Revista Científica del Centro Universitario de la Guardia Civil
Revista Lógos Guardia Civil

Rafael Bustamante Carrizosa
Lieutenant of the Civil Guard
Information Headquarters

IMPLEMENTATION OF A FACIAL RECOGNITION SYSTEM IN POLICE INVESTIGATIONS

IMPLEMENTATION OF A FACIAL RECOGNITION SYSTEM IN POLICE INVESTIGATIONS

Abstract: Facial recognition systems are built on computer programs that analyse images of human faces for the purpose of identifying them. It is a barometric system that can be used without the knowledge, consent or participation of the subject.

The goal of this study will try to identify, define and develop the procedures and requirements necessary to implement a use case that allows to put into operation a facial recognition system, based on open sources.

In essence, the operation will consist of introducing an image of a person concerned, the system will receive the images captured in real time and then it will make the comparison with an image of any person of police interest. If there is a case of positive correlation. The system will record the data and produce a warning.

Resumen: Los sistemas de reconocimiento facial se basan en programas Informáticos que analizan imágenes de rostros humanos con el propósito de identificarlos. Se trata de un sistema biométrico que puede ser usado sin el conocimiento, consentimiento o participación del sujeto.

El propósito de este trabajo consiste en identificar, definir y desarrollar los procedimientos y requisitos necesarios para implementar un caso de uso que permita poner en funcionamiento un sistema de reconocimiento facial basado en fuentes abiertas, mediante la construcción de un prototipo.

Básicamente, el funcionamiento consistiría en introducir una imagen de una persona de interés. El sistema recibirá imágenes capturadas en tiempo real y los comparará con la imagen de una persona de interés policial. En caso positivo deberá registrar los datos y producir un aviso.

Keywords: Face Recognition. Local Binary Pattern. Orange Pi. Haar Cascades.

Palabras clave: Reconocimiento Facial. Patrón Binario Local. Orange Pi. Haar Cascades.

Acronyms:

SF: Security Forces.
GPU: Graphic Process Unit
FR: Facial recognition
RGB: Red Green Blue
SBC: Single-Board Computer
OS: Operating System
SOC: System On a Chip
FRS: Facial Recognition System
SSH: Secure Shell or Secure Command Interpreter
VPN: Virtual Private Network
VPU: Video Process Unit

INTRODUCTION

There is no doubt that the Internet has not only revolutionised computing and communications but has also changed the world as it was 30 years ago.

This technological revolution has also led to the appearance of a wide variety of electronic tools. For example, the Internet of Things (IoT or Internet of Things) is a new concept that allows physical objects to be connected through the Internet, enabling the programming of specific events.

In addition, this technological explosion has led to significant progress in knowledge of the different fields of biometrics (fingerprints, iris recognition, facial recognition (FR), handwriting recognition, etc.), making it an essential component of identification systems.

In the fight against disruptive elements such as criminal and terrorist organisations, Security Forces (SF) have no option but to keep up with new technologies to investigate and prove criminal activities.

Since searching for, tracking and obtaining information about individuals involved in criminal activities are among the main activities of the SF to protect public safety, it is logical to consider FRS as a powerful tool to achieve this.

This paper hypothesises that Facial Recognition Systems (FRS) can be used passively, i.e., without the subject's knowledge, consent or participation, and to achieve a fundamental objective. They are obtaining information of interest to the police to fight crime.

This paper sets out to assess the possibility of equipping SF with an effective tool to prosecute crime in accordance with the law. The purpose is to identify, define and develop the necessary procedures and requirements to model and design an FRS through a use case that allows the implementation of a prototype.

MODEL AND DESIGN OF THE FRS

1.- THE LEGAL FRAMEWORK

With the rise of biometrics and artificial intelligence, legislators have been forced to introduce regulatory changes to protect citizens from possible violations of their fundamental rights.

Of particular note in this regard is the EU General Data Protection Regulation, which provides that the processing of biometric data, including facial recognition data, is considered a special category of personal data and therefore, subject to additional protection and safeguarding requirements. (EU Regulation 2016/679).

Likewise, the Court of Justice of the European Union has issued several relevant rulings1 that establish that the use of facial recognition systems by police must comply with the principles of proportionality and necessity.

More specifically, according to a European Parliament resolution, "AI applications may offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies and judicial authorities, and combating certain types of crime more efficiently, in particular financial crime, money laundering and terrorist financing, online sexual abuse and exploitation of children as well as certain types of cybercrime"(European Parliament, 2021).

In Spain, according to the Organic Law 4/1997, the competence for installing video cameras in public places corresponds exclusively to the SF. Its articles also establish the principles, conditions and limitations for their authorisation and use. (Organic Law 4/1997).

More recently, with the publication of Organic Law 7/2021, it was established that the data controller must conduct a risk analysis or a data protection impact assessment in public places where video cameras are installed to establish the potential level of harm to citizens and the purpose pursued (Organic Law 7/2021).

In short, biometric data collected by the FRS are considered to be specially protected and their use by the SF is limited to the prevention, detention and investigation of criminal offences, governed by the principles of proportionality, minimum intervention and appropriateness.

2.- TOOLS FOR DEVELOPMENT

Different types of diagrams will be used to carry out the modelling of this FRS. They are useful to efficiently document and detail the processes and tasks that make up any system.

In addition to modelling, we will develop a prototype FRS, establishing the requirements, functionalities and appropriate components. We will continue with the coding of functions using OpenCV2.

The library3 is licensed under BSD4, is cross-platform and has numerous functions that address a wide range of areas such as artificial intelligence and facial recognition.

To programme the prototype, the Python interpreted, cross-platform programming language is used. It was created in the late 1980s by Guido van Rossum at the Centre for Mathematics and Informatics (CWI, Centrum Wiskunde & Informática) in the Netherlands.

1 Source: https://curia.europa.eu/jcms/jcms/p1_3252415/es/ Retrieved 21 May 2023.
2 This library was initially developed by Intel in 1999. Source: https://opencv.org Retrieved 20 May 2023

[3] A library is a set of tools coded in a programming language, and invoked by executable programmes to perform a task.

4 The BSD licence allows free use for both commercial and research purposes.

Python is a language with a clear syntax and a shallow learning curve. It is widely supported in all types of projects thanks to the wide variety of its libraries, which is why it has become the most widely used programming language5.

3.- SUBDIVISION OF FUNCTIONS IN THE FRS

The following processes must be carried out to develop of the prototype.

- *Registration phase.* This function is used when working within the verification scenario. It consists of registering the user or users to be authenticated. During this function, facial features are extracted, and the individual's identification data is added. All these data are stored in a database. The facial features are used to create templates. A template makes it possible to calculate and obtain an unambiguous representation of an individual's face.

- *Image processing.* It requires the use of an image capturing device. There are two image processing methods.
  - *In real time*. The camera sends the images to the system for real-time processing.
  - *Deferred or forensic processing*. In this case, the system does not require a direct connection to the camera while the images are being captured, which are stored on some kind of device for further processing.

- *Face detection.* Once the image has been captured, you need to know if there is a face in it using some kind of classifier. This classifier first detects the possible face and then the eyes. This order reduces the detection time, as the search for the eyes is limited to a small area, the area of the face.
  - *Face detection. Based on the knowledge gained from observing faces, characteristics such as the eye area being darker than the cheek or nose area, tracking head movements to detect whether or not it is a face, etc. have been determined. All this information is used for face detection.*
  - *Eye detection. Although the process is similar to that of face detection, the location is more important as it is used in the image normalisation phase to obtain the rotation angle of the face to determine its orientation.*

In this prototype, the Haar classifier, which has already been trained to recognise faces, is used.

Haar uses the sliding windows approach. They consist of scanning the image from left to right and from top to bottom in different sizes. As the window moves from left to right and from top to bottom, the classifier determines if there are any faces.

If the classifier detects a face, the method returns a list of tuples containing the bounding box (the window) of the faces in the image. This tuple contains the face location, width and height.

5 According to the PYPL PopularitY of Programming Language Index, Python is used by 27.91% of programmers, ranking first. Source: https://pypl.github.io/PYPL.html. Retrieved 13 March 2023

Haar is an algorithm that subdivides the image into rectangular sections. In turn, these are divided into several sub-sections to make up a comprehensive picture. The integral image is the representation of the image obtained by summing the intensity (RGB6) of the pixels above and to the left of a point. (Nikisins et al., 2015)

In the figure below, the larger rectangle shows the full image while the boxes represent the integral images.

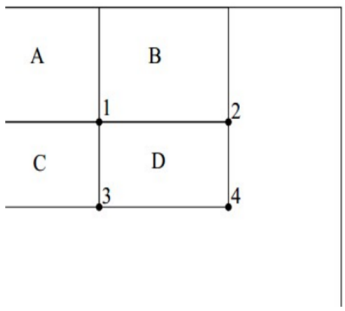

Illustration 1.- Integral Image

For example, the integral image value at location 1 is the sum of the pixels in rectangle A. The value at location 2 is the sum of the pixels in A + B, location 3 is A + C, and location 4 is A+B+C+D.

The sum of pixels in D can be calculated as: 4+1-(2+3).

- *Image normalisation.* Once the valid coordinates of the facial contour have been obtained, the image undergoes a series of transformations. The purpose of standardisation is to make the extraction of characteristic features more efficient. With normalisation, the image is rotated, scaled, cropped and finally converted to greyscale.
  - *Rotation*. The purpose of the rotation is to align the face vertically. Therefore, in addition to the position of the eyes obtained in the detection phase, the location of the central point of the face is required for use as the rotation axis. With these three points and trigonometric calculations, the angle of rotation is obtained.
  - *Scaling*. The specific size of the face image is obtained through scaling so that all the faces that are worked on have the same proportion. According to the standard proposed by ISO/IEC 19794-5, the recommended distance between the centres of the eyes should be a minimum of 60 pixels and a maximum of 96 pixels. (Vázquez et al. 2012). Taking this range of distances as a reference, all images have similar proportions, making them easier to compare.
  - *Cropping*. It consists of giving each image the same dimension. As in the case of scaling, the standard indicated by ISO/IEC 19794-5 applies, with dimensions of 168 x 192 pixels.
  - *Greyscale*. The aim is to make the image representation as uniform as possible, mitigating any changes in brightness that introduce noise into the feature extraction algorithms. The aim is to ensure that the number of pixels for each grey level (0 to 255) is as homogeneous as possible.

[6] RGB (red, green, blue). Defines colour composition in terms of the intensity of the primary colours of light.

To convert a coloured pixel to greyscale, an intensity-weighted average of each of the three RGB colours is performed, whereby each colour is assigned a value. The values used by OpenCV are grey = 0.2989 * red + 0.5870 * green + 0.1140 * blue.

All these operations make it easier to compare faces, increase the amount of useful information and reduce noise.

- *Feature extraction*. A set of characteristic values is obtained from each image, which must define each face as accurately as possible and at the same time be able to distinguish the face. During feature extraction, the algorithm obtains values that provide information about the face, discarding any information that is not useful.

- *Comparison.* In this phase, the information obtained, or doubtful sample, is compared with the existing information or indubitable sample. The Euclidean distance is used to calculate the distance between each of the samples. During the comparison process, the algorithm receives an identification record and a template as input and calculates and compares the distances between them. The result is translated into a percentage that represents the likelihood that the two records represent the same individual.

A pseudocode outlining the different functionalities proposed is proposed below.

```
START()
    While () Do:
        If (face (image) detection) Then;
            image := normalise (image);
            image := feature extraction (image);
            result := face recognition (image);
            If (result < threshold) Then:
                RECOGNITION SATISFACTORY();
```

WORK SCENARIOS

The proposed FRS has two functions depending on whether the system is used as an identification method or as a verification method.

To clarify these concepts, an <<*unidentified person*>> is defined as a person whose identity is not known, a <<*person of interest to law enforcement*>> is an individual whose identity is known and who is wanted to be found and located, and an <<*identified person*>> is an individual that matches an unidentified subject and an individual registered in the police database.

Face verification or authentication compares matches between an unidentified subject and a person of interest to law enforcement. In contrast, an identification or forensic task is defined as the search for an unidentified subject among a set of registered individuals.

In short, while verification matches a captured image against a stored face (one:one comparison), identification matches a captured image against many stored faces (one:many comparison).

Framing these concepts in the use of an FRS applied within the field of police investigation, there are two kinds of scenarios. Each one is differentiated by a set of specific needs, properties and characteristics, which will be analysed in the requirements set out in section 4.

3.1.- Verification or authentication scenario

This consists of installing the system in a location known to be likely to be the location of the person(s) of interest.

The system compares each of the faces captured by the camera with the unambiguous image of the faces of the persons of interest to law enforcement stored in the system.

This scenario consists of real-time processing and, if a match occurs, programming the system to automatically send some kind of notification.

3.2.- Identification or forensic scenario

In this case, the system stores the images obtained for further processing to establish the detection and identification of faces through police databases.

This scenario applies to the case of images of criminal activities where the subjects involved needs to be identified.

4.- ANALYSIS OF REQUIREMENTS

These requirements will determine the conditions to be met by the FRS, considering the two scenarios.

These requirements can be classified into functional requirements that describe information input, its processing and subsequent information output from the system, and non-functional requirements related to the characteristics of the system, and therefore focus on describing the limitations of the system, e.g. reliability, processing capacity, data transfer speed, security, portability, etc.

4.1.- Functional requirements

Since the system must be able to operate in both verification mode and identification mode, to define the requirements, it is necessary to consider each of these scenarios separately. Figure 3 shows some of the aspects that will be discussed below conceptually.

- *Requirements in verification mode*

- The system allows the profile of persons of interest to law enforcement to be stored for real-time comparison.
- When images are captured by the system camera, they are stored on a temporary storage device, and those that have been in the system the longest are discarded, so that the storage capacity does not collapse.

- In the event of a positive result of a person of interest, the system permanently stores the latest images gathered by the camera for subsequent monitoring.
- Following a positive result, the system should allow an instant alert signal to be issued.
- When an alert signal occurs, the system must also send information about the event, including at least the location, date and time of the start of the recording, the identity of the subject, the capture of an image(s) and the name of the device that obtained it. This is because there may be more than one device operating.

- *Requirements in identification mode*

- It should offer the possibility to work with deferred images, regardless of whether they were captured by the FRS, as well as with images captured by other devices.
- If the FRS captures images for delayed processing, it must have an event log where the information related to the captured images is stored. It must include the location where the recording starts, the date and time of recording, the duration and the name of the device.
- The system does not handle queries in real time, but must allow the possibility to connect to and query distributed databases.
- In addition to querying police databases, the system should correlate captured images with those contained in social network profiles, receiving the web addresses where each of the social network profiles found is hosted from the system.

4.2.- Non-functional requirements

- The system must have an integrated digital camera, capable of image capture.
- When the system is working in verification mode, it must be able to process images in real time, and:

  - Locate each face in the scene.
  - Compare them with the person of interest to law enforcement stored in the system.
  - Generate the corresponding events.
- Adequate bandwidth is available to send data in the verification scenario in case of a positive result.
- The device must have a geo-positioning facility.
- The system must be remotely accessible for queries and management, so it must have a secure VPN connection[7] (Virtual Private Net) and an SSH console[8] (Secure Shell).
- Availability is an important factor, so the system can send events related to battery charge level and available memory space when recommended thresholds are exceeded.

[7] A VPN allows multiple devices to be connected as if they were physically in the same place, emulating local network connections. It is considered virtual, because it connects two physical networks; and private, because only computers in the local network on one side of the VPN can access it.
[8] SSH is a remote administration protocol which allows operators to connect to, control and modify a remote computer over the Internet by encrypting the communication.

5.- DIAGRAMS

Once the requirements for the planning and design of the FRS have been determined, the following diagrams are implemented.

5.1.- Entity-relationship model

The model entity-relationship model facilitates data modelling to obtain a representation of the most relevant entities of the system, including their interdependencies and characteristics. The model has the following components.

Entity. Objects or things that are different from each other. Graphically, they are represented by a rectangle.

Relationship. It consists of grouping two or more entities. Each relationship is assigned a name that distinguishes it from the others. Its graphic representation is the rhombus.

<<One to one (1:1)>> For each event that appears in an entity, there is a maximum of one event in the entity to which it is related.

<<One to many (1:M)>> Each event generated from an entity may contain several events with the related entity.

<<Many to many (M:M)>> Each occurrence in one entity may correspond to several occurrences in the other related entity and vice versa.

Attribute: A property contained in an entity or a relationship. In the case of the entity there must be at least one attribute able to uniquely identify the entity by a unique value. In addition, each attribute must have a name that distinguishes it from the others. The following figure sets out the entity-relationship model of the FRS.

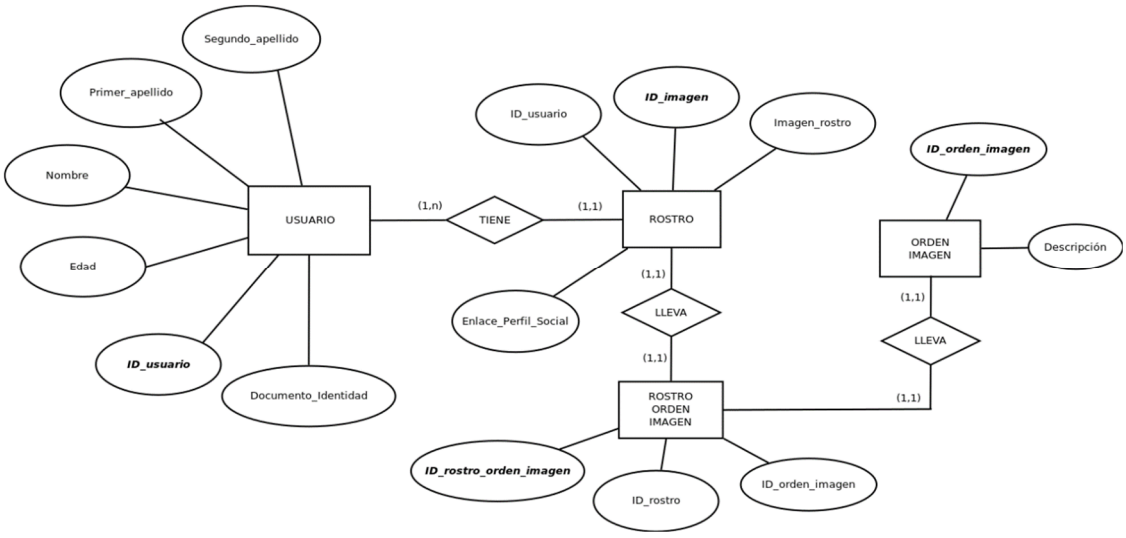

Illustration 2. Entity-Relationship Model of the FRS

5.2.- Relational model

The relational model is used to obtain the modelling of the database. It uses relationships that could be logically thought of as datasets called tuples. It is currently the most widely used model for database management.

This model considers the database as a collection of relationships. A relationship is considered as a table with a set of rows, each row containing a set of fields and each field representing a value.

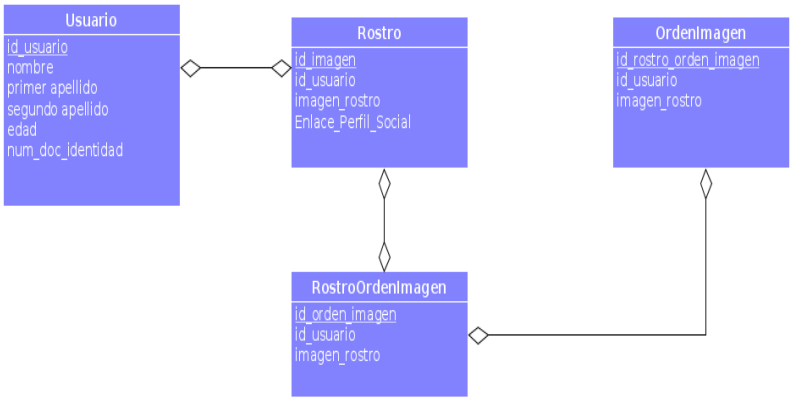

Illustration 3. Relational Model of the FRS

The relational model has the advantage that:

- It ensures non-duplication of records by using unique key fields.
- It enables integrity, so deleting a record deletes all records referenced by and dependent on that record.
- It promotes standardisation by being more understandable and applicable.

5.3.- Context diagram

This diagram is used to define the entities, their boundaries and how they interact within the system.

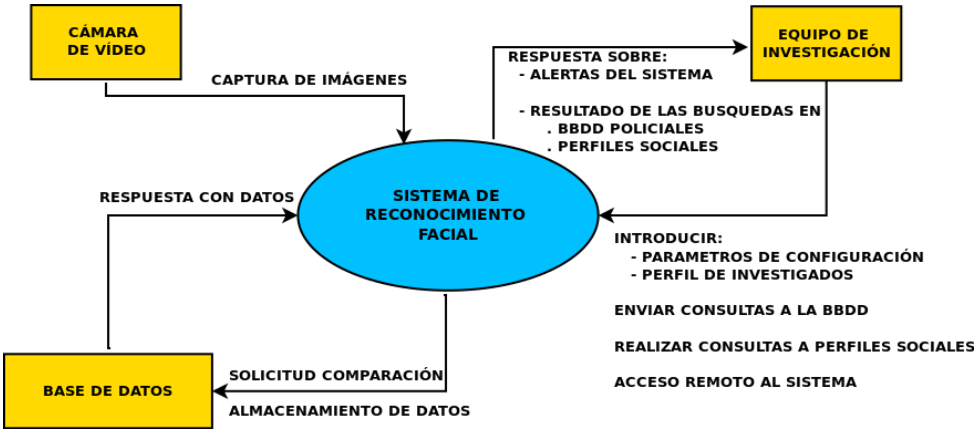

Illustration 4. FRS Context Diagram

5.4.- Use case diagram

Diagram that writes the activities that take place in the FRS. It consists of the following elements.

- *The actors*. Characters or entities interacting with the system.
- *Use case*. A sequence of actions that represents the behaviour when the system interacts with an actor or another use case.
- *Relationships*. Three types of relationships are defined in the use cases.
  - <<*Communicate*>> When there is a relationship from the actor to a use case.
  - <<*Include*>> Occurs when one base use case explicitly integrates the behaviour of another. It is used when you obtain a similar group of features in several cases and you do not want to keep description copies of those features.
  - <<*Extend*>> Occurs if the behaviour of one primary use case implicitly integrates the behaviour of another. It is used when one use case has similar characteristics to another, copying them to the latter.

Use case: Register candidate - verification scenario
Actor: User
Description: The user enters information into the system about a person of interest to the law enforcement.
Normal sequence: 0. Click on the option <<*enter candidate*>>. 1. Enter the name of the device. 2. Enter the identifying information of the person of interest to law enforcement. 3. Add image of the face of the person of interest. You can upload one or more images to the system, until you click on the<<*finish*>>option. 4. Define recipients to be notified in case of recognition.
Exceptions: 1. The device already has a name assigned to it: Change or keep name. 2. The identifying information is in the system: Ask whether you want to edit, keep or delete existing data. 3. An image already exists. Ask if you want to add more images, or delete existing images. 4. There are already recipients assigned to that device. Ask if you want to edit, keep or delete a recipient.

Use case: Check FRS status
Actor: User.
Description: The user wants to know the identity of the persons of interest loaded in the FRS, the name of the device, the battery charge.
Normal sequence: 0. Click on the <<consult *status*>> option. 1. A menu is displayed from which you can select: 1a device name, 1b battery status, 1c recipients to receive notifications, 1d query persons loaded. 2a. The user selects one of the following options. 1a, 1b, 1c. The information about selected option is displayed, with the possibility going back to 2b. The user selects option 1d and a list of each the persons of police interest loaded on the device is displayed. 3. The user selects option 1d.

Use case: Search for profiles on social networks[9].
Actor: User
Description: The user wants to consult the profiles on social networks.
Normal sequence: 0. Click on the option<<*profiles*>>. 1. A window is displayed to enter the path where the images are stored. 2. A window is displayed with options to determine which profiles to search in. 3. The system starts the search for network profiles 4. The result is returned in the form of a link to the profiles found.
Exceptions: 1. No matching profiles are found in the social networks searched. A window is displayed stating that it has not been possible to obtain any results.

Use case: Identification
Actor: User
Description: The user wants to know the identity of the person or persons in an image.
Normal sequence: 0. Click on the option<<*identify*>>. 1. A window for entering the database connection parameters is displayed. 2. A window is displayed to locate the file containing the image. 3. You request the comparison of faces identified in the image with those contained in the database. 4. The system locates the face in an image 4. A result of
Exceptions is returned: 1. It is not possible to connect to the database: A message is issued and it waits for the parameters to be changed until the connection is made.

[9] Section 6.2 goes into more detail on the search for social profiles.

6.- TOOLS FOR PROTOTYPE IMPLEMENTATION

This prototype uses open source hardware and software, which allows a more flexible and economical development and implementation thanks to the availability of the code and schematic circuits and the reduction of costs compared to commercial utilities.

In addition, there is have a large, active community of participants, which has certain advantages, such as the reduction of development time with the reuse of other prototypes, the expansion of applications, connectivity with other systems and the correction of errors.

6.1.- Hardware

Most hardware devices that require high data processing for their operation use a System On a Chip (SOC), where the processor, RAM, input and output controllers as well as storage memory are integrated in a single chip.

There is an extensive range of small-board computers ideal for project development. The best if these is Raspberry Pi, due in part to being the first to be marketed with the free use label, for both private and educational use. It has a large community of users. Since it was first launched in 2011 (Rory Cellan-Jones, 2019), its models have evolved to adapt to current technology.

In the author's opinion, there are better alternatives to this prototype. These are slightly more expensive devices, but with more computing power and therefore higher performance. Such is the case with the Orange Pi 5 model[10]. Its design makes it an optimal product to implement an FRS prototype, highlighting, among its main features, the Rockchip RK3588S octa-core processor. It also supports up to 32 GB of RAM and has an integrated Graphic Process Unit.

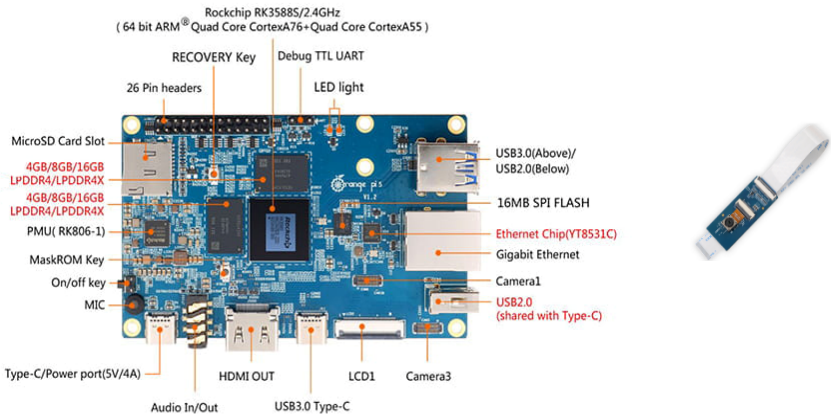

Illustration 4. Orange PI 5 and Orange Pi 13 MP Camera

Video image management is critical for FR, so another strength of this board is its support for hardware-accelerated 8K video playback. It can also be connected to up to 3 cameras.

[10] 10 Best Raspberry Pi alternatives to buy published on 17 February 2023. https://beebom.com/best-raspberry-pi-4-alternatives/ Retrieved 15 March.

Orange Pi 5 is compatible with Arbian, Ubuntu, Debian and Android 12 OS and has its own open source operating system Orange Pi OS.

For this prototype, the *Orange Pi 13 megapixel Camera*[11], which enables high definition video, will be integrated.

For system storage memory, a 64 Gb eMMC memory module[12] is used. This type of memory is small and low power consumption.

The approximate total budget to obtain the complete unit of this prototype is €193.93.

Orange Pi 5 32GB DDR3 Rockchip RK3588S	*€ 152,75*
Orange Pi 13MP camera module – MIPI	*€ 32.89*
TF Card (MicroSD) 8GB	*€ 8.29*
	Total €193.93

6.2.- Software

To manage the board's resources, and to service application programmes, an operating system (OS) must be installed in memory. As already mentioned, there are different operating system options specially adapted to these small-board computers. In this case, Ubuntu Desktop is used.

In addition to the OS, in order to be able to interact with Orange Pi 5 for image capture and processing, some kind of programming language that allows instructions to be used is required. As already mentioned, Python 3.4 is used as the programming language, in addition to the OpenCV library for Python in Ubuntu[13].

7.- RESULTS OBTAINED.

Tests on the prototype[14]have resulted in an FRS capable of detecting and identifying faces.

However, as shown in the illustration below, identification with glasses and mask yielded a negative result, partly because SRFs rely on specific facial features to identify individuals.

[11] http://www.orangepi.org/html/hardWare/cameras/details/orange-pi-13MP-Camera.html. Retrieved 16 March.

[12] eMMC, which stands for embedded Multi-media Card, is a NAND-based flash memory. It integrates the memory chip together with the controller, which makes this memory faster than an SD card.

[13] https://docs.opencv.org/3.4/d2/de6/tutorial_py_setup_in_ubuntu.html. Retrieved 16 March 2023.

[14] The following tutorial has been used to support the implementation of the FRS. https://github.com/informramiz/opencv-face-recognition-python. Retrieved 19 March 2019

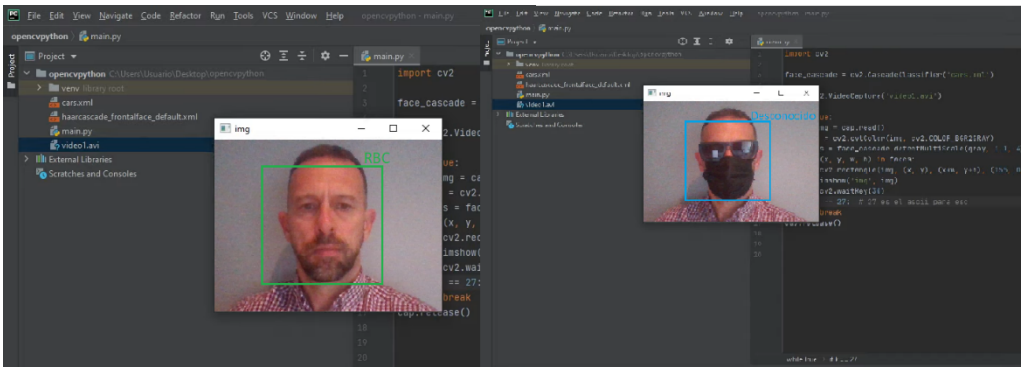

Illustration 6. Results obtained from the FRS prototype.

The presence of a mask may hinder the extraction of these features. However, there are approaches that overcome this pitfall, such as the use of contextual pattern analysis. Thus, in addition to facial features, other elements, such as clothing, walking style and ways of interacting with the environment, are taken into account to help identify people.

CONCLUSIONS

Given the hypothesis set out in the introduction, having conducted a feasibility analysis of the implementation of an FRS in the police field, and having implemented a prototype, it is considered that: the first element of the hypothesis. "SRFs can be used passively, i.e. without the knowledge, consent or participation of the subject". This is subject to compliance with stringent requirements to protect fundamental rights in line with the law.

As for the second element of the hypothesis. "The use of FRS to obtain information of interest to police in the fight against crime". By implementing a pilot, the feasibility of developing an FRS as a useful tool for the SF in the fight against crime has been demonstrated.

At this point, it should be mentioned that, in addition to fulfilling the objective of estimating and resolving the hypothesis set out, it has been possible to obtain not only the design and modelling of an FRS on an ad hoc basis but also the definition of a use case for this policing tool. As well as the implementation of a prototype that fulfils the requirements for the purpose for which this system has been designed.

As future lines of research, this author considers that work is needed improve and promote the use of facial recognition tools in different areas of public safety, through the use of the Tetrapol network15.

Furthermore, it should be remembered that biometric data processing is considered a special category of personal data and therefore subject to additional protection and safeguarding requirements, such as carrying out risk analyses, keeping a register of processing activities and under appropriate security levels. These aspects were not analysed due to the additional time they would have taken.

[15] Tetrapol is a professional digital radio communication system standard focused primarily on providing radio communication services to law enforcement agencies.

The author of this project only hopes that the work developed both at the documentary level and in the implementation of a prototype of the FRS can be considered when deciding to start a project for incorporating facial recognition in police work.

BIBLIOGRAPHY

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF 27 APRIL 2016 ON THE PROTECTION OF NATURAL PERSONS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA.
- EUROPEAN PARLIAMENT RESOLUTION OF 6 OCTOBER 2021ON ARTIFICIAL INTELLIGENCE IN CRIMINAL LAW AND ITS USE BY THE POLICE AND JUDICIAL AUTHORITIES IN CRIMINAL MATTERS
- ORGANIC LAW 4/1997, OF 4 OF AUGUST, WHICH REGULATES THE USE OF VIDEO CAMERAS BY THE FORCES AND CORPS OF SAFETY IN PUBLIC PLACES.
- ORGANIC LAW 7/2021, OF 26 MAY, ON THE PROTECTION OF PERSONAL DATA PROCESSED FOR THE PURPOSES OF THE PREVENTION, DETECTION, INVESTIGATION AND PROSECUTION OF CRIMINAL OFFENCES AND THE EXECUTION OF CRIMINAL SANCTIONS.
- NIKISINS, OLEGS & FUKSIS, RIHARDS & KADIKIS, ARTURS & GREITANS, MODRIS. (2015). FACE RECOGNITION SYSTEM ON RASPBERRY PI. INTERNATIONAL CONFERENCE ON INFORMATION PROCESSING AND CONTROL ENGINEERING. Retrieved 21 May 2023 from: https://www.researchgate.net/publication/275302784_Face_recognition_system_on_Raspberry_Pi
- RORY CELLAN-JONES (5 MAY 2011) ARTICLE TAKEN FROM THE BBC MAY 2011 outlining the launch of the Raspberry Pi, its main features, the developer, its low price (£15). Retrieved 21 May 2023 from: https://www.bbc.co.uk/blogs/thereporters/rorycellanjones/2011/05/a_15_computer_to_inspire_young.html
- VÁZQUEZ, HEYDI & CHANG, LEONARDO & RIZO, DAYRON & MORALES-GONZÁLEZ, ANNETTE. (2012). EVALUACIÓN DE LA CALIDAD DE LAS IMÁGENES DE ROSTROS UTILIZADAS PARA LA IDENTIFICACIÓN DE LAS PERSONAS. COMPUTACIÓN Y SISTEMAS. Retrieved 21 May 2023 from: www.researchgate.net/publication/233733399_Evaluacion_de_la_calidad_de_las_imagenes_de_rostros_utilizadas_para_la_identificacion_de_las_personas.