As per UGC guidelines an electronic bar code is provided to seure your paper

International Journal for Modern Trends in Science and Technology, 8(03):241-243, 2022

ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST0803044
Available online at: http://www.ijmtst.com/vol8issue03.html

Detection of Image Tampering Attacks using Deep Learning

P.Narendra Babu[1] | B.N.Iswarya Lakshmi[1] | Ch.Siri Chandana[1] | I.Satish[1] | V.Pavan Kalyan[2]

[1]Department of CSE, NRI Institute of Technology, Vijayawada, A.P., India.
[2]Professor, Department of CSE, NRI Institute of Technology, Vijayawada, A.P., India.

To Cite this Article

P.Narendra Babu, B.N.Iswarya Lakshmi, Ch.Siri Chandana, I.Satish and V.Pavan Kalyan. Detection of Image Tampering Attacks using Deep Learning. International Journal for Modern Trends in Science and Technology 2022, 8(03), pp. 241-243. https://doi.org/10.46501/IJMTST0803044

Article Info

Received: 16 February 2022; Accepted: 19 March 2022; Published: 24 March 2022.

ABSTRACT

Image Tampering Attacks turn out to be one of the biggest issues in the society these days. Everything that appears on social media is a sensation in this generation. Never blindly trust your eyes, it may seem to be realistic, but it is actually not real. It is the time to flip the coin to the other side and understand. There might be a simple video released in social media of some famous celebrity or any other popular person saying something. But what if that person in the video is not actually him. This is called as Image tampering attacks or deep fakes. And it is most widely happening technique now-a-days in order to spread the negative information to misguide millions of people by simply releasing a forged video into the media. It is a media which can create fake information by replacing their faces and their speech. It can cause a huge damage to the affected person's name and fame. This Image Tampering Attacks are increasing two times for every six months. It can make anyone say anything at any place. Therefore, as the impact of creating of tampered attacks in increasing widely, it also needs best technologies for its detection and hope for its prevention as well in future.

1. INTRODUCTION

Detection of Image Tampering Attacks" is the concept of detecting images or videos that are fake which are indistinguishable from the original ones. This is a technology which is used in the wrong hands to spread misinformation. The creation of this type of content has triggered several social issues which is mostly targeted upon famous and influential people. This detection can be done by using several techniques and algorithms by using Deep learning and python. There should be a better approach for identifying these image tampering attacks, and this can be done by one of the most effective technique called convolutional neural network. This Detection of Image Tampering Attacks provides its result as the identification of the difference between the tampered or fake image and the real one's by using neural networks and Resnext CNN in deep learning. Detection of such attacks requires a better solution to avoid the major spread of many unauthorized information to the public. Hence to stop this flow of negative spread in the society we need the most appropriate solution for detecting the image tampering attacks all over the world.

2.EXISTING SYSTEM

The existing system is built using MTCNN (Multi tasked cascaded convolutional neural networks) which slow in its detection process and contains a bit complex in its methodology comparatively. The accuracy seems to be changing depending upon the circumstances. The existing system also uses logit prediction and weighted

aggregation with automatic face weighting (AFW) which is for sequence processing and identification and used GRU for final prediction which is complex while its implementation and for its detection.

3. PROPOSED SYSTEM

The proposed system is built by using ResNext CNN and LSTM. Initially, the dataset is loaded to drive which can be easily mounted from google colab. The videos are divided into frames by using Open CV and each frame is cropped to the face and all the unrequired background is eliminated. Each preprocessed video (face cropped) contains first 150 frames as threshold value. Among those preprocessed videos we divide 80% for training and 20% for testing. The video names and labels are loaded from the given metadata.

The prediction part requires LSTM (Long Short-Term Memory) for sequence processing and ResNext Convolutional Neural Networks for feature extraction. It identifies the facial landmarks and compares the pixel values and calculates the accuracy. Based on the accuracy it predicts whether the video is real or fake.

4. IMPLEMENTATION

We have imported face recognition library which is used to identify the face from digital images or from a video frame. And ResNext Convolutional Neural Networks for feature extraction, and also Long Short-Term Memory (LSTM) for sequence processing. We have used Open source computer vision (Open CV) for image processing and Pytorch for efficient image and video transformation in deep learning. Using google colab, an online platform to easily import required libraries and for execution.

OUTPUT SCREEN

Division of frames for each video:

```
frames are  [148, 148, 148, 148, 148, 148, 148,
Total no of video:  20
Average frame per video: 147.6
```

The above output is division of frames for each video.

Detection of train & test videos:

```
train :  16
test :  4
TRAIN:  Real: 4  Fake: 12
TEST:  Real: 1  Fake: 3
```

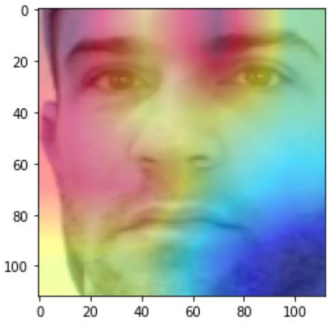
The above output is detection of real/ fake while training and testing the preprocessed face cropped dataset.

Final prediction:

The following output is predicted as real video having its confidence of prediction as 96.66 percentage.

Output 1: -

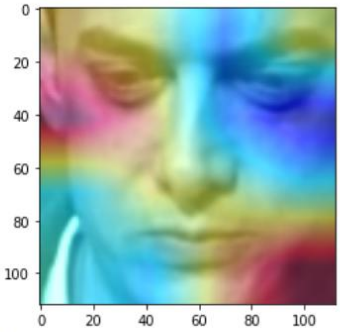
```
confidence of prediction: 96.66560292243958
```



REAL

Output 2: -

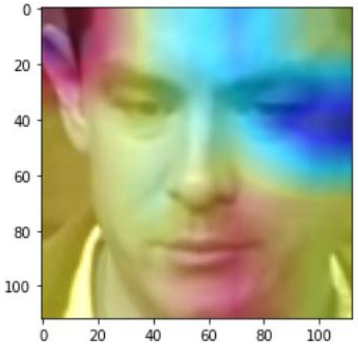
```
/content/drive/My Drive/dataset/id0_0002.mp4
/usr/local/lib/python3.7/dist-packages/ipyker
Clipping input data to the valid range for im
confidence of prediction: 85.04379987716675
```



REAL

The above output is predicted as a real video.

```
/content/drive/My Drive/dataset/id0_id3_0002.mp4
/usr/local/lib/python3.7/dist-packages/ipykernel_
Clipping input data to the valid range for imsho
confidence of prediction: 89.72108960151672
```



FAKE

The above output is predicted as a fake video.

5. CONCLUSION

Detection of Image tampering attacks is one of the most required solution to avoid the spread of fake news to the public. This reduces the trust of the people and cause several issues in the society. We have used the detection model which can detect the fake videos with higher accuracy out of several models present. As there are many issues occurring in the society which is mostly concentrated upon the targeted people, this technology of detecting them plays a key role in handling the fake news. Therefore, an accurate detection of Image tampering attacks can reduce the spread of falsified information and help the victims easily to get out of the problem in the future.

FUTURE SCOPE FOR FURTHER DEVELOPMENT

Detection of Image Tampering Attacks can be furtherly developed by adding greater models which can give more accurate results while detecting. It can also be developed as an application which can have an easy access in order to detect the fake video easily which can help the public to detect and understand the tampered or forged video easily. Apart from detecting the tampered videos (deep fakes), there should be a proper prevention of creating this forged or tampered videos of most popular and targeted people should definitely have an end.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] https://ieeexplore.ieee.org/document/9302547

[2] https://www.researchgate.net/publication/336058980_Deep_Learning_for_Deepfakes_Creation_and_Detection_A_Survey

[3] https://ieeexplore.ieee.org/document/9105991

[4] https://towardsdatascience.com/deepfake-detection-is-super-hard-38f98241ee49

[5] https://jonathan-hui.medium.com/how-deep-learning-fakes-videos-deepfakes-and-how-to-detect-it-c0b50fbf7cb9

[6] https://arxiv.org/pdf/2001.00179v3.pdf