IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DETECTION OF DEEPFAKE

Dev Mamgain, Dushyant Bhardwaj
Department of Computer Science and Engineering
Inderprastha Engineering College, Sahibabad,
Ghaziabad, India

Ms. Archana Agarwal
Assistant Professor
Department of Computer Science and Engineering
Inderprastha Engineering College, Sahibabad,
Ghaziabad, India

***Abstract*-- In recent months, free software tools based on deep learning have made it easier to create reliable facial transformations in videos that appear out of nowhere without control effects, so-called "DeepFake" (DF) videos. Digital video management has been proven for many years using the view.Recent advances in deep learning have led to major improvements in the accuracy and accessibility of false content where possible . created. These are called AI Synthetic Media (often called DF). However, this represents a significant challenge when it comes to the discovery of these DFs. Because training the algorithm to find DF is not easy. We take a step forward in DF detection by using neural networks and recurrent neural networks. The system uses a convolutional neural network (CNN) to extract phase models. These features are used to train a Recurrent Neural Network (RNN) that can detect inconsistencies between, which learns to determine whether videos have been modified and physical disparities between frames represented by DF Design. tool. Expected results for many fake videos collected from the dataset. We show that our system achieves competitive results on this task using a simple reference model.**

Keywords: Deepfake video detection, recurrent neural network (RNN), convolutional neural network (CNN).

I .INTRODUCTION

The growth of smartphone cameras and the availability of good internet connections around the world have contributed to the growth of social and media sharing portals, making it easier than ever to create and share digital video.

The growth of computing power has made deep learning possible; just a few years ago this was thought impossible. Like every new change, it brings new challenges. The so-called "DeepFake" consists of well-established models and can replace video and audio clips. The spread of DF on social media platforms has become widespread, leading to spam and misinformation on the platforms.

Such DFs can be dangerous and cause the public to be threatened and misinformed.

To overcome this situation, detection of DF is very important.

Therefore, we define a new approach based on deep learning that can distinguish fake videos (DF videos) created from videos from real videos.

In order to detect DF and prevent its spread online, it is important to develop technology that can identify counterfeit products.

To detect DF, it is important to understand how create DF. GANs take videos and photos of a specific person ("target") and broadcast another video ("location-") in which the target's face is replaced with another person's face. The neural network is trained on facial images and target videos to obtain a target face map and facial expression.

By creating appropriate post-production, the resulting video can achieve a high level of GAN image processing in every frame. video. This process is usually done using autoencoders.

We define a new model based on deep learning that can distinguish DF videos from real videos. Our approach is based on the same process as generating the DF of the GAN.

This method is based on the DF video product. Due to the limitation of computing power and generation time, the DF algorithm can only generate large size face images and they need to be final degraded. to match the resource location configuration.

This conflict leaves some ambiguity in the deepfake video output due to the conflict in the resolution of the distorted area of the face and the surrounding environment.

Our method captures the GAN-oriented effects of GANs during DF reconstruction by dividing the video into frames and using ResNext Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) Short Term (LSTM). not consistent. To train the ResNext CNN model, we simplify the process by directly modeling the non-uniformity problem in affine face wrapping.

II. Literature Survey

PAPER NAME	JOURNAL(S)	YEAR	METHODS	RESULT
Transferable deep-CNN features for detecting digital and print-scanned morphed face images	R. Raghavendra	2017	The proposed method is extensively evaluated on the newly constructed database	Improved detection
Can face anti spoofing	Tiago de Freitas Pereira	2013	Analyze the joint color-texture information from the luminance	Promising generalization capabilities
Distinguishing computer graphics from natural images	Nicolas Rahmouni	2017	Distinguishing computer generated graphics from real photographic images.	Evaluate our work on recent photo-realistic computer graphics
Eyes closeness detection from still images	F. Song	2014	Multiple feature sets to characterize the rich information of eye patches	Handles a much wider range of eye appearance

III. PROPOSED SYSTEM

There are many tools for generating DF in the proposed system, but very few tools for DF detection. Our approach to identifying DF will be effective in preventing DF from entering the World Wide Web.

We will provide a web-based platform for users to upload videos and classify them as fake or real. The project can be expanded from creating a web-based website to a browser plug-in for automatic DF detection. Even with major applications like WhatsApp, Facebook can integrate this project with their own applications to easily check the DF before sending it to other users. One of the main objectives is to evaluate its performance and its guarantee of security, user-friendliness, accuracy and reliability.

Our approach focuses on identifying all types of DF, such as substitution DF, dismissal DF, and interpersonal DF.

Figure 1 represents the basic structure of the preparation process: -

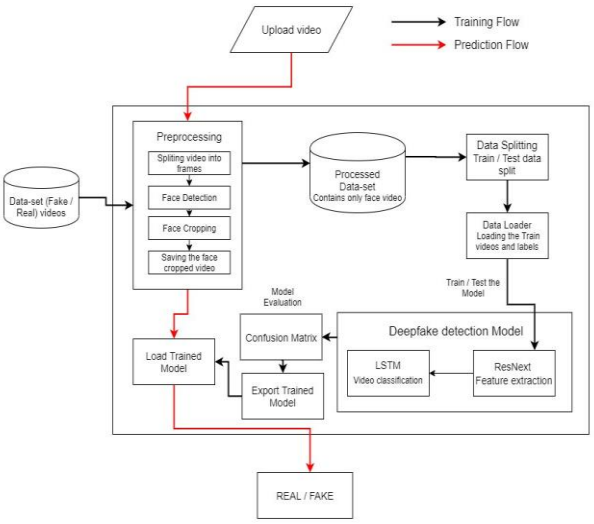

Fig. 1: System Architecture

A. Dataset:

We use a hybrid dataset containing data from various sources such as YouTube, FaceForensics++[14], deepfake search competition dataset [13]. Our new documentary is planned to consist of 50% original footage and 50% full depth of field footage. The data set is divided into 70% training set and 30% test set.

B.Preprocessing:

Next is face detection and cropping the frame with face detection. To ensure equality of the number of frames, the average of the movie data set is calculated and a new face crop is created with frames equal to the average. Posts without faces will be ignored at first. Shooting 10 seconds of video at 30 frames per second, or 300 total frames, requires a lot of energy. Therefore, we recommend using the first 100 frames to show the model for testing purposes.

C. Model:

The model consists of resnext50_32x4d and LSTM layers. The file uploader first loads the face cropped video and splits the video into training and test sets. Additionally, the process derived from the video became a model for training and testing in small groups.

D. ResNext CNN for Feature Extraction

Next, we will fine-tune the network by adding the necessary layers and choosing the appropriate training value to accurately distinguish the slope of the model. The 2048-dimensional feature vector after the last pooling layer will be used as LSTM input.

E. LSTM for Sequence Processing

Suppose the input frame is a ResNext CNN feature vector sequence as input and a 2-node neural network,

As a result, the sequence is part of a deepfake video or an unedited video. The real challenge we need to

solve is to create a model that tracks the recycling process efficiently. For this problem, we recommend using 2048 LSTM units with a loss factor of 0.4, which achieves our goal. LSTM is used to process the sequence of frames to perform sequence analysis of the video by comparing the frame of the t-th second with the frame of the t-n< second. where n can be the number of frames before t.

F. Predictions:

Turn new videos into predictive learning models. New videos have also been introduced in the model of the working model. The video is divided into frames and then the face is cropped and the crop frames are not stored in local storage but are stored directly for training standards to know.

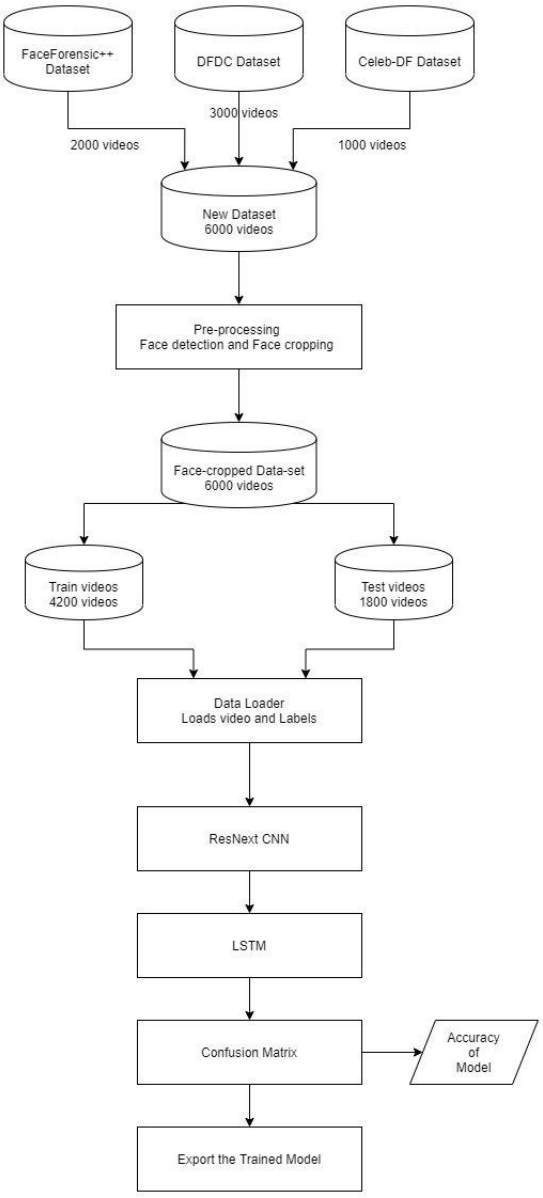

Fig. 2: Training Flow

IV. Results

The results of the model will be whether the video is arXiv:1901.02212v2. deep or real video and the reliability of the model.

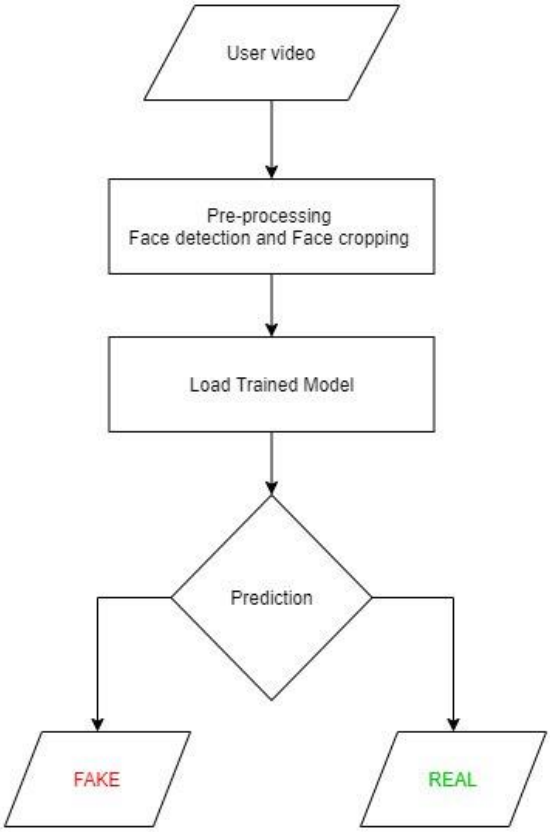

Fig. 3: Prediction flow

V. Conclusion

We proposed a neural network method to classify videos as deep videos or real videos and reliability of the design. The plan was inspired by the way GANs create deepfakes with the help of autoencoders. Our method uses ResNext CNN for phase detection and RNN and LSTM for video classification. The proposed method can capture the video as deep or real as not stated in the document. We believe that it will provide instant information with high accuracy.

VI. Limitations

Our approach does not consider sound. Therefore, our method will not be able to detect deep sounds. However, we recommend using deep voice spoofing detection in the future.

VII. 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] Huy H. Nguyen , Junichi Yamagishi, and Isao Echizen “ Using capsule networks to detect forged images and videos ”.

[4] Hyeongwoo Kim, Pablo Garrido, Ayush Tewari and Weipeng Xu “Deep Video Portraits” in

[5] Umur Aybars Ciftci, ˙Ilke Demir, Lijun Yin "Detection of Synthetic Portrait Videos using Biological Signals" in arXiv:1901.02212v2.
[6] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. In NIPS, 2014.
[7] David G¨uera and Edward J Delp. Deepfake video detection using recurrent neural networks. In AVSS, 2018.
[8] Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun. Deep residual learning for image recognition. In CVPR, 2016.
[9] An Overview of ResNet and its Variants : Vision and Pattern Recognition, pages 5967–5976, July 2017. Honolulu, HI.
[10] R. Raghavendra, Kiran B. Raja, Sushma Venkatesh, and Christoph Busch, "Transferable deep-CNN features for detecting digital and print-scanned morphed face images," in CVPRW. IEEE, 2017.
[11] Tiago de Freitas Pereira, Andr´e Anjos, Jos´e Mario De Martino, and S´ebastien Marcel, "Can face anti spoofing countermeasures work in a real world scenario?,"in ICB. IEEE, 2013.
[12] Nicolas Rahmouni, Vincent Nozick, Junichi Yamagishi, and Isao Echizen, "Distinguishing computer graphics from natural images using convolution neural networks," in WIFS. IEEE, 2017.
[13] F. Song, X. Tan, X. Liu, and S. Chen, "Eyes closeness detection from still images with multi-scale histograms of principal oriented gradients," Pattern Recognition, vol. 47, no. 9, pp. 2825–2838, 2014.
[14] D. E. King, "Dlib-ml: A machine learning toolkit," JMLR, vol. 10, pp. 1755–1758, 2009.
https://towardsdatascience.com/an-overview-of-resnet and-its-variants-5281e2f56035 [10] Long Short-Term Memory: From Zero to Hero with Pytorch: https://blog.floydhub.com/long-short-term memory-from-zero-to-hero-with-pytorch/
[15] Sequence Models And LSTM Networks https://pytorch.org/tutorials/beginner/nlp/sequence_mo d els_tutorial.html
[16] https://discuss.pytorch.org/t/confused-about-the-image preprocessing-in-classification/3965
[17] https://www.kaggle.com/c/deepfake-detection challenge/data
[18] Y. Qian et al. Recurrent color constancy. Proceedings of the IEEE International Conference on Computer Vision, pages 5459–5467, Oct. 2017. Venice, Italy.
[19] P. Isola, J. Y. Zhu, T. Zhou, and A. A. Efros. Image-to image translation with conditional adversarial networks. Proceedings of the IEEE Conference on Computer.