International Journal of Modern Developments in Engineering and Science
Volume 2, Issue 4, April 2023
https://www.ijmdes.com | ISSN (Online): 2583-3138

Deepfake Detection Using Deep Learning

Jayshri Mankar[1], Shriyash Ingle[2*], Tejas Dalvi[3], Abhishek Bhalerao[4], Manasi Pol[5]

[1]*Professor, Department of Computer Engineering, Genba Sopanrao Moze College of Engineering, Pune, India*

[2,3,4,5]*Student, Department of Computer Engineering, Genba Sopanrao Moze College of Engineering, Pune, India*

***Abstract*: Four billion images are uploaded to the internet every day, according to polls. With the widespread use of digital photography, new methods for modifying image content employing tools, apps, and editing software like Adobe's have emerged. Deepfake techniques were used to create a fake movie and photos, which has raised significant public concern. The majority of face-manipulation techniques used in videos today, such as Faceswap and Deepfake, have been created successfully. It has both benefits and drawbacks. On the one hand, it broadens the application to new fields (such as visual arts, visual studies, filmmaking, etc.), but on the other, it also fosters harmful users. Consequently, we can determine whether the video is real or not by applying Deep Learning algorithms. We're going to create a system that can identify this dangerous data in order to recognise it.**

***Keywords*: Deep Learning, Faceswap, DeepFake, DeepFake techniques.**

1. Introduction

Deepfakes are AI-generated or generative works of art in which the image of a person in an earlier work of art is changed to that of another person. Since deepfakes are being used more frequently to produce various types of fake information, from fake news to humbug of content, such as pornography, ragging, etc., both academic fields and the technology industry have made significant efforts to develop machine controllable detection of deepfake videos. After being deemed to be reliable sources, photos and videos are frequently used as evidence in criminal investigations to resolve legal disputes. Female reporters and journalists have already been threatened with deep-fake porn movies. Because of this, this project will contribute to the security of every woman's future. Our goal is to find harmful data so that we can honesty and keep person in protection.

A. Deep Learning

Computer and machine vision, as well as natural language processing, have all made extensive use of the effective and practical Deep Learning technique. This technology is used by Deepfakes to alter pictures and videos of people so that it is impossible for people to tell whether they are real or fake.

2. Related Work

The deepfake was mint from the affiliation of Deep Learning, fake videos created using deepfakes consists of two parts, face swapping and face reenactment. Face swapping has automatic replacement of a face in a video or image with someone else's face. This original Face swapping method can be dated by to a Reddit user post in 2017. Faceswap-GAN is a popular faceswap method. Face reenactment is a transferal of expression and pose of fake person to a targeted person in a video, while the specification of the target person remains the same using Dliband OpenCV it first detects the face in the fake image with the face detector. There have been several works considering deepfake video detection methods. For eg., The blinking rate of human beings is about once every two to ten seconds and the time for each blink about half or a quarter of a seconds. People in a deepfake videos rarely blink, making deepfake videos a bit more detectable from real videos. Apart from the manipulated contents itself, some other variable created as byproducts of the natural process can be used for deepfake detection. Compare to manual detection done by humans, Convolutional Neural Network's (CNN's) can detect deepfake contents through image analysis feature neural networks allows computers to learn from features that can be hardy noticeable human eyes.

3. Dataset

Fake videotape data (UADFV) fake image data (DARPAMedi for GAN image or videotape challenge). Face forensic, deepfake, computer generated images, and photographic images. Datasets that contain colorful face images with different judgments. Face Forensics++ provides a dataset consisting of 1000 original video sequences that have been manipulated based on four automated using different face manipulation methods, namely: Deepfakes, Face2Face, Face Swap and Neural Textures. These 5000 videos were downloaded to the University of Melbourne High Performance Computing System (SPARTAN) [24]. All h264 videos were downloaded using a 23x compression rate for time and storage efficiencies. The original videos, and the deep fake versions of these videos created using Deepfakes, Face2Face, FaceSwap and Neural Textures.

4. Methodology

Firstly, have to take a video to detect is it fake or not. After that the first step is to capture the input video into frames. The frame rate is of 30 frames per second. The second step was to detect the faces that appear in the image and label them. The

*Corresponding author: shriyash.ingle@gmail.com third step was to save the detected area of the face as a new image.

A. CNN

CNN is a type of deep literacy model for processing data that has a grid pattern, similar as images, which is inspired by the association of beast visual cortex and designed to automatically and adaptively learn spatial scales of features, from low-to grandly- position patterns. CNN is a fine construct that's generally composed of three types of layers (or erecting blocks) complication, pooling, and completely connected layers.

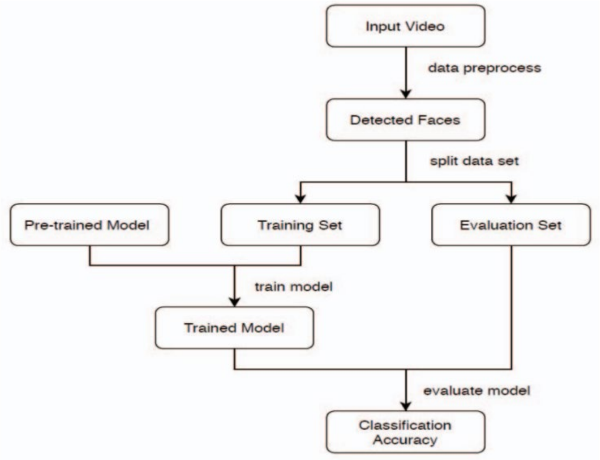

Fig. 1. Overall process flowchart

1. Convolution Layer is an abecedarian element of the CNN armature that performs point birth.
2. Pooling Subcaste provides a typical down sampling operation which reduces the in-aeroplane dimensionality.
3. Completely Connected Subcaste affair point charts of the final complication or pooling subcaste is generally smoothed.

5. Proposed Outcomes

The expected outcome from the system is to detect original and fake image frames on video as well as at the end to detect percentage i.e., how much percent video is real or fake.

It is not unusual to find deepfake videos where the manipulation is only present in a small portion of the video (i.e., the target face only appears briefly on the video).

6. Conclusion

Deepfake has become more famous because of large and upcoming availability of content in social media. This is specifically imp nowadays because the tools for making deepfakes are becoming more easily available and social media easily allowed people to share fake contents. In this paper, we discuss applications now available and tools that have been used in large quantity to create fake content. Then we discuss major technique to detect fake video content i.e., CNN (Convolutional Neural Network). Hence the current deep learning methods are successfully detecting fake content.

References

[1] Bayar, B., and Stamm, M. C. (2016, June). A deep learning approach to universal image manipulation detection using a new convolutional layer. In Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security, pp. 5-10.

[2] Zhou, P., Han, X., Morariu, V. I., and Davis, L. S. (2017, July). Two-stream neural networks for tam- pered face detection. In 2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1831-1839.

[3] Yang, W., Hui, C., Chen, Z., Xue, J. H., and Liao, Q. (2019). FV-GAN: Finger vein representation using generative adversarial networks. IEEE Transactions on Information Forensics and Security, 14(9), 2512-2524

[4] Li, Y., Chang, M. C., and Lyu, S. (2018, December). In ictu oculi: Exposing AI created fake videos by detecting eye blinking. In 2018 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1-7.

[5] Guera, D., and Delp, E. J. (2018, November). Deepfake video detection using recurrent neural networks. In 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), pp. 1-6.

[6] Li, Y., and Lyu, S. (2019). Exposing deepfake videos by detecting face warping artifacts. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 46-52.

[7] Nguyen, H. H., Yamagishi, J., and Echizen, I. (2019, May). Capsule-forensics: Using capsule networks to detect forged images and videos. In 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 23072311.