Universidad de Granada
Grado en Ingeniería Informática

Periféricos y Dispositivos de Interfaz Humana

Trabajo de Teoría - 2021

EL RECONOCIMIENTO FACIAL

Alumnos: Irene Muñoz y Juan Carlos Pineda

Introducción:

Dentro de la visión por computador, el reconocimiento de caras se ha convertido en uno de los problemas que más esfuerzo investigador ha generado en los últimos años. El objetivo no es reconocer la cara en sí, sino la identidad de la persona. Del mismo modo que la cara es un atributo intrínseco a cada persona, también pueden utilizarse otras características como la voz o el iris. La cara es, sin embargo, el atributo que más usamos los humanos a la hora de reconocer a nuestros semejantes. Además, a diferencia de con el iris, adquirir imágenes de una cara es relativamente fácil y no supone esfuerzo por parte del individuo. Aunque para nosotros reconocer caras no supone apenas esfuerzo, el problema es muy difícil de resolver desde un punto de vista computacional. Cada mínimo cambio de luz ambiental, de expresión de la cara, de posición, inclinación, pelo, etc. supone una imagen totalmente distinta. De hecho, nunca obtendremos dos imágenes iguales de una misma cara. La mayor dificultad del reconocimiento de caras está precisamente en lograr reconocer la identidad independientemente de la luz, posición, etc.

Definición:

El **reconocimiento facial** es una tecnología capaz de identificar o verificar a un sujeto a través de una imagen, vídeo o cualquier elemento audiovisual de su rostro. Esto es posible mediante un análisis biométrico de las características faciales del sujeto (medidas corporales de cara y cabeza) pero extraídas de la imagen o de un fotograma clave de una fuente de vídeo, y comparándolas con una base de datos.

El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara "desconocida", o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes "conocidas", o imágenes de entrenamiento. La gran dificultad añadida es la de conseguir que este proceso se pueda realizar en tiempo real. El sistema identificará las caras presentes en imágenes o videos automáticamente. Puede operar en dos modos:

- **Verificación o autenticación de caras:** compara una imagen de la cara con otra imagen con la cara de la que queremos saber la identidad. El sistema confirmará o rechazará la identidad de la cara (por ejemplo, un sistema de reconocimiento facial de un móvil).

- **Identificación o reconocimiento de caras:** compara la imagen de una cara desconocida con todas las imágenes de caras conocidas que se encuentran en la base de datos para determinar su identidad.

Por su naturaleza amigable, este tipo de sistemas siguen siendo atractivos a pesar de la existencia de otros métodos muy fiables de identificación personal biométricos, como el análisis de huellas dactilares y el reconocimiento del iris.

Fases:

El reconocimiento facial consta de cuatro fases:

1. **Capturar la imagen:** El primer paso es el de capturar la imagen de la persona que va a ser identificada. Aunque bien es cierto que con una toma de imagen frontal de calidad se obtienen mejores resultados, el avance de esta tecnología permite que variaciones en la posición del rostro o utilizando imágenes sin una alta definición se puedan obtener resultados fiables. Al capturar la imagen no es necesario un dispositivo fotográfico especial, ya que en esta tecnología tiene mayor importancia el software empleado.

2. **Análisis de la imagen:** El siguiente paso es la extracción de características faciales para obtener la información biométrica y así poder realizar un análisis y poder conformar un patrón biométrico facial. En el rostro humano hay una gran cantidad de puntos característicos como la distancia de los ojos o la forma de los pómulos, que son determinantes para calcular la huella facial que es única en cada persona. En este proceso, se utiliza la inteligencia artificial y *machine learning* para alcanzar un alto grado de fiabilidad en los resultados.

3. **Comparar la imagen:** Para realizar la comparación se suelen utilizar imágenes en 2D pues permiten una mayor y mejor combinación, y así acceder a bases de datos u otras fuentes de comparación. En esta fase se comparan las huellas faciales de la foto tomada en el proceso de identificación con las fotos que se dispongan en bases de datos. Estas bases de datos pueden ser privadas de la organización o empresa, o públicas (como las fotos de Facebook o Instagram, por ejemplo).

4. **Toma de decisión:** La parte final del proceso es la toma de la decisión de qué foto coincide en mayor porcentaje o tiene mayor similitud. De esta forma se podrá identificar a las personas con un alto grado de fiabilidad.

Técnicas:

La primera solución que se tomó históricamente consistía básicamente en extraer de la imagen de la cara una serie de medidas identificativas, como la distancia entre los ojos, tamaño de la boca, distancia nariz-boca, etc. De esta forma, para cada individuo a reconocer se tiene un rango posible de estos parámetros. Ante una imagen a reconocer, se medirían estos parámetros y se compararían con los

previamente almacenados. Esta aproximación al problema consiguió dar resultados relativamente buenos, pero resultaba muy compleja y poco robusta. Muchas veces era necesario hacer las mediciones manualmente (un operador medía las distancias sobre una imagen en pantalla), lo cual era muy tedioso. Cuando se trataba de automatizar este proceso siempre surgían problemas de precisión, pues las mediciones degeneraban enormemente dependiendo de la luz, expresión, etc.

Otra aproximación al problema, más reciente, consiste en utilizar como parámetros imágenes que representan partes importantes de la cara, desde el punto de vista del reconocimiento. La técnica más representativa de esta aproximación es la de las **autocaras** (eigenfaces). Con la técnica de autocaras, se utilizan como representación imágenes como las que aparecen en la siguiente figura:

En este tipo de imágenes, las zonas más claras y más oscuras representan zonas que tienen mayor importancia de cara al reconocimiento. Las imágenes que sirven de representación se obtienen automáticamente en base a un conjunto de imágenes de caras de entrenamiento. Esta aproximación ha demostrado que es no solo menos tediosa y compleja, sino que en ciertas condiciones permite obtener mejores resultados que con la aproximación anterior. Por ello, es la vertiente más estudiada en la actualidad.

También contamos con el **método LDA**, que permite utilizar la información entre miembros de la misma clase (imágenes de la misma persona) para desarrollar un conjunto de vectores de características donde las variaciones entre las diferentes caras se enfatizan mientras que los cambios debidos a la iluminación, expresión facial y orientación de la cara no. Es decir, maximiza la varianza de las muestras entre clases, y la minimiza entre muestras de la misma clase.

La **técnica FLD** es equivalente al LDA. Los resultados obtenidos con FLD son bastante mejores que los que podemos obtener con autocaras, sobre todo cuando las condiciones lumínicas varían entre el conjunto de imágenes de entrenamiento y de test, y también con cambios de expresión facial, dando más peso a zonas como los ojos, la nariz o las mejillas que a la boca, porque son zonas más invariables en las diferentes expresiones que puede tener una persona.

Últimamente ha incrementado la tendencia del **reconocimiento facial tridimensional**, donde se utilizan imágenes 3D tanto en el entrenamiento como en el reconocimiento. Esta técnica utiliza sensores en 3D para captar información sobre la forma de la cara. Esta información se utiliza posteriormente para identificar rasgos característicos del rostro como por ejemplo la barbilla, el contorno de los ojos, la nariz o los pómulos, y reteniendo información espacial, aparte de la textura y la profundidad. Una ventaja del reconocimiento facial en 3D es que no les afectan los cambios de iluminación, como pasa en el caso de otras

técnicas. Además, otro punto a favor es que pueden reconocer una cara en diferentes ángulos, incluso de perfil. El problema es que es difícil obtener imágenes 3D fidedignas en la fase de reconocimiento, ya que los sensores 3D tienen que estar muy bien calibrados y sincronizados para adquirir la información correctamente. Es por eso que se utiliza el método de Análisis de Componentes Principales Parcial, donde se utilizan imágenes en 3D en la fase de entrenamiento y en la base de datos, pero en la fase de test puede utilizar tanto imágenes en 2D como en 3D. La técnica intenta reconstruir modelos faciales en 3D a partir de múltiples imágenes de la misma persona adquiridas mediante un sistema multicámara o a partir de aparatos 3D. Las imágenes 3D son imágenes de 180° en coordenadas cilíndricas.

Casos de uso:

Para controlar el acceso a un espacio, para pagar, para desbloquear el teléfono, para iniciar sesión en aplicaciones... El reconocimiento facial está cada vez más extendido en todo el mundo y también en España, aunque su uso no siempre se publicita (el reciente caso de Mercadona es una excepción). Tampoco se publicita de dónde salen esas imágenes que nutren las bases de datos con las que comparar las que toman las cámaras para el reconocimiento facial ni está nunca lo suficientemente claro para qué quiere una empresa o administración almacenar nuestro rostro.

Nuestro país carece de una normativa específica y se atiene a lo que indica el Reglamento europeo de Protección de Datos (RGPD), que aun siendo muy estricto en la salvaguarda de los derechos de los ciudadanos deja resquicios a diferentes interpretaciones de qué se puede hacer y qué no. En la legislación española el RGPD se desarrolla en la Ley Orgánica 3/2018, en la que no aparece un apartado específico sobre el reconocimiento facial y la única mención a datos biométricos tiene que ver con su tratamiento (al igual que sucede con otros aspectos de identificación personal, es muy restringido, salvo consentimiento expreso, en línea con lo que postula el RGPD).

Desde hace más o menos un año un grupo de expertos en inteligencia artificial de la Unión Europea trabaja en cómo adaptar la normativa actual a los retos que plantea el uso de datos biométricos y especialmente cómo se protege esa información tan sensible. Entre otros aspectos una futura modificación del RGPD podría incluir el consentimiento del ciudadano y una justificación legal para tomar y archivar imágenes del rostro y que las personas sepamos quiénes y por qué acceden a esas fotografías nuestras.

El uso del reconocimiento facial se centra en la verificación o autenticación de rostros y, con ello, de personas. Esta tecnología se utiliza, por ejemplo, en situaciones como:

- **Segundo factor de autenticación**, para añadir un extra de seguridad, en cualquier proceso de login (inicio de sesión).
- **Acceso a una aplicación** móvil sin necesidad de contraseña.

- **Acceso a servicios online** previamente contratados (inicio de sesión en plataformas online, por ejemplo.).
- **Acceso a un recinto** (oficinas, eventos, instalaciones de cualquier tipo...).
- **Método de pago**, tanto en tiendas físicas como online.
- **Acceso a un dispositivo bloqueado**.
- **Check-in en servicios turísticos** (Aeropuertos, hoteles...).

Algunos ejemplos concretos:

Control de accesos:

Una de las aplicaciones más importantes y que supone un gran avance para el sector, es el uso del **reconocimiento facial para el control de accesos**. Utilizando esta tecnología, las empresas garantizan que el acceso de sus empleados se realiza de forma segura, rápida y real.

Con el uso del reconocimiento facial en los controles de acceso de una organización o empresa se podrá:

- Conocer quién accede y cuándo.
- Garantizar los accesos sólo a personas autorizadas.
- Acelerar los procesos de entrada y salida del trabajo.
- Controlar el acceso a todas las instalaciones como parkings, almacenes, oficinas, edificios, etc.
- Evitar robos y suplantación de identidad.

Videovigilancia:

Dentro de la seguridad y la videovigilancia, el uso del reconocimiento facial permite **identificar a las personas de manera automática con un alto grado de fiabilidad**. De esa forma se incrementa el nivel de seguridad al reconocer fácilmente a personas no autorizadas, que se encuentren en una lista negra, y otras situaciones similares.

Los cuerpos de seguridad del estado utilizan este tipo de tecnología para detectar delincuentes utilizando para ello cámaras en lugares como aeropuertos o carreteras, y disponiendo de una base de datos de fotografías propia para comparar.

Otros usos de seguridad:

El reconocimiento facial se utiliza para incrementar la seguridad en diversos aspectos de nuestra vida cotidiana. Hoy en día podemos encontrarlo en:

- **Desbloquear dispositivos móviles**. Con la tecnología Face ID que incorporan los últimos dispositivos móviles de Apple como el iPhone o el iPad, se puede desbloquear el teléfono enfocando al rostro del usuario la

cámara. Y dispositivos como los Samsung Galaxy, algunos Xiaomi y Huawei, entre otros, disponen de servicios equivalentes o iniciar sesión en Windows Hello. Este método es más rápido, cómodo y fiable que el tradicional de la huella dactilar o el código de acceso.
Luego están las imágenes que compartimos voluntariamente y los servicios a los que permitimos que procesen fotos de nuestro rostro para identificarnos. Por ejemplo, que Facebook nos etiquete en fotos que nuestros contactos publican en la red social (también lo hace Google Fotos), jugamos con FaceApp (con imágenes propias y ajenas, lo que multiplica los riesgos) y compartimos *selfies* y *stickers* o *emojis* creados a partir de ellos, por poner solamente algunos ejemplos

- **Operaciones en cajeros automáticos y tiendas**. Aunque no está aún extendido, el uso del reconocimiento facial como sustituto de tarjetas bancarias o como sistema de pago en tiendas, incrementa de manera notable la seguridad de las transacciones. Se evita que un tercero pueda hacer uso de los sistemas de pago del usuario, necesitando la presencia física del mismo para la validación del pago.

Mercadona:

En el caso de Mercadona, la cadena de supermercados asegura que la usa para detectar si en sus tiendas entran sospechosos o delincuentes con órdenes policiales en vigor o personas que tengan prohibido el acceso. La compañía dice que sus sistemas son capaces de procesar los rostros y la información en 0,3 segundos y que después las imágenes se eliminan. Algo complicado, porque para que el reconocimiento facial funcione esas caras deben ser contrastadas con las almacenadas en una base de datos. La Agencia Española de Protección de Datos está investigando este caso.

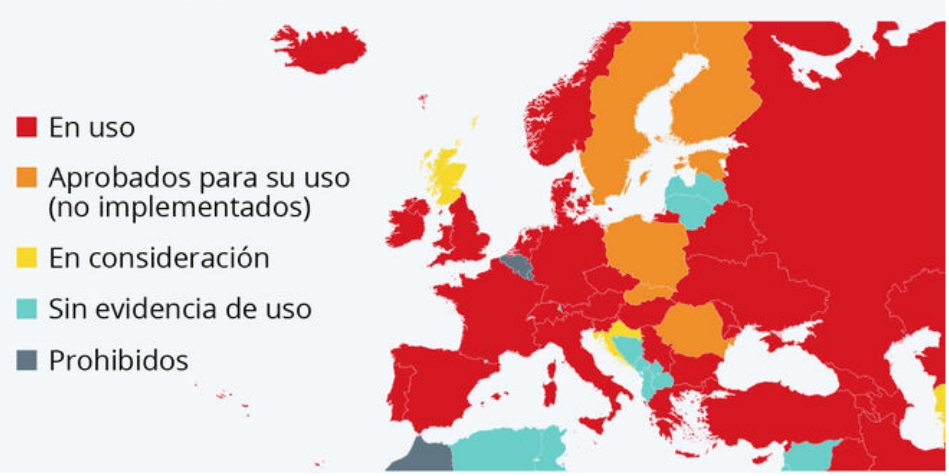
¿Dónde se utiliza en España?

A un proyecto piloto anunciado a finales del año pasado para pagar con la cara en varios autobuses municipales de Madrid (el usuario se da de alta en una web y al acceder al autobús una cámara le identifica y le carga automáticamente el importe del billete en su cuenta) se unió, también en la capital de España, el reconocimiento facial en la Estación Sur para identificar a delincuentes. Se comenzó a implantar en 2016 y según sus responsables ha servido para reducir la actividad de los carteristas en esta estación de autobuses.

Es también conocido el sistema de identificación biométrica instalado por Aena en varios de los principales aeropuertos españoles. El viajero se acerca a una cámara y puede acceder al embarque sin necesidad de mostrar su documentación.

Otros espacios como Ifema, el centro de congresos de Madrid, comenzó a implantar cámaras de reconocimiento facial el año pasado, pero no queda claro si el objetivo es facilitar los accesos o vigilar las actividades de los asistentes a eventos. Y los salones de juego también se están apuntando a esta tendencia, aunque se repiten las dudas sobre su finalidad: ¿quieren controlar que no acceda a ellos quien no debe poder hacerlo o buscan algo más?

Éstos son algunos de los ejemplos más conocidos, pero son muchas las empresas privadas y ayuntamientos que cuentan con la tecnología (hardware y software) para llevar a cabo reconocimientos faciales (probablemente muchos lo hagan ya), aunque por el momento no se ha extendido su uso por las calles de nuestro país.



Reconocimiento facial en la era de la Covid-19:

En estos tiempos de coronavirus y mascarillas podría pensarse que toda esta tecnología es, como mínimo, poco útil. ¿Cómo identificar a alguien que lleva la cara cubierta? Es más difícil, pero no imposible.

De hecho, la empresa alicantina **FacePhi**, especializada en servicios biométricos, dice haber desarrollado un reconocimiento facial a prueba de mascarillas: su software se centra en la biometría periocular, es decir, en la zona de los ojos y no en toda la cara. FacePhi, que tiene entre sus clientes a diversas entidades bancarias, incluirá esta tecnología primero en Selphi, un producto que permite a los bancos aprobar transacciones financieras con un selfie, y más adelante en SelphID, para autentificar usuarios con reconocimiento facial.

Hemos visto qué es y cómo funciona el reconocimiento facial, una tecnología que cada vez tiene mayor presencia en seguridad por las distintas ventajas que ofrece a organizaciones, empresas y usuarios. En los próximos años veremos cómo este tipo de tecnología empieza a aparecer de manera habitual en nuestro día a día.

Demostración:

Por último, vamos a realizar una demostración con unos programas sencillos de cómo funcionaría la detección facial y el reconocimiento facial. A priori, esto puede parecer una tarea difícil de programar, sin embargo, haciendo uso de la librería *OpenCV* para detección facial, y *Face_Recognition* para reconocimiento facial, la tarea se vuelve realmente sencilla, ya que con unas pocas líneas de código, tendremos un programa funcional. Seguiremos los pasos indicados en la siguiente página.

Antes de empezar, tendremos que instalar las librerías indicadas, puesto que pertenecen a Python, las instalaremos con los comandos ***pip3 install opencv-python*** y ***pip3 install face_recognition*** fácilmente. Una vez instaladas, podremos pasar a programar nuestros pequeños programas.

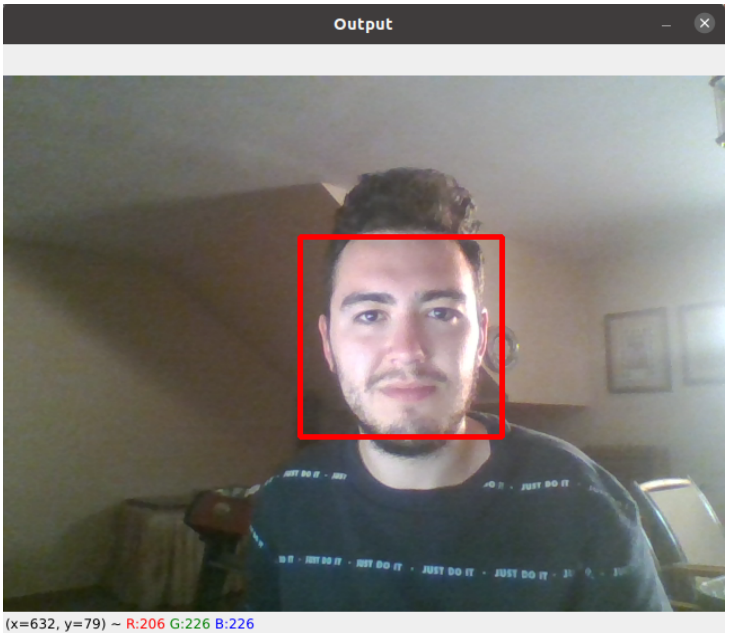
Detección Facial en Foto:

En este primer programa, usaremos la tecnología que nos brinda OpenCV para la detección facial en una foto estática. Esto es tremendamente sencillo de programar, a pesar de parecer que es una tarea difícil, y, para ello, usaremos el código (*deteccion_facial_imagen.py*) que nos ofrece la página que hemos mencionado antes.

Para demostrar el funcionamiento del código, hemos usado una imagen de ejemplo, y como se puede observar en la siguiente captura, la detección facial funciona perfectamente:

Detección Facial en Video:

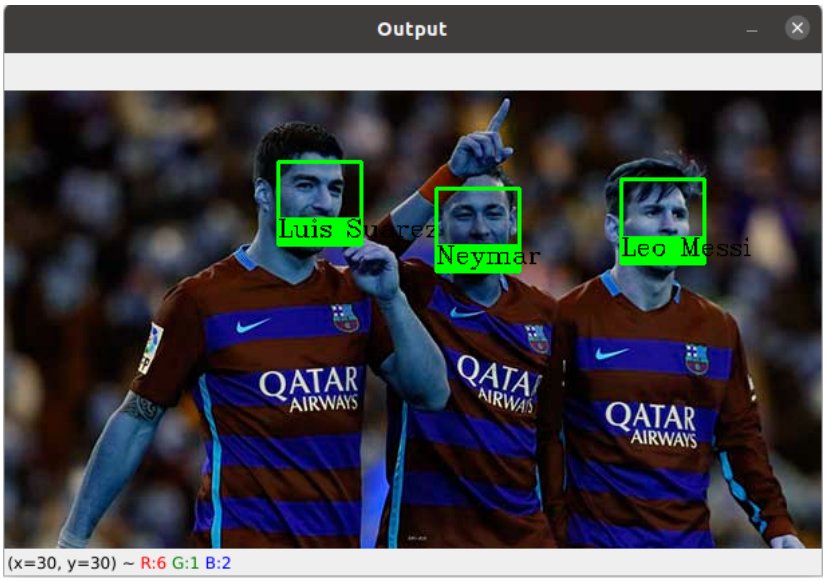
Pero lo interesante de esta tecnología es realizar la detección facial en un video en tiempo real, es decir, usando, por ejemplo, la webcam de nuestro ordenador. Esto se consigue realizando unas pequeñas modificaciones (*deteccion_facial_video.py*) al código anterior, con las cuales, se consigue este propósito fácilmente:



Reconocimiento Facial en Foto:

Una vez realizada la detección facial, lo más interesante es programar un código para que se reconozcan las caras en las imágenes estáticas, esto se puede lograr con la librería *Face_Recognition*, y, usando el código del archivo *reconocimiento_facial_imagen.py*. Pero para que esto funcione, hay que "entrenar" el algoritmo con fotos de las caras que queremos que reconozca en la imagen, por lo que, ya que vamos a usar la imagen de ejemplo usada en el apartado anterior, usaremos las siguientes imágenes para entrenarlo:

Una vez cargadas las imágenes en el programa, este ya podrá realizar el reconocimiento facial en una imagen en la que aparezcan las caras aprendidas, como se puede ver en la siguiente captura:



Reconocimiento Facial de Video:

Cómo pasaba con la detección facial, lo interesante es probar esta técnica en video en tiempo real, para ello, cómo antes, se realizarán unos pequeños cambios en el código (*reconocimiento_facial_video.py*) para realizar esto, además, sigue siendo necesario cargar una imagen de la cara que queremos que reconozca:

El funcionamiento sería el siguiente, y, cómo se puede observar, el código funciona bastante bien, ya que a pesar de que en la foto de ejemplo de la cara tengo menos barba, pelo más corto y la sonrisa con la boca abierta, el algoritmo es capaz de detectarme perfectamente a través de la webcam: