Deep Detect

Nirzara Manade[1*], Shravani Shinde[1], Sonal Patil[1], Sunetra Bhambure[1], S.V.Chavan [2]
[1]Under Graduate Student, Department of Computer Science and Engineering, Sanjay Ghodawat Institute,Atigre, Kolhapur, Maharashtra, India
[2]HOD, Department of Computer Science and Engineering , Sanjay Ghodawat Institute, Atigre, Kolhapur, Maharashtra, India

[*]Corresponding Author: nirzaramanade@gmail.com

Abstract

The deepfake technology which has been evolved over the past few years, threatened the way our society perceives reality and might be a catalyst for disruptions on an ethical, social or security level. These skills at manipulating video and audio with precision open up a whole universe of potential risks ,misinformation, identity theft, privacy. In this paper it describes similar work in that it leverages writing style to detect deepfake content but it aims to develop a web-based application as an alternative way of detecting such malicious videos. The web-application, built on machine learning algorithms and deployed in an easily usable GUI form factor, acts as a robust tool for detecting manipulations applied to media. It covers the key challenges like model accuracy, dataset quality & real-time processing various problematic areas are handled. From the results of implementation and tests, we will achieve some reasonable outcomes that demonstrate an easy way to cope up with them if it becomes more difficult in future times due to this rapidly increasing its technology and becoming more realistic day by day.

Keywords- Deep Fake, Machine Learning Algorithms, Identity theft, Real Time Processing, Webapplication

INTRODUCTION

A new twist in the story comes from emerging trends like deepfake technology that have allowed redactors to mix fabricated video content with legitimate footage. The term deepfake was namedis by the reddit user and it refers to an AI based technique which creates a hyper realistic alterations or fully fabricated images, videos, audios using AI techniques like Generative Adversarial Networks (GANs) or autoencoder, deepfakes can create extremely realistic audio, video and image manipulations.

In solution, by tackling technology with technology deepfake detection web application comes in frame. It can effectively tackle the disadvantages of deepfake technology by providing users a tool and knowledge needed to identify manipulated or altered content. By enhancing transparency, protecting individual privacy, supporting regulatory compliance, and fostering public trust in media, such applications can prevent the potential harms associated with deepfakes and promote a safer digital environment.

REVIEW OF LITERATURE

Study of Existing System

- **Deepfake apps:** There are many tools available that detect deepfake videos by analyzing video and audio cues and use AI based deep learning but there is lack of accuracy in them.
- **Datasets:** The tools available in the market are mostly just datasets or they require corporate access to use the functionality so it is hard to access by the end user.
- **Probability:** the existing system do not give clarification or basis on which the video is identified as real or deepfake. The lack of probability makes end user uncertain of the generated result.
- **Pre-trained models:** There are some pre-trained models but they are not that much useful for direct implementations. These models require

further training on multiple datasets to improve the quality

Findings from Literature Review

Media Forensics Considerations on Deep Fake Detection with Hand-Crafted Features.
Dennis Siegel, Christian Kraetzer, Stefan Seidlitz, Jana Dittmann
Publisher's Note MDPI remains neutral with regard to jurisdictional claims in published maps and institutional affiliations. Besides this issue in estimating decision plausibility of current (mainly neural network-based) detection methods, a second limitation to the state of the art has to be assigned here: As part from their efficiency considerations

(i.e., detection performance and plausibility), any forensic method would strive for being adherent to some sort of forensic conformity Criteria addressing admissibility, arrived from such an Examination as basis for expert witnesses' evidence in legal disputes.

PROPOSED SYSTEM

This web application is titled, and the focus to detect the deep fake especially the face swapping deepfakes. This proposed system will be available as web app on web browser and it will accept the videos from user's side. After loading the video by using deep learning technique which will extracts the videos into frames and by analyzing the frame content it will predict that uploaded content is manipulated or not. After predicting it will generate a report of the content where the flaws or manipulated contain will be highlighted. The detection engine built with the core, which based on machine learning libraries of python is TensorFlow, OpenCV and PyTorch. Deep Forensic is based on pre-trained deep learning models specifically fine-tuned to recognize deepfakes. They use frame-by-frame analysis for video files. By this methodology it will achieve itsmilestone.

Advantages

- The web-application helps identify and reduce the spread of fake media
- It provides tools for journalists, fact-checkers, and the general public to criti- cally evaluate the authenticity of content.
- Users can receive immediate feedback on the authenticity of videos.

PROJECT SCOPE

The project aims to create an easy-to-use web app that detects deepfakes, helping journalists, fact-checkers, and the general public spot fake videos. The web-based application will use advanced technology to provide real-time detection and will include features like media uploads, detailed reports, and educational materials. It will help the people especially the one who get affected by the misinformation.
This will not only detect the deepfake butalso a step towards revolution into the technology and innovation.

The Objective of the Proposed System

- **Real-Time Detection:** Develop an application which could detect and flag deepfakes in a real-time period of time to cross- check whether it is a video created by manipulation techniques while consuming it.
- **Usability:** Offer a user-friendly interface such that transferring and enabling the facilitation of media analysis is very easy for anybody, regardless of technical know- howfor things.
- **Data Privacy and Security:** Generally, user privacy is dealt with utmost confidentiality through proper data handling and processing such that the privacy policiesare conveyed to users.
- **Education Resources and Training Modules:** To enable journalists and fact- checkers to determine whether they can identify and present the issue, education resources and training modules will be developed on this specific area.

Software Requirements

- **Frontend Technologies:** HTML, Tailwind CSS, JavaScript, React, Bootstrap
- **Backend Technologies:** Node JS, Python ,JavaScript
- **Deep Learning Frameworks:** PyTorch, TensorFlow, OpenCV
- **API's and Deployment:** RESTful, AWS
- Datasets: FaceForensics++ , Google's Deep

fake dataset

- **Database:** Firebase
- **File Storage:** Amazon S3/ Google Cloud Storage

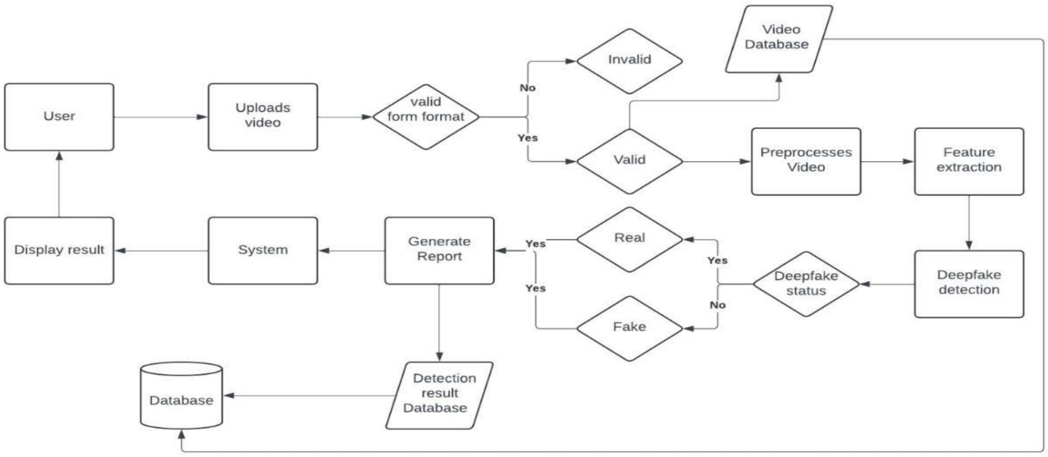
Hardware Configurations

- **Processor (CPU):** Intel Core i9 / AMDRyzen 9 (for faster data processing and multitasking)
- **2. Graphics Card (GPU):** NVIDIA GeForce RTX 3080 or higher (8 GB to 16 GB VRAM)
- **3. RAM:** 32 GB (for better performance with large datasets)
- **4. Storage:** 1 TB SSD (preferably NVMefor faster read/write speeds)

UML DIAGRAMS

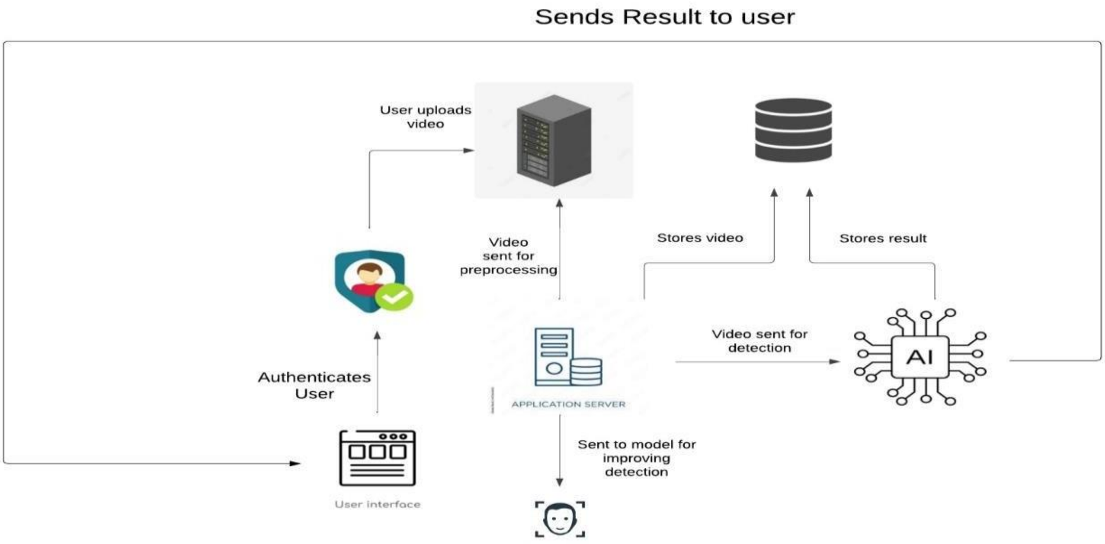
Flowchart

Figure 1: *Flow diagram*



.

Figure 2: *System Architecture*



ER Diagram

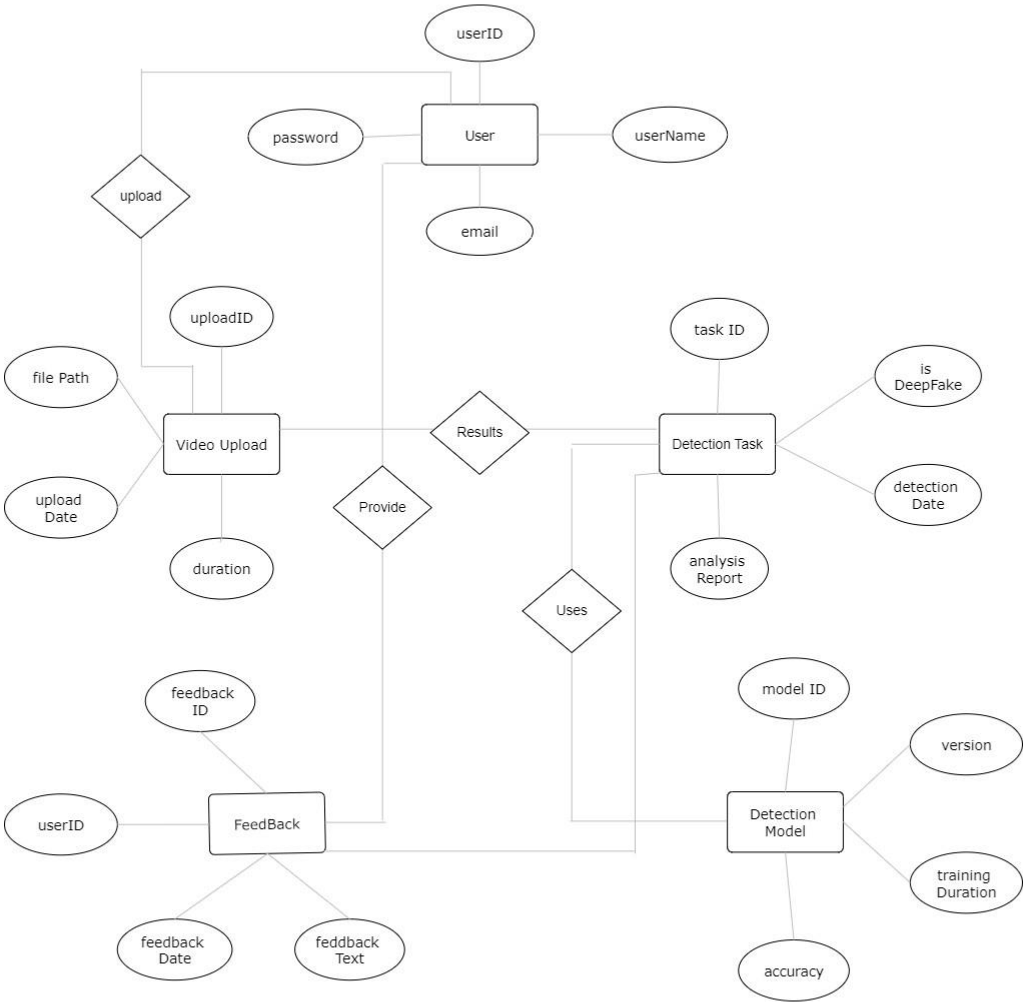


Figure 3: *ER diagram.*

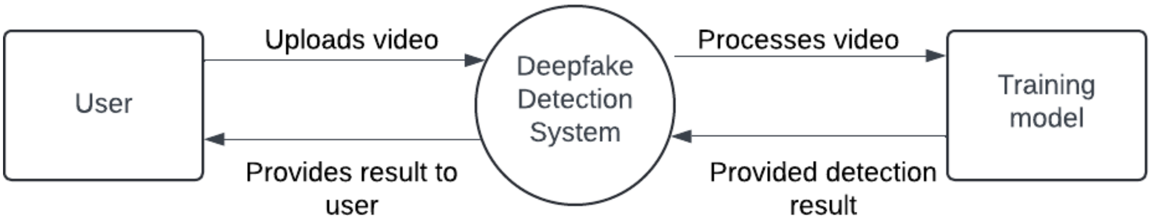


Figure 4: *Level 0 DFD.*

Challenges and Limitations

While this system has worked very well, there are still several hurdles:
Limited Datasets: A key issue is data diversity and scale to build effective deep learning models. In the real-world, deepfakes differ widely in quality and approach, thereby restraining the generalisability of models that are trained on the present datasets.
Scalable Real-Time Processing — Video content real-time detection assisting real-time requirements can be expensive as well. The processing times need more optimization, especially with high-resolution video files.

CONCLUSION AND FUTURE ENHANCEMENT

In this work, a deepfake detection web-app utilizing cutting-edge machine learning methodologies for identifying manipulated media is introduced. Not only does the app provide a smooth user experience, but it opens deepfake detection to those that may not be technically inclined. In future, we plan on research to achieve real-time performance for robustness and change the attributes in the dataset which apply to a different type of deepfake so that acquire with broader range of deepfake technique, we also want to approach a blockchain technology by adding Media Press Release as current 3rd party service to increase how reliable as media press releases in detected inputs. By pursuing these initiatives, the project aims not only to create a more informed society but also to empower individuals to make better decisions about the authenticity of the mediathey encounter.

REFERENCES

1. Rossler, A., et al. (2019). "FaceForensics++: Learning to Detect Manipulated Facial Images." *IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019.

2. Li, Y., et al. (2020). "Celeb-DF: A Large-scale Challenging Dataset for DeepFake Forensics." *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020.

3. Afchar, D., Nozick, V., Yamagishi, J., Echizen, I. (2018). MesoNet: A Compact Facial Video Forgery Detection Network. IEEE Transactions on Information Forensicsand Security.

4. Afchar, D., Nozick, V., Yamagishi, J., Echizen, I. (2018). MesoNet: A Compact Facial Video Forgery Detection Network. *IEEE Transactions on Information Forensicsand Security*.

5. Kaur, A., Noori Hoshyar, A., Saikrishna, V., Firmin, S., & Xia, F. (2024). Deepfake Video Detection: Challenges and Opportunities. *Artificial Intelligence Review*.

6. Siegel, D., Kraetzer, C., Seidlitz, S., & Dittmann, J. (2021). *Media Forensics Considerations on DeepFake Detection with Hand-Crafted Features*. Journal of Imaging,7(7), 108.