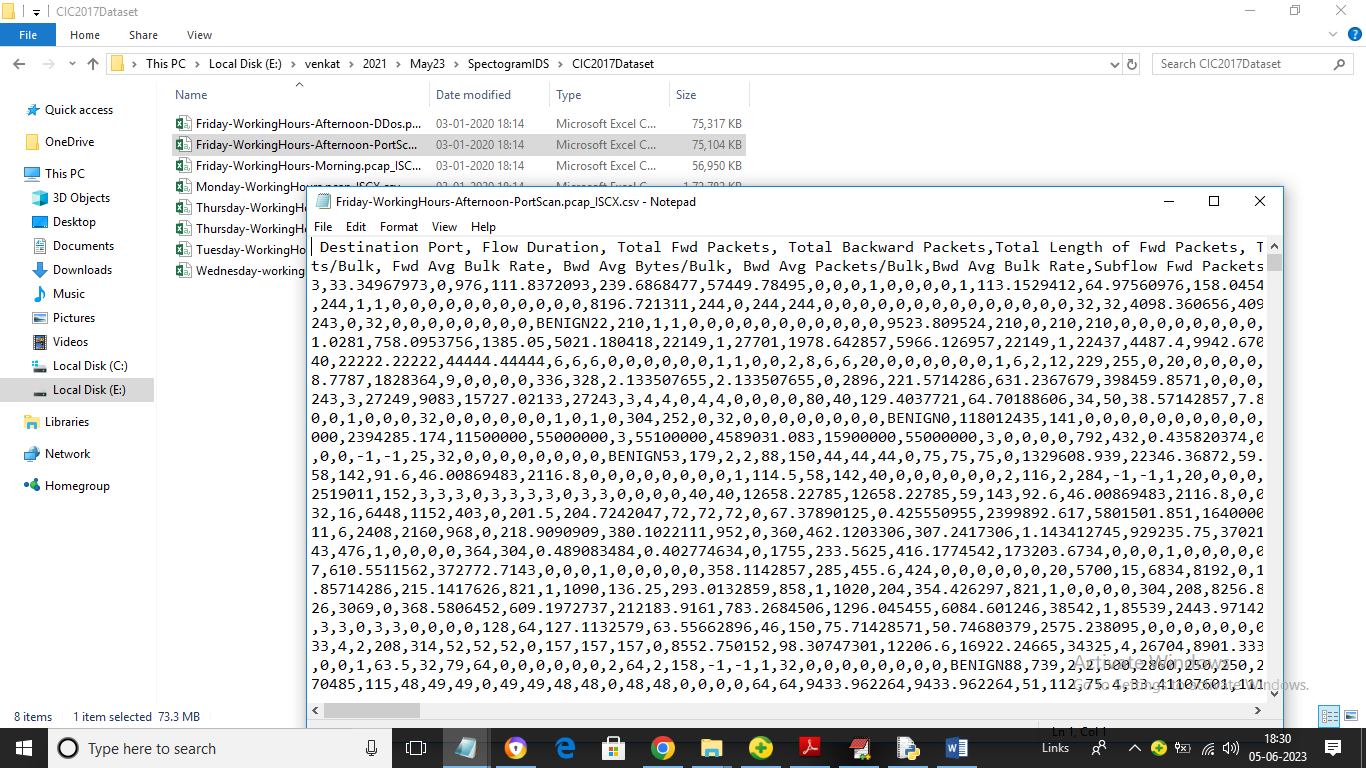
A Spectrogram Image-Based Network Anomaly Detection System Using Deep Convolutional Neural Network

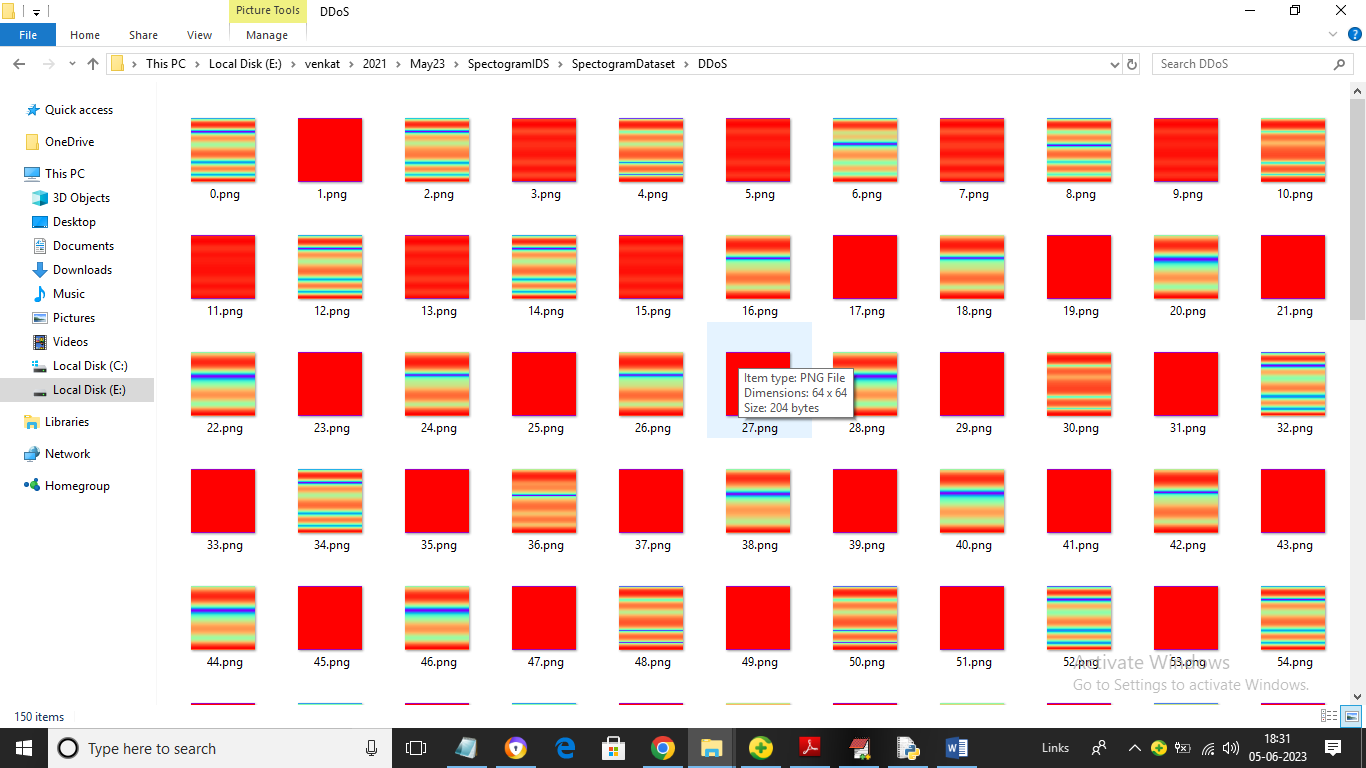
Networks are always vulnerable to attacks and there are many algorithm exists to detect and combat such attacks but still attackers may find way to intrude into networks and then perform malicious operations. To enhance detection rate author of this paper employing Deep CNN algorithm which utilizes Spectrogram images generated using the short-time Fourier transform from the Network Intrusion dataset called CIC-IDS2017. Propose algorithm is called as Spectrogram Deep CNN (SDCNN). Signals generated from Spectrogram FFT technique contains accurate information about network packets and this CNN will get trained on such packet features. This features helps CNN in detecting malicious packets accurately. Author has modified CNN algorithm with extra layers called MAXPOOLING2D, RELU Function and Dense which help CNN in collecting optimized features from the dataset. Propose SDCNN is designed as a Fully Connected CNN algorithm.

To train CNN we have collected CID\_IDS dataset and then convert all those dataset values into Spectrogram images and this images get trained with various deep learning algorithms called GRU, LSTM, CNN1D and propose SDCNN and in all algorithms propose SDCNN is giving better accuracy. Each algorithm performance is evaluated in terms of accuracy, precision, recall, FSCORE and Confusion Matrix.

To train above algorithms we have used below dataset CIC dataset



In above dataset we have destination port, source port and many other features and all the above dataset values will be converted to spectrogram images like below screen



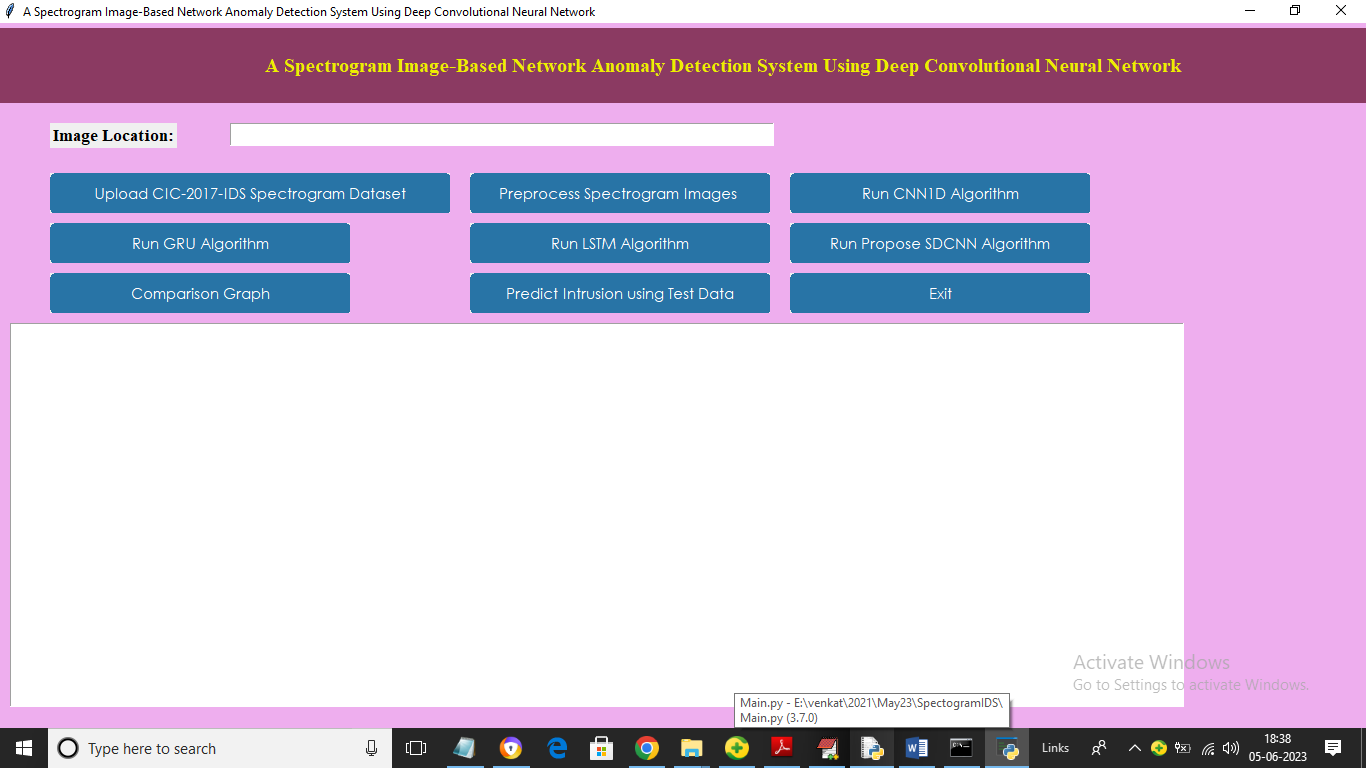
So by using above spectrogram images we will train and test all algorithms performance.

To implement this project we have designed following modules

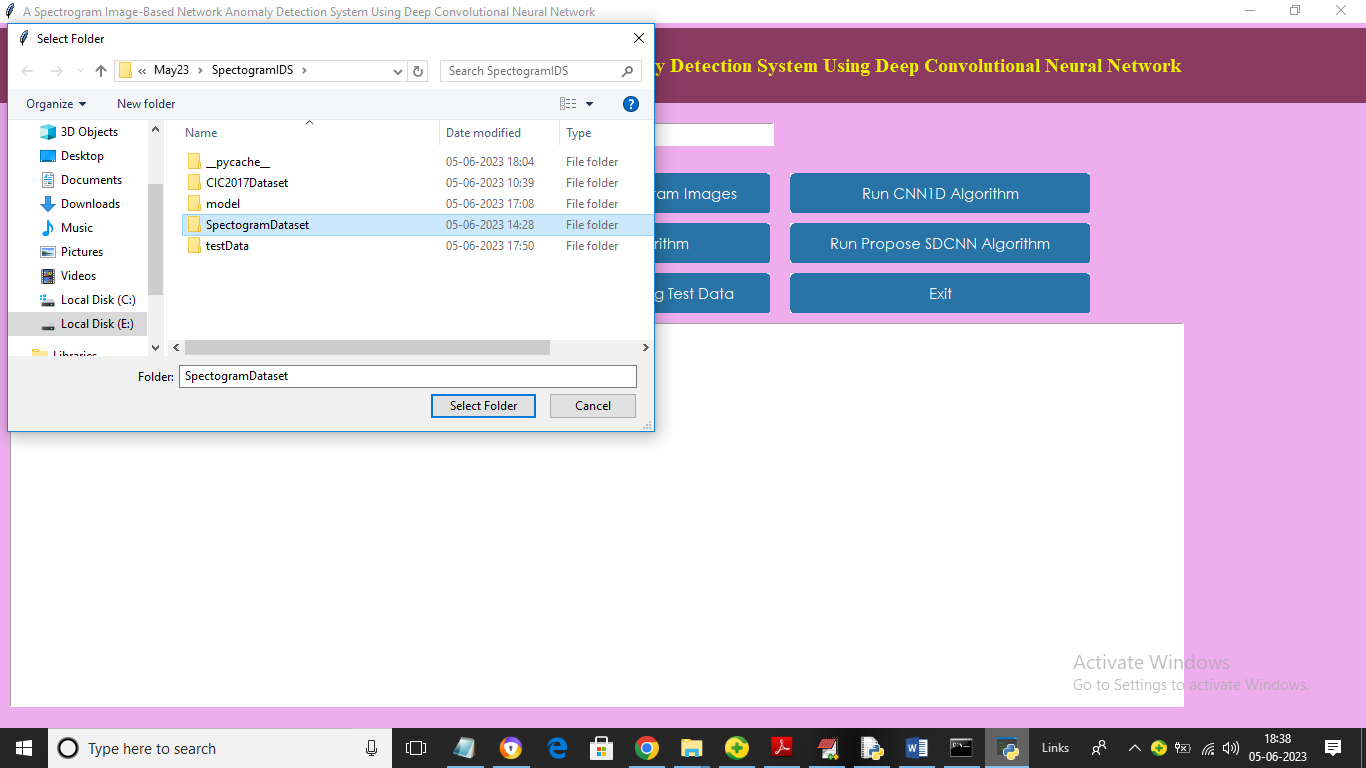
1. Upload CIC-2017-IDS Spectrogram Dataset: using this module we will upload spectrogram dataset images to application
2. Preprocess Spectrogram Images: using this module we will read all spectrogram images and then resize, normalized, shuffle and then split all images into train and test where application using 80% dataset images for training and 20% for testing
3. Run CNN1D Algorithm: 80% training images will be input to this module to train CNN1D model and this model will be applied on 20% test data to calculate prediction accuracy
4. Run GRU Algorithm: 80% training images will be input to this module to train GRU model and this model will be applied on 20% test data to calculate prediction accuracy
5. Run LSTM Algorithm: 80% training images will be input to this module to train LSTM model and this model will be applied on 20% test data to calculate prediction accuracy
6. Run Propose SDCNN Algorithm: 80% training images will be input to this module to train Propose SDCNN model and this model will be applied on 20% test data to calculate prediction accuracy
7. Comparison Graph: using this module we will plot comparison graph between all algorithms
8. Predict Intrusion using Test Data: using this module we will upload CIC network packets data and then application will convert packets into Spectrogram images and then predict type of attack

SCREEN SHOTS

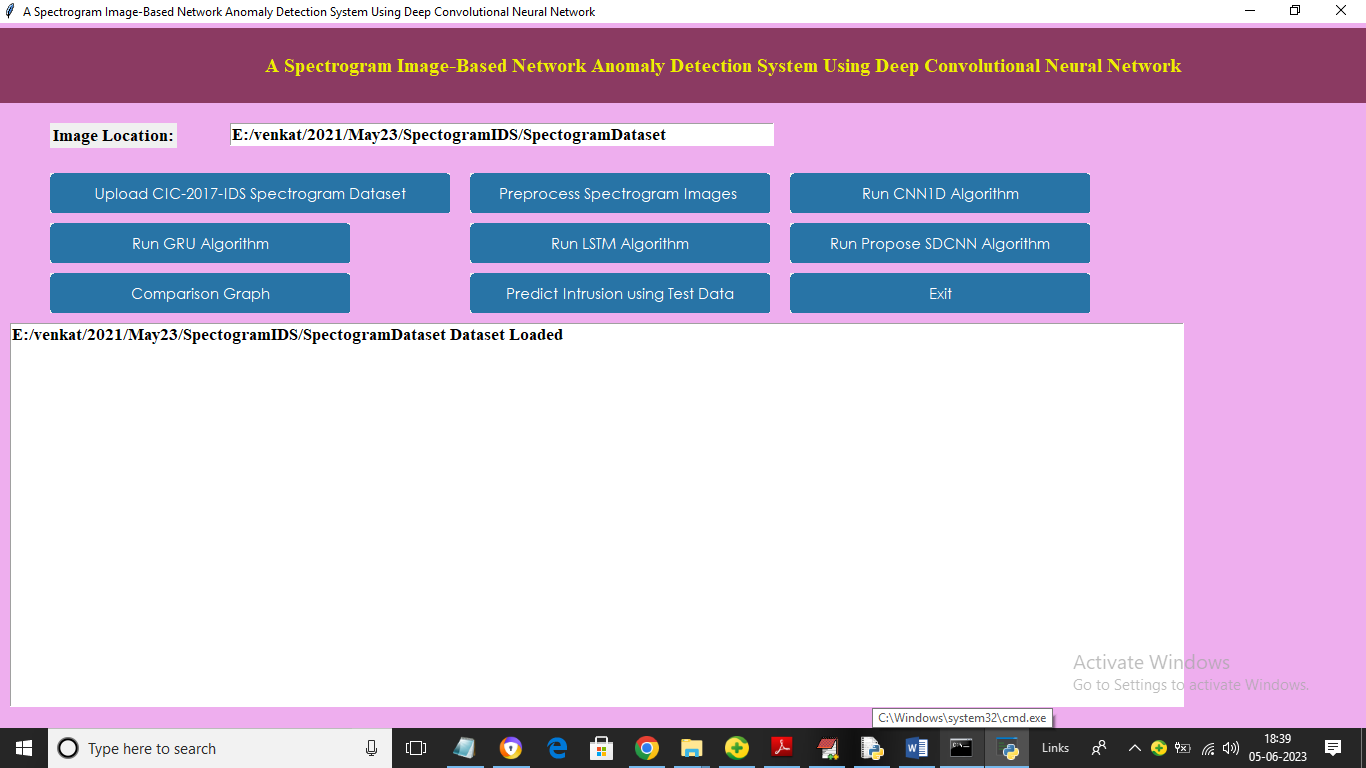
To run project double click on ‘run.bat’ file to get below screen



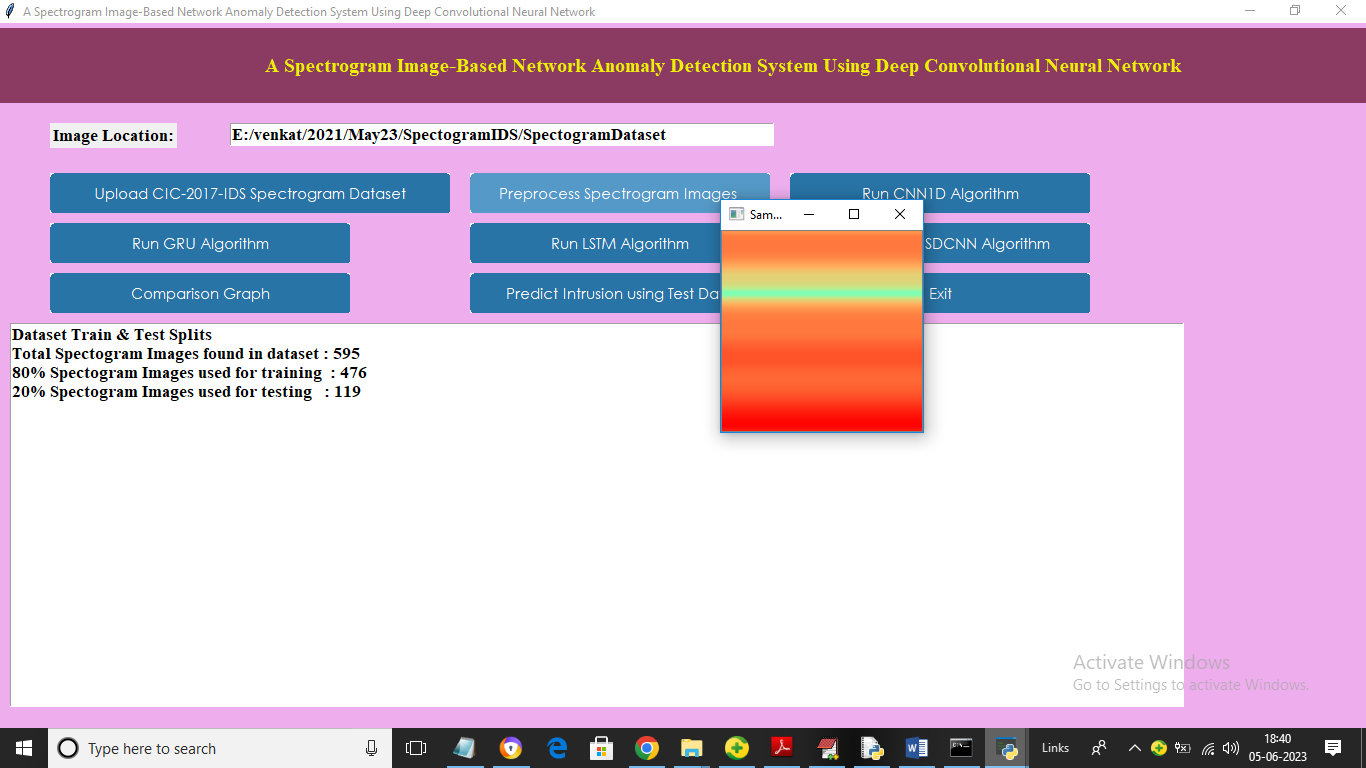
In above screen click on ‘Upload CIC-2017-IDS Spectrogram Dataset’ button to upload dataset and get below output



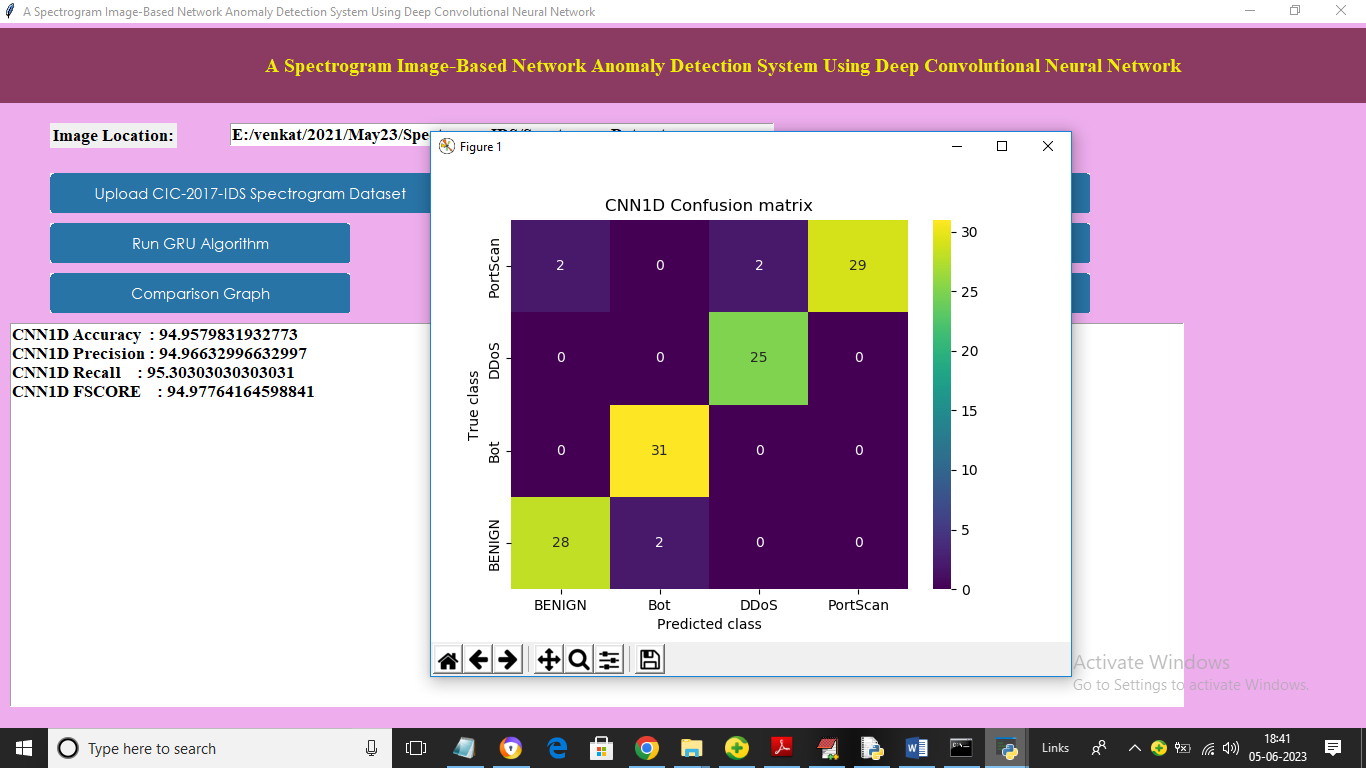
In above screen selecting and uploading Spectrogram dataset and then click on ‘Select Folder’ button to load dataset and get below output.



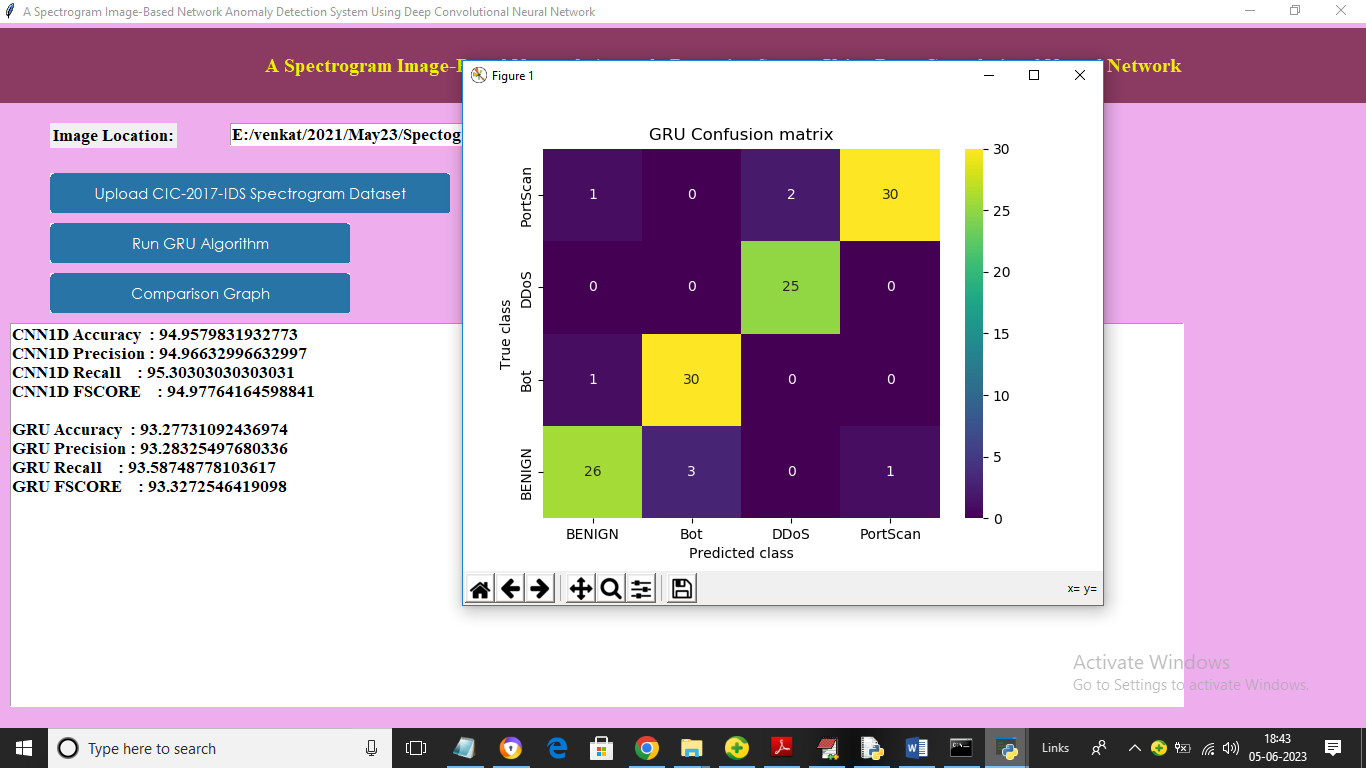
In above screen dataset loaded and now click on ‘Preprocess Spectrogram Images’ button to process images and then split into train and test part



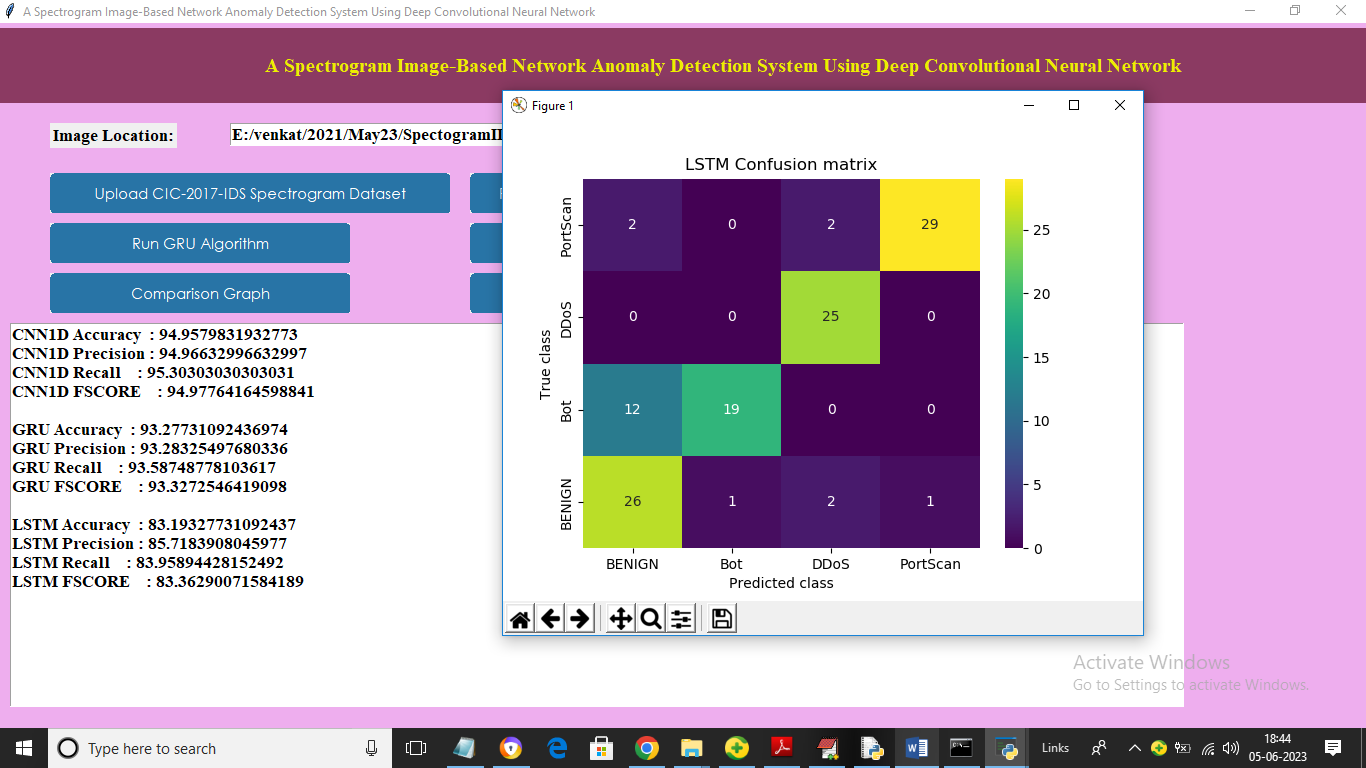
In above screen we can see total spectrogram images found in dataset and then can see 80 and 20 train and test data size and then we can see sample Spectrogram image generated from dataset values and now close above image and then click on ‘Run CNN1D Algorithm’ button to train CNN1D and get below output



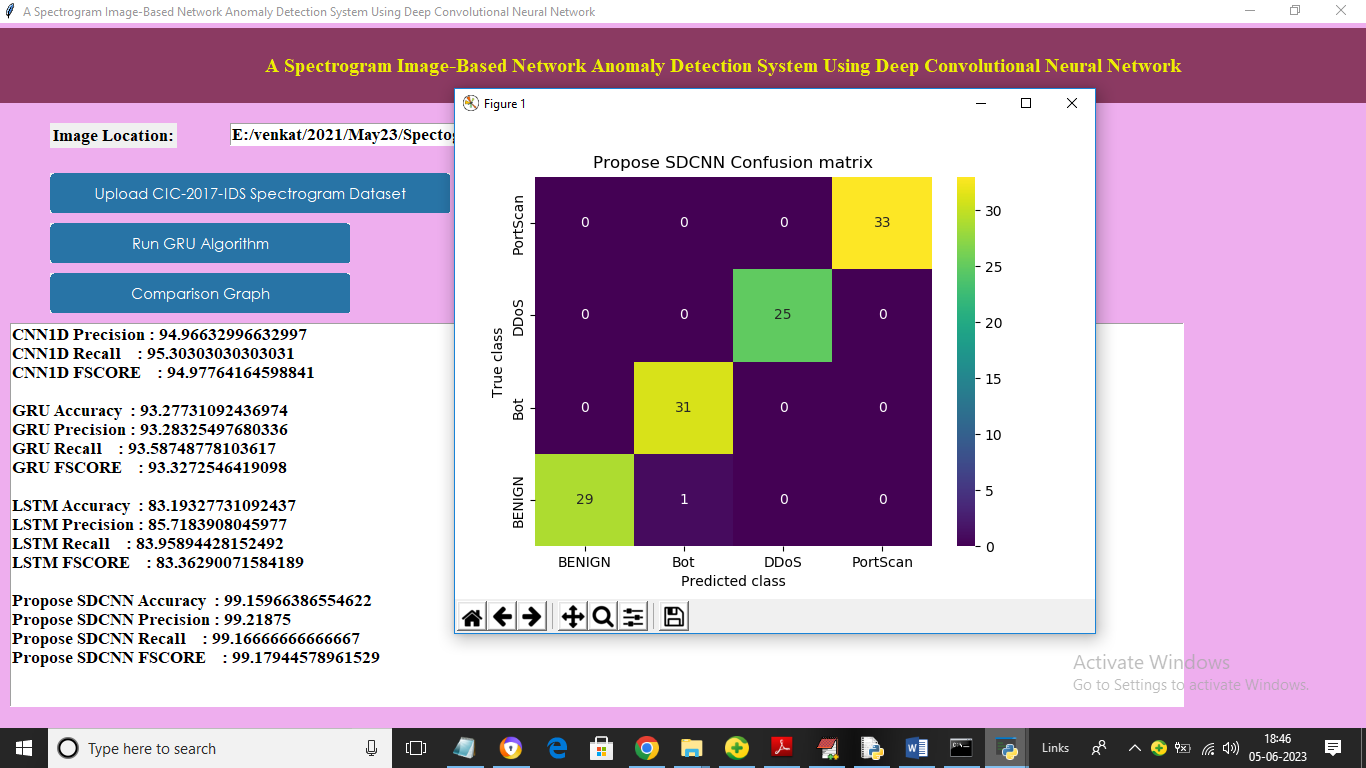
In above screen CNN1D training completed and we got its accuracy as 94% and we can see other metrics also and in confusion matrix graph x-axis represents Predicted Labels and y-axis represents True Labels and all different colour boxes in diagnol represents correct prediction count and all blue boxes represents incorrect prediction count which are very few and now close above graph and then click on ‘Run GRU Algorithm’ button to train GRU and get below output



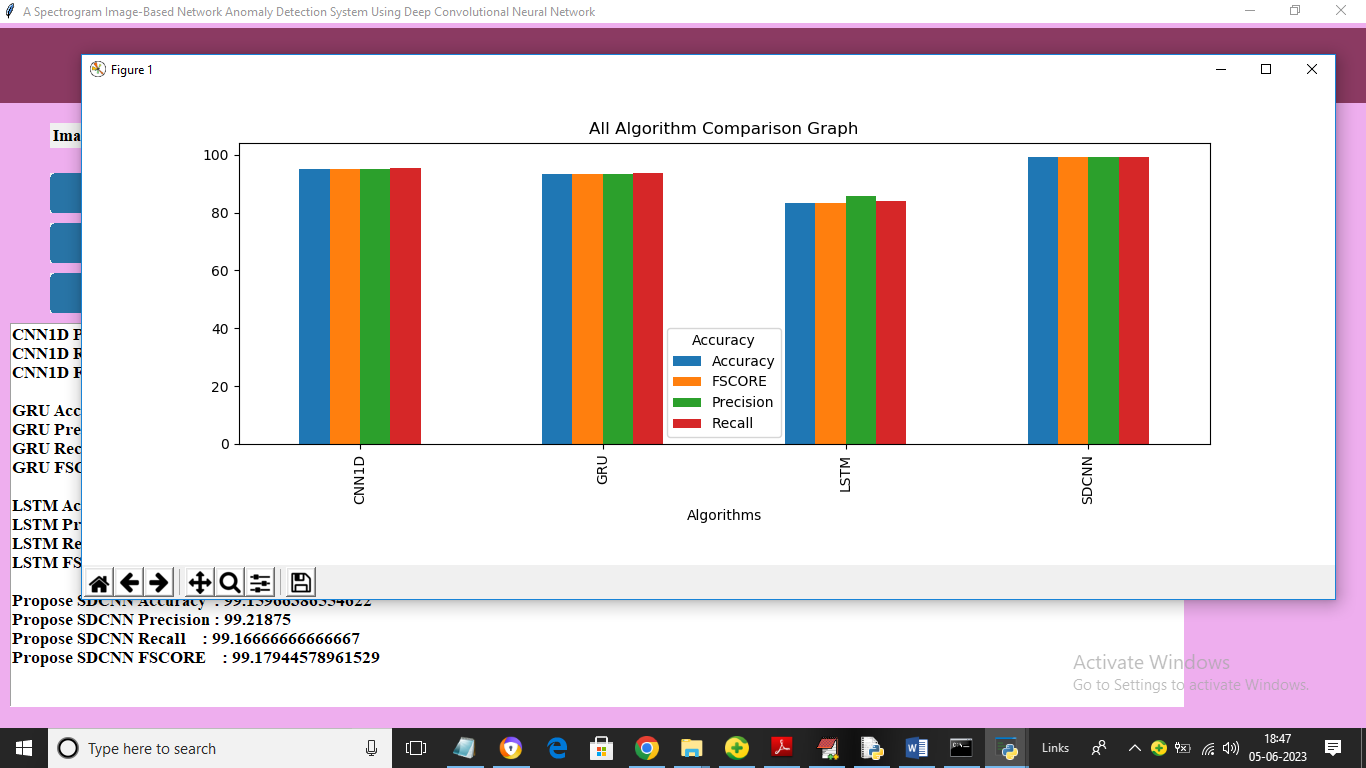
In above screen GRU got 93% accuracy and now click on ‘Run LSTM Algorithm’ button to train LSTM and get below output



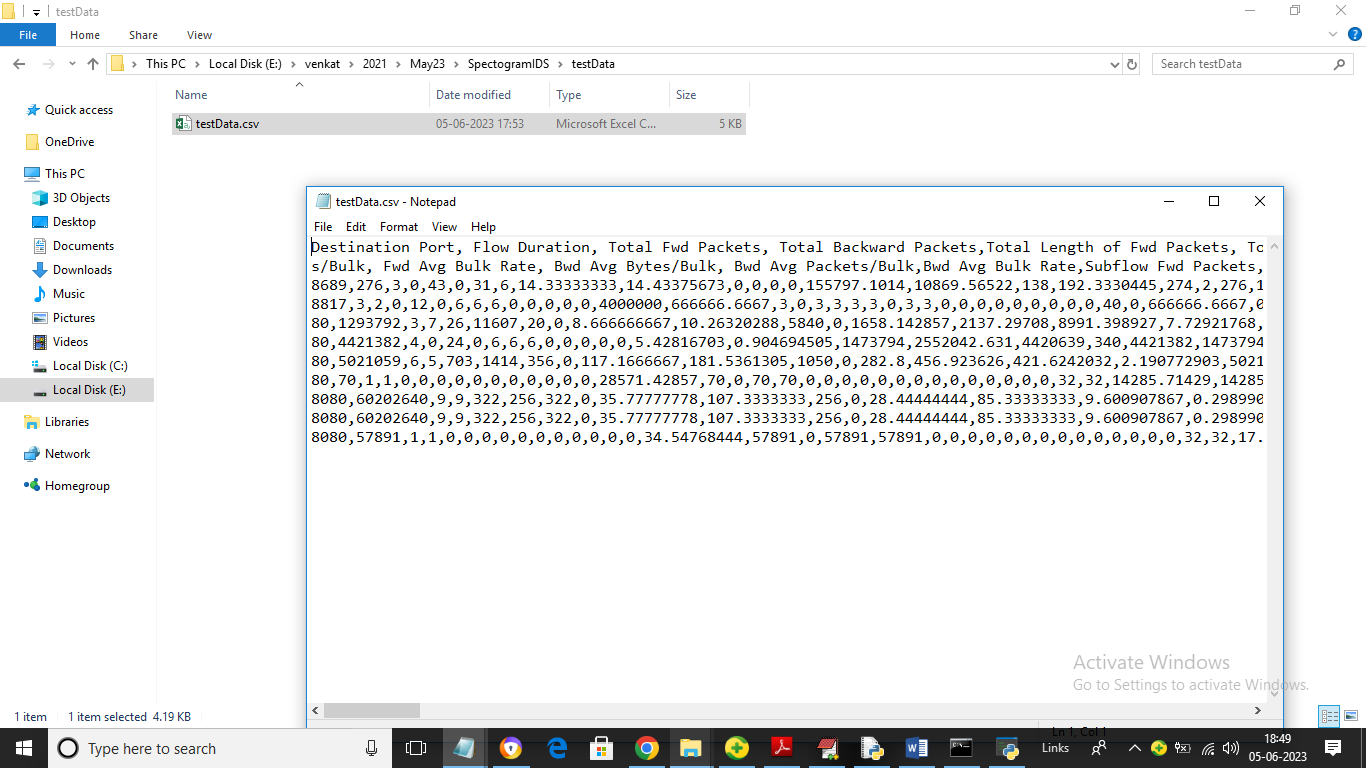
In above screen LSTM got 83% accuracy and now click on ‘Run Propose SDCNN Algorithm’ button to train SDCNN and get below output



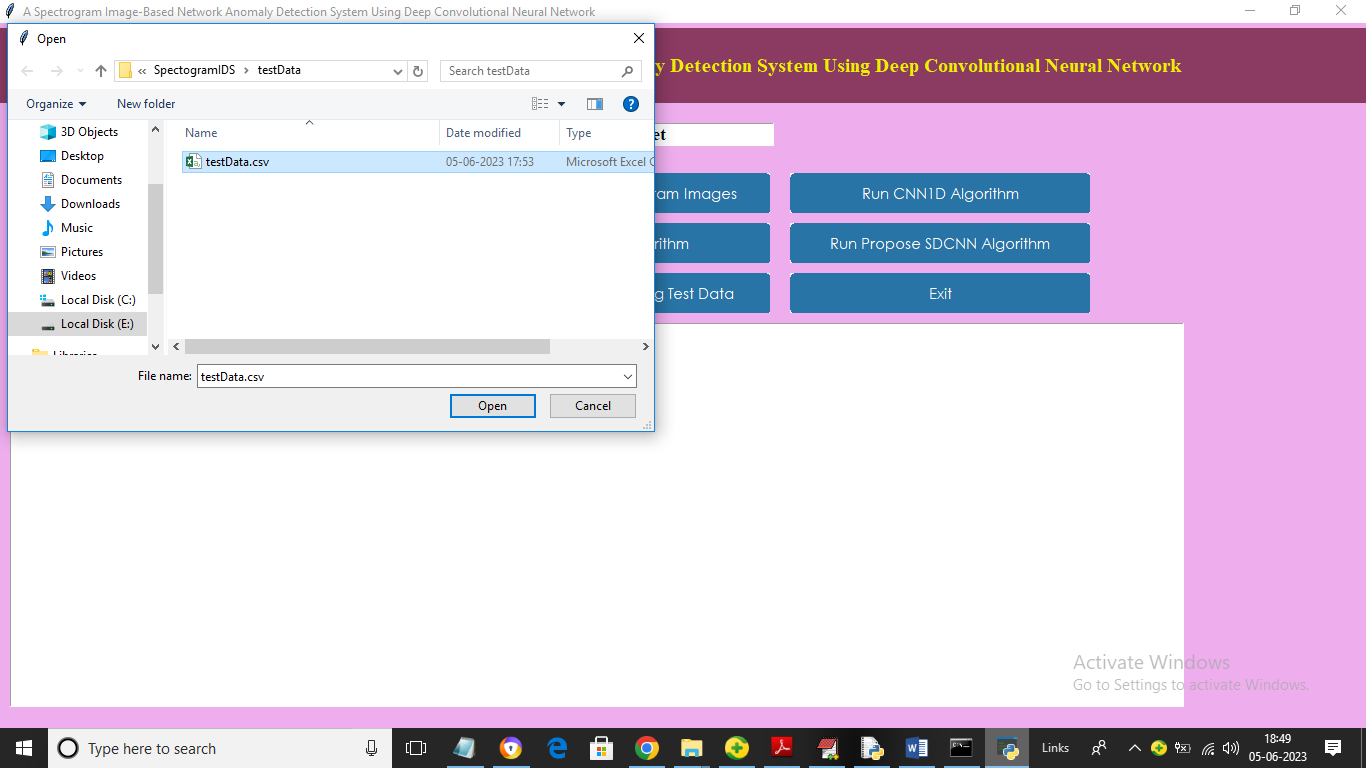
In above screen with Propose SDCNN we got 99% accuracy and we can see other metrics and confusion matrix graph and now click on ‘Comparison Graph’ button to get below graph



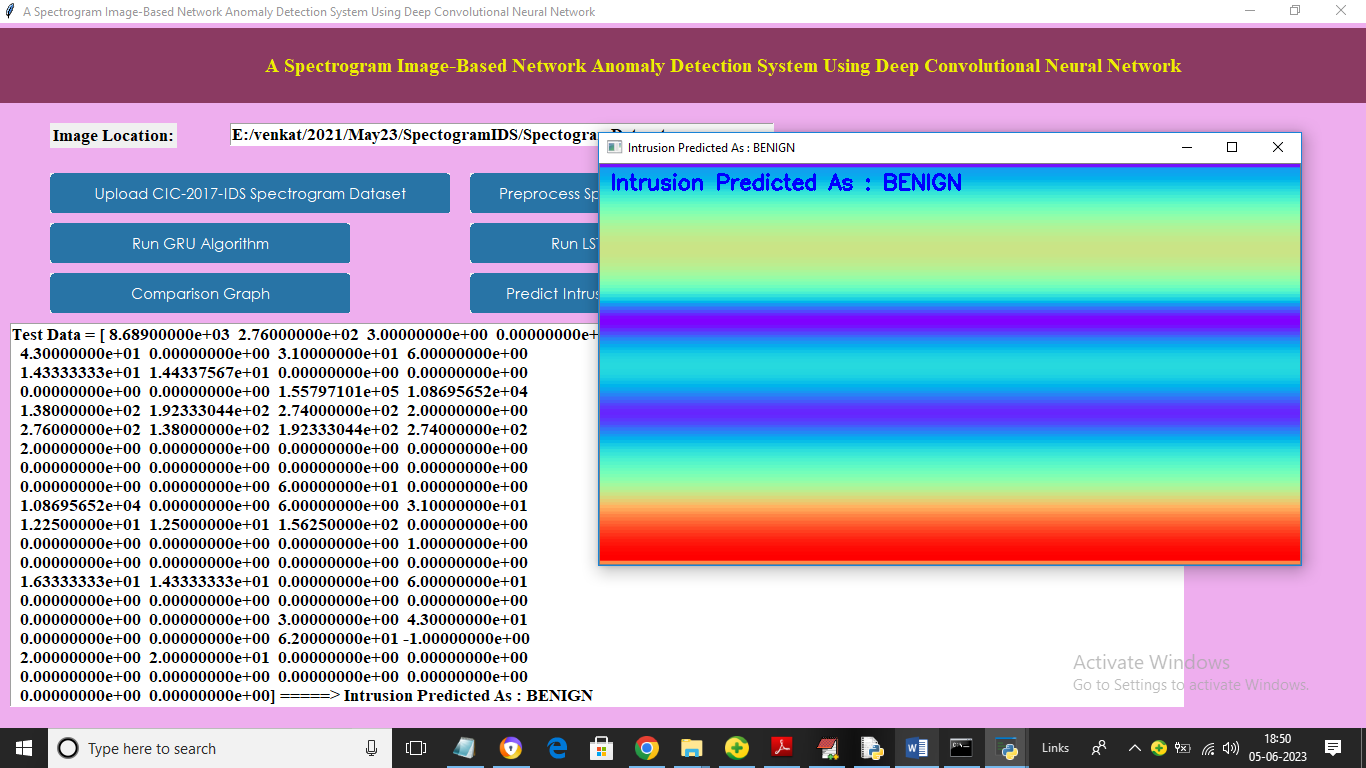
In above graph x-axis represents algorithm names and y-axis represents accuracy and other metrics in different colour bars and in all algorithms propose SDCNN has got high performance and now click on ‘Predict Intrusion using Test Data’ button to upload test data and then predict intrusion and in below screen we are showing test packet data



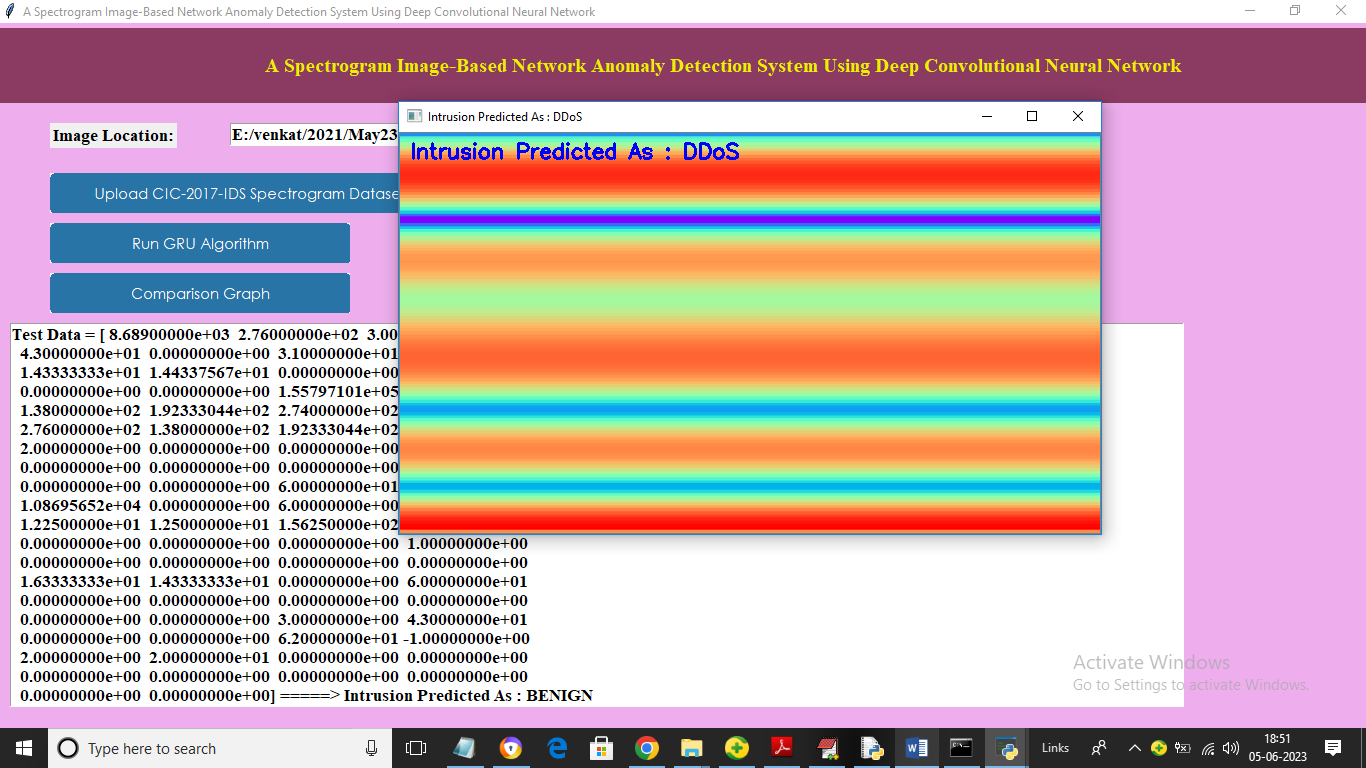
So by using above test data we will generated spectrogram image and then predict intrusion



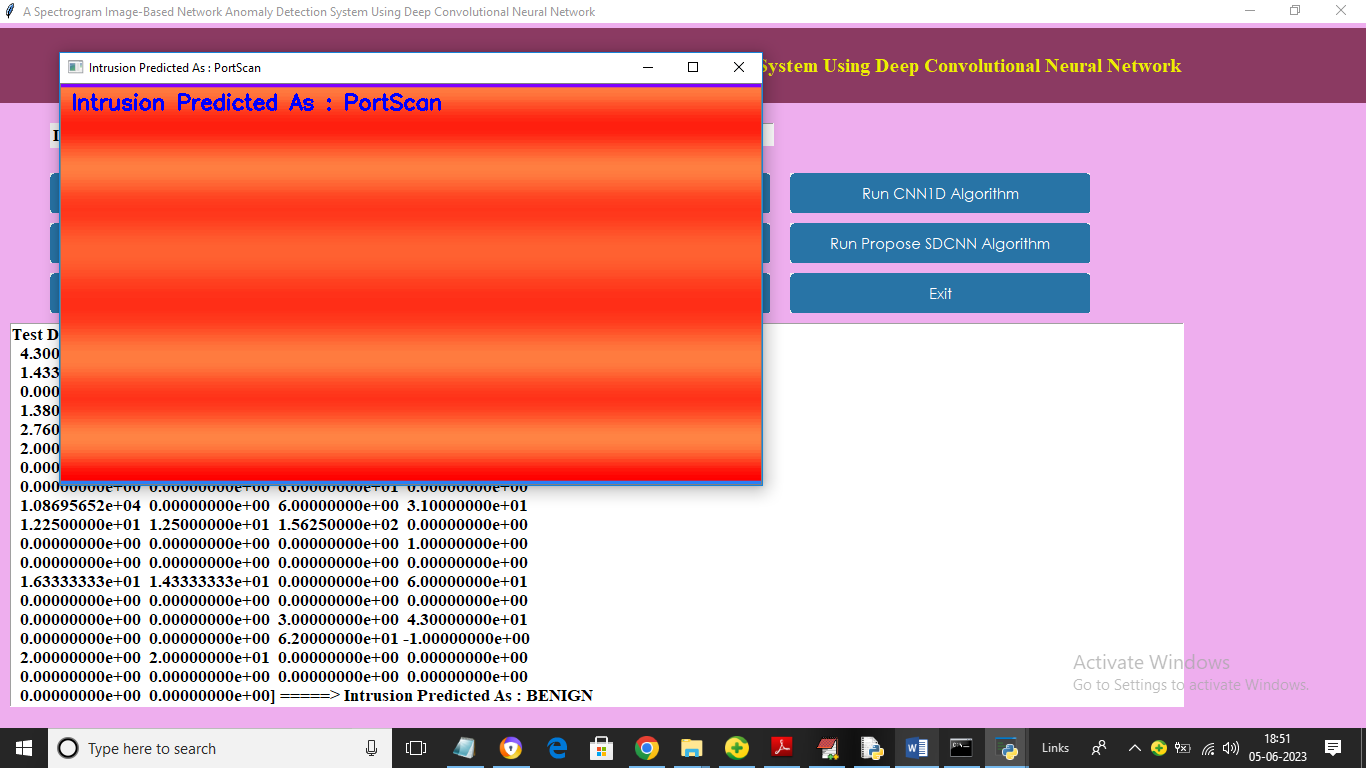
In above screen selecting and uploading testData.csv file and then click on ‘Open’ button to load test data and get below prediction



In above screen we can see test data values in text area and then we can see generated spectrogram image and then in blue colour text we can see predicted output as ‘benign’ and now close above graph to get another prediction



In above screen DDOS attack predicted



In above screen “PortScan” attack detected. Similarly by following above screens you can run and test application output