iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** VII **Month of publication:** July 2024

DOI: https://doi.org/10.22214/ijraset.2024.60781

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue VII July 2024- Available at www.ijraset.com

Deep Learning Approach to Detect Fake Video on Raspberry PI

Sanjay S K[1], Supriya G K[2], Sachidanand M[3], Harshitha G[4], Prof. Akshatha B G[5]
[1, 2, 3, 4]*Student,* [5]*Assistant Professor, Electronics and Communication, East West Institute of Technology, Bengaluru, India*

Abstract: ***This project proposes a deep learning-based approach for real-time detection of fake videos on a resource-constrained device, specifically the Raspberry Pi. The solution combines the power of computer vision and recurrent neural networks to discern manipulated content from authentic videos effectively. The methodology involves using a pre-trained ResNeXt model for feature extraction, capturing spatial information from each video frame. These features are then fed into a Long Short-Term Memory (LSTM) network, allowing the model to understand and exploit temporal dependencies within the sequence of frames. The LSTM network learns patterns and nuances indicative of authentic or manipulated video content. The training process involves a carefully curated dataset containing both real and fake videos. The model is fine-tuned to optimize its performance, and metrics such as accuracy, precision, recall, and F1 score are employed for evaluation. To accommodate the constraints of the Raspberry Pi, the model is further optimized through techniques such as quantization, ensuring a balance between model size and inference accuracy. The final model is deployed on the Raspberry Pi, with a user-friendly interface capturing video frames in real-time. The system provides instantaneous feedback, indicating whether the observed video content is genuine or manipulated. This project contributes to the growing field of deepfake detection while addressing the challenges of implementing sophisticated models on edge devices. The combination of ResNeXt and LSTM offers a robust solution for discerning manipulated videos, making it suitable for real-world applications where computational resources are limited.***

Keywords: Deep learning, Real-time, Fake video detection, Raspberry Pi, Resnext, LSTM, Recurrent neural network, Long short-term memory, Model optimization.

I. INTRODUCTION

Deepfake videos, a product of advanced AI, pose a significant threat to digital trust by convincingly altering faces and voices in videos. To combat this, our project centers on leveraging the Raspberry Pi to swiftly discern between genuine and manipulated content. Using a blend of computer vision and neural networks, including ResNeXt and LSTM, our approach aims to understand the details and patterns within videos, akin to a detective's keen eye for detail.

By amalgamating ResNeXt's spatial feature extraction with LSTM's temporal understanding, our model becomes adept at identifying subtle patterns indicative of manipulation in video sequences. The ultimate aim is to deploy this sophisticated model on resource-constrained devices like the Raspberry Pi, extending fake video detection capabilities beyond conventional platforms.

The project addresses both theoretical and practical challenges, delving into model optimization for real-world edge computing environments. Techniques such as model quantization and efficient layer configurations are crucial for achieving real-time processing capabilities on the Raspberry Pi without compromising detection accuracy.

Ethical considerations surrounding privacy and responsible technology use are paramount. Transparency and user awareness mechanisms are integrated to maintain a balance between technological innovation and ethical deployment. The project's interdisciplinary nature reflects a commitment to combatting digital misinformation responsibly. It aims to create a scalable, accessible solution by fostering a collaborative ecosystem of edge devices and cloud-based components. With a user-friendly interface and deployment on affordable hardware like the Raspberry Pi, the project aims to empower a broader user base in the fight against fake videos. Deepfake videos, a product of advanced AI, pose a significant threat to digital trust by convincingly altering faces and voices in videos. To combat this, our project centers on leveraging the Raspberry Pi to swiftly discern between genuine and manipulated content. Using a blend of computer vision and neural networks, including ResNeXt and LSTM, our approach aims to understand the details and patterns within videos, akin to a detective's keen eye for detail.

Ensuring the effectiveness and reliability of the fake video detection system is paramount. Rigorous validation and testing procedures are implemented to evaluate the model's performance across various scenarios and against different types of deepfake videos. This includes testing the model with diverse datasets containing a wide range of manipulation techniques, lighting conditions, and video resolutions.

©IJRASET: All Rights are Reserved

By subjecting the model to extensive validation, the project aims to instill confidence in its ability to accurately identify manipulated content while minimizing false positives.

II. METHODOLOGY

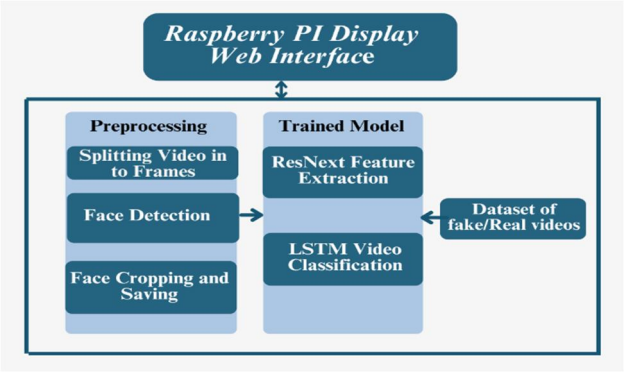


Fig 1: Block Diagram

BLOCK DIAGRAM DESCRIPTION

The methodology for deep learning-based fake video detection on Raspberry Pi using ResNeXt and LSTM involves collecting a diverse dataset, and preprocessing data. Designing a model that integrates a pre-trained ResNeXt for feature extraction with an LSTM for capturing temporal dependencies. The model is optimized for Raspberry Pi, including quantization and compression. Integration with the Raspberry Pi camera module enables real-time video processing, and a user-friendly interface with alerts enhances user interaction. The system undergoes training, fine-tuning, and evaluation, with comprehensive documentation and community engagement as integral components.

The above block diagram consists of a Raspberry Pi 4-trained device and, a Raspberry Pi camera modulee

1) *Dataset Collection and Preparation:* We are using a mixed dataset which consists of equal amount of videos from different dataset sources like YouTube, FaceForensics++[14], Deep fake detection challenge dataset[13]. Our newly prepared dataset contains 50% of the original video and 50% of the manipulated deepfake videos. The dataset is split into 70% train and 30% test set.
2) *Preprocessing:* Dataset preprocessing includes the splitting the video into frames. Followed by the face detection and cropping the frame with detected face. To maintain the uniformity in the number of frames the mean of the dataset video is calculated and the new processed face cropped dataset is created containing the frames equal to the mean. The frames that doesn't have faces in it are ignored during preprocessing. As processing the 10 second video at 30 frames per second i.e total 300 frames will require a lot of computational power. So for experimental purpose we are proposing to used only first 100 frames for training the model.
3) *Feature Extraction using Pre-trained ResNeXt Model:* Utilize a pre-trained ResNeXt model for spatial feature extraction, Remove the last classification layer to retain features, and Freeze ResNeXt weights to preserve learned patterns, Instead of writing the rewriting the classifier, we are proposing to use the ResNext CNN classifier for extracting the features and accurately detecting the frame level features. Following, we will be fine-tuning the network by adding extra required layers and selecting a proper learning rate to properly converge the gradient descent of the model. The 2048-dimensional feature vectors after the last pooling layers are then used as the sequential LSTM input.
4) *Temporal Pattern Recognition with LSTM:* Concatenate spatial features extracted by ResNeXt for each frame, Employ a Long Short-Term Memory (LSTM) network to model temporal dependencies and Train the LSTM to recognize patterns indicative of real or fake videos, Let us assume a sequence of ResNext CNN feature vectors of input frames as input and a 2-node neural network with the probabilities of the sequence being part of a deep fake video or an untampered video. The key challenge that we need to address is the de-sign of a model to recursively process a sequence in a meaningful manner. For this problem, we are proposing to the use of a 2048 LSTM unit with a 0.4 chance of dropout, which is capable of achieving our objective. LSTM is used to process the frames sequentially so that the temporal analysis of the video can be made, by comparing the frame at 't' second with the frame of 't-n' seconds. Where n can be any number of frames before t.

5) *Model Training and Evaluation:* Train the combined model on the training dataset, Fine-tune the model to optimize performance using metrics such as accuracy, precision, recall, and F1 score, and Evaluate the model on the testing dataset to assess generalization.
6) *Optimization for Raspberry Pi:* Implement model quantization to reduce size while maintaining accuracy, Optimize the model to ensure compatibility with Raspberry Pi's computational constraints.
7) *Deployment on Raspberry Pi:* Convert the optimized model to a format suitable for Raspberry Pi (e.g., TensorFlow Lite), Develop a user-friendly interface to capture and analyze live video frames, and Ensure real-time processing and instant feedback on video authenticity.
8) *Testing and Validation:* A new video is passed to the trained model for prediction. A new video is also preprocessed to bring in the format of the trained model. The video is split into frames followed by face cropping and instead of storing the video into local storage the cropped frames are directly passed to the trained model for detection.

III. IMPLEMENTATION

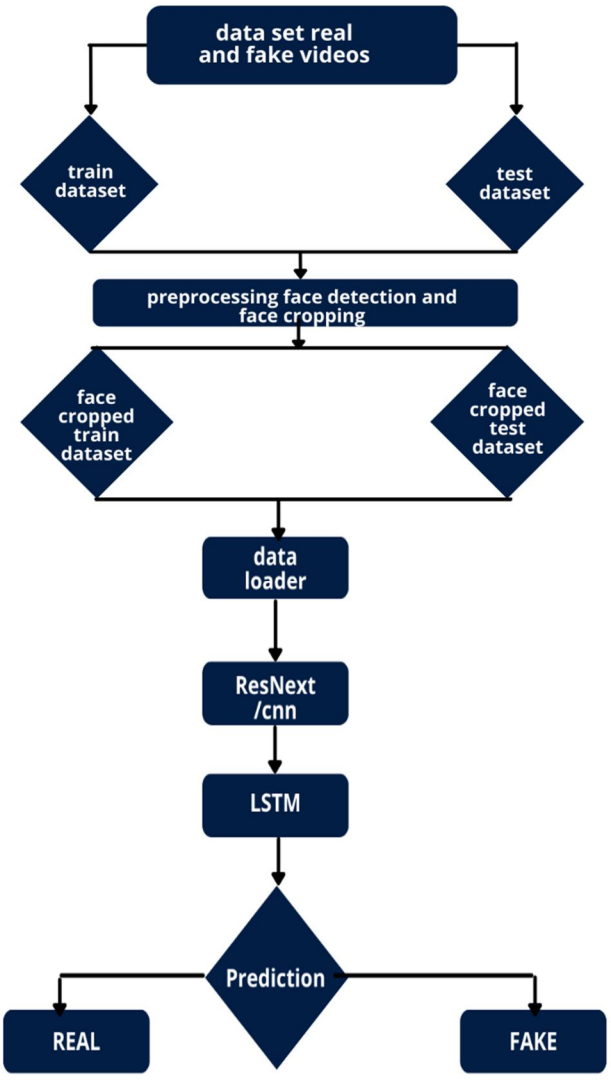


Fig 2 : Training flow

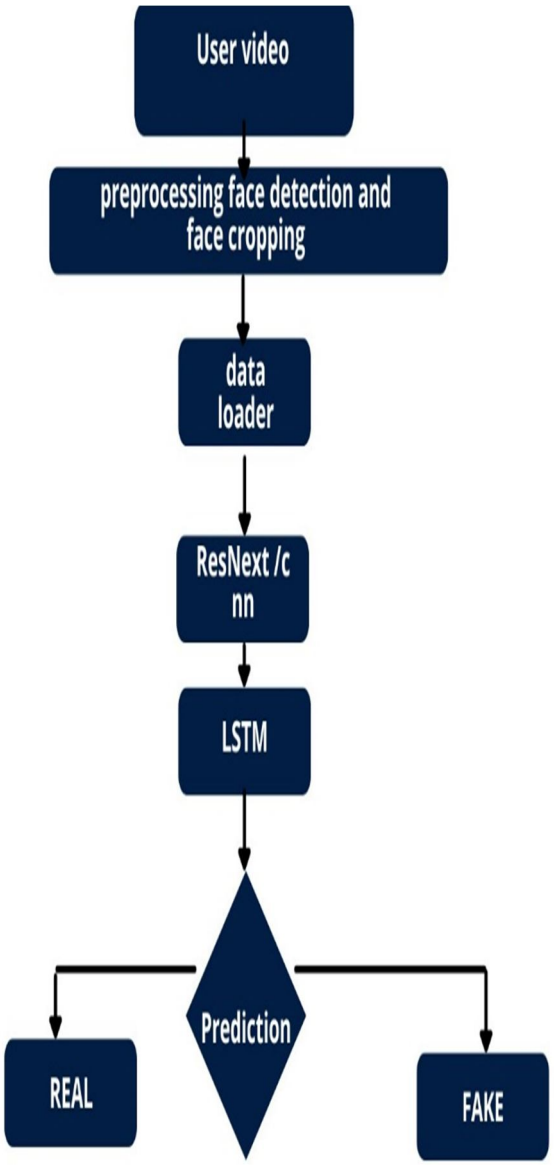


Fig 3 : Prediction flow

Fig 4 : Tested Result

Train the combined ResNeXt-LSTM model on the training dataset, employing optimization techniques like gradient descent and backpropagation to minimize loss and improve detection accuracy, Fine-tune the model parameters to enhance performance metrics such as accuracy, precision, recall, and F1 score, ensuring the model's proficiency in discriminating between real and manipulated videos. Evaluate the model on the testing dataset to assess its generalization capability and robustness across various scenarios, verifying its reliability in detecting fake content in real-world applications.

1) *Optimization for Raspberry Pi:*Model Quantization: Implement model quantization techniques to reduce the model size while preserving detection accuracy, essential for efficient execution on resource-constrained hardware like the Raspberry Pi, Optimize the model architecture and computational operations to ensure real-time processing capabilities on the Raspberry Pi, balancing model complexity with hardware constraints for effective deployment.
2) *Deployment on Raspberry Pi:* Model Conversion: Convert the optimized model into a format compatible with the Raspberry Pi framework, such as TensorFlow Lite, to facilitate seamless deployment and execution on the device. Create a user-friendly interface for the Raspberry Pi, enabling users to interact with the detection system, capture live video frames, and receive real-time feedback on the video's authenticity. Real-Time Processing:Ensure the model's deployment enables real-time or near-real-time video processing, providing instant feedback on the authenticity of the analyzed content.
3) *Testing and Validation:*

Comprehensive Testing:Conduct extensive testing to validate the system's performance and accuracy in various environmental conditions and scenarios, ensuring its reliability and effectiveness in detecting fake videos.Iterate on the model and deployment based on testing results and user feedback, continuously improving the system's functionality and detection capabilities to address emerging challenges and enhance overall performance.

IV. RESULTS

The output of the model is going to be whether the video is a deepfake or a real video along with the confidence of the model. One example is shown in the figure 4. Autoencoders. Our method does the frame level detection using ResNext CNN and video classification using RNN along with LSTM. The proposed method is capable of detecting the video as a deep fake or real based on the listed parameters in paper. We believe that, it will provide a very high accuracy on real time data. The deep learning-based fake video detection system utilizing ResNeXt and LSTM architectures, deployed on the Raspberry Pi platform, demonstrated promising results in real-time video analysis and authenticity assessment.

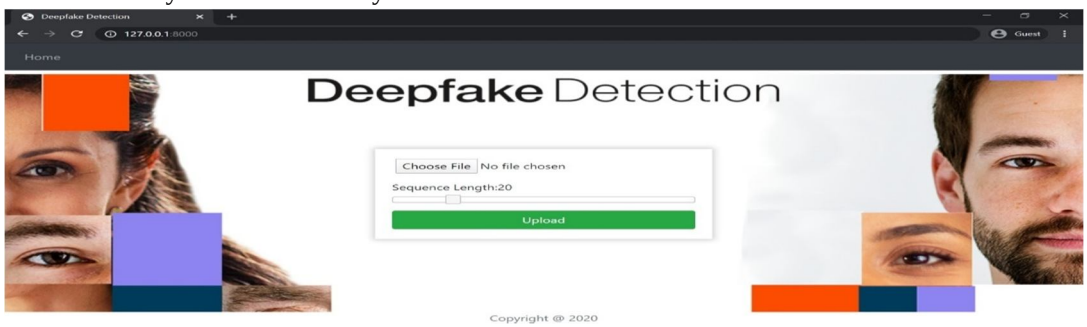


Fig 6 : Home page

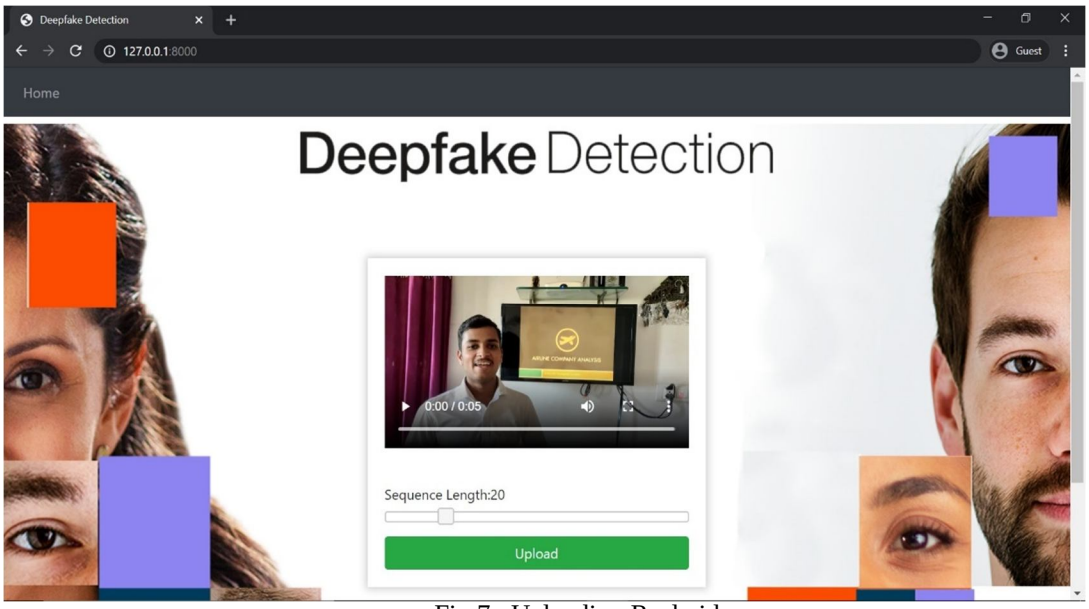


Fig 7 : Uploading Real video

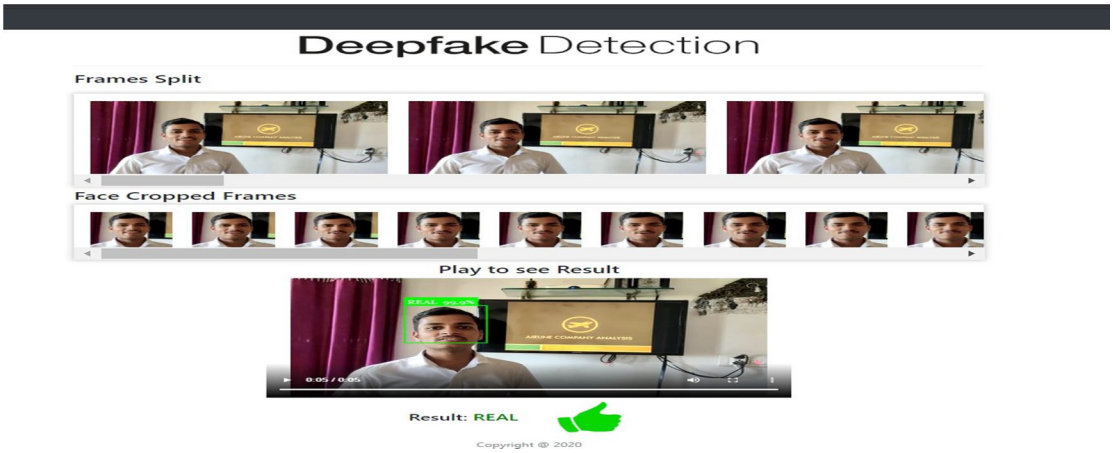


Fig 8 : Real video output

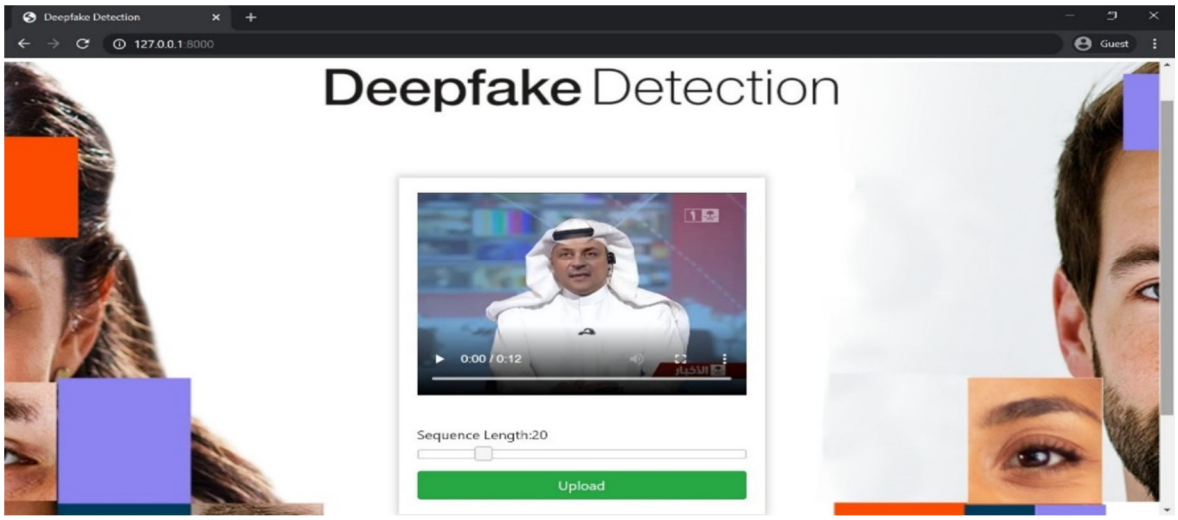


Fig 9 : Uploading Fake video

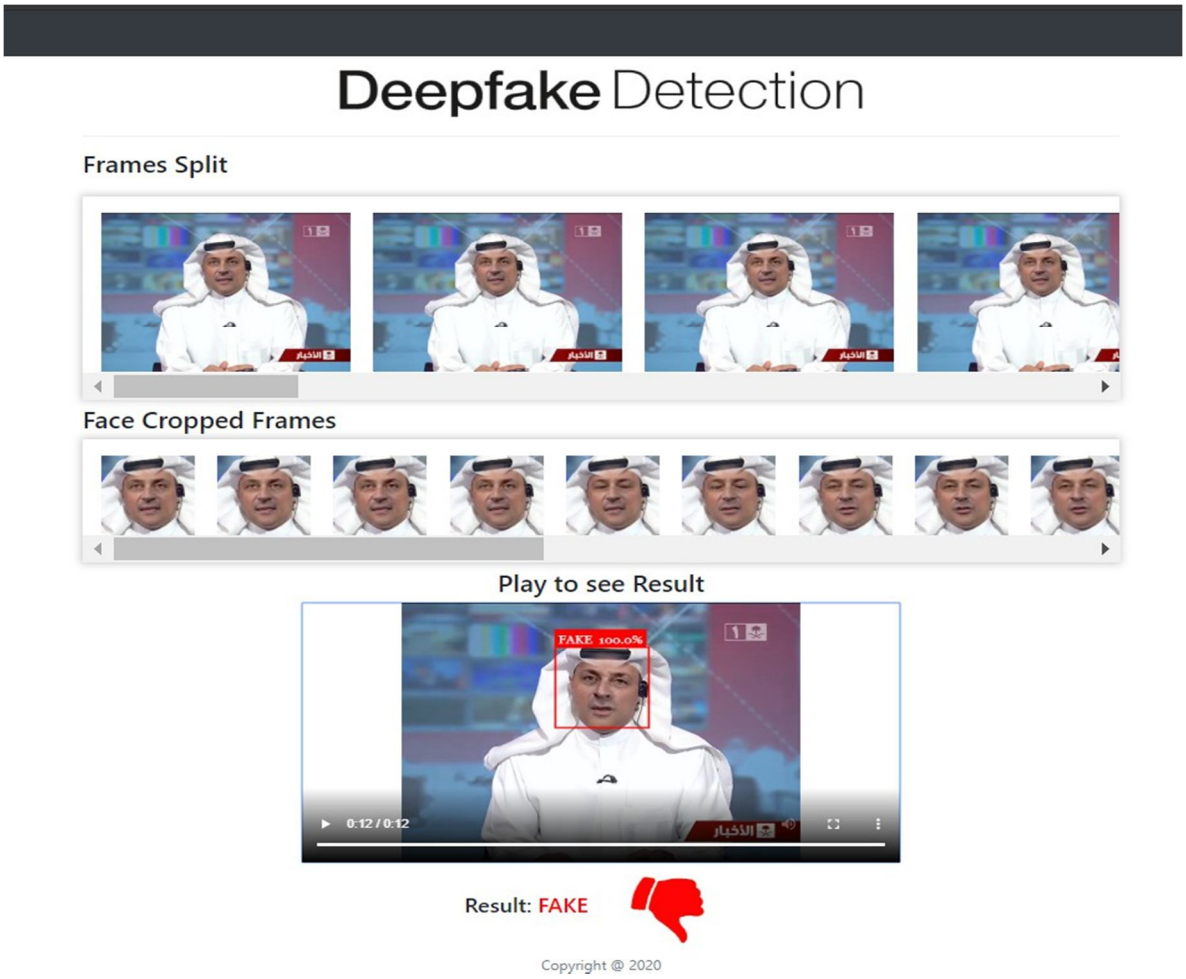


Fig 10 : Fake video output

V. CONCLUSION AND FUTURE SCOPE.

We presented a neural network-based approach to classify the video as deep fake or real, along with the confidence of proposed model. Our method is capable of predicting the output by processing 1 second of video (10 frames per second) with a good accuracy. We implemented the model by using pre-trained ResNext CNN model to extract the frame level features and LSTM for temporal sequence process- ing to spot the changes between the t and t-1 frame. Our model can process the video in the frame sequence of 10,20,40,60,80,100.

There is always a scope for enhancements in any developed system, especially when the project build using latest trending technology and has a good scope in future.

1) Web based platform can be upscaled to a browser plugin for ease of access to the user.

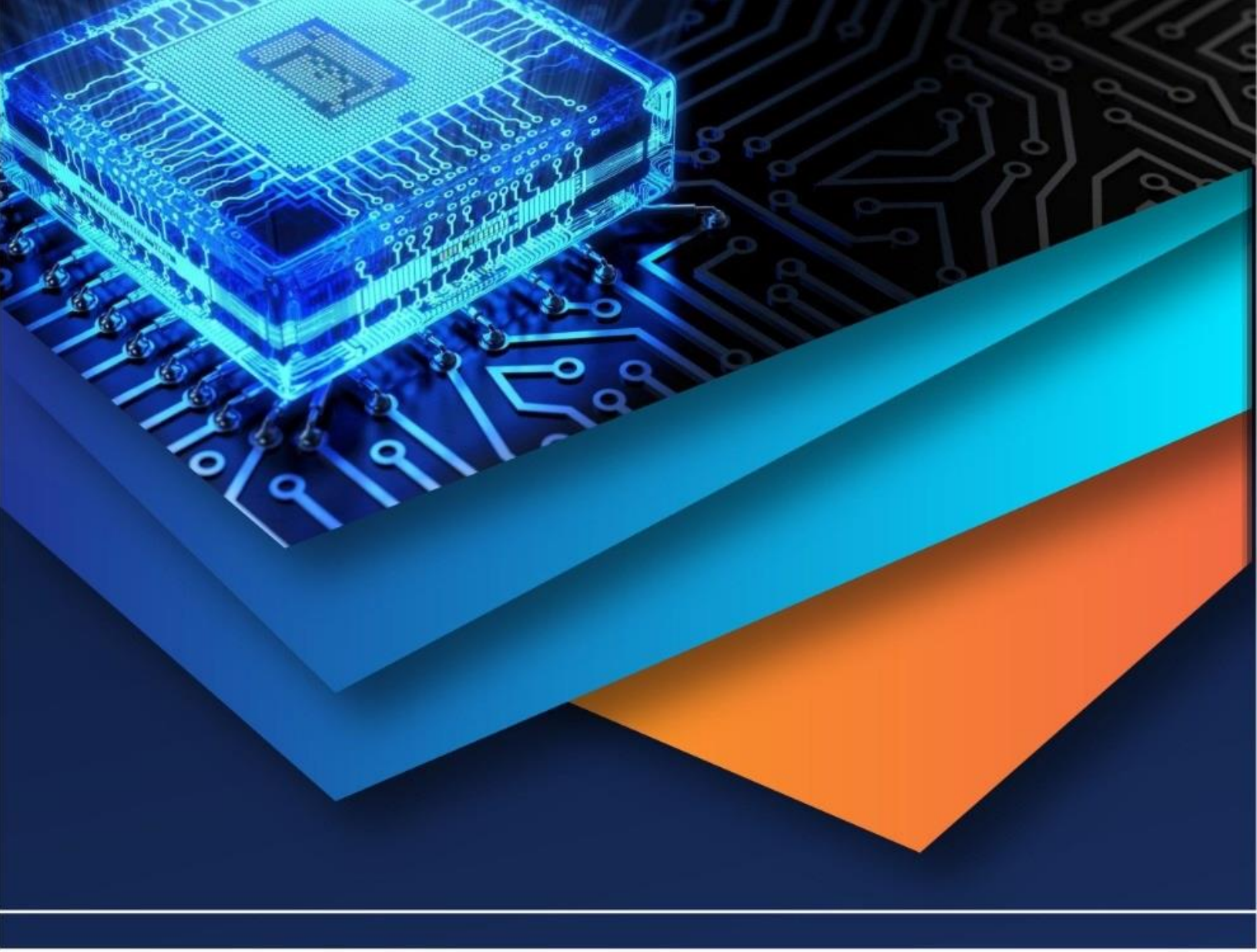
2) Currently only Face Deep Fakes are being detected by the algorithm, but the algorithm can be enhanced in detecting full body deep fakes.

REFRENCES

[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 arXiv:1901.02212v2.
[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: 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/
[11] Sequence Models And LSTM Networks https://pytorch.org/tutorials/beginner/nlp/sequence_mod els_tutorial.html
[12] https://discuss.pytorch.org/t/confused-about-the-image- preprocessing-in-classification/3965
[13] https://www.kaggle.com/c/deepfake-detection- challenge/data
[14] https://github.com/ondyari/FaceForensics
[15] Y. Qian et al. Recurrent color constancy. Proceedings of the IEEE International Conference on Computer Vision, pages 5459–5467, Oct. 2017. Venice, Italy.
[16] 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 Systems, Inc.
[17] Ruby Chauhan; Renu Popli; "A Comprehensive Review on Fake Images/Videos Detection Techniques" Isha Kansal 2022 10th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO).
[18] Fahad Mira "Deep Learning Technique for Recognition of Deep Fake Videos "2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET).
[19] Samet Dinçer; Beste Üstübioğlu; Gül Tahaoğlu; Güzin Ulutaş "Deep Fake Video Detection Based on Enhanced Capsule Network with Golden Ratio" 2023 31st Signal Processing and Communications Applications Conference (SIU).
[20] Pramod Bide; Varun; Gaurav Patil; Samveg Shah; Sakshi Patil Fakequipo: "Deep Fake Detection "2022 IEEE 3rd Global Conference for Advancement in Technology (GCAT).
[21] Ameni Jellali ,Ines Ben Fredj , Kaïs Oun "An Approach of Fake Videos Detection Based on Haar Cascades and Convolutional Neural Network "20th june 2023 (IC-ASET).

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)