Intelligent Forensic Analysis for Deepfake Video Detection Using AI

[1]Dr. P. V. S. Sarma,[2]Alladi Harika,[3]Bondu John,[4]Kathi Daniel Christopher

[1]Associate Professor, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

[2,3,4]B. Tech Student, Dept of Computer Science and Engineering, St. Ann's College of Engineering and Technology, Chirala-523187, India.

ABSTRACT

The Intelligent Forensic Analysis for Deepfake Video Detection using AI project tackles the rising problem of synthetic and altered videos that can be used for identity fraud, disinformation, and cybercrime. When it comes to advanced deepfake creation technologies, human inspection methods and traditional forensic approaches are frequently laborious, prone to errors, and ineffectual. In order to automatically evaluate video information and identify minute visual, temporal, and physiological irregularities that point to deepfake manipulation, this system makes use of artificial intelligence and deep learning techniques. By utilizing automated feature extraction, frame-level analysis, and trained neural network models, the proposed system ensures accurate, reliable, and scalable deepfake detection.

KEYWORDS: Deepfake Detection, Intelligent Forensic Analysis, Artificial Intelligence, Machine Learning, Video Forensics, Deep Learning, Face Manipulation Detection, Multimedia Security, Digital Forensics, Synthetic Media Analysis.

INTRODUCTION

Deepfake video highly realistic but altered digital material produced by changing facial characteristics, expressions, or speech—have emerged as a result of the quick development of artificial intelligence and deep learning technology. Although deepfake technology has useful uses in entertainment and the

production of digital content, its abuse has grown to be a serious concern in areas including the spread of false information, identity impersonation, cybercrime, and the manipulation of digital evidence. By utilizing cutting-edge machine learning and deep learning models, the Intelligent Forensic Analysis for Deepfake Video Detection using AI project offers an automated and trustworthy way to detect falsified video footage.

LITERATURE REVIEW

In recent years, several researchers have explored automated techniques for detecting deepfake videos using artificial intelligence, highlighting both advancements and existing limitations in digital forensic analysis. The first notable work was proposed by **Afchar et al (2018)**, who introduced MesoNet, a convolutional neural network designed to detect facial manipulation in deepfake videos by learning mesoscopic visual features. The second study by **Rossler et al. (2019)** presented the *Face Forensics++* benchmark, which provided a large-scale dataset and evaluated multiple CNN-based detection models.

RELATED WORK

Due to the growing realism of synthetic media, artificial intelligence-based methods for deepfake video detection have been thoroughly investigated in recent study. MesoNet, a CNN-based model developed by Afchar et al. that learns mesoscopic features to identify facial manipulation, performs poorly on high-quality deepfakes.

EXISTING METHOD

The majority of deepfake detection approaches now in use rely on manual verification and conventional forensic

methods, which are laborious and frequently imprecise. Early methods concentrated on detecting obvious faults in individual frames, such as mismatched skin tone, abnormal blinking, or blurry face areas. Metadata, compression noise, and encoding patterns were examined using rule-based algorithms; however, when videos are heavily manipulated or reprocessed, these techniques fall short.

PROPOSED METHOD

The suggested system employs an AI-based deep learning technique to more accurately and consistently identify deepfake movies. To ensure consistent data representation, the input video is first preprocessed to extract frames and identify facial regions. Each frame's pixel-level artifacts, edges, and facial textures are all analyzed by a CNN model.

A GRU/RNN model analyzes temporal patterns over successive frames to capture movement-based abnormalities. The system detects small manipulation cues that conventional approaches frequently overlook by fusing temporal and spatial learning. The retrieved elements are then categorized together with a confidence score to ascertain if the video is authentic or fraudulent.

SYSTEM ARCHITECTURE

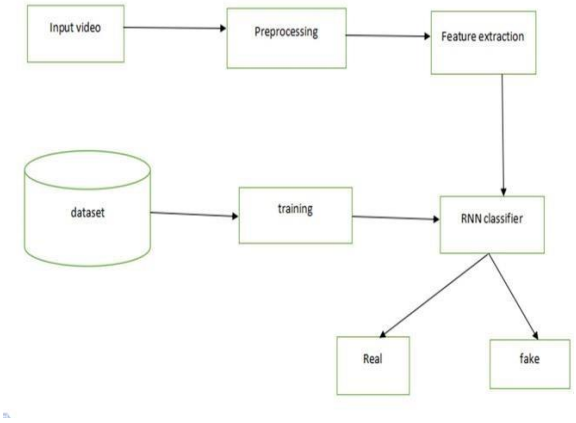

Fig 1: Architecture of the Deep Fake Video Detection using AI

METHODOLOGY DESCRIPTION

User Registration and Authentication:

For users like investigators, analysts, and administrators, the system begins with secure registration and login.

Video Input Module:

For verification, users upload video files to the system. The module verifies the uploaded video by examining its resolution, duration, and file format.

Video Preprocessing:

To get ready for model analysis, the uploaded videos go through preprocessing. In this step, frames are extracted, face regions are

identified, frames are resized, and pixel values are normalized.

Feature Extraction using CNN:

A Convolutional Neural Network (CNN) is used to extract spatial characteristics from the preprocessed frames, including pixel-level distortions, illumination fluctuations, and facial texturing.

Temporal Pattern Analysis using RNN/GRU:

To examine temporal patterns across frame sequences, the retrieved frame-level features are fed into a Recurrent Neural Network (RNN/GRU) classifier.

Deepfake Classification Module:

The model determines if the uploaded video is authentic or fraudulent based on both temporal and spatial analysis. To aid in decision-making and forensic dependability, a confidence score is produced.

Result Display and Forensic Reporting:

The user interface displays the final findings, including the confidence score and categorization outcome.

RESULTS AND DISCUSSIONS

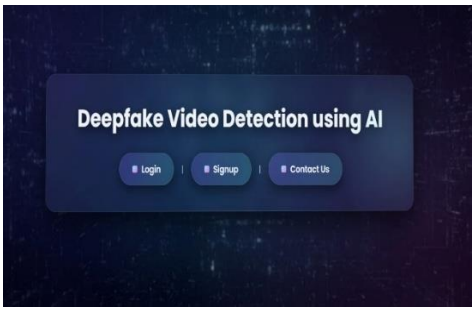

Fig 2: Home Page

The home page provides primary navigation for users to access login, signup, and contact modules, serving as the entry point to the deepfake detection system.

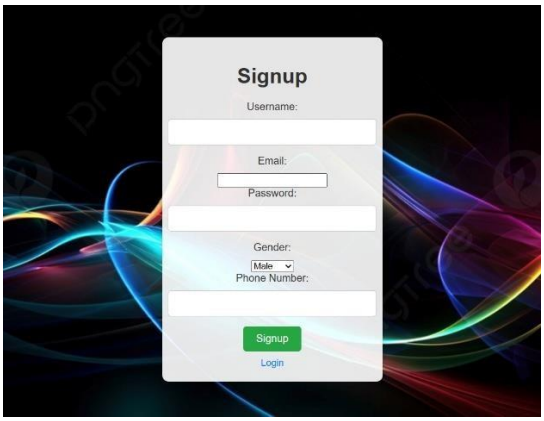

Fig 3: Signup Page

The signup interface enables new users to register by entering basic credentials, ensuring authenticated access to the system.

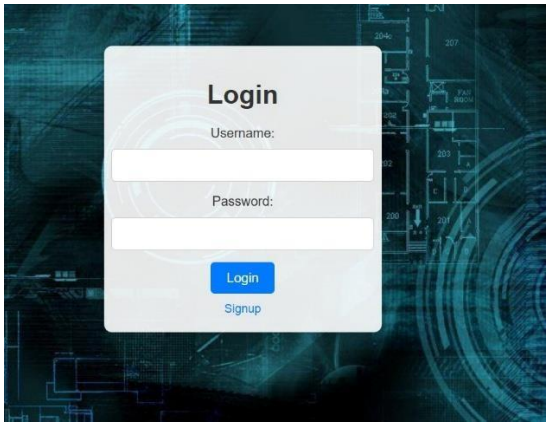

Fig 4: Login Page

The login screen verifies registered users before allowing access to video upload and detection functionalities, maintaining system security.

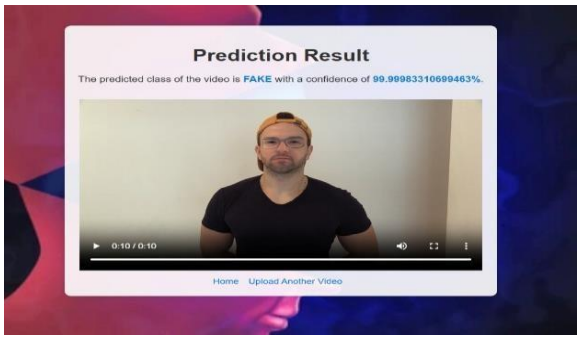

Fig 5: Prediction Result – Fake Video

The model detects the uploaded sample as a deepfake and presents a high confidence score, demonstrating the effectiveness of the classification approach.

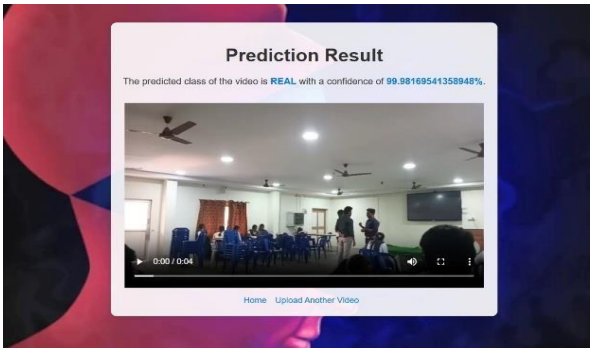

Fig 6: Prediction Result – Real Video

The system successfully identifies the uploaded video as real and displays the confidence score along with video playback for user verification.

CONCLUSION AND FUTURE ENHANCEMENT

In conclusion, the suggested Intelligent Forensic Analysis for Deepfake Video Detection using AI offers a dependable and automated method for spotting altered video footage. The method reliably and accurately separates actual movies from deepfakes by combining temporal pattern analysis using RNN/GRU models with spatial feature extraction using CNNs.

FUTURE ENHANCEMENT

This approach could be improved in the future by incorporating transformer-based designs or using multimodal analysis to identify deepfakes that manipulate both audio and visual. Mobile application deployment, cloud-based forensic services, and current deepfake detection for live streaming.

REFERENCES

1. Harini, D. P. (2024). Electronic Health Record Stage Identification using Principal Component Analysis. *Machine Intelligence Research*, 864-873.
2. Rössler, A., Cozzolino, D., Verdoliva, L., Riess, C., Thies, J., & Nießner, M., "FaceForensics++: Learning to Detect Manipulated Facial Images," IEEE International Conference on Computer Vision (ICCV), pp. 1-11, 2019.
3. Afchar, D., Nozick, V., Yamagishi, J., & Echizen, I., "MesoNet: A Compact Facial Video Forgery Detection Network," IEEE International Workshop on Information Forensics and Security (WIFS), pp. 1-7, 2018.
4. Güera, D., & Delp, E. J., "Deepfake Video Detection Using Recurrent Neural Networks," IEEE AVSS, pp. 1-6, 2018.
5. Dang, H., Liu, F., Stehouwer, J., Liu, X., & Jain, A. K., "On the Detection of Digital Face Manipulation," IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 5781-5790, 2020.
6. Korshunov, P., & Marcel, S., "Deepfakes: A New Threat to Face Recognition? Assessment and Detection," arXiv preprint arXiv:1812.08685, 2018.
7. Li, Y., Chang, M. C., & Lyu, S., "In Ictu Oculi: Exposing AI Generated Fake Face Videos by Detecting Eye Blinking," IEEE WIFS, pp. 1-7, 2018.
8. Nguyen, T. T., & Nguyen, C. M., "Deep Learning for Deepfake Detection: A Survey," IEEE Access, vol. 9, pp. 145814-145831, 2021.
9. Tolosana, R., et al., "DeepFakes and Beyond: A Survey of Face Manipulation and Fake Detection," Information Fusion, vol. 64, pp. 131-148, 2020.

10. Verdoliva, L., "Media Forensics and DeepFakes: An Overview," IEEE Journal of Selected Topics in Signal Processing, vol. 14, no. 5, pp. 910-932, 2020.
11. Tariq, S., et al., "Detecting Deepfake Videos Using CNN-LSTM Architecture," IEEE International Conference on Information Fusion (FUSION), pp. 1-8, 2021.
12. Haliassos, A., et al., "Lips Don't Lie: A Generalisable and Robust Approach To Face Forgery Detection," IEEE/CVF CVPR, pp. 5039–5049, 2021.
13. Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H., "Protecting World Leaders Against Deep Fakes," CVPR Workshops, pp. 1-7, 2019.
14. Zhang, Y., & Qi, H., "Detection of Deepfake Video Manipulation Using Convolutional Vision Transformers," MDPI Electronics, vol. 11, no. 3, pp. 455-465, 2022.
15. Khalid, H., Woo, S. S., & Lee, J. C., "Fake Video Detection Using Attention-Based CNN-BiLSTM Model," Applied Sciences, vol. 12, no. 9, pp. 4320-4331, 2022.
16. Matern, F., Riess, C., & Stamminger, M., "Exploiting Visual Artifacts to Expose Deepfakes," ACM SIGGRAPH Posters, pp. 1–2, 2019.
17. Zhang, X., & Liang, X., "A Lightweight CNN Model for Real-Time Deepfake Detection," International Journal of Computer Applications, vol. 175, no. 7, pp. 12-18, 2020.
18. Jain, A., & Patel, K., "Video Forensics Using Hybrid Deep Learning Approaches," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 6, pp. 225-232, 2021.
19. Wang, X., & Kim, J., "Deepfake Detection Using Hybrid Multimodal Feature Extraction," Springer Lecture Notes in Networks and Systems, vol. 320, pp. 45-55, 2023.
20. Basu, A., & Mishra, S., "Temporal Feature Learning for Deepfake Detection Using GRU Networks," International

Conference on Machine Learning and Applications (ICMLA), pp. 1-6, 2022.

21. Sahu, R., & Rai, A., "Secure Video Authentication Using AI-Based Deepfake Detection," International Journal of Scientific Research in Engineering and Management (IJSREM), vol. 7, no. 4, pp. 112-119, 2023.
22. Narayan, P., "Deepfake Detection Techniques and Tools: A Comparative Study," Elsevier Computer Vision and Image Understanding, vol. 223, pp. 103545, 2022.