Face Spoofing Detection using Mixed Feature with Deep Convolutional Neural Networks

Jesslin Melba N V, Poonima U, Blessy J

Abstract: Nowadays, face biometric-based access control systems are becoming ubiquitous in daily life while they are still vulnerable to spoofing attacks. Developing robust and reliable methods to prevent such frauds is unavoidable. As deep learning techniques have achieved satisfactory performances in computer vision, they have also been applied to face spoofing detection. However, the numerous parameters in these deep learning-based detection methods cannot be updated to optimum due to limited data. In this paper, a highly accurate face spoof detection system using multiple features and deep learning is proposed. The input video is broken into frames using content-based frame extraction. From each frame, the face of the person is cropped. From the cropped images multiple features like Histogram of Gradients (HoG), Local Binary Pattern (LBP), Center Symmetric LBP (CSLBP), and Gray level co-occurrence Matrix (GLCM) are extracted to train the Convolutional Neural Network (CNN). Training and testing are performed separately by using collected sample data. Experiments on the standard spoof database called Replay-Attack database the proposed system outperform other state-of-the-art techniques, presenting great results in terms of attack detection.

Keywords: Histogram of Gradients (HoG), Local Binary Pattern (LBP), Center Symmetric LBP (CSLBP), and Gray level co-occurrence Matrix (GLCM) are extracted to train the Convolutional Neural Network (CNN).

I. INTRODUCTION

Cybercrime is on the ascent in our digitally advanced world. Numerous organizations are presently investigating biometric face acknowledgment as a reasonable security arrangement. This imaginative innovation shows a great deal of guarantee and could change how we get to delicate data. [1] Be that as it may, as promising as facial acknowledgment seems to be, it has defects. Client photographs can without much of a stretch be found through interpersonal organizations and used to parody facial acknowledgment programming. That is the reason it is significant for organizations to have face against caricaturing frameworks set up to secure delicate information, decrease robbery, and alleviate misrepresentation. These frameworks upgrade existing facial acknowledgment arrangements by improving their capacity to identify misrepresentation. While this appears to be incredible on paper, obviously shortcomings do exist. What's preventing somebody from utilizing a phony face to access delicate information. This is the place the requirement for against mocking arrangements become an integral factor. We depend on liveness identification to approve a person's personality. These checks can confirm whether an individual is really present or utilizing a photograph to parody the framework.

Liveness identification is a security include that can guarantee organic identifiers are from the correct client and not from another person. Conventional types of recognitions can incorporate eye or lip development examination, incited movement guidelines, surface/reflection discovery in video nourishes or zooming movement identification. Another new method is the 3D profundity examination. [2] There are two methodologies for liveness discovery: dynamic and latent. Dynamic liveness identification alludes to strategies where the client plays out an activity, for example, squinting, making facial developments or keystroking, which makes it increasingly troublesome and tedious for the client to parody the framework. Inactive liveness location utilizes inner calculations to identify parodies and requires nothing from the client. When signing into a banking application utilizing facial acknowledgment, for instance, a functioning liveness discovery framework may expect clients to squint while it checks their face. [3] Inactive liveness recognition, in the interim, may filter a client’s face to guarantee that a genuine human face is available with the person's appropriate profundity shapes. Numerous liveness discovery techniques, particularly dynamic methodologies, take more time to recognize clients, diminishing the speed, accommodation, and straightforwardness of biometric ID.

To secure face acknowledgment frameworks against caricaturing assaults, many face anti-spoofing strategies have been proposed. The assessment of these strategies on the current face anti-spoofing databases shows generally excellent exhibitions. For example, on the NUAA [4] and the Replay-Attack databases, numerous strategies have accomplished amazing exhibitions (close to 0 % error rate). Nonetheless, these face against ridiculing databases were recorded in controlled conditions and their assessment conventions do not mirror this present reality situation, which utilizes these strategies in real-world applications faulty. To be sure, late examinations have uncovered that the presentation of the best in class strategies debases definitely under this present reality-variety (e.g., enlightenment and camera gadget varieties), [5, 6] which shows that more robust face anti-spoofing methods are needed to reach the deployment levels of the face biometric systems.

This paper proposes a deep color and texture-based anti-spoofing technique using deep learning techniques. The rest of the paper is organized as follows: Section II reviews the related work. Section III explains the proposed segmentation model. Section IV gives a detailed analysis of the results. Section V concludes the paper.

Revised Manuscript Received on January 15, 2020

Jesslin Melba N V*, Department of Electronics and Communication Engineering, Narayanganuru college of Engineering, Manjalumoodu, India.
Email: jessinmelba@gmail.com

Poonima U., Department of Electronics and Communication Engineering, Narayanganuru college of Engineering, Manjalumoodu, India.
Email: Poonimau1991@gmail.com

Blessy J., Department of Electronics and Communication Engineering, Narayanganuru college of Engineering, Manjalumoodu, India.
Email: bressyben298@gmail.com

Published By:
Blue Eyes Intelligence Engineering & Sciences Publication

ISSN: 2277-3878, Volume-8 Issue-5, January 2020

International Journal of Recent Technology and Engineering (IJRTE)
II. LITERATURE SURVEY

Haoliang Li et al. proposed a paper on Learn Convolutional Neural Network for Face Anti-Spoofing. In spite of the fact that having accomplished a few advances, the hand-created surface highlights, e.g., LBP LBP-TOP are still unable to catch the most discriminative cues between genuine and fake appearances. In this paper, rather than planning, instead of designing features by themselves, they depend on the deep convolutional neural network (CNN) to learn features of high discriminative capacity in a directed way. Joined with certain information pre-handling, the face against ridiculing execution improves radically. [7] In the tests, over 70% relative lessening of Half Total Error Rate (HTER) is accomplished on two testing datasets, CASIA and REPLAY-ATTACK contrasted and the - state-of-the-art. In the interim, the experimental results from inter-tests between two datasets show CNN can get highlights with better generalization capacity. Additionally, the nets prepared to utilize consolidated information from two datasets have fewer predispositions between two datasets.

A Performance Evaluation of Convolutional Neural Networks for Face Anti Spoofing was proposed by Li, Lei et al. The recently evolved advanced Convolutional Neural Network (CNN) based profound learning system has demonstrated as one of the excellent methods to manage the visual data adequately. CNN learns the various leveled highlights at the middle layers naturally from the information. A few CNN based methods, for example, Inception and ResNet have indicated exceptional execution for image classification problems. In this does an exhibition assessment of CNNs for face antspoofing. [8] The Inception and ResNet CNN architectures are utilized in this examination. The outcomes are computed over the benchmark MSU mobile Face Spoofing Database. The investigations are finished by considering the various perspectives, for example, the depth of the model, irregular weight initialization versus weight transfer fine-tuning vs from scratch training and distinctive learning rate. The study claims great results are gotten using these CNN architectures for face antspoofing in various settings.

A Biometric Face Presentation Attack Detection with Multi-Channel Convolutional Neural Network paper was proposed by Anjith George, Zohreh Mostaani, David Geissenbuhler, Olegs Nikisins, Andre Anjos ’ and Sebastien Marcel. [9] they argue that analysis in multiple channels might help to address this issue. In this context, we propose a multi-channel Convolutional Neural Network-based approach for presentation attack detection (PAD). We also introduce the new Wide Multi-Channel Presentation Attack (WMCA) database for face PAD which contains a wide variety of 2D and 3D presentation attacks for both impersonation and obfuscation attacks. Data from different channels such as color, depth, near-infrared and thermal are available to advance the research in face PAD. The proposed method was compared with feature-based approaches and found to outperform the baselines achieving an ACER of 0.3% on the introduced dataset. And they made a database and the software to reproduce the results are made available publicly.

M. Shamim Hossain et al. proposed a deep architecture for face liveness detection that uses a combination of texture analysis and a convolutional neural network (CNN) to classify the captured image as real or fake. Our development greatly improved upon a recent approach that applies nonlinear diffusion-based on an additive operator splitting scheme and a tridiagonal matrix block-solver algorithm to the image, which enhances the edges and surface texture in the real image. We then fed the diffused image to a deep CNN to identify the complex and deep features for classification. We obtained 100% accuracy on the NUAA Photograph Impostor dataset for face liveness detection using one of our enhanced architectures. [10] Further, we gained insight into the enhancement of the face liveness detection architecture by evaluating three different deep architectures, which included deep CNN, residual network, and the inception network version 4. We evaluated the performance of each of these architectures on the NUAA dataset and present here the experimental results showing under what conditions an architecture would be better suited for face liveness detection. While the residual network gave us competitive results, the inception network version 4 produced the optimal accuracy of 100% in liveness detection.
### III. PROPOSED METHOD

The proposed system uses a color texture analysis-based face anti-spoofing. Face spoofing attacks are most likely performed by displaying the targeted faces using prints, video displays or masks to the input sensor. The proposed system is shown in Fig. 1. It has two phases namely training and testing. In training phase, the Convolutional Neural Network (CNN) is trained with the videos from the database initially the video files are split into individual frames after extracting frames the faces of the person are cropped after that the features from the faces are extracted that extracted features are used to train CNN. In the testing phase, the trained CNN is tests the testing video to evaluate the performance of the system.

#### A. Frame Extraction

This paper uses a content analysis-based method to extract the frames from the video input. In this method, keyframes are extracted on the basis of the color, texture and other valuable visual information of each frame. All the frames of the video in which this information is changing significantly are considered as the keyframes. In this approach, the first frame is selected as the new frame and hence the reference frame, the next subsequent frames are then compared with the reference frame in order. [11] Kth frames become the new frame if and only if the distance between the Kth frame and the reference frame exceeds some predefined threshold. From this description, it is clear that this method selects the keyframe on the basis of the degree of change in the content of the frame.

#### B. Histogram Orient Gradient (HOG)

HOG features, which were associated with image segmentation are registered by counting the events of angle direction in limited parts of a picture. HOG features depend on the way that the appearance and state of the facial features can be delineated by the dissemination of force inclinations. [12] The includes so obtained are significantly discriminative and speak to a picture trademark dependably. Impressed by the critical outcomes for inclination affirmation, we have used HOG features for picture segmentation.

Let \( v \) be the non-normalized vector containing all histograms in a given block \( ||v||_1 \) be its k-nor for k=0, 1, 2 and e be some small constant. Then the normalization factor can be one of the following:

\[
L2 \text{ norm: } f = \frac{v}{||v||_2 + e^2} \\
L1 \text{ norm: } f = \frac{v}{||v||_1 + e} \\
L1 \text{ Sqt: } f = \frac{v}{\sqrt{||v||_1 + e}}
\]

#### C. Local Binary Patterns (LBP):

LBP is a sort of visual descriptor utilized for characterization in PC vision. LBP operator is frequently utilized to the greyscale picture, where a code is performed for every pixel. But in our proposed system the LBP operator is used for color image for that initially the R, G and B component of the image is extracted separately and stored in a matrix after that the LBP is applied to the R, G, and B components separately. For instance, when thinking about a cell of 3x3 pixels, the focal pixel is looked at to neighbor pixels. Any order of pixels is conceded, be that as it may, thus the begin is the upper left pixel, when utilizing clock-wise course. In the event that the estimation of the center pixel is littler than or on the other hand equivalent to the estimation of the neighbor then an “1” will be taken into the record, generally a “0” is considered.[13] The resulted value is a binary number that is associated with a pattern. A weight is doled out to every digit of the got double number and a comparing thing can be determined.

#### D. Compound Local Binary Pattern (CLBP)

The original LBP operator discards the magnitude information of the difference between the center and the neighbor gray values in a local neighborhood. As a result, this method tends to produce inconsistent codes.[14]One example is shown in Figure 3. Here, the 8-bit uniform LBP code (11111111) corresponds to a flat area or a dark spot at the center pixel [16], which is not correct in this case.

As the LBP operator considers only the sign of the difference between two gray values, it often fails to generate appropriate binary code. Being motivated by this, we propose CLBP, an extension of the original LBP operator that assigns a 2P-bit code to the center pixel based on the gray values of a local neighborhood comprising P neighbors. Unlike the LBP that employs one bit for each neighbor to express only the sign of the difference between the center and the corresponding neighbor gray values, the proposed method uses two bits for each neighbor in order to represent the sign as well as the magnitude information of the difference between the center and the neighbor gray values. Here, the first bit represents the sign of the difference between the center and the corresponding neighbor gray values like the basic LBP pattern and the other bit is used to encode the magnitude of the difference with respect to a threshold value, the average magnitude (Mavg) of the difference between the center and the neighbor gray values in the local neighborhood of interest. [19] The CLBP operator sets this bit to 1 if the magnitude of the difference between the center and the corresponding neighbor is greater than the threshold \( M_{\text{avg}} \). Otherwise, it is set to 0. Thus, the indicator \( s(x) \) of (2) is replaced by the following function:
Face Spoofing Detection using Mixed Feature with Deep Convolutional Neural Networks

\( s(i_p, i_c) = \begin{cases} 0 & i_p = i_c < 0, |i_p - i_c| \leq M_{avg} \\ 1 & i_p = i_c < 0, |i_p - i_c| > M_{avg} \\ 10 & i_p = i_c \geq 0, |i_p - i_c| \leq M_{avg} \\ 11 & Otherwise \end{cases} \) (4)

Here, \( i_c \) is the gray value of the center pixel \( i_p \) is the gray value of a neighbor, and \( M_{avg} \) is the average magnitude of the difference between \( i_p \) and \( i_c \) in the local neighborhood.

\[ \text{Contrast} = \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} (x - y)^2 f(x, y) \] (5)

\[ \text{Energy} = \sum_{p=0}^{i-1} \sum_{q=0}^{j-1} f^2(p, q) \] (6)

\[ \text{Correlation} = \frac{\sum_{p=0}^{i-1} \sum_{q=0}^{j-1} (p - q)(f(p, q) - M_{p,q})}{\sigma_{p,q}} \] (7)

\[ \text{Homogeneity} = \frac{1}{\sum_{p=0}^{i-1} \sum_{q=0}^{j-1} (1 + (p - q)^2 f(p, q))} \] (8)

E. **Gray Level Co-Occurrence Matrix (GLCM):**

Image composed of several pixels and each pixel having its own intensity level. The Grey Level Co-occurrence matrix [15] is a method of tabulating the pixels with different intensity levels. It is the most classical second-order statistical method for texture analysis. GLCM improves the accuracy level by choosing an effective quantitative level for early diagnosis. In the first step, the first-order statistical textural analysis-features information of the image was extracted and frequencies of the gray level at a random image position were measured without considering neighbor pixels. In the second step, the second-order textural analysis-features were extracted by considering neighbor pixels. The statistical features were extracted using GLCM, also known as gray-level spatial dependence matrix (GLSDM). GLSDM is an approach that describes the spatial relation between pixels of various gray-level values. Gray-level co-occurrence matrix (GLCM) is a 2D histogram in which \((p, q)\)th elements is the frequency of event \( p \) occurs with \( q \). It is a function of distance \( S=1 \), angle at 0° (horizontal), 45° (with the positive diagonal), 90° (vertical) and 135° (negative diagonal) and gray scales \( p \) and \( q \), and calculates how often a pixel with intensity \( p \) occurs in relation with another pixel \( q \) at a certain distance \( S \) and orientation. In the GLCM method, the gray-level co-occurrence matrix has the textural features such as contrast, correlation, energy, homogeneity, entropy, and variance were obtained from LL and HL subbands of first four levels of the wavelet decomposition. The textural features extracted are listed below.

\[ \text{Contrast} = \sum_{x=0}^{m-1} \sum_{y=0}^{n-1} (x - y)^2 f(x, y) \] (5)

\[ \text{Energy} = \sum_{p=0}^{i-1} \sum_{q=0}^{j-1} f^2(p, q) \] (6)

\[ \text{Correlation} = \frac{\sum_{p=0}^{i-1} \sum_{q=0}^{j-1} (p - q)(f(p, q) - M_{p,q})}{\sigma_{p,q}} \] (7)

\[ \text{Homogeneity} = \frac{1}{\sum_{p=0}^{i-1} \sum_{q=0}^{j-1} (1 + (p - q)^2 f(p, q))} \] (8)

*Fig.4. CNN Architecture*

**F. Convolutional Neural Network (CNN)**

A legitimate choice of network architecture is crucial to CNNs. Our deep CNN shares the basic architecture of the classical LeNet-5. The proposed method uses 2 convolution layer former layers will repeat 32 times and the latter will 64 times. Fig.4. shows the structure of CNN which is proposed in this work.

*Fig.4. CNN Architecture*

**a.) Convolution layers:**

The Conv layer is the inside structure square of a Convolutional Network that does most of the computational hard work. The CONV layer’s parameters contain a lot of learnable filters. Each channel is little, spatially (along width and stature), yet reaches out through the full profundity of the info volume.[16] For instance, an average channel on the first layer of a ConvNet may have estimate 32x32x3 (for example 32 pixels width and stature, and 3 on the grounds that the pictures have profundity 3, the shading channels). During the forward pass, we slide (even more unequivocally, convolve) each channel over the width and height of the information volume and process dot products between the channels and the commitment at any position. As we slide the filter over the width and tallness of the info picture we will convey a 2-dimensional incitation map that gives the responses of that channel at each spatial position.

**b.) Pooling layer:**

A Pooling layer intermittently embeds in the middle of progressive Conv layers in a ConvNet architecture. Its capacity is to continuously diminish the spatial size of the portrayal to decrease the measure of parameters and computation in the system, and subsequently to likewise control overfitting. Max or Average pooling is used as a pooling layer. Max pooling returns maximum value and Average pooling returns average of all values from the portion of the image. Our network uses the Max pooling layer.

**a.) Classification Layer:**

The classification layer consist of one or two fully connected layers. It is Shoddy methods for learning non-direct blends of the abnormal state feature as presented by the yield of the ordinary Layer. Our network contains two fully connected layers.
First, a fully connected layer takes the feature maps of the second convolution layer as input. The final fully connected layer is the output it takes input from the previous fully connected layer. [17] The flattened output is sustained to a feed-forward neural system and backpropagation connected to each iteration of training. Over a progression of epochs, the model can recognize overwhelming and certain low-level features in images and group them utilizing the Softmax Classification procedure.

b.) CNN Training

Due to the non-arched property of the cost capacity of deep CNNs, suitable setting network training parameter is essential for the smooth converge to the solution. Our deep CNN is parameterized by the weights and biases of different convolutional layers and fully-connected layers. In our Deep CNN, for feature extraction, the histogram of oriented gradients HOG and LBP methodologies are used. The hog strategy includes occasions of inclination direction in confined segments of a picture. LBP technique is a texture operator that names the pixels of a picture by thresholding the area of each pixel and sees the yield as a double number. The average of this both outputs are fed to train CNN.

IV. RESULT AND DISCUSSION

The proposed face spoofing detection model is implemented in MATLAB 2018a in an i5 system with 4 GB RAM. In this work, we have used the Replay-Attack database. Performances of the model is measured in terms of Accuracy, Equal Error Rate (EER) and Half Total Error Rate (HTER). For the analysis purpose, our method is analyzed with the existing methods [18 19 20 21]. The resultant graphs with respect to detection performance are given below. Additionally, Fig 5 shows the sample images used in the anti-face spoof model.

A. Dataset

This paper uses the Replay-Attack database for the training and testing of CNN. The Replay-Attack Database for face spoofing consists of 1300 video clips of photo and video attack attempts to 50 clients, under different lighting conditions. This Database was produced at the Idiap Research Institute, in Switzerland. All videos are generated by either having a (real) client trying to access a laptop through a built-in webcam or by displaying a photo or a video recording of the same client for at least 9 seconds. The webcam produces color videos with a resolution of 320 pixels (width) by 240 pixels (height). Fig 5. shows some sample images from the databases.

![Sample images from Replay-Attack database](image)

B. Evaluation Metrics

a.) Equal Error Rate

Equal error rate or crossover error rate (EER or CER): the rate at which both acceptance and rejection errors are equal. The value of the EER can be easily obtained from the ROC curve. The EER is a quick way to compare the accuracy of devices with different ROC curves. In general, the device with the lowest EER is the most accurate.

b.) Half Total Error Rate

A classifier is subject to two types of errors, either the event one wishes to detect is rejected (false negative) or a noise or background one wishes to discard is accepted (false positive). A possible way to measure the detection performance is to use the Half Total Error Rate (HTER), which combines the False Negative Rate (FNR) and the False Positive Rate (FPR) and is defined in the following formula:

\[
\text{HTER}(\tau, D) = \frac{\text{FPR}(\tau, D) + \text{FNR}(\tau, D)}{2}
\]

(9)

c.) Accuracy

Accuracy of a system is defined as the ratio between a numbers of correct predictions to the total number of predictions. Table - I show that the proposed system yields high accuracy rather than the other methods.

\[
\text{Accuracy} = \frac{TP + TN}{(TP + TN + FP + FN)}
\]

(10)

C. Results

The anti-spoofing systems to discriminate between real accesses and spoofing attacks, anti-spoofing can be regarded as a binary classification problem. The spoofing databases and the evaluation methodologies for anti-spoofing systems most often comply with the standards for binary classification problems. However, the anti-spoofing systems are not destined to work stand-alone, and their main purpose is to protect a verification system from spoofing attacks. In the process of combining the decision of an anti-spoofing and a recognition system, effects on the recognition performance can be expected. Table-I gives the performance of the proposed system.

<table>
<thead>
<tr>
<th>Method</th>
<th>Accuracy</th>
<th>EER</th>
<th>HTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proposed</td>
<td>0.92</td>
<td>0.6</td>
<td>1.3</td>
</tr>
<tr>
<td>[18]</td>
<td>0.87</td>
<td>0.7</td>
<td>3.1</td>
</tr>
<tr>
<td>[19]</td>
<td>0.88</td>
<td>0.9</td>
<td>4.9</td>
</tr>
<tr>
<td>[20]</td>
<td>0.9</td>
<td>2.9</td>
<td>4.3</td>
</tr>
<tr>
<td>[21]</td>
<td>0.82</td>
<td>4.6</td>
<td>1.7</td>
</tr>
</tbody>
</table>

![Performance of the Proposed System](image)

Fig 6. Shows the performance of the proposed system. From fig.6, it is clear that our proposed system performs better than the other existing methods.
Fig. 6. Performance of the proposed system

V. CONCLUSION

In this paper, a highly accurate face spoof detection system using multiple features and deep learning is proposed. The input video is broken into frames using content-based frame extraction. From each frame, the face of the person is cropped. From the cropped images multiple features like HoG, LBP, CSLBP, and GLCM are extracted to train CNN. Training and testing are performed separately by using collected sample data. From the evaluation result, it is clear that the proposed algorithm obtained the highest accuracy of 92% percentage it is higher when compared to the conventional algorithms.

REFERENCES


AUTHORS PROFILE

Jesslin Melba N V, received Masters Degree in Communication Systems from Anna University Chennai, India. Presently a full time Assistant Professor in ECE Department of the Narayanaguru College of Engineering, Tamil Nadu India. Her Area of Interest includes Image Processing and Neural Networks.

Porunima U, currently pursuing thedegree in Applied Electronics at Narayanaguru College of Engineering, Anna University Chennai, India. Her Area of Interest includes Bio-Metrics and Medical Image Processing.

Blessy J, received Masters Degree in Communication Systems from Anna University Chennai, India. Presently a full time Assistant Professor in ECE Department of the Narayanaguru College of Engineering, Tamil Nadu India. Her Area of Interests includes Image Processing and Wireless Communication.