Secure crypto-biometric system for cloud computing

Now-a-days all organizations or techie peoples are using cloud services to store and manage their business data as this cloud services provide heavy computing resources in cheaper cost but this advantage leads to an issue called data security as data store at cloud is away from user’s hand and can be misuse by cloud service provider or hacker.

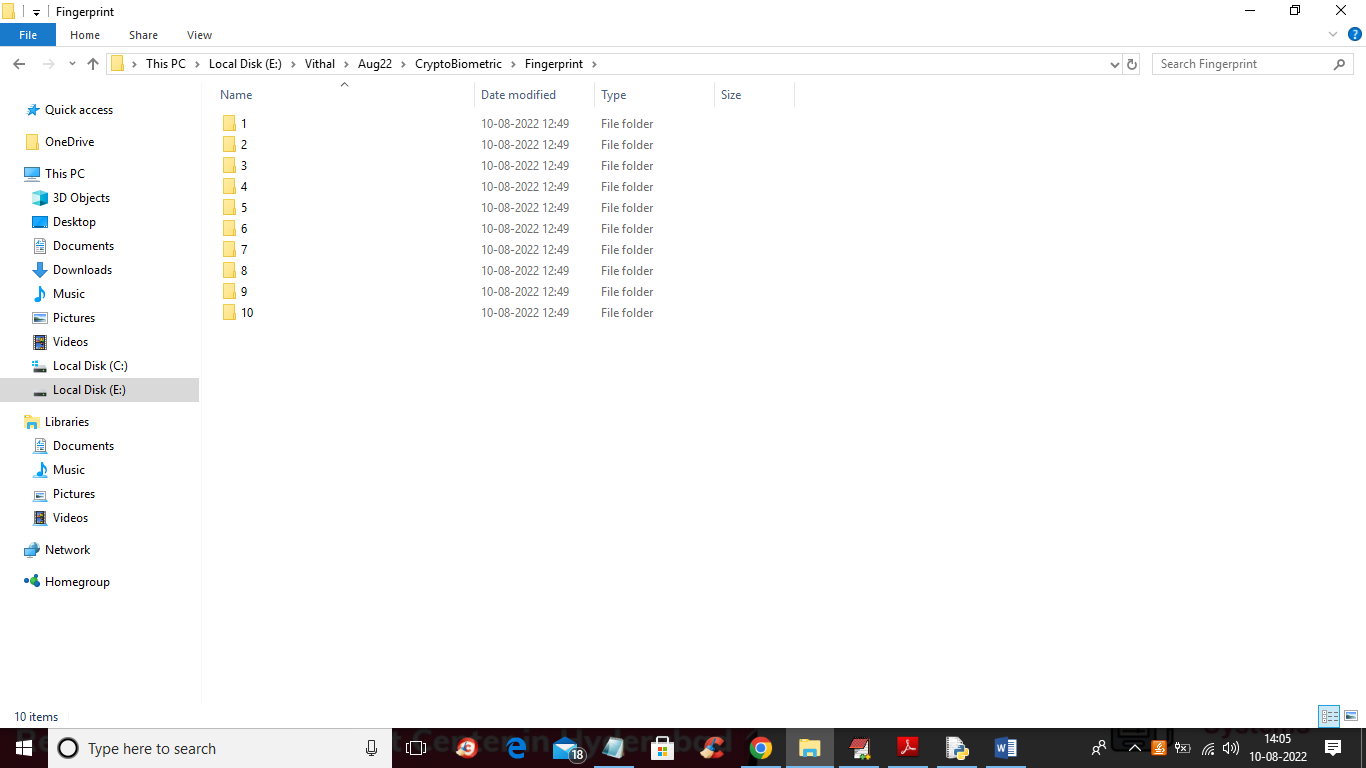
In propose paper author is providing security to user’s data by employing HMM model. Many organizations will use employee’s biometric data for verification but storing such biometric data at cloud can be dangerous as it may steal or hack by hackers to gain access to company servers.

To overcome from this problem author is employing Crypt-Biometric which will convert user biometric data into encrypted format and only genuine verification system can only verify such data so if hacker get crypto-biometric data then he will not aware of decoder key so he cannot verify himself.

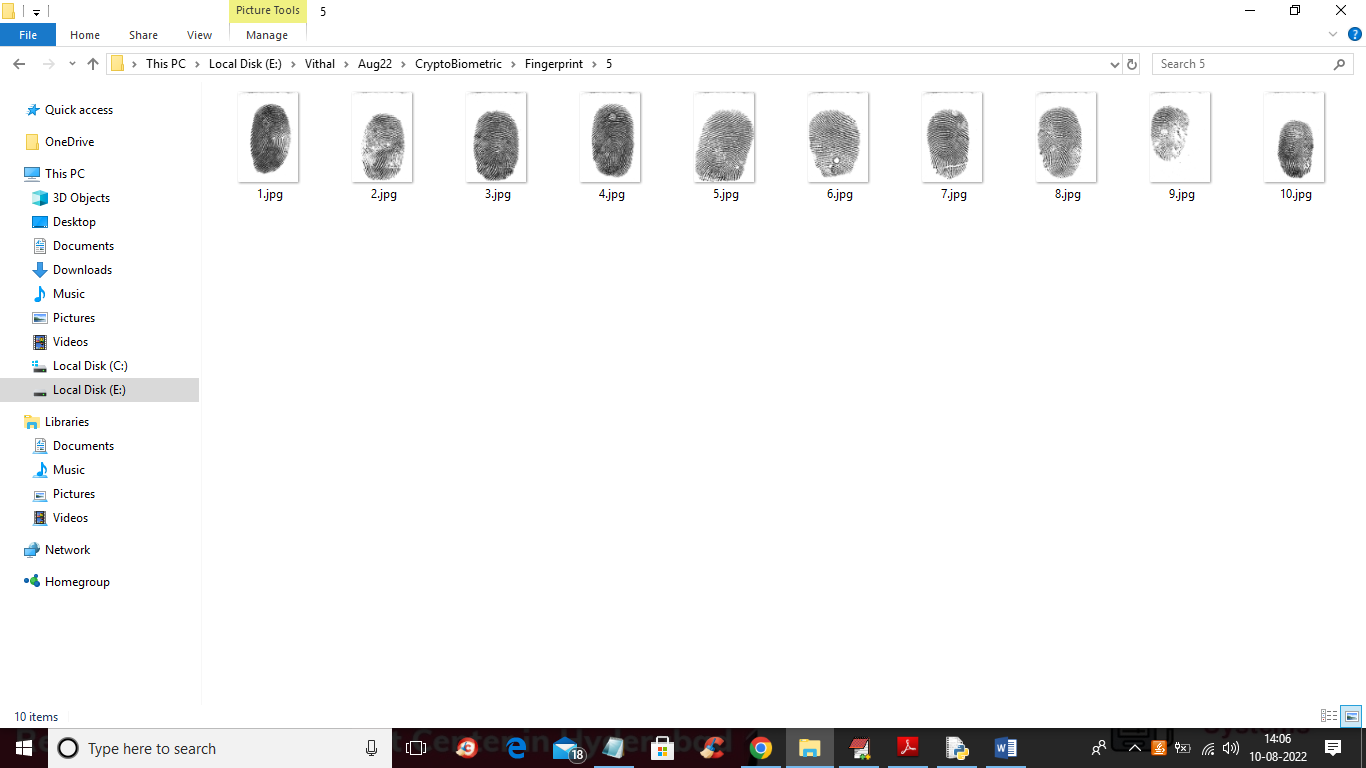
In propose paper author is using biometric database as Universal Background Model (UBM) whose features will be extracted using HMM (hidden markov model) algorithm and this algorithm will use Baum-Welch and LBG clustering technique to extract features from biometric template. Extracted features will get through PCA algorithm for features selection and then selected features will be encoded using Private Key. Encoded features will get train with GMM algorithm and above features encoding process is called as Fuzzy Commitment Template Protection.

Above procedure used for biometric template enrolment and then we apply same process for verification also.

To implement this project we have used biometric database of 10 persons and below screen showing those images

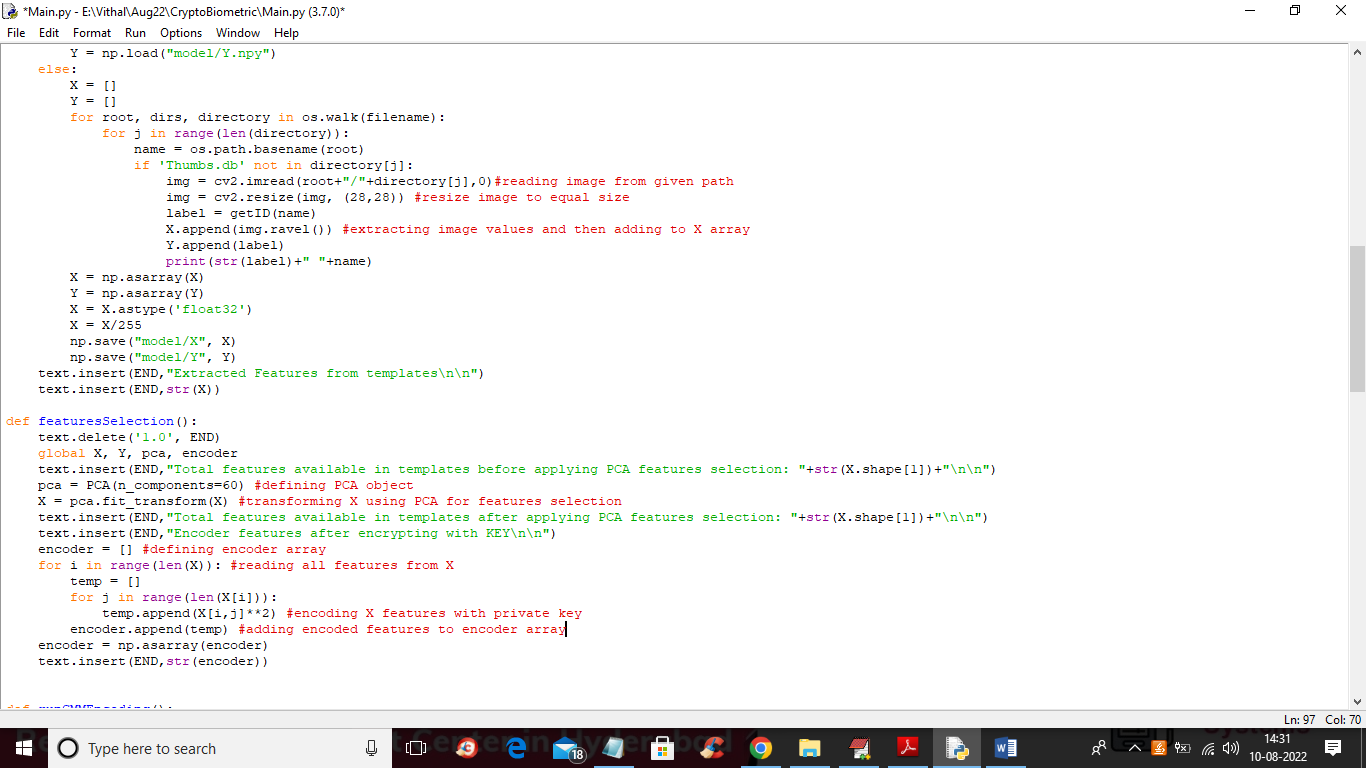


In above screen we have 10 folders for 10 person biometric details and below screen showing biometric images from above folders

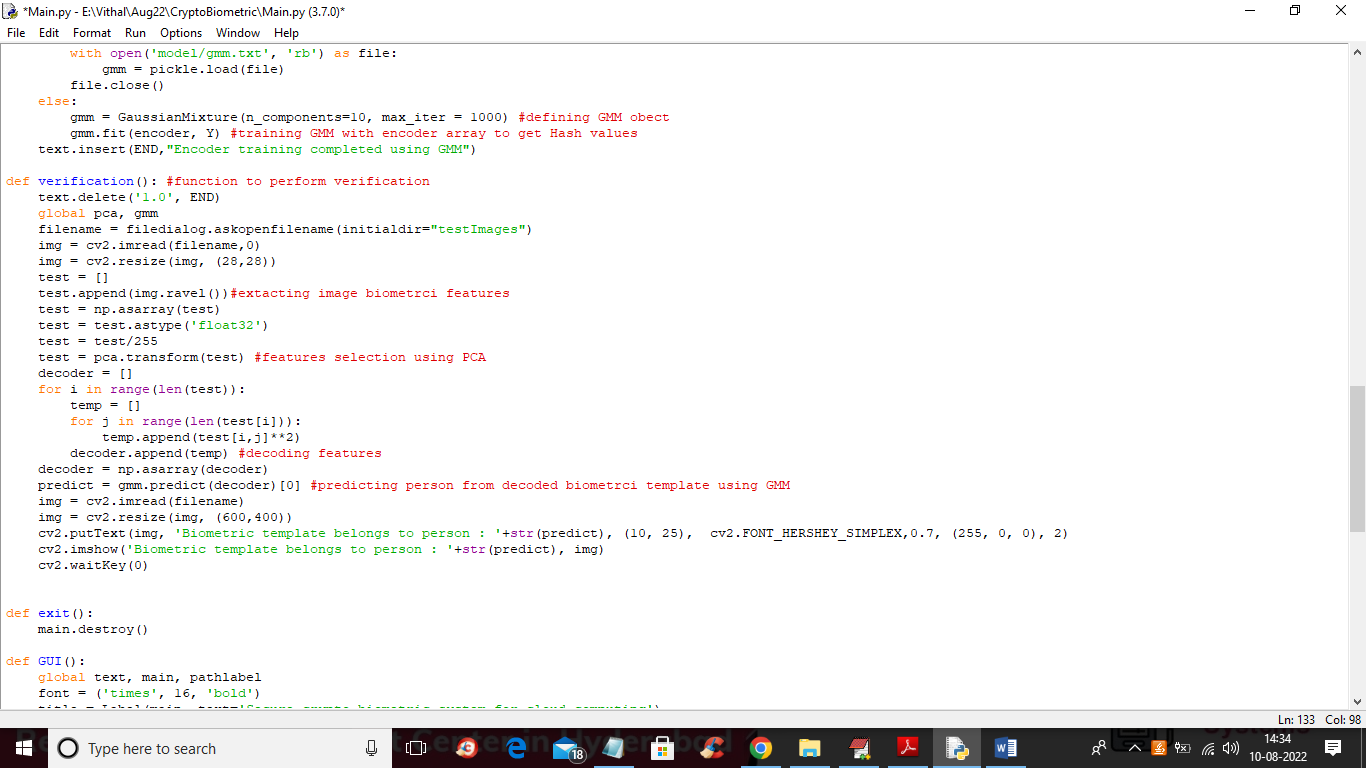


So by using above biometric database we are implementing crypto biometric concept.

In below screen we are showing code for Features extraction, features selection and then encoding with key and then training with GMM



In above screen read red colour comments to know about features extraction, selection and encoding and in below screen we can see training with GMM



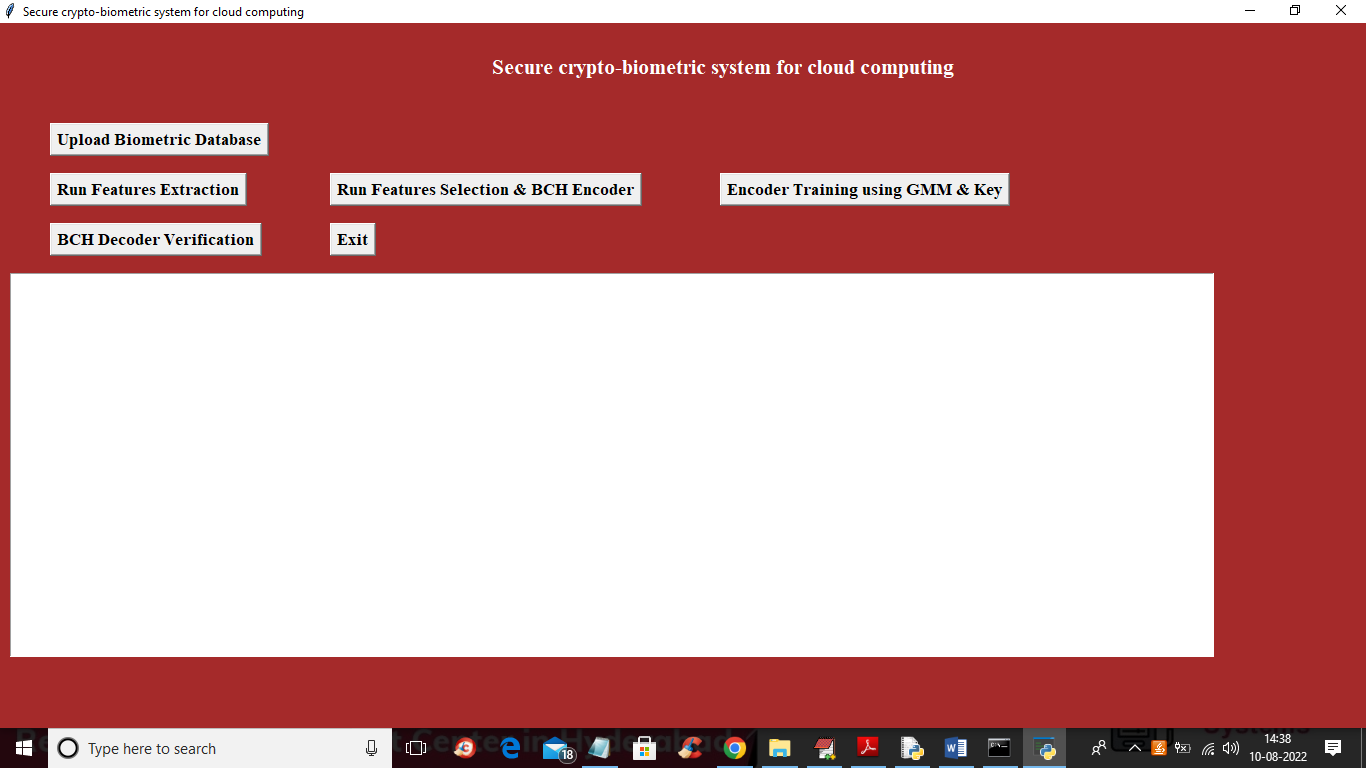
In above screens read red colour comments to know about crypto biometric implementation

To implement this project we have designed following modules

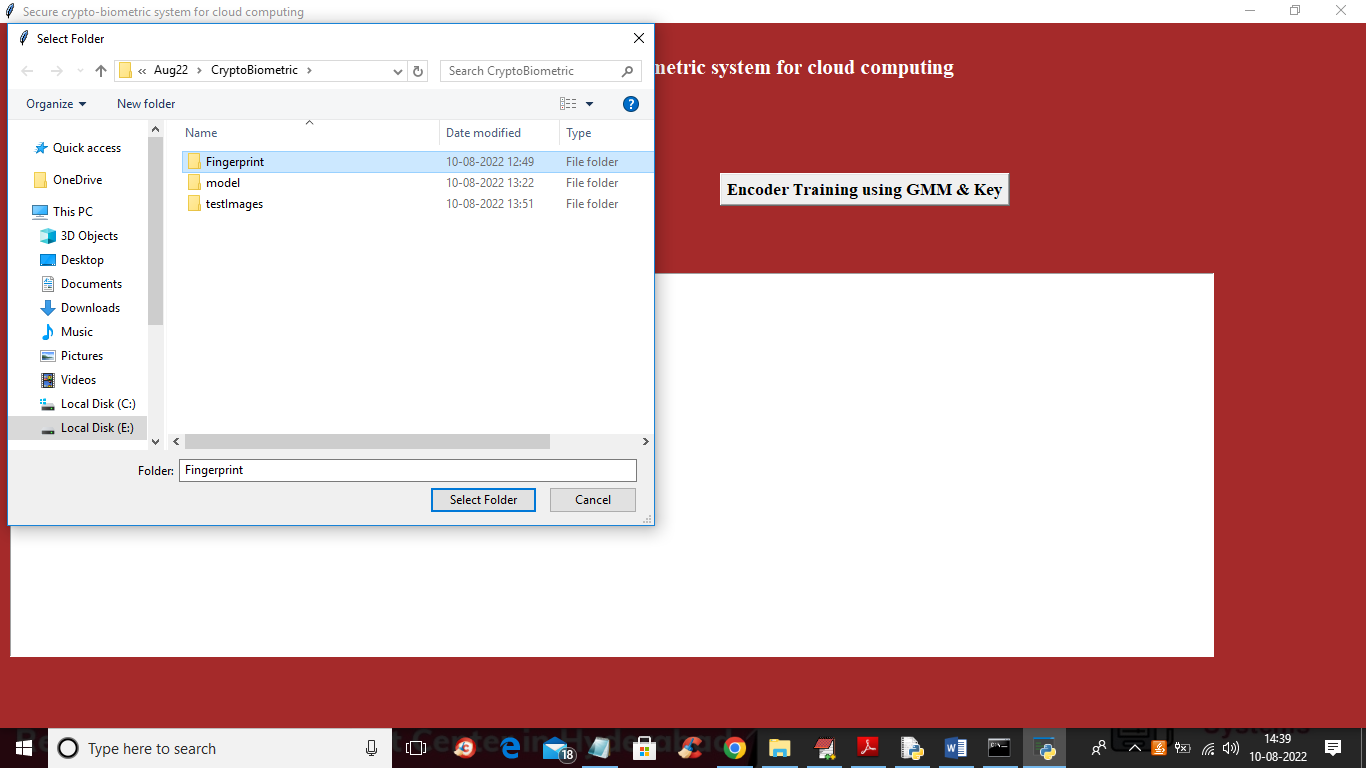
1. Upload Biometric Database: using this module we will upload biometric templates database to application
2. Run Features Extraction: using this module we will extract features from templates
3. Run Features Selection & BCH Encoder: in this module using PCA we will select features and then encode the features
4. Encoder Training using GMM & Key: encoded features will key get trained with GMM
5. BCH Decoder Verification: using this module we will upload test image and then decode and perform verification

SCREEN SHOTS

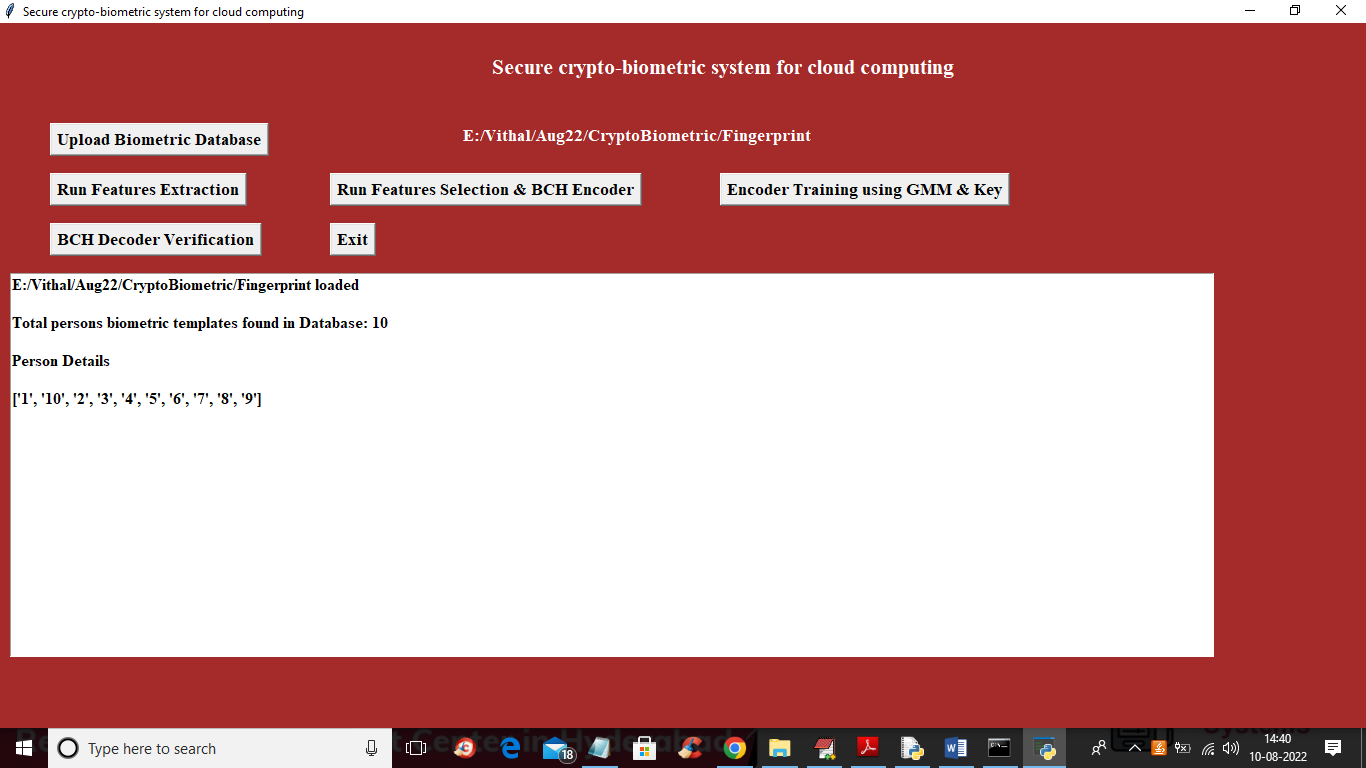
To run project double click on ‘run.bat’ file to get below screen



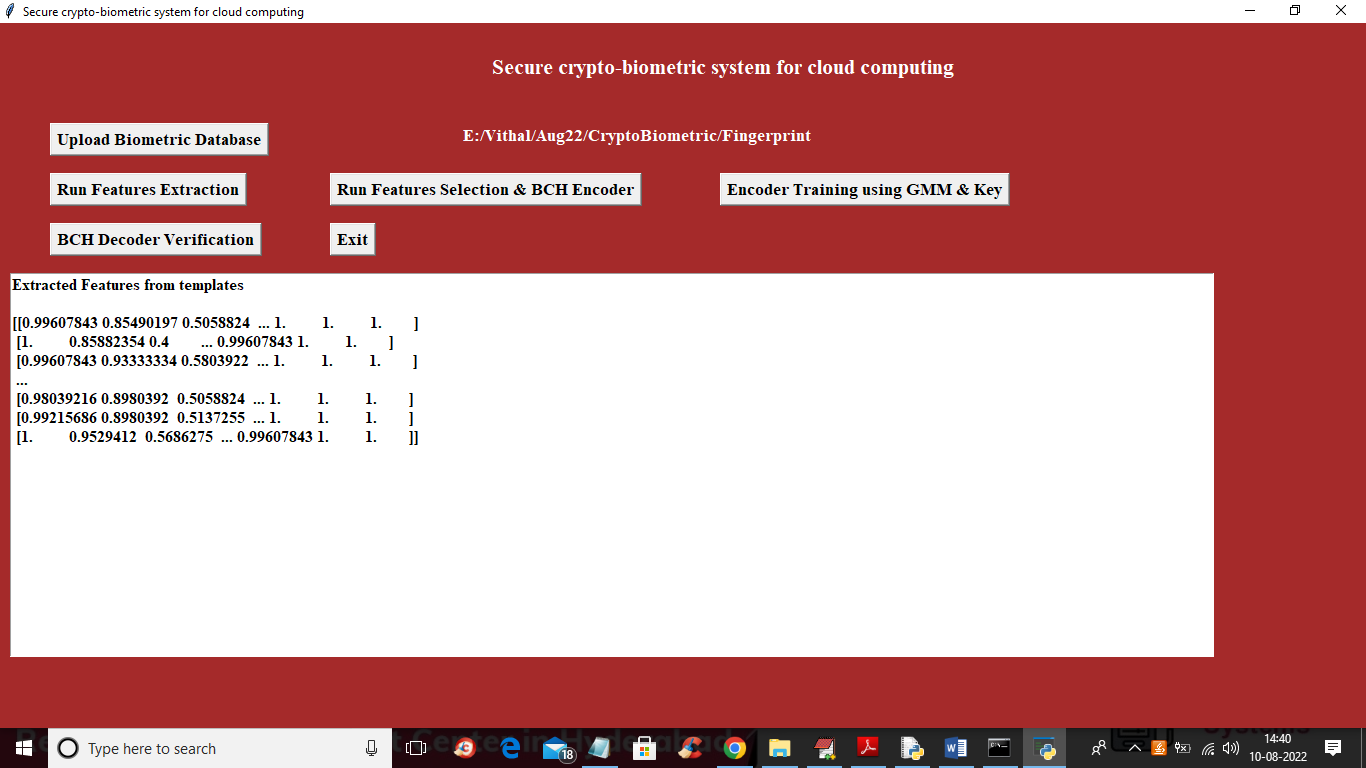
In above screen click on ‘Upload Biometric Database’ button to upload database and get below screen



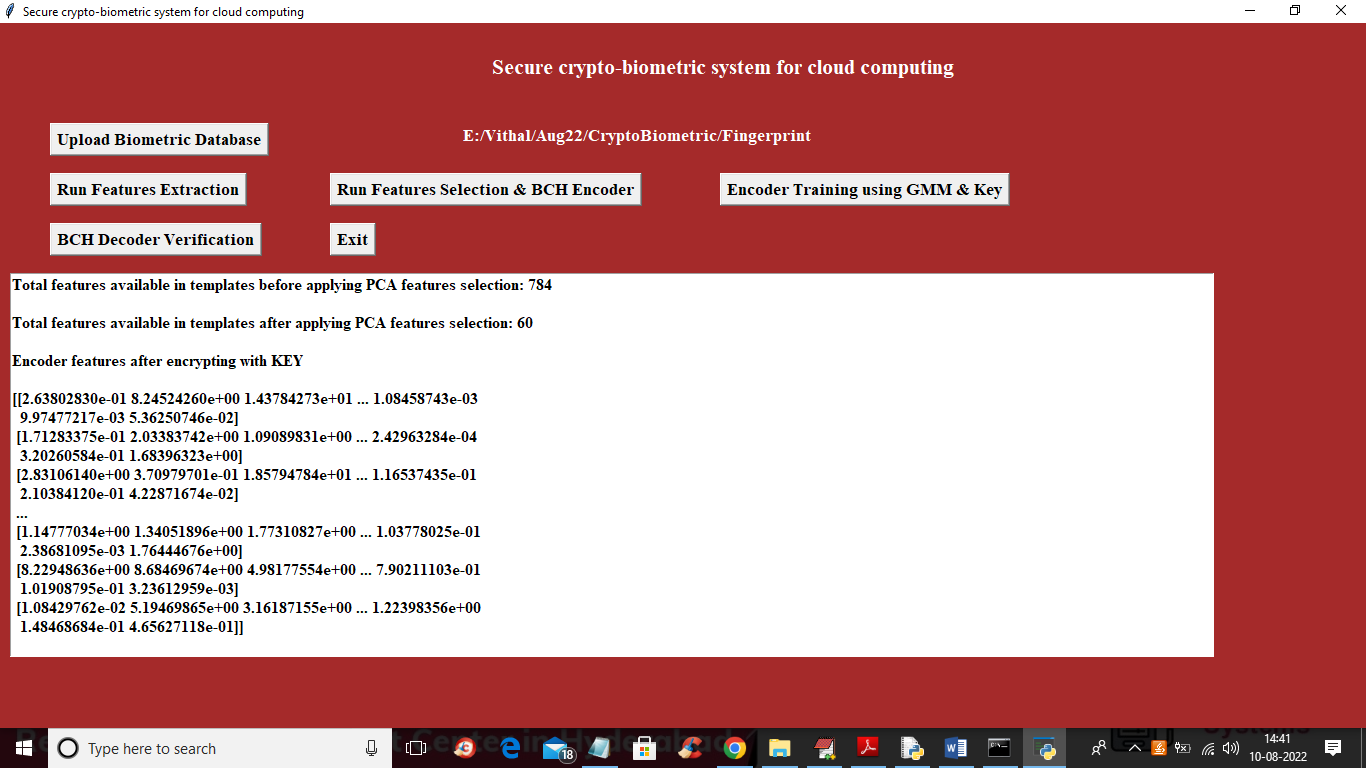
In above screen selecting and uploading finger print database and then click on ‘Select Folder’ button to load database and get below output



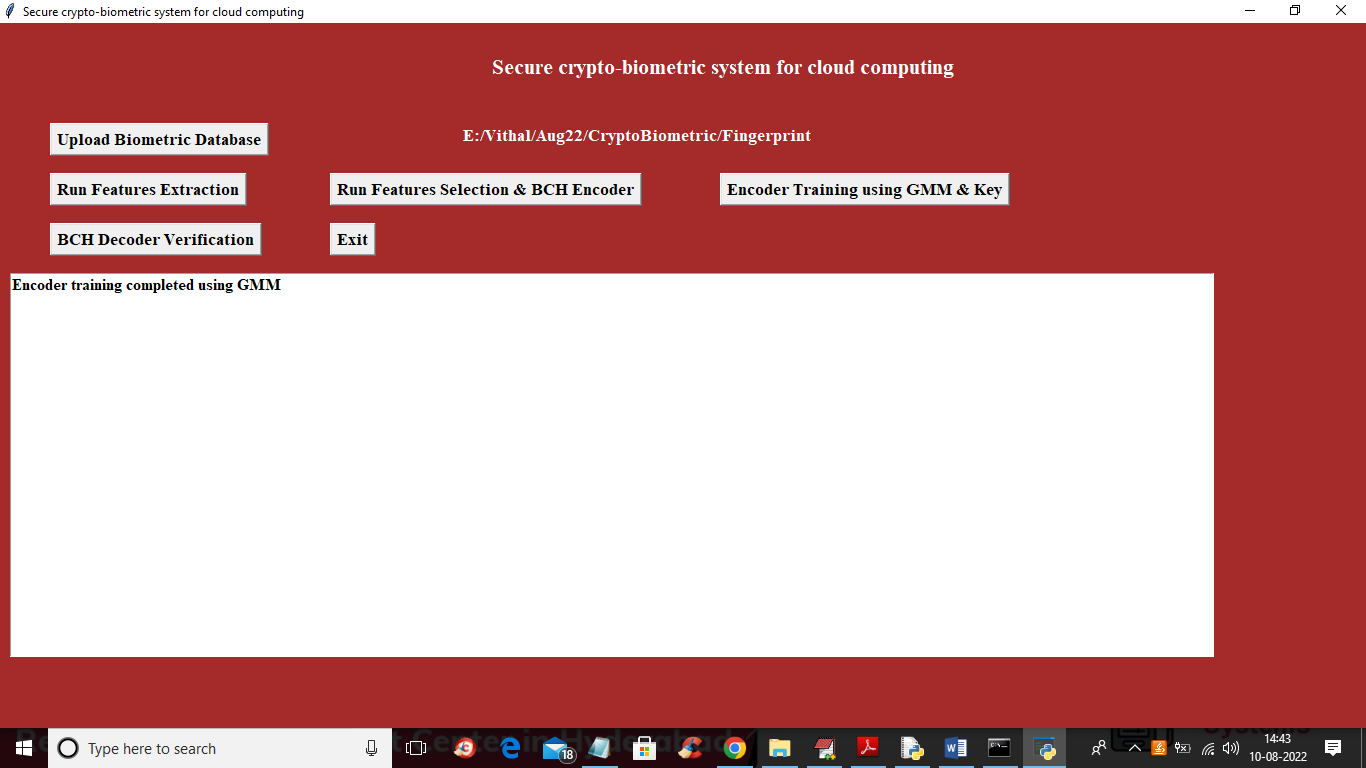
In above screen database loaded and it contains details of 10 persons and now click on ‘Run Features Extraction’ button to extract features from database and get below output



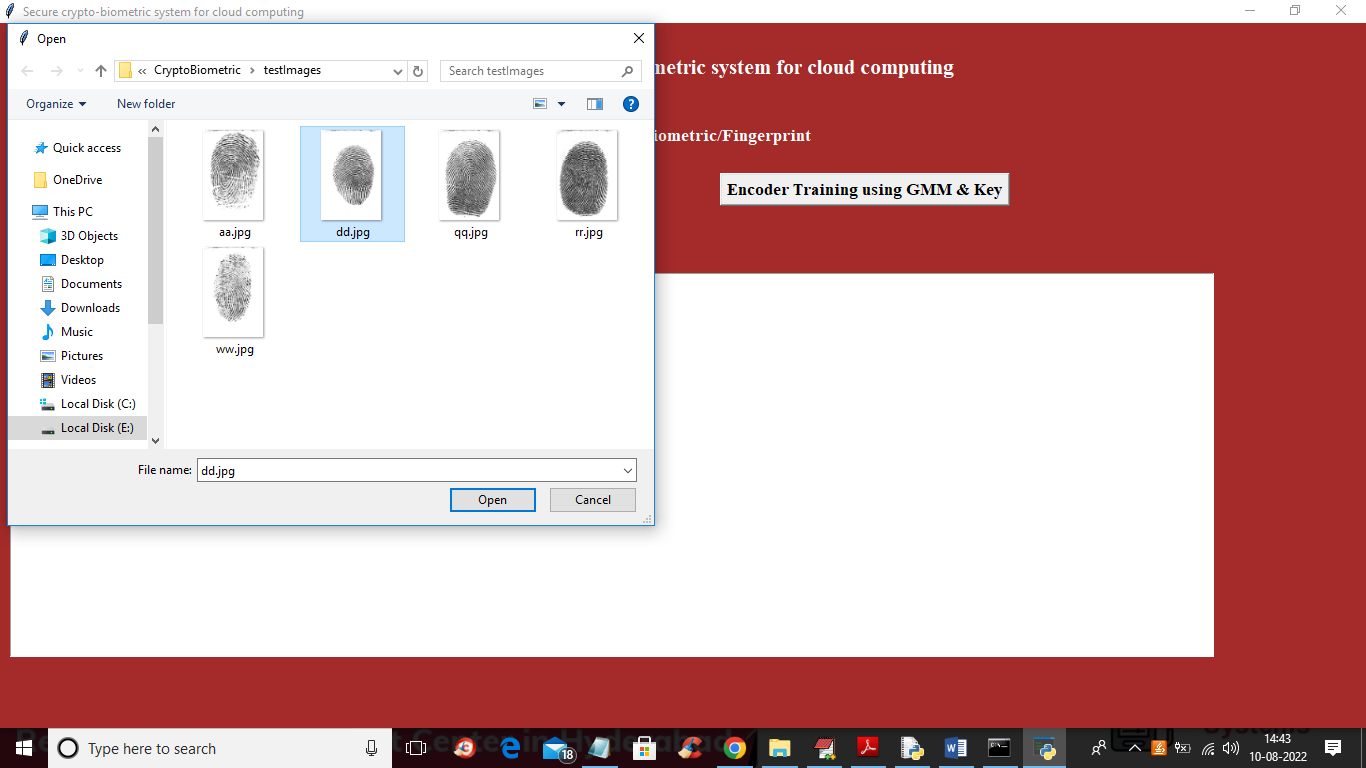
In above screen showing some extracted features from database and now click on ‘Run Features Selection & BCH Encoder’ button to select features and then apply encoding



In above screen in first line we can see database contains 784 features in each template image and after applying PCA, selected features are 60 and then displaying encoder values after encryption with Key and this encoded features will get store in cloud instead of storing plain template so from above encoded values attacker wont gain access to server. Now click on ‘Encoder Training using GMM Key’ button to train GMM and get below output



In above screen GMM training completed and now click on ‘BCH Decoder Verification’ button to upload TEST template and get below output



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



In above screen we can see uploaded template belongs to person 4 and similarly you can upload and verify other templates

