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

Rafael Bustamante Carrizosa
Teniente de la Guardia Civil
Jefatura de Información

IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL APLICADO A INVESTIGACIONES POLICIALES

IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL APLICADO A INVESTIGACIONES POLICIALES

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.

Abstract: Facial recognition systems are built on computer programs that analyze 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.

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

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

ACRÓNIMOS:

FFCCS: Fuerzas y Cuerpos de Seguridad.
GPU: Graphic Process Unity o unidad de proceso de gráfico
RF: Reconocimiento Facial
RGB: Red Green Blue
SBC: Sigle Board Computer
SO: Sistema Operativo
SOC: System On a Chip
SRF: Sistema de Reconocimiento Facial
SSH: Secure Shell o Interprete de Ordenes Seguro
VPN: Virtual Private Net o Red Privada Virtual
VPU: Vídeo Process Unity o unidad de proceso de vídeo

INTRODUCCIÓN

Sin duda alguna, Internet no solo ha revolucionado la informática y las comunicaciones, sino que también ha cambiado el mundo tal y como se conocía hace 30 años.

Esta revolución tecnológica, ha propiciado además la aparición de una extensa variedad de herramientas electrónicas. El Internet de las Cosas (conocido por sus siglas IoT o Internet of Things) es un nuevo concepto que permite la interconexión de objetos físicos a través de Internet, pudiendo de esta forma programar eventos específicos.

A todo esto, hay que añadir que esta explosión tecnológica ha propiciado una importante evolución en el conocimiento de los diferentes campos de la biometría (huellas dactilares, reconocimiento de iris, reconocimiento facial (RF), reconocimiento de escritura…) convirtiéndola en un elemento clave para la implementación de sistemas con capacidad identificativa.

En la lucha contra elementos desestabilizadores tales como organizaciones criminales y grupos terroristas, las Fuerzas y Cuerpos de Seguridad (FFCCS) en su labor de averiguación y esclarecimiento de hechos delictivos, están obligadas a mantenerse alineadas con las nuevas tecnologías.

Siendo la búsqueda, seguimiento y obtención de información de individuos relacionados con actividades delictivas, una de las principales actividades que han de llevar a cabo las FFCCS con la finalidad de proteger la seguridad ciudadana, es lógico considerar el RF como una potente herramienta para su consecución.

La hipótesis planteada en este trabajo es que los Sistema de Reconocimiento Facial (SRF) pueden ser usados de manera pasiva, esto es, sin el conocimiento, consentimiento o participación del sujeto y con la consecución de un objetivo fundamental. La obtención de información de interés policial en la lucha contra el crimen.

La finalidad de este trabajo es valorar la posibilidad de que las FFCCS dispongan de una herramienta eficaz para perseguir el fenómeno de la delincuencia bajo el amparo de la legalidad normativa. Tratando de identificar, definir y desarrollar los procedimientos

y requisitos necesarios para modelar y diseñar un SRF mediante un caso de uso que permita la implementación de un prototipo.

MODELO Y DISEÑO DEL SRF

1.- APROXIMACIÓN AL MARCO JURÍDICO

Con el auge de la biometría y la inteligencia artificial, el legislador se ha visto forzado a introducir cambios normativos que protejan a la ciudadanía de posibles injerencias en sus derechos fundamentales.

Destaca en este sentido el Reglamento General de Protección de Datos de la Unión Europea, que ha dispuesto que el procesamiento de datos biométricos, incluidos los datos de reconocimiento facial, sea considero una categoría especial de datos personales y por tanto ha de estar sujeta a requisitos adicionales de protección y salvaguarda (Reglamento UE 2016/679).

Por su parte, el Tribunal de Justicia de la Unión Europea ha emitido varias sentencias relevantes[1] en la que establece que el uso de sistemas de reconocimiento facial dentro del ámbito policial, debe cumplir con los principios de proporcionalidad y necesidad.

Más concretamente, según resolución del Parlamento Europeo, "*la aplicación de la Inteligencia Artificial puede ofrecer grandes oportunidades en el ámbito de la garantía del cumplimiento de la ley, en particular en lo que respecta a la mejora de los métodos de trabajo de las autoridades policiales y judiciales y al aumento de la eficacia de la lucha contra determinados tipos de delitos, especialmente los delitos financieros, el blanqueo de capitales y la financiación del terrorismo, los abusos sexuales y la explotación sexual en línea, así como determinados tipos de ciberdelincuencia*" (Parlamento Europeo, 2021).

En España, según se recoge en la Ley Orgánica 4/1997, la competencia en la instalación de videocámaras en lugares públicos, corresponde exclusiva a las FFCCS. En su articulado se establecen además los principios, condiciones y limitaciones para su autorización y uso (Ley Orgánica, 4/1997).

Más recientemente, con la publicación de la Ley Orgánica 7/2021, se estableció que en lugares públicos donde se instalen videocámaras, el responsable del tratamiento deberá llevar a cabo un análisis de los riesgos o una evaluación de impacto de protección de datos según el nivel de perjuicio que se pueda derivar para la ciudadanía y de la finalidad perseguida (Ley Orgánica, 7/2021).

En definitiva, los datos biométricos recogidos por los SRF son considerados de especial protección y su uso por parte de las FFCCS está limitado a fines de prevención, detención o investigación de hechos delictivos, bajo los principios de proporcionalidad, intervención mínima e idoneidad.

1 Fuente: https://curia.europa.eu/jcms/jcms/p1_3252415/es/ Recuperado el 21 de mayo de 2023.

2.- HERRAMIENTAS PARA EL DESARROLLO

Para llevar a cabo el modelado de este SRF, se va a hacer uso de diferentes tipos de diagramas. Su uso ayuda a documentar y detallar de forma más eficiente los procesos y tareas que componen cualquier sistema.

Además del modelado, se va a llevar a cabo el desarrollo de un prototipo de SRF, estableciendo los requisitos, funcionalidades y componentes adecuados. Se procederá con la codificación de funciones utilizando OpenCV[2].

Esta librería[3] se encuentra bajo licencia BSD[4], es multiplataforma y cuenta con numerosas funciones que abordan áreas muy diversas como la inteligencia artificial o el reconocimiento facial.

Para programar el prototipo, se hará uso del lenguaje de programación interpretado y multiplataforma Python. Fue creado a finales de los ochenta por Guido van Rossum en el Centro para las Matemáticas y la Informática (CWI, Centrum Wiskunde & Informática), en los Países Bajos.

Python es un lenguaje con una sintaxis clara y con una de curva de aprendizaje elevada. Cuenta con un amplio respaldo en todo tipo de proyectos gracias a la amplia variedad de sus bibliotecas, por estos motivos se ha convertido en el lenguaje de programación más usado[5].

3.- SUBDIVISIÓN DE FUNCIONES EN EL SRF

Para el desarrollo del prototipo, se han de distinguir los siguientes procesos.

- *Fase de registro*. Esta función es utilizada cuando se trabaja dentro del escenario de verificación. Consiste en dar de alta al usuario o usuarios que han de ser autenticados. Durante esta función se realiza la extracción de los rasgos faciales a los que se les añaden datos identificativos del individuo. Todos estos datos son almacenados en una base de datos.

A través de los rasgos faciales se elaboran las plantillas. Una plantilla permite calcular y obtener una representación univoca del rostro de un individuo.

- *Procesado de imágenes*. Requiere del uso de un dispositivo de captura de imágenes. el procesamiento de imágenes podrá realizarlo de dos formas.
  - *En tiempo real*. La cámara envía al sistema las imágenes capturadas para que éstas sean procesadas en tiempo real.

2 Esta biblioteca fue desarrollada inicialmente por Intel en 1999. Fuente: https://opencv.org Recuperado el 20 de mayo de 2023.
3 Una biblioteca o librería es un conjunto de herramientas codificadas en un lenguaje de programación, e invocadas por programas ejecutables para llevar a cabo alguna tarea.
4 La licencia BSD permite su uso libre tanto para fines comerciales como de investigación.
5 Según el PopularitY of Programming Language Index, Python es utilizado por el 27.91% de los programadores, ocupando la primera posición. Fuente: https://pypl.github.io/PYPL.html. Recuperado el 13 de marzo de 2023.

◦ *Procesado en diferido o forense*. En este caso, el sistema no requiere una conexión directa con la cámara mientras se está produciendo las capturas de imágenes, sino que estas son almacenadas en algún tipo de dispositivo para su posteriormente procesamiento.

- *Detección del rostro.* Una vez capturada la imagen, se requiere conocer si dentro de ésta, existe algún rostro, utilizando algún tipo de clasificador. Este clasificador realiza primero la detección del posible rostro y después el de los ojos. Este orden reduce el tiempo de detección, ya que la búsqueda de los ojos se lleva a cabo dentro de un área reducida, la del rostro.

◦ Detección del rostro. Según los conocimientos extraídos de la observación de rostros, se han determinado características tales como que la zona de los ojos es más oscura que la zona de las mejillas o de la nariz, el seguimiento de los movimientos de la cabeza para detectar si se trata o no de una cara, etc. Toda esta información es utilizada para llevar a cabo la detección del rostro.

◦ Detección de los ojos. Aunque el proceso es similar al de la detección del rostro, su localización adquiere mayor importancia, pues será utilizada en la fase de normalización de la imagen para obtener el ángulo de rotación del rostro a fin de determinar su orientación.

En este prototipo, se va a utilizar el clasificador Haar, puesto que ya se encuentra entrenado para reconocer rostros.

Haar utiliza el enfoque de las ventanas deslizantes. Consisten en el escaneado de la imagen de izquierda a derecha y de arriba a abajo, en diferentes tamaños. A medida que la ventana se mueve de izquierda a derecha y de arriba a abajo, el clasificador intenta determinar si existe alguna cara.

Si el clasificador detecta un rostro, el método devuelve una lista de tuplas que contiene el cuadro delimitador (la ventana) de las caras en la imagen. Esta tupla contiene la ubicación de la cara, la anchura y la altura.

Haar es un algoritmo que subdivide la imagen en secciones rectangulares. Éstas son nuevamente divididas en varias sub-secciones para convertirla en una imagen integral. La imagen integral consiste en la representación de la imagen obtenida mediante la suma de la intensidad (RGB[6]) de los pixeles existentes arriba y a la izquierda de un punto. (Nikisins et al., 2015)

En la siguiente figura el rectángulo mayor se corresponde con la imagen completa mientras que los recuadros representan las imágenes integrales.

[6] RGB (sigla en inglés de red, green, blue, en español «rojo, verde y azul»). Define la composición del color en términos de la intensidad de los colores primarios de la luz.

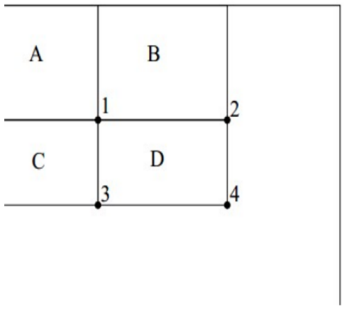

Ilustración 1.- Imagen Integral

A modo de ejemplo, el valor de la imagen integral de la posición 1 es la suma de los píxeles en el rectángulo A. El valor en la ubicación 2 es la suma de los píxeles en A + B, la ubicación 3 es A + C, y la ubicación 4 es A+B+C+D.

Se puede calcular la suma de pixeles en D como: 4+1-(2+3).

- *Normalización de la imagen.* Una vez obtenidas las coordenadas válidas del contorno del rostro, se lleva a cabo una serie de transformaciones en la imagen. La finalidad de la normalización es hacer que la extracción de los rasgos característicos sea más eficiente. Con la normalización la imagen se rota, se escala, se recorte y finalmente se convierte a escala de grises.
  - *Rotación*. El objeto de la rotación es alinear el rostro de forma vertical. Por lo que además de la posición de los ojos obtenidos en la fase de detección, se requiere la localización del punto central de la cara para utilizarlo como eje de rotación. Con estos tres puntos y mediante cálculos trigonométricos, se obtiene el ángulo de rotación.
  - *Escalado*. A través del escalado se consigue un tamaño específico de la imagen del rostro, de tal forma que todos los rostros con los que se trabajen tengan la misma proporción. Según el estándar propuesto por la norma ISO/IEC 19794-5, se aconseja que la distancia entre el centro de los ojos sea como mínimo de 60 píxeles y como máximo 96. (Vázquez et al. 2012). Tomando como referencia ese rango de distancias, se consigue que todas las imágenes tengan proporciones similares, facilitando su comparación.
  - *Recorte*. Consiste en dar a cada imagen la misma dimensión. Al igual que en el escalado, se aplica el estándar indicado por la norma ISO/IEC 19794-5, que marca unas dimensiones de 168 x 192 píxeles.
  - *Escala de grises*. Se trata de conseguir que la representación de la imagen sea lo más uniforme posible, mitigando los cambios de luminosidad que introducen ruido en los algoritmos de extracción de rasgos característicos. Lo que se pretende es que el número de pixeles para cada nivel de grises (0 a 255) sea lo más homogéneo posible.

  Para convertir un pixel de color a escala de grises se realiza un promedio ponderado en la intensidad de cada uno de los tres colores RGB, en donde a cada color se le asigna un valor. Los valores utilizados por OpenCV son gris = 0,2989 * rojo + 0,5870 * verde + 0,1140 * azul.

  Con todas estas operaciones se facilita la comparación entre rostros, se aumenta la información realmente útil y se reduce el ruido.

- *Extracción de características*. De cada imagen se obtiene un conjunto de valores característicos que han de definir con la mayor exactitud posible cada rostro y al mismo tiempo, deben tener la capacidad de discriminar el rostro.

Durante la extracción de características, el algoritmo obtiene los valores que realmente aportan información en relación al rostro, desechando aquella información que no aporta información útil.

- *Comparación.* En esta fase se compara la información obtenida o muestra dubitada con la que ya existía o muestra indubitada. Para calcular la distancia entre cada una de las muestras se utiliza la distancia Euclídea. Durante el proceso de comparación el algoritmo recibe como entrada un registro de identificación y una plantilla, calculando y comparando las distancias entre ellos. El resultado se traduce en un porcentaje que determina la probabilidad de que los dos registros representen a un mismo individuo.

A continuación, se propone un pseudocódigo que esquematiza las diferentes funcionalidades planteadas.

```
INICIO()
    Mientras () Hacer:
        Si (detección cara(imagen)) Entonces;
            imagen := normalizar (imagen);
            imagen := extracción características (imagen);
            resultado := reconocimiento cara (imagen);
            Si  (resultado < umbral) Entonces:
                RECONOCIMIENTO SATISFACTORIO();
```

ESCENARIOS DE TRABAJO

El SRF que se propone tiene una doble funcionalidad, según el sistema sea utilizado como método de identificación o como método de verificación.

Para aclarar estos conceptos se definirá como *<<sujeto no identificado>>* la persona de la cual no se conoce su identidad, *<<persona de interés policial>>* al individuo cuya identidad es conocida y que se interesa su hallazgo y localización, y *<<sujeto identificado>>* aquel individuo en el que se ha producido una coincidencia entre un sujeto no identificado y un individuo registrado en la base de datos policial.

Se define la verificación o autenticación de rostros, la comparación en busca de coincidencias entre un sujeto no identificado y una persona de interés policial. Mientras que se define como tarea de identificación o forense, la búsqueda de un sujeto no identificado entre un conjunto de individuos registrados.

En definitiva, mientras que la verificación realiza el cotejo de una imagen capturada con un rostro almacenado (comparación uno:uno), en la identificación se coteja una imagen capturada con muchos rostros almacenados (comparación uno:muchos).

Enmarcando esos conceptos en el empleo de un SRF aplicado dentro del ámbito de la investigación policial, se precisa identificar dos clases de escenarios. Cada uno

diferenciado por sus necesidades, propiedades y características concretas que serán analizadas en los requerimientos establecidos en el apartado 4.

3.1.- Escenario de verificación o autenticación

Consiste en situar el sistema en una ubicación conocida por la previsible actividad de la persona o personas de interés policial.

El sistema deberá realizar una comparación de cada uno de los rostros capturados por la cámara en la imagen indubitada del rostro de las personas de interés policial y que ha sido previamente almacenada en el sistema.

Este escenario consiste en el procesamiento en tiempo real y si se produce una coincidencia, programar el sistema para que lleve a cabo el envío de forma automatizada de algún tipo de notificación.

3.2.- Escenario de identificación o forense

El sistema en este caso almacena las imágenes obtenidas para su posterior procesamiento, a fin de establecer la detección e identificación de rostros a través de bases de datos policiales.

Este escenario aplica al caso de imágenes de actividades delictivas donde se precisa obtener la identificación de los sujetos involucrados.

4.- ANÁLISIS DE REQUERIMIENTOS

Estos requerimientos van a determinar las condiciones a cumplir por el SRF, teniendo en cuenta los dos escenarios planteados.

Estos requerimientos pueden ser clasificados en requisitos funcionales que describen los procesos de entrada de información en el sistema, su procesamiento y posterior producción de información, y en requisitos no funcionales que están relacionados con las características del sistema, y por tanto se centran en describir la limitación de éste, como por ejemplo la fiabilidad, la capacidad de procesamiento, la velocidad de transferencia de datos, la seguridad, la portabilidad, etc.

4.1.- Requerimientos funcionales

Dado que el sistema ha de poder funcionar tanto en modo verificación como en modo identificación. Para poder definir los requerimientos, es necesario contemplar cada uno de estos escenarios por separado. La figura 3 muestra conceptualmente algunos aspectos que van a ser tratados a continuación.

- *Requerimientos en modo verificación*

- El sistema deberá permitir que se almacene el perfil de las personas de interés policial, para ser comparado en tiempo real.

- Cuando las imágenes son capturadas por la cámara del sistema, éstas se guardarán en algún dispositivo de almacenamiento temporal, desechándose las que lleven más tiempo en el sistema, a fin de que la capacidad de almacenamiento no se colapse.
- En caso de producirse un resultado positivo de alguna persona de interés policial. El sistema deberá almacenar permanentemente las últimas imágenes recogidas por la cámara para permitir su posterior supervisión.
- Tras un resultado positivo, el sistema debe permitir enviar una señal de alerta instantánea.
- Cuando se produzca una señal de alerta, el sistema deberá enviar además la información del evento, incluyendo al menos la ubicación, la fecha y la hora en que se inicia la grabación, la identidad del sujeto, la captura de una o varias imágenes y el nombre del dispositivo que ha obtenido el resultado. Teniendo en cuenta que podría haber más dispositivos operando.

- *Requerimientos en modo identificación*

- Deberá ofrecer la posibilidad de trabajar con imágenes diferidas, independientemente de que hayan sido capturadas por el SRF, como con imágenes capturadas por otros dispositivos.
- Si es el SRF quien realiza la captura de imágenes para ser procesadas de forma diferida, deberá disponer de un registro de eventos en donde se almacenará la información relacionada con las capturas obtenidas. Deberá incluir la ubicación desde donde se inicia la grabación, la fecha y hora de grabación, la duración y el nombre del dispositivo.
- El sistema no gestiona las consultas en tiempo real, pero ha de permitir la posibilidad de conectarse y realizar las correspondientes consultas con bases de datos distribuidas.
- Además de la consulta a bases de datos policiales, el sistema deberá permitir correlacionar las imágenes capturadas con las contenidas en los perfiles de redes sociales, recibiendo del sistema las direcciones webs donde se aloja cada uno de los perfiles de redes sociales encontrados.

4.2.- Requerimientos no funcionales

- El sistema debe contar con una cámara digital integrada, capaz de realizar capturas de imagen.
- Cuando el sistema trabaja en modo verificación, debe poder procesar las imágenes en tiempo real capaz de:

  - Localizar cada uno de los rostros que se encuentren en el escenario.
  - Comparar cada uno de ellos con la persona de interés policial almacenadas en el sistema.
  - Generar los correspondientes eventos.
- Deberá disponer de un ancho de banda adecuado para enviar datos en el escenario de verificación al producirse un resultado positivo.
- El dispositivo ha de ofrecer la posibilidad de geo posicionarse.

- El sistema debe ser accesible remotamente para permitir su consulta y gestión, por lo que dispondrá de una conexión segura por VPN[7] (Virtual Private Net) y de una consola SSH[8] (Secure Shell).
- La disponibilidad es un factor importante, por lo que el sistema deberá enviar eventos relacionados con el nivel de carga de la batería y el espacio de memoria disponible cuando se rebasen los umbrales recomendados.

5.- DIAGRAMAS

Una vez determinados los requisitos, para la planificación y el diseño del SRF, se procede a implementar los siguientes diagramas.

5.1.- Modelo entidad-relación

El modelo entidad-relación facilita el modelado de datos a fin de obtener una representación de las entidades más notables del sistema a representar, incluyendo sus interdependencias y características. Este modelo cuenta con los siguientes componentes.

Entidad. Representa objetos o cosas diferentes entre sí. Gráficamente se representan a través de un rectángulo.

Relación. Consiste en la agrupación de dos o más entidades. A cada una de estas relaciones se le asigna un nombre que lo diferencie de los demás. Su representación gráfica es el rombo.

<<Uno a uno (1:1)>> De cada suceso que aparezca en una entidad le corresponde como máximo un suceso de la entidad con la que tenga relación.

<<Uno a Mucho (1:N)>> De cada suceso que se genere de una entidad le puede contener varias con la entidad que guarda relación.

<<Muchos a muchos (N:M)>> De cada suceso que se produzca en una entidad puede corresponder varias de la otra entidad relacionada y viceversa.

Atributo: Determina una propiedad contenida en una entidad o en una relación. En el caso de la entidad debe haber al menos un atributo capaz de identificarla de forma unívoca mediante un valor único. Además, cada uno de los atributos debe disponer de un nombre que lo diferencie del resto. En la siguiente figura se establece el modelo entidad-relación del SRF.

[7] Una VPN permite conectar varios dispositivos como si se encontrasen físicamente en el mismo lugar, emulando las conexiones de redes locales. Se dice que es virtual, porque conecta dos redes físicas; y privada, porque solo los equipos que forman parte de una red local de uno de los lados de la VPN pueden acceder.

[8] SSH es un protocolo de administración remota que ofrece la posibilidad de conectarse, controlar y modificar un equipo remoto a través de Internet cifrando la comunicación.

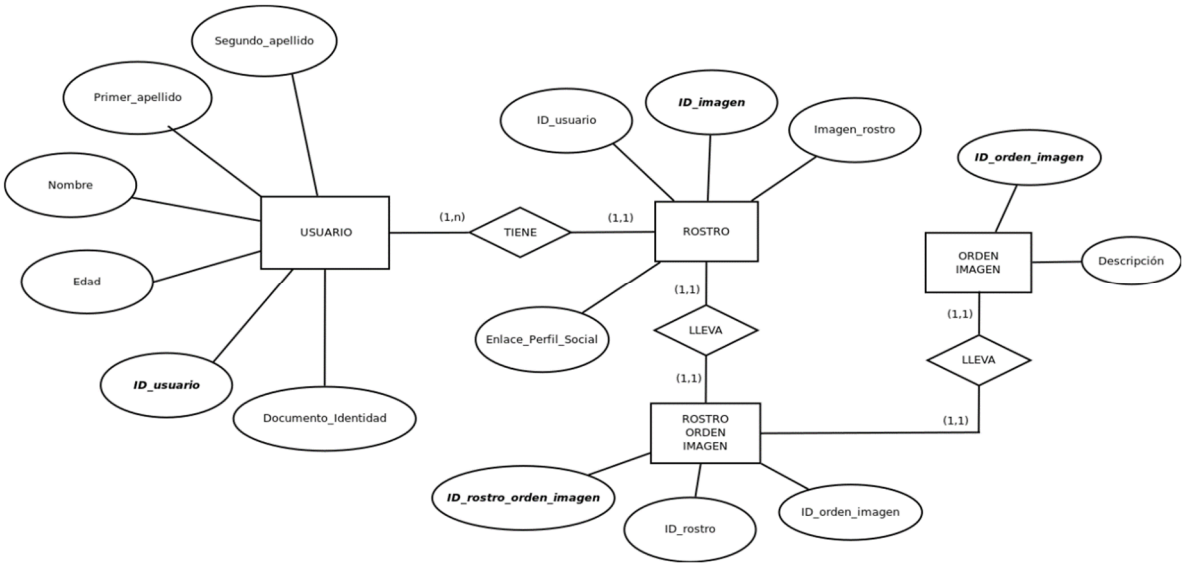

Ilustración 2.- Modelo Entidad-Relación del SRF

5.2.- Modelo relacional

Con el modelo relacional es posible obtener el modelado de la base de datos. Se centra en la utilización de relaciones que podrían considerarse en forma lógica como conjuntos de datos llamados tuplas. Es a día de hoy el modelo más usado para la gestión de las bases de datos.

Este modelo considera la base de datos como una colección de relaciones. Una relación se considera como una tabla con un conjunto de filas, cada fila contiene un conjunto de campos y cada uno de estos representa un valor.

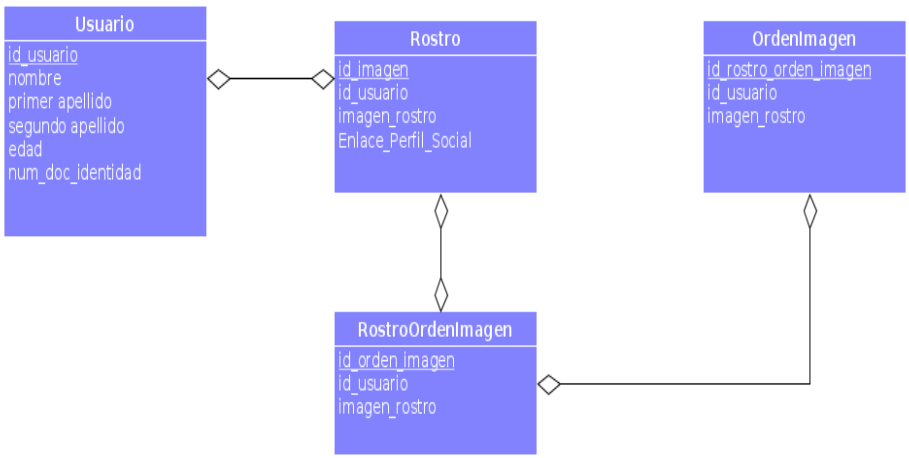

Ilustración 3.- Modelo Relacional del SRF

El modelo relacional tiene la ventaja de que:

- Permite que no se produzca la duplicidad en los registros, utilizando para ello los campos de clave única.
- Posibilita la integridad, así al borrar un registro se borran todos los registros referenciados y dependientes de aquel.
- Favorece la normalización por ser más comprensible y aplicable.

5.3.- Diagrama de contexto

Este diagrama es utilizado para definir las entidades, sus límites y la forma que estos interactúan dentro del sistema.

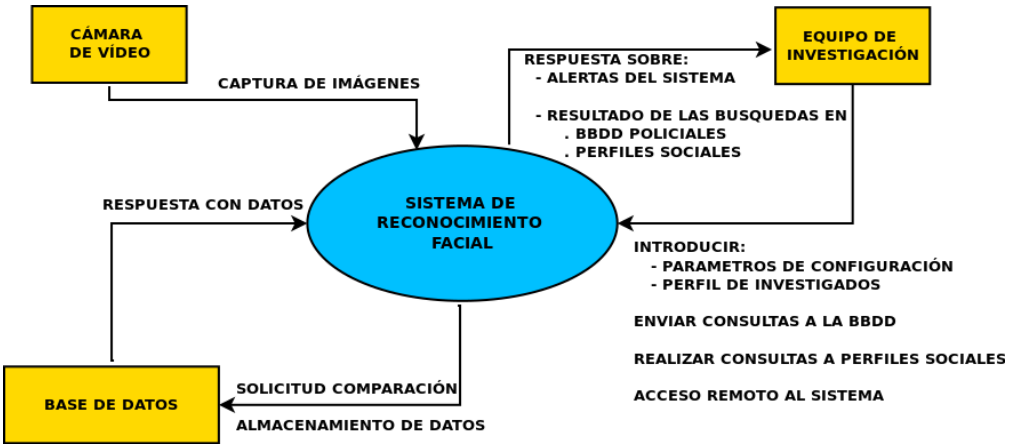

Ilustración 4.- Diagrama del contexto del SRF

5.4.- Diagrama de casos de uso

Diagrama que escribe las actividades que se producen en el SRF. Consta de los siguientes elementos.

- *Los actores*. Personajes o entidades que interactúan con el sistema.
- *Caso de uso*. Secuencia de acciones que representa el comportamiento cuando el sistema interactúa con un actor o con otro caso de uso.
- *Relaciones*. Se definen tres tipos de relaciones en los casos de uso.
  - <<*Communicate*>> Cuando existe una relación desde el actor hacia un caso de uso.
  - <<*Include*>> Se produce cuando un caso de uso base incorpora explícitamente el comportamiento de otro. Se utiliza al obtener un grupo de características similares a varios casos y no se quiere mantener copias de descripción de esas características.
  - <<*Extend*>> Ocurre si el comportamiento de un caso de uso primario incorpora de forma implícita él de otro. Se utiliza cuando un caso de uso tiene características similares a otro, copiándolas a este último.

Caso de uso: Registrar candidato – escenario de verificación
Actor: Usuario
Descripción: El usuario introduce información en el sistema sobre una persona de interés policial.
Secuencia normal: 0. Pulsar sobre la opción <<*introducir candidato*>>. 1. Introducir el nombre del dispositivo. 2. Introducir datos identificativos de la persona de interés policial. 3. Añadir imagen del rostro de la persona de interés policial. El sistema permite subir una o varias imágenes, hasta pulsar la opción <<*finalizar*>>. 4. Definir destinatarios que reciban aviso en caso de reconocimiento.
Excepciones: 1. El dispositivo ya tiene un nombre asignado: Modificar o mantener nombre. 2. Los datos identificativos se encuentran en el sistema: Preguntar si se quiere modificar, mantener o eliminar los datos existentes. 3. Ya existe una imagen. Preguntar si se quiere añadir más imágenes, o eliminar las imágenes existentes. 4. Ya existen destinatarios asignados a ese dispositivo. Preguntar si se quiere modificar, mantener o eliminar algún destinatario.

Caso de uso: Consultar estado SRF
Actor: Usuario.
Descripción: El usuario quiere conocer la identidad de las personas de interés policial cargadas en el SRF, el nombre del dispositivo, la carga de la batería.
Secuencia normal: 0. Pulsar sobre la opción <<*consultar estado*>> 1. Se despliega un menú donde se puede seleccionar: 1a. nombre del dispositivo, 1.b estado de la batería, 1.c destinatarios que recibirán notificaciones, 1.d consulta de personas cargadas. 2a. El usuario selecciona alguna de las siguientes opciones. 1.a, 1.b, 1.c. Se visualiza la información correspondiente a la opción seleccionada, con la posibilidad de retornar al paso 2b. El usuario selecciona la opción 1.d. se muestra un listado de cada una de las personas de interés policial cargada en el dispositivo 3. El usuario selecciona la opción 1.d.

Caso de uso: Búsqueda de perfiles en redes sociales[9].
Actor: Usuario
Descripción: El usuario quiere consultar los perfiles en redes sociales.
Secuencia normal: 0. Pulsar sobre la opción <<*perfiles*>> 1. Se despliega una ventana para introducir la ruta donde se encuentran las imágenes 2. Se despliega una ventana con opciones para determinar en qué perfiles buscar. 3. El sistema inicia la búsqueda de perfiles en red 4. Se devuelve el resultado en forma de enlace a los perfiles encontrados
Excepciones: 1. No se encuentran perfiles coincidentes en las redes sociales buscadas. Se muestra una ventana de que no ha sido posible obtener ningún resultado.

Caso de uso: Identificación
Actor: Usuario
Descripción: El usuario quiere conocer la identidad de la persona o personas que aparecen en una imagen.
Secuencia normal: 0. Pulsar sobre la opción <<*identificar*>> 1. Se despliega una ventana para introducir los parámetros de conexión a la base de datos. 2. Se despliega una ventana para ubicar el archivo que contiene la imagen. 3. Se ordena la comparación de rostros identificados en la imagen con los contenidos en la base de datos. 4. El sistema localiza el rostro en una imagen 4. Se devuelve el resultado de
Excepciones: 1. No es posible conectar con la base de datos: Se emite un mensaje y se espera a que los parámetros sean modificados hasta que se produzca la conexión.

6.- HERRAMIENTAS PARA LA IMPLEMENTACIÓN DEL PROTOTIPO

Para acometer este prototipo se utilizan medios hardware y software de distribución libre que permiten un desarrollo e implementación más flexible y económico gracias a la disponibilidad del código y circuitos esquemáticos y a la reducción de costes en comparación con utilidades comerciales.

Además, cuentan con una comunidad amplia y activa de participantes, lo que aporta ciertas ventajas, como la reducción de tiempo de desarrollo con la reutilización de otros prototipos, la expansión de aplicaciones, conectividad con otros sistemas y la corrección de errores.

[9] En el apartado 6.2 se profundizará en la búsqueda de perfiles sociales.

6.1.- Hardware

La mayor parte de dispositivos hardware que requieren un elevado procesamiento de datos para su funcionamiento utilizan un sistema en chip o SOC (del inglés System On a Chip), en un único chip se integra el procesador, la memoria RAM, los controladores de entrada y salida, así como la memoria de almacenamiento.

Existe una amplia oferta de ordenador de placa reducida ideales para el desarrollo de proyectos. De todos, el más conocido es Raspberry Pi, debido en parte a ser el primero en comercializarse con la etiqueta de uso libre, tanto para uso particular como educativo. Cuenta con una amplia comunidad de usuarios. Desde su primer lanzamiento en 2011 (Rory Cellan-Jones, 2019) sus modelos han ido evolucionando adaptándose a la tecnología actual.

Existe, a juicio del autor, alternativas más recomendables para este prototipo. Se trata de dispositivos ligeramente más costosos, pero con mayor potencia de cálculo y por tanto mayor rendimiento. Como es el caso del modelo Orange Pi 5[10]. Su diseño lo convierten en un producto óptimo para implementar un prototipo de SRF, destacando entre sus características principales, el procesador octa-core Rockchip RK3588S. Soporta además hasta 32 GB de memoria RAM y lleva integrada una Unidad de Procesamiento Gráfica o GPU (del inglés Graphic Process Unity).

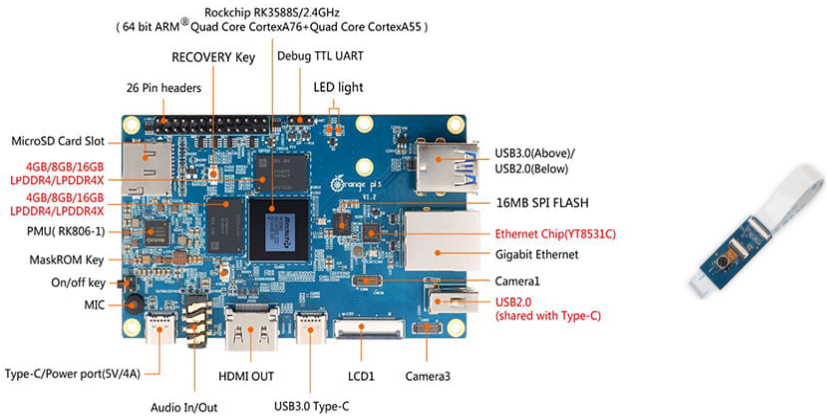

Ilustración 4.- Orange PI 5 y Cámara Orange Pi 13 MP

Para el RF, es fundamental la gestión de imágenes de vídeo, por lo que otro punto fuerte de esta placa es su adaptabilidad a reproducción de vídeo de 8K acelerada por hardware. Permite además la conexión de un máximo de 3 cámaras.

Orange Pi 5 es compatible con los SO Arbian, Ubuntu, Debian y Android 12 e incluye su propio sistema operativo de código abierto Orange Pi OS.

[10] 10 Best Raspberry Pi alternatives to buy publicado el 17 de febrero de 2023. https://beebom.com/best-raspberry-pi-4-alternatives/ Recuperado el 15 de marzo.

Para este prototipo, se va a integrar la cámara *Orange Pi 13 megapixel Camera*[11], que permite obtener videos de alta definición.

Para la memoria de almacenamiento del sistema, se va a utilizar un módulo de memoria eMMC[12] de 64 Gb. Este tipo de memoria es de reducido tamaño y consumo.

El total del presupuesto aproximado para obtener la unidad completa de este prototipo es de 193,93 €.

Orange Pi 5 32GB DDR3 Rockchip RK3588S	*152,75 €*
Módulo de la cámara Orange Pi 13MP - MIPI	*32,89 €*
Tarjeta TF (MicroSD) 8GB	*8,29 €*
	Total 193,93 €

6.2.- Software

Para gestionar los recursos de la placa, y dar servicio a los programas de aplicación, es necesario instalar en memoria un sistema operativo (SO). Como ya se ha mencionado, existen diferentes opciones de sistemas operativos especialmente adaptados a estos ordenadores de placa reducida. En el caso que nos ocupa, se va a utilizar Ubuntu Desktop.

Además del SO, para poder interactuar con Orange Pi 5 para la captura y el procesado de imágenes, se precisa utilizar algún tipo de lenguaje de programación que permita emplear instrucciones. Como ya se comentó, se va a utilizar Python 3.4 como lenguaje de programación, además de la librería OpenCV para Python en Ubuntu[13].

7.- RESULTADOS OBTENIDOS.

Con las pruebas realizadas en el prototipo[14], se ha conseguido obtener un SRF capaz de detectar e identificar rostros.

No obstante, como se muestra en la siguiente ilustración, la identificación con gafas y mascarilla arrojó un resultado negativo, debido en parte a que los SRF se basan en características faciales específicas para identificar personas.

[11] http://www.orangepi.org/html/hardWare/cameras/details/orange-pi-13MP-Camera.html. Recuperado el 16 de marzo.

[12] eMMC de las siglas embedded Multi-media Card, es una memoria flash basada en NAND. Integra el chip de memoria junto con el controlador, esto permite que la velocidad de esta memoria sea mejor que la de una tarjeta SD.

[13] https://docs.opencv.org/3.4/d2/de6/tutorial_py_setup_in_ubuntu.html. Recuperado el 16 de marzo de 2023.

[14] Como apoyo a la implementación del SRF se ha usado el siguiente tutorial. https://github.com/informramiz/opencv-face-recognition-python. Recuperado el 19 de marzo de 2019

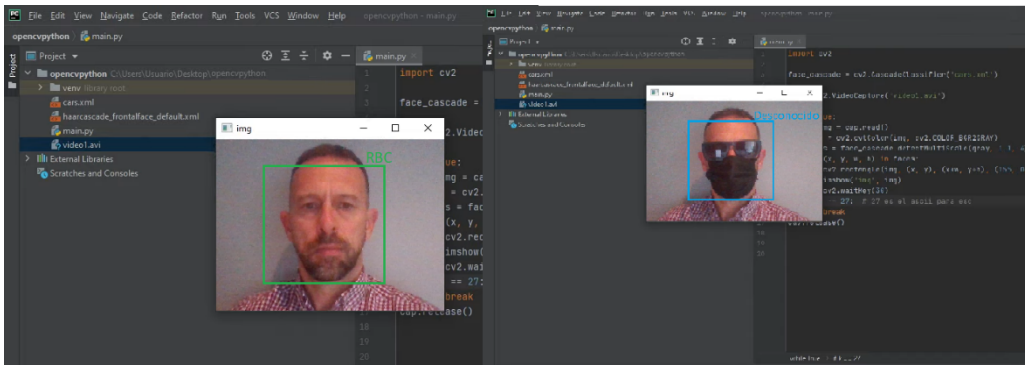

Ilustración 6.- Resultados obtenidos del prototipo de SRF

La presencia de una mascarilla puede dificultar la extracción de esas características. No obstante, existen enfoques que solucionan este escollo, como el uso de análisis de patrones contextuales. Así, además de las características faciales, se tiene en cuenta otros elementos, como la ropa, el estilo de caminar o la forma de interactuar con el entorno, para ayudar a la identificación de personas.

CONCLUSIONES

Dada la hipótesis expuesta en la introducción, habiendo realizado un análisis de viabilidad de la implantación de un SRF en el ámbito policial, e implementado un prototipo, se considera que: el primer elemento de la hipótesis. "*Los SRF pueden ser usados de manera pasiva, esto es, sin el conocimiento, consentimiento o participación del sujeto*". Este hecho queda limitado al cumplimiento de rigurosos requisitos de protección de derechos fundamentales en línea con la legislación vigente.

En cuanto al segundo elemento de la hipótesis. "*El uso de SRF en la obtención de información de interés policial para la lucha contra el crimen"*. Ha quedado demostrado mediante la implementación de un piloto, la viabilidad de desarrollar un SRF que proporcione una herramienta de utilidad a las FFCCS en la lucha contra la comisión de actividades delictivas.

Es preciso mencionar en este punto que, además de cumplir con el objetivo de estimar y resolver la hipótesis ya expuesta. Se ha conseguido obtener no solo el diseño y el modelado de un SRF sobre una base ad hoc. Sino también la definición de un caso de uso de esta herramienta policial. Así como la implementación de un prototipo que cumpla con las características propias para la finalidad con la que se ha diseñado este sistema.

Como futuras líneas de investigación, este autor considera que se debería trabajar en mejorar y potenciar el uso de herramientas de reconocimiento facial en los diferentes ámbitos de la seguridad ciudadana, a través de la utilización de la red Tetrapol[15].

Además, hay que considerar que el procesamiento de datos biométricos, es considero una categoría especial de datos personales y por tanto sujeta a requisitos

[15] Tetrapol es un estándar de sistema de radiocomunicaciones digitales profesionales enfocado principalmente para dar servicio de radiocomunicación a fuerzas y cuerpos de seguridad.

adicionales de protección y salvaguarda, tales como la realización de análisis de riesgos, mantenimiento de un registro de actividades de tratamientos y bajo unos niveles de seguridad adecuados. Aspectos que no han sido posibles tener en cuenta debido a la extensión que supondría.

El autor de este proyecto, solo espera que el trabajo desarrollado tanto a nivel documental, como en la puesta en funcionamiento de un prototipo de SRF, pueda ser tenido en cuenta a la hora de decidir iniciar un proyecto de implementación de reconocimiento facial propio en el ámbito policial.

BIBLIOGRAFÍA

- REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS
- RESOLUCIÓN DEL PARLAMENTO EUROPEO, DE 6 DE OCTUBRE DE 2021, SOBRE LA INTELIGENCIA ARTIFICIAL EN EL DERECHO PENAL Y SU UTILIZACIÓN POR LAS AUTORIDADES POLICIALES Y JUDICIALES EN ASUNTOS PENALES
- LEY ORGÁNICA 4/1997, DE 4 DE AGOSTO, POR LA QUE SE REGULA LA UTILIZACIÓN DE VIDEOCÁMARAS POR LAS FUERZAS Y CUERPOS DE SEGURIDAD EN LUGARES PÚBLICOS.
- LEY ORGÁNICA 7/2021, DE 26 DE MAYO, DE PROTECCIÓN DE DATOS PERSONALES TRATADOS PARA FINES DE PREVENCIÓN, DETECCIÓN, INVESTIGACIÓN Y ENJUICIAMIENTO DE INFRACCIONES PENALES Y DE EJECUCIÓN DE SANCIONES PENALES.
- NIKISINS, OLEGS & FUKSIS, RIHARDS & KADIKIS, ARTURS & GREITANS, MODRIS. (2015). FACE RECOGNITION SYSTEM ON RASPBERRY PI. INTERNATIONAL CONFERENCE ON INFORMATION PROCESSING AND CONTROL ENGINEERING. Recuperado el 21 de mayo de 2023 de: https://www.researchgate.net/publication/275302784_Face_recognition_system_on_Raspberry_Pi
- RORY CELLAN-JONES (5 DE MAYO DE 2011) ARTÍCULO EXTRAÍDO DE LA BBC DE MAYO DE 2011 donde se expone el lanzamiento de la Raspberry Pi, sus características principales, el desarrollador, su bajo precio (15£). Recuperado el 21 de mayo de 2023 de: 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. Recuperado el 21 de mayo de 2023 de: www.researchgate.net/publication/233733399_Evaluacion_de_la_calidad_de_las_imagenes_de_rostros_utilizadas_para_la_identificacion_de_las_personas