



# International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

*(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)*



**Impact Factor: 8.699**

**Volume 14, Issue 3, March 2025**

# **Deepfake Detection: A Hybrid Approach using ResNeXt and LSTM for Video Authentication**

**Keval Katariya, Krutarth Dumlawkar, Prof. Nandakishor Sirdeshpande**

Department of Computer Science & Engineering, Parul University, Vadodara, Gujarat, India

**ABSTRACT:** With the advent of deep learning and advanced computing, it is now surprisingly simple to create extremely realistic deepfake videos. Those AI-created videos in which faces are replaced or altered with almost perfect accuracy are a serious menace - propagating political disinformation, fake news, blackmail, and even cybercrimes based on deepfakes. As deepfakes become more realistic, it is becoming a race between AI and AI - where one creates fakes, and the other one detects them.

In this work, we present a deep learning-based solution to address the issue of deepfakes directly. Our approach utilizes a ResNeXt convolutional neural network (CNN) to examine a single frame from a video, identifying minute features that suggest manipulation. These are subsequently fed through a Long Short-Term Memory (LSTM)-based Recurrent Neural Network (RNN), which examines the frame sequence to decide whether a video is authentic or manipulated. This configuration enables us to identify both face substitution and reenactment deepfakes accurately.

In order to enable our system to function optimally in real-world environments, we trained and evaluated it on a large and balanced dataset, merging videos from popular sources such as FaceForensics++, the Deepfake Detection Challenge (DFDC), and Celeb-DF. Our method demonstrates that deepfake detection is both efficient and trustworthy even using a straightforward but effective architecture.

**KEYWORDS:** Res-Next Convolution neural network, Recurrent Neural Network (RNN), Long Short Term Memory(LSTM), Computer vision.

## **I. INTRODUCTION**

“Can you trust everything you see on the internet? Think again deepfakes are making it more difficult than ever to know what’s real and what’s fake.”

Deepfakes have rapidly emerged as one of the most threatening issues in the current digital age. Such AI-created videos can replace faces, duplicate voices, and change expressions of an image or video so realistically that it's almost impossible to distinguish what's real and what's fake. As this technology has been applied for creative goals in social media, entertainment, and film, it has also been promoted for misinformation, cybercrimes, blackmail, and political manipulation. The capability of generating realistic videos has generated serious risks for trust in digital media, and thus the demand for detecting deepfakes is greater than ever. To combat this increasing problem, we suggest an AI-based deepfake detection system that counterattacks with the same sophisticated technology used to produce them.

Our solution uses : ResNeXt convolutional neural networks (CNNs) and Long Short-Term Memory (LSTM) based Recurrent Neural Networks (RNNs) to examine videos frame by frame, detecting tiny inconsistencies that reveal deepfakes. By examining both the spatial and temporal attributes of a video, our model can accurately identify face-swapping and reenactment based fakes. Deepfakes are frequently made using applications such as FaceApp, FaceSwap, and other GAN-based models, so they're becoming even more advanced. To make sure that our model does well under practical scenarios, we trained the model on a large scale and diverse dataset consisting of videos from FaceForensics++, Deepfake Detection Challenge (DFDC), and Celeb-DF.

Secondly, we built a simple front-end application that users can easily upload a video into, and our AI model will process the video, sending back a prediction (real or fake) together with a confidence level. As deepfake tech advances, so do the methods for stopping them. Social media, news sites, and messaging apps already have deepfakes growing

rapidly on them, altering reality. Consider a deepfake of a world leader announcing war in error, or a created video of a famous person behaving outrageously such fakes could incite panic, destroy reputations, or even fuel political wars.

The need to fight this problem has never been more pressing. Our work is intended to enlighten individuals, social media platforms, and law enforcement agencies with a trustworthy and real-time deepfake detection tool. We intend to safeguard the integrity of digital media and ensure that truth can still be told from falsehood in an age where "seeing is no longer believing."

## II. LITERATURE SURVEY

Deepfake technology is evolving at an incredible pace, making it harder than ever to distinguish between real and fake manipulated content. Researchers across the globe have been working on different ways to detect deepfakes, using everything from image artifacts and eye movements to biological signals and deep learning models. This section explores some of the most significant approaches that have shaped the field of deepfake detection, highlighting their strengths and weaknesses. One of the initial methods used is Face Warping Artifacts, where scientists applied a Convolutional Neural Network (CNN) to detect anomalies between the fake face and the area around it. Deepfakes are generally produced at lower resolution and then tuned to the level of the original video, causing minute distortions. While this approach was effective in finding low-quality deepfakes, it did not take into account how faces move over time and therefore failed in the case of more sophisticated manipulations. Another innovative method included identifying deepfakes based on eye-blinking patterns.

Early models of deepfakes tended to have issues imitating natural blinking, and so one study proposed a Long-term Recurrent Convolutional Network (LRCN) that monitored eye movement. Yet, as deepfake algorithms became better, more recent models started to produce realistic eye blinking, which reduced the viability of this technique. According to experts, for even more accuracy, we might want to consider facial wrinkles, abnormal teeth structures, and misalignment of eyebrows all of which are hard for AI to exactly duplicate. Certain researchers tested Capsule Networks, a neural network that was specifically created to identify forgeries in images and videos. Although this method was successful on test datasets, it added random noise during training, which may lead to problems when identifying deepfakes in real-world settings. Our approach, on the other hand, aims to train using clean, real world datasets to enhance reliability in real-world applications.

Another deepfake detection approach entailed Recurrent Neural Networks (RNNs) integrated with an ImageNet pre-trained model to study the video frames sequence wise. The researchers utilized the HOHO dataset, having only 600 videos. Although their technique was promising, the limited dataset size and non-diverse nature created challenges for the model to apply to actual real-world cases. Our method mitigates this drawback by training on large-scale and diverse datasets, making it more adaptable across various forms of deepfakes. Another more distinct method entailed examining biological signals from human faces to ascertain whether a video was authentic or deepfaked. Scientists tapped subtle signals such as blood flow patterns from face areas with the help of photoplethysmography (PPG) maps, and then they trained a Support Vector Machine (SVM) and CNN to differentiate between videos. Although this approach was promising, it was not easy to retain biological signals consistently for various videos, rendering it less feasible for actual deepfake detection. One of the most sophisticated deepfake detection models currently available is FakeCatcher, which can detect fake videos with high accuracy, no matter what content, resolution, or deepfake generator is used. But its greatest weakness is the absence of a discriminator, meaning it cannot maintain biological signals, and thus may not perform as well in certain situations.

In order to train and test deepfake detection models, researchers have assembled a number of **\*\*large-scale deepfake datasets\*\*** that assist in training AI models. A few of the most popular datasets are:

- FaceForensics (Rossler et al., 2019) :- A popular dataset of real and forged videos created using four manipulation methods.
- Deepfake Detection Challenge (DFDC) (Dolhansky et al., 2020) :- One of the largest datasets, developed by Facebook AI to evaluate deepfake detection models.
- Celeb-DF (Li et al., 2020) :- A dataset of high-quality deepfake videos with few artifacts, hence more difficult to detect.

- DF-TIMIT (Korshunov & Marcel, 2018) :- One of the first deepfake datasets, created with FaceSwap and DeepFaceLab.
- DeeperForensics 1.0 (Jiang et al., 2020) :- A dataset with real world deepfakes and compressed deepfakes that assist models in generalizing to real-world situations.

Though deepfake detection has progressed significantly, there are still several challenges. Deepfake algorithms continue to get better, so it becomes increasingly difficult for current models to catch up. Some of the most significant challenges are :- 1). Evolving Deepfake Models, 2). Generalization Problems, 3). Adversarial Attacks, 4). Real-Time Detection. To overcome such challenges, future work must emphasize hybrid models that incorporate several detection methods, incorporate explainable AI (XAI) for better transparency, and increase real time detection rates for mass deployment. Our proposed algorithm integrates CNN based feature extraction (ResNeXt) with LSTM based temporal analysis, seeking to overcome major limitations of current models while providing scalability and real-world usability.

### III. METHODOLOGY

Our suggested deepfake detection system adopts a systematic problem solving strategy, encompassing analysis, design, development, and evaluation. The approach ensures that the model is developed with high precision, low bias, and practical application. Through the use of a hybrid deep learning model using ResNeXt CNN for feature extraction and LSTM based RNN for temporal analysis, we strive to provide solid deepfake detection.

#### 1. Analysis :

The initial step toward solving the deepfake detection issue was an in-depth problem analysis and identification of solution requirements. On the basis of literature survey, we found primary feasibility limitations and possible challenges. Bias in model training is one of the primary issues in deepfake detection. Certain models only train on fake or real videos, which results in overfitting and incorrect predictions. To address this, we made sure to have balanced training, with an equal proportion of real and deepfake videos to improve generalization and minimize bias. To create an efficient deepfake detection model, we had identified important facial and video-based artifacts that distinguish deepfakes from authentic videos:

- Eye blinking
- Teeth mismatches
- Iris segmentation
- Double edges in facial details
- Wrinkles and skin texture
- Irregular head pose
- Face angle deformations
- Higher cheekbones and double chins
- Inconsistencies in hairstyle
- Variations in skin tone
- Inconsistencies in facial expression
- Inconsistencies in lighting

#### 2. Design :

Once we completed the analysis stage, we designed the system architecture and deep learning model. The baseline architecture used is:

- ResNeXt CNN for frame-level feature extraction, detecting subtle spatial deepfake artifacts.
- LSTM-based RNN for temporal inconsistency analysis in sequential video frames.
- Fully connected layers for end-to-end classification (real or deepfake).

This is a hybrid solution that allows the model to effectively identify both face-swapping and reenactment deepfakes.

### 3. Development :

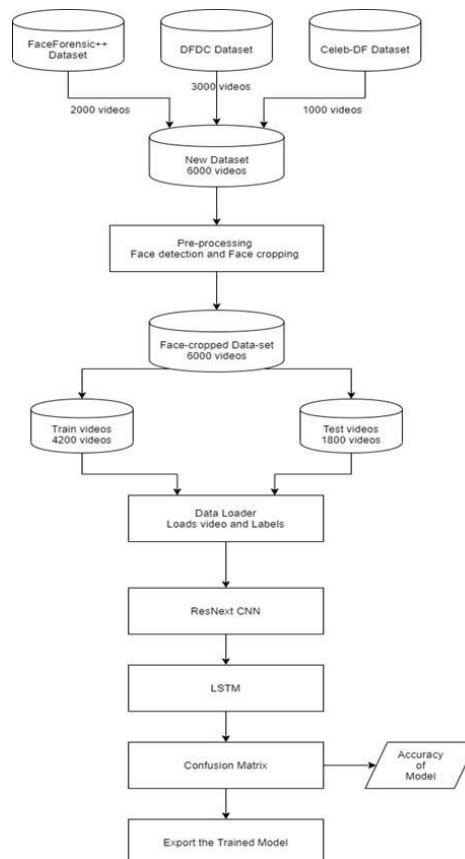
For implementation in the model, we employed PyTorch with Python 3 for its GPU acceleration and versatility, and Google Cloud Platform (GCP) for distributed training at large scale.

#### 3.1) Dataset Preprocessing :

- We trained our model on FaceForensics, DFDC, Celeb DF, and DeeperForensics 1.0, providing a balanced dataset of real and deepfake videos.
- Extraction of frames at a fixed frame rate.
- Face detection and face cropping through MTCNN.
- Data augmentation (blurring, brightness change, flipping).
- Normalizing pixel ranges to 0 and 1.

#### 3.2) Model Training Strategy :

- Pretraining ResNeXt CNN on ImageNet and then fine-tuning on deepfake datasets.
- Training LSTM-RNN to examine sequential inconsistencies between frames.
- Training workflow :



### 4. Evaluation :

We extensively tested our model on real-time video datasets, such as YouTube-based deepfakes. Traditional performance metrics were applied to estimate the accuracy and generalizability of the trained model.

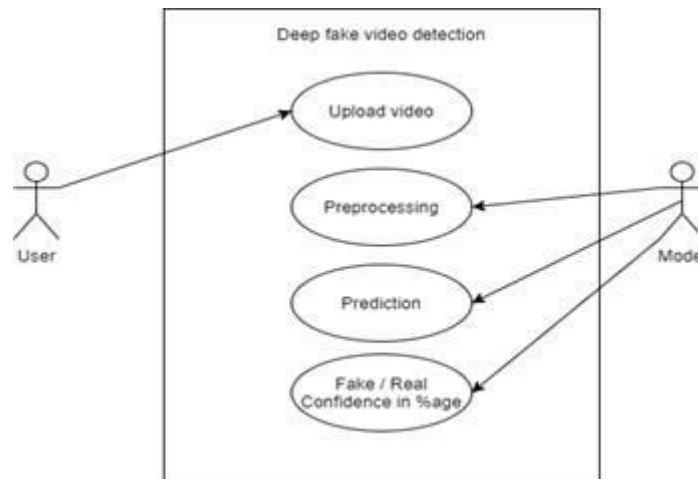
5. Deployment & Real-World Application :

For ease of use and accessibility, we built a front-end web application where users can input videos for deepfake detection.

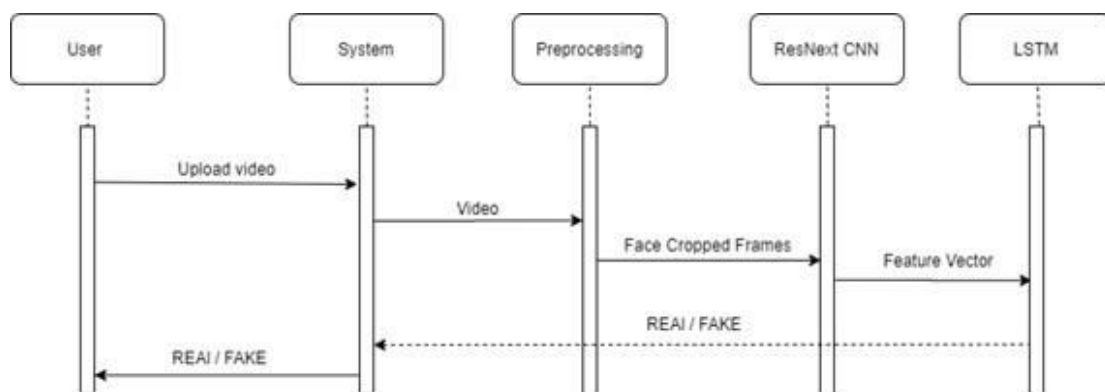
Workflow:

- User uploads a video.
- System extracts frames and feeds them through the ResNeXt + LSTM detection pipeline.
- Model classifies as "Real" or "Deepfake" with a confidence score.

6. Use case diagram :

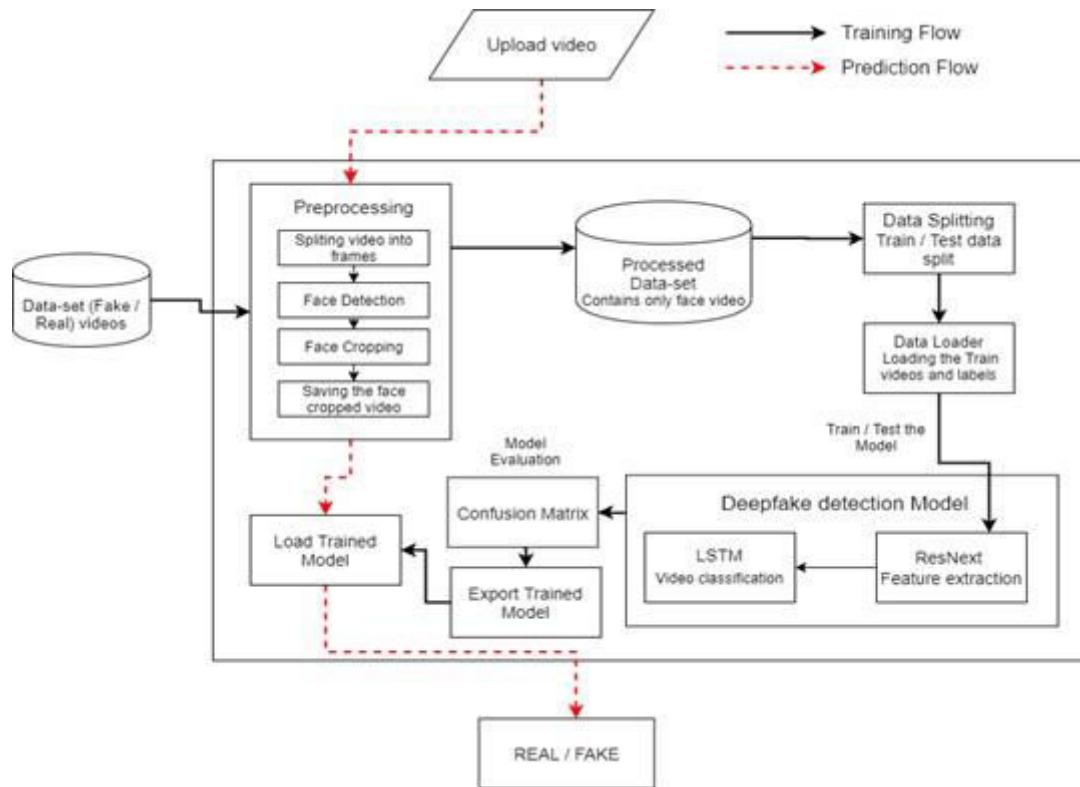


7. Sequence diagram :

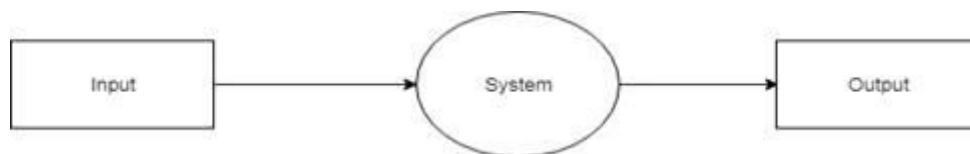


IV. SYSTEM ARCHITECTURE

- Figure of system architecture :

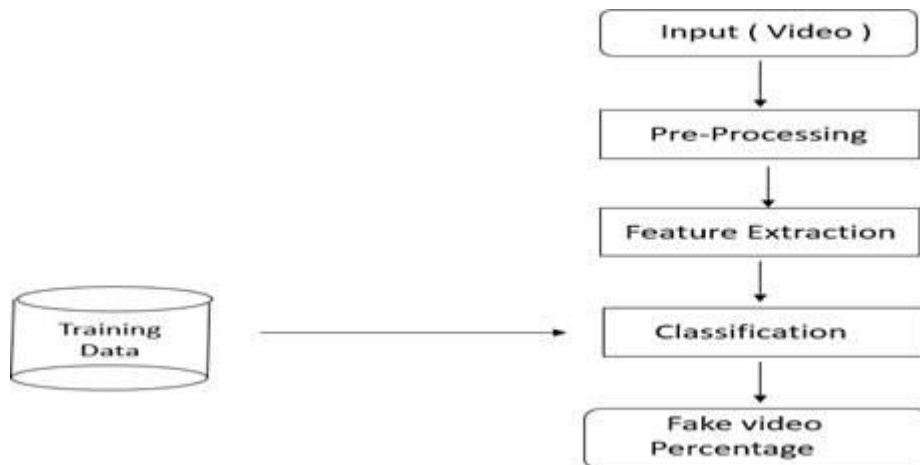


- DFD level 0 :

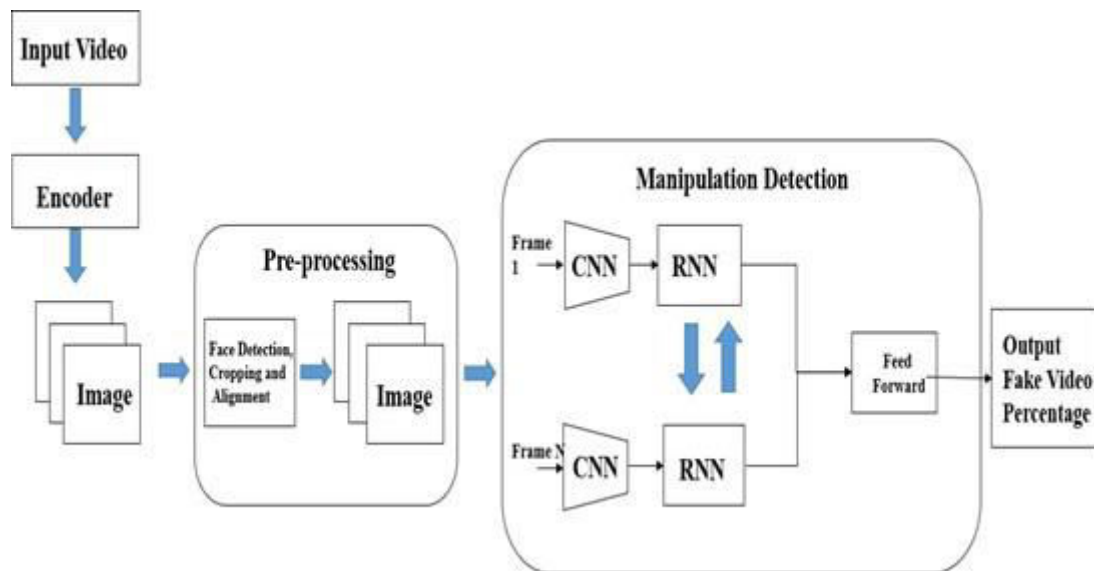


- Input: Here input to the system is uploading video.
- System: In system it shows all the details of the Video.
- Output: Output of this system is it shows the fake video or not.

- DFD level 1 :
- DFD level 1 gives more in and out information of the system.



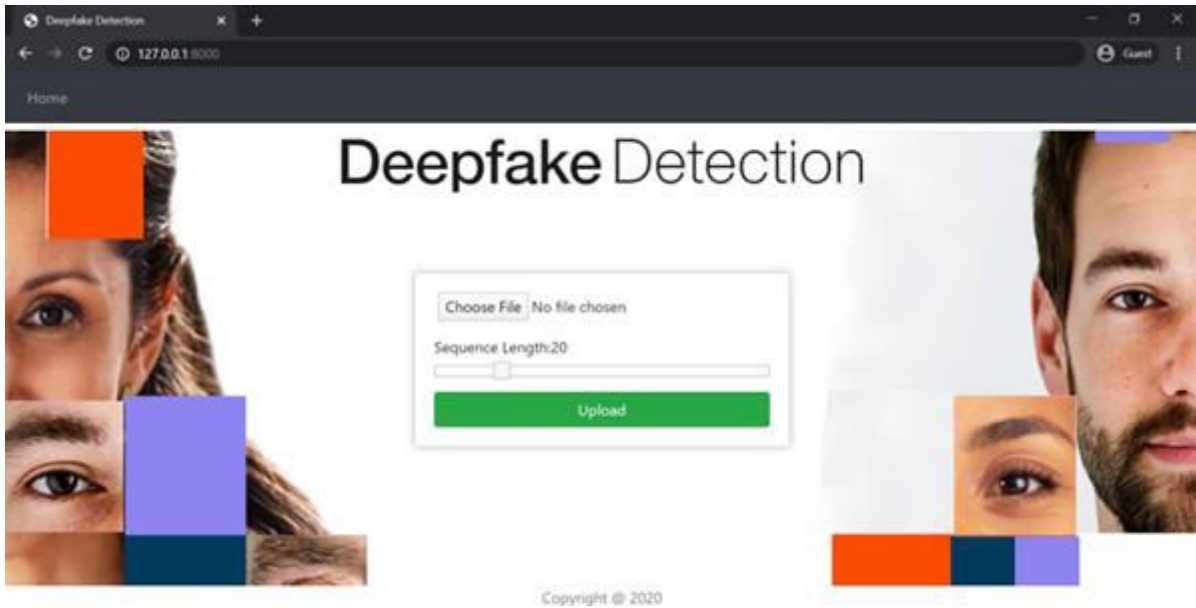
- DFD level 2 :
- It shows the enhance functionality used by user.



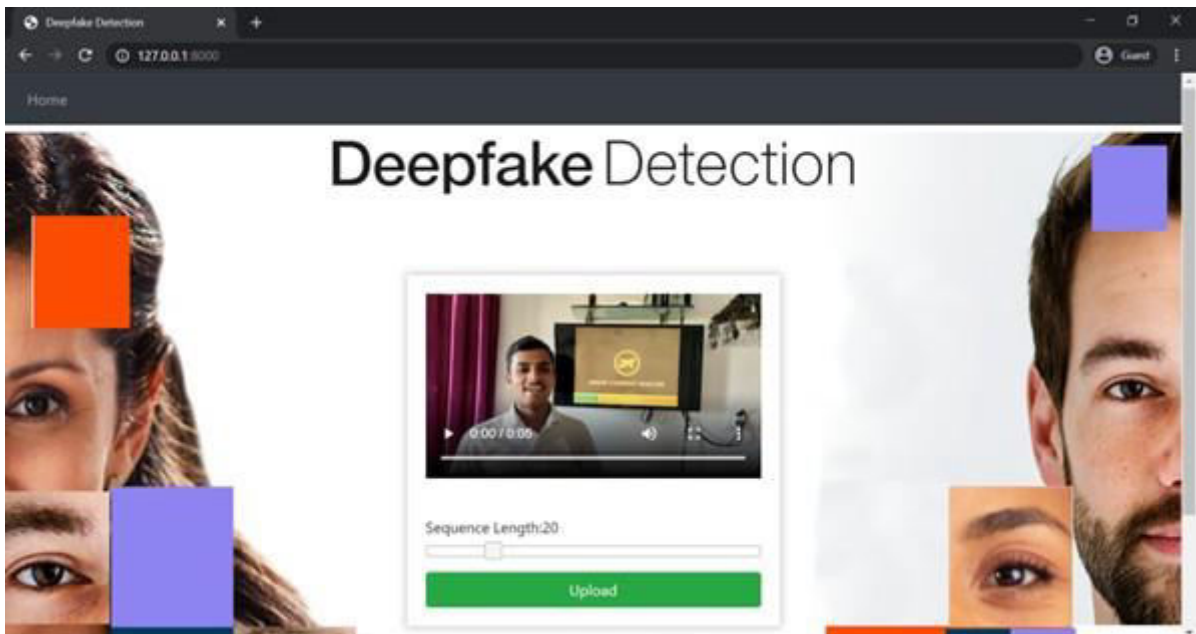


### V. TECHNICAL RESULT

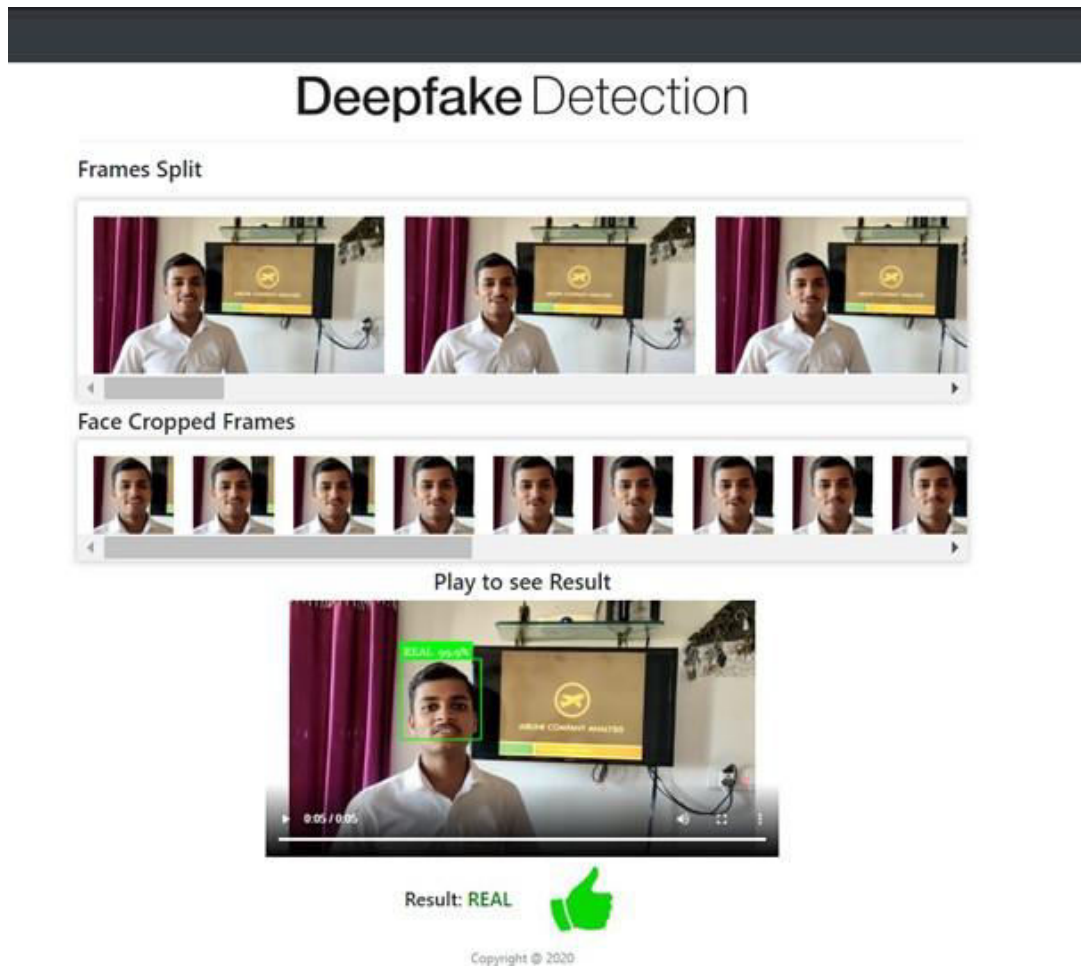
- Home Page :



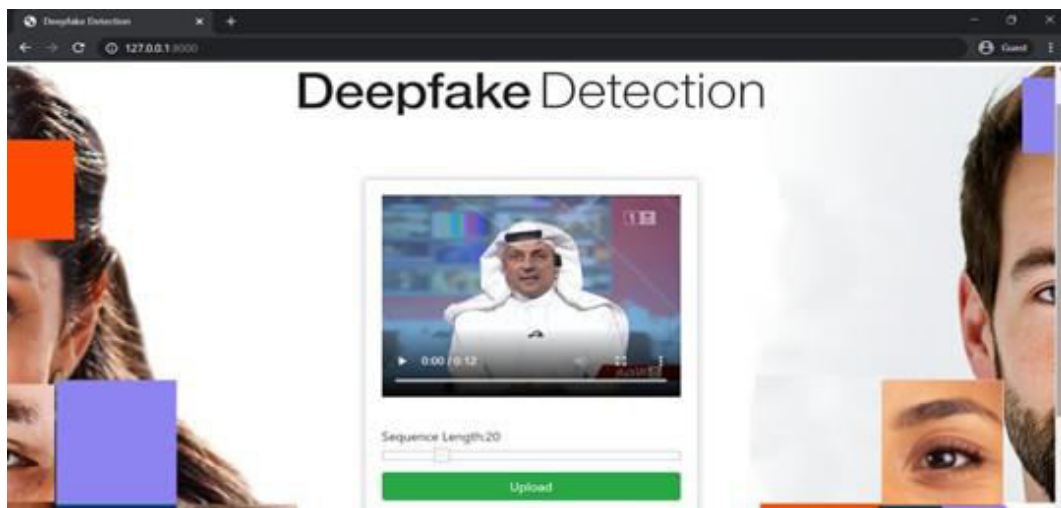
- Uploading a real video :



- Output of the real video :



- Uploading a fake video :



- Output of the fake video :



**Deepfake Detection**

Frames Split

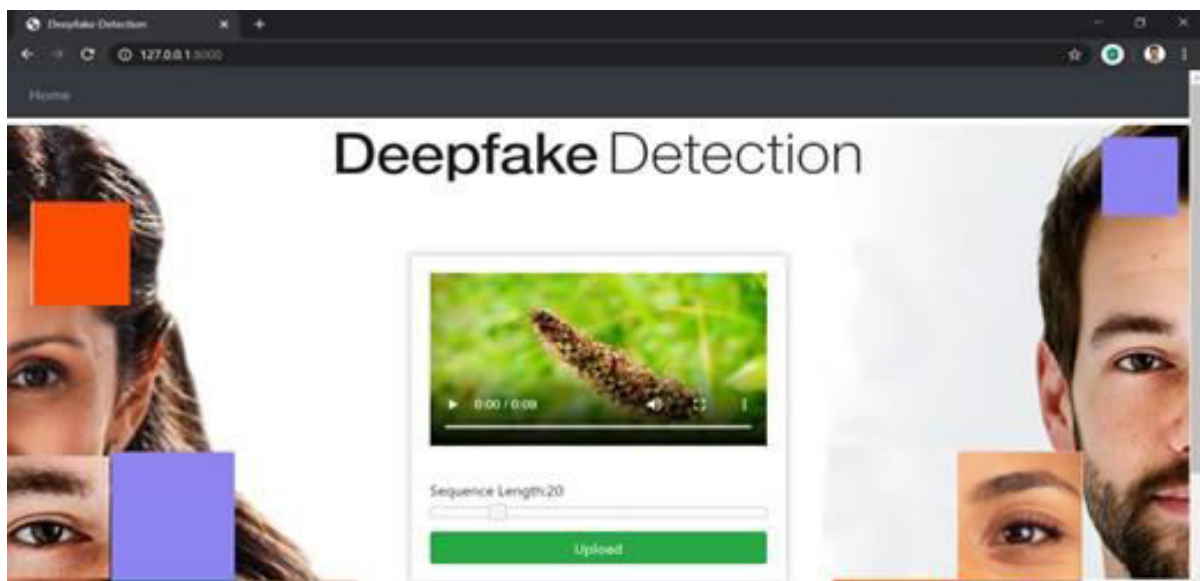
Face Cropped Frames

Play to see Result

Result: **FAKE**

Copyright © 2020

- Uploading video with no faces :



**Deepfake Detection**

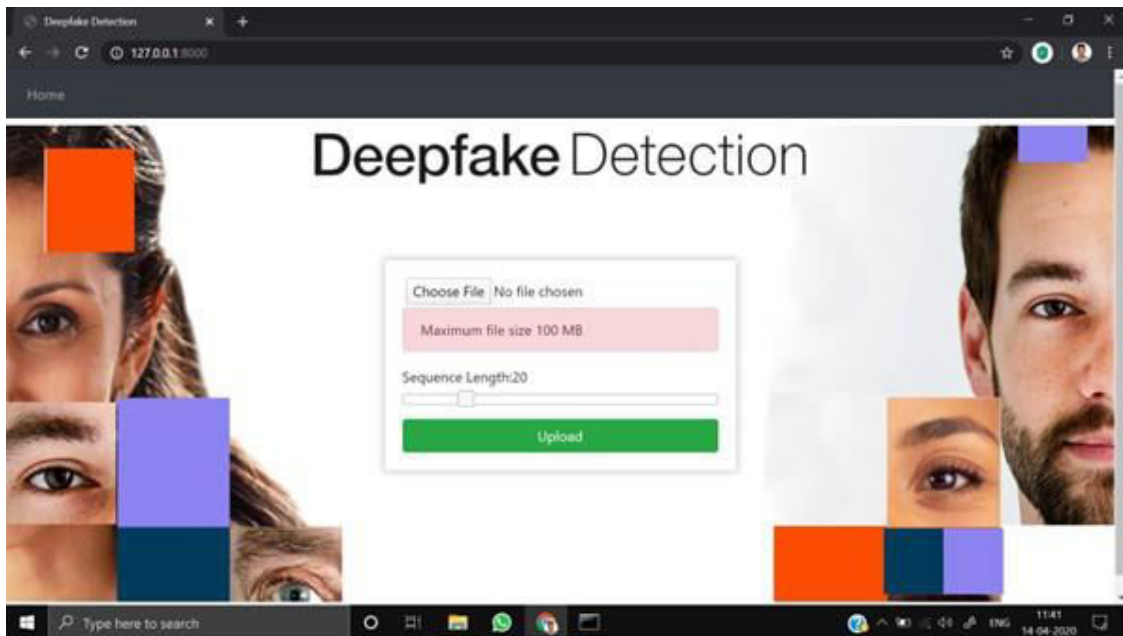
Sequence Length: 20

Upload

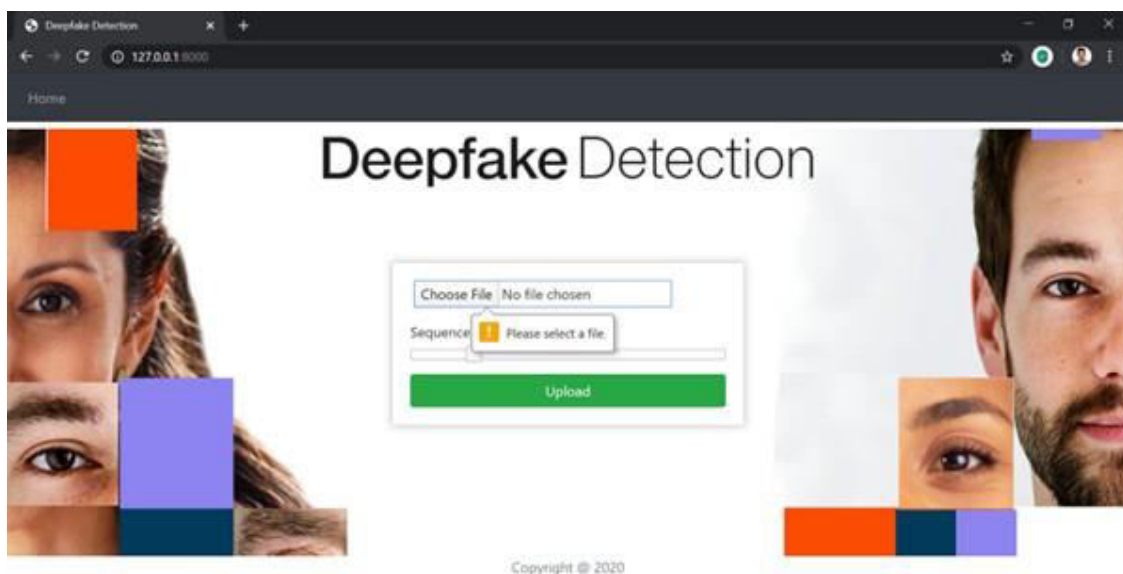
- Output of the no face video :



- Uploading a file greater than 100MB :



- Pressing Upload button without selecting a file :



## VI. CONCLUSION

Deepfake technology is increasingly sophisticated, and it is becoming increasingly difficult to differentiate between authentic and forged content. This is a cause of great concern regarding misinformation, identity theft, and media manipulation, and hence the importance of accurate detection techniques.

We created in this paper a neural network-based deepfake detection system that categorizes videos as real or fake and gives a confidence score for the prediction. Our strategy involves a pre-trained ResNeXt CNN for frame-level analysis and an LSTM-based RNN for inconsistency tracking across frames over time. The model handles 1 second of video (10 frames per second) and is capable of supporting various frame sequences (10, 20, 40, 60, 80, 100 frames) to provide flexibility in real-world applications. To make our system robust, we trained it on FaceForensics++, DFDC, Celeb DF, and DeeperForensics 1.0, which enabled it to identify deepfakes with good accuracy from various sources. We also developed a user-friendly application so that deepfake detection can be made available for social media monitoring, news verification, and digital forensics.

While our model does a good job, deepfake detection is an ongoing problem as the generated content is increasingly getting better with AI. Ongoing efforts must be dedicated to real-time detection, bolstering strength against adversarial attacks, and combining more cues such as audio and biometric signals. With deepfakes getting progressively sophisticated, being ahead of them with better and more versatile detection techniques will be ever-important in maintaining digital authenticity and curbing false information diffusion in the era where "seeing is no longer believing."

## REFERENCES

1. Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, Matthias Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images" in arXiv:1901.08971.
2. Deepfake detection challenge dataset : <https://www.kaggle.com/c/deepfake-detection-challenge/data> Accessed on 26 March, 2020
3. Yuezun Li , Xin Yang , Pu Sun , Honggang Qi and Siwei Lyu "Celeb-DF: A Large-scale Challenging Dataset for DeepFake Forensics" in arXiv:1909.12962
4. Deepfake Video of Mark Zuckerberg Goes Viral on Eve of House A.I. Hearing : <https://fortune.com/2019/06/12/deepfake-mark-zuckerberg/> Accessed on 26 March, 2020
5. deepfake examples that terrified and amused the internet : <https://www.creativebloq.com/features/deepfake-examples> Accessed on 26 March, 2020
6. TensorFlow: <https://www.tensorflow.org/> (Accessed on 26 March, 2020)
7. Keras: <https://keras.io/> (Accessed on 26 March, 2020)
8. PyTorch : <https://pytorch.org/> (Accessed on 26 March, 2020)
9. G. Antipov, M. Baccouche, and J.-L. Dugelay. Face aging with conditional generative adversarial networks. arXiv:1702.01983, Feb. 2017
10. J. Thies et al. Face2Face: Real-time face capture and reenactment of rgb videos. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 2387–2395, June 2016. Las Vegas, NV.
11. Face app: <https://www.faceapp.com/> (Accessed on 26 March, 2020)
12. Face Swap : <https://faceswaponline.com/> (Accessed on 26 March, 2020)
13. Deepfakes, Revenge Porn, And The Impact On Women : <https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact-on-women/>
14. The rise of the deepfake and the threat to democracy :
15. <https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy>(Accessed on 26 March, 2020)
16. Yuezun Li, Siwei Lyu, "ExposingDF Videos By Detecting Face Warping Artifacts," in arXiv:1811.00656v3.
17. Yuezun Li, Ming-Ching Chang and Siwei Lyu "Exposing AI Created Fake Videos by Detecting Eye Blinking" in arXiv:1806.02877v2.
18. Huy H. Nguyen , Junichi Yamagishi, and Isao Echizen " Using capsule networks to detect forged images and videos " in arXiv:1810.11215.
19. D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6.

20. Laptev, M. Marszalek, C. Schmid, and B. Rozenfeld. Learning realistic human actions from movies. Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pages 1–8, June 2008. Anchorage, AK
21. Umur Aybars Ciftci, İlke Demir, Lijun Yin “Detection of Synthetic Portrait Videos using Biological Signals” in arXiv:1901.02212v2
22. D. P. Kingma and J. Ba. Adam: A method for stochastic optimization. arXiv:1412.6980, Dec. 2014.
23. ResNext Model : [https://pytorch.org/hub/pytorch\\_vision\\_resnext/](https://pytorch.org/hub/pytorch_vision_resnext/) accessed on 06 April 2020
24. <https://www.geeksforgeeks.org/software-engineering-cocomo-model/> Accessed on 15 April 2020
25. Deepfake Video Detection using Neural Networks <http://www.ijrsrd.com/articles/IJSRDV8I10860.pdf>
26. International Journal for Scientific Research and Development <http://ijrsrd.com/>



INTERNATIONAL  
STANDARD  
SERIAL  
NUMBER  
INDIA



# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  [ijirset@gmail.com](mailto:ijirset@gmail.com)



[www.ijirset.com](http://www.ijirset.com)

Scan to save the contact details