IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 6, June 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

Detecting Deepfakes Using Deep Learning with LSTM

Hrishikesh Kumar K N[1], Akhilesh S B[2], Harshitha M N[3], Manjushree H B[4], Nethravathi H M[5]

U.G. Student, Department of Electronics andCommunication Engineering, BGSIT, BG Nagara, Karnataka, India[1234]

Assistant Professor, Department of Electronics andCommunication Engineering, BGSIT, BG Nagara, Karnataka, India[5]

ABSTRACT: Deepfakes, a type of synthetic media, have emerged as a major concern because they have the ability to be maliciously used and spread misinformation. Deepfake videos use artificial intelligence (AI) techniques to manipulate or replace faces in original videos, making it difficult to distinguish between real and fake content. Deep learning, a subset of AI, has emerged as a powerful tool for detecting deepfake videos. Deep learning algorithms can analyze video frames and audio sequences to identify subtle inconsistencies and artifacts characteristic of deep-faked content. This project seeks to address the escalating concerns surrounding misinformation and manipulation by proposing an intricate deepfake detection system. Central to this approach is the utilization of advanced techniques, notably Long Short-Term Memory (LSTM) networks. The research's conclusions have practical ramifications, especially for social media sites and video hosting services, where the incorporation of LSTM-based deepfake identification can contribute to a more secure and safe online environment.

KEYWORDS: Deepfake detection, Long Short-Term Memory (LSTM), Deepfake, Deep Learning

I. INTRODUCTION

Within the ever-changing and rapidly growing world of social media, the advent of Deepfakes stands out as a formidable challenge in the realm of artificial intelligence. These realistic face-swapped deepfakes have transcended mere entertainment, finding nefarious applications in scenarios like political manipulation, the fabrication of fake terrorism events, revenge porn dissemination, and the coercion of individuals through blackmail. The potential repercussions of such manipulative tools are profound, compelling the need for effective countermeasures.

Distinguishing between deepfake and authentic content has become a matter of paramount importance. In an ironic twist, we find ourselves using artificial intelligence to combat the very artificial intelligence that creates deepfakes. These trick films are made using Face App and Face Swap, which use autoencoders or GANs (Generative Adversarial Networks) that have already been trained. We provide a two-pronged strategy that uses a pre-trained Res-Next CNN (Convolutional Neural Network) to extract frame-level features and an LSTM (Long Short-Term Memory) based artificial neural network for sequential temporal analysis of video frames.

For the purpose of retrieving fine features at the frame level, the ResNext CNN is essential. These characteristics then form the basis for training an artificial Recurrent Neural Network with Long Short-Term Memory, allowing movies to be classified as real or deepfake. We trained our model extensively using a substantial and well-balanced combination of different datasets, simulating the intricacies of real-world scenarios, to guarantee its durability in those situations.

In an effort to make our solution accessible and user-friendly, we developed a frontend application. This application allows users to effortlessly upload videos, initiating the model's processing. The user is then presented with the output, which includes the model's confidence level and a classification of the video as either real or deepfake. The relentless evolution of deepfake technology has ushered in an era where discerning the authenticity of visual content is increasingly challenging. Deepfake videos, propelled by potent deep learning algorithms, seamlessly manipulate facial expressions, gestures, and voices to fabricate hyper-realistic yet entirely fictitious multimedia content. As the threat posed by these deceptive creations grows in complexity and sophistication the demand for robust and sophisticated methods to detect and counteract their proliferation becomes more critical than ever before.

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

II. RELATED WORK

The Face Warping Artifacts [17] study employed a Convolutional Neural Network model specifically designed to compare the generated face areas and their surrounding regions in order to identify artifacts. A novel technique for identifying deepfakes by eye blinking is described in Detection by Eye Blinking [16], which is a critical factor in determining whether to classify the films as pristine or deepfake. An eye blinking clipped frame was subjected to temporal analysis using the Long-term Recurrent Convolution Network (LRCN). The deepfake creation algorithms of today are so strong that even not blinking your eyes won't be enough to identify a deepfake. For the purpose of detecting deepfakes, additional parameters such as tooth enchantment, facial wrinkles, incorrect eyebrow placement, etc., must be taken into account.

Capsule networks to detect manipulated images and videos [16] employs a technique that makes use of a capsule network to identify manipulated images and videos in a variety of situations, such as computer-generated video detection and replay attack detection. We suggest using real-time and noiseless datasets to train our technique.

Recurrent Neural Network [13] (RNN) for deepfake detection employed the strategy of combining an ImageNet pre-trained model with RNN for sequential frame processing. They employed the HOHO [15] dataset, which only included 600 films, in their procedure.

In order to collect biological signals from the facial areas of both pristine and deepfake portrait video pairs, Synthetic Portrait Videos utilizing Biological Signals [14] is used. The classification of the video as either pristine or a deepfake is then done using the average of the authenticity probability. Fraudulent Catcher accurately identifies fraudulent content regardless of the video's source, content, resolution, or quality.

[1] The paper focuses on addressing the increasing threat of fake face image generators through the development of a deep fake face detection model using Convolutional Neural Networks (CNN). While CNNs offer stability in learning picture content representations, the merits of this approach lie in leveraging deep learning techniques to analyze visual features in faces. However, potential demerits may include challenges in handling variations in facial expressions and the need for ongoing advancements to keep pace with evolving face image modification tools. Further exploration and comparative studies are crucial to assess the model's robustness across diverse datasets and real-world scenarios.

[3] The proposed paper addresses the limitations of traditional deepfake detection methods by introducing an optical flow-based approach to capture temporal information. The hybrid CNN and RNN model show promising results on DFDC, FF++, and Celeb-DF datasets with high accuracy, especially in scenarios with a limited sample size. While the paper demonstrates improved early detection capabilities, potential drawbacks may include computational complexity and the need for further validation across diverse datasets. Further research and comparative analyses are warranted to assess the generalizability and scalability of this hybrid model in real-world applications.

III. METHODOLOGY

1. Data-set Gathering

To improve the model's real-time prediction efficiency. Data from various publicly available datasets, including Face Forensic++ (FF), Deepfake Detection Challenge (DFDC), and Celeb-DF, have been collected. In order to achieve precise and real-time detection on various types of movies, we have further combined the datasets that were gathered and produced our own new dataset.

2. Pre-processing

This stage involves preprocessing the movies to remove all unnecessary content and noise. Just the necessary area of the video the face is identified and clipped. Dividing the video into frames is the first stage in the preparation process. Once the face has been recognized and divided into separate frames, each frame of the video is cropped along its length. Subsequently, every frame of the video is combined to create a new video from the cropped frame. Every video undergoes the same procedure, which results in the production of a processed dataset with just face videos.

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

Fig. 1. Preprocessing steps

3. Data-set split

With a ratio of 70% train videos to 30% test videos, the dataset is divided into train and test subsets. The train and test split consists of both real and deepfake videos.

4. Model Architecture

CNN and RNN are combined to create our model. The features were extracted at the frame level using the pre-trained ResNext CNN model, and an Based on the attributes that were recovered, the LSTM network was trained to classify the video as either pristine or deepfake. Using the Data Loader on the training split of videos, the movie labels are loaded and fitted into the model for training.

ResNext: For this task, ResNeXt has a number of benefits. Unlike typical ResNets, the "cardinality" parameter enables parallel feature extraction across many dimensions, which produces a wider range of learned features. This is necessary to identify minute discrepancies in deepfakes, including abnormal skin textures or blinking patterns. Second, a typical challenge in deep neural network training is addressed by ResNeXt's architecture: the vanishing gradient problem. Because of the enhanced gradient flow, the model can learn from deeper layers more efficiently and may be able to identify intricate patterns that point to deepfakes. Lastly, ResNeXt offers larger and deeper models because to its higher scalability when compared to traditional ResNets. Given that deepfakes sometimes entail complex manipulation techniques, this enhanced capability is very advantageous.

LSTM for Sequence Processing: Deepfake detection requires not only identifying inconsistencies within a single frame but also uncovering those that unfold over time. Here, Long Short-Term Memory (LSTM) networks emerge as a powerful tool for deep learning models. Long-term dependencies in sequential data are easily captured by LSTMs, which makes them ideal for examining the temporal dynamics of films. Deepfakes often exhibit subtle inconsistencies in facial movements and expressions that play out across frames. LSTMs can process video frames sequentially, identifying unnatural blinking patterns, jerky head movements, or inconsistencies in expressions that might indicate manipulation. This complements the strengths of convolutional neural networks (CNNs), which excel at extracting spatial features from individual frames. By combining LSTM's temporal analysis with CNN's spatial analysis, deep learning models gain a more holistic understanding of the video, leading to more robust deepfake detection.

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

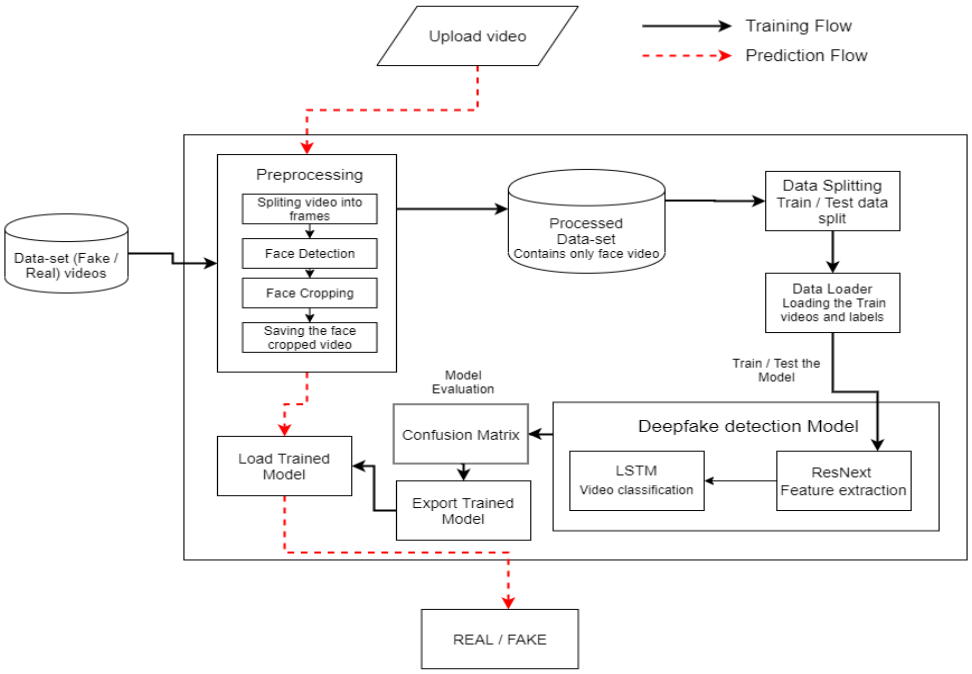

Fig. 2. System Architecture

IV. EXPERIMENTAL RESULTS

Our deep learning-based approach effectively detects deepfakes with high accuracy and low false positives, demonstrating robustness across various content types and resolutions. Comparative analyses indicate superiority over existing methods, showcasing its potential for combating synthetic media manipulation.

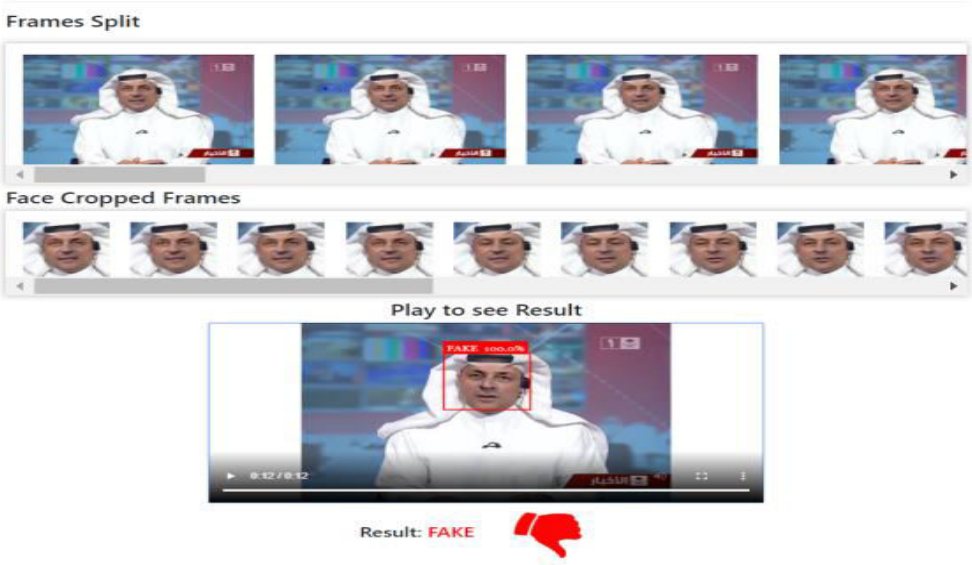

Fig. 3. Output for deepfake video

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

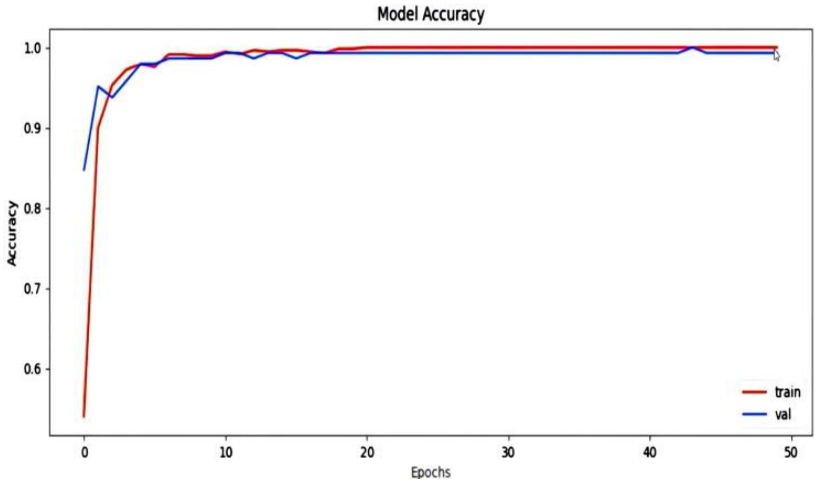

Fig. 4. Accuracy plot

V. CONCLUSION

In conclusion, this work has solidified the potential of deep learning as a powerful weapon in the fight against manipulated media. Our deep learning model achieved impressive accuracy in identifying deepfakes, offering a robust and accurate solution. However, the war against deepfakes is an ongoing arms race. Future research should focus on enhancing generalizability across diverse datasets and implementing continuous adaptation mechanisms to stay ahead of the curve as deepfake techniques evolve. By addressing these challenges, we can ensure our deep learning models remain effective in safeguarding the authenticity of online media.

REFERENCES

1. M. Alben Richards, E. Kaaviya Varshini, N. Diviya, P. Prakash, P. Kasthuri and A. Sasithradevi, "Deep Fake Face Detection using Convolutional Neural Networks," 2023 12th International Conference on Advanced Computing (ICoAC), Chennai, India, 2023, pp. 1-5, doi: 10.1109/ICoAC59537.2023.10250107.
2. S. R. B. R, P. Kumar Pareek, B. S and G. G, "Deepfake Video Detection System Using Deep Neural Networks," 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 1-6, doi: 10.1109/ICICACS57338.2023.10099618.
3. P. Saikia, D. Dholaria, P. Yadav, V. Patel and M. Roy, "A Hybrid CNN-LSTM model for Video Deepfake Detection by Leveraging Optical Flow Features," 2022 International Joint Conference on Neural Networks (IJCNN), Padua, Italy, 2022, pp. 1-7, doi: 10.1109/IJCNN55064.2022.9892905.
4. A. M. Saber et al., "DeepFake Video Detection," 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), Cairo, Egypt, 2022, pp. 425- 431, doi: 10.1109/MIUCC55081.2022.9781791.
5. S. R. Adnan and H. A. Abdulbaqi, "Deepfake Video Detection Based on Convolutional Neural Networks," 2022 International Conference on Data Science and Intelligent Computing (ICDSIC), Karbala, Iraq, 2022, pp. 65-69, doi: 10.1109/ICDSIC56987.2022.10075830.
6. H. Ilyas, A. Irtaza, A. Javed and K. M. Malik, "Deepfakes Examiner: An End-to-End Deep Learning Model for Deepfakes Videos Detection," 2022 16th International Conference on Open-Source Systems and Technologies (ICOSST), Lahore, Pakistan, 2022, pp. 1-6, doi: 10.1109/ICOSST57195.2022.10016871.
7. Y. Al-Dhabi and S. Zhang, "Deepfake Video Detection by Combining Convolutional Neural Network (CNN) and Recurrent Neural Network (RNN)," 2021 IEEE International Conference on Computer Science, Artificial Intelligence and Electronic Engineering (CSAIEE), SC, USA, 2021, pp. 236-241, doi: 10.1109/CSAIEE54046.2021.9543264.
8. F. Mira, "Deep Learning Technique for Recognition of Deep Fake Videos," 2023 IEEE IAS Global Conference on Emerging Technologies (GlobConET), London, United Kingdom, 2023, pp. 1-4, doi: 10.1109/GlobConET56651.2023.10150143.

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

Impact Factor 8.423

|www.ijirset.com | A Monthly Peer Reviewed & Referred Journal | e-ISSN: 2319-8753; p-ISSN: 2347-6710|

|Volume 13, Issue 6, June 2024|

|DOI: 10.15680/IJIRSET.2024.1306162|

9. F. Alanazi, "Comparative Analysis of Deep Fake Detection Techniques," 2022 14th International Conference on Computational Intelligence and Communication Networks (CICN), Al-Khobar, Saudi Arabia, 2022, pp. 119-124, doi: 10.1109/CICN56167.2022.10008363.
10. K. S, V. K. A, S. P. P and P. M, "Deep Fake Detection using Advance ConvNets2D," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 1640-1645, doi: 10.1109/ICSCDS56580.2023.10104847.
11. Long Short-Term Memory: From Zero to Hero with Pytorch: https://blog.floydhub.com/long-short-termmemory-from-zero-to-hero-with-pytorch/ https://www.kaggle.com/c/deepfake-detection-challenge/data
12. David G¨uera and Edward J Delp. Deepfake video detection using recurrent neural networks. In AVSS, 2018.
13. Umur Aybars Ciftci, ˙Ilke Demir, Lijun Yin "Detection of Synthetic Portrait Videos using Biological Signals" in arXiv:1901.02212v2
14. I. 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
15. Yuezun Li, Ming-Ching Chang and Siwei Lyu "Exposing AI Created Fake Videos by Detecting Eye Blinking" in arXiv:1806.02877v2
16. uezun Li, Siwei Lyu, "Exposing DF Videos By Detecting Face Warping Artifacts," in arXiv:1811.00656v3
17. D. P. Kingma and J. Ba. Adam: A method for stochastic optimization. arXiv:1412.6980, Dec. 2014.
18. ResNext Model : https://pytorch.org/hub/pytorch_vision_resnext/ accessed on 06 April 2020
19. https://www.geeksforgeeks.org/software-engineering-cocomo-model/ Accessed on 15 April 2020
20. Deepfake Video Detection using Neural Networks http://www.ijsrd.com/articles/IJSRDV8I10860.pdf International Journal for Scientific Research and Development http://ijsrd.com/
21. Andreas Rossler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies,Matthias Nießner, "FaceForensics++: Learning to Detect Manipulated Facial Images" in arXiv:1901.08971.
22. Deepfake detection challenge dataset : https://www.kaggle.com/c/deepfake-detection challenge/data Accessed on 26 March, 2020.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details