DEEP FAKE VIDEO DETECTION BASED ON REAL TIME APPLICATION USING DEEP LEARNING

SHADAN WOMEN'S COLLEGE OF ENGINEERING AND TECHNOLOGY

Ishrath Khader Ishrathkhadar@gmail.com

Dr.K.Palani principalswcet2020@gmail.com

ABSTRACT

Deepfake videos have emerged as a critical challenge in the digital age, with their ability to manipulate and fabricate video content convincingly. These videos pose significant threats to privacy, security, and the dissemination of truthful information. Real-time detection of Deepfake videos is essential for mitigating their misuse, especially in applications requiring immediate responses, such as social media platforms, video conferencing, and live broadcasts. This project focuses on the development of a real-time Deepfake video detection framework utilizing deep learning techniques, specifically convolutional neural networks (CNNs). The proposed system processes video frames dynamically, extracting temporal and spatial features to identify subtle artifacts and inconsistencies introduced during the generation of Deepfake videos. By leveraging optimized CNN architectures, the framework ensures high accuracy while maintaining computational efficiency to meet the demands of real-time analysis.

KEYWORDS: Deep Learning, Convolutional Neural Network, Recurrent Neural Network

INTRODUCTION

The rise of Deepfake technology has introduced significant challenges in the realms of digital media, privacy, and information security. Deepfakes, generated using advanced deep learning techniques such as generative adversarial networks (GANs) and convolutional neural networks (CNNs), manipulate or fabricate video and audio content to create hyper-realistic synthetic media. While these advancements have numerous positive applications in entertainment, education, and virtual reality, they also pose severe threats. The malicious use of Deepfake videos for misinformation campaigns, identity theft, fraud, and defamation has created an urgent need for effective detection mechanisms. Deep learning, particularly CNN-based models, has shown promise in addressing this challenge.CNNs excel at capturing spatial and temporal patterns in video data, making them well-suited for detecting the subtle artifacts and inconsistencies characteristic of Deepfake videos. By integrating CNNs with real-time processing capabilities, it is possible to develop robust detection systems that operate efficiently in dynamic environments. This study aims to design and implement a real-time Deepfake video detection framework leveraging CNN models. By analyzing both spatial and temporal features in video frames, the proposed system seeks to achieve high accuracy without compromising computational speed. This introduction provides the foundation for exploring the methodology, implementation, and evaluation of the framework, contributing to the broader efforts to safeguard digital integrity in the age of synthetic media.

LITERATURE SURVEY

Title-1: DEEP FAKE VIDEO DETECTION USING DEEP LEARNING

Authors: Rushikesh Potdar*1, Ajay Gidd*2, Shreya Kulkarni*3, Rohit Chavan*4, Prof. Nikam*5

Published in: 2021

Abstract: Lately, an AI-based free programming device has made it simple to make trustworthy face trades in videos that leave not many hints of control, in what is known as "deepfake" videos. Situations, where these sensible phony recordings are utilized to make political trouble, coerce somebody or phony psychological warfare occasions, are effortlessly imagined. Convolutional Neural Network and Recurrent Neural Network. System makes use of a convolutional Neural network (CNN) to extract capabilities on the body level. These capabilities are used to train a recurrent neural network (RNN) which learns to categorize if a video has been concern to manipulation or now no longer and is also capable of hit upon the temporal inconsistencies among frames presented by DF introduction tools.. Expected end results in opposition to a huge set of fake films collected from trendy information set. We display how our device can be aggressive bring about this assignment outcomes in the usage of an easy architecture.

Title-2: Deepfakes Detection Techniques Using Deep Learning: A Survey

Authors: Abdulqader M. Almars

Published in: 2021

Abstract: Deep learning is an effective and useful technique that has been widely applied in a variety of fields, including computer vision, machine vision, and natural language processing. Deepfakes uses deep learning technology to manipulate images and videos of a person that humans cannot differentiate them from the real one. In recent years, many studies have been conducted to understand how deepfakes work and many approaches based on deep learning have been introduced to detect deepfakes videos or images. In this paper, we conduct a comprehensive review of deepfakes creation and detection technologies using deep learning approaches. In addition, we give a thorough analysis of various technologies and their application in deepfakes detection. Our study will be beneficial for researchers in this field as it will cover the recent state-of-art methods that discover deepfakes videos or images in social contents. In addition, it will help comparison with the existing works because of the detailed description of the latest methods and dataset used in this domain.

Title-3: Deep fake Detection through Deep Learning

Authors: Deng Pan School of Computing and Information Systems, The University of Melbourne, Melbourne, Australia

Published Year: 2020

Abstract: Deepfakes allow for the automatic generation and creation of (fake) video content, e.g. through generative adversarial networks. Deepfake technology is a controversial technology with many wide-reaching issues impacting society, e.g. election biasing. Much research has been devoted to developing detection methods to reduce the potential negative impact of deepfakes Application of neural networks and deep learning is one approach. In this paper, we consider the deepfake detection technologies Xception and Mobile Net as two approaches for classification tasks to automatically detect deepfake videos. We utilize training and evaluation datasets from Face Forensics++ comprising four datasets generated using four different and popular deepfake technologies. The results show high accuracy over all datasets with an accuracy varying between91-98% depending on the deepfake technologies applied. We also developed a voting mechanism that can

detect fake videos using the aggregation of all four methods instead of only one.

EXISTING SYSTEM

Existing systems for Deep Fake video detection primarily rely on deep learning and machine learning techniques to identify manipulated content. These systems utilize models such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs) to detect inconsistencies in video data. Many existing solutions analyze spatial artifacts (e.g., facial inconsistencies, unnatural textures) and temporal dynamics (e.g., irregularities in motion or lip synchronization) within videos to distinguish between real and manipulated content. Most detection frameworks operate offline, requiring significant time to process and analyze video files. These systems often lack real-time capabilities, making them unsuitable for applications involving live streams or immediate response needs. Additionally, their accuracy may vary depending on the dataset used, with performance typically degrading under conditions such as low resolution, poor lighting, or video compression.

DISADVANTAGES

- Lack of Real Time Capability
- Limited Feature Analysis
- Poor Performance in Adverse Condition

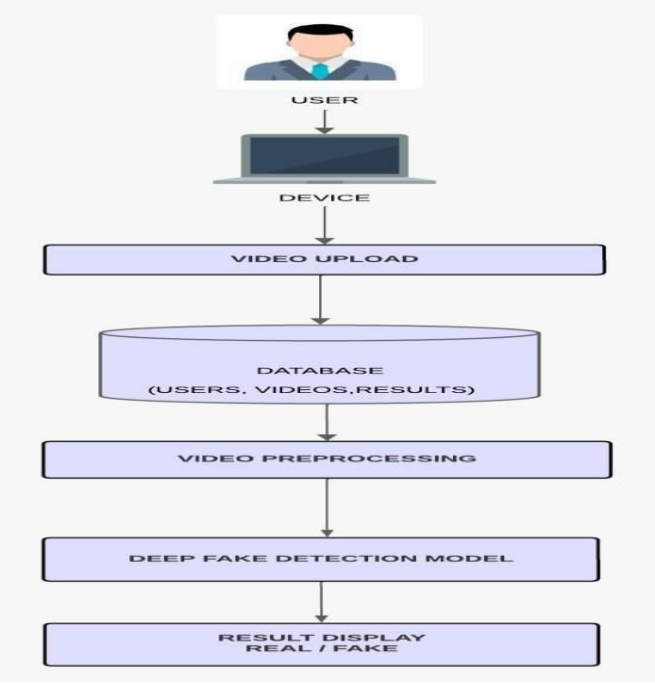
PROPOSED SYSTEM

In this project, we propose a real-time Deep Fake video detection system leveraging convolutional neural networks (CNNs) to address the limitations of existing solutions. Unlike conventional approaches, the proposed system is designed to operate with minimal latency, enabling the detection of manipulated video content in live-streamed environments and other real-time applications.DeepFake technology in spreading misinformation, identity theft, and malicious activities. By addressing the gaps in existing detection methods, this project offers a robust and practical tool for safeguarding digital media integrity in real-time applications like live broadcasting, social media monitoring, and video conferencing.

ADVANTAGES

- Real Time Detection
- Comprehensive Feature Analysis
- Efficient and Scalable

SYSTEM ARCHITECTURE



FLOW DESCRIPTION:

1. User Signs Up/Logs In:

- The user accesses the frontend (UI), which communicates with the

Authentication Service. • After successful login or registration, the user's session is created.

2. User Uploads Video:

• The frontend sends the video file to the Video Upload Service.

• The video is saved to cloud storage (e.g., AWS S3) and metadata (e.g., file path, user ID) is stored in the database.

3. Video Processing and Deep fake Detection:

• The Video Processing Service retrieves the video, performs any necessary preprocessing (e.g., resizing, format conversion), and sends the processed video to the Deepfake Detection Model.

• The model analyzes the video and returns a result (real/fake) with a confidence score.

4. Result Display:

• The result of the analysis is stored in the database and sent back to User display

ALGORITHMS

Step 1: Video Upload & Preprocessing

Step 2: Load Pre-trained Deepfake Detection Model

Step 3: Frame Classification (Deepfake Detection)

Step 4: Aggregate Predictions (Average Method)

Step 5: Final Deepfake Detection Algori

CONCLUSION

The Deepfake Detection Web Application is an essential tool in addressing the growing challenges posed by deepfake technology, which can lead to misinformation, fraud, and manipulation. This project provides an effective solution for detecting manipulated videos, offering users a reliable way to verify content before sharing it. The system uses advanced machine learning models, facial recognition, and video frame analysis to accurately identify deepfakes while minimizing false positives. Key features such as customizable profiles, real-time detection, and detailed analytics ensure a user-friendly experience. Future enhancements like audio detection, social media integration, and improved machine learning techniques will further strengthen the system's capabilities. Overall, this application plays a critical role in promoting media literacy, safeguarding online content, and helping individuals and organizations navigate the growing threat of deepfakes manipulated digital media.

REFERENCES

[1] Y. Li, M. C. Chang, and S. Lyu, “In Ictu Oculi: Exposing AI created fake videos by detecting eye blinking,” in 10th IEEE International Workshop on Information Forensics and Security, WIFS 2018, 2019.

[2]H. Li, B. Li, S. Tan, and J. Huang, “Detection of Deep Network Generated Images Using Disparities in Color Components,” Aug. 2018.

[3]Y. Li and S. Lyu, “Exposing DeepFake Videos By Detecting Face Warping Artifacts.”

[4]D. Guera and E. J. Delp, “Deepfake Video Detection Using Recurrent Neural Networks,” in Proceedings of AVSS 2018 - 2018 15th IEEE International Conference on Advanced Video and Signal-Based Surveillance, 2019.

[5] X. Yang, Y. Li, and S. Lyu, “Exposing Deep Fakes Using Inconsistent Head Poses,” in ICASSP, IEEE International

Conference on Acoustics, Speech and Signal Processing - Proceedings, 2019.

[6] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2016, vol. 2016Decem, pp. 770–778.

[7] D. E. King, “Dlib-ml: A machine learning toolkit,” J. Mach. Learn. Res., 2009.

[8] Adam Geitgey, “Machine Learning is Fun! Part 4: Modern Face Recognition with Deep Learning,” Medium, 2016.

[9] G. Bradski, “The OpenCV Library,” Dr Dobbs J. Softw. Tools, 2000.

[10] F. Pedregosa et al., “Sc