

PHASE -1

Problem Statement

What is DeepFake?

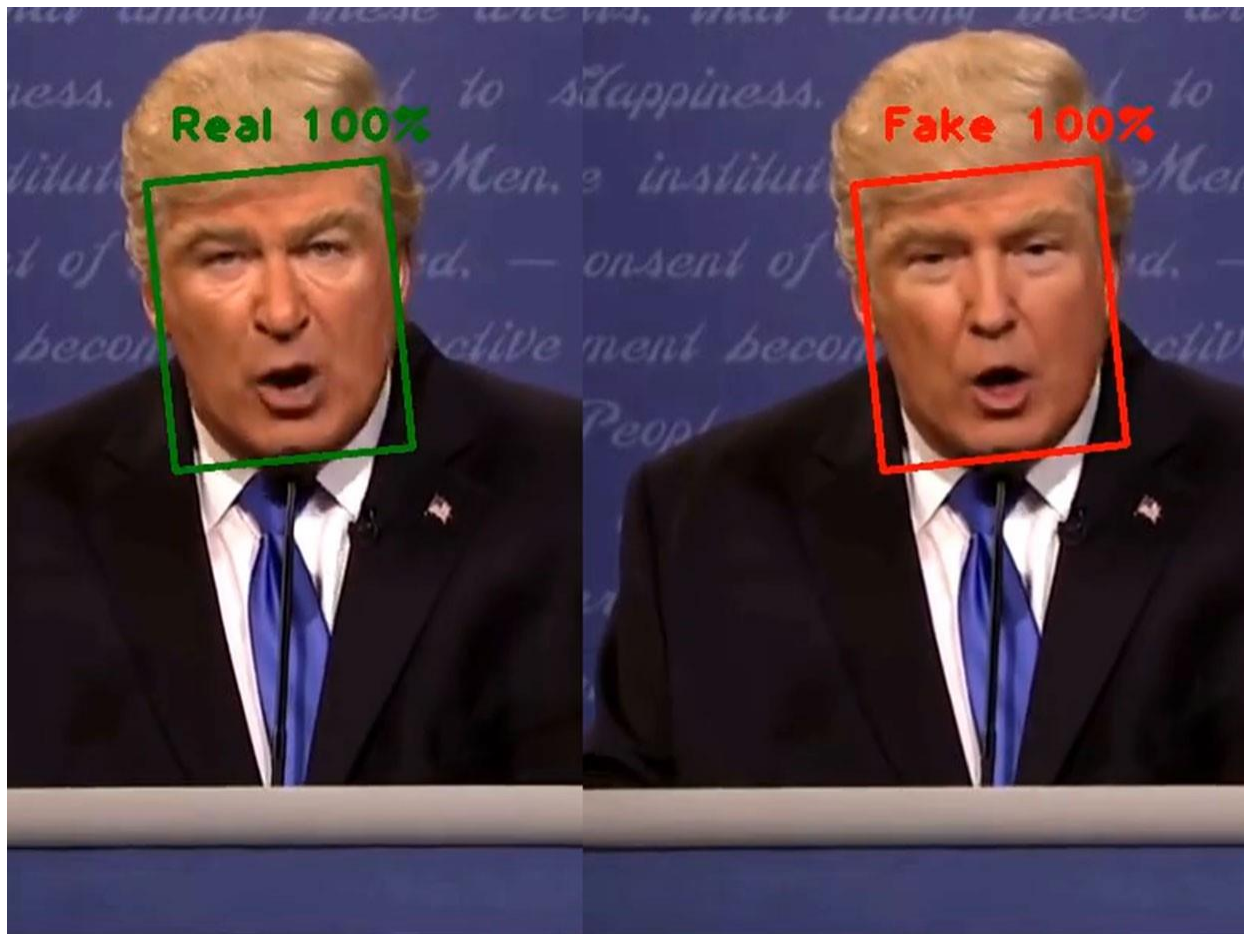
DeepFakes are images or videos which have been altered to feature the face of someone else, like an advanced form of Face Swapping, using an AI DeepFake Converter.

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





Dataset

DeepFake Detection Challenge Dataset consists of the large collection of video and audio altered files.

A Sample of this Dataset is used for our project.

Link:

Deepfake Detection Challenge

Identify videos with facial or voice manipulations

<https://www.kaggle.com/c/deepfake-detection-challenge/data>

#DFDC

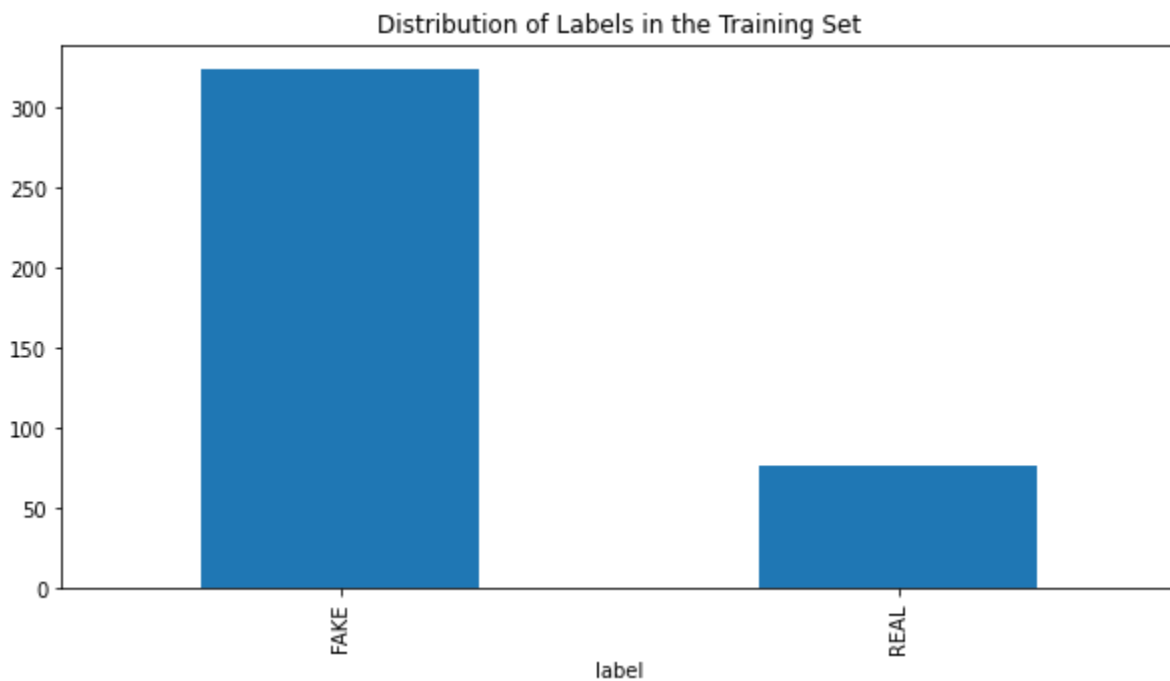
- Train Data: It consists of 400 videos in .mp4 format.
- Test Data: It consists of 400 videos in .mp4 format.

MetaData of the Dataset

- ♦ `filename` - the filename of the video
- ♦ `label` - whether the video is REAL or FAKE
 - `y` is 1 if the video is FAKE, 0 if REAL
- ♦ `original` - in the case that a train set video is FAKE, the original video is listed here
- ♦ `split` - this is always equal to “train”.

Exploratory Data Analysis

Distribution of Labels in the Training set




Analysis of the dataset

	label	split	original
Total	400	400	323
Most frequent item	FAKE	train	atvmxvwyns.mp4
Frequency	323	400	6
Percent from total	80.75	100.0	1.858

Notebook Link

Google Colaboratory

 https://colab.research.google.com/drive/1HikKRZYnpP39E93OwJnhJ9HY8zBd1_oq?usp=sharing



Preprocessing pipeline specific to data

Pipeline

step 1	Loading the datasets
step 2	Extracting videos from the dataset
step 3	Extract all frames in the video for both real and fake
step 4	Recognize the face subframe
step 5	Locating the facial landmarks
step 6	Frame-by-frame analysis to address any changes in the face landmarks

Project Objectives:

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

We intend to,

- To Build a model that processes the given video and classifies it as REAL or FAKE.
- To deploy a feature in the social media apps that can detect and give a warning to the content provider who is willing to do viral by uploading deepFaked images or videos.

Goal: Create a deep learning model that is capable of recognizing deepfake images. A thorough analysis of deepfake video frames to identify slight imperfections in the face head and the model will learn what features differentiate a real image from a deepfake.

References:

- [2004.07676v1.pdf \(arxiv.org\)](#)
- [https://www.ijitee.org/wp-content/uploads/papers/v9i6/E2779039520.pdf](#)
- [Deepfake Detection Software: Types and Practical Application - Antispoofing Wiki](#)