FTC 2018

Embedded System for Access Control Based on Facial Biometry and RFID

Cristian Souza

What is the problem?

- The current methods require a lot of photos of each user to make the correct identification;
- It is also necessary to validate the recognized user to make sure that is really him trying to be authenticated, not an photo.

The high cost of deployment is a factor that prevents the spread of such systems; because in most cases it is necessary to have powerful hardware to perform the processing, not to mention the cost of producing the software.

Conclusion

This project proposes the use of a Raspberry Pi for the identification and validation of faces, using a low cost hardware and free softwares to create a system for access control with a good performance and high accuracy.

The current methods

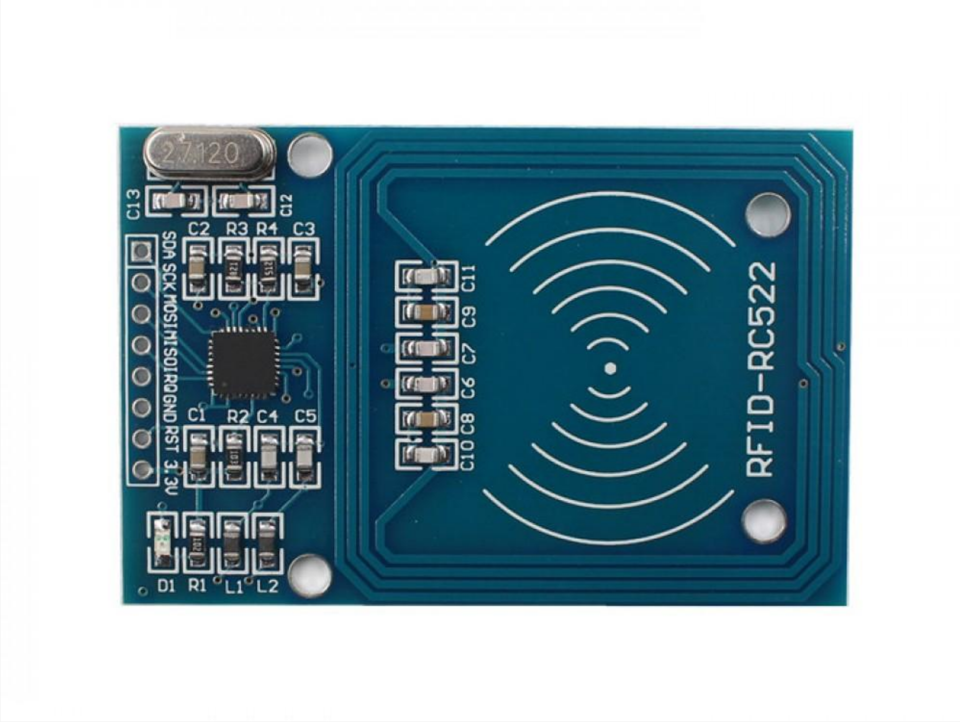
- Eigenfaces
  - The idea of this method is to identify the existing variability in the database with known faces and to use this information to encode and compare the faces.
- Fisherfaces
  - This method is characterized by using all the pixels of the image that contains the face and for this reason is considered very effective.
- Local Binary Pattern
  - This algorithm uses the concept of sliding window, based on the parameters of radius and neighbors. The facial identification process begins by generating a new image that describes the original highlighting the facial features.

Our Solution

We built an embedded system capable of performing facial recognition through deep learning methods and, at the same time, validating the user's authenticity.

Advantages

- Low-cost (built only with cheap hardware and open source softwares)
- High Accuracy (98.7% on the LFW database)
- Very fast (about 0.8s to perform the entire procedure)

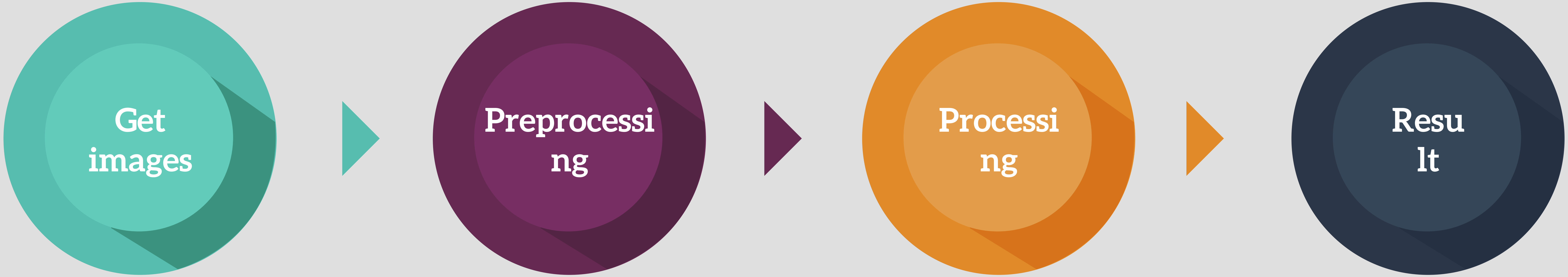


OpenCV

Techniques used

- Local Binary Pattern: for face identification;
- Face landmark estimation: to identify key points on a face and transform it before recognition;
- Deep Convolutional Neural Network: to generate 128 measurements for each face – **OpenFace**;
- Support Vector Machine algorithm: to find who has the closest measurements to the first image – **Dlib**;
- MSE and SSIM: to verify the authenticity.

Flow Chart



Get
images

Preprocessi
ng

Processi
ng

Resu
lt

The first step is to get some images from the user. The user needs to present his RFID card so that the system loads its image from the database while the camera captures some images.

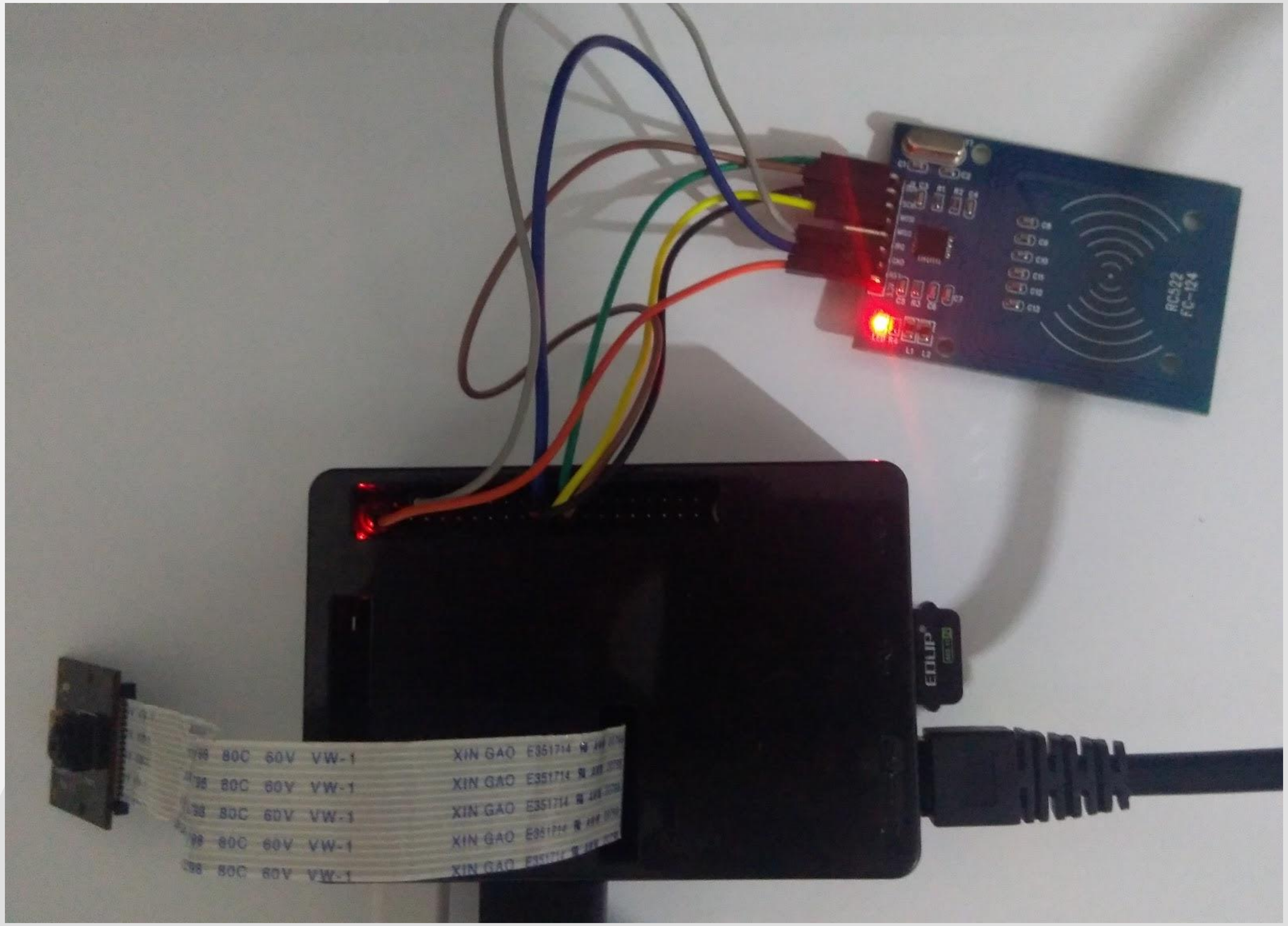
At this point, the system needs to perform some tasks to make the images ready for processing: convert the frame to black and white, identify the face and identify the place where is the user.

If the user is actually in the predefined location, the system makes some adjustments, generates the measurements and compare with the stored image.

The user is notified that the authentication operation was successful.

System description

- Local mode;
- Uncoupled mode;
- Face recognition API.



Demonstration

Use cases

- Control access to sensitive areas;
- Surveillance system;
- Identify criminals;
- Find missing persons;
- Use facial biometry instead of fingerprint (Brazilian elections scenario).

Contact

Federal Institute of Education, Science and Technology of Rio Grande do Norte (IFRN)

Avenida Senador Salgado Filho, n° 1159, Tirol –
Natal, Rio Grande do Norte, Brazil.

cristianmsbr@gmail.com

ivanilson.junior@ifrn.edu.br

robinson.alves@ifrn.edu.br

melquiades.pereira@ifrn.edu.br