International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Deepfake Detection through Deep Learning

Prof. Kalyani Bodake ,Gauri Khake , Prapti Chavan , Mahesh Rathod

Genba Sopanrao Moze College of Engineering,Balewadi

ABSTRACT :

According to surveys about four billion pictures are uploaded on internet everyday. This lot of use of digital pictures have been followed by new techniquesto edit picture contents by using editing software,tools,apps like adobe. A fake video and images generated by deepfake techniques have become great public issue. These days most of the techniques for face manipulation in videos has been developed successfully like Faceswap,Deepfake,etc. It has both advantages and disadvantages. On one side it increases scope to new areas (eg. Visual arts,Visual Studies, Movie making,etc.) and on other side ,controvert,it also developes malicious users. Therefore by using Deep Learning techniques we can detect the video is real or not. For recognizing these malicious data, we are going to make a system which can find and examine the incurraptability of digital visual media is therefore essential.

Keyword :Deep Learning, Faceswap, DeepFake, DeepFake Techniques

1.INTRODUCTION

Deepfakes are AI generated or generative media in which a person in an existing media is replaced with some one else’s image. The fast growth of deepfakes has made both academic fields and technology industry put significant efforts on machine controllable detection of deepfake videos, after more frequently people are using deepfakes to create many forms of fake information from fake news to humbug of content, eg. Pornography, ragging, etc.

Photos and videos are mostly used as proof in crime investigations to solve legal cases after they are considered to be good sources. Deepfake porn videos have already been used to blackmail female reporters and journalists. That is why this project will help in keeping every women’s future secure. Our objective is to detect malicious data to deal with honesty and keep person in protection.

Deep Learning:

Deep Learning is successful and useful technique that has been broadly applied in a various fields including computer and machine vision and also natural language processing. Deepfakes uses this technology to manipulate images and videos of a person that humans cannot recognize them from real or fake.

RELATED WORK

The deepfake was mint from the affiliation of Deep Learining, 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 reenactmant 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.

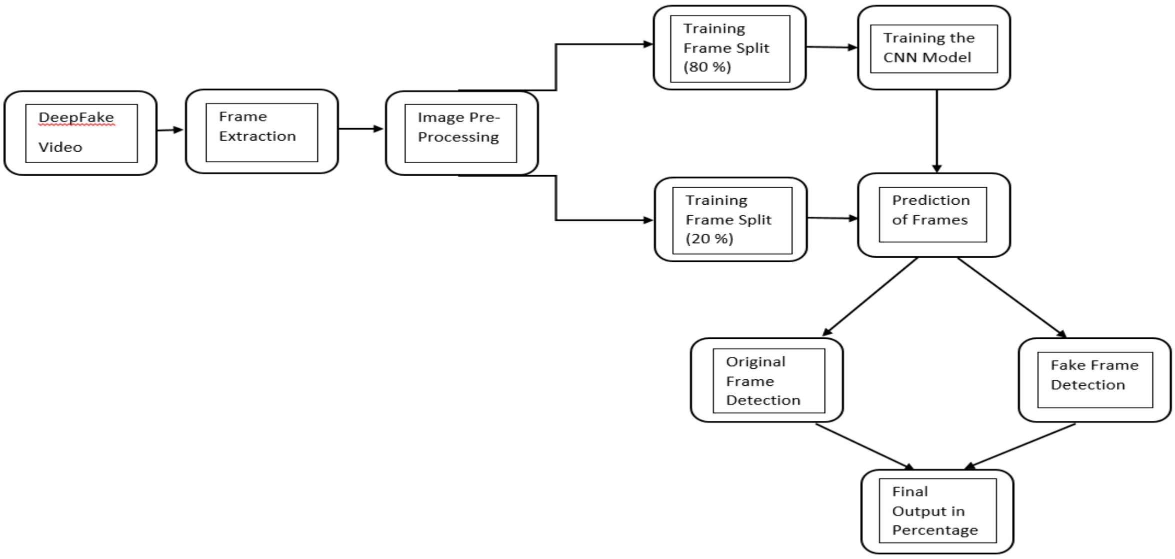
There have been several works considering deepfake video detection methods.Foreg. The blinking rate of human beings is about once every two to ten seconds and the time for each blink about half or a quarter of a seconds. People in a deepfake videos rarey blink, making deepfake videos a bit more detectable from real videos.

Apart from the manipulated contents itself, some other variable created as by products 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.

DATASET

- Fake videotape data (UADFV) fake image data (DARPAMedi for GAN image or videotape challenge).
- Faceforensic, deepfake, computer generated images, and photographic images.
- Datasets that contain colorful face images with different judgments.

METHEDOLOGY



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 third step was to save the detected area of the face as a new image.

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.

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

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).

CONCLUSION

Deepfake has become more famous because of large and upcoming availability of content in social media. This is specifically imp nowdays 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 apllications now availables and tools that have been used in large quantity to create fake content. Then we discuss major technique to detect fake video content i.eCNN(Convolutional Neural Network). Hence the current deep learning methods are successfully detectfakr 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).ACM.

[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).IEEE.

[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).IEEE.

[6] 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).IEEE.

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

[8]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).IEEE.