International Journal for Research in Engineering Application & Management (IJREAM)
ISSN : 2454-9150 Vol-07, Issue-01, APR 2021

# *Face Spoofing Detection using Deep Learning*

**Anushree Deshmukh, Professor, MCT's RGIT Mumbai India, Anushree.deshmukh@mctrgit.ac.in**
**Drishti Gandhi, Student, MCT's RGIT Mumbai India, Drishti0927@gmail.com**
**Priya Govekar, Student, MCT's RGIT Mumbai India, priyagovekar505@gmail.com**
**Ajay Padwal, Student, MCT's RGIT Mumbai India, ajaypadwal73@gmail.com**

**Abstract: Face Spoofing is a type of attack on a face recognition system. What would happen if any unauthorized user purposely tried to access the face recognition system? Such a user may have a photo or video on their smartphone that they could hold up to the camera responsible for performing face recognition. In those situations, the camera can easily give access, but ultimately it will lead to an unauthorized user bypass the face recognition system. Our proposed system able to spot Spoof and real faces. In this system, we treated face spoofing detection as a binary classification problem. The model is trained using Keras and OpenCV. A Caffe Face detector is used to locate the face ROIs. Then the extracted features are trained using VGGNet-esque CNN architecture. We trained a Convolutional Neural Network capable of distinguishing real faces from fake/spoofed faces.**

***Keywords — Liveness Detection, Convolutional Neural Network, Face recognition.***

## I. INTRODUCTION

It is no surprise that cybercrime is on the rise in our increasing digital world. Many companies are now exploring biometric face recognition as viable security solution. The general public has immense need for security measures against spoof attack. Biometrics is the fastest growing segment of such security industry. Some of the familiar techniques for identification are facial recognition, fingerprint recognition, handwriting verification, hand geometry, retinal and iris scanner. Among these techniques, the one which has developed rapidly in recent years is face recognition technology and it is more direct, user friendly and convenient compared to other methods. This innovative technology shows a lot of promise and change the way in which we can access sensitive information. But as promising as facial recognition is it does have flaws. User photos can easily be found on social networking sites and images can be spoofed. This is where the need of anti-spoofing comes into play. Face anti spoofing is the task of preventing false facial verification by using a photo, video/substitute for an authorized person's face.

## II. LITERATURE SURVEY

Earlier face spoofing detection mainly focused on motion, texture, frequency and quality parameters to detect real and non-real or spoof face.

D. Wen et.al [1] proposed an approach to detect spoof faces based on Image Distortion Analysis (IDA). The features considered are colour diversity, reflection, blurriness and chromatic moment. Here the features are trained and classified using Support Vector Machine (SVM) to identify the face to be either real or spoof face.

Frequency and Texture based analysis this approach is used by Gahyun Kim et al [2]. The basic purpose is to differentiate between live face and fake face (2-D paper masks) in terms of shape and detailedness. The authors have proposed a single image-based fake face detection method based on frequency and texture analyses for differentiating live faces from 2-D paper masks. The authors have carried out power spectrum-based method for the frequency analysis, which exploits both the low frequency information and the information residing in the high frequency regions. Moreover, description method based on Local Binary Pattern (LBP) has been implemented for analysing the textures on the given facial images. They tried to exploit frequency and texture information in differentiating the live face image from 2-D paper masks. The authors suggested that the frequency information is used because of two reasons. First one is that the difference in the existence of 3-D shapes, which leads to the difference in the low frequency regions which is related to the illumination component generated by overall shape of a face. Secondly, the difference in the detail information between the live faces and the masks triggers the discrepancy in the high frequency information. The texture information is taken as the images taken from the 2-D objects (especially, the illumination components) tend to suffer from the loss of texture information compared to the images taken from the 3-D objects. For feature extraction, frequency-based feature extraction, Texture-based feature extraction and Fusion-based feature extraction are being implemented.

VGGNet is a Convolutional Neural Network architecture proposed by Karen Simonyan and Andrew Zisserman from the University of Oxford in 2014. The input to VGG based convNet is a 224*224 RGB image. Pre-processing layer takes the RGB image with pixel values in the range of 0–255

 DOI : 10.35291/2454-9150.2021.0182 

and subtracts the mean image values which is calculated over the entire ImageNet training set.

The Caffe framework from UC Berkeley is designed to let researchers create and explore CNNs and other Deep Neural Networks (DNNs) easily, while delivering high speed needed for both experiments and industrial deployment [5]. Caffe provides state-of-the-art modelling for advancing and deploying deep learning in research and industry with support for a wide variety of architectures and efficient implementations of prediction and learning. To locate face ROIs, pretrained Caffe face detector is used. In order to perform face detection, it is required to create a blob from the image. This blob has a 300×300 width and height to accommodate our Caffe face detector.

## III. PROPOSED SYSTEM

Spoofing occurs when the attacker presents a non-real image or sample of identity of valid user to the acquisition sensor. In this proposed system there are two stages:

i. Face detection in an image,
ii. Face Verification of real or spoof face in an image,

as shown in Fig (1)

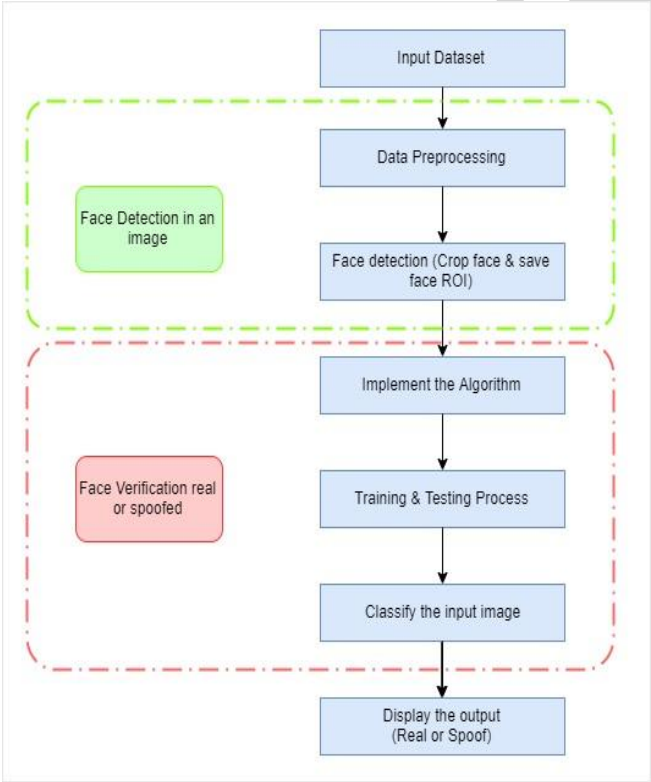


Fig. 1 Flow of the spoof detection process

**Following are the steps explained precisely,**

**Step 1**: Gathering of data:

Real: Here, we recorded videos of people having different skin tones.

Spoofed: Then we recorded another video of the same person holding mobile displaying the original video which will be considered as fake

**Step 2**: Preprocessing of data:

We detected faces in each frame and labeled them as real or fake, thereby creating two folders namely. Real and fake thus creating our dataset

**Step 3**: Implementation of CNN model
Convolutional Neural Network (CNN) is trained to classify the Real and Spoof faces. It consists of several hidden layers such as Convolutional Layer, Activation function, Pooling layer, Fully connected layers between
the input and final output layer. The neurons in the hidden layer learn the features of the input images and finally predict the classes i.e., real and spoof. The output layer predicts the input image and gives the percentage
of resemble of input image to each class. The class with maximum probability is the final output result.

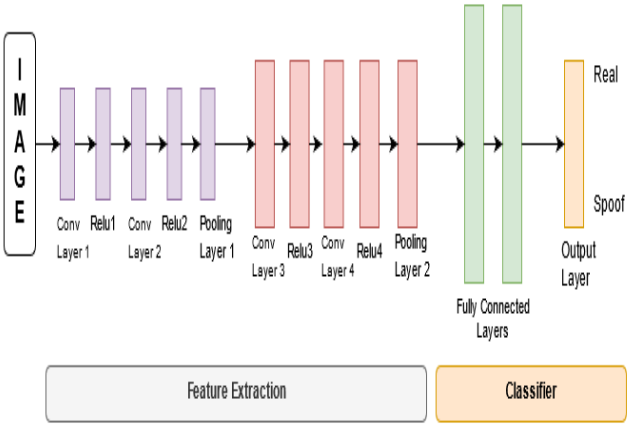


Fig. 2

VGGNet CNN architecture as shown in Fig. (2) consists of four convolutional layers and the four-activation function (ReLU activation function). There are two max-pooling layer of size 2x2, after the convolutional layer, batch normalization and dropout are also added. Two fully-connected dense layer and to classify the SoftMax classifier is used. The dataset is divided into 75% which is used for training and 25% reserved for testing Real or Spoof face detection is carried out using VGGNet CNN architecture. There are two phases in classifying, namely,

I. Training - Phase
II. Testing – Phase

**Step 4**: Training model:

Training phase contains dataset consisting of both Real and Spoof images as in fig (3). The face cropped images are of 300X300 size. VGGNet-esque architecture of Convolutional Neural Network Model as shown in Fig (2) is used to train the dataset.

 DOI : 10.35291/2454-9150.2021.0182 

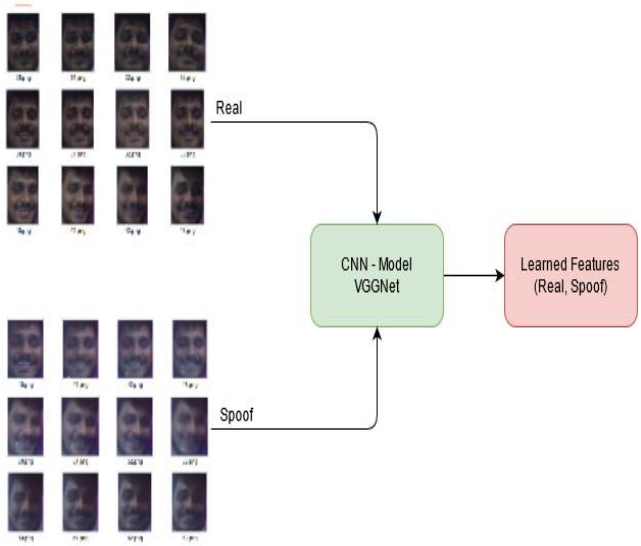


Fig. 3

**Step5**: Script to show demo:

We will access our webcam, then apply face detection to each frame. For each face detected, apply the model that is trained.

## IV. RESULT

Results in the input images, that are faces are verified as shown in Fig (4) and Fig (5).

Fig. 4

Fig. 5

As discussed in the previous section, a Caffe face detector is used to detect the face and face ROIs located. Then it is classified as Real or Spoof as shown in Fig (6) and Fig (7).

Fig. 6

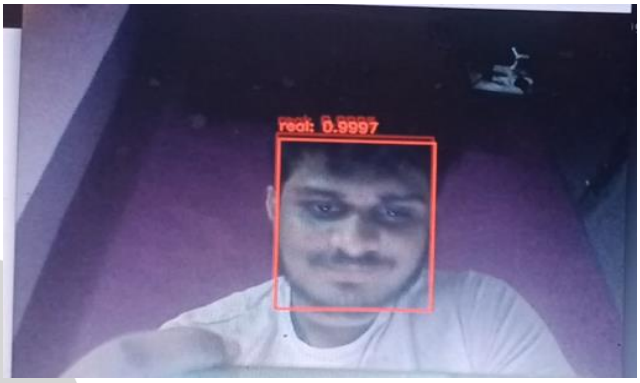


Fig.7

Real and Spoof face is detected as shown in Fig. (8).

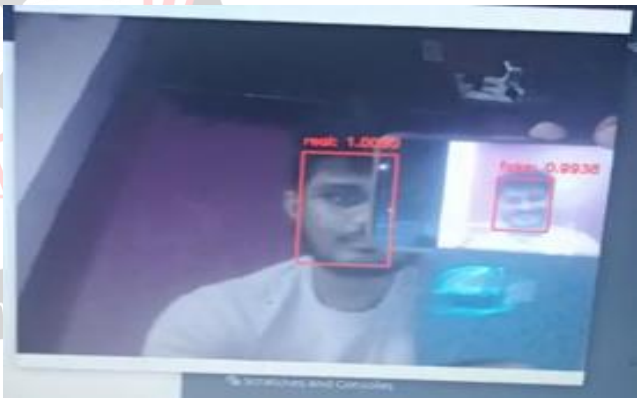

Fig. 8

## IV. CONCLUSION

This work provided an overview of approaches of face spoofing detection. It presented a categorization based on the type of techniques used and types of liveness indicator used for face spoofing detection which helps understanding different spoof attacks scenarios and their relation to the developed solutions. A review of most interesting approaches for spoofing detection was presented. The most common problems that have been observed in case of many spoofing detection techniques are the effects of illumination change, effects of amplified noise on images which damages the texture information. For blinking and movement of eyes based spoofing detection methods, eyes

 DOI : 10.35291/2454-9150.2021.0182 

glasses which causes reflection must be considered for future development of spoofing detection solutions. VGGNet Convolutional Neural Network (CNN) used in classifying, is more advantageous and produce better accurate result than that of other Machine learning and classifying techniques such as, Support Vector Machine (SVM) [5], the datasets, which play an important role in the performance of spoofing detection solutions, must be informative and diverse that mimics the expected application scenarios. Non-interactive video sequences must include interactive sequences where the users perform certain tasks. Future attack datasets must consider attacks like 3D sculpture faces and improved texture information. Our main aim is to give a clear pathway for future development of more secured, user friendly and efficient approaches for face spoofing detection.

## REFERENCES

[1] Di Wen, Hu Han and Anil K. Jain, "Face Spoof Detection with Image Distortion Analysis" in IEEE Transactions on Information Forensics and Security, 2015.

[2] G. Kim, S. Eum, J. K. Suhr, D. I. Kim, K. R. Park, and J, Kim, Face liveness detection based on texture and frequency analyses, 5th IAPR International Conference on Biometrics (ICB), New Delhi, India. pp. 67-72, March 2012.

[3] Zhenqi Xu, Shan Li, Weihong Deng, "Learning Temporal Features Using LSTM-CNN Architecture for Face Anti-spoofing" in 3rd IAPR Asian Conference on Pattern Recognition, 2015

[4] Y. Jia, E. Shelhamer, J. Donahue, S. Karayev, J. Long, R. Girshick, S. Guadarrama, and T. Darrell. "Caffe: Convolutional architecture for fast feature embedding". arXiv preprint arXiv:1408.5093, 2014.

[5] Mahitha M. H, "Face Spoof Detection Using Machine Learning with Colour Features" in International Research Journal of Engineering and Technology (IRJET) Volume 5 Issue 3, 2018.

 DOI : 10.35291/2454-9150.2021.0182 