iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** IX **Month of publication:** September 2022

DOI: https://doi.org/10.22214/ijraset.2022.45829

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue IX Sep 2022- Available at www.ijraset.com

Fake Face Detection Using CNN

Priyadarshini Patil[1], Vipul Deshpande[2], Vishal Malge[3], Abhishek Bevinmanchi[4]
[1]*Professor,* [2, 3, 4]*Student, Computer Science and Engineering, PDA College of Engineering, Gulbarga, India*[1]

Abstract: ***Real and Fake face recognition using CNN and deep learning is presented in the paper. Searching for the authenticity of an image with the naked eye becomes a complicated task in detecting image forgeries. The goal of this study is to evaluate how well different deep learning approaches perform. The initial stage of the proposed strategy is to train several pre-trained deep learning models on the image dataset for recognizing real and fake images to identify fake faces. In order to assess the effectiveness of these models, we consider how well they separate two classes - false and true. Regarding the models tested so far, the VGG models have the best training accuracy (86%) on VGG-16, while VGG-16 shows an excellent test set. accuracy with 10 epochs or less, which is competitively better than all other methods. The outputs of these models were examined to find out exactly.***

Keywords*: CNN: Convolution Neural Network, VGG- 16: Visual Geometry Group 16.*

I. INTRODUCTION

Image forensics is a method to determine whether an image is genuine or has been tampered with. With hundreds of photos, it was difficult to discern the reality behind each one. Many feature extraction approaches for image processing and computer vision are effective when features are taken from related images and trained using deep learning models. Deep learning is a machine learning method that uses learned information to solve related problems. Pre-trained models are among the most commonly used deep learning techniques. These models are sophisticated and can increase the effectiveness of the model because they have been trained on large datasets. For the "Real and Fake Face Detection" dataset, which contains much fewer photos, we use these pre-trained models in this study. In order to identify thousands of different categories, deep learning models are pre-trained on millions of photos; if we talk about classifying real and fake photos then we have two categories to categorize.

Another element of deep learning is the ability to refine and reuse previously learned models. We modify the pre-trained model and replace its output layers with CNN layers in accordance with the categorization required by the categories of the supplied dataset. Machine learning algorithms are used in a variety of ways to identify the legitimacy of an image. A particularly powerful deep learning method that classifies data provided for a specific job is a convolutional neural network.

[1] Exist fake face recognition used to describe something that is now using capsule networks to detect fake images and videos uses a method that uses a capsule network to detect fake, manipulated images and videos in various scenarios such as detecting replay attacks playback and computer. Detection of generated video. Detecting fake AI-generated videos using eye blink detection describes a new method for detecting fake face videos generated using deep neural network models. The method is based on the detection of eye blinks in videos, which is a physiological signal that is not well represented in synthesized fake videos.

[2] a slight modification of the existing task that takes a dataset of fake and real images as input and is trained with a CNN algorithm and a model is built. A performance evaluation is performed and accuracy and loss are calculated and graphs are displayed.

The trained model is used in a web application that is developed using the flask framework and is given an input image to check whether the image is fake or real.

There are many tools available to create DF, but almost no tool is available to detect DF. [2] Our approach to DF detection will be of great benefit in preventing DF from infiltrating the global network. We will provide a web platform for the user to upload an image and classify it as fake or real.

II. LITERATURE SURVEY

[3] Anti-forensic facial approaches now face a new threat due to the rapid growth of Generative Adversarial Networks (GAN(GAN)). Many apps use GAN to create fake photos and videos, which can lead to identity theft and privacy issues. They proposed a deep convolutional neural network for forensic face identification in this study. To augment the data, we use GANs to generate dummy faces in different sizes and resolutions. We also add weight to our effective facial feature extraction technology using a deep facial recognition algorithm. The network is also improved to be suitable for real and fake image classification. We ran experiments using validation data from the AI Challenge and had successful results.

[4] The use of AI technology to create realistic human faces has advanced rapidly in recent years. Such false faces can be used as a weapon with harmful personal and social effects. By sabotaging potential training data, they create systems to protect people from falling prey to current AI-generated scam movies. This is achieved by degrading the quality of the discovered faces by interfering with the deep neural network (DNN) based face identification algorithm using specifically designed unobservable enemy perturbations. They discuss attack strategies in white-box, gray-box, and black-box situations with progressively less knowledge about DNN-based face detectors in each case. They empirically demonstrate on different datasets how well our techniques disrupt state-of-the-art DNN-based face detectors.

[5] In this work, the authors provide a novel deep learning-based system that can successfully identify authentic movies and artificial intelligence-generated fake videos (hence referred to as DeepFake videos). Our approach is based on the realization that the DeepFake algorithm in its current form can only produce finite-resolution images, which must be further warped to match the original faces in the source video. Such transformations produce various artifacts in the final DeepFake movies and show how convolutional neural networks (CNNs) can effectively capture them. Our technique does not need photos created by DeepFake as negative training examples, unlike other approaches that did, because we focus on artifacts in affine facial distortion as a distinguishing characteristic to separate real and fake images. Our approach has two key advantages: (1) By performing basic image processing operations on the image to create a negative example, such artifacts can be directly replicated. Our technique saves a lot of time and money by eliminating the need to train the DeepFake model to create negative instances; (2) since these artifacts are often present in DeepFake movies from many sources, our method is more reliable than others. Two sets of DeepFake video datasets are used to assess the practical utility of our technique.

[6] Today's authentication methods use the user's biometrics as credentials. Use biometric data as an authentication mechanism to provide a higher level of security, but biometric data has become the target of several attacks. One type of biometric attack is facial spoofing. This research offers a fake face detection algorithm based on color texture analysis. The main topic of this essay is facial falsification in images and videos. In this case, use color spaces to extract regional texture and distortion properties. Then collect all the feature values to train the SVM. Here, a supervised machine learning method called SVM is used to distinguish between real and fake faces.

III. METHODOLOGY

VGG-16 - This study proposes a VGG model based on a convolutional neural network deep learning model for target identification and location. This model has a pre-trained version called the VGG-19 trained network. [Giant. 1] The parameters of the pre-trained model optimize the parameters of the convolutional layer model and solve the classification problem of rice leaf disease detection by fine-tuning the transfer learning approach. The three FC layers are the primary focal points for VGG-19 parameters. To avoid this, it is recommended to use three fully bonded layers of VGG-19 rather than one Flatten layer and two fully bonded layers.

The merged layer is introduced because the convolutional layer cannot be connected directly to the Dense layer, which is completely connected. Using transfer learning, the parameters of the pre-trained VGG-19 model are transferred to the convolutional layer of the rice disease detection model, the pooling layer and the fully connected layer, replacing the original 2-label SoftMax classification layer, sparse functions through omission, maximum number pooling and matching the detection model .

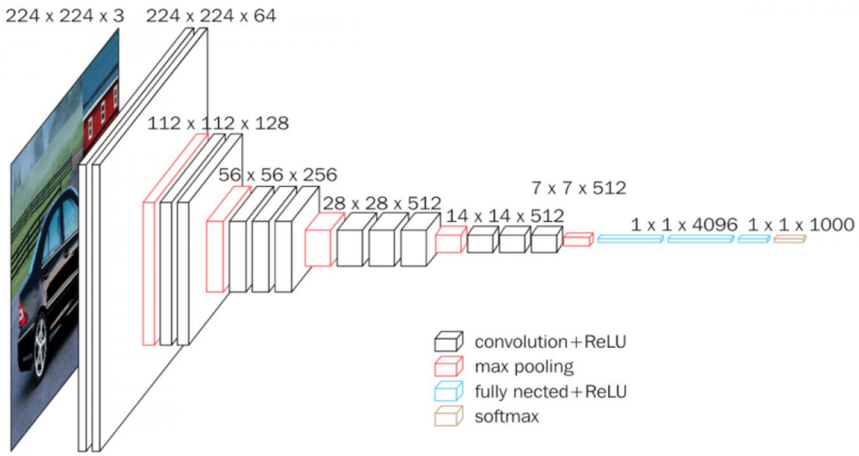


Fig- 1

Working with CNN: Convolutional neural networks, a kind of artificial neural networks, are used in computer vision. A CNN was used to reduce the size of the images using convolutional and pooling layers before sending the reduced input to the fully connected layers. [Fig-2] A deep learning system called Convolutional Neural Network (ConvNet/CNN) can take an image as input, assign meaning (learnable weights and biases) to various characteristics and objects in the image, and then discriminate between them. Compared to other classification methods, ConvNet needs much less pre-processing. The basic techniques require human filter engineering, but ConvNets can learn these filters and attributes with enough practice. The structure of ConvNet is based on how the visual cortex is set up and resembles the connections between neurons in the human brain. Individual neurons can only respond to information in a small area of the visual field called the Receptive Field. To fully occupy the field of view, many equivalent fields can be stacked on top of each other.

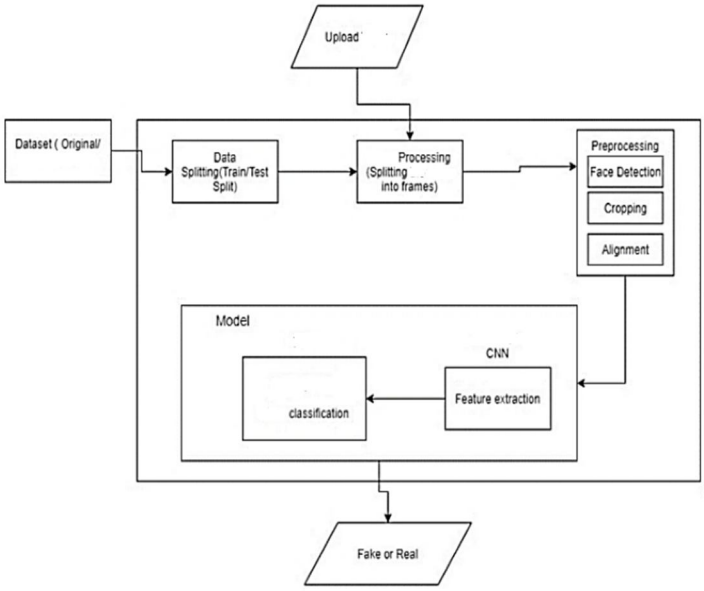
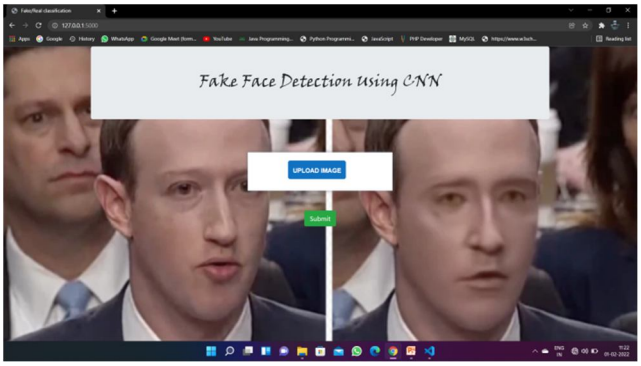


Fig- 2

Using input datasets of dummy and authentic images, the image is first preprocessed and then smoothed. This process improves image quality while reducing image noise. The input image serves as the starting point for the feature extraction network. Facial feature extraction is necessary to initiate processing techniques such as face tracking, facial expression detection, or face recognition. The images are trained using a CNN algorithm to evaluate whether the input image is a real face or a synthetic face.



Due to the fact that this project includes two datasets—one false and the other real—each including 1500 photos. The accuracy of these pictures may be increased to 86 percent by further training them at 10 Epoch. The value of accuracy grows along with the epoch. because CNN is the only inspiration for my endeavour. In order to implement the system quickly, a graphic card is required; otherwise, it will take 10 epoch and up to 5-8 hours to train the pictures. [Table-1] The precision of the duration with regard to epoch is described in this table. [Fig-3] Both train loss and val loss have been applied to this graph. since accuracy is a concern. The graph in [Fig. 4] has also completed train accuracy and val accuracy tests.

Table -1

EPOCH	ACCURACY	DURATION(hr)
5	53 %	2-3
7	71 %	3-5
10	86 %	8-10
20	93 %	20-25

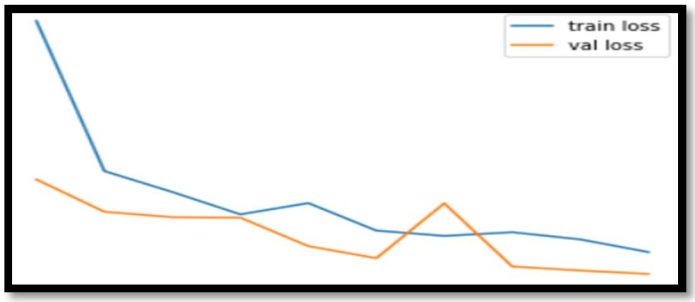


Fig-3

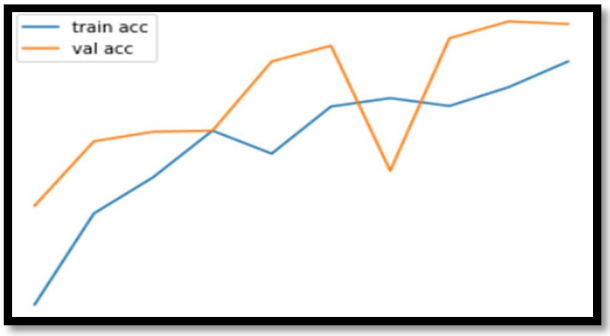


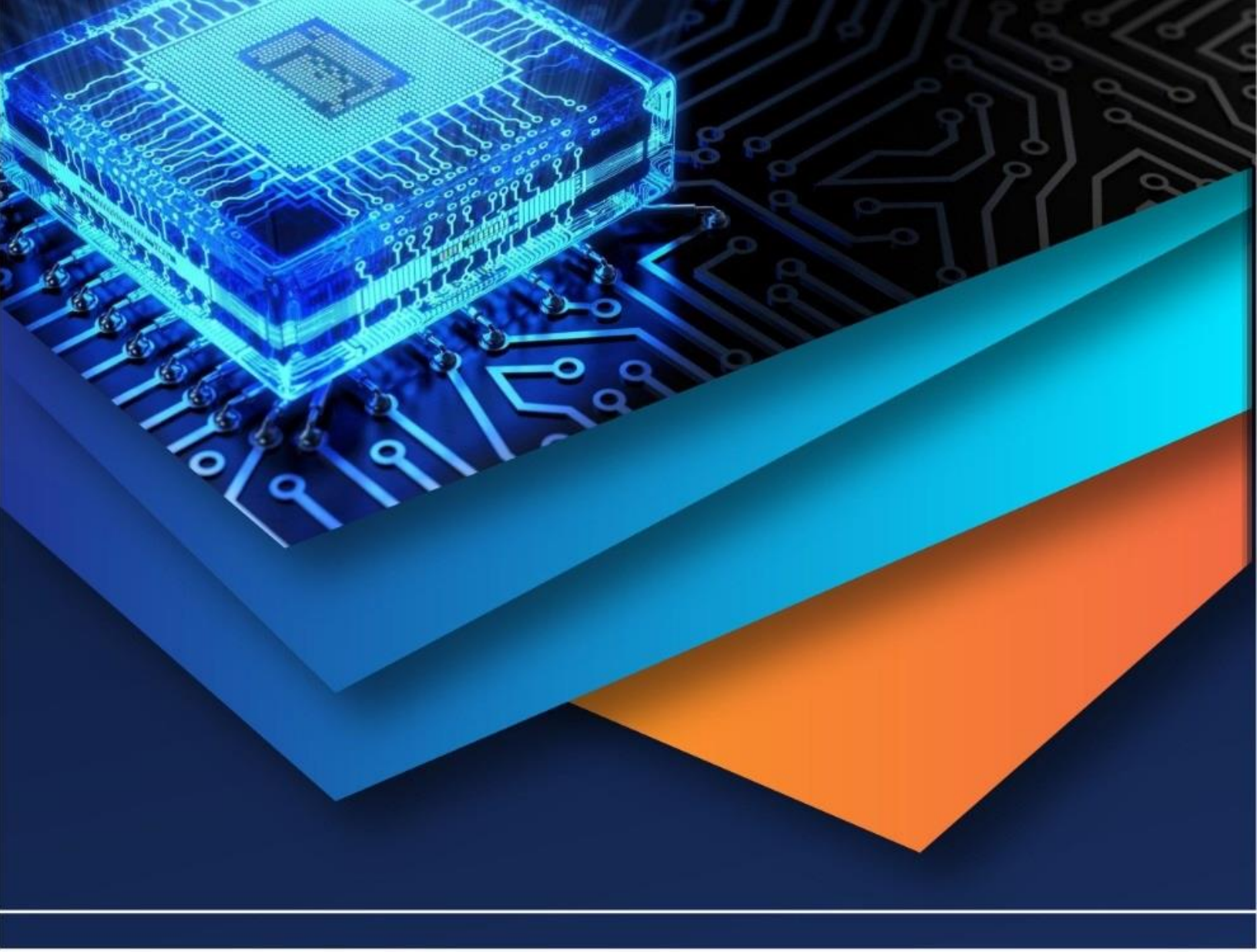
Fig- 4

IV. CONCLUSIONS

In order to identify authentic and fake photos, this study compares several state-of-the-art pre-trained deep learning models. Using the original and saved versions of photos from the "Real and Fake Face identification" dataset from the Computational Intelligence Photography Lab, Yonsei University, we used ELA to identify and authenticate the images. Compared with other pre-trained models on the same data sets, we found that both VGG 16 and 19 provide excellent training accuracy of 91.97 percent and 92.09 percent, but VGG-16 provides 64.49 percent test set accuracy. In a future study, we want to generalize our findings. To distinguish between fake and real images using live video recognition, we propose a CNN architecture using different feature extraction techniques. This will provide the highest accuracy on many data sets.

REFERENCES

[1] Yuezun Li, Siwei Lyu, “ExposingDF Videos By Detecting Face Warping Artifacts,” in arXiv:1811.00656v3.
[2] Yuezun Li, Ming-Ching Chang and Siwei Lyu “Exposing AI Created Fake Videos by Detecting Eye Blinking” in arxiv.
[3] Tai Do Nhu, In Na, and S.H. Kim. Forensics face detection from gans using convolutional neural network, 2018.
[4] Yuezun Li, Xin Yang, Baoyuan Wu, and Siwei Lyu. Hiding faces in plain sight: Disrupting ai face synthesis with adversarial perturbations, 2019.
[5] Yuezun Li and Siwei Lyu. Exposing deepfake videos by detecting face warping artifacts, 2018.
[6] 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.
[7] Huy H. Nguyen , Junichi Yamagishi, and Isao Echizen “ Using capsule networks to detect forged images and videos ”.
[8] Hyeongwoo Kim, Pablo Garrido, Ayush Tewari and Weipeng Xu “Deep Video Portraits” in arXiv:1901.02212v2.
[9] Umur Aybars Ciftci, ˙Ilke Demir, Lijun Yin “Detection of Synthetic Portrait Videos using Biological Signals” in arXiv:1901.02212v2.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY