**Deepfake Detection System (Real✔️or fakE❌)**

# **Project Report**

First I read the document which was provided by Postulate Faculty on WhatsApp, and go through with both project’s Objective, Project Workflow & steps, and deliverables required to complete weekly and did the full analysis that which project from both suits best to my interest and expertise.

And I choose the Project 2: Deepfake Detection System.

* Why I Choose Project 2 Over Project 1

I chose this project because it aligns with my interest in AI and its real-world impact, allowing me to develop practical solutions to a critical problem while expanding my expertise in machine learning and deep learning.

Deepfake technology is rapidly evolving, making it increasingly difficult to distinguish real videos from manipulated ones, leading to serious risks.

**Real World Problem:-**

1. Misinformation and Fake News
2. Fraud and Identity Theft
3. Defamation and Reputational Damage
4. Cybersecurity Threats
5. Legal and Law Enforcement Challenges

**Advantages** :-

1. Prevention of Misinformation
2. Security & Privacy Protection
3. Legal & Forensic Applications
4. Enhanced Media Integrity

Then after I clearly made my mind to work on Deepfake Detection System I Started my more research on What is deepfake exactly is ? , How it is created ?. And I found that deepfakes are being created through deep learning algorithms like generative adversarial networks (GANs). I watched some deepfake videos and images with their originals (Side by side) to see the clear difference between them. So, this research gave me a clear understanding that how this project is going to be, where and how model will work on a deepfake video to predict its real or fake.

Then after I started following the document steps and its Step1: Dataset Collection. So, I started my research on choosing a right dataset for my project and that is easy to get. And come know through document , ChatGPT, Google that there are 4-5 Options of dataset which can be used to build this kind of

project. I also searched about the dataset sizes, where to get, contents, structure, format.

Different Datasets :-

|  |  |
| --- | --- |
| 1. FaceForensics++ | 470GB |
| 1. Celeb-DF (v2) | 39GB |
| 1. DFDC | 470GB+ |
| 1. DF-TIMIT | 4GB |

* **Approach 1** :-

Dataset :- DF-TIMIT

Model :- Basic CNN

Link :- [DeepfakeVideosdetectionsystem.ipynb](https://github.com/Apkajai/DeepFakeDetectionSystem/blob/abe0187e5a05646578eec0f73017f51b3dfcb025/DeepfakeVideosdetectionsystem.ipynb)

**Challenges faced :-**

* Data Downloaded from :- [**Idiap Research Institute**](https://www.idiap.ch/en/scientific-research/data/deepfaketimit)
* Complete dataset should contain 16 Pairs(means 32 persons) each person have 10 videos( means total 320 Deepfake Videos)
* But yet the dataset was not complete. It only contained fake videos and only two original as sample. Class Imbalanced
* Tried a lot but unable to find complete dataset because its not available publicly.

Yet keep proceeded with available resources AND COMPLETED but model performance not as expected. DROPPED THIS IDEA!!!

* **Approach 2 :-**

Dataset :- celeb-df(V2)

**Challenges faced :-**

* Data Downloaded from :- Got a google form link from Official Github account of dataset creator.
* Dataset was available on Drive, direct link to download Unable to process this dataset due to size of dataset is large
* **Approach 3 :-**

Dataset :- Already Extracted Frames from FaceForensics++ and Celeb-df dataset found on Kaggle.

Model :- CNN

Link :- [aug.ipynb](https://github.com/Apkajai/DeepFakeDetectionSystem/blob/a4ffb56d7b88e715e678cd070482f6cfb0a018f7/aug.ipynb)

**Challenges faced :-**

* Data Loading :- Local System to Google Drive
* Dataset downloaded from Kaggle in .zip format. I extracted that data on local system it contains 16500+ extracted frames from 1000 videos(Real & fake both)
* I need to upload that on drive but a 400MB dataset containing 16500+ png files took 3hrs to upload with 10Mbps internet Speed Then I uploaded from this method only but don’t stopped research how to upload data faster. Then found a solution
* I uploaded zip file(400MB) onto drive it took 5 mins and used python to unzip the file on drive itself on the given path it took 5 mins to unzip file

Code used :- [ZiptoUnzip.ipynb](https://github.com/Apkajai/DeepFakeDetectionSystem/blob/1825c2caaeb7df94987cb6c042c9bba98efece3e/ZiptoUnzip.ipynb)

* Total time to load dataset :-

1. 3hrs(Uploaded Unzip file to drive)
2. 10 mins(Uploaded zip file and unzip using python on Drive)

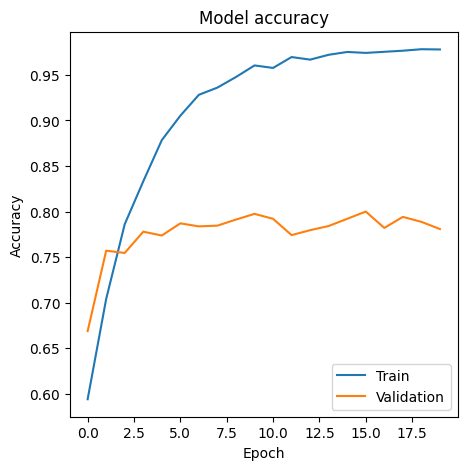
* Face detection and Frame cropped

Did the face detection on frame extracted from videos and cropped the box from the image around the face.

* Model training:-

See the graph below

This graph representing training accuracy in blue curve and Validation accuracy in orange curve.

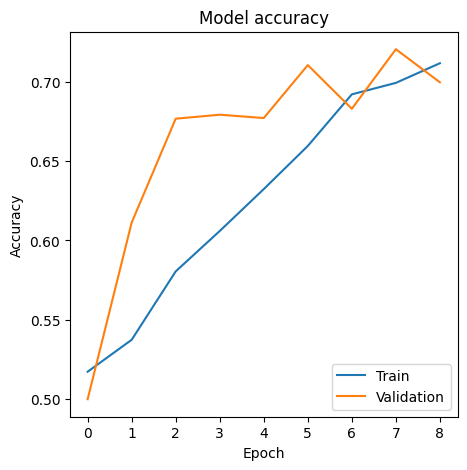
The gap between this two curves showing that model is totally overfitted because the model is remembering the training instead of learning from it.

As you can see on the above graph the gap between both line that is model overfitting now I used the following to overcome these challenges are :-

Early stopping :- It monitor the matrices after every epoch and stops model training if the accuracy stop increasing.

Data Augmentation :- This step augment by making small changes to existing data, such as cropping, rotating, or flipping image.

Model Checkpoint :- It also monitor the matrices while model training same like early stopping and if model keeps improve this saves the model.

Now, the new graph is this

After applying this above techniques the model stopped training at epoch 9 and saved best model weights of epoch 6.

Now the project is complete and webpage also created using streamlit and my model is capable of both image as well as videos.

## Thank You ❤️