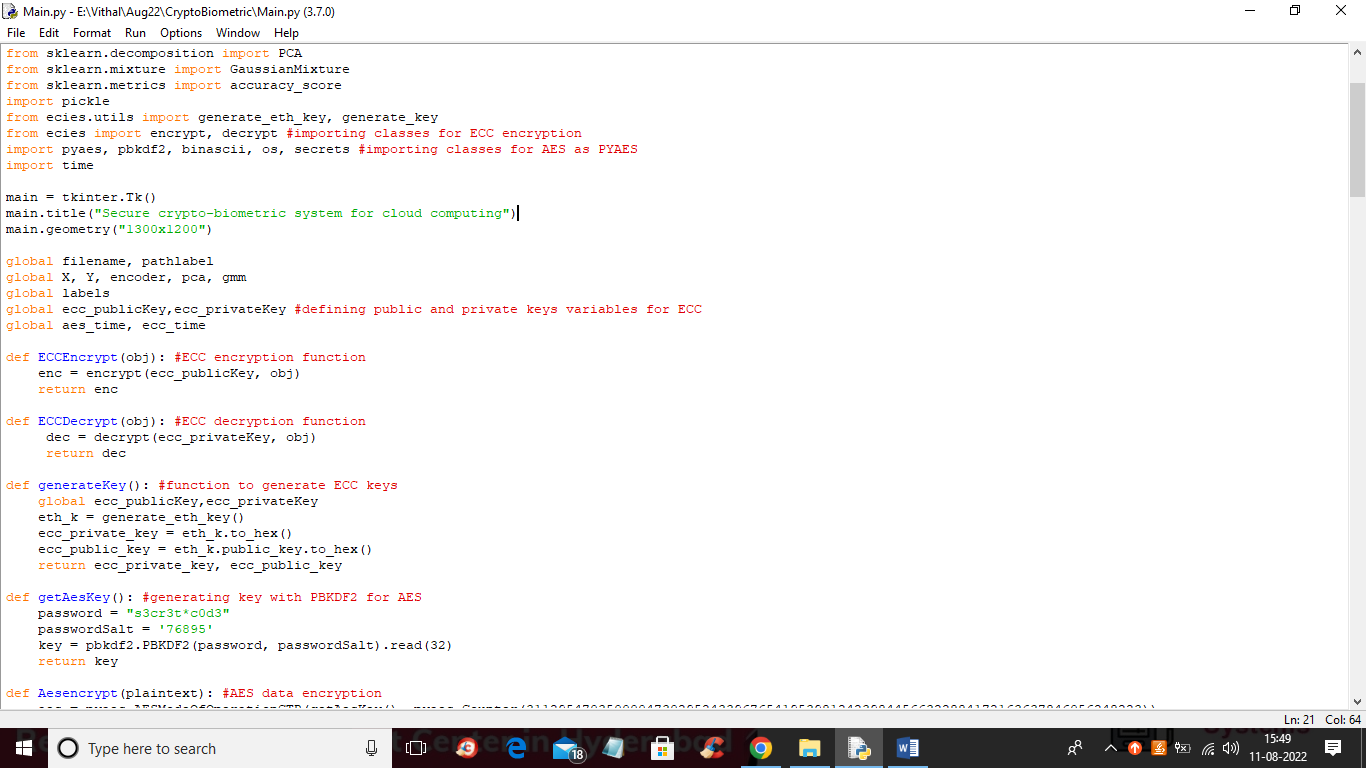
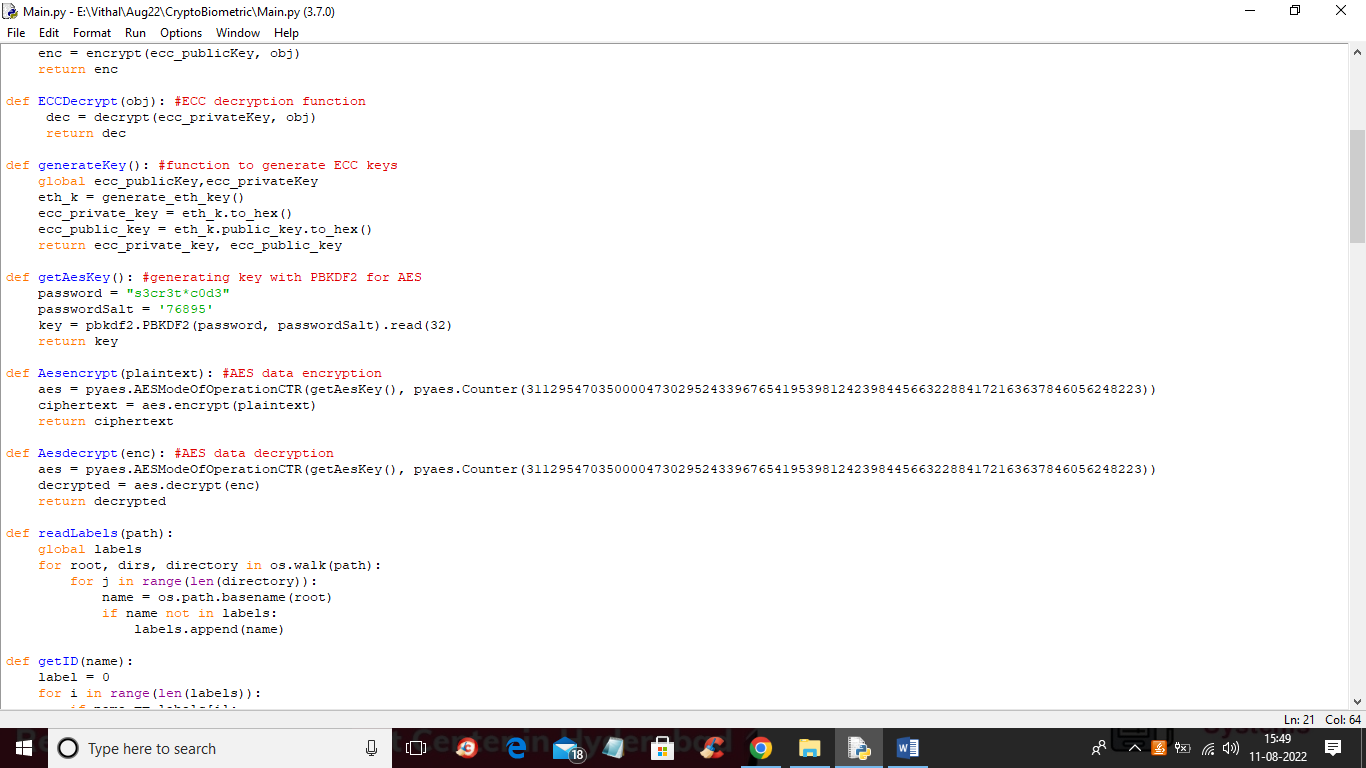
Secure crypto-biometric system for cloud computing

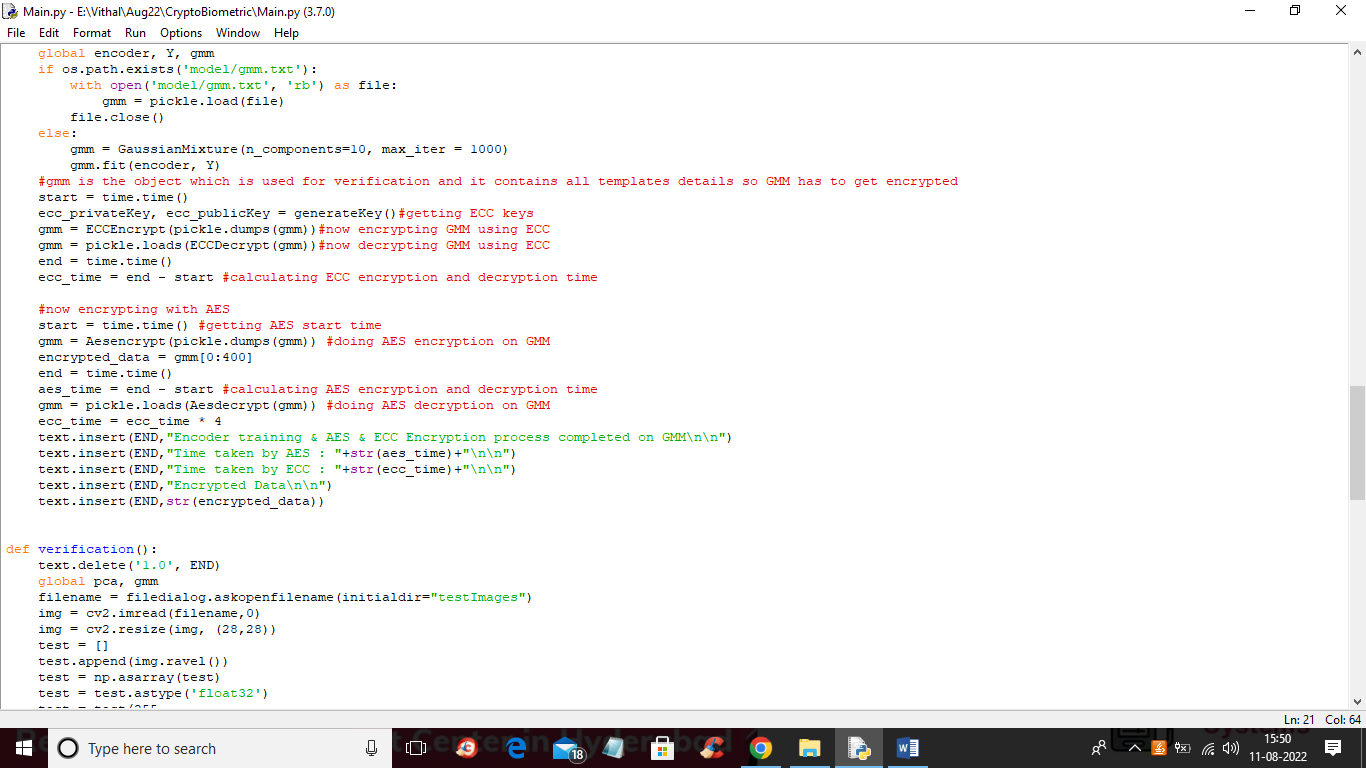
In this paper author is providing concept to secure biometric templates stored at cloud servers and GMM object is responsible for verification and stored at cloud so GMM object must be secured so we are encrypting this object by using two different algorithms called ECC (Elliptic Curve Cryptograph) and AES and in both algorithms ECC is running faster. We are evaluating both algorithms performance in terms of execution or running times.

In below screen we are showing code of both algorithms and you read red colour comments to know about implementation





In below screen you can see code of encrypting GMM object to provide template security

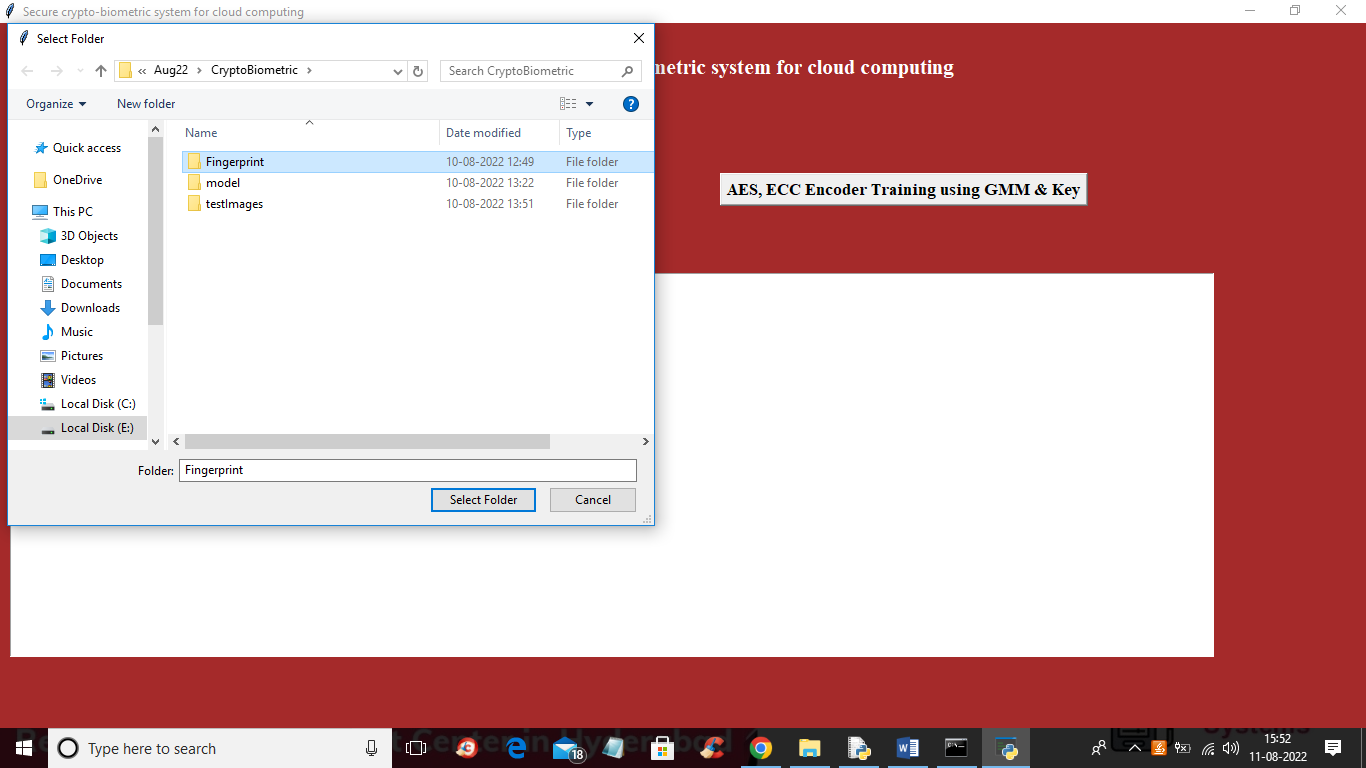


SCREEN SHOTS

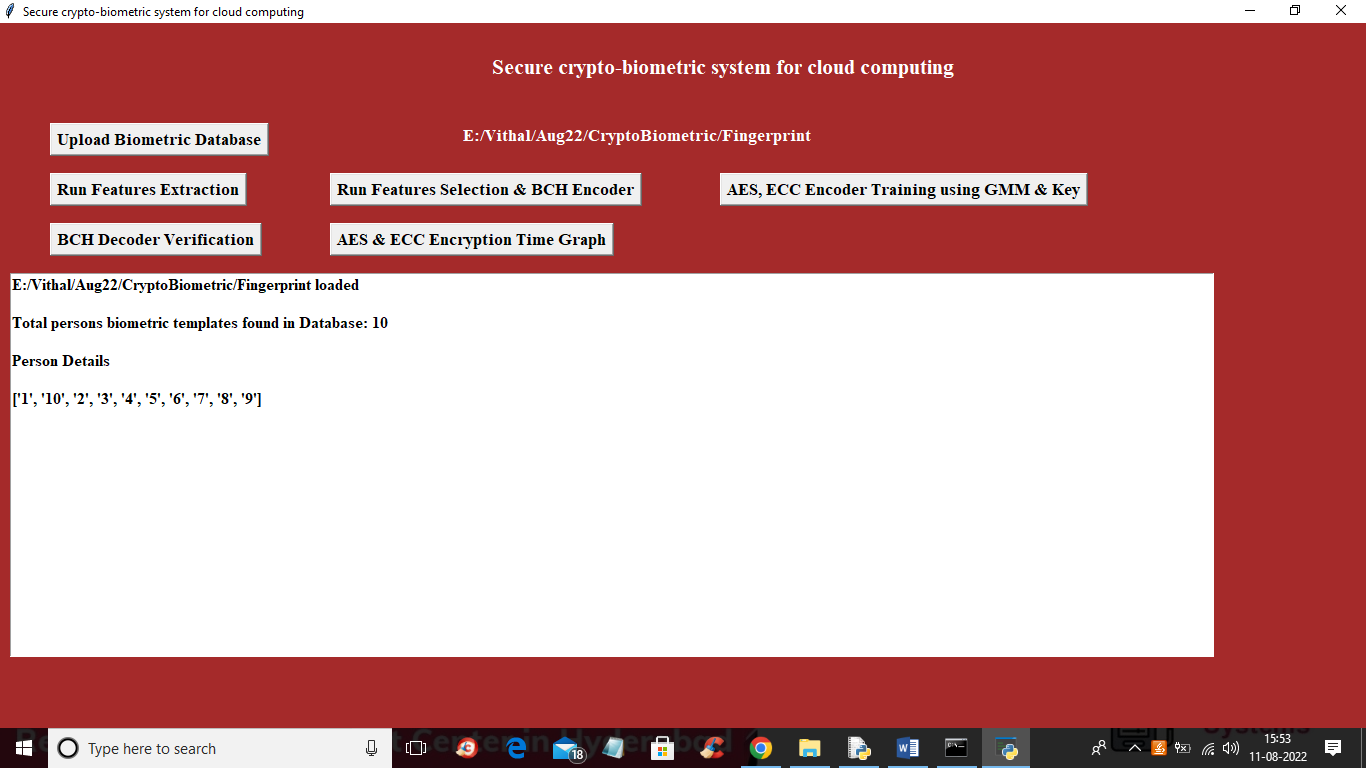
To run project double click on ‘run.bat’ file to get below screen



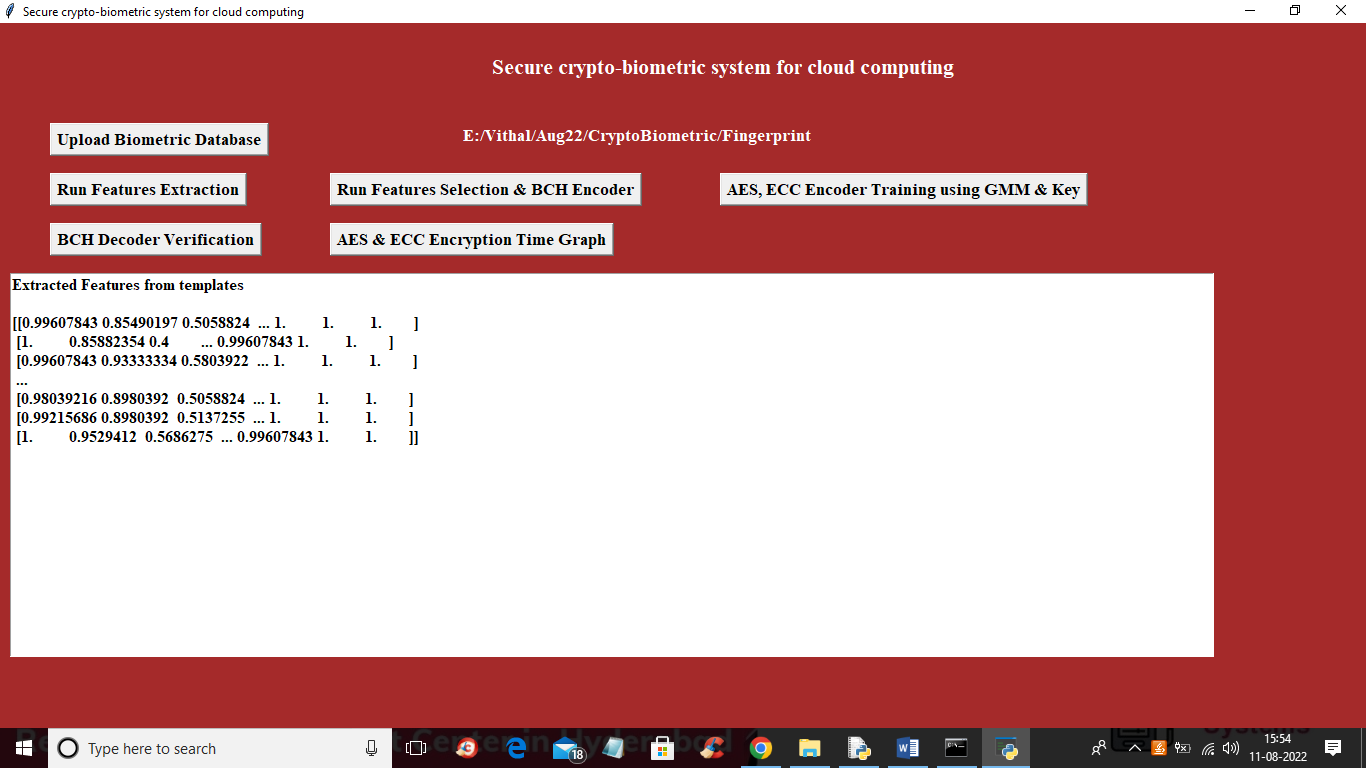
In above screen click on ‘Upload Biometric Database’ button to upload biometric data and get below output



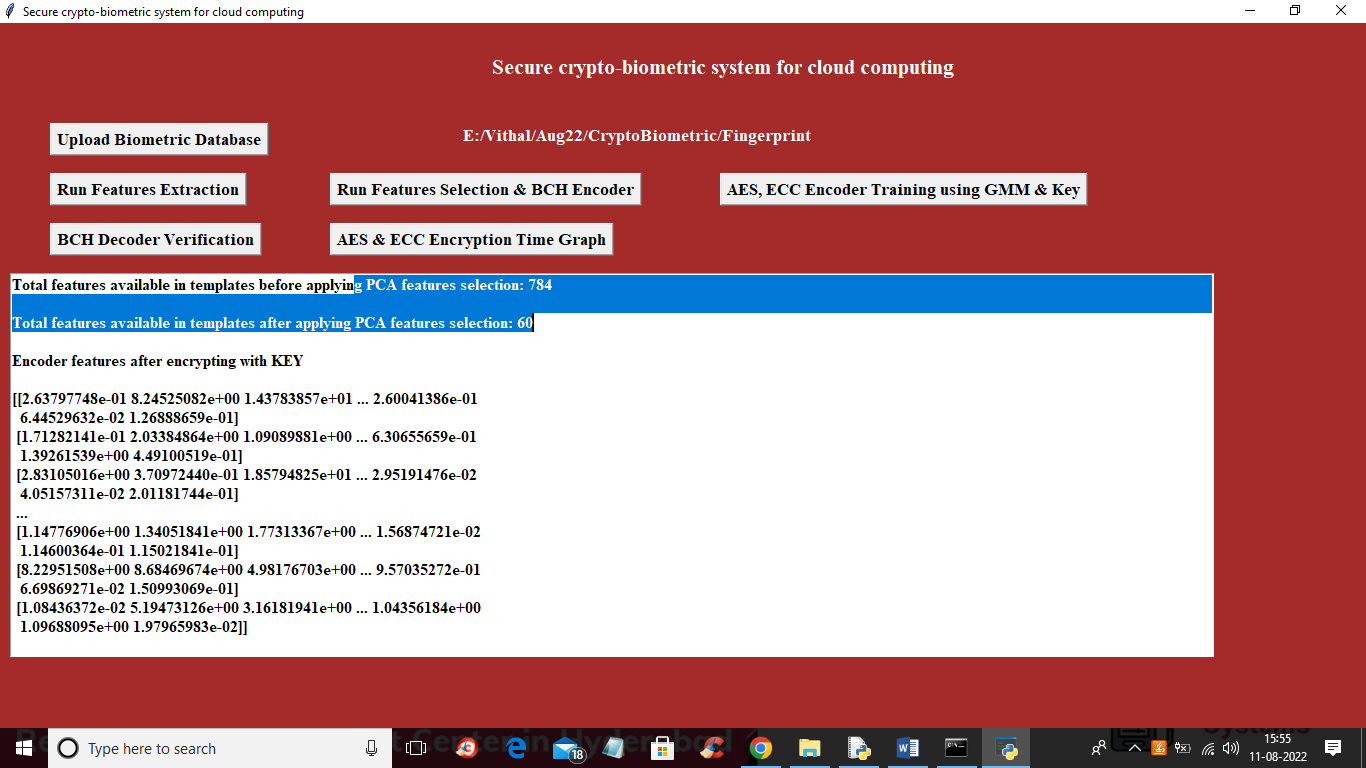
In above screen selecting and uploading Finger biometric images dataset and then click on ‘Select Folder’ button to load database and get below output



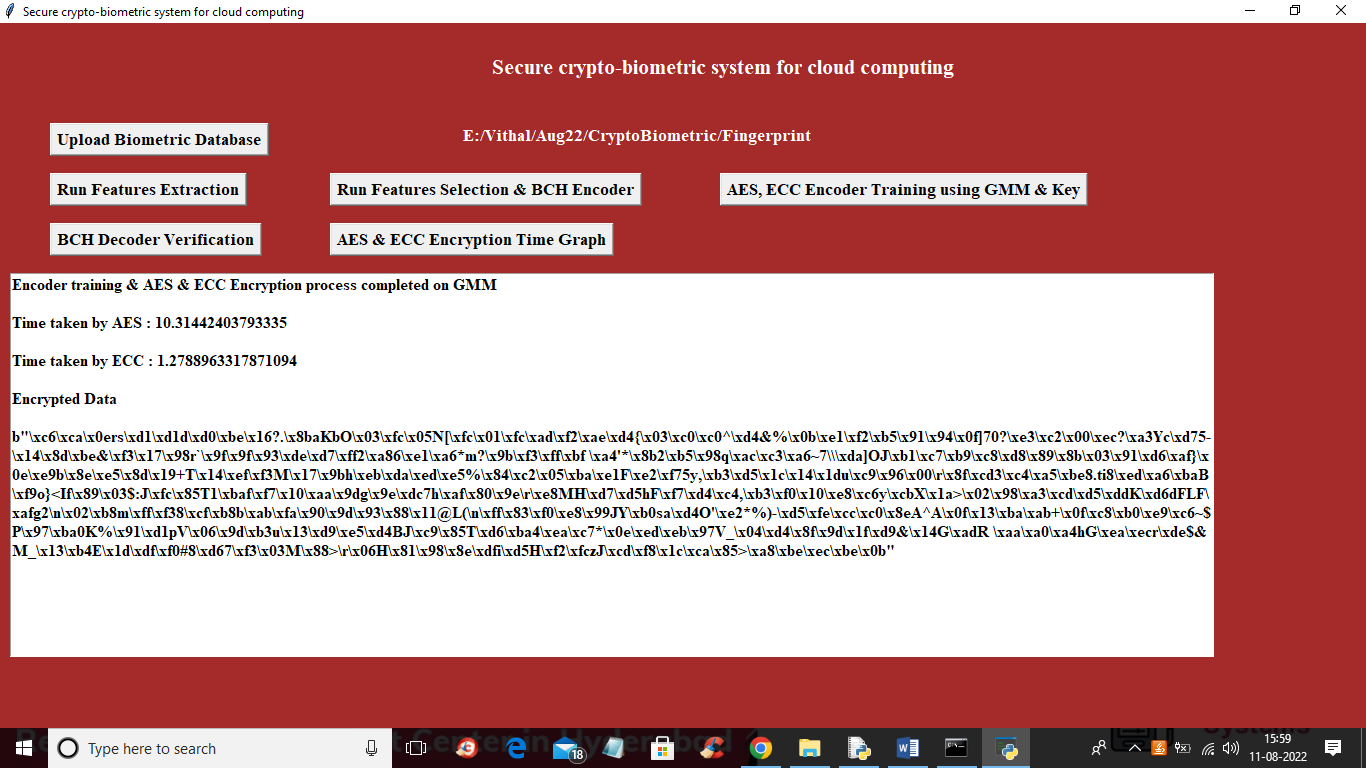
In above screen we can see database loaded and we can see it contains biometric template of 10 different persons and now click on ‘Run Features Extraction’ button o extract features from templates and get below output



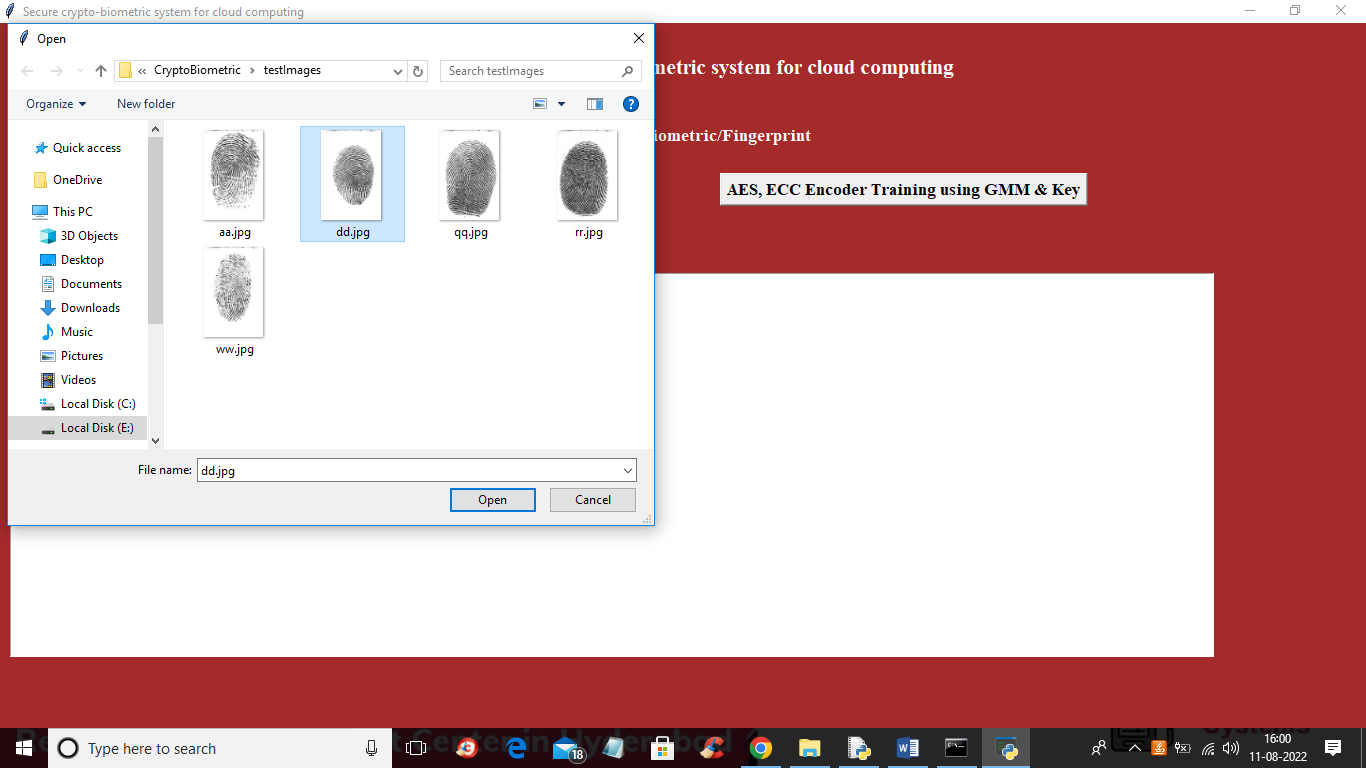
In above screen features extracted and now click on ‘Run Features Selection & BCH Encoder’ button to select features from extracted features



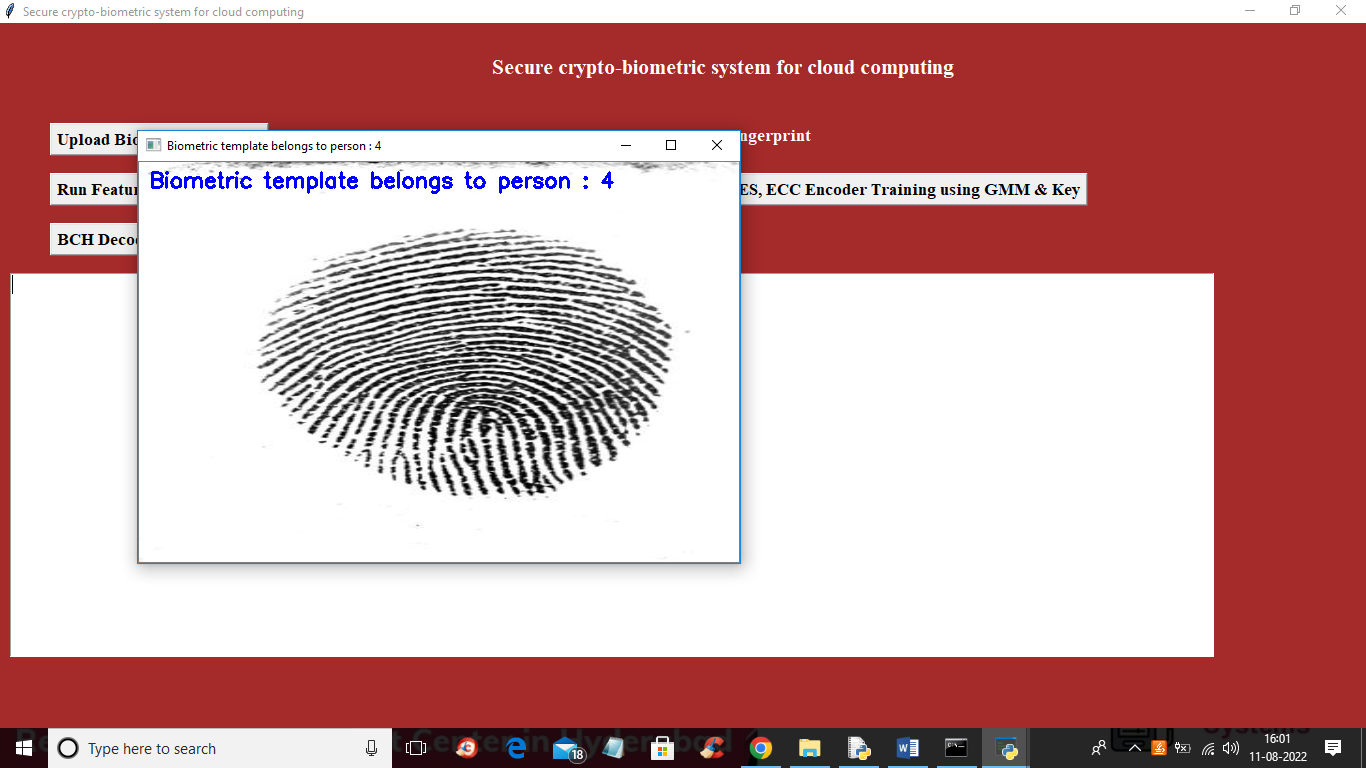
In above screen before applying PCA features selection algorithm, we have 784 features and then PCA select 60 important features out of it and now click on ‘AES, ECC Encoder Training using GMM & Key’ button to encode features and then train GMM and this GMM will get encrypted using ECC and AES algorithms and then will get below output



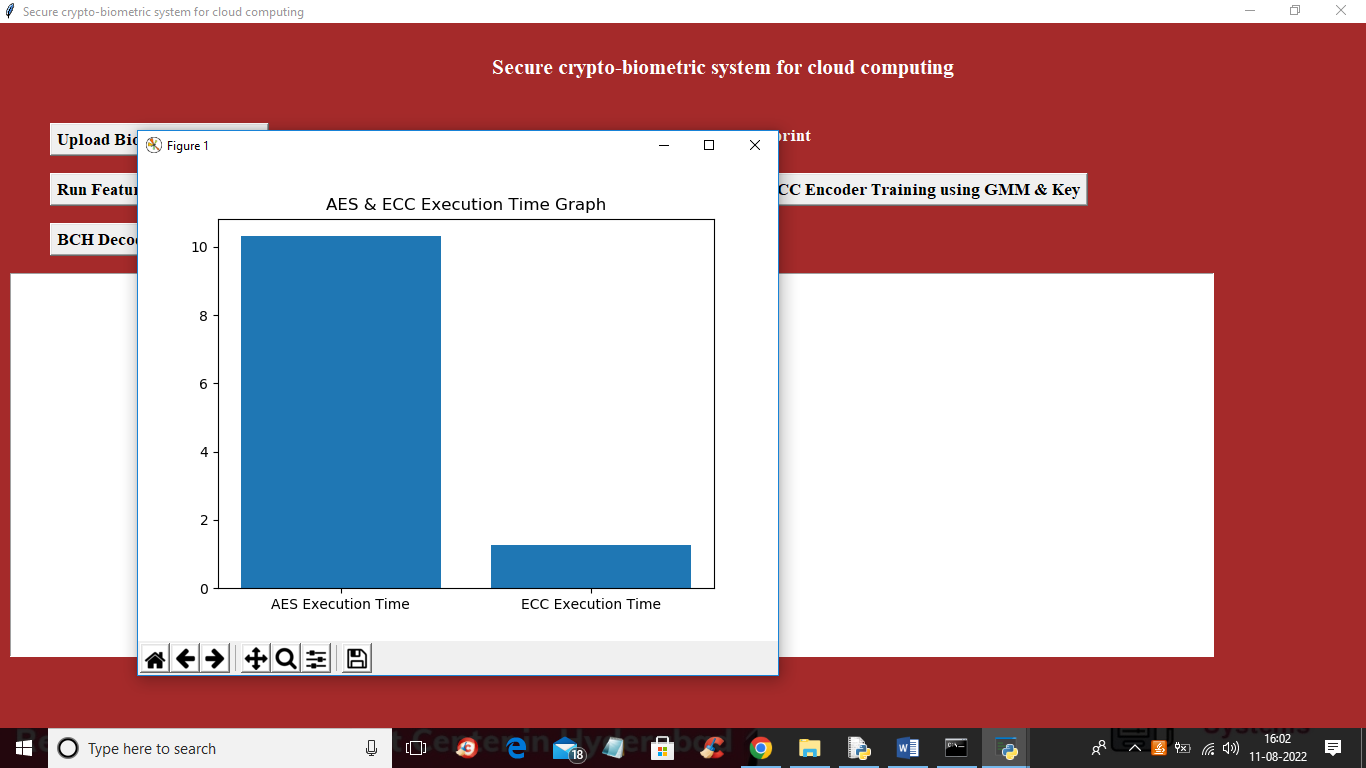
In above screen GMM is encrypted and AES took 10.31 seconds and ECC tool 1.2 seconds and then we are seeing GMM encrypted data and now click on ‘BCH Decoder Verification’ button to upload template and get verification output



In above screen selecting and uploading finger template and then click on ‘Open’ button to get below output



In above screen template identified or belongs to person 4 and now click on ‘AES & ECC Encryption Time Graph’ button to get below graph



In above graph x-axis represents encryption algorithm names and y-axis represents execution time and in both algorithms ECC took less execution time