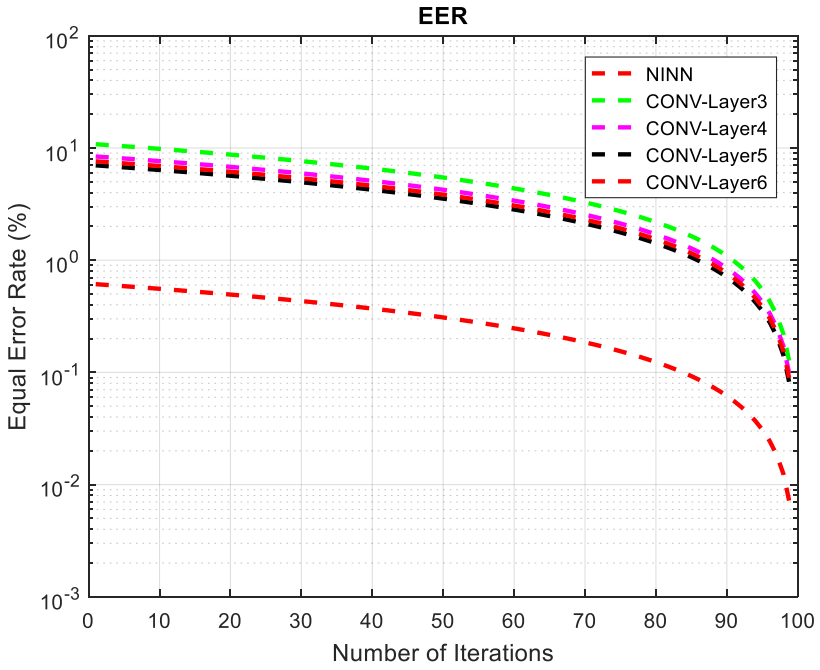

Fig.7: Comparison - EER

Here fig 7 shows that the comparison performance analysis with various METHODS such as NINN and different CONV layers. The Comparison Analysis the performance of the proposed BPNN and PSOA method and CNN Classifier Technique which is existing technique. In PSO + BPNN classifier work smartly and fetch the data with knowledge base. Improve the performance metrics with accuracy rate (%), Error rates as compared to previous one.

Table 2. Comparison Parameters

Parameters	Cov_layer3	Cov_layer4	Cov_layer5	Cov_layer6	PSOA+BPNN
EER	10.80	8.4	7	7.6	0.6113

Table 2 shows the comparison between proposed and existing methods with Cov_layer3,cov_layer4, cov_layer5, cov_layer6 and proposed method PSOA+BPNN is reduced the error rates.

V. CONCLUSION AND FUTURE SCOPE

In this research concluded defined the various methods used in face spoofing detection system. An extended deep learning model (n-LBPnet) with LBP to determine the face spoofing in the face recognition applications. The existing model is evaluated on NUAA database, and is observed with highest equal error rate (EER), accuracy rate (Acc), half-total error rate (HTER) and false rejection rate (FRR). On the contrary, area under curve (AUC) and false acceptance rate (FAR) are observed lower than existing model, which shows the points of improvement. The AUC of existing model is 0.996 against CDD model's 0.998, which shows the significant difference for improvement. Similarly, the FAR (0.019) is observed significantly lower than MLBP (0.006), which shows the underperformance of existing model. The existing model uses the ordinary LBP feature descriptor along with CNN classifier, which can be further improved by using the improved LBP feature descriptor. The improved LBP feature descriptor option can be Diamond sampling structure based Local Adaptive Binary Pattern (DLABP) model, learned from another scheme designed to recognize the texture for the texture classification. Also, the performance of face spoofing detection models using CNN is observed lower for the CASIA dataset in comparison with NUAA dataset in another study. The Implementation work concluded, extract the features which are unique properties and selection of feature based on nature inspiring algorithm. After that classification methods implement to classify the selected and extracted features in knowledge base and validate the performance metrics. In the experimental tool used for research is MATLAB 2016a and compute parameters like accuracy and error rate. In research work, to enhance the accuracy rate value is 98% with PSO and BPNN and minimize the error rate value is 0.6113.

It can implement optimization methods to enhance the feature quality parameters. Secondly, it can implement an encryption method to improve the security rate and time complexity in face spoofing detection system.

VI. REFERENCES

[1]. de Souza, G. B., da Silva Santos, D. F., Pires, R. G., Marana, A. N., and Papa, J. P. (2017), " Deep texture features for robust face spoofing detection",. IEEE Transactions on Circuits and Systems II: Express Briefs, vol 64(12),pp. 1397-1401.

[2]. Aziz, A. Z. A. and Wei, H. (2018), "Polarization Imaging for Face Spoofing Detection: Identification of Black Ethnical Group" , In 2018 International Conference on Computational

Approach in Smart Systems Design and Applications (ICASSDA) ,vol 2(1), pp. 1-6, IEEE.

[3]. Chakka, M. M., Anjos, A., Marcel, S., Tronci, R., Muntoni, D., Fadda, G. and Roli, F. (2011, October), " Competition on counter measures to 2-d facial spoofing attacks", In 2011 International Joint Conference on Biometrics (IJCB) ,vol. 3(2) ,pp. 1-6.IEEE.

[4]. Nixon, K. A., Aimale, V and Rowe, R. K. (2008), "Spoof detection schemes" , In Handbook of biometrics ,vol. 2(1), pp. 403-423, Springer, Boston, MA.

[5]. Määttä, J., Hadid, A., & Pietikäinen, M. (2012, " Face spoofing detection from single images using texture and local shape analysis", IET biometrics, vol. 1(1),pp. 3-10.

[6]. Maturana, D and Scherer, S. (2015), " Voxnet: A 3d convolutional neural network for real-time object recognition", In 2015 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS) ,vol3(2),pp. 922-928, IEEE.

[7]. Ji, S., Xu, W., Yang, M. and Yu, K. (2012)., "3D convolutional neural networks for human action recognition",. IEEE transactions on pattern analysis and machine intelligence, vol. 35(1), pp.221-231.

[8]. Zhou, X., Wang, K. and Fu, J. (2016), " A Method of SIFT Simplifying and Matching Algorithm Improvement" , In 2016 International Conference on Industrial Informatics-Computing Technology, Intelligent Technology, Industrial Information Integration (ICIICII) ,vol 2(1), pp. 73-77, IEEE.

[9]. Jindal, R. and Vatta, S. (2010). , "Sift: Scale invariant feature transform. IJARIIT,vol2(1),pp. 1-5.

[10]. Zhang, Q., Chen, Y., Zhang, Y and Xu, Y. (2008)., " SIFT implementation and optimization for multi-core systems" ,In 2008 IEEE International Symposium on Parallel and Distributed Processing ,vol3(2),pp. 1-8, IEEE.

[11]. Ojha, V. K., Dutta, P., Saha, H.and Ghosh, S. (2012), "Detection of proportion of different gas components present in manhole gas mixture using backpropagation neural network." ,International proceedings of computer science and information technology, vol.1, pp.11-15.

[12]. Hecht-Nielsen, R. (1992), " Theory of the back propagation neural network. ",In Neural networks for perception , vol 3(2), pp. 65-93,Academic Press.

[13]. Komulainen, J., Hadid, A., & Pietikäinen, M. (2012, November). Face spoofing detection using dynamic texture. In *Asian Conference on Computer Vision* (pp. 146-157). Springer, Berlin, Heidelberg.

[14]. Mei, L., Yang, D., Feng, Z., & Lai, J. (2015, November). WLD-TOP based algorithm against face spoofing attacks. In *Chinese Conference on Biometric Recognition* (pp. 135-142). Springer, Cham.

[15]. Y.Binny Reeba, SPOOFING FACE RECOGNITION , 2015 International Conference on Advanced Computing and Communication Systems (ICACCS -2015), Jan. 05 – 07, 2015, Coimbatore, INDIA

[16]. Qi, W. S., Ding, H. M., Wang, Y. B., & Xie, Z. F. (2018, July). Scene-Independent Feature Representation for Face Anti-Spoofing. In *2018 International Conference on Audio, Language and Image Processing (ICALIP)* (pp. 123-127). IEEE.

[17]. Yadav, M., & Gupta, K. (2018, June). Novel Technique for Face Spoof Detection in Image Processing. In *2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1989-1992). IEEE.

[18]. Yousefi, M., Omid, M., Rafiee, S and Ghaderi, S. (2013), " Strategic planning for minimizing CO2 emissions using LP model based on forecasted energy demand by PSO Algorithm and ANN., J Homepage www. IJEE. IEEFoundation. org, vol 4(6),pp 1041-1052.

[19]. X.Tan, Y.Li, J.Liu and L.Jiang. Face Liveness Detection from A Single Image with Sparse Low Rank Bilinear Discriminative Model, In: Proceedings of 11th European Conference on Computer Vision (ECCV'10), Crete, Greece. September 2010.

[20]. NUAA Imposter Database. (2019). Retrieved from http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html.