# DeepFake\_Detection

## Table of Contents:

- What is DeepFake?

- Demo of the Project

- Impact of DeepFake Videos

- Project Objectives

- Project Pipeline

- - Pre-processing WorkFlow

- - Prediction WorkFlow

- Models Usage and their Architecture

- Deploy

- - Code Running Commands

- Technologies Used

- Conclusion

- Team

## What is DeepFake?

DeepFakes are images or videos which have been altered to feature the face of someone else, like an advanced form of Face Swapping, using an AI DeepFake Converter.

Many Deep Fakes are done by superimposing or combining existing images into source images and videos using Generative Adversarial Networks (GAN) and these networks are developing better every day.

## Impact of DeepFake Videos

DeepFakes can be used to create fake news, celebrity unusual videos, politician content videos, and financial fraud.

False Rumours can be spread using DeepFake videos which causes unrest and mental anxiety among people.

Many fields in Film Industry, content providers, and social media platforms are fighting against DeepFake.

## Project Objectives

Identification of deepfakes is necessary to prevent the use of malicious AI.

We intend to:

- Build a model that processes the given video and classifies it as REAL or FAKE.

- Deploy a feature in social media apps to detect and warn content providers about deepfake images or videos.

## Goal:

To Create a deep learning model capable of recognizing deepfake images.

A thorough analysis of deepfake video frames to identify slight imperfections in the face and head. The model will learn features differentiating real images from deepfakes.

## Project Pipeline

| Steps | Description |

| --- | --- |

| Step1 | Loading the datasets |

| Step2 | Extracting videos from the dataset |

| Step3 | Extract all frames in the video for both real and fake |

| Step4 | Recognize the face subframe |

| Step5 | Locating the facial landmarks |

| Step6 | Frame-by-frame analysis to address any changes in the face landmarks |

| Step7 | Classify the video as REAL or FAKE |

## Models Usage:

Models with CNN Architecture:

\*\*MesoNet:\*\*

- Pre-trained to detect deepfake images; bad at detecting fake video frames.

\*\*ResNet50v:\*\*

- Trained using deepfake images cropped from videos with preset weights of the imagenet dataset.

\*\*EfficientNetB0:\*\*

- Trained using deepfake images cropped from videos with preset weights of the imagenet dataset.

## Running Code

Combination of CNN and RNN models is used to detect Fake Videos.

We achieved a test accuracy ~85% on a sample DFDC dataset.

To run this code, first run:

```bash

pip install -r requirements.txt

```

Run the `main.py` file in the deploy folder:

```bash

python main.py

```

\*Ensure required packages are installed. Preferably run on GPU.\*

## Technologies Used

Languages and Tools: Python, TensorFlow, OpenCV, Pandas, Scikit-learn, Seaborn, etc.

## Conclusion

In this project, we implemented a method for the detection of deepfake videos using CNN and RNN architectures.

We experimented with CNN-only models like EfficientNet and ResNet and achieved better results by combining CNN and RNN models, obtaining a maximum test accuracy of ~85%.