MANTECH Publications

Journal of Research in Computer Science and Engineering
Volume 10, Issue 1, January-April, 2025
ISSN: 2457-0818(Online)

Development of a Deep Fake Detection Web Application Using Machine Learning

S.V.Chavan[1], Nirzara Manade[2], Shravani Shinde[2], Sonal Patil[2], Sunetra Bhambure[2]

HOD[1], Student[2]

Department of Computer Science and Engineering

Sanjay Ghodawat Institute, Atigre, Kolhapur, Maharashtra, India

Corresponding Author Email Id: *shravanishinde307@gmail.com[3]*

Abstract

The emergence of deepfake technology has increased suspicions regarding the trustworthiness and authenticity of digital media specifically video content as ai-manipulation techniques have developed exponentially identifying deepfakes is more difficult than ever before to combat this challenge we introduce deep detect a comprehensive web-based system specifically built to identify fake videos driven by state-of-the-art deep learning algorithms deep detect performs fast analysis on uploaded video materials to detect fake facial areas and delivers users true real-time results it accommodates many video formats and is designed to process compressed and low-quality video providing a wide range of applications having a user-friendly interface and scalable architecture deep detect is a robust tool for the public media outlets and forensic professionals to fight the dissemination of deep fakes furthermore the system learns and evolves with continuous model updates adjusting to new deepfake methods our solution helps in the ongoing process of upholding digital media integrity and shielding against disinformation in today's digital world.

Keywords: *Deep Detect, Deep fake technology, Digital media, Real-time results, AI manipulation, Fake videos, Authenticity*

INTRODUCTION

Of late, creative technologies have attracted considerable attention as vehicles for generating hyper-realistic audio and videos that are basically pieced together with deceptive ends in

mind. Such manipulations render it all the more challenging to discern real media from themselves and all other false media-not only shaming, slandering, and presenting false perceptions, but while going so far as to guide public perception. The more advanced the technology, the more sensational the title in using it for misuses; hence, a very high requirement demands to be set unto detection solutions capable enough to eradicate this menace. Deep Detect prides itself on being such a technological and advanced tool, a deepfake detection platform that can scan and detect the existence of manipulated media with a high degree of accuracy. We are several points high on the list of optimism that users shall trust Deep Detect to fight against digital deception; to secure media integrity while protecting the interests of individuals and organizations against possible attacks using deepfake technology. As development continues, such as AI-driven updates, Deep Detect will become a leader among tools helping lower the risks associated with synthetic media while championing transparency and trust in the virtual world.

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 systems 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 is 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. In addition to the detection over those validation set based tests, our approach has a comparable or even better generalization as evidenced by an AUC value drop from >0.9 to <0.7 whenever being tested on different training and test sets, with existing neural network-based methods.

Deepfake Video Detection: Challenges and Opportunities

Achhardeep Kaur, Azadeh Noori Hoshyar, Vidya Saikrishna, Selena Firmin, Feng Xia

In this research article publishers explained comprehensive use of deep learning methods for deep fake detection. As the deep fake technique uses advanced deep learning methods and neural network technique to replicate or to generate the fake content on the basis of given input. Because of this technique deep fakes are becoming more realistic. To detect the deep fake contents there should have the module which is trained using large amount of dataset where dataset contains both real and fake content and the use of GAN or auto encoder method and use of neural network such as CNN (Convolutional Neural Network) and RNN (Recurrent Neural Network) for detection. It also emphasis on the limitations and the drawbacks which occurs while using the advanced technique. There can be limitations on computational efficiency. It uses standardized approach to captures data from desired research about the study's aims, methodology or approach, major findings, and deep fake detection contributions.

PROPOSED SYSTEM

The system is a web-based application whose primary focus is to detect face-swapping deepfakes. A user can upload a video via the web browser, and the system will further perform frame extraction and further analyze these frames for manipulation. Once the analysis has been completed, a report is generated, and any identified flaws will be highlighted within the report. The detection engine employs ML libraries such as Tensor Flow, Open CV, or PyTorch, making use of pre-trained models that have been fine-tuned in order to look for deepfakes. The analysis is carried out frame by frame, guaranteeing that no deep fake

manipulations are missed. It's a user-friendly web app that gets the job done in terms of deepfake video content detection.

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 critically evaluate the authenticity of content.
- Users can receive immediate feedback on the authenticity of videos.

PROJECT SCOPE

The proposed system aims to address deepfake detection through a comprehensive approach. It will identify and classify real versus deepfake media, empowering users with the tools needed to identify deepfakes in order to discuss media trustworthiness. The platform will encourage building up the community where users may share insights and experiences about deepfake content. A feedback mechanism in place will help improve detection algorithms based on user input over time. Privacy and consent will be in place to avoid biases in detection algorithms. Moreover, public awareness will be raised through the education of users regarding the risks posed by deepfakes and the importance of critical skills in consuming media. A real-time detection mechanism will finally secure timely identification of manipulated content.

The Objective of the Proposed System

- **Real-Time Detection:** The development of one such application that will work with the real-time detection of deep fake videos and will flag them in line with cross-checking those that the videos are manipulated for the audience view.
- **Usability:** The interface should be meant to be user-friendly so that the transfer and enabling of media analysis can become very easy even for any user with little or no technical know-how about things.
- **Data Privacy and Security:** User privacy would generally be handled very delicately under stringent data processing and handling, where privacy policies would be communicated to the users.
- **Educational Resources and Training Modules:** An educational resource and training modules will be developed on this specific area that will assist journalists and

fact-checkers with an easy determination of whether they can identify and present the issue.

DESIGNING

React js: React.js is a JavaScript library for building interactive UIs, mostly single-page applications. It uses a component-based architectural style so that UI elements can be made modular and reusable, while the Virtual DOM gives performance by updating only the changed elements. Some key features that make React a top choice for building fast, scalable web and mobile apps include support for readable JSX-compressed code, one-way data binding that ensures the expected flow, and Hooks that enable control over lifecycle and state in functional components. Other driving factors are a large community support, SEO-friendly, and cross-platform abilities through React Native.

Tailwind Css: With Tailwind, a utility-first framework, web application developers can speed their efforts a great deal by means of a more or less predefined set of classes for background colors, e.g., bg-blue-500, or text size, for instance, text-xl, rather than writing custom CSS. It is highly customizable by way of a configuration file, sorted in responsive design with built-in utilities for different screen sizes. Dark mode support is included in Tailwind alongside purging in production for performance, which reduces the CSS files' final weight. Therefore, it is straight to be the first choice for any maintainable, scalable web application.

DEVELOPMENT

Python: Excellent selection of Python for AI and ML (and ease of learning). It can be used for natural languages processing, computer vision, and robotics. Some of them are scikit-learn, TensorFlow, PyTorch, and NLTK. Python's flexibility is also enhanced because any big data, cloud computing, IoT, etc., could be integrated with it. Flask is a Python-based web framework; hence, it is pretty swift and flexible, so that developers focus on project logic while managing the setup and environment comfortably.

Firbase: Firebase is a Backend as a Service by Google that offers a plethora of handy features for web and mobile application development. This includes simplified user authentication, real-time syncing of data, and deployment of applications, push notifications, and serverless backend code, among others. Firebase is very popular in Android, Web, and Python

applications owing to its scalability, real-time syncing, and nice integration with Google Cloud.

SOFTWARE REQUIREMENTS

- **Operating System:** Windows 10 or higher
- **Front-End Languages:** react.js, tailwind css
- **Back-End Languages:** Python
- **Data Server:** Firebase
- **Code Editor:** VSCode, Google collab

HARDWARE CONFIGURATIONS

RAM : 8 GB MINIMUM – 64 GB MAXIMUM

STORAGE: 1, TB

CPU: A multi-core, high-frequency processor

GPU: NVIDIA GPUs with CUDA support/cards with at least 10–12 GB of VRAM

UML DIAGRAMS

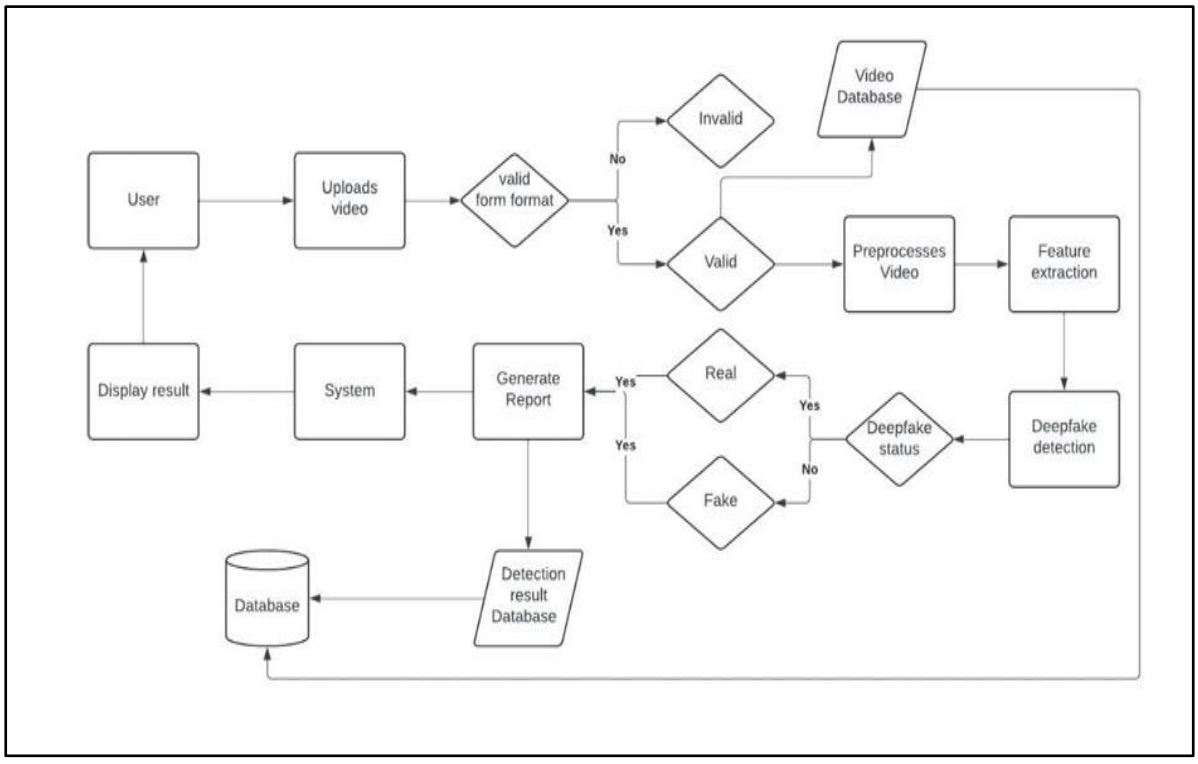

Figure no 1: Flowchart

As shown in the above Fig. 1. The user uploads a video that, after format validation, undergoes preprocessing. In order to perform deep fake detection technologies, throughout this process, some important features are extracted. A deep learning model analyzes the video and decides if it is true or fake. If the answer is fake, then it fills in the table of detection result status in the database; if it is real, it goes on with report generation.

The system saves the detection results into the database and presents the final outcome of deep fake detection to the user. Such a well-thought-out workflow guarantees validation, processing, and detection in an efficient manner along with digital media integrity.

ER Diagram

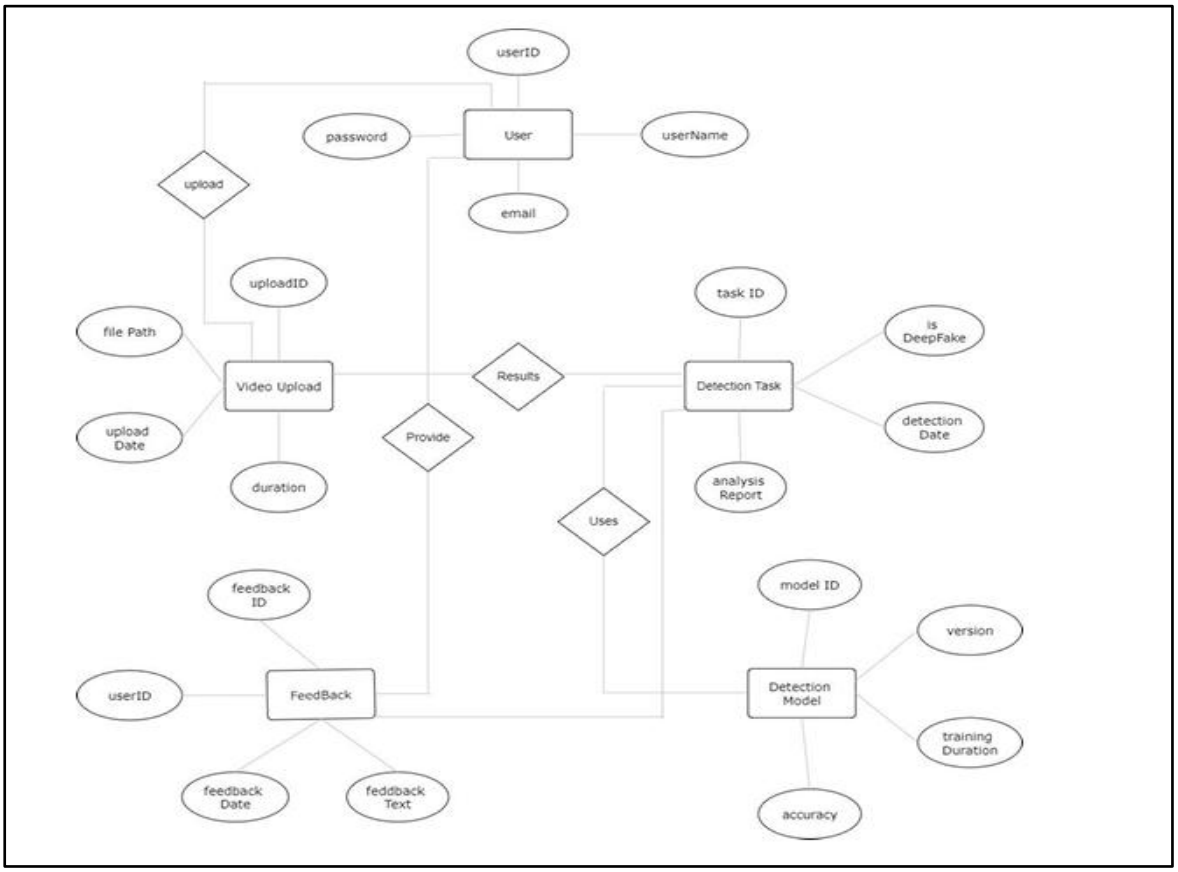

Figure no.: 2

The User entity covers the particulars of the user, while the Video Upload entity does for the video uploads. The Detection Task does video assessments to determine whether they are deepfakes, using the Detection Model that includes model specifications and modeling accuracy. The user can provide feedback to improve the performance of the system through

the Feedback entity. So, these entities work together with the system to enable efficient deepfake detection.

Level 0 DFD

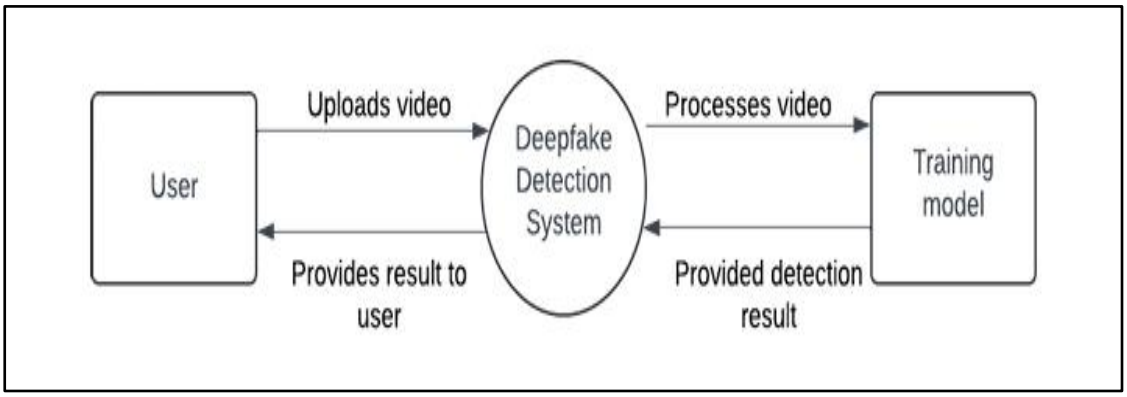

Figure no.: 3

Within the Deepfake Detection System, there exist basic components of interaction between components. A user uploads a video into Deepfake Detection System, through which a Training Model processes the video. It unapologetically examined the video and relayed back the result to the system. The system finally communicates the detection result back to the User, saying whether the video is real or a deepfake. The implementation of this fairly simple infrastructure is an effective and efficient means of detecting deepfakes, giving out the results.

Level 1 DFD

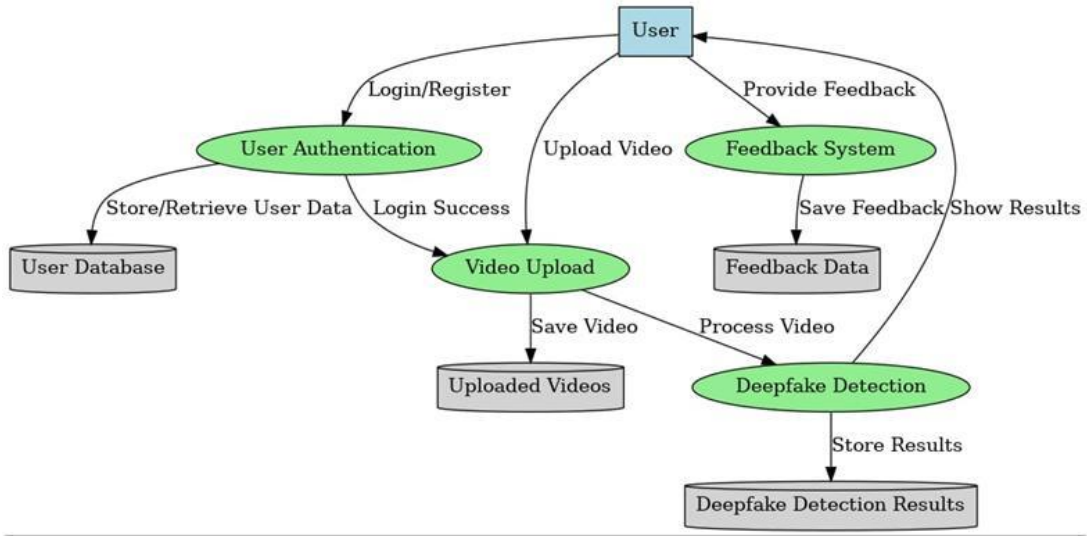

Figure no.: 4

The Level 1 Data Flow Diagram (DFD) for the Deepfake Detection Application illustrates how users interact with the system and how data flows between different components. Users first authenticate through the User Authentication process, which verifies their credentials using the User Database. Once authenticated, they can upload videos, which are stored in the Uploaded Videos database and then processed by the Deepfake Detection module. The detection results are saved in the Deepfake Detection Results database and displayed to the user. Additionally, users can provide feedback, which is stored in the Feedback Data database for system improvement. This diagram ensures a streamlined representation of data movement, focusing on authentication, video analysis, and feedback collection while excluding the training module for simplicity.

USE CASE DIAGRAM

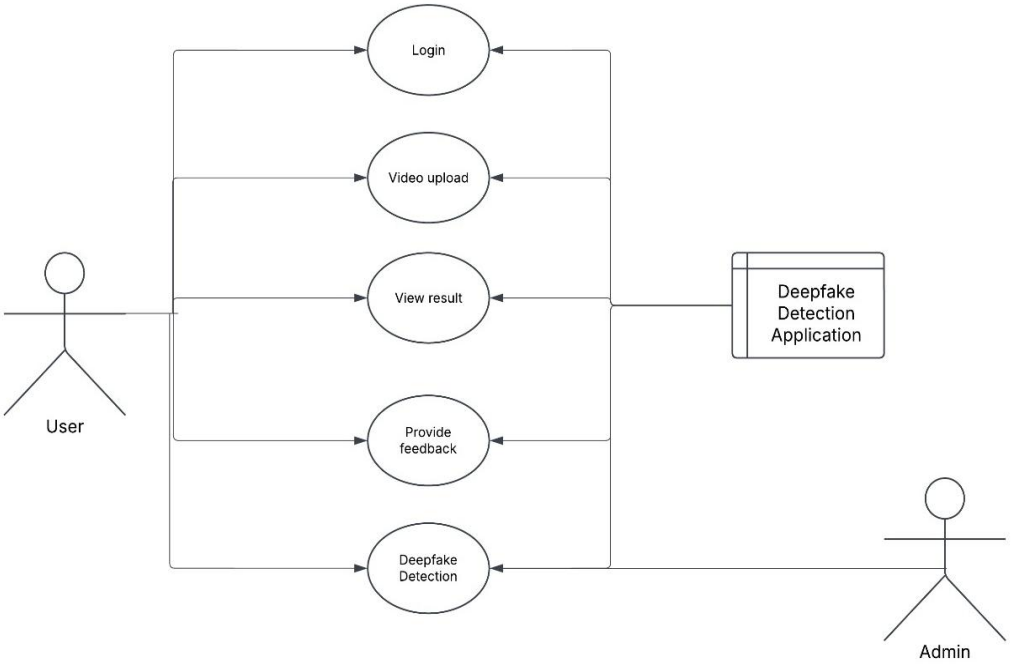

Figure no.: 5

SNAPSHOTS OF THE SYSTEM

The home page of Deep Detect introduces deepfake technology, its development, dangers, and consequences. It has a clean design with a navigation bar to access Upload and Feedback easily. A"Get Started" button invites users to try out the platform and use its deepfake detection feature.

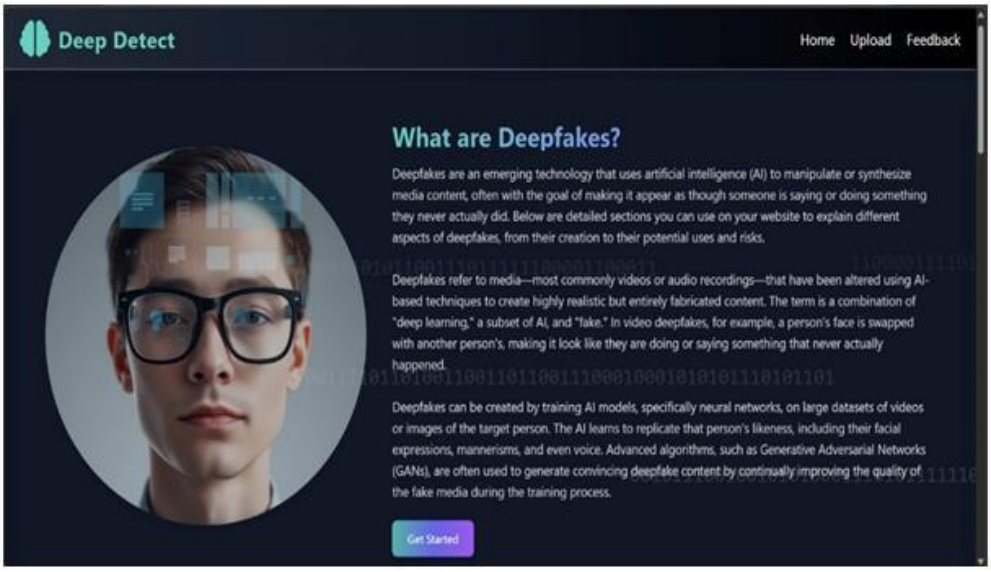

Figure no.: 6

The upload page for Deep Detect enables individuals to upload video files for deepfake detection. One can drag and drop or browse to upload a file and then click "Upload & Detect Deepfake" to process detection. An "Open Dashboard" button is available for viewing detailed results and analysis.

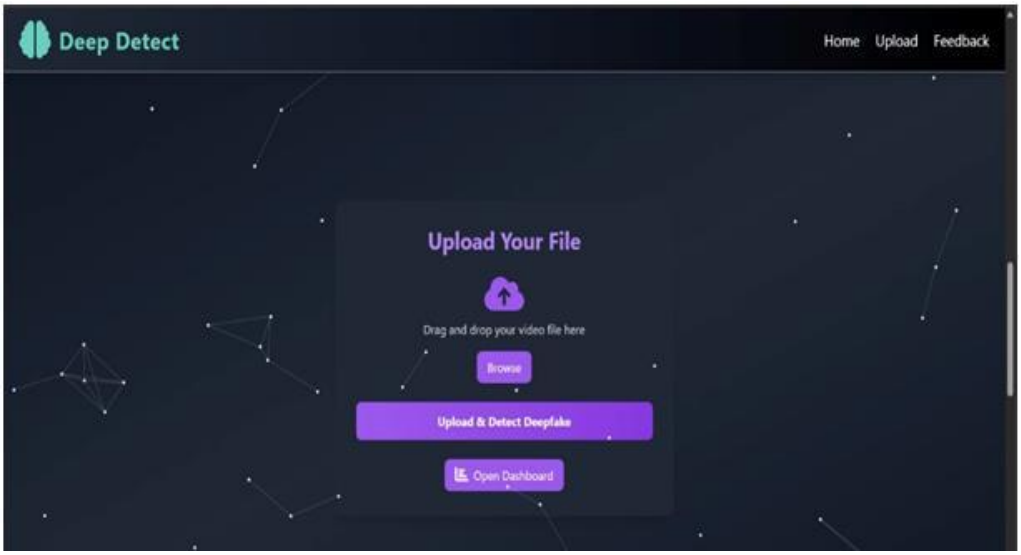

Figure no.: 7

The feedback page on Deep Detect provides the facility to upload one's views regarding the site. The user can input a rating, leave comments, and submit feedback by clicking on the "Submit Feedback" tab. This assists in making the system better with regard to user experience.

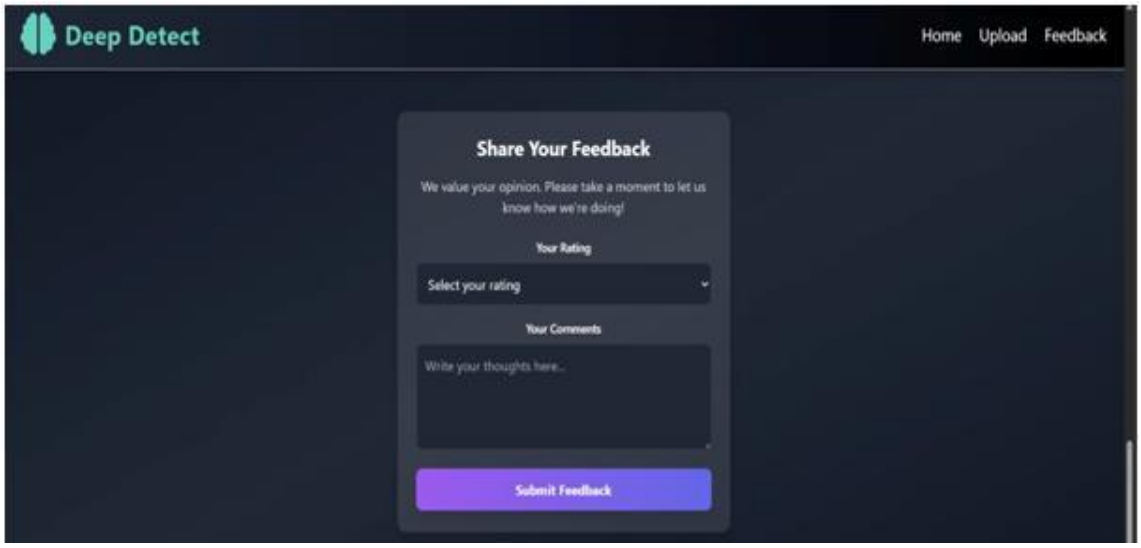

Figure no.: 8

The sign-up page permits users to register for an account by inputting their first name, last name, email address, and password. The users may register with the "Sign Up" icon or sign up through Google authentication. Registered users can go to the Sign In page.

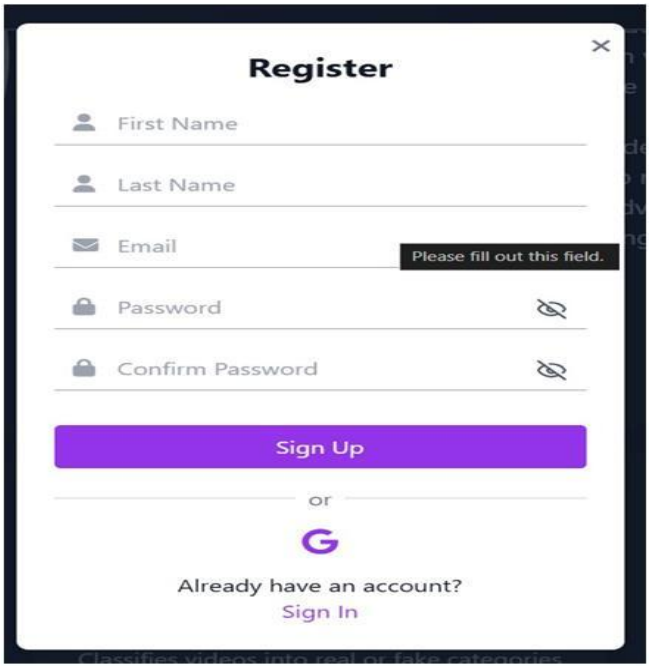

Figure no.: 9

The Sign In page permits users to log in utilizing their email and password, has an option for recovering forgotten passwords, and allows them to sign in through Google authentication. New users may go to the Sign Up page to create their account.

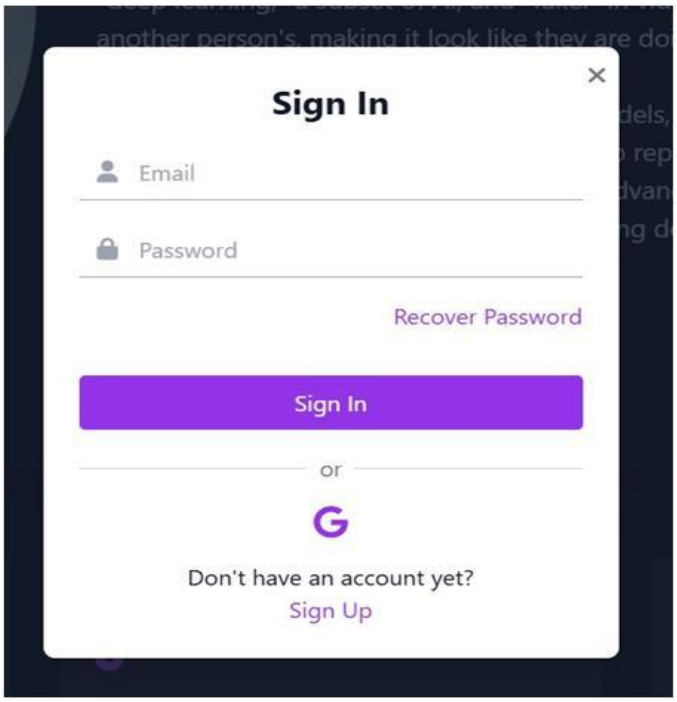

Figure no.: 10

CONCLUSION AND FUTURE ENHANCEMENT

The increasing danger of deepfake material decreases the credibility of digital media and poses risks to individuals, media outlets, and society as a whole. Deep Detect offers a complete as well as scalable solution to this risk through a solid web-based platform developed specifically for fake videos detection. Using the strength of strong advanced deep learning algorithms, this app aims to give the most precise and effective detection of altered facial material even under problematic situations such as low-quality and compressed video mode.

The intuitive interface of Deep Detect makes it accessible to the widest range of users-from individual users to media professionals and forensic experts, helping them to maintain content integrity and fight against false information. 'Deep Detect' is poised to empower its users in the continuous fight against misinformation and fraudulent media with real-time analysis and scalable architecture.

With deepfake technology becoming increasingly sophisticated, the demand for new detection solutions is even more paramount. Ongoing development in order to onboard increasingly advanced algorithms, improve detection accuracy, and increase its ability to deal with

increasingly sophisticated video manipulation, through such advancements Deep Detect reaffirms its dedication to digital media authenticity, thereby opening up the way to a safer and more trusted digital space.

REFERENCES

1. Rossler, A., et al. (2019). "Face Forensics++: 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 Forensics and Security.
4. Afchar, D., Nozick, V., Yamagishi, J., Echizen, I. (2018). MesoNet: A Compact Facial Video Forgery Detection Network. IEEE Transactions on Information Forensics and 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.