UNIVERSITAT POLITÈCNICA DE VALÈNCIA

ADE
FACULTAD DE ADMINISTRACIÓN Y DIRECCIÓN DE EMPRESAS. UPV

Facultad de Administración y Dirección de Empresas
Universitat Politècnica de València

Estudio de las variables a considerar para el desarrollo de un modelo viable de aplicación de un sistema de identificación facial segura en un entorno de organizaciones de servicios

TRABAJO FIN DE GRADO

Grado en Administración y Dirección de Empresas

Autor: Francisco Morcillo Vizuete

Contutores: Ignacio Gil Pechuán y José Miguel Albarracín Guillem

Curso 2020-2021

Resumen

El reconocimiento facial es el campo de la biometría que ha atraído un mayor interés durante los últimos años en la mayoría de países, ya que proporciona un medio discreto y no intrusivo de detección, identificación y verificación. Esta tecnología se utiliza en numerosas aplicaciones: seguridad aeroportuaria, investigaciones policiales, búsqueda de desaparecidos, etiquetado de fotos, forma de pago, desbloqueo del *smartphone*, etc.

La incorporación de técnicas de aprendizaje profundo o *Deep Learning*, que usan una cascada de múltiples capas de unidades de procesamiento para la extracción y transformación de características faciales, ha contribuido a la rápida evolución de esta tecnología.

El principal objetivo del presente trabajo es determinar y estudiar las principales variables a considerar para el desarrollo de un modelo viable de aplicación de un sistema de reconocimiento facial seguro en organizaciones de servicios (como juzgados, centros deportivos, oficinas de consultoría, etc.) para tareas de autentificación en los equipos informáticos y control de acceso en instalaciones, tanto de trabajadores como de clientes.

En este trabajo se han estudiado las tecnologías más relevantes de reconocimiento facial de última generación y se ha creado un marco de referencia o guía que pueden tener en cuenta las compañías de servicios antes de instalar un sistema de identificación facial. Además se ha desarrollado una solución práctica, utilizando Wordpress, que consiste en una página web capaz de filtrar por uso y tipo de solución algunas de las mejores tecnologías de reconocimiento facial del mercado para ayudar a las compañías de servicios a escoger la opción más conveniente.

Palabras clave: autentificación, empresas de servicios, estudio de variables, marco de referencia, página web, reconocimiento facial, seguridad, sistema de identificación facial, viabilidad.

Resum

El reconeixement facial és el camp de la biometria que ha atret un major interès durant els últims anys en la majoria de països, ja que proporciona un mitjà discret i no intrusiu de detecció, identificació i verificació. Aquesta tecnologia s'utilitza en nombroses aplicacions: seguretat aeroportuària, investigacions policials, recerca dedesaparecidos, etiquetatge de fotos, forma de pagament, desbloqueig del *smartphone*, etc.

La incorporació de tècniques d'aprenentatge profund o *Deep Learning*, que usen una cascada de múltiples capes d'unitats de processament per a l'extracció i transformació de característiques facials, ha contribuït a la ràpida evolució d'aquesta tecnologia.

El principal objectiu d'aquest treball és determinar i estudiar les principals variables a considerar per al desenvolupament d'un model viable d'aplicació d'un sistema de reconeixement facial segur en organitzacions de serveis (com jutjats, centres esportius, oficines de consultoria, etc.) per tasques d'autenticació en els equips informàtics i control d'accés a instal·lacions, tant de treballadors com de clients.

En aquest treball s'han estudiat les tecnologies més rellevants de reconeixement facial d'última generació i s'ha creat un marc de referència o guia que poden tenir en compte les companyies de serveis abans d'instal·lar un sistema d'identificació facial. A més s'ha desenvolupat una solució pràctica, utilitzant Wordpress, que consisteix en una pàgina web capaç de filtrar per ús i tipus de solució algunes de les millors tecnologies de reconeixement facial del mercat per ajudar les companyies de serveis a escollir l'opció més convenient.

Paraules clau: autenticació, empreses de serveis, estudi de variables, marc de referència, pàgina web, reconeixement facial, seguretat, sistema d'identificació facial, viabilitat.

Abstract

Facial recognition is the field of biometrics that has attracted the most interest in recent years in most countries, as it provides a discreet and non-intrusive means of detection, identification and verification. This technology is used in many applications: airport security, police investigations, search for missing persons, photo tagging, payment method, smartphone unlocking, etc.

The incorporation of deep learning techniques, which use a multilayer cascade of processing units for the extraction and transformation of facial features, has contributed to the rapid evolution of this technology.

The main objective of this work is to determine and study the main variables to consider for the development of a viable model for the application of a secure facial recognition system in service organizations (such as courts, sports centers, consulting offices, etc.) for authentication tasks in computer equipment and access control in facilities, both for workers and customers.

In this work, state-of-the-art facial recognition technologies have been studied and a framework of reference or guide has been created that service companies can take into account before installing a facial identification system. In addition, a practical solution has been developed, using Wordpress, which consists of a web page capable of filtering by use and type of solution some of the best facial recognition technologies on the market to help service companies choose the most convenient option.

Key words: authentication, facial identification system, facial recognition, frame of reference, security, service companies, study of variables, website, viability.

Índice general

Índice de figuras

Índice de tablas

CAPÍTULO 1
Introducción

El reconocimiento facial es el campo de la biometría que ha atraído un mayor interés durante los últimos años en la mayoría de países, ya que proporciona un medio discreto y no intrusivo de detección, identificación y verificación [24].

La incorporación de técnicas de aprendizaje profundo o *Deep Learning*, que usan una cascada de múltiples capas de unidades de procesamiento para la extracción y transformación de características faciales, ha contribuido a la rápida evolución de esta tecnología.

Como información curiosa, Apple ha registrado una patente que permitirá distinguir a dos usuarios físicamente parecidos (como los gemelos) mediante un complejo sistema de mapeado en 3D logrado por sensores infrarrojos capaces de capturar patrones *subepidérmicos* del rostro como las venas [13].

Durante la última década, el uso del reconocimiento facial en la seguridad se ha ido haciendo cada vez más común en el mundo [38]. Se espera que el mercado de la tecnología de reconocimiento facial alcance los 3 100 millones de dólares estadounidenses en el año 2022 [30]. Esta tecnología se utiliza en numerosas aplicaciones: seguridad aeroportuaria, investigaciones policiales, búsqueda de desaparecidos, etiquetado de fotos, forma de pago, desbloqueo del *smartphone*, etc.

Más del 50 % de los estadounidenses se encuentran actualmente en las bases de datos de reconocimiento facial de la policía. China es el país con mayor proporción de cámaras de seguridad por habitante y también es el proveedor líder de *hardware* de reconocimiento facial en todo el mundo. En Moscú, han desplegado más de 100 000 cámaras de seguridad para vigilar que no se infrinjan las normas. El gobierno de Serbia está desarrollando el proyecto de «ciudad segura» en Belgrado, que incluye la instalación de cámaras de vigilancia en toda la ciudad, con tecnología de reconocimiento facial, suministradas por el fabricante chino Huawei. Es la única ciudad del continente europeo que cuenta con este sistema [29].

En España, esta tecnología permite extraer dinero en cajeros automáticos sin necesidad de introducir un PIN, abrir una cuenta bancaria con un selfi y asistir a conciertos y a otros eventos multitudinarios. También se utiliza en varios de sus principales aeropuertos para realizar la facturación y el embarque de los viajeros sin que tengan que mostrar su documentación [23].

La expansión de la tecnología de reconocimiento facial ha planteado cuestiones importantes sobre el impacto en la privacidad de una vigilancia tan generalizada y problemas legales que han causado la cancelación de algunos proyectos relacionados con esta tecnología. A pesar de esto, solamente se ha prohibido en tres países del mundo: Bélgica, Luxemburgo y Marruecos.

Las ventajas de implementar un sistema de reconocimiento facial en una organización de servicios para permitir la autentificación del personal en sus equipos informáticos o para acceder a las instalaciones son numerosas: es un sistema de identificación no intrusivo, sin contacto y por tanto, proporciona una mayor higiene; el usuario no manipula el sistema; no requiere tarjetas, llaves u otros dispositivos externos, ni tampoco recordar contraseñas; es extremadamente seguro y de rápida acción (inferior a un segundo).

En el presente trabajo se determinan y estudian las principales variables a considerar para el desarrollo de un modelo viable de aplicación de un sistema de reconocimiento facial seguro en organizaciones de servicios (como juzgados, centros deportivos, oficinas de consultoría, etc.) para tareas de autentificación en los equipos informáticos y control de acceso, tanto de trabajadores como de clientes. Con esto, se crea un marco de referencia o guía que pueden tener en cuenta las compañías de servicios antes de instalar un sistema de identificación facial. También se exponen las tecnologías de reconocimiento facial de última generación del mercado. Además se desarrolla una solución práctica, utilizando Wordpress, que consiste en una página web capaz de filtrar por uso y tipo de solución algunas de las mejores tecnologías de reconocimiento facial del mercado para ayudar a las compañías de servicios a escoger la mejor opción.

1.1 Motivación

A lo largo de los últimos años ha aumentado considerablemente la inversión en inteligencia artificial por parte de empresas (como Apple, Amazon, Google y Microsoft) y gobiernos de todo el mundo para conseguir una mayor eficiencia en sus actividades o fines. En tareas de seguridad, el reconocimiento facial es el campo de la biometría que ha suscitado un mayor interés en la mayoría de países, ya que proporciona un medio discreto y no intrusivo de detección, identificación y verificación.

Me impresionan aplicaciones como Google Fotos, capaz de detectar y reconocer texto, objetos y personas en fotografías con mucha precisión, y como el Face Id de Apple, implementado en los iPhone, capaz de desbloquear dispositivos identificando caras incluso a oscuras usando un proyector de luz infrarroja. Esto, unido al estudio de la asignatura Sistemas Inteligentes cursada en el grado de Ingeniería Informática y a que grandes empresas están invirtiendo en evolucionar esta tecnología, me ha motivado para elegir esta temática, que es común también al trabajo de Ingeniería Informática [24], el cual considero que se complementa muy bien con este.

1.2 Objetivos

El principal objetivo de este trabajo es estudiar las variables a considerar para el desarrollo de un modelo viable de aplicación de un sistema de identificación facial segura en un entorno de organizaciones de servicios con el fin de ayudarles a elegir la mejor solución. Este objetivo global se descompone en los siguientes objetivos.

1. Comprender el funcionamiento de un sistema de reconocimiento facial a partir de sus componentes principales.

2. Conocer la evolución histórica del reconocimiento facial.

3. Estudiar las mejores soluciones de reconocimiento facial que existen actualmente en el mercado.

4. Conocer el contexto legal y social del reconocimiento facial.
5. Estudiar la viabilidad de la implementación de un sistema de reconocimiento facial en compañías de servicios para tareas de autentificación y control de acceso.
6. Determinar y estudiar las variables a considerar para la aplicación de un sistema de identificación facial segura en un entorno de organizaciones de servicios para control de acceso y autenticación.
7. Crear una guía teórica que sirva de referencia para las compañías de servicios que deseen instalar un sistema de reconocimiento facial seguro.
8. Desarrollar una solución práctica y tecnológica para facilitar la elección del sistema de reconocimiento facial óptimo para la empresa.

Es necesario la consecución de todos los objetivos mencionados para finalmente alcanzar el objetivo global.

1.3 Estructura de la memoria

El presente trabajo se divide en los siguientes seis capítulos:

- **Capítulo 1. Introducción:** se introduce la temática de la memoria, se expone el problema global, se describen las motivaciones que han llevado a realizar el trabajo y los objetivos que se pretenden alcanzar. Por último, se presenta la estructura de la memoria.
- **Capítulo 2. Contexto tecnológico:** se describen los componentes de un sistema de reconocimiento facial con el objetivo de comprender su funcionamiento. También se resume la historia del reconocimiento facial nombrando los cuatro principales enfoques en el estudio de este campo y se presentan algunas de las mejores soluciones tecnológicas *software* y *hardware* actuales.
- **Capítulo 3. Contexto legal y social:** se expone el contexto legal y social a nivel mundial, europeo y en España a partir de algunas de las noticias más relevantes relacionadas con el reconocimiento facial y la protección de datos personales de los últimos años. También se presentan algunos de los problemas asociados a las tecnologías de reconocimiento facial.
- **Capítulo 4. Variables a considerar en la aplicación de un sistema de identificación facial:** se estudia la viabilidad de instalar un sistema de reconocimiento facial para acceder a las instalaciones o autenticarse en los equipos informáticos de una compañía de servicios (como juzgados, centros deportivos, oficinas de una consultoría, etc.). Por último, se explican las principales variables a tener en cuenta a la hora de implementar un sistema de identificación facial en una compañía de servicios.
- **Capítulo 5. Diseño y desarrollo de la solución:** se describen el objetivo, el diseño, las tecnologías utilizadas y el desarrollo de la solución tecnológica.
- **Capítulo 6. Conclusiones:** se describen las conclusiones del trabajo realizado y se presentan los trabajos futuros.

CAPÍTULO 2
Contexto tecnológico

Este capítulo presenta un resumen de la historia del reconocimiento facial así como las tecnologías actuales de este campo. Para ello, primeramente, se define qué es un sistema de reconocimiento facial y se describen sus componentes. A continuación, se explican los avances más importantes hasta la actualidad mencionando los cuatro principales enfoques en el estudio del reconocimiento facial. Por último, se comentan algunas de mejores soluciones tecnológicas *software* (gratuitas y de pago) y *hardware* actuales.

2.1 Componentes de un sistema de reconocimiento facial

Un **sistema de reconocimiento facial** (o identificación facial) es un sistema capaz de comparar un rostro humano con imágenes digitales o con fotogramas de vídeo almacenados en una base de datos, con el objeto de identificar o reconocer una cara. Puede ser usado para tareas de verificación (comprobar si dos imágenes son del mismo sujeto) o de identificación (determinar la identidad específica de un sujeto comparándola con todas las imágenes de caras de la base de datos). Actualmente, por lo general, un sistema de reconocimiento facial por aprendizaje profundo (*deep face recognition system*) está formado por los siguientes componentes o módulos [24, 42].

- **Detector facial:** es un componente fundamental en un sistema de reconocimiento facial y se utiliza para localizar caras en una imagen o fotograma (v. Figura 2.1 (a)).

- **Detector de puntos de referencia faciales:** se utiliza para localizar rasgos faciales relevantes como pueden ser el centro de los ojos, las comisuras de los labios y la punta de la nariz. Una vez identificados estos puntos de referencia, la cara se alinea (*face alignment*) de acuerdo con unas coordenadas canónicas normalizadas (v. Figura 2.1 (b)).

- **Reconocimiento facial:** antes de que una imagen de una cara alineada pase al módulo de reconocimiento facial, puede hacerse pasar por un módulo de *anti-spoofing*, para reconocer si la cara está viva o es una falsificación (artefacto inanimado). El módulo de reconocimiento facial consta de tres fases: procesamiento de caras, extracción de características y coincidencia facial. En el **procesamiento de caras** se tratan las variaciones intrapersonales antes del entrenamiento y evaluación (pruebas) del sistema, como poses, iluminación, expresiones y oclusiones; en la fase de **extracción de características**, el extractor de características aprende durante el entrenamiento mediante las funciones de pérdida (*Loss function*), y se utiliza para extraer características discriminatorias de caras durante las pruebas; y, por último,

en la **coincidencia facial**, mediante el cálculo de puntuaciones de similitud de características (las de entrada y las de una base de datos), se verifica o determina la identidad específica de las caras (v. Figura 2.1 (c)).

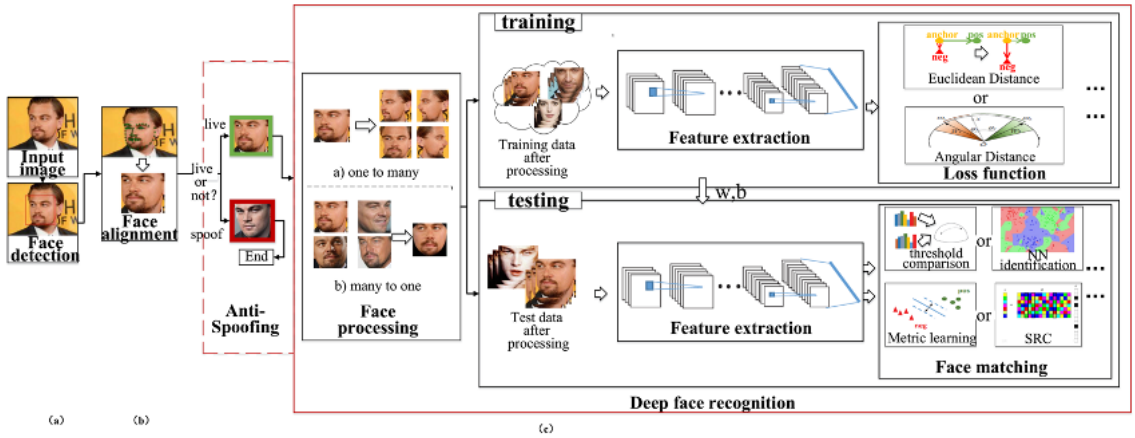

Figura 2.1: Sistema de reconocimiento facial profundo. Recuperada de [42].

2.2 Historia del reconocimiento facial

Entre 1964 y 1965, Woodrow Wilson «Woody» Bledsoe, junto con Helen Chan Wolf y Charles Bisson, fueron pioneros del reconocimiento facial automático, ya que fueron capaces de extraer manualmente, mediante una tableta gráfica RAND [1], las coordenadas de un conjunto de características de fotografías de caras (centro de las pupilas, esquina interna y externa de los ojos, punto del pico de viuda, etc.) (v. Figura 2.2), calcular distancias entre varias coordenadas y almacenarlas en una base de datos, para después reconocer caras. Este proyecto fue etiquetado como **hombre-máquina** [12, 24].

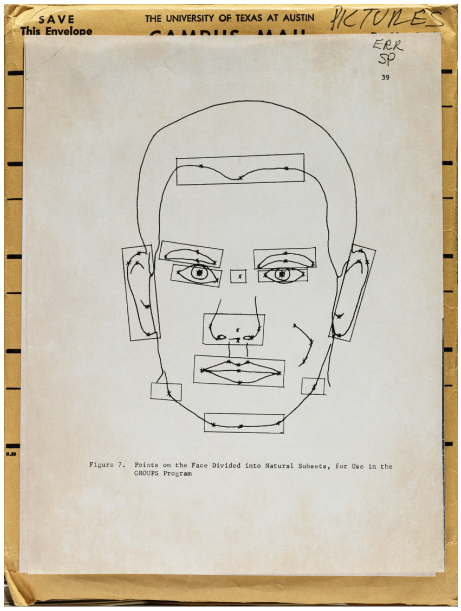

Figura 2.2: Características faciales de Bledsoe. Recuperada de [24].

[1] https://www.rand.org

Entre 1987 y 1990, Lawrence Sirovich y M. Kirby desarrollaron una técnica para representar imágenes de caras de manera eficiente utilizando el análisis de componentes principales. Demostraron que cualquier cara particular puede ser representada fácilmente en términos de un mejor sistema de coordenadas que ellos denominaron imágenes propias o ***eigenpictures***. Por lo tanto, en principio, se podría clasificar cualquier colección de caras almacenando solamente un pequeño conjunto de datos por cada cara y un pequeño conjunto de imagénes estándar o *eigenpictures* [35, 40, 41].

En 1991, Matthew A. Turk y Alex P. Pentland, principalmente a partir de la técnica desarrollada por Syrovich y Kirby, descubrieron una forma relativamente sencilla de detectar e identificar caras automáticamente (es decir, de manera no supervisada) en un entorno controlado, mediante un sistema de reconocimiento facial casi en tiempo real. Las imágenes de caras se proyectaban en un espacio de características, llamado espacio facial (*face space*) (v. Figura 2.3) que estaba definido por las ***eigenfaces*** o caras propias, llamadas así por su apariencia (v. Figura 2.4) y por ser los vectores propios del conjunto de caras [24, 41].

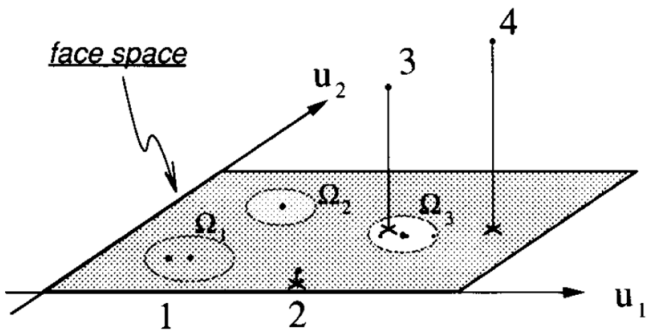

Figura 2.3: Versión simplificada del espacio facial para ilustrar los cuatro resultados de proyectar una imagen en el espacio facial. En este caso, hay dos *eigenfaces* (u_1 y u_2) y tres individuos conocidos (Ω_1, Ω_2 y Ω_3). Recuperada de [41].

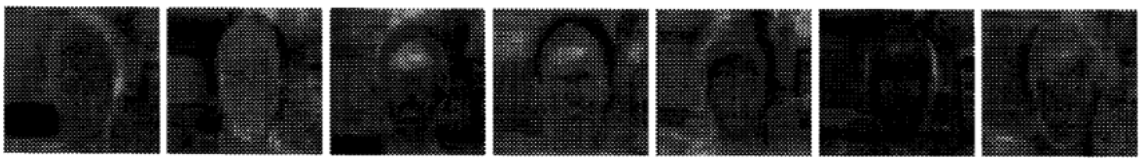

Figura 2.4: Siete caras propias o *eigenfaces*. Recuperada de [41].

En 2001, Paul Viola y Michael Jones desarrollaron el algoritmo **Viola-Jones**, un marco de reconocimiento de objetos que permitía la detección rápida de características de imágenes en tiempo real usando características de tipo Haar (*Haar-like Features*) (v. Figura 2.5). Este enfoque minimizaba el tiempo de cálculo a la vez que lograba una alta precisión de detección [24].

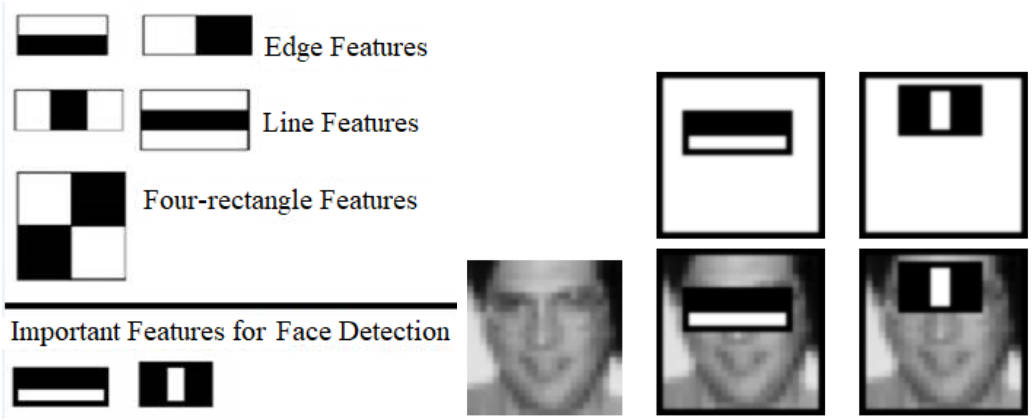

Figura 2.5: Caraterísticas de tipo Haar (*Haar-like features*). Recuperada de [24].

A partir de los trabajos de Turk y Pentland y de Viola y Jones, aumentó de forma significativa el interés por el reconocimiento facial [24, 36]. El progreso en este campo puede dividirse en cuatro áreas de interés de estudio o enfoques (v. Figura 2.6): reconocimiento por aprendizaje supervisado mediante el uso de características globales (**aprendizaje holístico**), reconocimiento por aprendizaje supervisado mediante el uso de características locales (**aprendizaje manual local o *local handcraft***), reconocimiento por aprendizaje no supervisado mediante clasificadores automáticos con redes neuronales (**aprendizaje superficial o *shallow learning***) y reconocimiento por aprendizaje profundo no supervisado mediante clasificadores automáticos (***Deep Learning***).

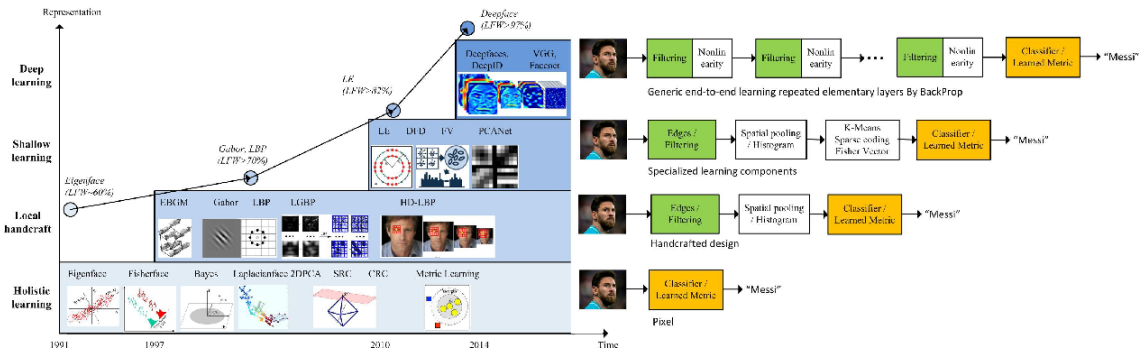

Figura 2.6: Enfoques e hitos de la representación facial para el reconocimiento. Recuperada de [42].

En el reconocimiento por aprendizaje profundo o *Deep Learning* se usa una cascada de múltiples capas de unidades de procesamiento (por lo tanto, muchas capas ocultas o *hidden layers*) con diferentes niveles jerárquicos de abstracción para extraer y transformar características (v. Figura 2.7), a diferencia del aprendizaje superficial o *shallow learning* en el que se utilizan redes neuronales con pocas capas ocultas (v. Figura 2.8) [24].

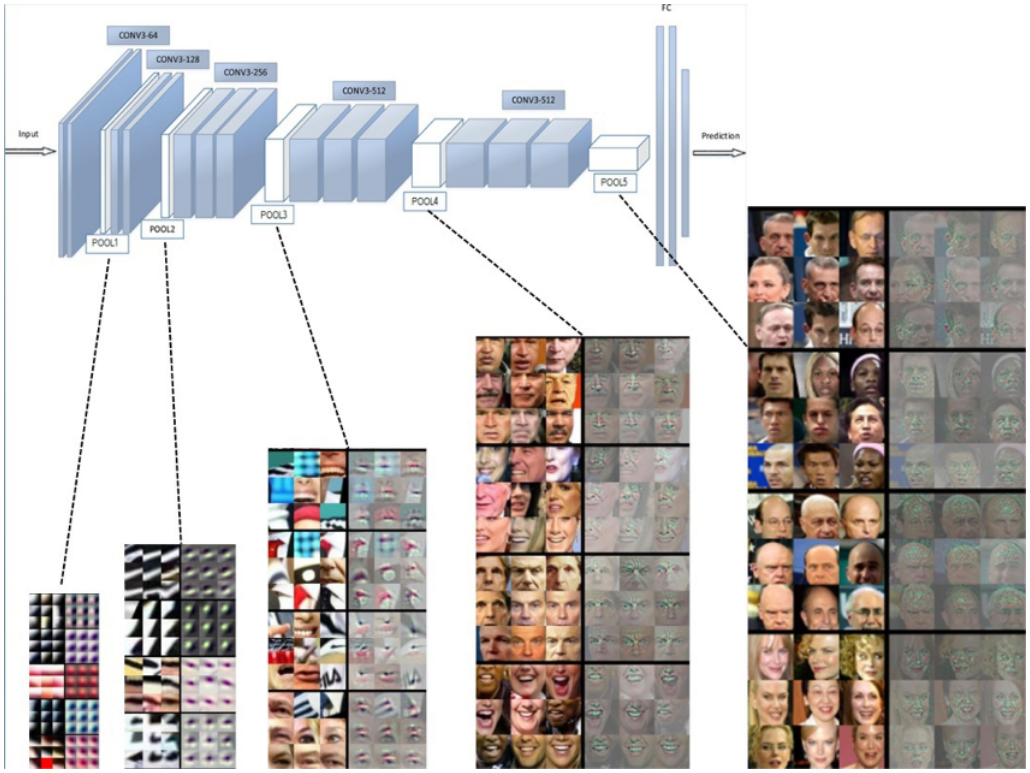

Figura 2.7: La arquitectura jerárquica del modelo de aprendizaje profundo. Recuperada de [42].

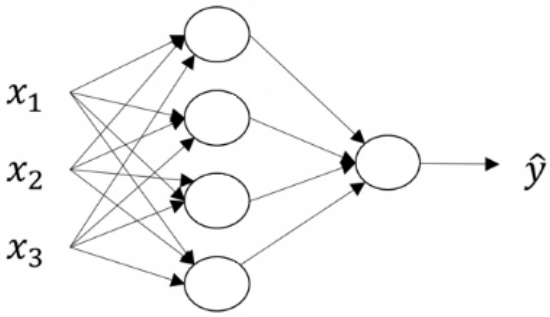

Figura 2.8: Representación gráfica de una red neuronal superficial o *shallow neural network* con una capa oculta, una capa de entrada y una capa de salida. Recuperada de [24].

La precisión de los métodos de reconocimiento facial por *Deep Learning* fue mejorando gracias al uso de nuevas arquitecturas de red de clasificación de objetos (Alexnet, VGG-Net, GoogleNet, ResNet, SENet) (v. Figura 2.9) y de funciones de pérdida (*contractive loss*, *triplet loss*, *center loss*, softmax, L-softmax, A-softmax, cosface, arcface) (v. Figura 2.10) [24, 42]. También ayudó a la mejora de la precisión la creación del programa FERET y de grandes bases de datos (MegaFace Challenge, *Labeled Faces in the Wild* (LFW) y WIDER FACE), así como las mejoras significativas en *hardware*, por ejemplo la alta capacidad de las GPUs (*Graphics Processing Units*) [24, 36].

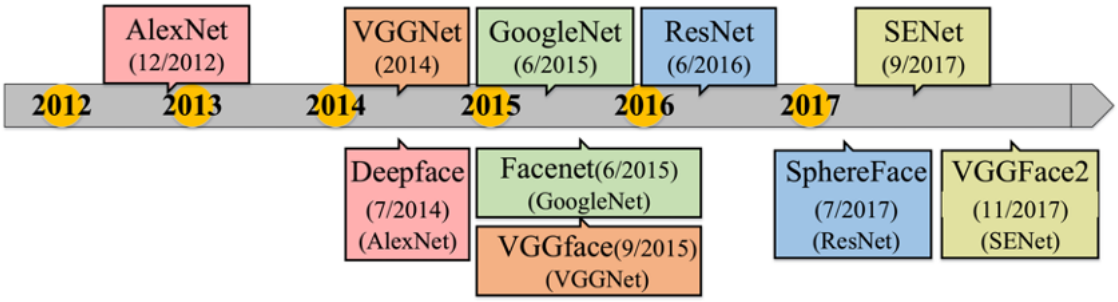

Figura 2.9: Las arquitecturas de red típicas en la clasificación de objetos (fila superior) y los algoritmos de reconocimiento facial profundo más conocidos que utilizan esas arquitecturas (fila inferior). Los rectángulos del mismo color significan que usan la misma arquitectura. Se puede observar que las arquitecturas de reconocimiento facial por aprendizaje profundo han seguido a las de clasificación de objetos y han evolucionado desde a Alexnet hasta SENet rápidamente. Recuperada de [42].

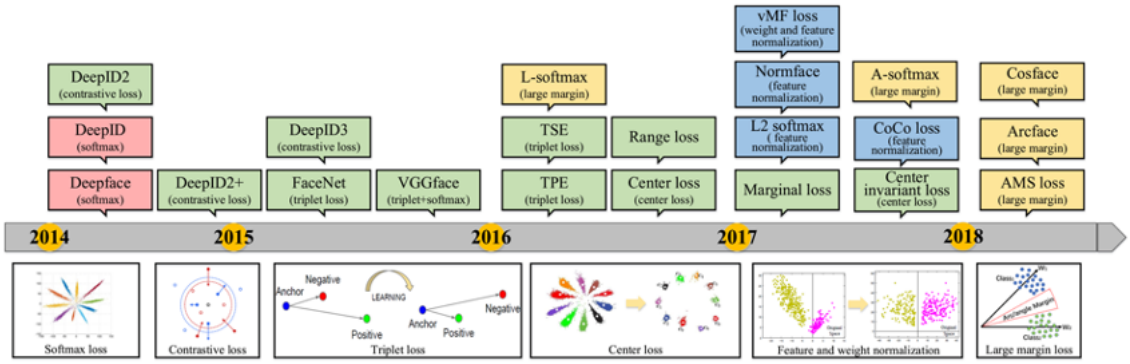

Figura 2.10: El desarrollo de las funciones de pérdida. Los rectángulos de color rojo, verde, azul y amarillo representan métodos de aprendizaje profundo con softmax, pérdida basada en la distancia euclidiana, pérdida basada en el margen angular o coseno y variaciones de softmax, respectivamente. Recuperada de [42].

2.3 Tecnologías *software* actuales de reconocimiento facial

Las soluciones o servicios *software* de reconocimiento facial disponibles en el mercado se pueden clasificar en tres tipos [28]:

- **Motores de reconocimiento facial basados en *Software* como Servicio (SaaS).** Un proveedor de servicios de reconocimiento facial es el que se encarga de todo, desde mantener actualizada la tecnología de aprendizaje automático hasta administrar y mantener los servidores de alta carga. Todo lo que tiene que hacer el cliente es integrar el software con sus sistemas de TI (Tecnologías de la Información) a través de una API (*Application Programming Interface*). A pesar de sus muchas ventajas, estas soluciones también tienen varios inconvenientes. En primer lugar, es la opción más cara, debido a que todo lo maneja el proveedor. Además, el cliente necesita una conexión a Internet estable, ya que deberá enviar imágenes pesadas a un servidor. Por último, podría haber problemas de seguridad, ya que las fotos se envían a una empresa externa y el cliente no puede controlar lo que se hace con ellas.
- **Soluciones API REST *auto-hospedadas* (*self-hosted*).** Estos sistemas se pueden desplegar tanto localmente como en la nube. Almacenan datos en sus propios servidores (o en su nube privada), por lo que se puede controlar a dónde van, e incluso

se puede crear un sistema que funcione sin conexión. A cambio, el cliente tiene que administrar los servidores. Pero en la mayoría de los casos, los servidores se entregan como contenedores Docker[2], por lo que es bastante fácil organizarlos. Las soluciones *auto-hospedadas*, aunque no son tan caras como las SaaS, siguen siendo bastante caras. Afortunadamente, están comenzando a aparecer soluciones de API REST *auto-hospedadas* de código abierto y gratuitas. No son tan maduras como otras soluciones, pero son muy prometedoras.

– ***Frameworks* y bibliotecas de código abierto.** Se necesita algo de experiencia con el aprendizaje automático (*machine learning*) para utilizar este tipo de *software*. También es necesario utilizar una API REST si se desea integrar estas soluciones con aplicaciones personalizadas. La ventaja es que se puede obtener una solución que se conoce al completo.

2.3.1. Soluciones *software* gratuitas

El número de soluciones gratuitas de reconocimiento facial ha ido aumentando durante los últimos años. Se pueden encontrar en distintas etapas de madurez pero todas ellas pueden ser perfectamente utilizadas en pequeñas y medianas empresas. A continuación se va a presentar una lista de las mejores **soluciones gratuitas** según la precisión obtenida en el popular banco de pruebas o base de datos *Labeled Faces in the Wild* (LFW) [28].

Face Recognition

Face Recognition es la biblioteca de reconocimiento facial más sencilla del mundo, según [14]. Sirve para reconocer y manipular caras desde Python o desde línea de comandos. Ha sido desarrollada con los modelos de reconocimiento facial de última generación de Dlib[3], que usan aprendizaje profundo (*deep learning*). Su modelo tiene una precisión del 99,38 % en el banco de pruebas LFW [24, 28].

CompreFace

CompreFace [9] es un proyecto, publicado en julio de 2020 en Github, de detección y reconocimiento de caras gratuito y de código abierto. Esencialmente, es una aplicación basada en Docker que puede usarse como servidor independiente o implementarse en la nube. No se necesitan habilidades previas de *machine learning* para configurar y usar CompreFace.

CompreFace proporciona API REST (solución API REST *auto-hospedada*) para reconocimiento facial, verificación facial, detección facial, detección de puntos de referencia faciales, reconocimiento de edad y género. La solución es escalable y cuenta con un sistema de administración de roles de usuario que permite controlar fácilmente quién tiene acceso a los servicios de reconocimiento facial.

CompreFace se entrega como una configuración de *docker-compose* y es compatible con diferentes modelos que funcionan en CPU y GPU. La solución se basa en métodos y bibliotecas de última generación como FaceNet (99,63 % de precisión en LFW) e InsightFace (99,83 % de precisión en LFW). La desventaja es que todavía se encuentra en desarrollo activo [28].

[2] https://www.docker.com
[3] http://dlib.net

DeepFace

DeepFace [34], que tiene el mismo nombre que el método de reconocimineto facial de Facebook, es un marco ligero de reconocimiento facial y análisis de atributos faciales (edad, género, emoción y raza) para Python. Es un marco híbrido de reconocimiento facial que incluye modelos de última generación: VGG-Face, Google FaceNet, OpenFace, Facebook DeepFace, DeepID, ArcFace y Dlib. Esos modelos ya han alcanzado y pasado la precisión del ojo humano. La biblioteca se basa principalmente en TensorFlow y Keras. DeepFace proporciona una API REST, pero solo admite métodos de verificación, por lo que no se pueden crear colecciones de caras y encontrar una entre ellas. Es bastante sencillo comenzar a usar la biblioteca si se sabe programar en Python [28].

FaceNet

FaceNet [31] es una implementación de TensorFlow del reconocedor de rostros que se describe en [33]. La precisión de este método es de 99,65 % en LFW. Las desventajas de esta solución son que no tiene una API REST y que el repositorio no recibe actualizaciones [28].

InsightFace

InsightFace [17] es una biblioteca Python integrada para análisis de rostros 2D y 3D. Implementa de manera eficiente una amplia variedad de algoritmos de última generación de reconocimiento facial, detección facial y alineación facial, optimizados tanto para el entrenamiento como para el despliegue o utilización. Los institutos de investigación y las organizaciones industriales pueden beneficiarse de esta biblioteca. Esta solución también es muy precisa: 99,86 % en el conjunto de datos de LFW. La única desventaja es que no es fácil de usar [28].

InsightFace-REST

El repositorio InsightFace-REST [37] tiene como objetivo proporcionar una API REST práctica, fácil de implementar y escalable para la detección de rostros y reconocimiento de InsightFace utilizando FastAPI para el servicio y NVIDIA TensorRT para la inferencia optimizada. El código se basa en gran medida en el código API del repositorio oficial de DeepInsight InsightFace [17]. Este repositorio proporciona código fuente para crear la API REST de reconocimiento facial y convertir modelos a ONNX y TensorRT mediante Docker. La desventaja de esta solución es que solo proporciona características faciales (*face embeddings*) y no ofrece la API para el reconocimiento facial real, por lo que se necesita un clasificador propio. Además, el repositorio aún no tiene una licencia, por lo que hay que preguntar al autor si se puede usar [28].

Open CV

OpenCV (*Open Source Computer Vision Library*) [26] es una biblioteca de software de código libre de visión por computador y de aprendizaje automático (*machine learning*). OpenCV se creó para proporcionar una infraestructura común para aplicaciones de visión por computador y para acelerar el uso de la percepción de la máquina en los productos comerciales. Al ser un producto con licencia BSD (*Berkeley Software Distribution*), OpenCV facilita que las empresas utilicen y modifiquen el código.

La biblioteca tiene más de 2500 algoritmos optimizados, que incluyen un conjunto completo de algoritmos de aprendizaje automático y visión por computador clásicos y de última generación. Estos algoritmos se pueden usar para detectar y reconocer rostros, identificar objetos, clasificar acciones humanas en vídeos, extraer modelos 3D de objetos, buscar imágenes similares de una base de datos de imágenes, eliminar ojos rojos de imágenes tomadas con flash, seguir los movimientos oculares, reconocer paisajes y establecer marcadores para superponerlos con realidad aumentada, etc. OpenCV tiene más de 47 mil usuarios y un número estimado de descargas superior a 18 millones. La biblioteca se utiliza ampliamente en grupos de investigación, organismos gubernamentales y empresas como Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda y Toyota.

Cuenta con interfaces C ++, Python, Java y MATLAB y es compatible con Windows, Linux, Android y Mac OS.

2.3.2. Soluciones *software* de pago

A continuación se presentan algunas de las mejores **soluciones de pago** de *software* de reconocimiento facial (otras serían FaceX, Google Cloud Vision, Kairos, Machine Box, Paravision, SenseTime y Trueface) [2, 28, 39].

Amazon Rekognition

Amazon Rekognition [4] proporciona análisis faciales de alta precisión y capacidades de búsqueda facial que se pueden usar para detectar, analizar y comparar rostros con tecnología probada, altamente escalable y de aprendizaje profundo que no requiere experiencia en aprendizaje automático para su uso (v. Figura 2.11). Es posible implementar estos recursos en una amplia variedad de casos de uso vinculados con la verificación de usuarios, el conteo de personas y la seguridad pública. También es posible identificar objetos, texto, escenas y actividades en imágenes y vídeo.

Figura 2.11: Detección y análisis de rostros de Amazon Rekognition. Recuperada de [4].

Con Amazon Rekognition hay tres tipos diferentes de uso, cada uno con sus propios detalles de precio [4]: Amazon Rekognition Image, Amazon Rekognition Video y etiquetas personalizadas de Amazon Rekognition. En el caso de Amazon Rekognition Video para el análisis de vídeo en directo, en Europa (Londres), la búsqueda de rostros tiene un precio de 0,12 USD/minuto y el almacenamiento de metadatos de rostros, 0,00001 USD/-metadatos de rostros al mes. Como parte de la capa gratuita de AWS, se puede comenzar

con Amazon Rekognition Video de manera gratuita. La capa gratuita dura 12 meses e incluye 1 000 minutos gratis de análisis de vídeo al mes. La capa gratuita de Amazon Rekognition Video cubre la detección de etiquetas, la moderación de contenidos, la detección de rostros, la búsqueda de rostros, el reconocimiento de celebridades, la detección de textos y el recorrido de las personas.

Empresas como CBS Corporation, NFL, Here Technologies y Carbon, entre otras, utilizan las tecnologías de Amazon Rekognition.

Deep Vision AI

Deep Vision AI [7] es una empresa que destaca por proporcionar análisis inteligentes de imágenes y vídeos que facilitan nuevas formas de comprender y analizar datos visuales. Deep Vision proporciona visión por Inteligencia Artificial (*AI-vision*) a un amplio conjunto de socios y clientes (como por ejemplo, Amazon Web Services (AWS), Plug and Play, MicroStrategy, Veritone y Red Hat) para ayudarlos a operar de manera más eficiente y efectiva, crear nuevos productos y acelerar modelos comerciales.

Con su tecnología de Inteligencia Artificial, es capaz de detectar y reconocer rostros en imágenes y vídeos. Proporciona la ubicación de los rostros detectados y puede identificar coincidencias faciales para encontrar sujetos objetivo. Además, puede recopilar información demográfica de personas.

FaceFirst

FaceFirst [10] es una empresa que ofrece servicios personalizados de reconocimiento facial e Inteligencia Artificial. Su *software* patentado, llamado también FaceFirst, es altamente preciso, escalable, seguro y privado. La plataforma permite una gama completa de capacidades de vigilancia, interacción con el cliente, dispositivos móviles, control de acceso y reconocimiento facial forense de escritorio. FaceFirst ofrece una API y un SDK robustos para la integración en una amplia variedad de sistemas y plataformas.

Microsoft, Hewlett Packard Enterprise, General Dynamics, NVIDIA y Genetec son empresas asociadas con FaceFirst.

Face^{++}

Face^{++} AI Open Platform [11] es una plataforma de la empresa china Megvii[4] que ofrece tecnologías de visión por computador que permiten que las aplicaciones de los clientes lean y comprendan mejor el mundo. Face^{++} permite agregar fácilmente tecnologías líderes de reconocimiento de análisis de imágenes basadas en aprendizaje profundo en sus aplicaciones, con interfaces de programación de aplicaciones (APIs) y kits de desarrollo de *software* (SDKs) simples y potentes. Admite versiones SaaS y *auto-hospedadas*.

Face^{++} ofrece tres SDKs de reconocimiento facial: *Face Landmarks SDK* (que usa 106 puntos de referencia faciales o *face landmarks*), *Dense Facial Landmarks SDK* (que utiliza 1 000 puntos de referencia faciales) y *Face Compare SDK* (capaz de extraer características faciales y compararlas en 200 ms).

Esta plataforma también oferta una solución en la nube o de forma local llamada *FaceID Identify Verification*, con una robusta técnica de *anti-spoofing*, excelente precisión y actualización frecuente del modelo, capaz de detectar si la cara es realmente de un ser

[4] https://en.megvii.com

humano vivo o de un artefacto inanimado, habiendo interceptado decenas de millones de ataques de suplantación de identidad.

Face^{++} AI Open Platform dispone de opciones gratuitas y *premium* para todos los usuarios. El plan de reconocimiento facial gratuito no tiene limitación de uso total pero solamente permite tres solicitudes o peticiones por segundo a la API entre todos los usuarios que usan el plan. Esto puede provocar que el servicio no responda en determinados momentos. Los pagos por la API de la opción *premium* se pueden realizar según lo que el cliente utilice o también se puede contratar diariamente o mensualmente. En el caso de los SDKs, se pueden comprar paquetes de licencias mensuales o anuales.

Microsoft Azure Cognitive Services Face API

Microsoft Azure Cognitive Services Face API [22] permite integrar el reconocimiento facial en aplicaciones para una experiencia de usuario fluida y altamente segura. No se requiere experiencia en aprendizaje automático. Las funciones incluyen detección de rostros capaz de percibir rasgos y atributos faciales, como una mascarilla, gafas o vello facial, en una imagen y la identificación de una persona mediante coincidencias con un repositorio privado o mediante una identificación con foto. Hay bastantes SDKs compatibles: .NET, Python, Java, Node.js y Go. Tiene una versión gratuita que permite 20 transacciones por minuto y un máximo 30 000 transacciones gratis al mes. En Europa, hasta el primer millón de transacciones del plan estándar cuesta 1 USD ($) cada 1 000 transacciones con 10 transacciones por segundo. Microsoft dispone tanto de versiones SaaS como de *auto-hospedadas*.

2.4 Tecnologías *hardware* actuales de reconocimiento facial

La situación sanitaria provocada por la COVID-19 ha obligado a muchos clientes a preferir sistemas de control de acceso por reconocimiento facial en vez de por huella dactilar. Seguidamente, se exponen algunas de ls mejores dispositivos de reconocimiento facial para seguridad, concretamente, para control de acceso. Otros podrían ser Abraxas de AnyVision, DS-K1T671T de HIKVISION, iCAM D1000 e iT100 [19] de Iris ID, Y10 de JIESHUN, FaceStation 2 de Suprema y SpeedFace V5L [TD] de ZKTeco [1].

2.4.1. Anviz FacePass 7

FacePass 7 [3] es un producto de reconocimiento facial y RFID lanzado por Anviz, con tecnología de infrarrojos (v. Figura 2.12). Utiliza el algoritmo central BioNANO, líder en el mundo capaz de comparar caras en menos de 300 ms. La detección de rostros, la identificación y los mensajes en tiempo real se pueden implementar fácilmente. Puede realizar un reconocimiento facial preciso en varios entornos. Tiene un potente procesador *Dual-core* 1 GHz y una plataforma informática de *hardware* de 124 x 155 x 92 mm con cámara dual y pantalla táctil HD TFT de 3,2". Se puede comunicar mediante TCP/IP, RS485, USB y Wi-Fi. Dispone de tres modos de identificación: facial, con tarjeta, y con identificador y contraseña.

Figura 2.12: FacePass 7. Recuperada de [3].

2.4.2. CrucialTrak BACS Quattro

BACS Quattro [6] de CrucialTrack es el primer sistema de autenticación sin contacto multibiométrico del mundo que ofrece la opción de utilizar hasta cuatro métodos de autenticación en un dispositivo: huella dactilar, cara, iris y venas de la palma de la mano (v. Figura 2.13).

Tener diferentes combinaciones de tecnologías biométricas disponibles en un dispositivo proporciona un amplio espectro, desde una experiencia de usuario fluida hasta un alto nivel de seguridad.

Cuenta con un procesador *Intel Core i3*, opciones de almacenamiento de 8 GB, 64 GB y 128 GB, y comunicaciones Gigabit Ethernet, RS-485, Wiegand in/out y *Relay* x 2. Sus dimensiones son 200 *x* 192 *x* 200 mm.

Figura 2.13: BACS Quattro. Recuperada de [6].

Cara

La tecnología de reconocimiento facial única de CrucialTrak ofrece la experiencia de autenticación más rápida y avanzada, autenticando al usuario en menos de un segundo.

Huella dactilar

Debido a que cada huella dactilar individual es única, la modalidad de huella dactilar puede incluso distinguir entre gemelos idénticos. Permite una experiencia de usuario higiénica y sin contacto y es capaz de reconocer simultáneamente tres dedos y las venas de la palma de la mano.

Venas de la palma

La modalidad de venas de la palma de la mano es altamente fiable y ofrece una autenticación rápida mientras permite mantener la palma de la mano en una posición muy natural sobre el lector. Su tasa de falsa aceptación es de 0,00001 %, prácticamente cero. Dispone de detección anti fraude *liveness*.

Iris

El primer mecanismo de seguimiento automático del mundo garantiza una autenticación rápida y la tecnología infrarroja puede detectar el iris independientemente de la luz ambiental.

2.4.3. IDEMIA VisionPass

VisionPass es un dispositivo de control de acceso biométrico sin fricción de IDEMIA. Este dispositivo es robusto y fiable. Proporciona verificación en movimiento en un segundo en múltiples ángulos y en todas las condiciones de luz, y es resistente a todo tipo de intentos de suplantación de identidad (v. Figura 2.14).

VisionPass combina un conjunto óptico de última generación de cámaras 2D, 3D e infrarroja con los últimos avances de IDEMIA en inteligencia artificial y procesamiento de imágenes, lo que permite un alto nivel de seguridad y comodidad para el usuario.

VisionPass se puede implementar en cualquier lugar: interior (pared o montado en una puerta) o al aire libre (clasificación IP65).

Dispone de una CPU *Nvidia ARM Cortex-A15 Quad-Core* 2, 1 GHz, pantalla táctil capacitiva a color WVGA de 7”, opciones de comunicaciones Ethernet, RS485, RS422, USB3, Wi-Fi y 4G. Su tamaño es de 325 x 143 x 110 mm.

Figura 2.14: VisionPass. Recuperada de [16].

2.4.4. Invixium IXM TITAN

IXM TITAN [18] funciona con uno de los procesadores más avanzados, el *Qualcomm Snapdragon 820*, con lo último en potencia de procesamiento, conectividad, gráficos, detección de rostros, fiabilidad y eficiencia de la batería. Para adaptarse a los entornos de trabajo en evolución, TITAN incorpora reconocimiento facial sin contacto con o sin mascarilla, detección de mascarillas, modalidad de huellas dactilares y venas de los dedos y autenticación multifactor.

IXM TITAN cuenta con una gran cantidad de características. Con una cámara de 21 megapíxeles, TITAN puede realizar reconocimiento facial con o sin mascarillas (v. Figura 2.15) y detección de mascarilla con una velocidad y precisión inigualables. Tiene un rendimiento promedio de reconocimiento de 15 a 18 caras por minuto. El almacenamiento robusto de usuarios y transacciones, una pantalla LCD *Corning Gorilla Glass* de 5" y opciones de conectividad avanzadas como Wi-Fi, Bluetooth, NFC y conectividad móvil 3G y LTE completan una experiencia de usuario impecable de TITAN. Con el kit de mejora instalado, TITAN cuenta con una cámara termográfica infrarroja térmica para una detección rápida de la temperatura que puede realizarse simultáneamente con el reconocimiento facial (v. Figura 2.15). Y ahora, todas las funciones principales de TITAN se pueden realizar sin contacto.

Figura 2.15: IXM TITAN. Recuperada de [18].

Tiene sistema operativo Android Nougat, almacenamiento flash universal 2.0 de 64 GB, 4 GB de RAM PoP LPDDR4 a 1 886 MHz, GPU *Andreno 530*, pantalla 1 080 p (ultraHD), opciones de comunicaciones TCP/IP, RS232, RS485 (OSDP *Compliant*) y USB-Aux, Wi-Fi, y unas dimensiones de 27 *x* 9 *x* 9 cm. Soporta múltiples tipos de tarjeta de indentificación RFID.

2.4.5. LIPSFace AC770

LIPSFace AC770 [21] es un sistema de Inteligencia Artificial de reconocimiento facial 3D sin contacto basado en autenticación biométrica con detección *liveness* por visión avanzada 3D con tecnología *Intel RealSense* y acelerado por el kit de herramientas *Intel OpenVINO* para seguridad de alto nivel (v. Figura 2.16).

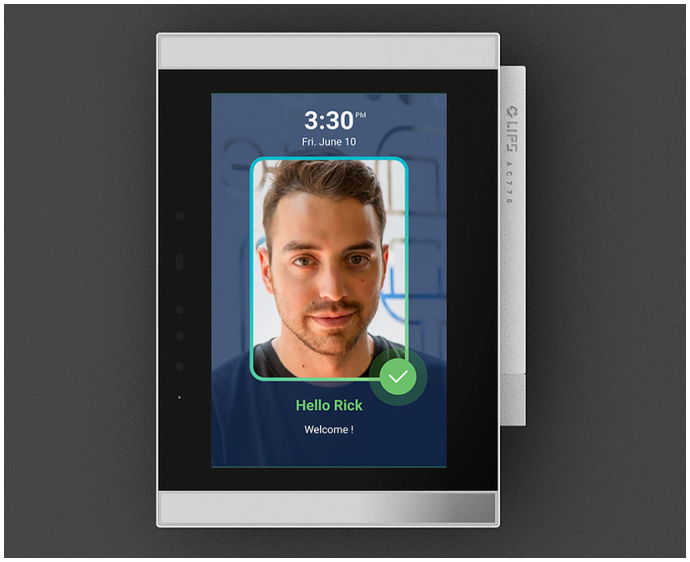

Figura 2.16: LIPSFace AC770. Recuperada de [21].

La detección de *liveness* 3D con IA y *anti-spoofing* o anti suplantación exclusiva de LIPS proporciona una experiencia de autenticación ultrarrápida, precisa y sin contacto de 0,3 segundos donde se requiere un nivel de seguridad superior, como centros corporativos, oficinas comerciales, estaciones, aeropuertos, bancos, clubes VIP, instituciones y fincas. Además, LIPSFace AC770 logra un 98,89 % de precisión con la base de datos MegaFace y un 99,83 % con LFW.

LIPSFace puede procesar hasta 20 000 usuarios localmente y ofrece dos paquetes de *software* de administración para escenarios de uno o varios terminales. *Edge Management Software* (EMS) es para la gestión de un solo terminal con un diseño de interfaz de usuario simple y fácil de usar. *Centralized Management Software* (CMS) se usa para la administración de múltiples terminales que proporciona una fácil integración en aplicaciones y plataformas de usuario con API RESTful.

Dispone de un procesador *Intel N4200 Quad-core* 2,5 Ghz, GPU *HD Graphics 505* y 4 GB de RAM. El almacenamiento es EMMC de 32GB, pero tiene opciones disponibles de almacenamiento adicional de 128GB, 256GB y 512GB. La pantalla táctil es LCD de 10,1". El dispositivo tiene lector de tarjetas de identificación e interfaces de red RJ45 1 Gb Ethernet, Wi-Fi y Bluetooth, Wiegand *in/out*, *Relay* y USB 2.0.

CAPÍTULO 3
Contexto legal y social

En este capítulo se expone el contexto legal y social a nivel mundial, europeo y en España a partir de algunas de las noticias más relevantes relacionadas con el reconocimiento facial y la protección de datos personales de los últimos años. También se presentan algunos de los problemas asociados a las tecnologías de reconocimiento facial.

3.1 Situación del reconocimiento facial en el mundo

Durante la última década, el uso del reconocimiento facial en la seguridad se ha ido haciendo cada vez más común en el mundo [38]. Se espera que el mercado de la tecnología de reconocimiento facial alcance los 3 100 millones de dólares estadounidenses en el año 2022 [30]. Esta tecnología se utiliza en numerosas aplicaciones en la mayor parte de países del mundo: seguridad aeroportuaria, investigaciones policiales, búsqueda de desaparecidos, etiquetado de fotos, forma de pago, desbloqueo del *smartphone*, etc. En el año 2020, según [38], habían 98 países utilizando tecnologías de reconocimiento facial para vigilancia y 11, que habían aprobado su uso pero todavía no las habían implementado. Solo se ha prohibido en tres países: en Bélgica, en Luxemburgo y en Marruecos. La expansión de esta tecnología ha planteado cuestiones importantes sobre el impacto en la privacidad de una vigilancia tan generalizada.

La mitad de los países de América del Norte utilizan actualmente la vigilancia por reconocimiento facial. Más del 50 % de los estadounidenses se encuentran actualmente en las bases de datos de reconocimiento facial de la policía. El Departamento de Seguridad Nacional de Estados Unidos espera realizar exploraciones de reconocimiento facial en el 97 % de todos los viajeros aéreos para 2023. Se espera que los ingresos del mercado global de biometría aeroportuaria alcancen los 389 millones de dólares estadounidenses para 2022 [30]. Estos sistemas también han comenzado a imponerse en los principales aeropuertos de India y China.

La tecnología de reconocimiento facial se utiliza o ha sido aprobada para su uso en dos docenas de aeropuertos de EE. UU. y está en uso en más de 30 departamentos de policía estatales y locales. Al mismo tiempo, un número creciente de ciudades estadounidenses luchan por prohibir esta tecnología. En mayo de 2019, San Francisco se convirtió en la primera ciudad del país en prohibir por completo la tecnología de reconocimiento facial. Desde entonces, varias otras ciudades, incluidas Oakland y Northampton, han votado a favor de prohibir esta tecnología.

China es el país con mayor proporción de cámaras de seguridad por habitante (hay aproximadamente una cámara CCTV por cada 12 ciudadanos en todo el país) y también es el proveedor líder de *hardware* de reconocimiento facial en todo el mundo. Hasta la

fecha, China ha vendido o proporcionado tecnología de reconocimiento facial a al menos 16 países fuera del sudeste asiático y se prevé que represente aproximadamente el 45 % del mercado mundial de reconocimiento facial para 2023. Desde hace meses, dicho país ha ampliado el uso de esta tecnología para utilizarlo como un medio para controlar los movimientos de las personas positivas en coronavirus, y otros países como Corea del Sur, Taiwán, Singapur o Rusia también están haciendo lo mismo. En Moscú, han desplegado más de 100 000 cámaras de seguridad para vigilar que no se infrinjan las normas.

3.2 Situación del reconocimiento facial en Europa

La tecnología de reconocimiento facial está actualmente en uso o ha sido aprobada para su uso en 32 países de Europa. La policía de Londres desplegó una serie de cámaras CCTV de reconocimiento facial en toda la ciudad en enero de 2020. La policía alemana actualmente usa esta tecnología y tiene planes para instalar cámaras de reconocimiento facial en 134 estaciones de trenes y 14 aeropuertos [38].

El gobierno serbio está desarrollando el proyecto de «ciudad segura» en Belgrado, que incluye la instalación de cámaras de vigilancia en toda la ciudad, con tecnología de reconocimiento facial, suministradas por el fabricante chino Huawei. Es la única ciudad del continente europeo que cuenta con este sistema [29].

Como en gran parte del mundo occidental, el uso del reconocimiento facial para la vigilancia en Europa se ha enfrentado a una reacción violenta sustancial. Francia y Suecia prohibieron recientemente el uso del reconocimiento facial en las escuelas. En 2019, Bélgica descubrió que un proyecto piloto que utilizaba tecnología de reconocimiento facial en un aeropuerto infringía la ley federal [38].

En Europa, el Artículo 9 del Reglamento General de Protección de Datos (RGPD) prohíbe de manera general el tratamiento de datos biométricos, que son categorizados como datos personales especiales. Esta prohibición tiene excepciones cuando concurren determinadas circunstancias, como por ejemplo:

- el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales;
- el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social;
- el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;
- el tratamiento es necesario por razones de un interés público esencial;
- el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud.

3.3 Situación del reconocimiento facial en España

En España, esta tecnología permite extraer dinero en un cajero automático de varias oficinas de CaixaBank en Barcelona sin necesidad de introducir un PIN, abrir una cuenta bancaria con un selfi y asistir a conciertos y a otros eventos multitudinarios [30]. La Estación Sur de autobuses de Madrid, por la que pasan más de 20 millones de viajeros al

año, también cuenta con más de un centenar de cámaras y un sistema de reconocimiento facial, que se empezó a implantar en 2016 para identificar a delincuentes y, según sus responsables, ha servido para reducir la actividad de los carteristas [30].

Desde octubre de 2019, la Empresa Municipal de Transportes (EMT) de Madrid está probando en una de sus líneas una tecnología de reconocimiento facial como método de pago [23].

España también utiliza en varios de sus principales aeropuertos un sistema de identificación biométrica instalado por Aena para realizar la facturación y el embarque de los viajeros sin que tengan que mostrar su documentación [23].

En marzo de 2019, Aena puso en funcionamiento, junto a Air Europa, un proyecto piloto en el aeropuerto de Menorca que permite a los pasajeros acceder a la zona de embarque y subirse al avión mediante reconocimiento facial.

En febrero de 2021, el aeropuerto Adolfo Suárez Madrid-Barajas también inició un proyecto piloto de reconocimiento facial que atiende a las nuevas medidas de seguridad sanitaria implantadas como consecuencia de la COVID-19. Este sistema cumpliría la exigencia fijada por la Comisión Europea (que entrará en vigor en 2022) de que todos los países que forman parte del espacio Schengen cuenten con una tecnología que permita que los visitantes no Schengen registren su identidad de forma rápida y segura, incluidos sus datos biométricos (rostro y huellas dactilares). La Unión Europea ya está trabajando en implementar esta medida con un gasto de hasta 302,5 millones de euros [8] y está preparando una gran base de datos que recopilará las huellas dactilares e imágenes faciales de más de 400 millones de personas de terceros países para controlar la entrada y salida del espacio Schengen [30].

La Justicia, a través de la Audiencia Provincial de Barcelona, se ha pronunciado sobre uno de los casos del sistema de reconocimiento facial de Mercadona implementado en julio de 2020 por la empresa AnyVision[1] y ha concluido que existe una violación de la privacidad. El reconocimiento facial de Mercadona fue creado para detectar, en menos de 0,3 segundos, personas con una sentencia firme de orden de alejamiento del establecimiento. Pero el tribunal entendió que Mercadona no estaba protegiendo el interés público sino los intereses privados o particulares de la empresa, de modo que consideraba que ese sistema suponía una violación de privacidad. Mercadona ha cancelado el sistema en pruebas que se había implementado incialmente en 40 tiendas de Valencia, Mallorca y Zaragoza [27].

España dispone de legislación sobre protección de datos (Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales) pero carece de una normativa específica sobre reconocimiento facial y se atiene a lo que indica el Reglamento General de Protección de Datos (RGPD), ya comentado en la sección 3.2 de este capítulo [23].

3.4 Problemas del reconocimiento facial

Las tecnologías de reconocimiento facial, así como otras tecnologías biométricas, pueden vulnerar derechos humanos, como el derecho a la privacidad, a la protección de datos o a la no discriminación.

El problema de la discriminación se debe a que los sistemas de reconocimiento facial son mucho menos precisos con con algunos grupos demográficos que con otros: no tienen tanta precisión identificando caras de personas asiáticas o de raza negra [23]. En

[1] https://www.anyvision.co

diciembre de 2019, un estudio del Instituto Nacional de Estándares y Tecnología (NIST), dependiente del Departamento de Comercio de EE. UU., vio, para la comparación uno a uno (*one-to-one matching*), tasas más altas de falsos positivos para rostros asiáticos y afroamericanos en comparación con las imágenes de caucásicos. Los diferenciales a menudo variaban desde un factor de 10 hasta 100 veces, según el algoritmo individual [25].

En 2019, Kneron[2], una empresa centrada en tecnología de inteligencia artificial, imprimió máscaras tridimensionales de alta calidad (v. Figura 3.1) para comprobar si los sistemas de reconocimiento facial extendidos por el mundo eran capaces de detectar estos dispositivos falsos, y no lo fueron. Pudieron pagar en comercios que permitían pagos a través de WeChat y AliPay utilizando la máscara con la cara de otra persona. En cambio, no fueron capaces de desbloquear dispositivos de Apple con Face ID [32].

Figura 3.1: Máscara tridimensional de alta calidad de Kneron. Recuperada de [32].

Además, estas tecnologías transgreden de forma sistemática la presunción de inocencia y ya ha habido más de un caso en el que un error de esta tecnología ha llevado a la cárcel a un inocente. A estos problemas se le suman cuestiones como el uso que se vaya a hacer con los datos biométricos, los posibles fallos de seguridad que permitan accesos no autorizados a las bases de datos y los polémicas usos en la vigilancia masiva que se han realizado en gran parte de los países de la Unión Europea [23].

[2] https://www.kneron.com

CAPÍTULO 4

Variables a considerar en la aplicación de un sistema de identificación facial

En el presente capítulo, primero, se expone la metodología a seguir en el estudio de las variables. A continuación, se estudia la viabilidad de instalar un sistema de reconocimiento facial para acceder a las instalaciones y autenticarse en los equipos informáticos de una compañía de servicios (como juzgados, centros deportivos, oficinas de una consultoría, etc.). Por último, se explican las principales variables a tener en cuenta a la hora de implementar un sistema de identificación facial en una compañía de servicios.

4.1 Metodología

Primeramente, se ha realizado un cuestionario para conocer la opinión de 16 expertos en la materia y poder identificar la predisposición, viabilidad y aplicabilidad de la implementación de tecnologías de reconocimiento facial para el control de acceso a instalaciones y la autentificación en los equipos informáticos en un entorno de organizaciones de servicios.

Seguidamente, se han analizado los sitios web y las hojas de especificaciones técnicas de las soluciones *hardware*, así como las API, las características y los requisitos de las soluciones *software* comentadados en las secciones 2.3 y 2.4 del Capítulo 2, para poder determinar las variables más relevantes a considerar antes de instalar un sistema de identificación facial seguro en una organización de servicios, tanto para acceder al lugar de trabajo como para autenticarse en los equipos informáticos.

4.2 Cuestionario a expertos

El cuestionario (v. Apéndice A), totalmente anónimo, se ha elaborado a través de la aplicación Formularios de Google y se ha enviado por correo electrónico a 16 expertos en la materia. Consta de tres principales preguntas de respuesta abierta y una última, no obligatoria, de múltiples opciones, para poder conocer la rama de actividad económica del puesto de trabajo del experto encuestado. Las cuatro preguntas se muestran a continuación.

1. *¿Qué sistema utiliza para identificarse o autentificarse en los equipos informáticos de su lugar de trabajo? (login y password, DNI electrónico, certificado digital, criptografía biométrica, ninguno...)*

2. *¿Cómo valoraría la utilización de un sistema de reconocimiento facial seguro para el acceso a su entorno de trabajo? ¿Podría detallarnos algunas razones?*

3. *¿Qué beneficios y problemas identificaría en la aplicación de un sistema de identificación facial seguro en el entorno profesional en el que usted trabaja habitualmente?*

4. *¿A qué rama de actividad económica pertenece su puesto de trabajo?*

De las respuestas a la pregunta número 1 del cuestionario, tal y como se observa en la Figura 4.1, se puede extraer que el 62,5 % de los expertos encuestados usan el usuario y la contraseña para identificarse en alguno de los equipos informáticos de su lugar de trabajo. Por lo tanto, es el método más común de autentificación. El 37,5 % usa sistemas biométricos y el 25 % de estos detalla que utiliza la huella dactilar. Otros métodos de identificación menos utilizados (12,5 % cada uno de ellos) son el certificado digital FNMT en tarjeta, la dirección de correo electrónico y un código, el DNI, el certificado digital y el código QR. Algunos de los expertos usan más de un sistema de autenticación en su trabajo.

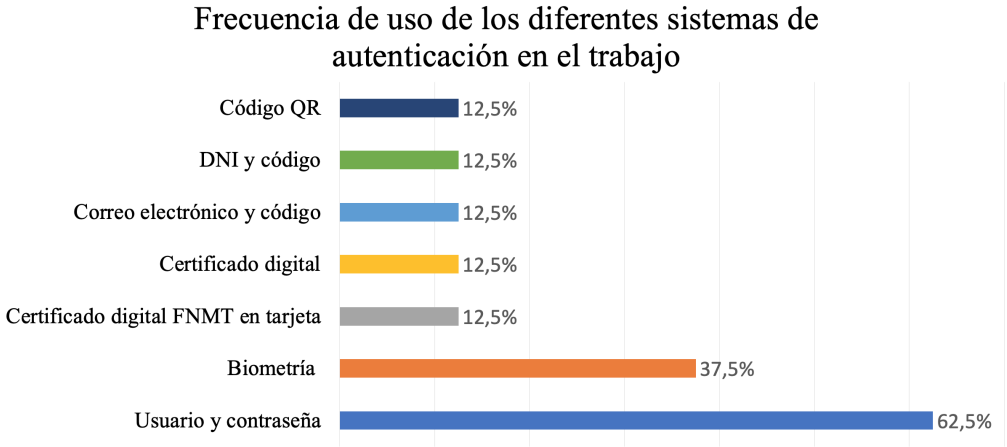

Figura 4.1: Frecuencia de uso de los expertos de los diferentes sistemas de autenticación en el trabajo. Elaboración propia.

El 87,5 % de las respuestas a la pregunta 2 valoran positivamente la utilización de un sistema de reconocimiento facial en su entorno de trabajo (v. Figura 4.2). Las principales razones son la comodidad y la rapidez de uso. Uno de los expertos añade que no caduca como las tarjetas, pudiendo así evitar trámites de renovación o reexpedición y que se evita la pérdida, olvido o sustracción. A otro de ellos le parece muy interesante que su computadora le permitiera abrir y cerrar sesión mediante un sistema de reconocimiento facial, debido a que es cómodo y aporta tranquilidad, ya que la sesión se puede cerrar si no está cerca después de un tiempo. El 12,5 % restante no confía en el reconocimiento facial como sistema de identificación.

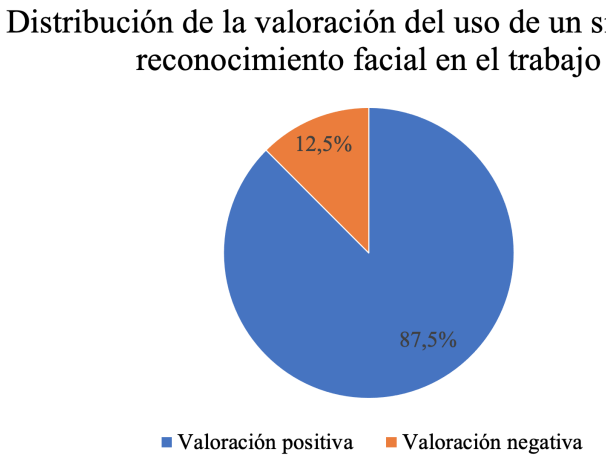

Figura 4.2: Distribución de la valoración de los expertos del uso de un sistema de reconocimiento facial en el trabajo. Elaboración propia.

Entre los beneficios de la aplicación de un sistema de identificación facial en el entorno profesional (comentados en las respuestas a la pregunta 3), destacan el fácil acceso, la seguridad, la comodidad y la eficiencia de uso. Se específica también que podría suponer un menor gasto económico en recursos humanos (ya que no se pierde tiempo en la identificación) y en expedición y mantenimiento de certificados y *hardware* asociado. Además, se menciona la confianza en la seguridad de la identificación, la robustez del proceso frente a posibles accesos en red y su gran proyección.

Los problemas de la aplicación de esta tecnología como sistema de autenticación que se han mencionado son: la necesidad de un segundo sistema de acceso para el caso de que no funcione, el requerimiento de cuidado en la custodia de la información personal, el coste económico del equipo necesario y su mantenimiento, la cesión y protección de datos, necesidad de procedimientos adicionales en entornos de trabajo, el consumo de recursos del equipo que realiza la identificación, y el binomio privacidad de los datos y necesidad de realizar la identificación en diferentes equipos del lugar de trabajo. El 12,5 % que no confiaba en la tecnología de reconocimiento facial en la pregunta 2 no menciona beneficios de esta e indica la posibilidad de ataques y la poca fiabilidad como problemas.

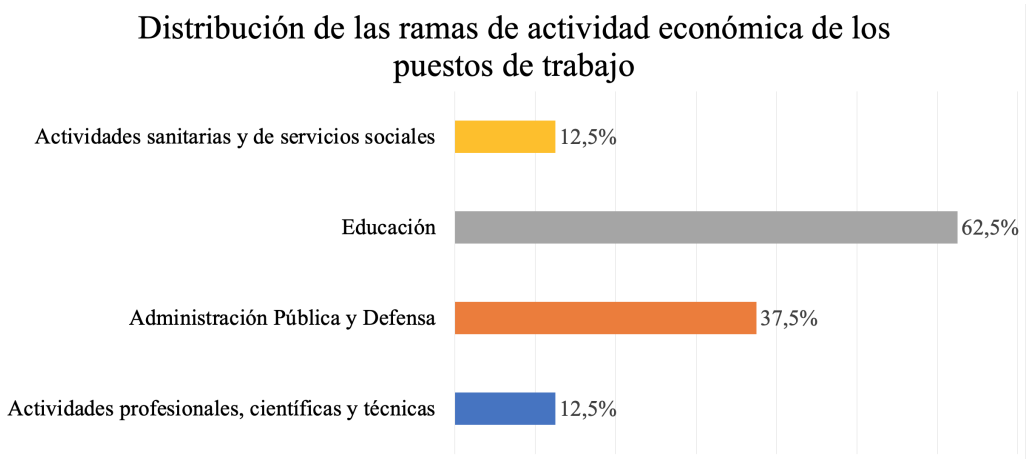

Figura 4.3: Distribución de las ramas de actividad económica de los puestos de trabajo de los expertos. Elaboración propia.

Las ramas de actividad económica pertenecientes a los puestos de trabajo de los expertos (pregunta 4) son: actividades sanitarias y servicios sociales (12,5 %), educación

(62,5 %), Administración Pública y Defensa (37,5 %), y actividades profesionales, científicas y técnicas (12,5 %). La distribución de estas se muestra en la Figura 4.3. Algunos de los expertos tienen más de un puesto de trabajo que pertenecen a distintas ramas.

4.3 Variables

En esta sección se exponen las variables más relevantes a considerar a la hora de instalar un sistema de reconocimiento facial en una compañía de servicios. En la Tabla 4.1 se muestra el resumen de estas variables que son explicadas en las siguientes secciones.

Variable	Comentario
4.3.1. Uso del sistema	Puede ser: **autenticación** en equipos informáticos, **control de acceso** a instalaciones o **videovigilancia**.
4.3.2. Tipo de solución	Se puede elegir una solución ***software*** gratuita o de pago (basada en SaaS, API REST *auto-hospedada* o biblioteca de código abierto) o bien, una solución ***hardware***.
4.3.3. Precisión	La gran mayoría de métodos superan el **99 %** de precisión en el banco de pruebas LFW.
4.3.4. Velocidad	La mayoría de soluciones son capaces de reconocer una cara en **menos de un segundo**.
4.3.5. Sistema secundario	Si tiene o no un sistema secundario de identificación (biométrico, código numérico, usuario y contraseña, tarjeta, código QR, etc.
4.3.6. Seguridad de los datos	Los datos personales pueden ser almacenados en el **dispositivo *hardware*** (encriptados), en un **servidor** propio o en uno ajeno.
4.3.7. Precio	Existen soluciones *software* **gratuitas** y también con pago por **paquete de licencias**, con planes de **pago por uso** y con **planes diarios** y **mensuales**. El rango de precios de las soluciones *hardware* es muy amplio.
4.3.8. Número de usuarios	El número de imágenes de caras de usuarios almacenados puede afectar tanto al precio como a la velocidad de reconocimiento facial.
4.3.9. Número de identificaciones	El número de identificaciones afecta principalmente al precio de soluciones *software* como la de Face^{++}.
4.3.10. Cámara	Hay que decidir el **tipo de cámara**, si tiene que tener **tecnología WDR**, la **resolución** y también cómo hacer la **instalación**.
4.3.11. Iluminación	Se debe tener en cuenta la iluminación y su variación a lo largo del día del lugar donde se va a instalar la cámara.

Tabla 4.1: Variables a considerar para la instalación de un sistema de reconocimiento facial.

4.3.1. Uso del sistema

La variable uso hace referencia al objetivo de la instalación del sistema de reconocimiento facial o al tipo de uso que se va a hacer de este. Este puede ser autentificación en equipos informáticos (que puede incluir firmar digitalmente), control de acceso a insta-

laciones (compañía de servicios) y videovigilancia. Dependiendo del uso, será más conveniente un tipo de solución u otro.

4.3.2. Tipo de solución

Según los conocimientos de programación y sobre aprendizaje automático (*machine learning*) que se tengan y según donde se quieran alojar los datos recogidos por el sistema, se puede escoger una de las soluciones *software* mencionadas en la sección 2.3, ya sea gratuita (como OpenCV y CompreFace) o de pago (como Face^{++} y Microsoft Azure Cognitive Services Face API). Y en el caso de que el sistema sea para autenticación en un equipo informático, es posible utilizar la cámara ya instalada en el equipo o conectar otra, por ejemplo, una *Logitech C920 HD Pro Webcam*, que se puede encontrar en Amazon.es por 79, 90 € , IVA incluído.

En el caso de desarrollar un aplicación de autentificación facial para iniciar sesión en un equipo usando el *software* nombrado anteriormente, el sistema operativo de la máquina debería permitir ejecutar la aplicación desarrollada antes de iniciar la sesión.

Otra posibilidad es escoger alguno de los dispositivos de la sección 2.4 que ya incorporan el *software* de identificación facial con una interfaz gráfica usable. Este tipo de soluciones está pensada para control de acceso a instalaciones.

Para tareas de vigilancia y seguridad en espacios más pequeños, una buena opción podría ser la Google Nest Cam o la Tend Secure Lynx Indoor.

4.3.3. Precisión

Es la precisión del sistema de reconocimiento facial en las tareas de identificación y está muy relacionada con el nivel de seguridad de la autentificación (por ejemplo, para evitar suplantaciones de identidad). La gran mayoría de métodos más populares (DeepID3, FaceNet, Cosface, ArcFace...) superan el 99 % de precisión [42]. ArcFace (2018) alcanzó un 99,83 % de precisión en el banco de pruebas LFW. Varias de las soluciones comentadas en las secciones 2.3 y 2.4 utilizan alguno de estos métodos.

4.3.4. Velocidad

La gran mayoría de soluciones del mercado son capaces de reconocer una cara en menos de un segundo. Por ejemplo, el dispositivo DS-K1T671T de HIKVISION realiza el reconocimiento facial en un tiempo menor o igual a 0,2 segundos por cara de usuario.

4.3.5. Sistema secundario

Se debe decidir si se necesita un sistema secundario al de reconocimiento facial, y si es así cuál o cuáles: biométrico (huella dactilar, venas de la palma de la mano, iris del ojo), código numérico o alfanumérico, usuario y contraseña, tarjeta, código QR, etc. Este sistema podría ser usado como complementario al de reconocimiento facial, o como auxiliar, en el caso de que el sistema principal de identificación de cara falle. Un sistema complementario intrusivo, con contacto, como por ejemplo, el usuario y contraseña o la huella dactilar, aportaría más seguridad al sistema, pero anularía las ventajas del reconocimiento facial (rapidez de acción y la no necesidad de que el usuario manipule el sistema). El iris sí que podría se una buena opción. Por ejemplo, BACS Quattro de CrucialTrack [6] permite usar cualquier combinación de hasta cuatro modalidades biométricas en un mismo lector.

Con la biblioteca de *software* OpenCV [26], es posible desarrollar un sistema capaz de leer códigos de barras y códigos QR, que podría usarse como sistema complementario.

4.3.6. Seguridad de los datos

El nivel de seguridad de los datos personales biométricos almacenados va a depender del tipo de solución escogida y de su configuración. Por ejemplo, si se escoge la solución de Amazon Rekognition [4] o de Microsoft Azure Cognitive Services Face API [22], los datos faciales personales se guardarían en sus respectivos servidores. Si en cambio, se opta por una de las soluciones *hardware* de la sección 2.4, los datos encriptados generalmente son almacenados en el propio dispositivo. Si se desarrolla una solución utilizando una biblioteca de *software*, como OpenCV [26] o Face Recognition [14], los datos se pueden guardar localmente en discos duros de la compañía de servicios que implementa el sistema, en servidores propios o también, en un servidor externo.

4.3.7. Precio

Como se ha comentado anteriormente en la sección 2.3.1 del Capítulo 2, existen diferentes bibliotecas *software* gratuitas. Por ejemplo, CompreFace [9] puede ser fácilmente integrada en cualquier sistema usando Docker y provee de una API REST para reconocimiento facial. También hay bibliotecas gratuitas que no disponen de una API REST, pero algunas de ellas son muy potentes, con una amplia cantidad de algoritmos optimizados y muchos tutoriales y ejemplos de código, como OpenCV, y otras son muy sencillas de usar, con muy buena precisión, como Face Recognition [14], utilizada en el trabajo de [24] para desarrollar un sistema de reconocimiento facial localmente.

Por otro lado, para poder tener una idea de los precios de las soluciones *software* de pago, por ejemplo, Amazon Rekognition [4] ofrece servicios de búsqueda de rostros en vídeo y en directo por 0,12 USD/min y almacenamiento de metadatos de rostros por 0,00001 USD/metadatos de rostros al mes.

Face^{++} [11] tiene precios según el uso que se haga de los diferentes servicios de la API (*pay as you go*) y también tiene planes de servicios de reconocimiento facial diarios (100 USD al día) y mensuales (1 000 USD al mes), que ofrecen una llamada a la API por segundo. Mil licencias *online* de un año del SDK de reconocimiento facial de Face^{++} tienen un precio de 4 000 USD.

FaceX tiene un servicio básico que ofrece 750 llamadas a la API por día a un precio de 3 USD por día.

Microsoft Azure Cognitive Services Face API [22] tiene una versión gratuita que permite 20 transacciones por minuto y un máximo 30 000 transacciones gratis al mes. En Europa, hasta el primer millón de transacciones del plan estándar cuesta 1 USD ($) cada 1 000 transacciones con 10 transacciones por segundo. El precio del almacenamiento de caras es de 0,01 USD por 1 000 caras y por mes.

El precio de todas estas soluciones *software* no incluye el coste de las cámaras ni de otros equipos o componentes *hardware*.

Los precios de las soluciones o dispositivos *hardware* de la sección 2.4 (que también incluyen el *software* de identificación facial) pueden ir desde los 320 € sin IVA la unidad (ANVIZ FACEPASS 7 + CROSSCHEX) hasta los 1 300 € sin IVA (SpeedFace V5L [TD] de ZKTeco). Aunque hay soluciones por encima y por debajo de este rango. También, hay que tener en cuenta que algunas de estas empresas fabrican bajo pedido, que para

saber el precio hay que consultarlo con ellas y que pueden exigir que el cliente compre un número mínimo determinado de unidades.

4.3.8. Número de usuarios

Esta variable indica el número de usuarios que se va a dar de alta en el sistema, es decir, cuántas imágenes de caras diferentes va a haber guardadas en dicho sistema. Es importante tener en cuenta el número de usuarios almacenados porque afecta directamente al precio de soluciones *software* como la de Amazon [4] y la de Microsoft Azure [22] y también, porque puede afectar a la velocidad de reconocimiento de una cara, tanto en soluciones *software* como *hardware* (v. secciones 2.3 y 2.4). Las compañías de los dispositivos mencionados en la sección 2.4 suelen indicar en las especificaciones técnicas de dichos dispositivos tanto su capacidad de almacenamiento (en GB) como el número máximo de caras que permite almacenar, para verificación (1:1) y para identificación (1:N). Por ejemplo, IXM TITAN de Invixium dispone de un almacenamiento de 64 GB, de un número máximo de usuarios de 100 000 para tareas de identificación y de 500 000, para verificación (comprobación de si la identidad del usuario coincide con la de la imagen almacenada).

4.3.9. Número de identificaciones

El número de identificaciones total del sistema de reconocimiento facial por unidad de tiempo (día, mes o año) es relevante si se escoge una solución *software* de pago, como Face^{++} [11] o Microsoft Azure Cognitive Services Face API [22], ya que estas tienen planes de pago según el número de llamadas a la API y por cada autentificación, se realiza mínimo una llamada a la API.

4.3.10. Cámara

Dentro de esta variable, habría que tener en cuenta estos aspectos: el **tipo de cámara**, el **contraste**, la **resolución**, la **instalación** (distancia, ángulo, altura y ubicación) de la misma y la variación de **iluminación** ambiente.

Tipo de cámara

A continuación se muestran los principales diferentes tipos de cámara de vigilancia existentes y que podrían ser usados con alguna de las soluciones *software* de la sección 2.3. Todos los tipos de cámara no son excluyentes, es decir, en el mercado se pueden encontrar productos que combinan varios tipos.

- **Cámara de interiores.** Es perfecta para lugares iluminados. No necesitan disponer de características especiales relacionadas con la luminosidad.
- **Cámara de exteriores.** Tienen carcasas resistentes a golpes, lluvia, calor, etc.
- **Cámara térmica o infrarroja.** Es ideal para lugares oscuros o de muy baja luminosidad. Se pueden utilizar para para tareas de vigilancia las 24 horas del día, ya que son capaces de encender el sensor infrarrojo automáticamente cuando hay menos luz.

- **Cámara HD sobre cables coaxiales.** Capaz de transmitir audio y vídeo en alta calidad sobre cables coaxiales y sin interferencias con redes, ya que pueden operar completamente aisladas de redes de datos.
- **Cámara IP o de red.** Dispone de su propia dirección IP y se puede conectar directamente a la red. Permite observar la imagen que esté capturando mediante un dispositivo conectado a la cámara a través de internet.
- **Cámara con movimiento y *zoom*.** Se suele usar con circuitos cerrados de televisión (CCTV).
- **Cámara oculta o *minicámara*.** También llamada cámara espía. Generalmente se instala dentro de algún objeto, como en sensores de movimiento, detectores de humo, espejos, etc.
- **Cámara corporal o portátil.** Pueden ser parte del equipamiento de la policía y también se utilizan como cámaras de acción.
- **Cámara con objetivo ojo de pez o *fisheye*.** Permite crear una imagen panorámica o hemisférica ancha. Consigue ángulos de vista extremadamente anchos.
- **Cámara de reconocimiento facial.** Son cámaras que incorporan *software* de reconocimiento facial (v. sección 2.4).

Contraste

El contraste es un problema que aparece recurrentemente con las cámaras de control de acceso a un local y es generado porque la luz que proviene del exterior es más intensa que la luz artificialmente creada en el interior. Para evitar este problema habría que utilizar una cámara con tecnología WDR (*Wide Dynamic Range*), que permite a las cámaras ajustar de manera automática la luminosidad ante escenarios de gran contraste [20].

Resolución

En [20] se recomienda una resolución de cámara de entre 4 y 8 megapíxeles para cámaras de videovigilancia, ya que la mayoría de sistemas de reconocimiento facial necesitan que existan al menos 100 píxeles entre los ojos de un individuo para poder identificarlo. La resolución necesaria va a depender del tipo de sistema o del objetivo de este (autentificación en un equipo, control de acceso o vigilancia) y de la distancia desde la cara del sujeto a identificar hasta el objetivo de la cámara. Por ejemplo, la cámara del dispositivo de control de acceso DS-K1T671T de HIKVISION tiene solamente 2 megapíxeles, mientras que la de IXM TITAN de Invixium tiene 21 megapíxeles.

Instalación

A la hora de instalar una cámara de reconocimiento facial, principalmente, se deben tener en cuenta los siguientes factores.

- **Distancia.** Es la distancia desde el objetivo de la cámara hasta la cara de la persona a reconocer o identificar (v. Figura 4.5). Varía según la distancia focal del objetivo, medida en milímetros. HIKVISION indica que su dispositivo DS-K1T671T es capaz de reconocer caras desde los 300 cm hasta los 3 m de distancia. Los dispositivos BACS Quattro [6] y AC770 [21] de CrucialTrack y LIPSFace, respectivamente, tienen

una distancia de reconocimiento facial segura de hasta 1,5 m. En cambio, FacePass 7 de Anviz [3], solamente de hasta 80 cm.

En bibliotecas como Face Recognition [14], según la distancia entre la cara y el objetivo de la cámara, hay funciones que permiten conseguir mayor precisión o menor tiempo de reconocimiento variando el valor de los argumentos de dichas funciones. En [24] se realizan pruebas acerca de esto.

- **Ángulo.** Es el ángulo sólido desde el objetivo de la cámara en el cual es posible reconocer una cara (v. Figura 4.5). iT100 de Iris ID [19] tolera una inclinación vertical de $\pm 25^{o}$ y FacePass 7 de Anviz [3] permite $\pm 20^{o}$ tanto de forma vertical como horizontal. En [24] se vio que no era posible reconocer caras con un ángulo superior a $\pm 15^{o}$ utilizando la biblioteca Face Recognition [14].

- **Ángulo de depresión.** Es el ángulo de inclinación de la cámara respecto a la horizontal. El ángulo de depresión (α) recomendado para las cámaras de videovigilancia varía entre los 15^{o} y los 30^{o} (v. Figura 4.4), dependiendo de la ubicación y del fabricante [5, 15, 20]. En dispositivos de control de acceso este ángulo suele ser de 0^{o} (v. Figura 4.5). La cámara de iT100 de Iris ID [19] encuentra automáticamente al usuario y se mueve a una ubicación donde se pueden fotografiar los ojos y la cara del usuario.

- **Altura.** Es la distancia vertical de la cámara respecto al suelo (v. Figura 4.5). Para la instalación de cámaras de videovigilancia, Huawei [15] recomienda una altura (h) entre 2,5 m y 3,5 m (v. Figura 4.4). En general se recomienda una altura de 1,8 m y 2,2 m [20]. Los motivos de no instalarla a una altura demasiado baja son evitar posibles obstrucciones en la escena capturada y evitar golpes. Tampoco se debería instalar muy alta porque habría que inclinar la cámara demasiado y su alcance se reducidiría. Además, se grabarían cabezas en vez de caras y desde una mayor distancia [5].

- **Ubicación.** Es el lugar donde se va a instalar la cámara y los anteriores factores dependen de este. El tipo de cámara a escoger dependerá de si es en interior o en exterior, de si hay polvo en el ambiente, de las condiciones meteorológicas del sitio (humedad, lluvia, temperatura...), etc.

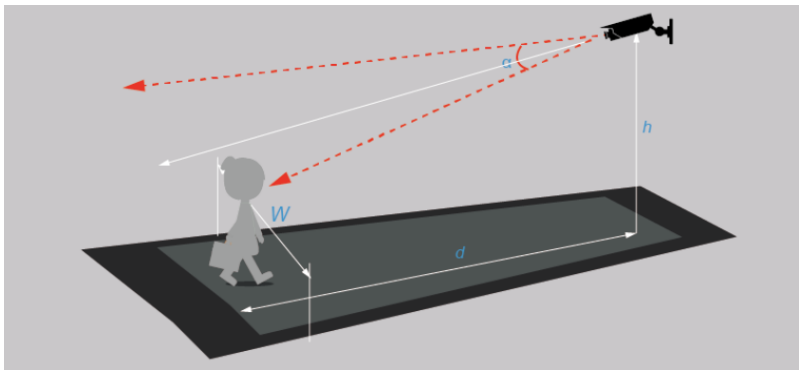

Figura 4.4: Requisitos de instalación de Huawei para la cámara de reconocimiento facial. Recuperada de [15].

Como ejemplo, en la Figura 4.5 se muestran las recomendaciones de instalación que hace la empresa Iris ID para su producto iT100 de control de acceso.

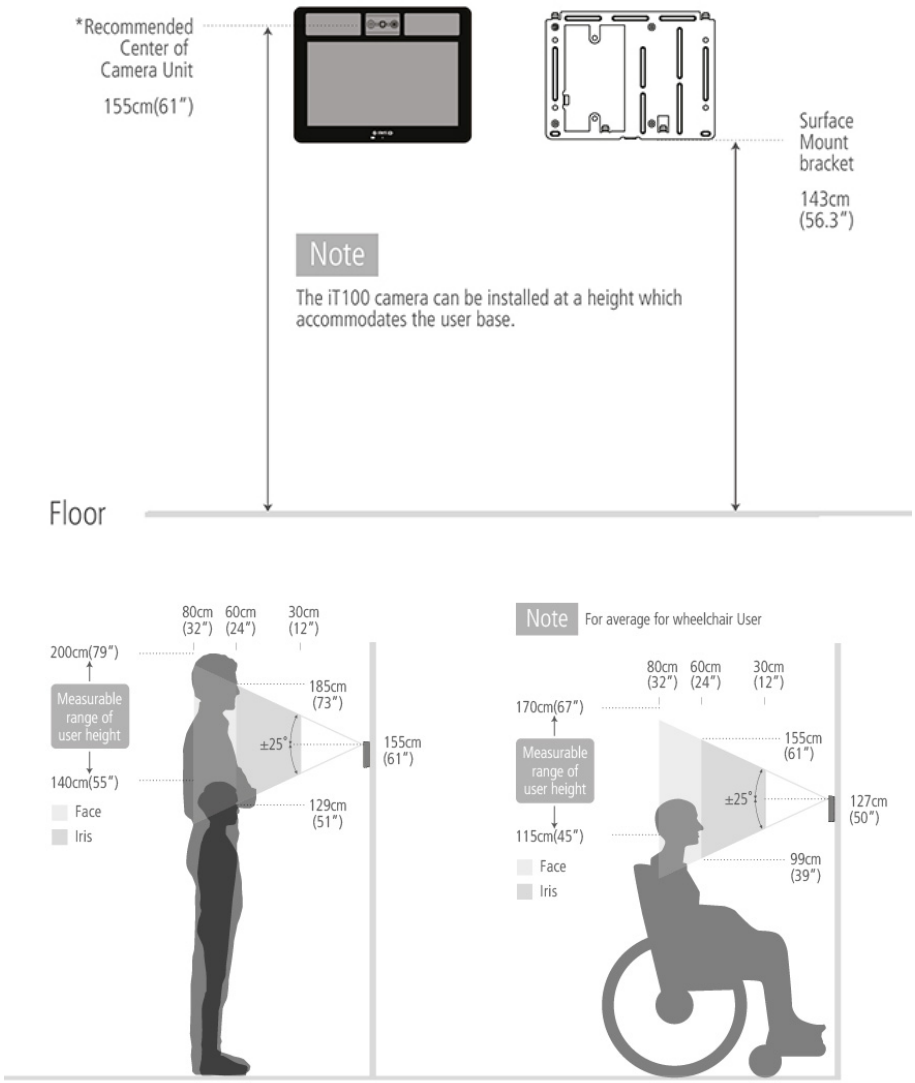

Figura 4.5: Instalación de iT100 de Iris ID. Recuperada de [19].

4.3.11. Iluminación

La iluminación ambiente del lugar donde se va a instalar el sistema y la variación de esta a lo largo del día afecta al reconocimiento facial. Tanto la exposición excesiva de luz como la escasa pueden afectar negativamente a la identificación de la cara. Lo ideal es una iluminación difusa, ya que no provoca grandes sombras ni brillos.

OpenCV [26] tiene funciones que permiten el tratamiento, el procesamiento o la transformación de imágenes que se pueden utilizar para solucionar los problemas de la iluminación.

CAPÍTULO 5
Diseño y desarrollo de la solución

En este capítulo se describen el diseño, las tecnologías utilizadas y el desarrollo de la solución tecnológica, Face Recognition Solutions, que, junto con las variables estudiadas y explicadas en el Capítulo 4, puede ayudar de una manera más práctica en la elección de una solución de reconocimiento facial.

5.1 Diseño de la solución

La solución práctica a desarrollar tiene el objetivo de ayudar a las compañías de servicios a escoger la solución de reconocimiento facial ideal para ellas, haciendo uso también de las variables mencionadas y descritas en el Capítulo 4.

Esta solución, llamada **Face Recognition Solutions**[1], va a consistir en una página web creada utilizando Wordpress[2], que tendrá un catálogo con todo tipo de soluciones de reconocimiento facial (catálogo de productos) en la página de inicio. En la barra lateral izquierda de esta página se situarán una serie de filtros para que la página muestre solamente los tipos de solución que el usuario quiera ver de todo el catálogo. Clicando en cualquiera de las soluciones mostradas en el catálogo, se mostrará el detalle de dicha solución en cuya descripción aparecerá un enlace que llevará a su sitio web oficial para poder ver así sus caractarísticas y sus especificaciones técnicas.

5.2 Tecnologías utilizadas

Antes de empezar a desarrollar la página web, es necesario instalar Wordpress y comprar un dominio y un *hosting*. En este caso se adquirirán ambos en Bluehost[3] por un año, por la rapidez y comodidad que ofrece, ya que se encargan ellos de configurar y gestionar la parte técnica.

Para desarrollar la página web, tal y como se ha dicho en la sección 5.1, se va a utilizar Wordpress y también los *plugins* WooCommerce (para crear la «tienda») y YITH WooCommerce Catalog Mode (que permite ocultar precios, el carrito y el proceso de pago de la tienda y lo convierte en un catálogo de productos). Asimismo, se va a usar el tema Storefront (que ha sido diseñado y desarrollado por los desarrolladores del núcleo de WooCommerce y cuenta con una integración profunda con el *plugin* WooCommerce y con muchas de las extensiones para WooCommerce) para personalizar la «tienda». Estos

[1] https://facerecognitionsolutions.com
[2] https://wordpress.org
[3] https://www.bluehost.com

dos *plugins* se pueden adquirir gratuitamente en la sección Plugins (tienda de *plugins*) de Wordpress.

5.3 Desarrollo de la solución

Una vez se ha configurado el dominio (facerecognitionsolutions.com) y el *hosting* de Bluehost con Wordpress, lo primero que se ha hecho es establecer el título del sitio web y la descripción corta, que aparecerán en la cabecera de la página (v. Figura 5.1).

Luego se han instalado y activado los *plugins* mencionados anteriormente (v. sección 5.2), WooCommerce y YITH WooCommerce Catalog Mode. Haciendo uso del *plugin* YITH WooCommerce Catalog Mode, se ha activado el modo catálogo para administradores y se ha desactivado la tienda. Después, usando el *plugin* de WooCommerce se ha cambiado la apariencia del catálogo indicando que se quieren cuatro productos por fila en vez de tres (v. Figura 5.1). En la opción «Personalizar» de la sección «Apariencia» de Wordpress se ha configurado la página de la tienda (llamada «Soluciones») como página de inicio («Ajustes de la página de inicio»).

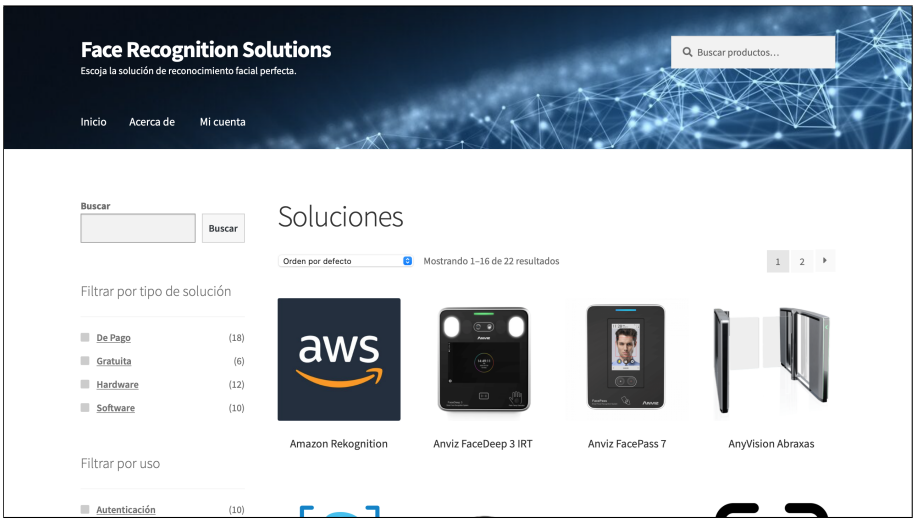

Figura 5.1: Página de inicio de Face Recognition Solutions. Elaboración propia.

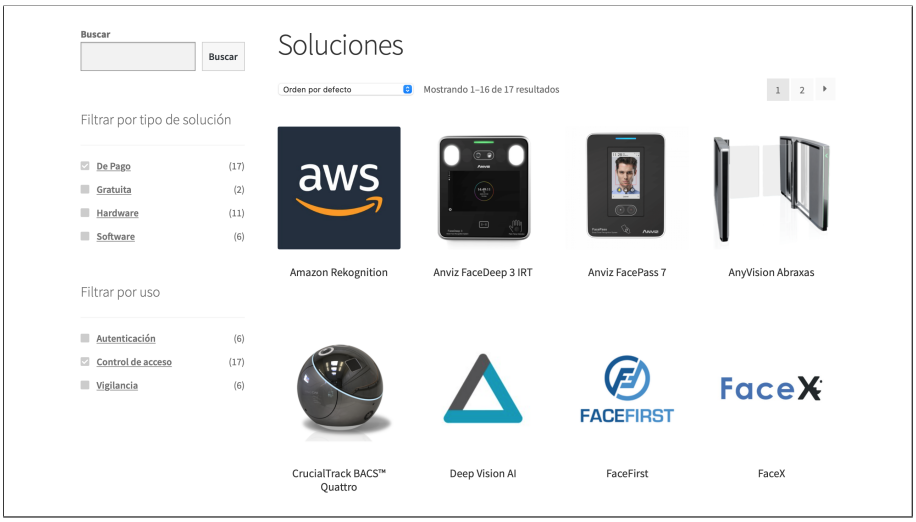

Figura 5.2: Filtros de producto de Face Recognition Solutions. Elaboración propia.

Seguidamente, se han creado los atributos de producto y sus respectivos términos («*Tipo de solución*: *De Pago*, *Gratuita*, *Hardware* y *Software*» y «*Uso*: *Autenticación*, *Control de acceso* y *Vigilancia*»), para luego poder crear los filtros de producto por atributo.

A continuación se han añadido todas las soluciones de reconocimiento facial como productos incluyendo en cada una el nombre, la descripción, la descripción corta, la imagen y los atributos que tiene (v. Figura 5.3).

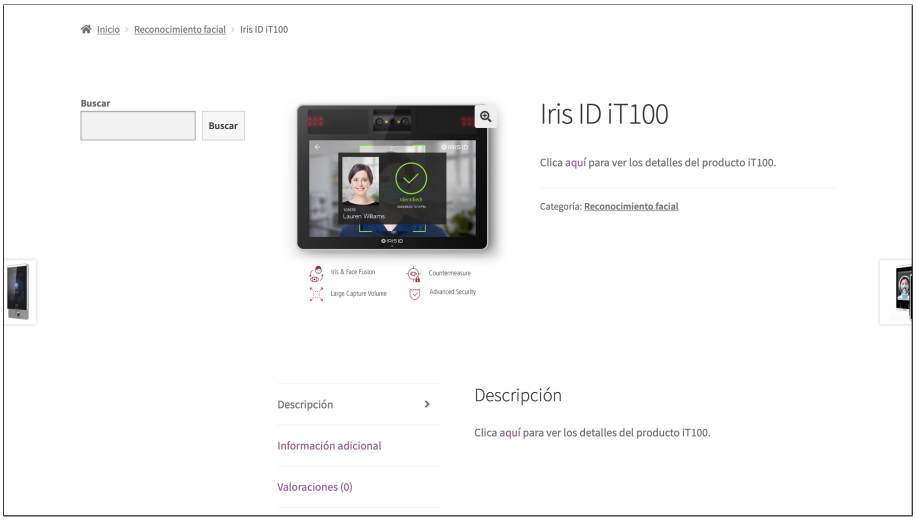

Figura 5.3: Página de detalle de producto de Face Recognition Solutions. Elaboración propia.

Después, con los *widgets* de WooCommerce se han añadido dos filtros de producto por atributo, uno para poder filtrar por tipo de solución y otro para filtrar por uso.

Por último, para terminar de personalizar la página web, en «Diseño», se ha indicado que se quiere que la barra lateral esté a la izquierda de la página, y en «Cabecera» se ha añadido una imagen y se ha cambiado el color del texto y de los enlaces a blanco para que destaquen sobre la imagen de la cabecera, que es de color oscuro.

CAPÍTULO 6
Conclusiones

Todos los objetivos propuestos para la realización de este trabajo se han llevado a cabo satisfactoriamente y es un verdadero orgullo haberlo conseguido. Gracias a este trabajo se han podido conocer las tecnologías de reconocimiento facial existentes en el mercado, tanto *software* como *hardware* y qué variables hay que tener en cuenta para implementarlas en una organización de servicios.

En primer lugar, se ha explicado el funcionamiento de un sistema de reconocimiento facial a partir de cada uno de sus componentes (detector facial, detector de puntos de referencia faciales y reconocimiento facial).

En segundo lugar, se ha estudiado la evolución histórica de las tecnologías de reconocimiento facial, las cuales aumentaron su precisión rápidamente gracias al uso de nuevas arquitecturas de red de clasificación de objetos, a la creación de grandes bases de datos y a las mejoras del *hardware*.

En tercer lugar, se han consultado los sitios web de las mejores soluciones *software* y *hardware* de reconocimiento facial que existen actualmente para conocer el contexto tecnológico, extraer sus características más relevantes e identificar variables importantes a considerar para la instalación de un sistema de identificación facial.

El contexto legal y social del reconocimiento facial en el mundo, en Europa y en España se ha conseguido conocer a partir de noticias de diferentes fuentes encontradas en internet.

Se ha logrado estudiar y establecer la viabilidad de la implementación de un sistema de autentificación facial tanto en los equipos informáticos como en el acceso a las organizaciones de servicios mediante un cuestionario formado por preguntas de respuesta abierta realizado a 16 expertos en la materia.

Gracias a las respuestas de los expertos al cuestionario y al estudio de las soluciones *software* y *hardware* actuales de reconocimiento facial, se han podido determinar y estudiar las principales variables a tener en cuenta para el desarrollo de un modelo viable de aplicación de un sistema de identificación facial segura en un entorno de organicaciones de servicios, creando así una guía teórica que puede servir de referencia para las compañías de servicios que deseen instalar un sistema con esta tecnología.

Por último, se ha conseguido crear una solución tecnológica con Wordpress consistente en una página web cuyo fin es complementar la guía teórica y ayudar de una forma más práctica a las empresas de servicios a elegir el sistema de reconocimiento facial más conveniente para ellas.

Para trabajos futuros, se puede pensar en el estudio de la aplicación de un sistema de identificación facial segura para una empresa de servicios concreta con demanda de niveles de seguridad elevados, como por ejemplo unos juzgados.

Bibliografía

[1] A&s Editorial Team. (3 de junio de 2020). Editor's choice: Top 10 facial recognition access control systems. Asmag.com. Recuperado el 15 de agosto de 2021 de https://www.asmag.com/showpost/31577.aspx.

[2] Analytics Insight. (29 de noviembre de 2019). Best facial recognition software. Recuperado el 14 de 2021 de https://www.analyticsinsight.net/best-facial-recognition-software/.

[3] Anviz Global. (s.f.). FacePass 7. Recuperado el 15 de agosto de 2021 de https://www.anviz.com/product/facepass7-face-recognition.html.

[4] AWS. (s.f.). Amazon Rekognition. Recuperado el 11 de agosto de 2021 de https://aws.amazon.com/es/rekognition/?blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc.

[5] Cortés Hernández, G. A. (26 de octubre de 2020). La altura correcta de la cámara. Recuperado el 28 de agosto de 2021 de https://www.ventasdeseguridad.com/20181026109 78/articulos/analisis-tecnologico/la-altura-correcta-de-la-camara.html

[6] CrucialTrack. (s.f.). Bacs Quattro. Recuperado el 15 de agosto de 2021 de http://www.crucialtrak.com/BACS/products/quattro.php.

[7] Deep Vision AI. (s.f). Recuperado el 11 de agosto de 2021 de https://www.deepvisionai.com.

[8] EFE. (6 de junio de 2020). La UE prepara una base de datos biométrica para controlar las fronteras Schengen. Expansión. Recuperado el 20 de agosto de 2021 de https://www.expansion.com/economia-digital/innovacion/2020/06/06/5edb6df6e5fdeade2a8b4578.html.

[9] Exadel Inc. (6 de julio de 2020). CompreFace. Recuperado el 6 de agosto de 2021 de https://github.com/exadel-inc/CompreFace.

[10] FaceFirst. (s.f.). Recuperado el 12 de agosto de 2021 de https://www.facefirst.com.

[11] Face^{++}. (s.f.). Recuperado el 13 de agosto de 2021 de https://www.faceplusplus.com.

[12] Facial recognition system. (s.f.). En *Wikipedia*. Recuperado el 3 de julio de 2021 de https://en.wikipedia.org/wiki/Facial_recognition_system.

[13] García Miguélez, A. (21 de julio de 2020). Infalible. Así será el Face ID de los futuros iPhone de Apple. La Manzana Mordida. Recuperado el 31 de agosto de 2021 de https://lamanzanamordida.net/noticias/one-more-thing/patente-face-id-julio-2020/.

[14] Geitgey, A. (3 de marzo de 2017). Face Recognition. Github. Recuperado el 5 de agosto de 2021 de https://github.com/ageitgey/face_recognition.

[15] Huawei. (18 de febrero de 2019). Requisitos de instalación para la cámara de reconocimiento facial. Recuperado el 28 de agosto de 2021 de https://forum.huawei.com/enterprise/es/requisitos-de-instalación-para-la-cámara-de-reconocimiento-facial/thread/499177-100259.

[16] IDEMIA. (s.f.). VisionPass. Recuperado el 15 de agosto de 2021 de https://www.idemia.com/wp-content/uploads/2021/02/visionpass-idemia-brochure-202103.pdf.

[17] InsightFace. (s.f.). Why InsightFace. Recuperado el 8 de agosto de 2021 de https://insightface.ai.

[18] Invixium. (s.f.). IXM TITAN. Recuperado el 16 de agosoto de 2021 de https://www.invixium.com/ixm-titan-face-recognition/.

[19] Iris ID. (s.f.). iT100. Recuperado el 27 de agosto de 2021 de https://www.irisid.com/productssolutions/hardwareproducts/it100/

[20] Las Condes. (s.f.). Guía para el buen uso de sistemas de cámaras de seguridad. Capítulo 1: Sistema de Reconocimiento Facial. Recuperado el 28 de agosto de 2021 de https://www.lascondes.cl/descargas/seguridad/manuales/camaras-seguridad.pdf.

[21] LIPS. (s.f.). LIPSFace AC770. Recuperado el 16 de agosto de 2021 de https://www.lips-hci.com/lipsface.

[22] Microsoft Azure. (s.f.). Face API. Recuperado el 13 de agosto de 2021 de https://azure.microsoft.com/en-us/services/cognitive-services/face/.

[23] Montes, S. (9 de abril de 2021). Sistemas de reconocimiento facial: así se extiende el uso de esta controvertida tecnología. Escudo Digital. Recuperado el 19 de agosto de 2021 de https://escudodigital.com/tecnologia/reconocimiento-facial-controvertida-imperfecta-tecnologia-extiende-mundo-solo-esta-prohibida-pais/.

[24] Morcillo Vizuete, F. (2020). Desarrollo de un sistema de reconocimiento facial utilizando Deep Learning con OpenCV. Universitat Politècnica de València. http://hdl.handle.net/10251/156694.

[25] NIST. (19 de diciembre de 2019). NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software. Recuperado el 21 de agosto de 2021 de https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software.

[26] OpenCV. (s.f.). About. Recuperado el 11 de agosto de 2021 de https://opencv.org/about/.

[27] Pérez, E. (11 de junio de 2021). El polémico reconocimiento facial de Mercadona no saldrá adelante: un juez impide su uso en un supermercado. Xataka. Recuperado el 20 de agosto de 2021 de https://www.xataka.com/privacidad/prohiben-a-mercadona-usar-su-reconocimiento-facial-justicia-obliga-a-detener-sistema-que-siempre-estuvo-fuera-lugar.

[28] Pospielov, S. (11 de marzo de 2021). What is the Best Facial Recognition Software to Use in 2021? Towards Data Science. Recuperado el 2 de agosto de 2021 de https://towardsdatascience.com/what-is-the-best-facial-recognition-software-to-use-in-2021-10f0fac51409.

[29] RFI. (7 de junio de 2021). En las calles de Belgrado, miles de cámaras suministradas por China observan a los serbios. Recuperado el 19 de agosto de 2021 de https://www.rfi.fr/es/europa/20210607-en-las-calles-de-belgrado-miles-de-cámaras-suministradas-por-china-observan-a-los-serbios.

[30] Rubio, I. (25 de mayo de 2019). Reconocimiento facial: la tecnología que lo sabe todo. EL PAÍS. Recuperado el 19 de agosto de 2021 de https://elpais.com/tecnologia/2019/05/21/actualidad/1558455279_966010.html.

[31] Sandberg, D. (12 de febrero de 2016). Facenet. Github. Recuperado el 7 de agosto de 2021 de https://github.com/davidsandberg/facenet.

[32] Sanz Fernández, J. (13 de diciembre de 2019). Las tecnologías de reconocimiento facial no son seguras, y eso es un problema. EL PAÍS. Recuperado el 21 de agosto de 2021 de https://cincodias.elpais.com/cincodias/2019/12/13/lifestyle/1576228886_849015.html.

[33] Schroff, F., Kalenichenko, D. y Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*. doi: 10.1109/cvpr.2015.7298682.

[34] Serengil, S. I. (8 de febrero de 2020). Deepface. Github. Recuperado el 7 de agosto de 2021 de https://github.com/serengil/deepface.

[35] Sirovich, L. y Kirby, M. (1987). Low-Dimensional Procedure for the Characterization of Human Faces. *Journal of the Optical Society of America. A, Optics and image science, 4*, 519-24. doi: 10.1364/JOSAA.4.000519.

[36] Shepley, A. J. (2019). Deep Learning For Face Recognition: A Critical Analysis.

[37] SthPhoenix. (15 de agosto de 2019). InsightFace-REST. Github. Recuperado el 8 de agosto de 2021 de https://github.com/SthPhoenix/InsightFace-REST.

[38] Surfshark. (s.f.). The Facial Recognition World Map. Recuperado el 18 de agosto de 2021 de https://surfshark.com/facial-recognition-map.

[39] Thakur, A. (16 de junio de 2019). All about Facial Recognition for Businesses. Geekflare. Recuperado el 14 de agosto de 2021 de https://geekflare.com/facial-recognition-for-business/.

[40] Tolba, A., El-Baz, A. y El-Harby, A. (2005). Face Recognition: A Literature Review. *International Journal of Signal Processing, 2*, 88-103.

[41] Turk, M. A. y Pentland, A. P. (1991). Eigenfaces for recognition. *Journal of Cognitive Neuroscience, 3*(1), 71-86.

[42] Wang, M. y Deng, W. (2018). Deep Face Recognition: A Survey.

APÉNDICE A
Cuestionario

Soy Francisco Morcillo Vizuete, estudiante de Doble Grado en Ingeniería Informática + ADE en la Universitat Politècnica de València que junto con el profesor Ignacio Gil Pechuán desarrollamos una investigación que me permitirá realizar mi Trabajo de Fin de Grado además de avanzar en el desarrollo de la aplicabilidad de la últimas técnicas biométricas, más concretamente de reconocimiento facial, en los entornos profesionales. Para ello necesitamos identificar la predisposición y viabilidad de las tecnologías en desarrollo, por lo que hemos elaborado el siguiente cuestionario, formado por tres preguntas abiertas y una de varias opciones, con el fin de extraer información útil de un grupo de 16 expertos, del cual usted forma parte. La información será tratada de manera confidencial y anónima. Sería importante para esta investigación que conteste todas las preguntas con la máxima amplitud que considere oportuna. La información que pueda brindar nos será de gran ayuda. Para cualquier consulta puede ponerse en contacto con nosotros a través del profesor Ignacio Gil (igil@doe.upv.es). Muchas gracias por su tiempo y amabilidad.

Francisco Morcillo.
Ignacio Gil.
Universitat Politècnica de València.

1. ¿Qué sistema utiliza para identificarse o autentificarse en los equipos informáticos de su lugar de trabajo? (*login* y *password*, DNI electrónico, certificado digital, criptografía biométrica, ninguno...)

2. ¿Cómo valoraría la utilización de un sistema de reconocimiento facial seguro para el acceso a su entorno de trabajo? ¿Podría detallarnos algunas razones?

3. ¿Qué beneficios y problemas identificaría en la aplicación de un sistema de identificación facial seguro en el entorno profesional en el que usted trabaja habitualmente?

4. ¿A qué rama de actividad económica pertenece su puesto de trabajo?