International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 12th June 2022.

Link : https://ijiemr.org/downloads/Volume-11/Issue-06

Title: Synthetic media Deepfake Video Detection using ResNeXt& LSTM

volume 11, Issue 06, Pages: 1471-1483

Paper Authors: **Mr.K.Sudhakar ,A.Mallikarjuna Reddy , Ms. K.Siddika Harsha , Ms. K.Sai Mallika , Mr. V.Bharadhwaja**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Synthetic media Deepfake Video Detection using ResNeXt& LSTM

Mr.K.Sudhakar[1] ,**A.Mallikarjuna Reddy**[2] , Ms. K.Siddika Harsha[3] , Ms. K.Sai Mallika[4] , Mr. V.Bharadhwaja[5]

[1]Associate Professor, CSE, PSCMRCET, Vijayawada, Andhra Pradesh

[2]Associate Professor, CSE, Anurag University, Hyderabad

[3,4,5]Student, CSE, PSCMRCET, Vijayawada, Andhra Pradesh

ABSTRACT:

Synthetic media Deepfake Attacks turn out to be one of the biggest issues in society these days. Everything that appears on social media is a sensation in this generation. Never trust your eyes blindly; they may appear to be realistic, but they are not. It is the time to flip the coin to the other side and understand. There might be a simple video released on 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 deepfakes. And it is the most widely happening technique now-a-days in order to spread 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 huge damage to the affected person's name and fame. This Deepfake Attacks are increasing two times for every six months. It can make anyone say anything at any place. Therefore, as the impact of creating tampered attacks is increasing widely, it also needs best technologies for its detection and hope for its prevention as well in future.

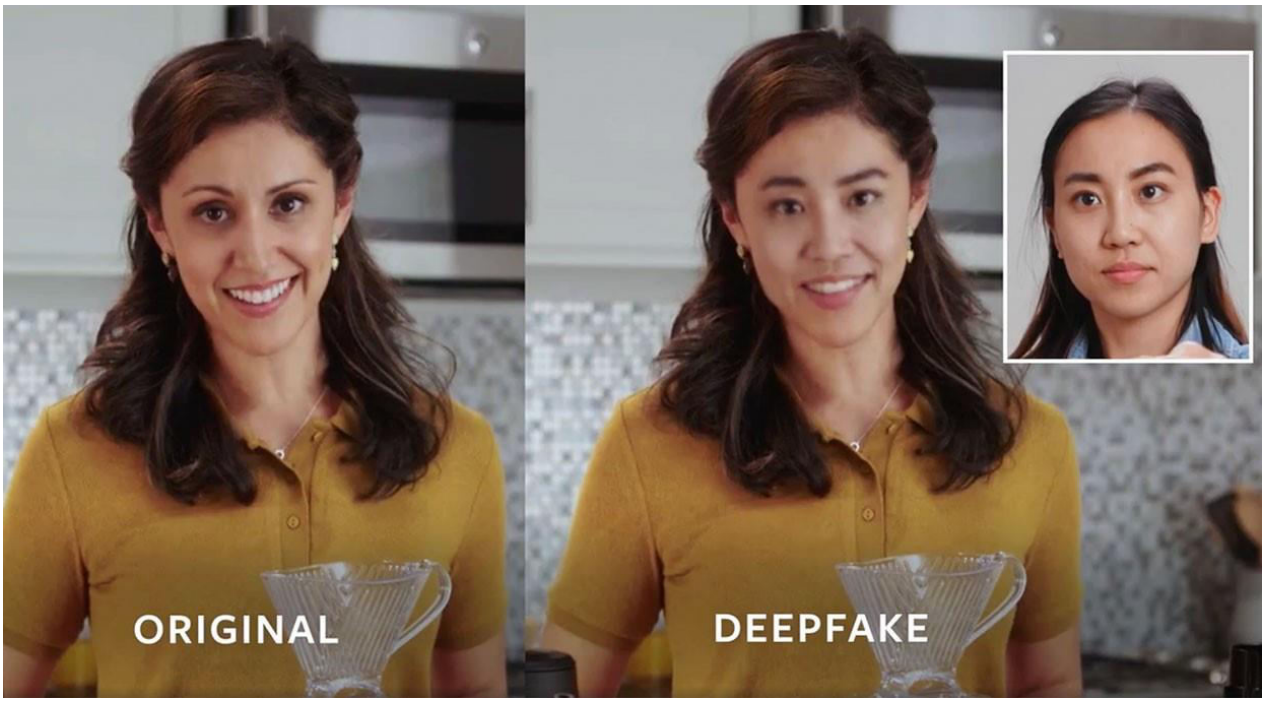
Keywords: Deepfake Video Detection, Synthetic media, Artificial Intelligence, Long Short-term Memory (LSTM), CNN, Res NeXt

1. INTRODUCTION:

"Synthetic media Deepfake video Detection using Res NeXt& LSTM" is the concept of detecting videos that are fake which are indistinguishable from the original ones. This is a technology which is utilized in the wrong hands to circulate misinformation. The invention of this kind of content has triggered several social consequences which is targeted upon notorious 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

deepfake attacks, and this can be done by one of the most effective techniques called convolutional neural network. This Synthetic media Deepfake video detection provides its result as the identification of the difference between the tampered or fake video and the real one's by using neural networks and Res Next CNN in deep learning. Detection of such attacks requires a better solution to avoid the major spread of unauthorized information to the public. Hence to stop

this flow of negative spread in society we need the most appropriate solution for detecting the deepfake attacks all over the world.



Now-a-days the increasing usage of the smartphones and the availability of excellent net connection throughout the global has extended the ever-growing reach of social media and content sharing has been made common and by the introduction of sharing virtual videos easier than ever before. In this age of technology it has created new challenges. The deep generative adversarial AI generated models were used to create "Deepfake," which can control video and audio samples. In particular, they could foresee deep fakes being exploited by purveyors of “fake news”. Anyone with access to this technology – from state-sanctioned propagandists to trolls – would be able to skew information, manipulate beliefs, and in so doing, push ideologically opposed online communities deeper into their own subjective realities. These type of forms of the DeepFake can be terrible, and lead to threating to anyone, deceptive of common people which maybe deceptive to naked eye. To overcome this kind of situations, Synthetic media detection is very crucial in this transformative era. So, in order to overcome this situation we

describe a unique deep learning-based technique/methodology that can be efficiently able to distinguish between AI-generated films/videos from the actual footage. It is critical to improve technology that can detect these kind of synthetic media so that they can be identified and prevented from spreading over the internet.

The Deepfake Detector is used for detecting the AI-Synthetic media. It is crucial to analyze and study how the Generative Adversarial Network (GAN) works generates the Tampered images/videos. While GAN takes a video and an image of a the original person as the input format and produces formatted layout video with the targeted person's face where it has been replaced with the fake/unoriginal person's face. These Deep adversarial neural networks trained on face photos and original person's videos in order to provide the backbone for the Synthetic media, where it can automatically transforms into the unoriginal face with the generated facial emotions to the original face. The output videos can be make it look like an high level of realistic facial features have been generated.

2. **RELATED WORK:**

Huy H [11] (et.al): has developed CAPSULE-FORENSICS: USING CAPSULE NETWORKS TO DETECT FORGED IMAGES AND VIDEOS here with the usage of the capsule networks are used to detect the tampered (or) manipulated images and video files that has been AI generated it can be used to detect these kind of forgeries of facial features. As they have been generated in different kinds of scenarios and need of detection in these attacked situations is vital.

However this algorithm is very slow and has not been tested on large datasets such as ImageNet

Ming-ChingChang [10] (et.al): has proposed Exposing AI Created Fake Videos through Detecting Eye Blinking describes a different kind of approach to detection of the synthetic media that has been generated by the usage of the different kinds of deep neural networks to propose their method. As in here the word blinking means that the motion of the eyelids.As we know that a normal healthy human can blink each blink in 2-10 where as the general blink count can be taken as for 0.1-1.4 seconds. Therefore, the shortage of eye blinking is shows that it could be a possible AI generated synthetic video.as their method only considers the eye blinking there are certain other main facial parameters that need to be considered in order to detect the synthetic media.

K. Zhu [7] (et.al): has described Deepfake Detection with Clustering-based Embedding Regularization by a unique approach for deepfake detection. By the usage of the open-source algorithms are used to simulate the process of generating artifacts during the deepfake generation

technique the usage of simple image processing operations on a picture, and make it as a generated example. Such as The Meso4 algorithm, FWA algorithm, EVA algorithm, multi-task

algorithm, Xception algorithm are used to compare with start-of-art. By training the Xception network for classification, the usage of positive samples, negative samples, and generated samples as input samples. The class range is set to three throughout the training process and in the testing process, the generated samples also are classified as negative samples to enhance the classification effect. At the same time, a regularization loss 6 is introduced all through the training process to ensure the inter-class distance and intraclass smoothness of the embedded space. Experimental effects on UAV, Celeb-Deepfake,andDeepfake Detection datasets exhibit the effectiveness of the techniques in deepfake detection

Lingzhi Li [8] (et.al): has proposed Face X-ray for more general face detection By proposing a unique methodology by gathering records from the face forgery evidence data records, face X-ray datasets as by the based on observation that shows that the most of the new facial tampering techniques has a common blending of the facial feature steps, and there exists the most of the intrnsic manipulations of the image spots throughout the blending boundary, where it has been neglected many of the brand-new techniques introduced by the deepfakedetectors.By the usage of more general facial forgery detector with the usage of the unique techniques yet simple with the Face X-ray it can be used to training does not includes any kinds of fake pictures to generate the face detector. But for this techniques it has some certain limitations. Therefore, while a picture is completely synthetic, it is practically possible that this technique may or may not work correctly.

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 googlecolab. 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. We have imported face recognition library which is used to identify the face from digital images or from a video frame. And Res Next for feature extraction, and also by the usage of Long Short-Term Memory (LSTM) in order to perform the 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 googlecolab, an online platform to easily import required libraries and for execution. 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. MODULES:

In order to develop the proposed System, we need these certain steps to perform the synthetic media detection:

1) Dataset - Data selection & Data loading

2) Data Pre-processing

3) Feature Extraction

4) Sequence Processing

1) **Dataset - Data selection & Data loading:**

Data selection & Data loading is the produre of choosing datasets which are used to train the Res NeXt model in order to predict the accuracy of the data we can choose from the different kinds of datasets such as the deep fake detection challenge dataset, Face forensics ++ dataset, or

celebdeepfake dataset is known as data selection. The dataset is put onto the drive and mounted to the Google colab file in this projec is known as the Data loading.

2) **Data Pre-processing:**

Data Pre-processing is the technique which can be used to extract the efficient data from the raw (or) unnecessary data to get the exact and efficient data. In this process by splitting the input video data into the seperate fames with the usage of the facial recognition. With the usage face recognition only the face part will be cropped and converted into new dataset.As the length of the footage is taken minimum count of 150 frames otherwise the video will be removed from the preprocessed data. In here for the sake of the experimentation we only take short videos with the mean fram rate of 300 frames average as we propose these first 100 to train the Res NeXt model

3) **Feature Extraction:**

For the purpose of Feature Extraction we propose using the Res Next CNN classifier model for extracting features from the frames and able to recognizing the frame level characteristics of the facial features. In addition to the process we'll continue the procedure by adding some of the other required layers to the network and then by setting the exact reliable learning rate to get the constant gradient descent so the prediction properly converged.

4) **Sequence Processing**:

Sequence Processing is done by assuming a model with 2-node neural network which can be used for the sequencing the frames that has been split to predict the result from the input video frames Res NeXt feature parameters of input frames as output with the sequence processing. In here we use the Long Short-Term Memory(LSTM) 2048 unit in order to solve the recursive analysis of the model it has 0.4 chance to work with it. As the LSTM can be used to analysis of the frames in the sequential order.

Prediction:

Prediction of the input data can be done while a new input video is uploaded into the trained model to get the results for the prediction. While the new input video is likewise will be preprocessed to carry withinside the layout of the trained model. The video footage is which has been splitted into frames are analyzed through the face recognition after the face cropping and it

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

will be stored into the local storage and the frames will be uploaded into the model for the detection to predict whether the input video is real or fake.

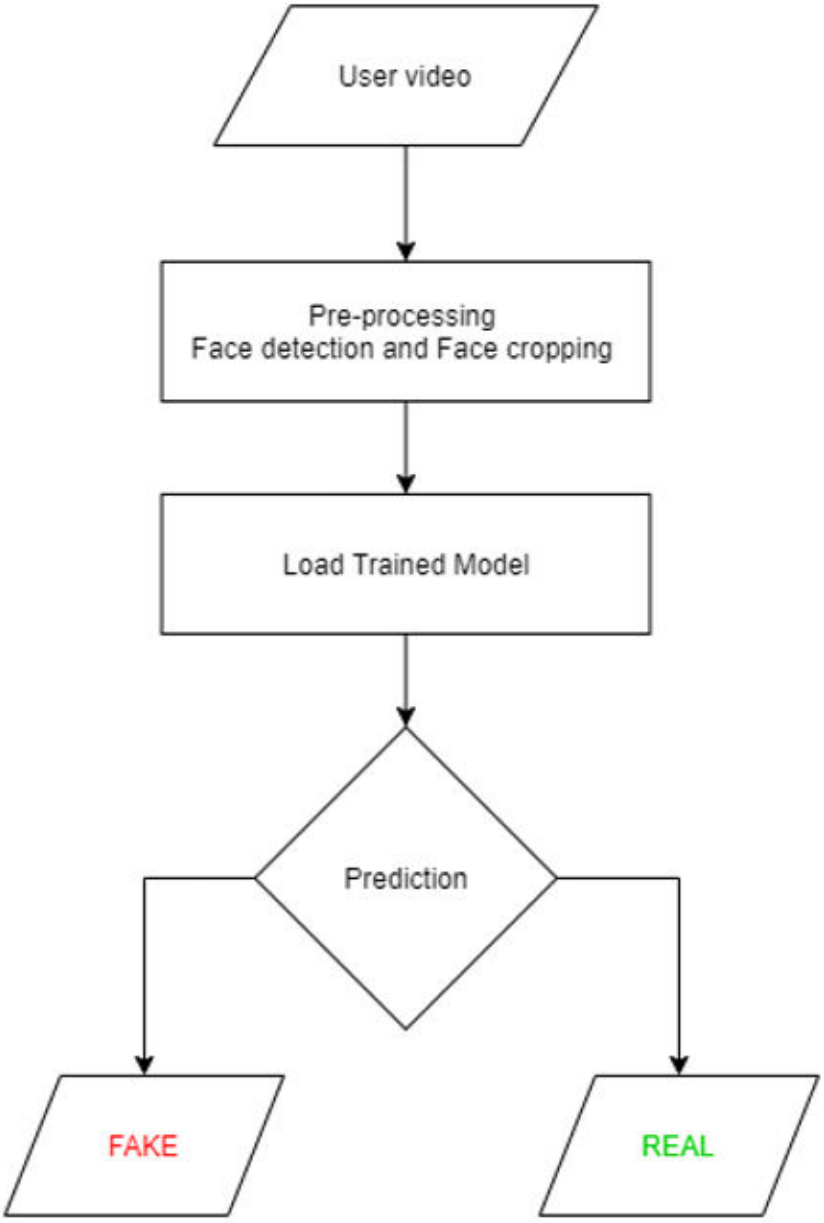


Fig.1 Training Workflow

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

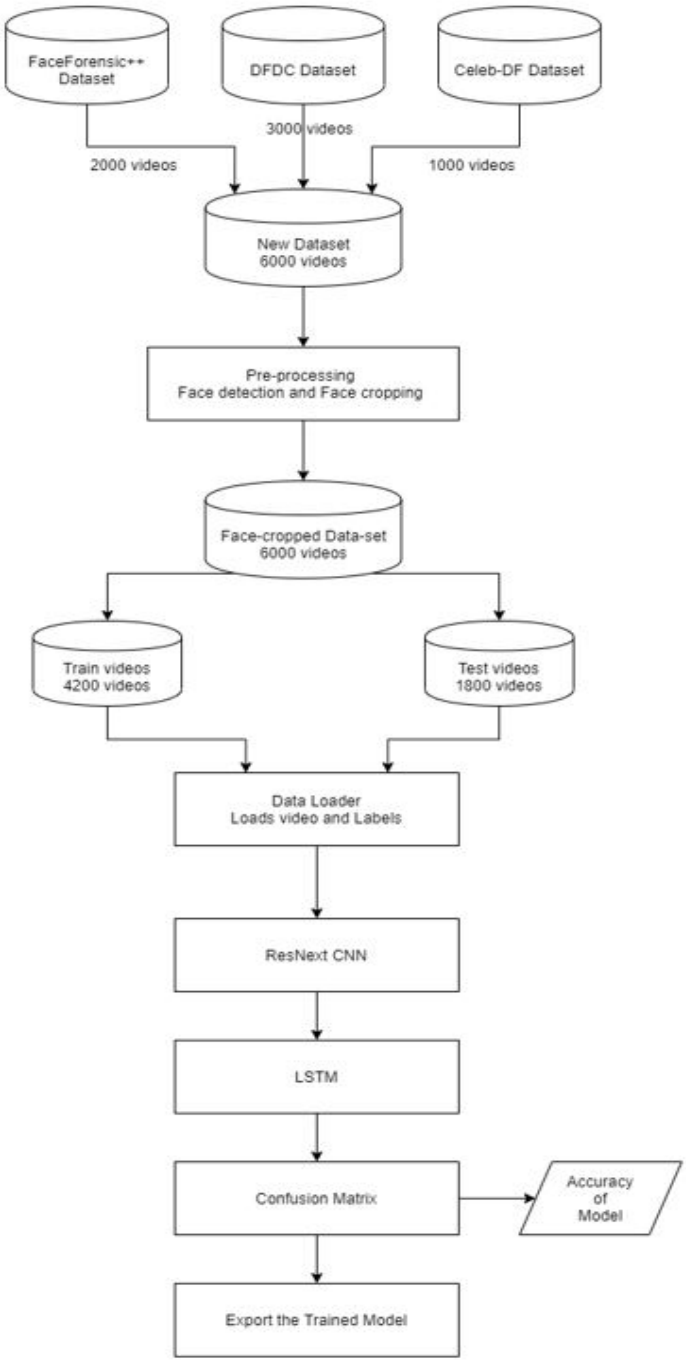


Fig.2 Prediction Workflow

4. RESULTS:

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Division of frames for each video:

```
frames [299, 299, 299, 299, 299, 299, 299, 300, 299, 299, 299, 300, 299, 300, 299, 300, 300, 300, 299, 300]
Total number of videos: 20
Average frame per video: 299.35
```

The above output is the 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
```

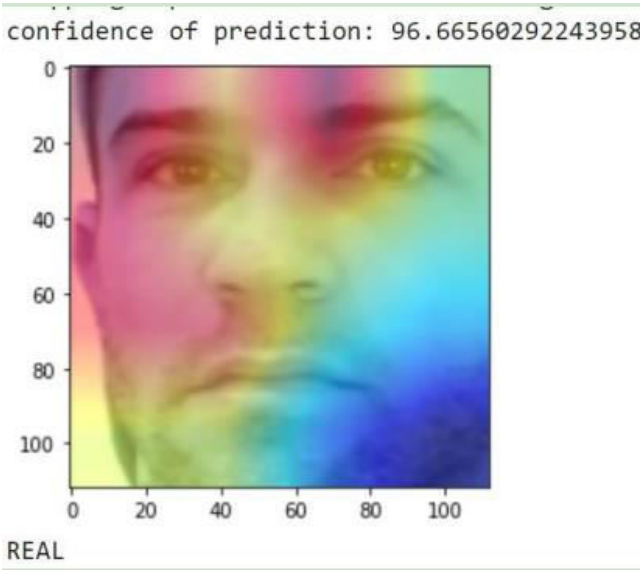
The above output is detection of real/ fake while training and testing the preprocessed face cropped dataset.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Final prediction:

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

Output 1: -

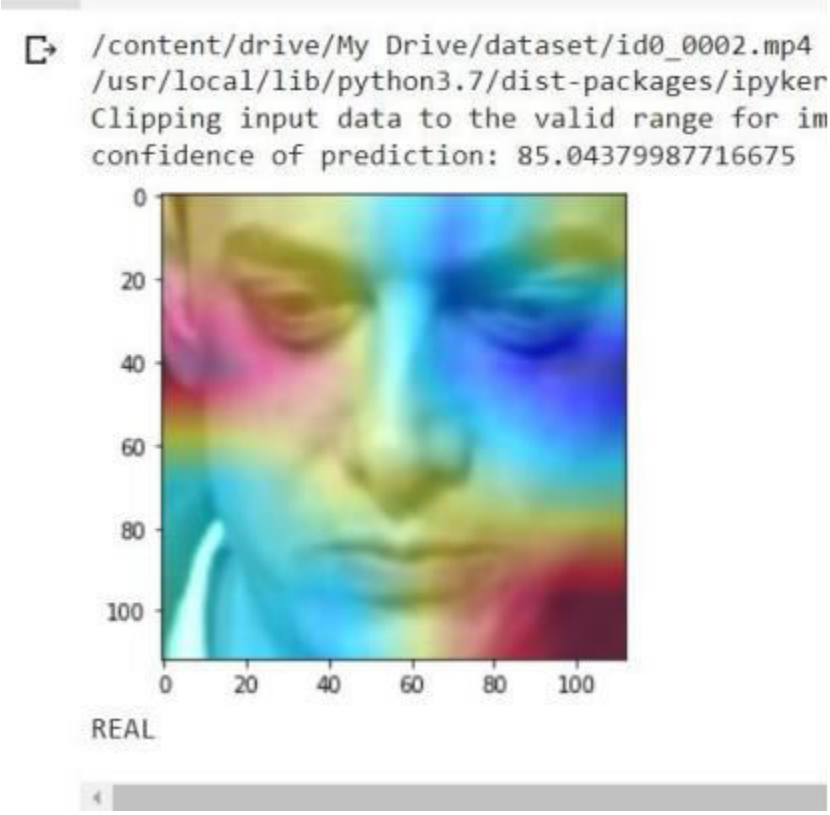


The above output video is predicted as a real video.

Output 2: -

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The following output is predicted as real video having its confidence of prediction as 85.043 percent.

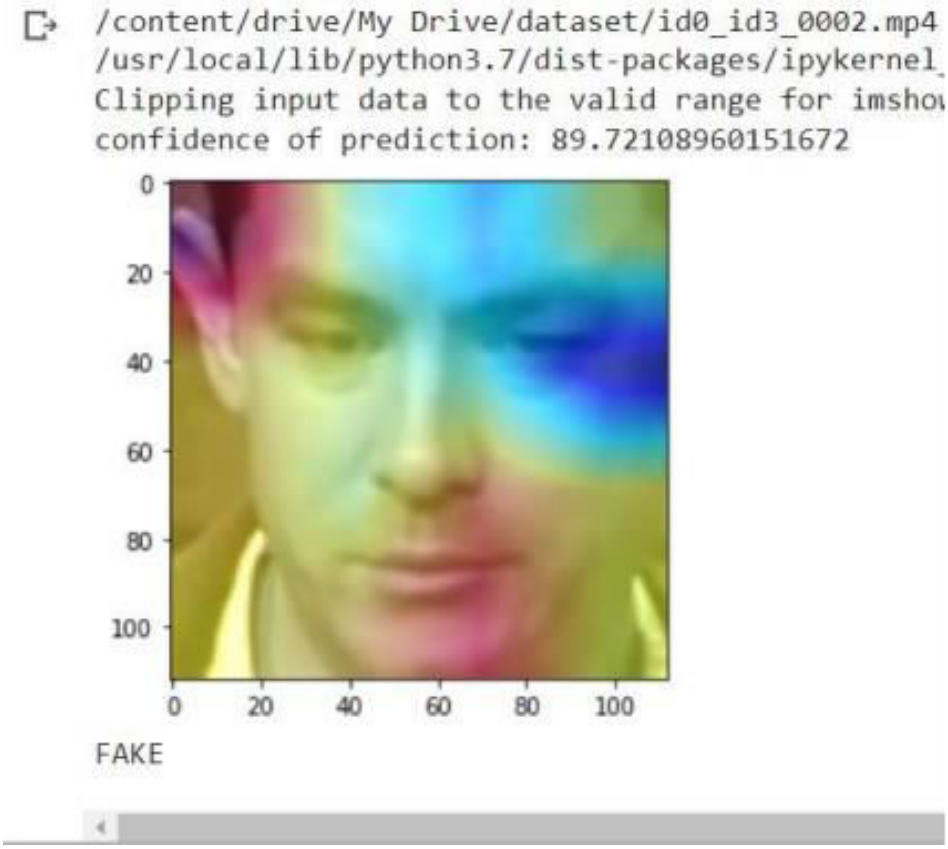


The above output video is predicted as a real video.

Output 3: -

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The following output is predicted as real video having its confidence of prediction as 89.72 percent.



The above output video is predicted as a fake video.

5. CONCLUSION

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

6.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. Mallikarjuna Reddy, A., Venkata Krishna, V. and Sumalatha, L. Face recognition approaches: A survey. International Journal of Engineering and Technology (UAE), 4.6,6(7)(2018) 117-121. doi: 10.14419/ijet.v7i4.6.20446.
6. M. R. Ayaluri, K. Sudheer Reddy, S. R. Konda, and S. R. Chidirala, "Efficient steganalysis using convolutional auto encoder network to ensure original image quality," PeerJ Computer Science, vol. 7, p. e356, 2021.
7. https://jonathan-hui.medium.com/how-deep-learning-fakes-videos-deepfakes-and-how-to detect-it-c0b50fbf7cb9
8. https://arxiv.org/pdf/2001.00179v3.pdf
9. Deepfake Detection with Clustering-based Embedding Regularization K. Zhu, B. Wu and B. Wang, "Deepfake Detection with Clustering-based Embedding Regularization," 2020 IEEE Fifth International Conference on Data Science in Cyberspace (DSC), 2020, pp. 257-264, doi: 0.1109/DSC50466.2020.00046.
10. Mallikarjuna Reddy A, RupaKinnera G, Chandrasekhara Reddy T, Vishnu Murthy G. 2019. Generating cancelable fingerprint template using triangular structures. Journal of Computational and Theoretical Nanoscience 16(5–6):1951-1955
11. A Mallikarjuna Reddy, VakulabharanamVenkata Krishna, LingamguntaSumalatha and AvukuObulesh, Age Classification Using Motif and Statistical Feature Derived On Gradient Facial Images, Recent Advances in Computer Science and Communications (2020) 13:965. https://doi.org/10.2174/2213275912666190417151247.
12. Exposing AI Created Fake Videos by Detecting Eye Blinking Yuezun Li, Ming-Ching Chang and SiweiLyu University at Albany, State University of New York, USA .
13. C Ramakrishna, G Kiran Kumar, A Mallikarjuna Reddy, and P. Ravi, "A Survey on various IoT Attacks and its Countermeasures," Int. J. Eng. Res. Comput. Sci. Eng., vol. 5, no. 4, pp. 2394–2320, 2018, [Online]. Available: http://ijercse.com/specissue/april-2018/27.pdf.
14. Swarajya Lakshmi V Papineni, SnigdhaYarlagadda, HaritaAkkineni, A. Mallikarjuna Reddy. Big Data Analytics Applying the Fusion Approach of Multicriteria Decision Making with Deep Learning Algorithms International Journal of Engineering Trends and Technology, 69(1), 24-28, doi: 10.14445/22315381/IJETT-V69I1P204.