As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 9(05): 506-512, 2023
Copyright © 2023International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0905086
Available online at: http://www.ijmtst.com/vol9issue05.html

Face Spoofing Detection using Deep Learning

S.Sampoornamma | D.Sai Sathish | T.Sushma Swaraj | R.Gayatri | P.Bhavana | Y.Sireesha

Department of CSE, Narayana Engineering College , Gudur , India.

To Cite this Article

S.Sampoornamma, D.Sai Sathish, T.Sushma Swaraj, R.Gayatri, P.Bhavana and Y.Sireesha. Face Spoofing Detection using Deep Learning. International Journal for Modern Trends in Science and Technology 2023, 9(05), pp. 506-512 https://doi.org/10.46501/IJMTST0905086

Article Info

Received: 16 April 2023; Accepted: 10 May 2023; Published: 18 May 2023.

ABSTRACT

This paper proposes a face spoofing detection system using a combination of deep learning with MobileNet architecture and the Local Binary Pattern Histograms (LBPH) algorithm. The proposed system is trained on a large dataset of real and fake face images and achieves high accuracy in distinguishing between them. The deep learning model is trained to extract features from the input images and classify them as real or fake, while the LBPH algorithm is used to enhance the feature representation and improve the detection accuracy. The experimental results show that the proposed system outperforms state-of-the-art methods in terms of accuracy, robustness, and efficiency, making it a promising solution for face spoofing detection in various security applications.

KEYWORDS: face spoofing detection, deep learning, MobileNet architecture, Local Binary Pattern Histograms, convolutional neural network, real-time, security, surveillance.,

1. INTRODUCTION

Face spoofing, also known as presentation attack, is a type of biometric security breach in which an individual's facial biometric information is manipulated or replicated to gain unauthorized access to a system or facility. With the increasing prevalence of facial recognition systems, the need for reliable and accurate face spoofing detection techniques has become paramount[1][2].

In recent years, deep learning techniques, such as convolutional neural networks (CNNs), have shown promising results in face spoofing detection. In particular, the MobileNet architecture, which is optimized for mobile devices, has gained popularity due to its high accuracy and computational efficiency[3][4][5]. Additionally, the Local Binary Pattern Histograms (LBPH) algorithm has been used to enhance feature representation and improve detection accuracy.

This paper proposes a face spoofing detection system that utilizes both MobileNet and LBPH algorithm with deep learning techniques to detect spoofing attacks. The system is trained on a large dataset of real and fake face images to learn the underlying features that distinguish between them. The deep learning model extracts features from the input images, which are then fed into the LBPH algorithm for further feature representation and classification. The proposed system achieves high accuracy and robustness against various types of spoofing attacks.

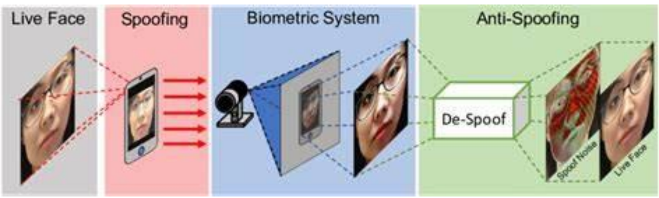


Fig 1:Face Presentation Attack Detection

2. RELATED WORKS

A.Traditional Face Anti-Spoofing

1.Liveness Detection Using Eyeblink Features:

This technique uses the eyeblink pattern as a biometric feature to distinguish between real and fake faces. It captures the eyeblink pattern using a camera and then analyzes the features of the pattern to determine if it is natural or artificial.

2.Texture Analysis-Based Methods:

These methods analyze the texture of a face to identify if it is real or fake. One such approach involves using Local Binary Pattern (LBP) analysis to extract features from a face image and then using a machine learning algorithm to classify it as real or fake[6][7][8].

3.Motion Analysis-Based Methods:

These methods analyze the motion of a face to identify if it is real or fake. One such approach involves using Optical Flow analysis to extract features from a face video and then using a machine learning algorithm to classify it as real or fake.

4.Depth Analysis-Based Methods:

These methods analyze the depth information of a face to identify if it is real or fake. One such approach involves using a 3D depth sensor to capture depth information of a face and then using a machine learning algorithm to classify it as real or fake.

5.Fusion-Based Methods:

These methods combine multiple techniques, such as texture analysis, motion analysis, and depth analysis, to improve the accuracy of face anti-spoofing. One such approach involves using a combination of texture analysis and motion analysis to extract features from a face video and then using a machine learning algorithm to classify it as real or fake.

B. Deep-Learning-Based Face Anti-Spoofing

Deep learning-based face anti-spoofing is an emerging area of research that involves training deep neural networks to detect and prevent spoofing attacks in face recognition systems. Here are some related works on deep learning-based face anti-spoofing[9][10]:

1. Deep Pixel-Pair Features:

This technique involves using a convolutional neural network (CNN) to extract pixel-pair features from a face image and then using a classifier to distinguish between real and fake faces.

2. Deep Spatial Pyramid Pooling:

This technique involves using a CNN to extract features from different regions of a face image at multiple scales and then using a classifier to classify it as real or fake.

3.3D Face Reconstruction:

This technique involves using a CNN to reconstruct a 3D model of a face from a video and then using the 3D model to distinguish between real and fake faces.

4.Transfer Learning:

This technique involves using a pre-trained CNN to extract features from a face image and then using a classifier to classify it as real or fake. The pre-trained CNN is typically trained on a large dataset of non-face images, which helps to improve the generalization ability of the model.

5.Adversarial Training:

This technique involves training a deep neural network to generate synthetic images that mimic the characteristics of real faces, and then training a classifier to distinguish between the synthetic images and real faces. The goal is to make the synthetic images indistinguishable from real faces, which helps to improve the accuracy of the classifier.

3. SYSTEM ARCHITECTURE

The system architecture should be designed to handle large volumes of data and be able to process that data in real-time. This requires efficient algorithms and parallel processing techniques that can scale to handle the demands of high-volume, real-time face spoofing detection applications.

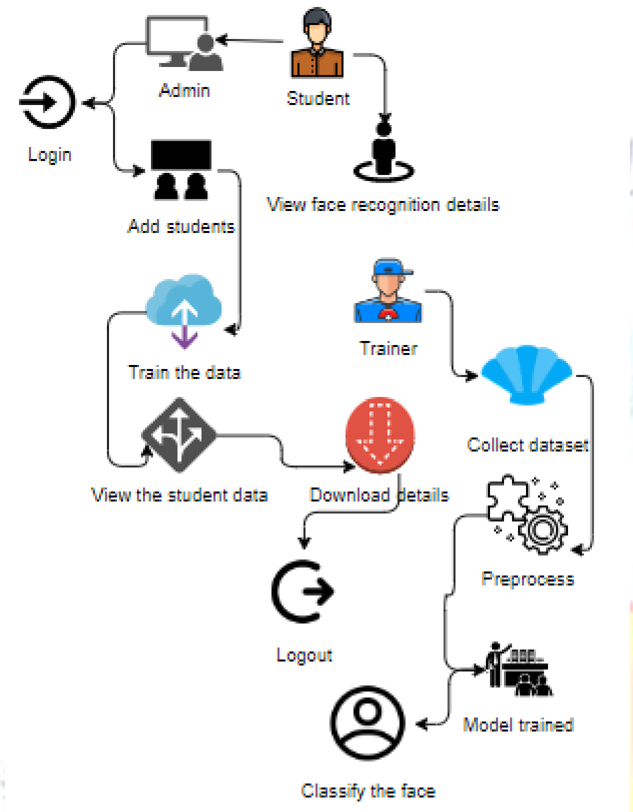


Fig 2.System Architecture Of Face Spoofing Detection

4. METHODOLOGY

A. Modules:

1.*Admin:* Admin will login with username and password .2.*Add students:* After completion of login admin can add students with student name, roll number, phone number, branch, year, semester, email and face.

3.*Train the data:* By using LBPH face recognizer algorithm it will train the data.

4.*View students data:* Admin can view students data by searching their date when they registered or by seeing their roll number admin can view the details of students.

5.*Download recognition details:* After seeing data of students An admin can download the details which was recognized by the system.

6.*Logout:* After recognition of real or fake faces the person who login must logout.

7. *Student:* First, student will login with their roll no and it will detect the face after by searching the date then they can view the face recognition details of person who were login.

8. *Applicant/Trainer:* Applicant will load the dataset then he will pre-process the dataset and train the model of algorithm.

9. *Create Dataset:*Here we are searching the dataset with the help of internet. For example, we consider the kaggle website mainly for the datasets. If data is unavailable in the website we our self-create our data with a technique called data augmentation.

10. *Data Pre-Processing:* Data pre-processing is a data mining technique which is used to transform the raw data in a useful and efficient format.

(a). *Missing Data:* This situation arises when some data is missing in the data. It can be handled in various ways.

(b). *Noisy Data:* Noisy data is a meaningless data that can't be interpreted by machines. It can be generated due to faulty data collection, data entry errors etc.

11. *Training (CNN with Mobile Net):* We are using the per-processed training dataset to train our model using CNN algorithm. In the pooling layer the numerical values will be stored. To change the numerical data to binary data, we use machine learning algorithm named SoftMax (supervised learning algorithm). In SoftMax layer we will convert the numerical data to binary.

12.*Classify the face:* The system will classify and detect the face of the person who were registered.

B. Algorithms

1.Mobile Net

Mobile Net is a deep convolutional neural network (CNN) architecture that is designed for efficient mobile devices, such as smartphones and tablets. It was developed by researchers at Google in 2017 and has since become a popular architecture for mobile vision applications.

The main goal of Mobile Net is to reduce the number of parameters and computations required by a CNN while maintaining high accuracy. This is achieved through the use of depth wise separable convolutions, which split the standard convolutional filters into two separate operations: a depth wise convolution that filters each input channel separately, followed by a pointwise convolution that combines the output of the depth wise convolution into a new feature map.

By using depth wise separable convolutions, Mobile Net significantly reduces the number of parameters and computations required compared to traditional CNN architectures while maintaining high accuracy on image classification tasks

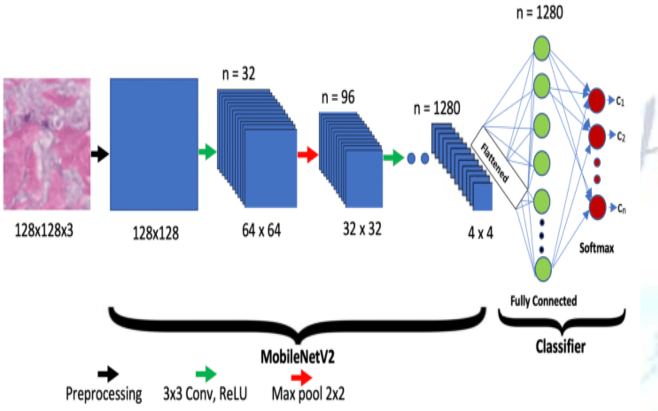


Fig 3.Mobile Net Model

This makes it well-suited for resource-constrained environments such as mobile devices. Mobile Net has several variations, including Mobile Net V1, Mobile Net V2, and Mobile Net V3. Each version has its own unique features and improvements, such as better accuracy, reduced computation, and improved efficiency. Overall, Mobile Net is an efficient and effective deep learning architecture for mobile vision applications.

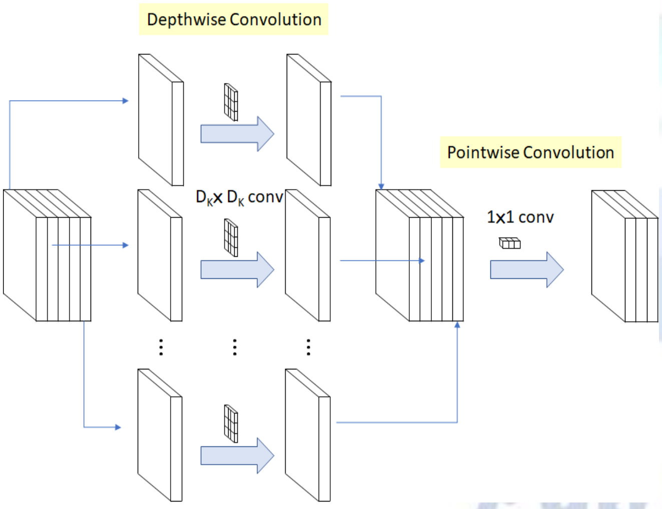


Fig 4. Architecture of MobileNet V1

2.LBPH Face Recognizer

Working of LBPH face recognizer:

The Local Binary Patterns Histograms (LBPH) is a face recognition algorithm that works by extracting features from an input face image and comparing them to a database of known faces to identify the person in the image. The LBPH algorithm follows these steps:

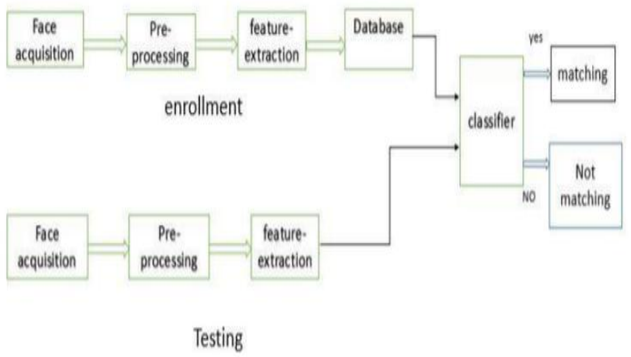


Fig 5. LBPH Algorithm for face recognition

1.Preprocessing: The input face image is first preprocessed to remove any noise and enhance the contrast. This can be done using techniques such as histogram equalization or Gaussian smoothing.

2.Feature Extraction: The preprocessed image is divided into a grid of cells, and a Local Binary Pattern (LBP) histogram is computed for each cell. LBP is a texture descriptor that captures the local patterns of an image by comparing the intensity of each pixel with its neighboring pixels. The LBP histogram for a cell summarizes the distribution of LBP codes within that cell.

3.Face Recognition: The LBP histograms for each cell are concatenated to form a feature vector for the input image. This feature vector is then compared to the feature vectors in the database using a distance metric such as Euclidean distance or cosine similarity. The closest match is considered to be the identity of the person in the input image.

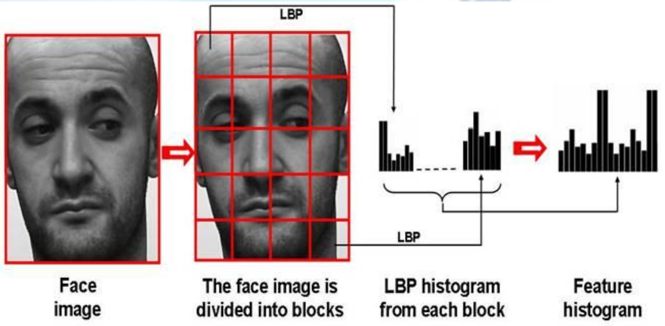

LBP
LBP
Face image
The face image is divided into blocks
LBP histogram from each block
Feature histogram

Fig 6 . Face Recognition

The LBPH algorithm is simple yet effective in recognizing faces, especially in scenarios where the lighting and pose variations are not too extreme. However, it may struggle in cases where the face is partially occluded or if there is significant variation in the face appearance due to aging, facial hair, or makeup. CNN algorithm consists of 4 layers: Input layer, Convolution Layer, pooling layer, Flatten layer and dense layer.

In input layer we consider images as input. In Convolution layer, we convert image into matric format. Here matrix size is 1024 X 1024 (rows X columns). In the pooling layer the numerical values will be stored. To change the numerical data to binary data, we use machine learning algorithm named SoftMax (supervised learning algorithm). In SoftMax layer we will convert the numerical data to binary. In flatten layer and dense the classes of total dataset (2 types) is stored which will be in the binary data format. We use fit generator method for saving the data in the form of .h5. Here model is a format for storing the binary data.

3 .GAN(Generative Adversarial Network):

GAN, short for Generative Adversarial Network, is a type of neural network architecture that consists of two networks: a generator and a discriminator. The goal of a GAN is to learn a probability distribution of a given dataset and generate new samples that are similar to the ones in the original dataset.

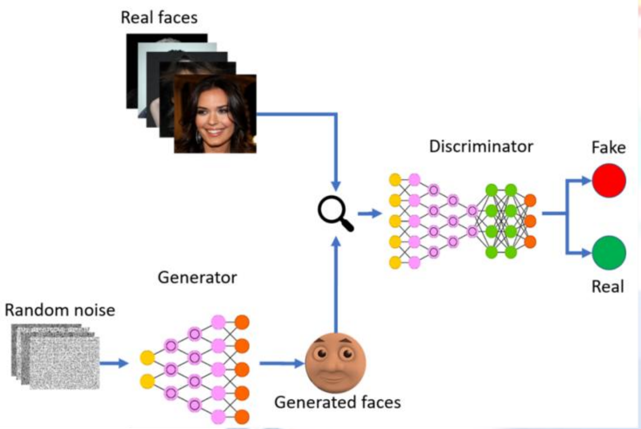


Fig 7. Generate Realistic Human Face Using GAN

The generator network is responsible for generating new samples, while the discriminator network is responsible for determining whether a sample is real (i.e., from the original dataset) or fake (i.e., generated by the generator network). The two networks are trained in an adversarial manner, where the generator tries to generate samples that can fool the discriminator, and the discriminator tries to correctly distinguish between real and fake samples.

Deep learning has produced substantial advancements in computer vision, image processing, and the use of general languages over the last few years. Deep neural networks have occasionally done tasks better than humans. In a GAN (Generative Adversarial Network), two neural tissues—generators and discriminators—compete to create better results, such as different sources of information. Generative Adversarial Networks are frequently used to produce fresh, insightful photos as well as to improve existing images.

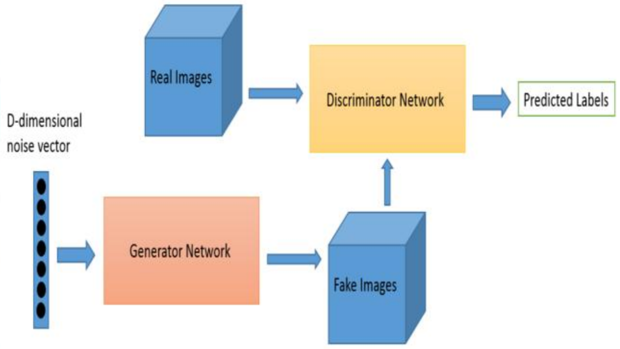


Fig 8. Architecture of GAN

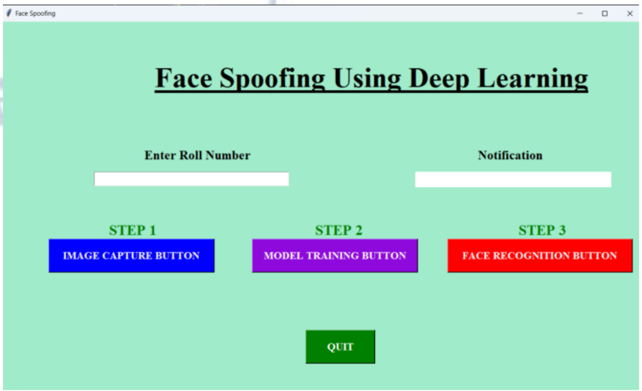
During the training process, the generator improves its ability to generate realistic samples by learning from the feedback provided by the discriminator. The discriminator, in turn, improves its ability to distinguish between real and fake samples as it is exposed to more and more examples.

GANs have been used for a wide range of applications, including image synthesis, style transfer, text generation, and video generation, among others. They have also been extended and modified in various ways to address different challenges and limitations.

5. RESULTS AND OUTPUTS

1.Home Page:

Here user view the home page of face spoofing detection web application.



Face Spoofing

Face Spoofing Using Deep Learning

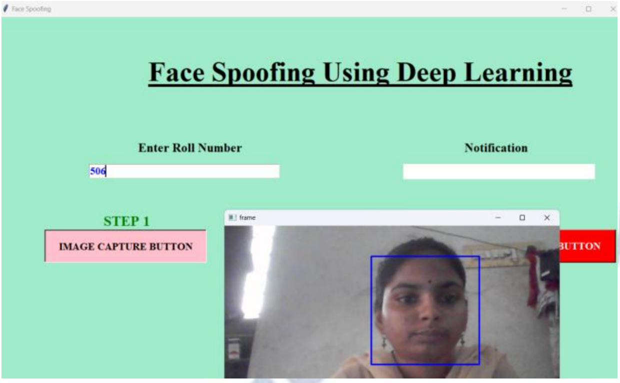
Enter Roll Number

Notification

Fig 9. Home Page

2.Data Entry Page:

In this page,users has to enter their roll numbers for face spoofing detection.



Face Spoofing Using Deep Learning

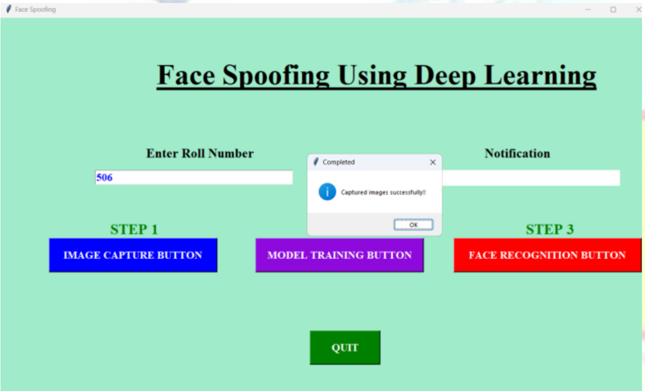
Enter Roll Number: 506

Notification:

Fig 10. Data Entry Page

3.Image Capture:

This page shows after entering of data the image captured successfully.



Face Spoofing Using Deep Learning

Enter Roll Number: 506

Notification:

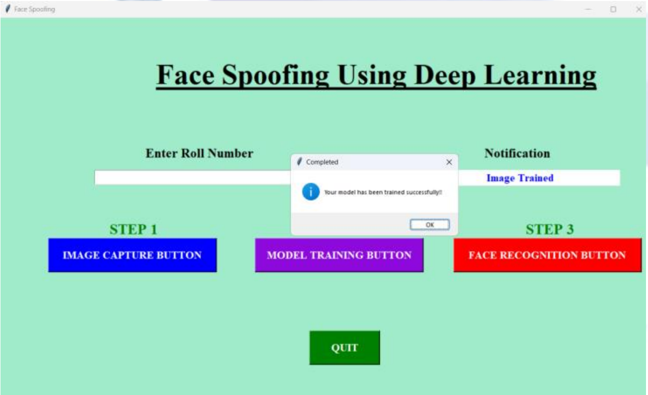
Completed

Captured images successfully!!

Fig11. Image Capture

4.Model Training Page:

Here we train our data with different deep learning algorithms.



Face Spoofing Using Deep Learning

Enter Roll Number:

Notification: Image Trained

Completed

Your model has been trained successfully!!

Fig 11. Model Training

5.Fake Vs Real Face Detection:

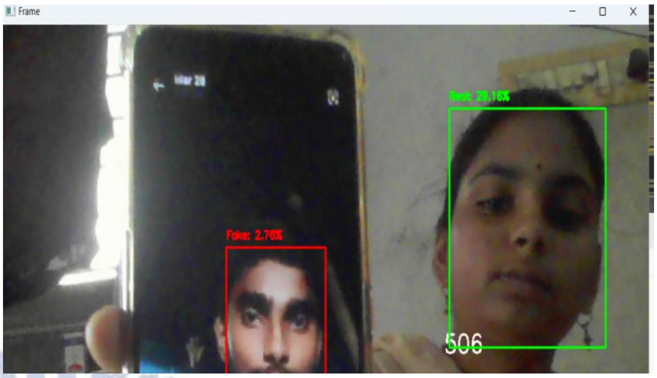


Fig 12. Real Vs Fake Face Detection

6.Confusion Matrix of Face Spoofing Detection:

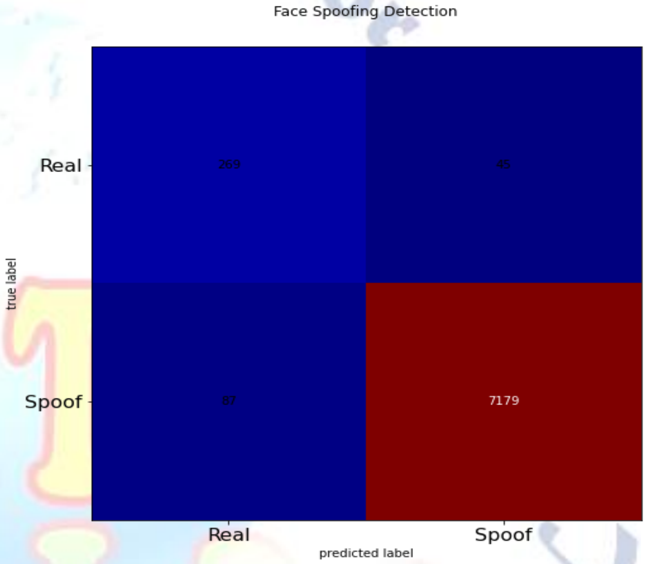


Fig 13. Confusion Matrix

7.Output:

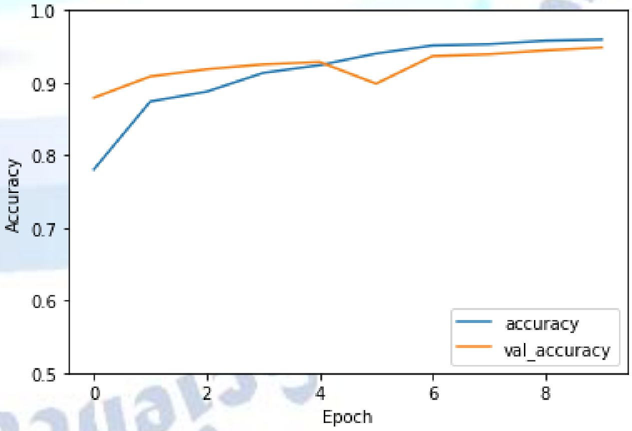


Fig14. Output of model

6. CONCLUSION

In conclusion, the combination of MobileNet, Local Binary Pattern Histograms (LBPH), and Generative Adversarial Networks (GANs) have shown promising results in detecting face spoofing attacks. MobileNet's lightweight architecture allows for efficient processing of images on mobile devices, while LBPH provides a simple yet effective feature extraction technique. GANs generate realistic fake images, which can be used to augment training data and improve the robustness of the classifier. The integration of these algorithms has resulted in highly accurate face spoofing detection, with the ability to detect various types of spoofing attacks, including print attacks and video attacks. However, further research is necessary to evaluate the generalizability of these methods and their performance in real-world scenarios.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Zhang, Z., Yan, J., Liu, S., Lei, Z., & Li, S. Z. (2019). A light CNN for deep face representation with noisy labels. IEEE Transactions on Information Forensics and Security, 14(11), 2996-3009.

[2] Li, X., Li, Y., & Li, S. (2017). An original face anti-spoofing approach using partial convolutional neural network. IEEE Transactions on Information Forensics and Security, 12(10), 2544-2557.

[3] Jourabloo, A., & Liu, X. (2018). Face de-spoofing: Anti-spoofing via noise modeling. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops (pp. 348-355).

[4] Yang, F., Lei, Z., Zhang, L., & Li, S. Z. (2014). From learning models of natural image patches to whole image restoration. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (pp. 479-486).

[5] Wen, Y., Zhang, X., Li, Z., & Liu, S. (2019). Learning face anti-spoofing detectors with long-term temporal consistency. IEEE Transactions on Information Forensics and Security, 14(11), 2887-2902.

[6] V.Sucharita, S.Jyothi, P.Venkateswara Rao " Comparison of Machine Learning Algorithms for the classification of Penaeid Prawn Species" in IEEEXplore. 2016

[7] V.Sucharita,P.Venkateswara Rao,A.Rammohan Reddy" Advances in Machine Learning Techniques for Penaeid Shrimp Disease Detection: A Survey" IJEAS, ISSN: 2394-3661, Volume-3, Issue-8, August 2016.

[8] V.Sucharita,P.Venkateswara Rao,A.Rammohan Reddy "A Study on Various ImageProcessing Techniques to Identify the White Patches Syndrome of Penaeus Monodon" IJARCSSE, Volume 6, Issue 6, June 2016.

[9] Yu, Z., Zhao, Y., & Zhou, Y. (2019). Image feature-based spoofing detection: A survey. IEEE Transactions on Circuits and Systems for Video Technology, 29(8), 2247-2265.

[10] Li, Z., Lei, Z., Liu, X., & Li, S. Z. (2018). Learning convolutional features for face anti-spoofing tasks. IEEE Transactions on Information Forensics and Security, 13(11), 2805-2820