Fingerprint Recognition

Group 2

Our aim

To create a fingerprint recognition, identification and authentication program.

Dataset Collection

- Images of fingerprints are provided as part of FVC2002: the Second International Competition for Fingerprint Verification Algorithms and can be find on this link :- http://bias.csr.unibo.it/fvc2002/databases.asp

- Out of the four available datasets choose to work with the second one: DB2, which consists of 80 images of fingerprints that belong to 10 different individuals (or classes), which gives 8 images per person.

Dataset Collection

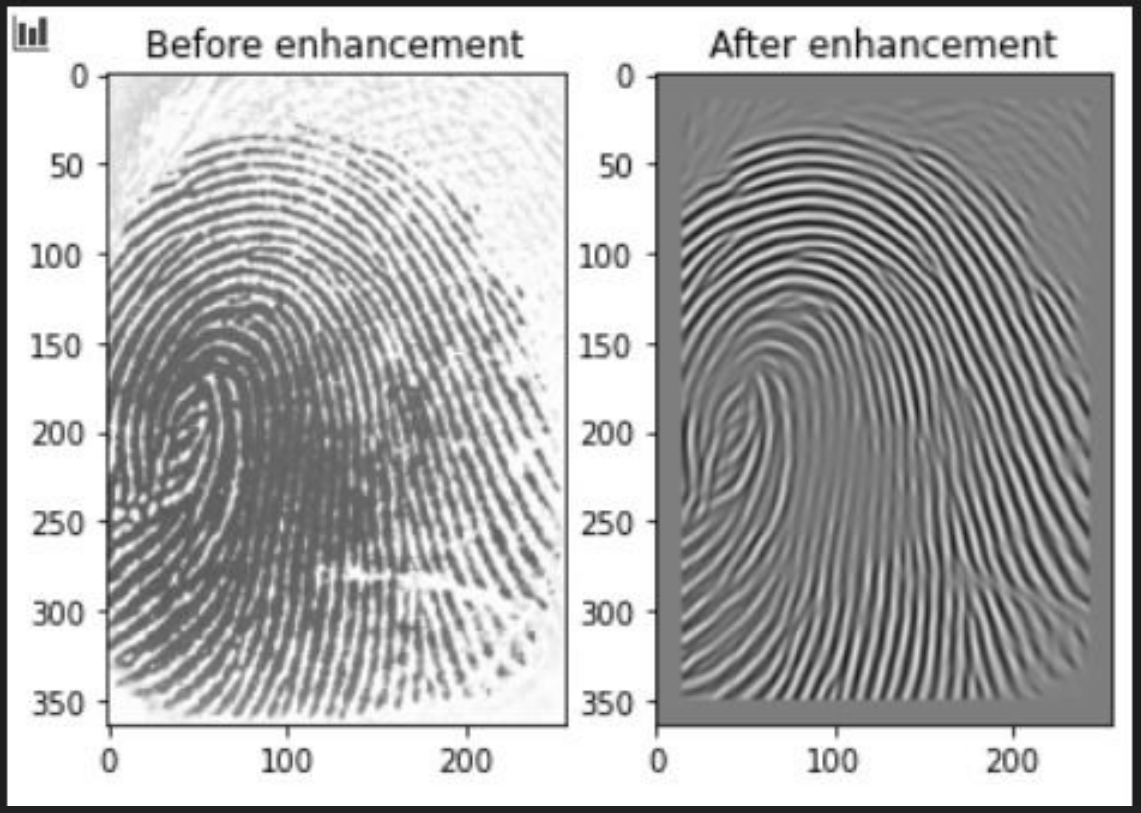
Sample Images :-

Preprocessing

- Firstly, we read the files and we prepare the dataset.
- Each image is converted to grayscale version and then enhancement is applied by using the following library for fingerprints enhancement in Python:-

  Fingerprint-Enhancement-Python.
- It uses oriented Gabor filter (a linear filter in image processing used for texture analysis) to enhance the fingerprint image.

Preprocessing



Feature Extraction

ORB (Oriented FAST and Rotated BRIEF) descriptor , developed by OpenCV labs, is used to extract features from the fingerprint sample image.

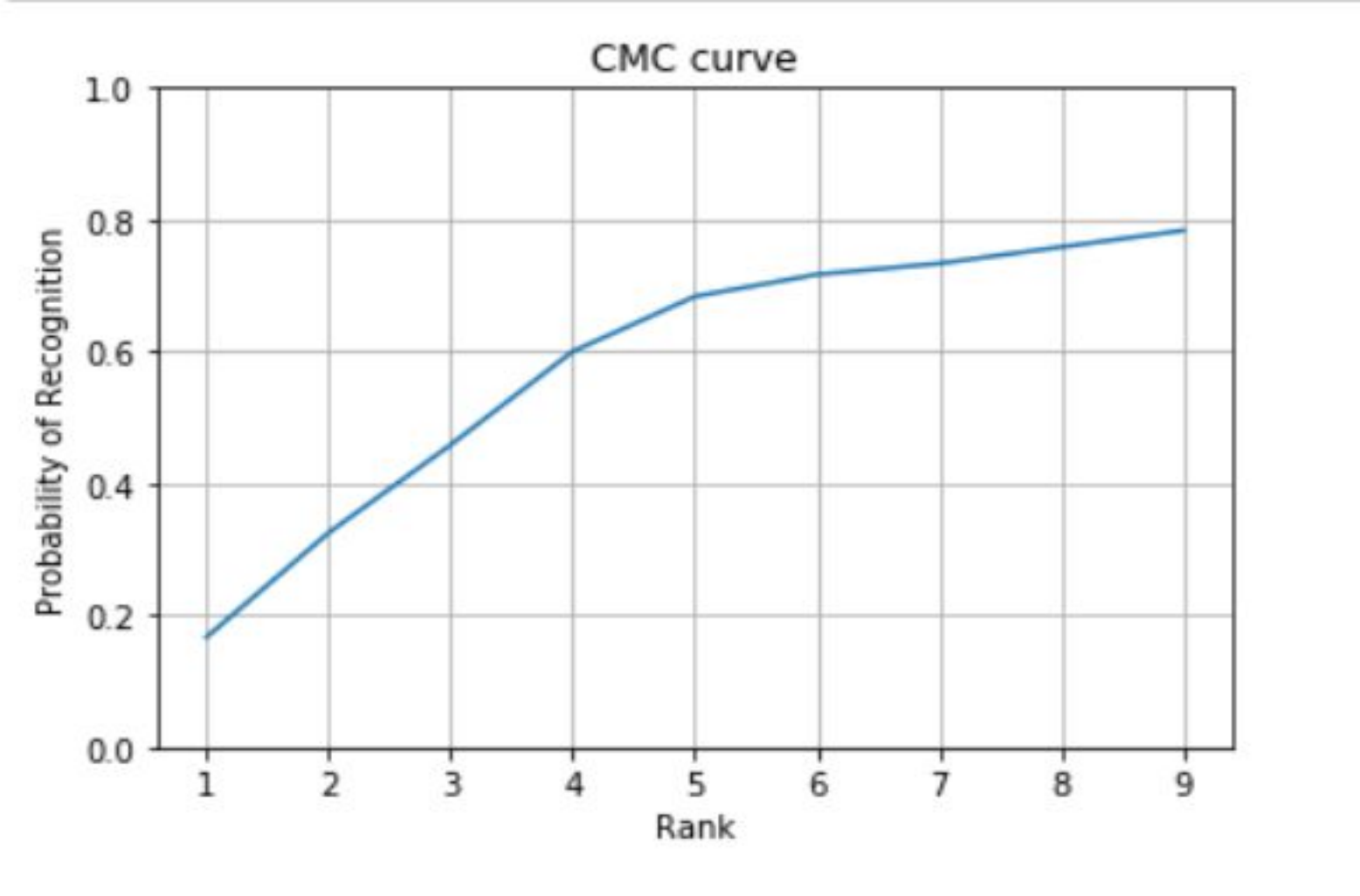
Furthermore, it is used to find matching keypoints. As a matching function we use number of matching features whose distance is below a given threshold.

Identification scenario

- First we analyse the identification scenario, which corresponds to 1:M classification problem. The organization captures a biometric from that individual and then searches in a database in order to correctly identify the person.

- The CMC curve is used as a evaluation measure in 1:M identification systems. It can be noticed that as the rank increases, the probability that a query image will be contained in that subset also increases.

Identification scenario

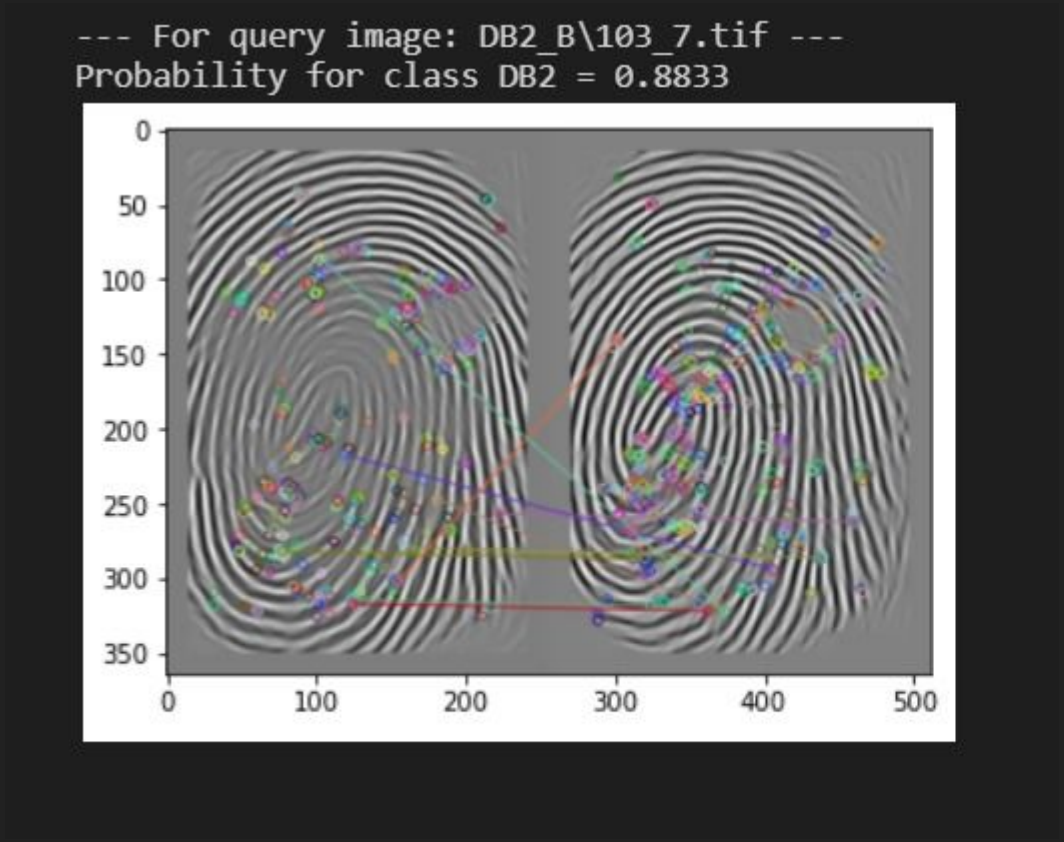


Authentication scenario

- Then, we analyse the authentication scenario, which corresponds to 1:1 problem or binary classification. A system will challenge someone to prove their identity and the person has to respond in order to allow them access to a system or service.

- The data structure for training is different, whereas the test set remains the same. For the training set, the already computed features are divided in separate dictionaries where the key denotes the class, and then every image features for the corresponding class are set in the dictionary as a value.

Authentication scenario



We can notice that there are ~ 83% chances that the person will be correctly authenticated.

Classification

- Then, we analyse the authentication scenario, which corresponds to 1:1 problem or binary classification. A system will challenge someone to prove their identity and the person has to respond in order to allow them access to a system or service.

- The data structure for training is different, whereas the test set remains the same. For the training set, the already computed features are divided in separate dictionaries where the key denotes the class, and then every image features for the corresponding class are set in the dictionary as a value.

Conclusion

We have successfully performed the Identification and Authentication of Fingerprint samples with an accuracy of 70% and an F1 score of 0.8235 during classification

```
----- START, Threshold = 60 -----
Accuracy is 0.700000
The precision score is 1.0
F1 score is 0.8235
```

Our Team

1	RA1811003010032	SMITH PATEL
2	RA1811003010036	DEVKUMAR PATEL
3	RA1811003010038	RUDRAKUMAR PATEL
4	RA1811003010041	AMAN OJHA
5	RA1811003010042	SHOBIT PURI