International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Face Spoofing Detection using Enhanced Local Binary Pattern

Karuna Grover, Rajesh Mehra

Abstract: -Among various biometric systems, over the past few years identifying the face patterns has become the centre of attraction, owing to this, a substantial improvement has been made in this area. However, the security of such systems may be a crucial issue since it is proved in many studies that face identification systems are susceptible to various attacks, out of which spoofing attacks are one of them. Spoofing is defined as the capability of making fool of a system that is biometric for finding out the unauthorised customers as an actual one by the various ways of representing version of synthetic forged of the original biometric trait to the sensing objects. In order to guard face spoofing, several anti-spoofing methods are developed to do liveliness detection. Various techniquesfordetection of spoofing make the use of LBP i.e. local binary patterns that make the difference to symbolise handcrafted texture features from images, whereas, recent researches have shown that deep features are more robust in comparison to the former one. In this paper, a proper countermeasure in opposite to attacks that are on face spoofing are relied on CNN i.e. Convolutional Neural Network. In this novel approach, deep texture features from images are extracted by integrating the modified version of LBP descriptor (Gene LBP net) to a CNN. Experimental results are obtained on NUAA spoofing database which defines that these deep neural network surpass most of the state-of-the-art techniques, showing good outcomes in context to finding out the criminal attacks.

Index Terms- Biometric, Convolutional Neural Networks, Face recognition, Spoofing attacks.

I. INTRODUCTION

These days, biometric identification systems are getting famous in many applicationsand the reason behind is that they are difficult to steal, accuracy rate is high, and can beeasily used by customers [1]. These methodsare based on the variations in particular physical or behavioural characteristics ofindividuals. With the advancementin technology, the susceptibility to fraudulent samplesbeing demonstrated during the image acquisition processinbiometric systems has become very common.

Face ID is the most generally utilized technique in applications, for example, PC/smart phone login, recognizable proof cards, and outskirt and identification control [2]. Appearance of the face is used in this biometric feature as a key to distinguish a person among group of individuals.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Karuna Grover, Pursuing Master's degree, Electronics and Communication Engineering from National Institute of Technical Teacher's Training and Research, Chandigarh, India
Dr. Rajesh Mehra, Head of Curriculum Development Center National Institute of Technical Teacher Training & Research, Chandigarh, India.

Though it has variousdisadvantages, including variations in illumination and head pose, still it can be utilized with other biometric characteristicslikefingerprints, finger-veins, palm-veins, etcetera to guarantee the high accuracy rate of recognition systems. Various components of a face recognition process are shown in Fig. 1 [3]. Firstly, to capture the image of users, theymustexhibit their faces in front of capturing devices. In this manner, the face restriction and highlight extraction steps are performed to separate picture highlights from the info face picture. At long last, a matchingalgorithm is performed to perceive the approved client in the information picture.

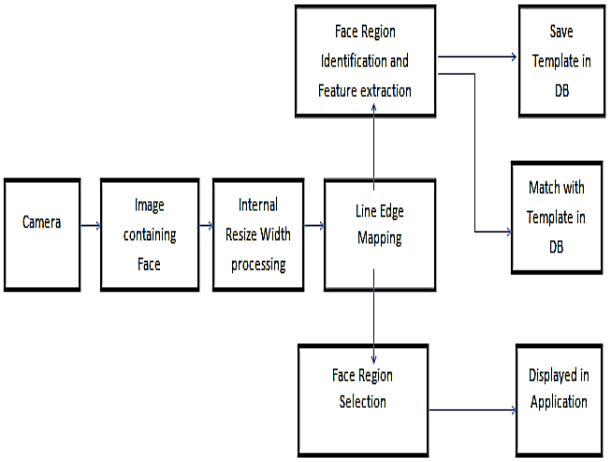

Fig. 1Components of Face Recognition System

However, a face recognition system can be attacked by various means such as (a) printed photos, (b) displayed image or motion video; (c) plastic surgery; (d) sketch; (e) make-up and accessory wearing; (f)3D mask; or (h) synthetic photograph or video, generated using computer graphics. To take care of this issue, the presentation attack detection (PAD) strategies have been looked into for such systems. Past investigations are ordered into two classes of feature extraction methods, training-based and non-training-based [2], [3].

The vast majority of the recently proposed PAD strategies for face identification systems have concentrated on utilizing handcrafted image characteristics [4]. Some of them are local binary pattern (LBP), local ternary pattern (LTP), Gabor filter and histogram of oriented gradients (HOG). Therefore, the detection accuracy it yields is less due to the reflection ofconstrained aspects of the issue by the extracted features of image. Also, itdiffers with the qualities of presentation attack face images [4].

To overcome the limitations of previously proposed PAD methods, there is scope to design new method to get better accuracy and these systems from such types of attacks [5], [6]. Apart from the good results of LBP, its amalgamation with CNNs can be proved productive as these networks are well known for the complex patterns that cannot be easily detected [1], [7].

The remainder of the paper is organized as follows: Section II briefly reviews the conventional methods for face spoofing detection along with the introduction to convolutional neural networks. Section III presents the proposed countermeasure in which modified LBP is employed with CNN. An experimental evaluation of the projected method is discussed in Section IV. Finally, concluding remarks are given in Section V.

II. RELATED WORK

A. Different types offeature descriptors

Face spoofing detection can be done by various ways, using different descriptors. Some of the descriptors based on global approaches are described as:-

1. Local Binary Pattern (LBP)
2. Gabor Filter
3. LDA (Local Descriptor Analysis)
4. PCA (Principle Component Analysis)

Table I depicts the comparative analysis ofthe above mentioned image feature descriptors along with their benefits and limitations.

Considering the various descriptors, LBP is used here to extract the texture information.Local binary pattern (LBP) is significantly intended for analysis and description oftexture of images [8]. It is for the most part utilized on account of its fantastic light invariance property and low computational unpredictability [8], [9]. The major aspect of working of LBP operator is a 3 x 3 pixel matrix. In this matrix, center pixel is considered as threshold and is surrounded by eight neighbours. Being threshold value, center pixel allows its surrounding pixels to bemarked as 1 or 0, former value if their gray value is higher or equal than center pixel, otherwisethey are given latter value.At last, a code is obtained whose decimal equivalent is computed and placed at centerpixel. Fig. 2 delineates the LBP operator [10].

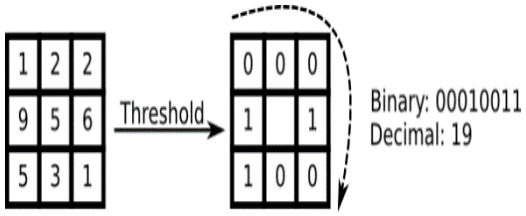

Fig. 2 Basic LBP operator

Binary code for an image pixel is provided by LBP which defines about the surrounding of that pixel. When the binary code of the pixel is produced, the comparison of gray value of the pixel is done with its neighbouring pixels [8], [11]. The intensity of the pixels is preserved in its neighbourhood by basic LBP operators as it is constant to monotonic gray-scale transformations [12].

Local binary patterns (LBP) is the well known example in which the pixel of an image is labelled by thresholdingthe neighborhood of each and every pixel which represents the local texture information with having the property of invariance to the monotonic grayscale transformation [12].

Usually,to perform the extraction of LBP histogram individually,division of an image can be done into several blocks. Also, with the help of bilinearly interpolating values at non-integer sampling points in its neighborhood, as vivid in (1), the LBP code of a pixel (xc;yc) is calculated for each block [13].

$$\mathrm{LBP}_{P,R}(x_c;y_c)=\sum_{i=0}^{p-1} g(p_i - p_c) \times 2^i \qquad (1)$$

where, the gray value of the pixel ($x_c;y_c$) is denoted by p_c and $p_i$definesthe gray value of the i^{th}pixel. Parameters of LBP are P,R , that denotes P sampling points on a clockwise circle of radius R for every pixel of neighborhood. Here, threshold function is referred as g(z) which gives output as 1 when z is non-negative; otherwise, 0. The existence of LBP codes are described by a histogram. For the training purpose the number of occurrences are applied as input vectors.

Table I: Comparison of various image feature descriptor

Feature Descriptor	Pros	Cons
PCA	The dimension of data is reduced, easy to use and learn the whole image of face taken into consideration.	Time required to find Eigen values is more so it is more time consuming. It is affected by lighting conditions.
LBP	Used in texture description, fast and efficient computation, moving objects by subtracting background of image.	Face localisation are not detected, large regions increase the error rate, can be used in binary and gray image only.
LDA	Identify individuals of same faces, grouped individual faces with same features ,lighting variations solved because it is used within class	More complex method, difference between classes affect within class.
GABOR FILTER	Captures spatial frequency, localisation, and orientation.	Sensitive to illumination changes.

B. Convolutional Neural Networks (CNN)

Convolutional Neural networks are considered as deep learning architectures which contain various layers where filters like convolution and sampling are employedas the input to two dimensional images data [1]. The final outcome of the initial layer is used as the input to the consecutive one till it reaches the top of the network. These type of networks give the simple topology in comparison to other fully connected networks.After the operation of convolution and sampling layers that are totally in contact can be indulged at the top for the classification[12]-[14].The layered network of CNN is revealed in Fig. 3.

Practically, for a two-dimensional image in each network layer,convolutional filter's are applied through which different channels of the original inputs are obtained.

Pooling which is also known as the sampling operations are done to get different kind of translational and scale invariance and decrease the quantity of data that is considered high level representation of original image is obtained at the top

of the network which is more robust then the raw pixels information for various applications [15].

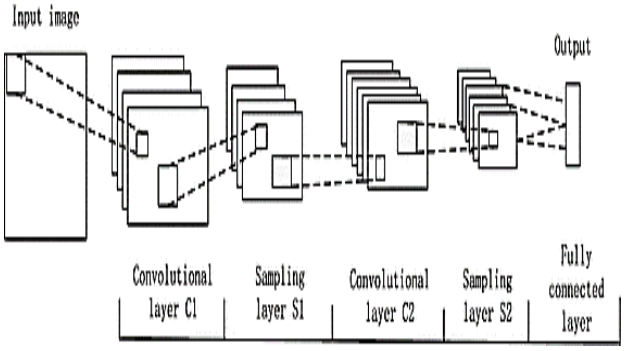

Fig. 3 Layers in Convolutional Neural Networks

C. LBP Based Convolutional Neural Network

Considering LBPnet network model as reference [1], a more robust architecture is proposed in which initially deep texture features are extracted using LBP which are later on classified using CNN for efficient face spoofing detection.

The initial step involves the convolution that is performed on the transformed LBP values of the image pixels, rather than their grayscale values.

The convolution operation is given in (2)

$$Ci(p) = \sum_{\forall q \in N(p)} LBP\big(I(q)\big).K_i(j) \qquad (2)$$

Where Ci (p)refers to the value in the output feature map C_i corresponding to position p, LBP (I(q)) is the LBP value of pixel q that belongs to the neighborhood of pixel p and K_i (j) is the value in i^{th} convolution kernel.

III. PROPOSED METHODOLOGY

The block diagram in Fig. 4 describes the flow of process followed in the experimental program for the evaluation of efficient face recognition. First of all, data acquisition of the training images is done. In this step, images from the given database are selected to be processed further. The training images here are referred as the knowledge base of the given dataset. This knowledge base consists of original as well as fake images. Moreover, the training images are 3D images in color format (RGB)which is basically a M*N*3 array of color pixel. On the other hand, a grayscale image can be viewed as a single layered image, that is, M*N array.

In the next step, RGB to gray scale conversion is seen. The reason behind this conversion is that in many morphological operations and image segmentation problems, it is easier to work with single layered image than a three-layered image. Notonly this, but it is more convenient to distinguish features of an image in former case.

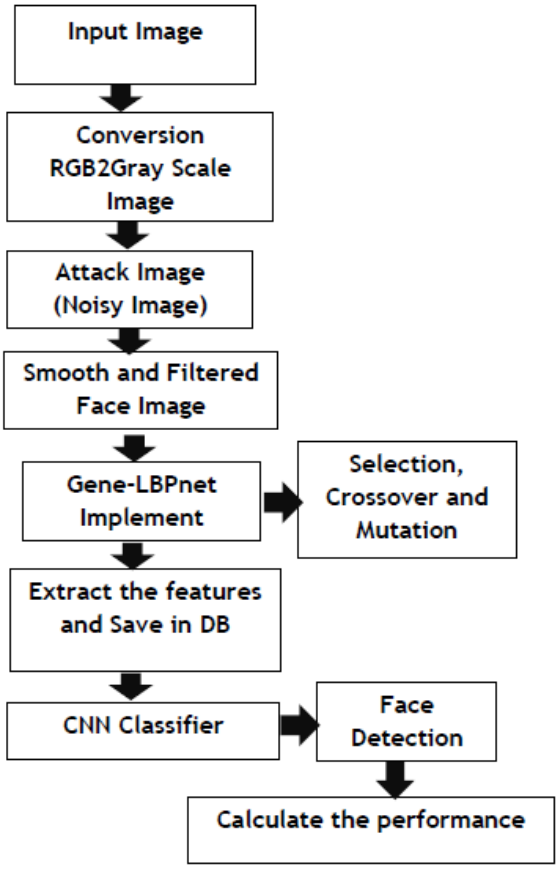

Fig. 4 Flow of process of proposed method

Further, it is revealed that distorted image is obtained which has salt and pepper type of noise. To incur filtered image an appropriate type of filter is used. To remove salt and pepper type of noise, generally, median filter is used. It is a non-linear digital filter that is used to optimize the interference from noisy images. The median filter works by moving through the image pixel by pixel, replacing each value with the median value of neighbouring pixels. The pattern of neighbours is called the “window”, which slides, pixel by pixel, over the entire image. This approach used for noise optimization is a normal pre-processing phase to enhance the consequences of later processing. The region of interest (ROI) of the filtered image is obtained by using prewitt methods. It is a Discrete Differentiation Operator (DDO) that computes the approximation of the gradient of the image intensity function.

The subsequentphase is to implement contrast limiting adaptive histogram equalization. Once the images are preprocessed, LBP (Local Binary Pattern)is performed separately to extract features of training images. The major texture descriptors, the real LBP with new advancement of Gene-LBP method is created to extract the feature and optimize the extracted feature with the help of three operators namely selection, crossover and mutation.These operators must work in conjunction with one another in order for the algorithm to be successful.

The above mentioned operatorswork to re-configure the extracted features and select the valuable features that depends on Fitness Values which are Binary values (0,1).

The histogram is constructed based on the gray scale values of LBP which further depends on image in order to define its real version.

After training, test images are selected and preprocessed in the same manner as that of training images. Then, the feature vectors of test images are also extracted. For classification, the feature vectors of training images, testing images and class label are transferred to CNN Classifierwhich is trained to calculate the class of novel face. It divides face image in patches and create an image histogram to each patch, which at the end are combined.

The final stage is face detection in which the classifier will distinguish between the "Real" or "Fake" face spoofing detection. Apart from this, various performance parameters are calculated to compare the results of the proposed method with various state of art spoofing detection techniques.

IV. EXPERIMENTAL RESULTS

A. Description of Dataset

The NUAA photo data base is collected using several webcams from an electronic market. The database is collected in three forms in an interval of two weeks between two sessions and the condition of every single session is different [11]. The 15 subjects that aregiven were numbered from 1 to 15 and every single session takes the images of together the subjects that are live with their photographs. The sample images from the three sessions are obtained from the database (Fig. 5). The left sidereveals the actual image of human whereas theright one is the photograph of the person. There will be alterations in appearance for the recognition system. Database contains all the colour images with the same value of pixels. Each subject from every session use webcams to capture series of data images.During image capturing, each subject see webcam with neutral expression. In this way live human looks like a photo [16].

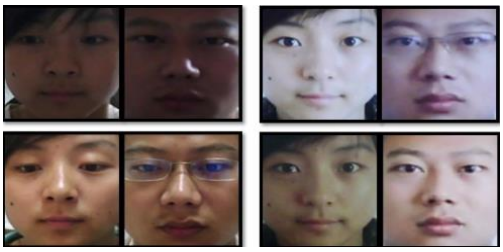

Fig. 5 Example of face image dataset

In order to collect the sample of the photo, highly defined photo for each subject use camera to take two by third of the overall region of the picture. There are different ways in which the photos are generated, firstly photos are printed on piece of paper with common size.

Fig. 6 Example of Dissimilar Attacks in Image Datasets [2]

Fig.6depicts examples of spoofing attacks with duplicate images of the persons whose original images are stored in database. It implies that if an intruder wants access to the authorised system, then using these dissimilar attacks it could have been possible. However, anti-spoofing techniques ensure that these attacks can be detected and corrected efficiently.

B. Testing Methodology

The figure below (Fig. 7) shows the steps involved in the testing module to upload the image, convert the image, find distortion and remove the attacks in the given dataset image. After that, the edges in the given image are calculated.

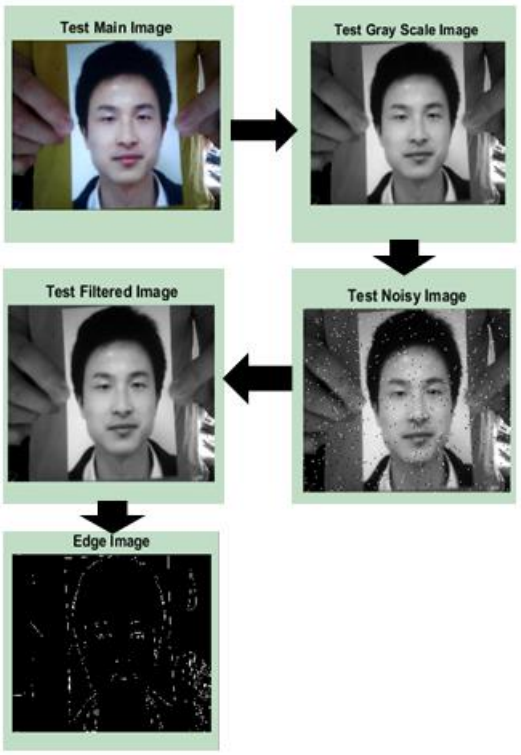

Fig. 7 Flow of process in testing procedure

The testing module is almost similar to training module. The steps involved are same, with a difference that in the latter one the knowledge base is created by the system so as to check it during the time of authentication check process in the former mentioned methodology.

After testing, LBP histogram is obtained for every test image for having further check on spoof attack. This histogram based LBP gives better results.

The testhistogram representation of proposed LBP is revealed in Fig.8. It is further divided into two categories, left one shows its sparse form whereas tight histogram is vivid on the right side. For a particular test image, this histogram is formed to check further whether the spoof detection is fake or real. Thereby, showing the final result in message box.

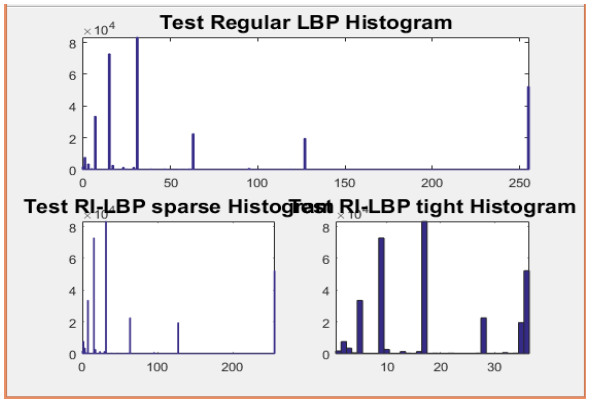

Fig.8 Gene-LBP histogram representation

C. Performance Parameters

In order to evaluate the performances of the existing n-LBPnet and proposed GeneLBPnet, a lot of performance metrics were calculated over the given NUAA imposter database. The comparative analysis is done with the help of graphical representation.

The parameters used for the evaluation of performance of the proposed system are FAR, FRR, HTER, EER, AUC. All these metrics are somehow inter related to each other. The comparison demonstrates that in some cases, the values of parameters are reduced whereas they have shown hike in others, eventually, resulting in the overall improvement in the proposed method.

1) False Acceptance Rate (FAR)

The proportion of recognition cases in which unauthorized individuals are falsely accepted is referred as FAR. Thus, system can make two types of errors,the first one is the case that when there is acceptance of a false person by the system then this case is defined as False Acceptance. Secondly, when a client is rejected by the system then this case is known as False Rejection. The performance of the system is measured by calculating the value of FAR using the following formula (3).

$$\text{FAR} = \frac{\text{Number of False Acceptances}}{\text{Number of Imposter Accesses}} \qquad (3)$$

Fig. 9 showsthat in contrast to other metrics, the value of the acceptance rate reduces in Gene-LBPnet method. Lesser the value of FAR, more will be the security of the system.

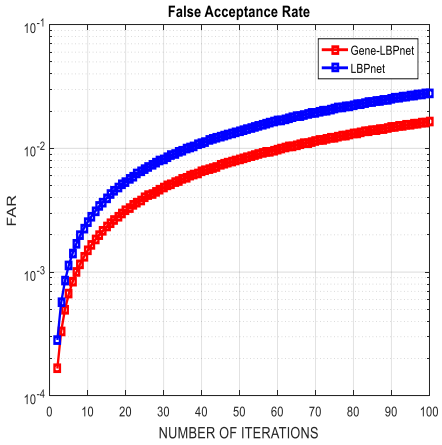

Fig. 9 Comparison- FAR

2) False Rejection Rate (FRR)

As the count of false acceptances goes down, the number of false rejections will go up and vice versa. Similar to FAR, following formula (4) is used to measure the rate of False Acceptances.

$$\text{FAR} = \frac{\text{Number of False Rejections}}{\text{Number of Client Accesses}} \qquad (4)$$

Fig.10 defines that the false rejection rate values increase as compared to the existing one. FRR means wrong data is declared as incorrect in Gene-LBPnet method.

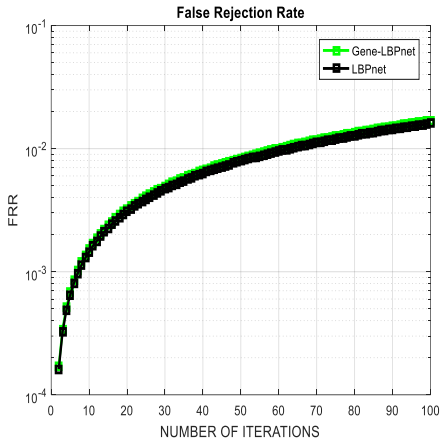

Fig.10 Comparison – False Rejection Rate

3) Half Total Error Rate (HTER)

Considering the other factor affecting the performance of the biometric system, it can be calculated as the average of the previously discussed two parameters, that is, FAR and FRR. The following equation (6) is used to compute the value of HTER.

$$\text{HTER} = \frac{\text{FAR} + \text{FRR}}{2} \qquad (5)$$

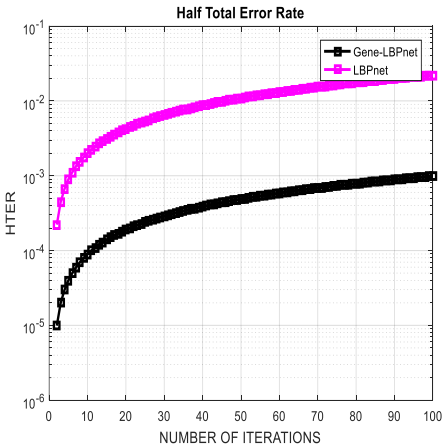

Fig.11 Comparison – HTER

Above figure shows the comparison of HTER value between proposed and existing work.

It is evident thatvalue of Half total Error rate is reduced in case of gene-LBPnet method in comparison to its value for existing work (LBPnet).

4) Equal Error Rate (EER)

Equal Error Rate is a biometric image security system method used to define the threshold values for its FAR (False Acceptance Rate) and FRR (false Rejection Rate). When the error rates are equal, the normal value is defined as its EER. The value shows that the proportion of FA (False Acceptances) is equal to the proportion of FR (False Rejections). Lesser the EER value, higher the recognition rate or accuracy rate of the biometric system.In other words, the point at which both the lines intersect is called as Equal Error Rate (EER).

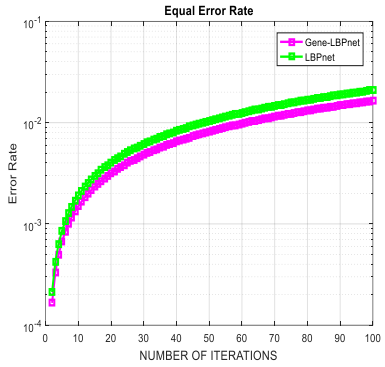

Fig.12 Comparison - Equal Error Rate

The above graphical comparative analysis reveals that in Gene LBPnet, Equal Error Rate is decreased as compared to the existing work which further means that proposed algorithm is more accurate, generating less errors in output.

5) Accuracy Rate (AUC)

Rate of accuracy can be measured in accordance to the percentile of the known faces as per the overall count of the faces those are certified that belong to the similar individual. Percentumexception is the ratio of the error to the real value multiplied by 100. The precise calculated value is a consideration of the reproducibility of a set of dimensions. Accuracy rate is computed as given by (6).

$$AUC = \frac{\text{Correctly localized images}}{\text{Total images}} \times 100 \qquad (6)$$

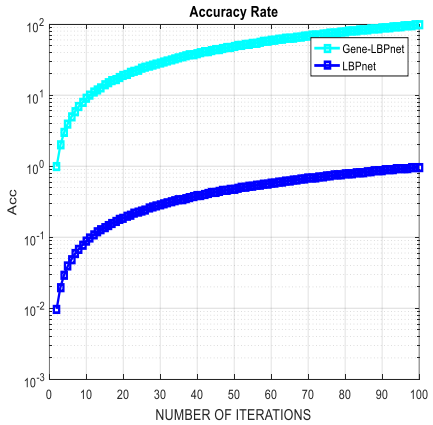

Fig.13 Comparison - Accuracy Rate

Above graph shows the comparison of accuracy rate for proposed and existing methodology. In proposed work, accuracy rate is improved as compared to the LBPnet existing method.

Table II exhibits the performance based gene-LBPNet method. This is a proposed module we are designing to detect the face by distinguishing it in two categories real or Fake. In this proposed method, accuracy rate is improved that is 98 %, Error Rate value is reduced to 0.02.

TableII: Proposed Parameters

Parameters	Values
Accuracy Rate %	97.85 ~ 98%
FAR	0.0204
FRR	0.0129
HTER	0.009
EER	0.02

TableIII: Comparison Performance Metrics

Parameters	Gene-LBP Net	LBP Net
Accuracy Rate %	97.85~ 98%	97%
FAR	0.0204	0.028
FRR	0.0129	0.0160
HTER	0.009	0.0220
EER	0.02	0.0210

Furthermore, Table III shows the comparative analysis with the help of various parameters such as accuracy rate, error rate,acceptance and rejection rate. Performance analysis between Gene-LBPnet and LBPNet Classifier Technique which is existing technique proves that Gene-LBPnet classifier works smartly and fetch the data with knowledge base.

V. CONCLUSION

In this paper, a new approach of Convolutional Neural Networks based on LBP, Gene LBPnet, is proposed for face spoofing detection. This technique outperformed the results of other state-of-the-art methods on NUAA dataset. Considering various evaluation parameters, it is proved that the proposed work gives high accuracy (~98%), less Equal Error Rate, resulting in better detection of spoofing attacks, thus enhancing the security of the system. Based on this analysis, it is concluded that the integration of modified LBP descriptor along with CNN is suitable and robust approach for detection of face spoofing attacks.

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. Additionally, measuring the efficiency of nose alterations for face spoofing purposes can also be considered as future research direction.

REFERENCES

1. Gustavo Botelho de Souza, Daniel Felipe da Silva Santos, Rafael Gonçalves Pires, Aparecido Nilceu Marana , and João Paulo Papa, "Deep Texture Features for Robust Face Spoofing Detection", IEEE Transactions on Circuits and Systems—II: Express Briefs, Vol. 64, No. 12, December 2017 pp. 1397-1401.
2. Aziz, A. Z. A., Wei, H., "Polarization Imaging for Face Spoofing Detection: Identification of Black Ethnical Group", IEEE, International Conference on Computational Approach in Smart Systems Design and Applications,2018, pp. 1-6
3. Dhawanpatil, T., &Joglekar, B. , "Face Spoofing Detection using Multiscale Local Binary Pattern Approach", IEEE, International Conference on Computing, Communication, Control and Automation, 2017, pp. 1-5.
4. Lei Li, Paulo Lobato Correia, Abdenour Hadid, "Face recognition under spoofing attacks: countermeasures and research directions", Special Issue: Face Recognition and Spoofing Attacks of IET Biometrics, Vol. 7, Issue: 1, Jan 2018, pp. 3 -14.
5. D. Menotti et al., "Deep representations for iris, face, and fingerprint spoofing detection", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 4, pp. 864–879, April 2015.
6. S. R. Arashloo, J. Kittler, and W. Christmas, "Face spoofing detection based on multiple descriptor fusion using multiscale dynamic binarized statistical image features", IEEE Transactions on Information Forensics and Security, Vol. 10, No. 11, pp. 2396–2407, Nov. 2015.
7. Zhibin Pan, Xiuquan Wu, Zhengyi Li, and Zhili Zhou, "Local Adaptive Binary Patterns Using Diamond Sampling Structure for Texture Classification", IEEE Signal Processing Letters, Vol. 24, Issue: 6, pp. 828 - 832, June 2017.
8. Galbally, J., Marcel, S., &Fierrez, J., "Biometric Antispoofing Methods: A Survey in Face Recognition". IEEE Access, Vol. 2, Dec 2014, pp. 1530-1552.
9. Chingovska, I., Yang, J., Lei, Z., Yi, D., Li, S. Z., Kahm, O., &Komulainen, J.,"The 2nd competition on counter measures to 2D face spoofing attacks", International Conference on Biometrics (ICB), June 2013, pp. 1-6
10. 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.
11. NUAA Imposter Database. (2019). Retrieved from http://parnec.nuaa.edu.cn/xtan/data/nuaaimposterdb.html.
12. Komulainen, J., Hadid, A., &Pietikainen, M, "Context based face anti-spoofing", IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)', September 2013, pp. 1-8.
13. Li, J., Wang, Y., Tan, T., & Jain, A. K. (2004, August), "Live face detection based on the analysis of fourier spectra", In Biometric Technology for Human Identification, Vol. 5404, pp. 296-304.
14. Tirunagari, S., Poh, N., Windridge, D., Iorliam, A., Suki, N., &Ho, A. T., "Detection of face spoofing using visual dynamics", IEEE transactions on information forensics and security, Vol. 10, Issue: 4, pp. 762-777, 2015
15. Määttä, J., Hadid, A., &Pietikäinen, M. (2012), "Face spoofing detection from single images using texture and local shape analysis", IET biometrics, Vol. 1, Issue: 1, pp. 3-10.
16. Bharadwaj, S., Dhameecha, T.I., Vatsa, M., & Singh, R., "Computationally efficient face spoofing detection with motion magnification", In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, 2013, pp. 105-110.

AUTHORS PROFILE

Karuna Grover, is currently pursuing Master's degree in Electronics and Communication Engineering from National Institute of Technical Teacher's Training and Research, Chandigarh, India. She has 05 years of teaching experience. She has completed her Bachelor of Technology from Kurukshetra University, India in year 2012. Her research areas include Digital Image Processing and Digital Signal Processing. Also, she has presented one research paper in IEEE Conference in year 2017.

Dr. Rajesh Mehra, is presently Head of Curriculum Development Center at National Institute of Technical Teacher Training & Research, Chandigarh, India. He has received his Doctor of Philosophy and Master's Degree in Electronics & Communication Engineering from Punjab University, Chandigarh, India. Dr. Mehra has completed his Bachelor of Technology from NIT, Jalandhar, India. Dr. Mehra has 23 years of Academic Experience along with 10 years of Research Experience. He has nearly 500 publications in Refereed Peer Reviewed International Journals and International Conferences. Dr. Mehra has guided more than 105 PG scholars for their ME thesis work and also guiding 03 independent PhD scholars in his research areas. His research areas include VLSI Design, Digital Signal & Image Processing, Renewable Energy and Energy Harvesting. He has authored one book on PLC & SCADA. Dr. Mehra is senior member IEEE and Life member ISTE.