Video Forgery Detection using DNN

Video forgery will manipulate video with fake or forge content to deceive viewer and this forge video cannot be detected with human eyes so we are using Deep Neural Network (DNN) algorithm which will get trained on Forge and Real videos and then this trained model can be applied on any new test video to detect weather video frame is Real or Forge.

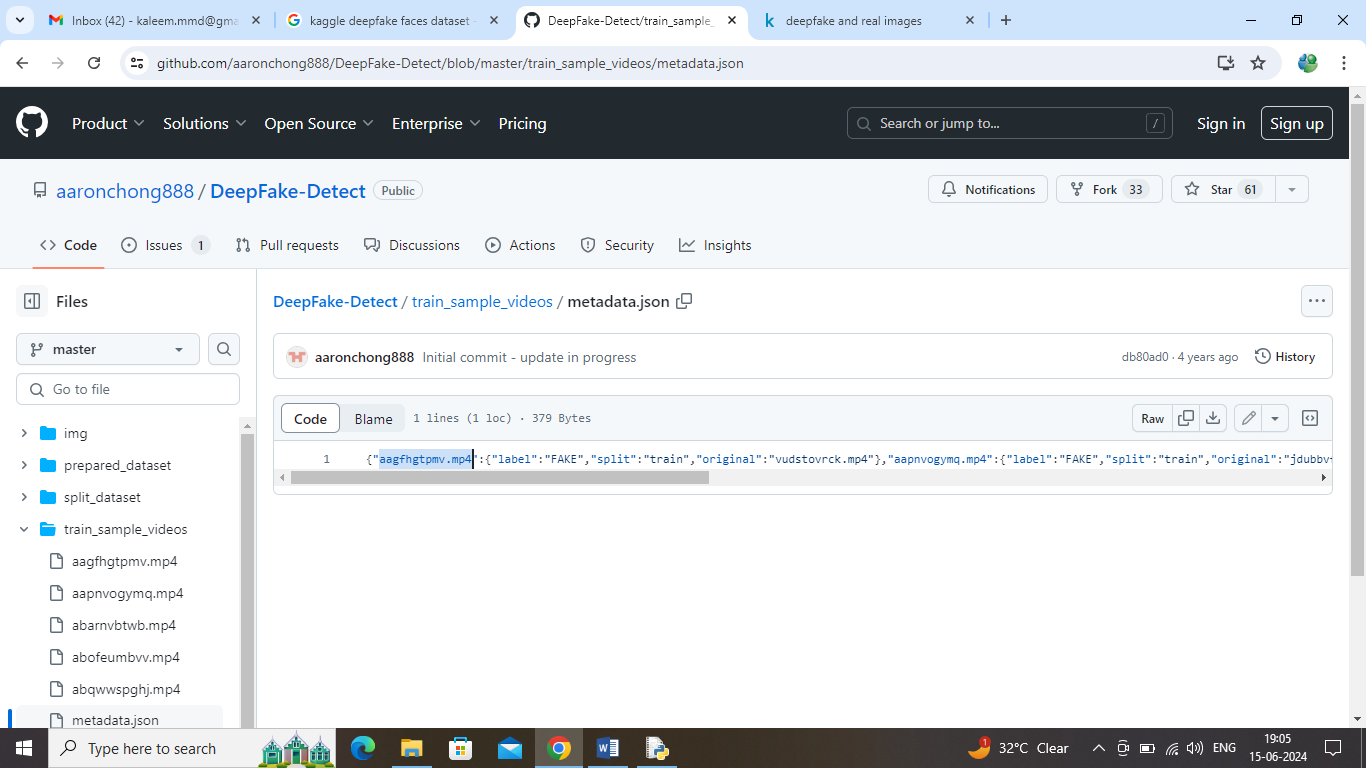
DNN algorithm get trained on features of Forge and Real videos so it can easily differentiate between real continuous frames and the frame with discontinue pattern. Often forge frame will have some kind of discontinuous pattern and such features will help DNN algorithm in detecting real or forge video.

To train DNN algorithm we have used dataset from KAGGLE which contains nearly 60 Real and Forge videos and can be download from below URL

<https://www.kaggle.com/datasets/neetusingla5/video-forgery-dataset>

When we train DNN models on large number of videos then system is going out of memory so we trained this model on 60 videos and then tested this model with some Forge and Real videos which downloaded from below GITHUB URL.

<https://github.com/aaronchong888/DeepFake-Detect/blob/master/train_sample_videos/metadata.json>



In above GITHUB URL screen you can see ‘aagfhgtpmv.mp4’ video is fake and ‘abarnvbtwb.mp4’ is the real video and this model is successfully predicting this videos as Forge and real. This link videos we used only for testing model

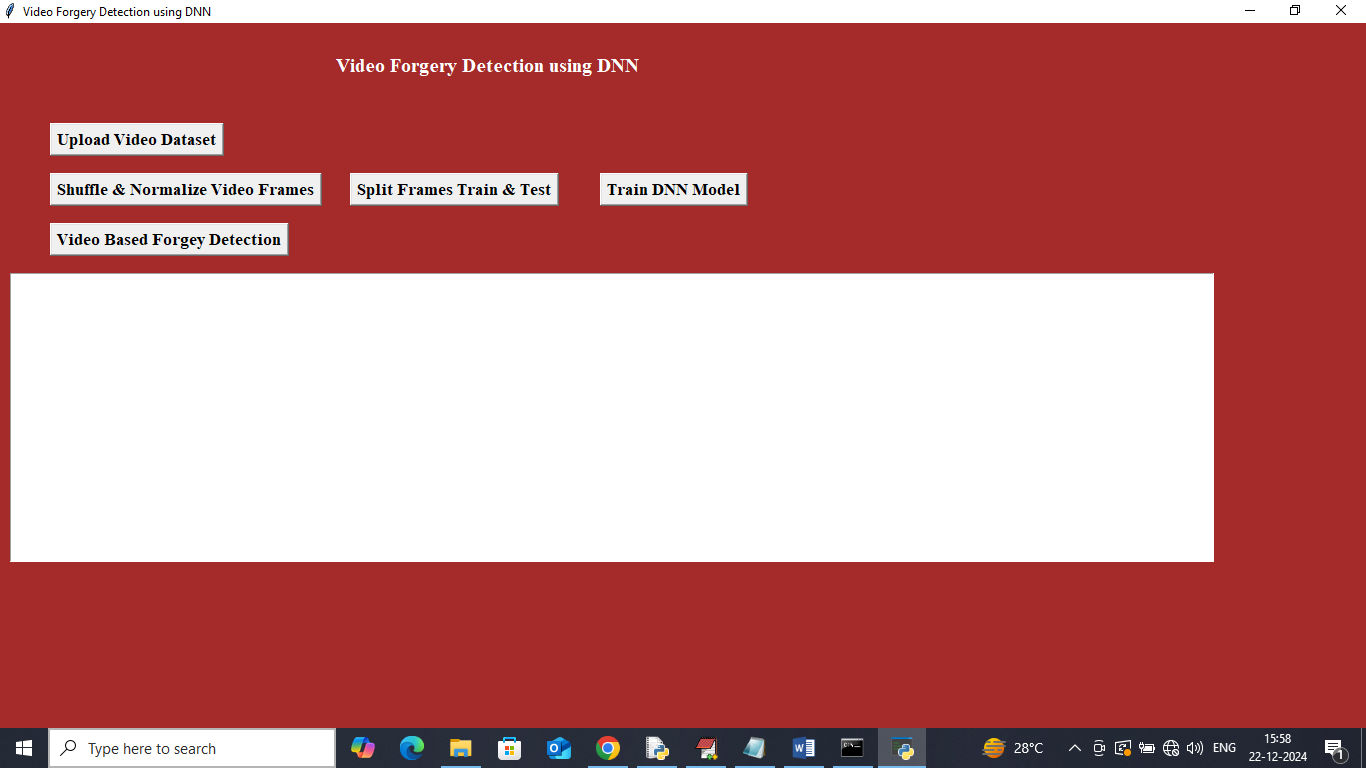
This project will take video as input and then generate new video by removing all forge frames and you can see generated real video in a file called ‘video\_after\_removing\_forge.mp4’.

To implement this project we have designed following modules

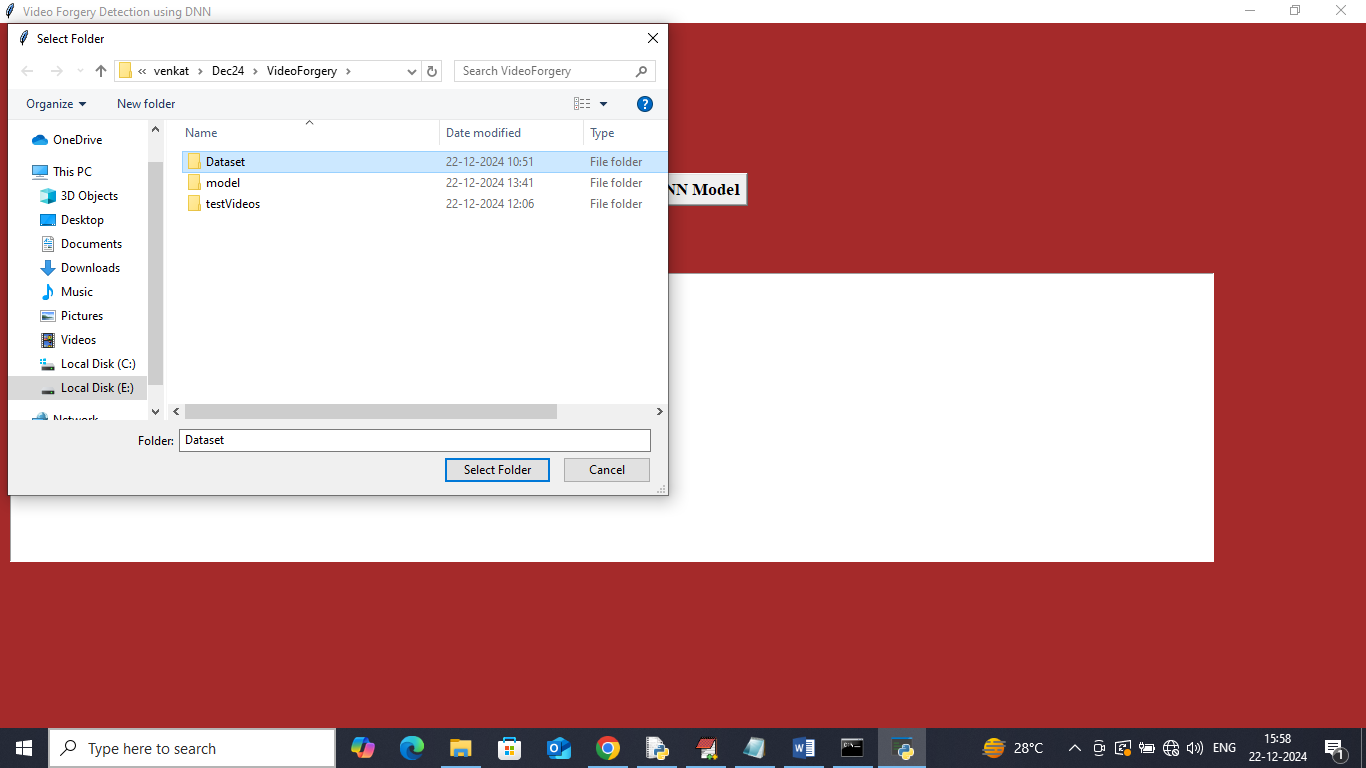
1. Upload Video Dataset: using this module will upload video dataset to application and then extract frames from each video and then create a training array with video features
2. Shuffle & Normalize Video Frames: all extracted video features will be processed by shuffling and normalization
3. Split Frames Train & Test: split frames features into train, validation and test part
4. Train DNN Model: training and validation features will be input to DNN algorithm to train a model and this model will be applied on test features to calculate prediction accuracy
5. Video Based Forgery Detection: input test video can be upload and then DNN will predict real and forge frame and then create a new video by ignoring forge frames.

SCREEN SHOTS

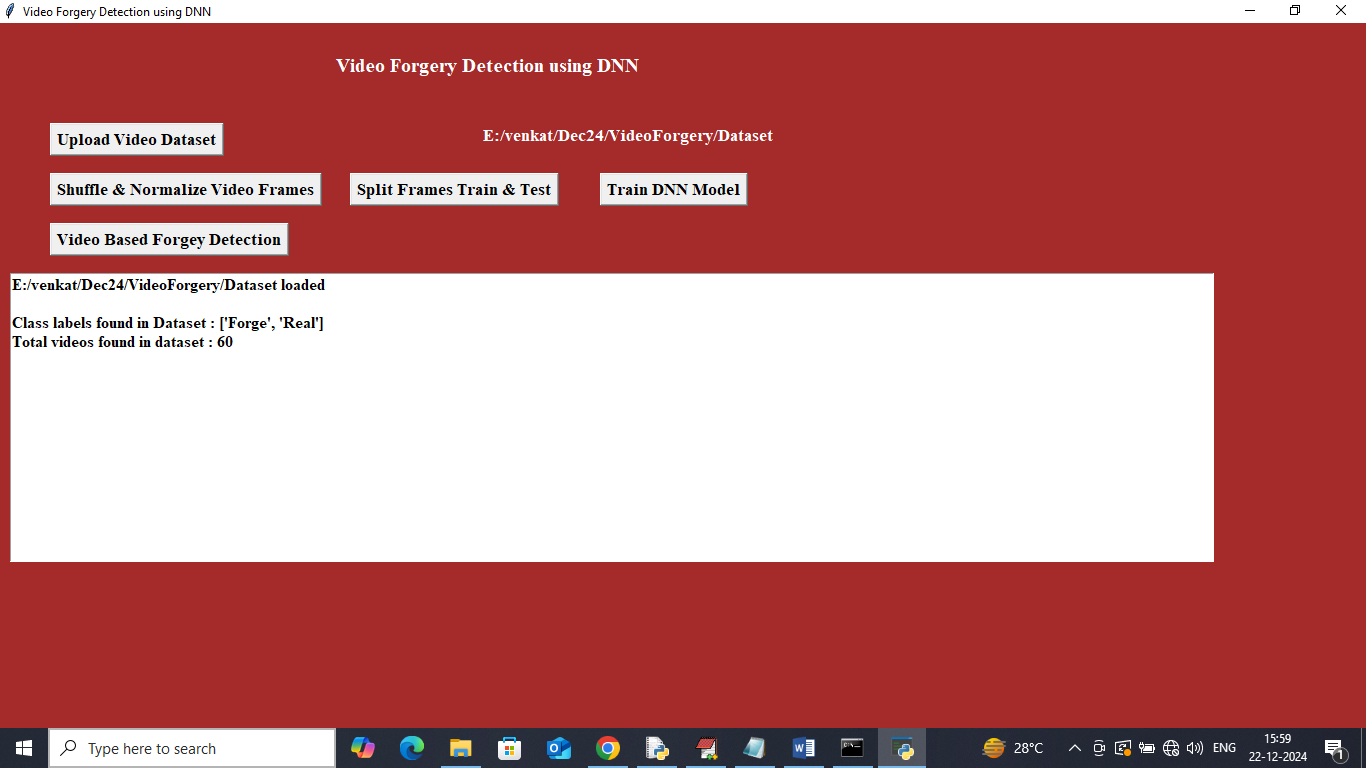
To run project double click on ‘run.bat’ file to get below page



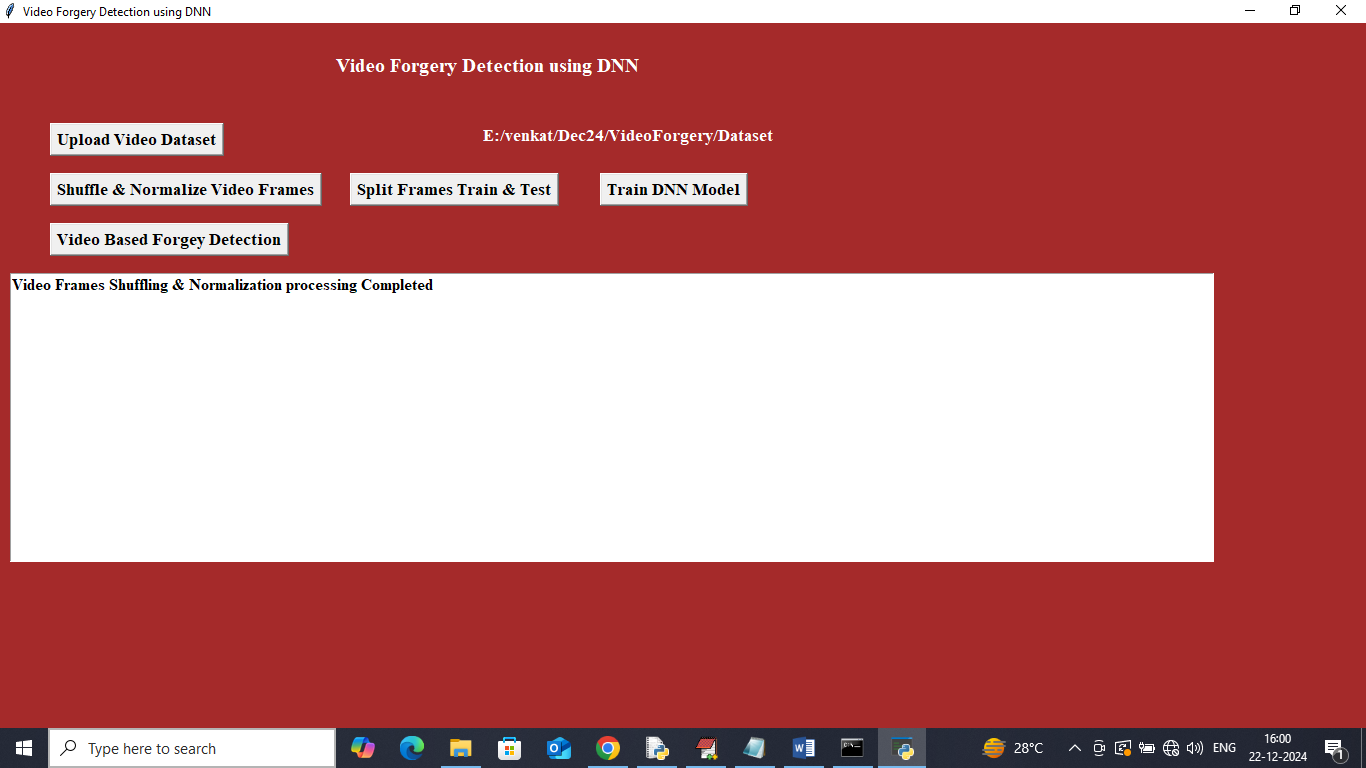
In above screen click on ‘Upload Video Dataset’ button to upload videos and get below page



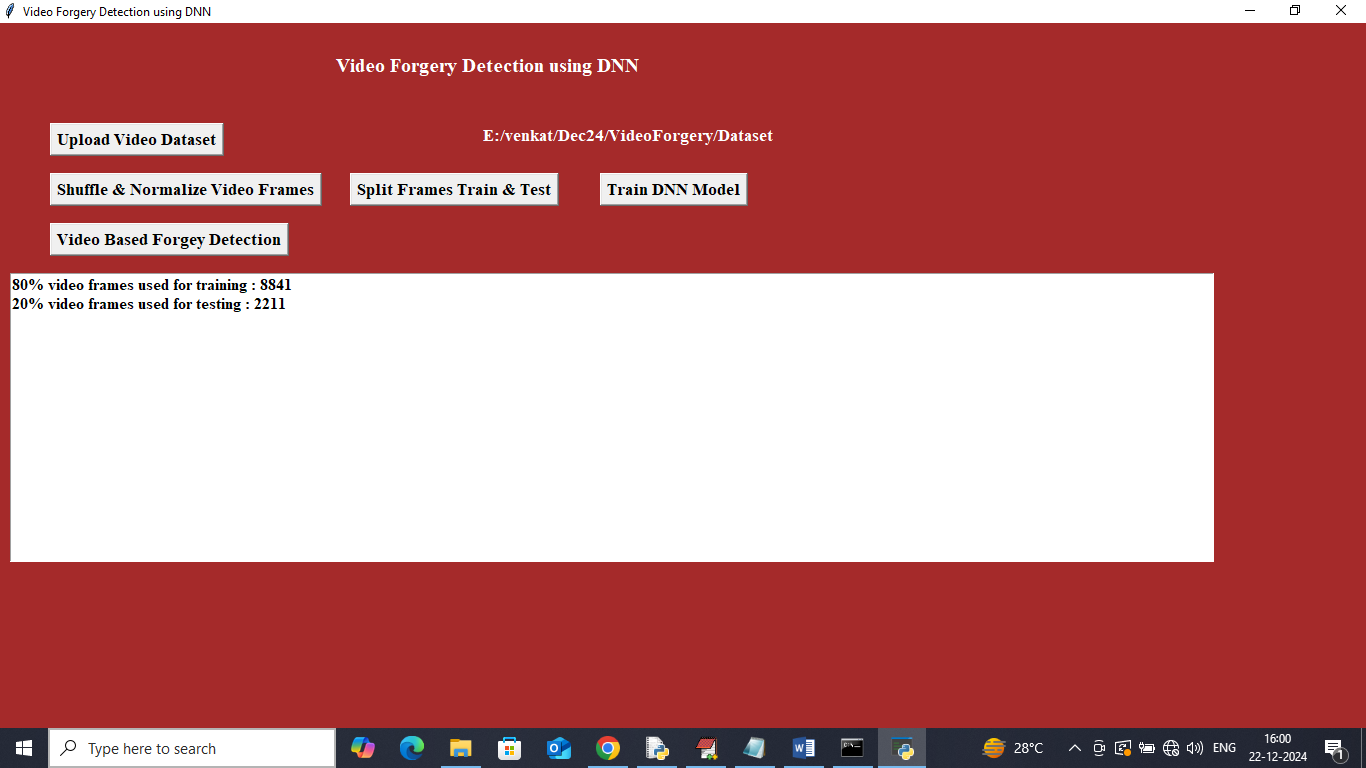
In above screen selecting and uploading entire ‘Dataset video folder’ and then click on ‘Select Folder’ button to get below page



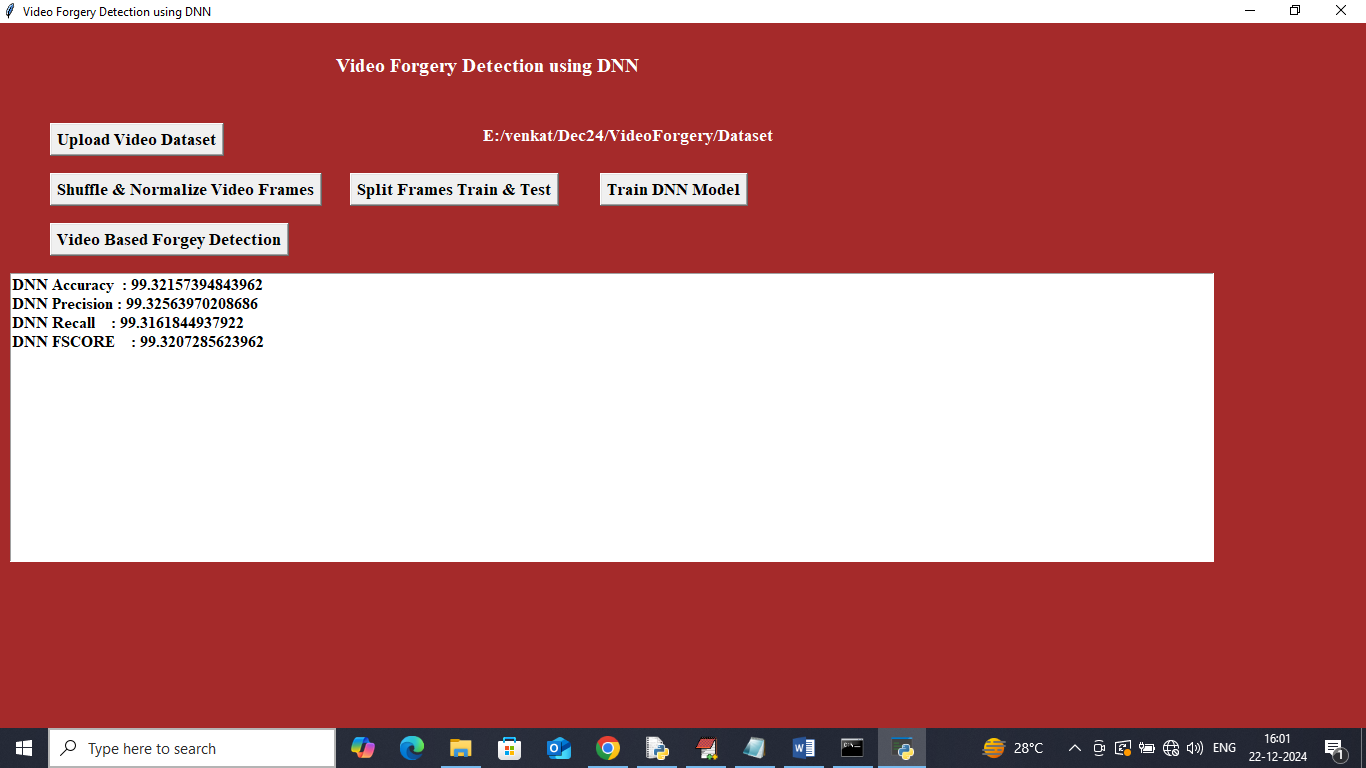
In above screen can see dataset contains 60 videos with Real and Forge classes and now click on ‘Shuffle & Normalize Video Frames’ button to process features and get below page



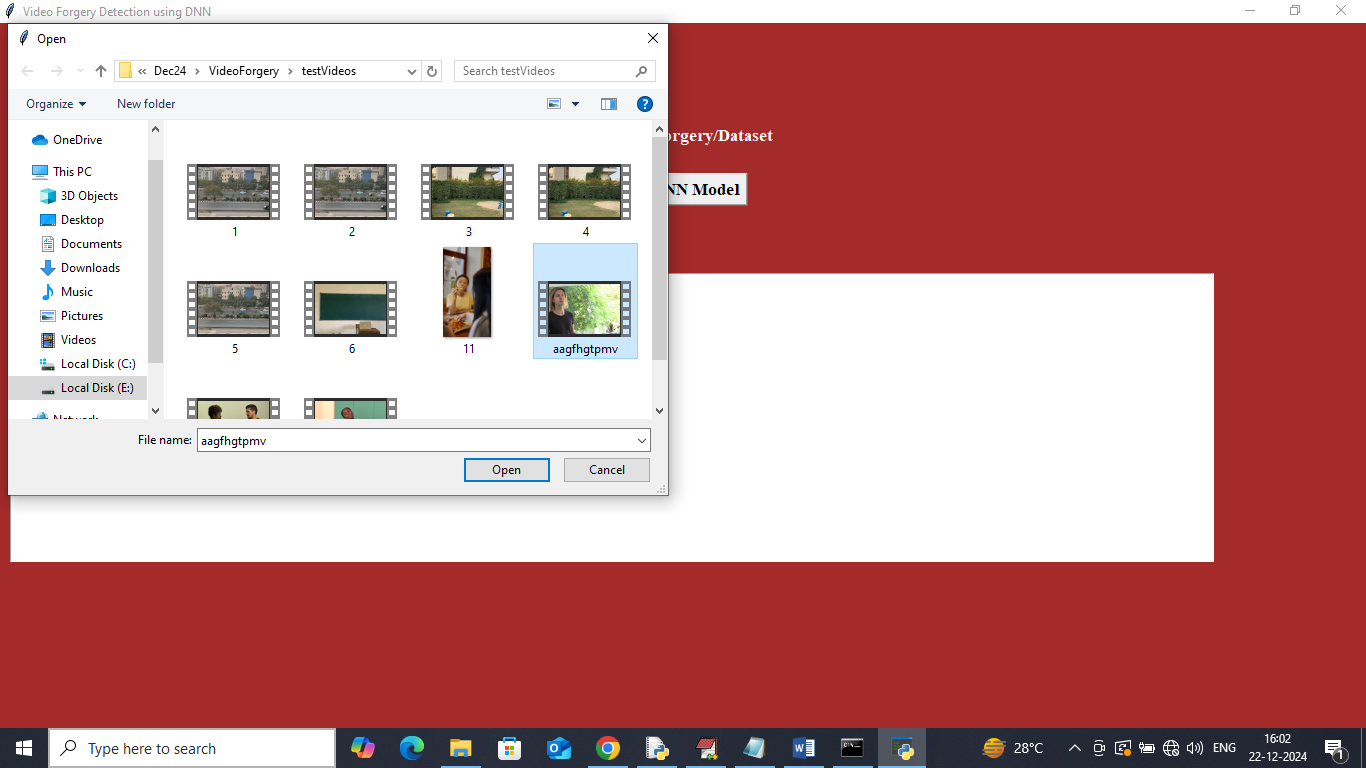
In above screen dataset shuffling and normalization processing completed and now click on ‘Split Frames Train & Test’ button to split features into train and test and then will get below output



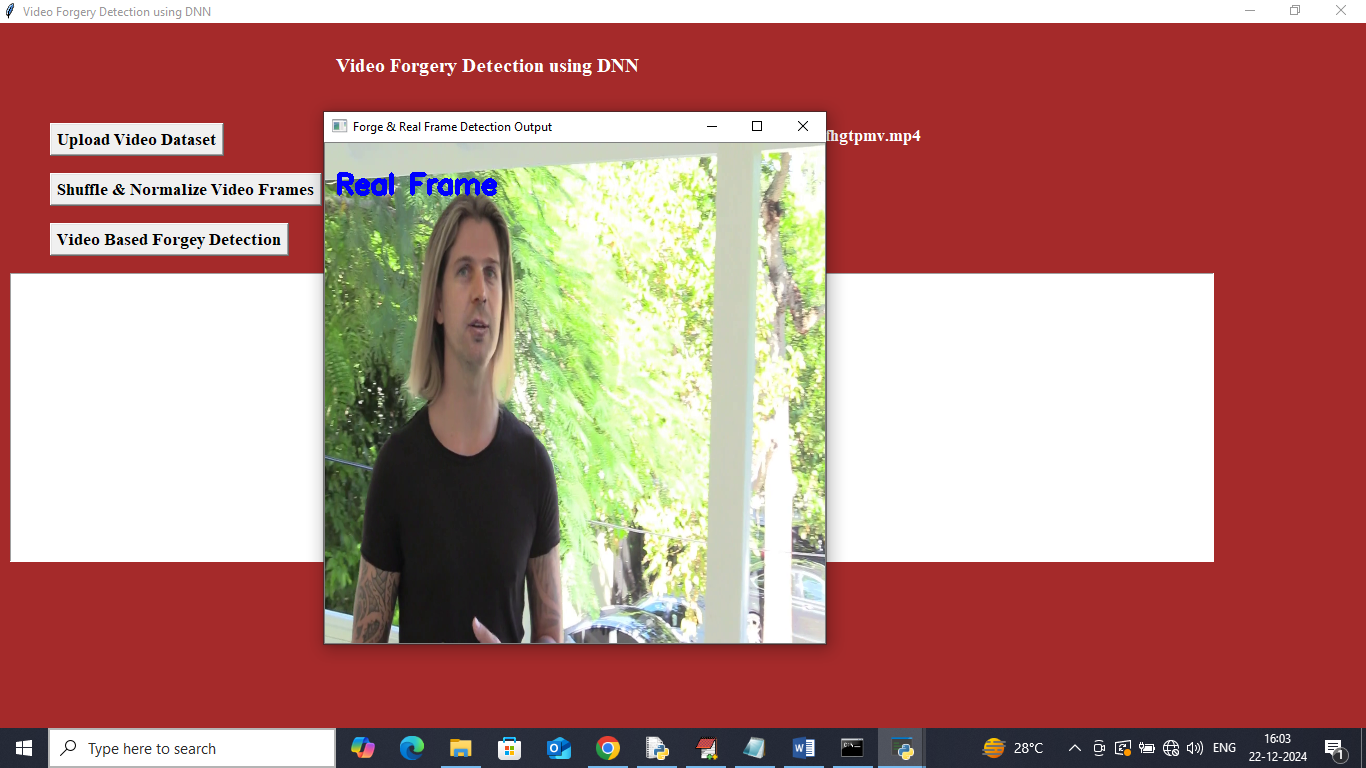
In above screen 8841 frames are using for training and 2211 frames are using for testing and now click on ‘Train DNN Model’ button to get below page



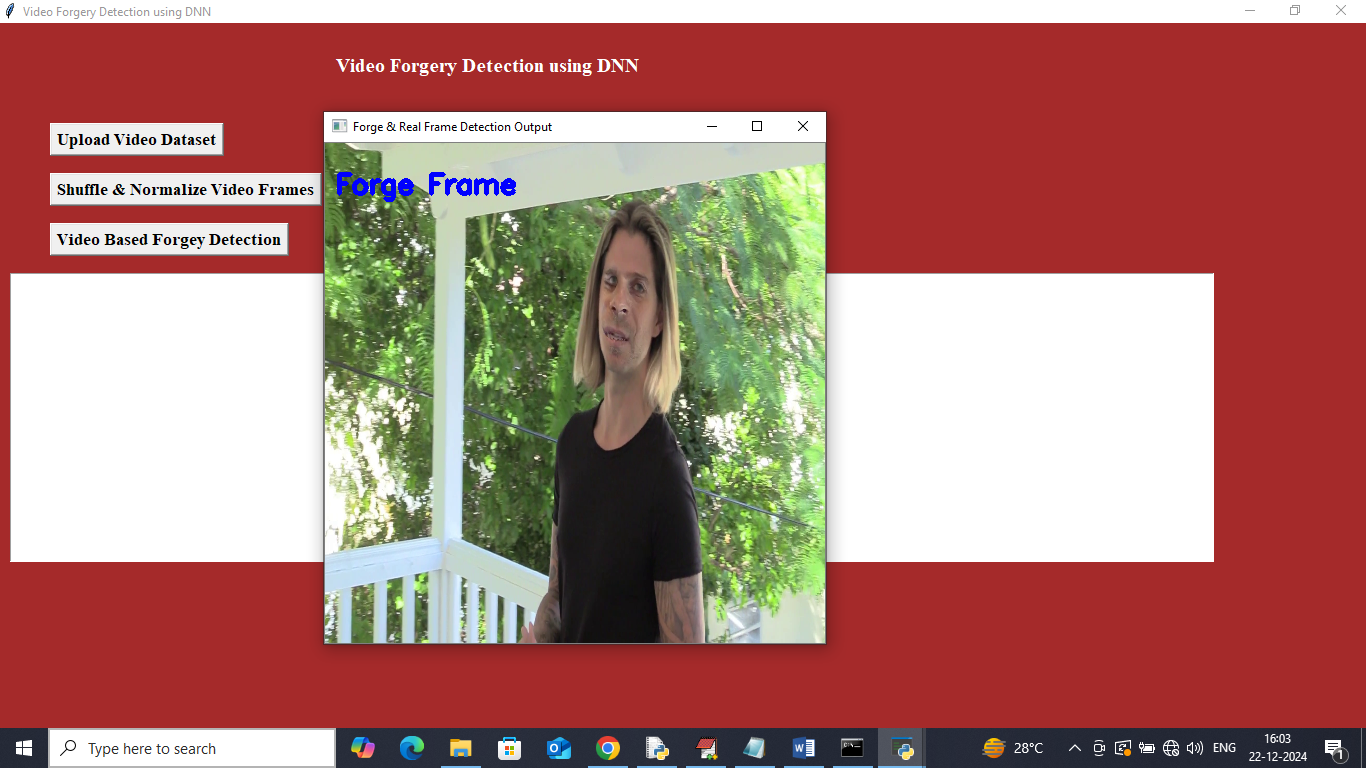
In above screen DNN model got 99% accuracy and can see other metrics like precision, recall and FSCORE. Now click on ‘Video Based Forgery Detection’ button to upload test video



In above screen selecting and uploading ‘test video’ and then click on ‘Open’ button to get below page

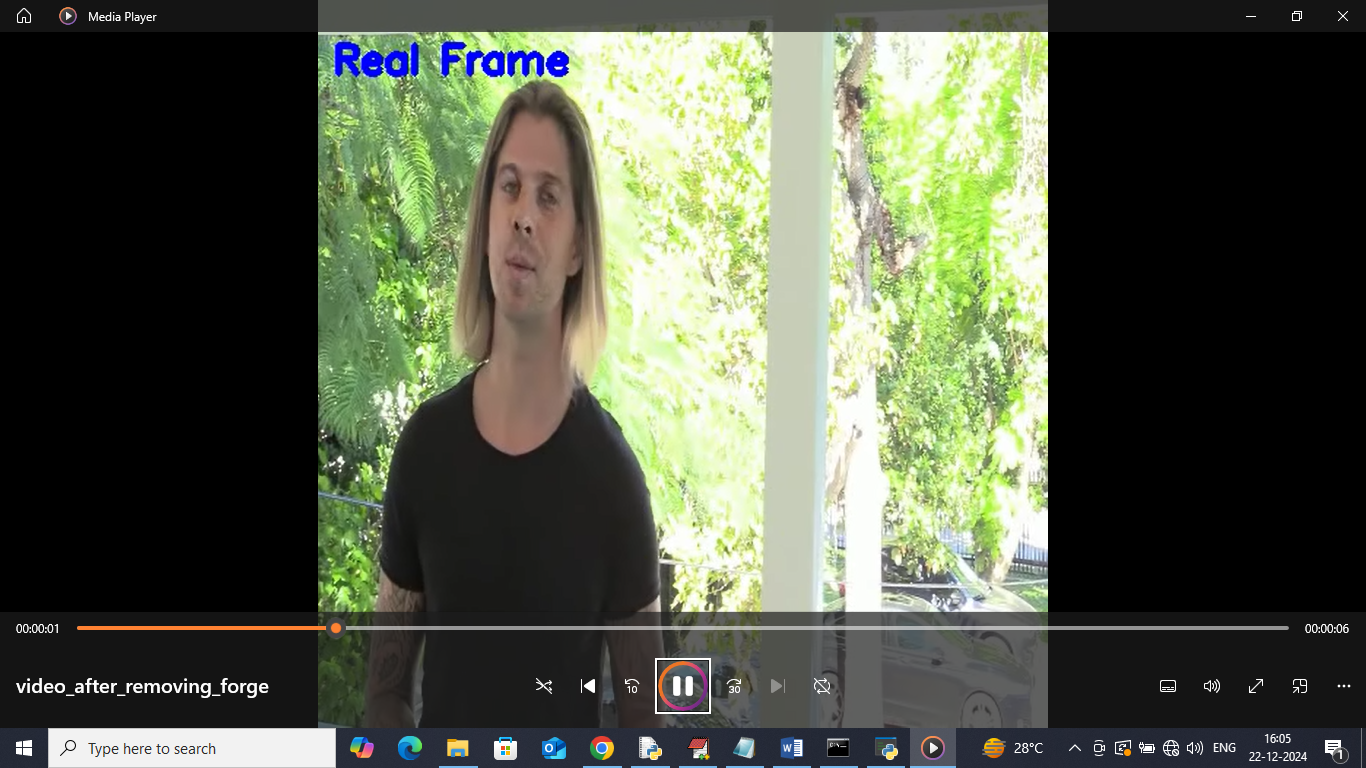


In above screen DNN detected frame as REAL



In above screen DNN detected frame as Forge. Similarly you can upload and test other videos

In below screen playing video after removing forge frames



In above screen frames which are playing in generated video containing only real frames