

DEEPPFAKE VIDEO DETECTION USING RECURRENT NEURAL NETWORK

¹Naveen kumar J,²Vinay K,³Anand G,⁴Dr. S. Suryanarayana

^{1,2,3}UG-Electronics and communication Engineering , Maturi Venkata Subba Rao Engineering College, Nadergul, Hyderabad-501510

⁴Professor, Electronics and Communication Engineering, Maturi Venkata Subba Rao Nadergul, Hyderabad-501510

Abstract:

The authenticity of visual content has become a serious concern due to the rapid growth of deepfake technology. Videos known as "deep fakes," which realistically superimpose one person's image over another, can be used for both harmful disinformation and innocent amusement. It's critical to identify these doctored recordings in order to preserve media accuracy and confidence. In this work, we present a novel method for deepfake video detection that combines a graphical user interface with deep learning algorithms. Our approach uses a sizable dataset of both real and deepfake films to train a deep neural network. To capture both spatial and temporal information, these features are subsequently fed into a sequence of convolutional and recurrent layers.

Keywords : Superimpose, Misinformation, Neural Network, spatial

1.Introduction:

The rapid development of deepfake technology has raised severe concerns about the validity of visual information. Videos that realistically superimpose one person's visage over another are referred to as "deep fakes," and they can be used for both benign entertainment and malicious misinformation. To maintain media credibility and integrity, it is imperative to identify these altered recordings. In this study, we provide a new approach to deepfake video detection by integrating deep learning algorithms with a graphical user interface. Our method trains a deep neural network on a large dataset of actual and deepfake movies. These features are then fed into a series of convolutional and recurrent layers to capture both temporal and spatial information.

2.LITERATURE SURVEY:

1.Deepfake video detection using res-next cnn and lstm. S. Jeevidha, S. Saraswathi, Kaushik J B, Preethi K, NallamVenkataramaya. This research uses a combo of ResNext CNN (for frame analysis) and LSTM (for video sequence analysis) to detect deepfakes. It extracts features from each frame and analyzes how they change over time to spot inconsistencies caused by manipulation. This method achieves good results in identifying deepfake videos.

The model's effectiveness relies heavily on the quality and size of the training data. Biases or limitations in the data can affect the model's generalizability.

2.Deepfake Detection using Spatiotemporal Convolutional Networks. Oscar de Lima, Sean Franklin, Shreshtha Basu, Blake Karwoski, Annet George. This study introduces a CNN-based method for identifying deepfake videos. In order to differentiate between authentic and fraudulent content, it focuses on extracting spatiotemporal data from video frames. It may not be able to identify deeper fake tactics that are more sophisticated because it mainly concentrates on spatial information.

3.Detection through Deep Learning. Deng Pan, Lixian Sun, Rui Wang, Xingjian Zhang, Richard O. Sinnott. In order to automatically detect deepfake films, the study provides two approaches for classification tasks: Xception and MobileNet, which are deepfake detection technologies. It is possible to train deepfake generators to generate adversarial examples, which are created with the

express purpose of misleading deepfake detection methods. These illustrations could be used by bad actors to take advantage of model flaws and produce more realistic deepfakes.

4. Deepfake Video Detection Using

Convolutional Neural Network. Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhikar, Saurabh Agrawal.

This research presents a method for identifying and differentiating between real and fake films by utilising CNNs, a type of deep learning. The techniques for creating deepfakes are always changing, so CNNs that have been trained on a particular set of deepfake variations might not be able to handle new and complex manipulations with ease.

5. Face Forensics++: Learning to Detect Manipulated Facial Images.

Andreas Rössler, Davide Cozzolino, Luisa

Verdoliva, Christian Riess, Justus Thies, Michael Nießner. This study offers a large dataset (Face Forensics++) for the identification of face picture alteration. It assesses how well different methods—including CNNs—identify photos that have been altered. Although it discusses picture manipulation, deep fake videos are not the main topic of discussion.

6. Exposing Deep Fake Videos by Detecting Face Warping Artifacts. Chih-Chung Hsu, Chia-Yen Lee, Yi-Xi u Zhuang. Finding distortions or discrepancies in facial characteristics that arise from the alteration procedure is the focus of this research. As deepfake technology advances, detection methods that are exclusively focused on face warping artefacts may become less effective.

7: Learning to Detect Fake Face Images in the Wild. Chih-Chung Hsu, Chia-Yen Lee, Yi-Xi u Zhuang. The paper introduces a deep learning-based approach for detecting fake face images. It presents a novel dataset and employs CNNs for effective classification of manipulated face images. The paper concentrates on images and does not delve into video-based deep fake detection.

8: Deep Fake Image Detection.

Omkar Salpekar. Identifying altered or synthetic photos produced with deep learning algorithms is known as deep fake image detection. Deep neural networks, including Generative Adversarial Networks (GANs), are usually used to create deep fake images. Deep fake detection models might not be real-time processing-optimized, which is necessary for applications like online platforms and video streaming services that need quick responses.

9: Spatial Video Forgery Detection and Localization using Texture Analysis of Consecutive

Frames Mubashar Sadique,

Khurshid Asghar, Usama Ijaz. The technique attempts to improve the detection accuracy of spatial video forgeries by utilising advances in electrical and computer engineering, making a significant contribution to the field of digital forensics. In circumstances where there are dynamic scenes or textures that change quickly, the efficacy of the suggested method to detect spatial video forgeries may be limited.

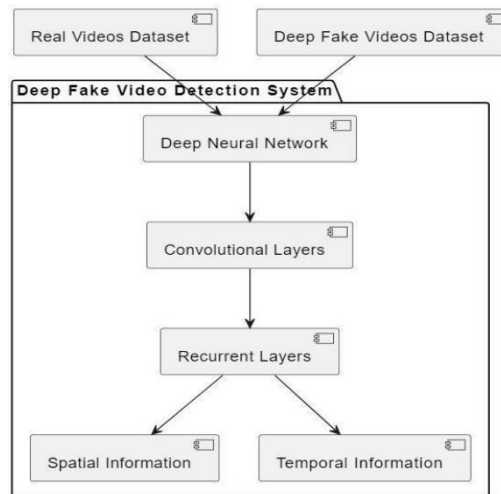
3. METHODOLOGY

A. Proposed System

The prepared dataset is used to train the deep neural network. The programme is supposed to pick up on the distinct patterns and traits connected to actual and deepfake films.

The model optimises its capacity to distinguish between real and modified information during training by adjusting its parameters to minimise the discrepancy between anticipated and actual labels. User-Friendly Graphical User Interface (GUI): You stress the significance of a user-friendly GUI in addition to the technical parts of your technique. This is an essential component for real-world use, making it simple for consumers to engage with and make use of the deep fake detection system. It is possible that the GUI offers features like the ability to submit movies for analysis, show detection findings, and have controls that are easy to use.

5. System Architecture:



Proposed Algorithm: The system uses LSTM is used for classification and DenseNet for feature extraction

Key components of LSTM and DENSENET

LSTM(Long Short Term Memory):

- Memory: It may recall significant information for extended or brief intervals.
- Forget Gate: Selects which historical data to disregard.
- Input Gate: Selects fresh data to append to the memory.
- Output Gate: Selects what should be output by using both recent and historical memory.

DenseNet(Dense Connected Convolutional Network):

- Connected Blocks: Every layer in a block is connected to every other layer.
- Feature Reuse: Promotes the reuse of features from lower tiers.
- Transition Layers: These lower block-to-block dimensions.
- Global Average Pooling: To simplify output, pooling is used in place of dense layers.
- Encourages Gradient Flow: During training, dense connections improve the flow of gradients.

6. Working:

The general working process of our proposed system:

Dataset Preparation:

• Start by collecting a large dataset containing both real and deep fake vids. A different dataset is pivotal for training a robust model.

Deep Neural Network Architecture:

- Propose the use of a deep neural network for video analysis. Since videos involve both spatial and temporal information, you incorporate convolutional and recurrent layers in your architecture.
- Convolutional layers are effective in capturing spatial features, allowing the model to identify patterns and features within individual frames of the video.

Feature Extraction:

- The features extracted from the videos serve as inputs to the deep neural network. These features likely include both spatial (frame-based) and temporal (sequencebased) information.
- The network learns to distinguish between features present in real videos and those introduced by the deep fake generation process.

Training Process:

- The deep neural network is trained using the prepared dataset. The objective is for the model to learn the unique patterns and characteristics associated with both real and deep fake videos.
- During training, the model adjusts its parameters to minimize the difference between predicted and actual labels, optimizing its ability to discern between real and manipulated content.

User-Friendly Graphical User Interface (GUI):

- In addition to the technical aspects of your methodology, you emphasize the importance of a user-friendly GUI. This is a crucial element for practical application, enabling users to easily interact with and utilize the deep fake detection system.
- The GUI likely provides functionalities such as uploading videos for analysis, displaying detection results, and offering user-friendly controls.

Evaluation and Validation:

- After training the model, you assess its performance using a separate validation dataset. This step ensures that the model generalizes well to new, unseen data.
- Metrics such as accuracy, precision, recall, and F1 score can be used to evaluate the model's effectiveness in distinguishing between real and deep fake videos.

Deployment:

- Once the model demonstrates satisfactory performance, it can be deployed for real-world use. The user-friendly GUI facilitates easy integration and adoption by users who may not have deep technical expertise.

7.OUTPUT:

Table 7.1 Comparative analysis of different sized datasets

Training data	Testing data	Accuracy
60%	40%	71%
70%	30%	75%
80%	20%	83%

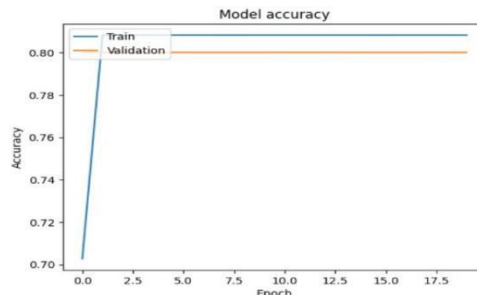


Fig 7.1 accuracy of train model

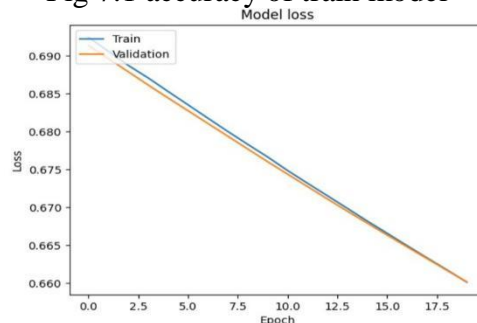


Fig 7.2 loss of the trained model

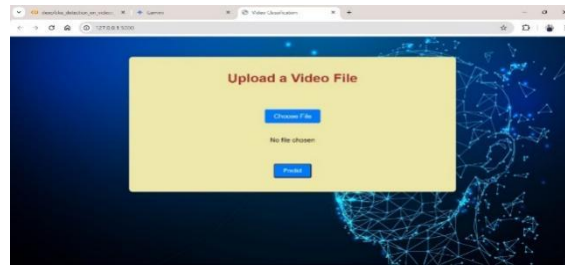


Fig 7.1 For Uploading video



Fig 7.2 Classified as a Real video



Fig 7.3 Classified as a Fake video

8. Conclusion:

In conclusion, the development of a deep fake video detection system utilizing deep learning and transfer learning, integrated into a user-friendly GUI application, represents a significant step towards addressing the challenges posed by the proliferation of deep fake content. Through meticulous data collection, preprocessing, and model training, we have created a robust solution capable of discerning between genuine and manipulated videos. The utilization of transfer learning, leveraging pre-trained facial recognition models, enhances the efficiency of our detection system. The integration of a finetuned model into an intuitive GUI application further democratizes access to this technology, allowing users to easily analyze videos and gain insights into potential deep fake content. Throughout the project, a strong emphasis was placed on user feedback, continuous improvement, and ethical considerations. The application not only serves as a practical tool for detecting deep fake videos but also educates users about the existence of such content and encourages responsible use of this technology. As we deploy this system, we acknowledge the dynamic nature of deep fake techniques, necessitating ongoing updates and enhancements. Regular evaluations, user engagement, and adaptability to emerging challenges will be crucial for maintaining the effectiveness of the detection system over time. In essence, our deep fake video detection project with its user-friendly GUI application contributes to the ongoing efforts in combating misinformation, protecting individuals and organizations from potential harm, and fostering a more responsible and informed digital landscape.

9. REFERENCE

1. Jeevidha, 2S. Saraswathi, 3Kaushik J B, 4Preethi K, 5, Nallam Venkataramaya, Deepfake video detection using res-next cnn and lstm, 2023.
2. Chesney, Robert and Citron, Danielle Keats, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security (July 14, 2018). 107 California Law Review (2019, Forthcoming); U of Texas Law, Public Law Research Paper No. 692; U of Maryland Legal Studies Research Paper No. 2018-21
3. Yuezun Li, Ming-Ching Chang and Siwei Lyu, In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking, arXiv:1806.02877v2 [cs.CV] 11 Jun 2018
4. Yuezun Li, and Siwei Lyu, “Exposing DeepFake Videos By Detecting Face Warping Artifacts”, arXiv:1811.00656v3 [cs.CV] 22 May 2019
[https://doi.org/10.1016/S0969-4765\(19\)30137-7](https://doi.org/10.1016/S0969-4765(19)30137-7)
5. Darius Afchar, Vincent Nozick, Junichi Yamagishi and Isao Echizen, “MesoNet: a Compact Facial Video Forgery Detection Network”, arXiv:1809.00888v1 [cs.CV] 4 Sep 2018
<https://doi.org/10.1109/WIFS.2018.8630761>
6. Xin Yang, Yuezun Li and Siwei Lyu, “Exposing Deep Fakes Using Inconsistent Head Poses”, ICASSP 2019 - 2019 IEEE ICASSP, 17 May 2019
7. Huy H. Nguyen, Junichi Yamagishi, and Isao Echizen, “Use of a capsule network to detect fake images and videos”, arXiv:1910.12467v2 [cs.CV] 29 Oct 2019