Universidad de Valladolid

Escuela de Ingeniería Informática

TRABAJO FIN DE GRADO

Grado en Ingeniería Informática
Mención en Tecnologías de la Información

Técnicas de autenticación biométrica en ciberseguridad: análisis y retos para la privacidad

Autor: Laura Bezanilla Matellán

Tutor: Valentín Cardeñoso Payo

A mis padres.

A mi hermana.

Gracias por ser siempre mi mayor apoyo.

El eslabón más débil de la cadena de seguridad es el factor humano.
Kevin Mitnick

Resumen

En un mundo digitalizado como el nuestro, la sociedad es cada vez más consciente de la relevancia que tiene la protección de nuestros datos personales. Desde esta perspectiva, la implementación de la biometría ha transformado la forma en la que nos autenticamos y, a su vez, ha generado grandes avances en términos de seguridad. Sin embargo, junto a ello, también han surgido numerosas amenazas asociadas a su uso.

En este Trabajo de Fin de Grado se presenta una investigación sobre el funcionamiento de las tecnologías biométricas, centrándose en dos de las técnicas más usadas en la actualidad, como son el reconocimiento de huellas digitales y el reconocimiento facial, analizando también su aplicabilidad en aquellos dispositivos cuyo sistema operativo es Android.

Así, el principal objetivo es evaluar las limitaciones de estos sistemas relacionadas con la privacidad de los individuos. Para ello, se ha llevado a cabo un análisis comparativo en términos de eficacia, seguridad y vulnerabilidades. Las conclusiones obtenidas indican que, aunque estas tecnologías proporcionan una solución útil, actualmente continúan existiendo desafíos en términos de seguridad, lo que subraya la necesidad de seguir un enfoque meticuloso tanto en su implementación, como en su regulación.

Palabras clave: *Biometría, reconocimiento de huellas digitales, reconocimiento facial, sistemas Android, privacidad, seguridad, vulnerabilidades, amenazas*

Abstract

In a digitalized world like ours, society is increasingly aware of the importance of protecting our personal data. From this perspective, the implementation of biometrics has transformed the way in which we authenticate ourselves and, in turn, has generated significant advances in terms of security. However, numerous threats associated with its use have also emerged.

This Final Degree Project presents an investigation on the functioning of biometric technologies, focusing on two of the most widely used techniques today such as fingerprint recognition and facial recognition. It also examines their applicability in those devices whose operating system is Android.

Thereby, the main objective is to evaluate the limitations of these systems related to the privacy of individuals. To archieve tihs, a comparative analysis has been conducted in terms of effectiveness, security and vulnerabilities. The findings indicate that, although these technologies provide a useful solution, there are still challenges in terms of security, emphasizing the need for a meticulous approach in both, their implementation and regulation.

Key words:*Biometrics, fingerprint recognition, facial recognition, Android systems, privacy, security, vulnerabilities, threats*

Índice general

Índice de tablas

Índice de figuras

Capítulo 1

Introducción

Este capítulo inicial pretende proporcionar al lector el contexto necesario para poder comprender la importancia de la biometría en el ámbito de la ciberseguridad actual, así como la motivación de por qué se ha elegido este tema para realizar el Trabajo de Fin de Grado.

1.1. Contexto

La seguridad informática, también conocida como ciberseguridad, se ha convertido en un pilar fundamental en la era digital, ya que protege tanto la integridad como la confidencialidad de la infraestructura de los sistemas e información crítica frente a las amenazas cibernéticas [45]. Ofreciendo no solo protección contra diferentes tipos de *malware* sino también contra posibles intrusiones y robo de datos personales, la ciberseguridad se presenta como la primera línea de defensa para toda empresa.

Según informes recientes, durante este último año, España ha sido uno de los países europeos más afectado por ciberataques, lo que ha dado lugar a unas pérdidas económicas de hasta 30.000 millones de euros al año [53]. Como consecuencia, en una sociedad que depende cada vez más de la tecnología, los ciberataques son uno de los principales riesgos para la estabilidad económica de cualquier país [50]. Por ello y con ánimo de minimizarlos, la ciberseguridad, que es considerada un sector clave para la economía mundial, generará más de 83.000 puestos de trabajo en España en el año 2024 [36].

Este tipo de ataques ponen de manifiesto las crecientes preocupaciones de los consumidores sobre las nuevas tecnologías emergentes [57]. Con el auge de la Inteligencia Artificial y su habilidad para crear cualquier tipo de contenido, el cual es muy difícil distinguir del que es generado por una persona, las amenazas digitales cada vez son más complejas de identificar, lo que está provocando una mayor inquietud y escepticismo entre los usuarios. Estos problemas han enfatizado la necesidad de las empresas de instaurar nuevas medidas de seguridad [1] [10].

Tradicionalmente, los sistemas de autenticación se basaban en la posesión de un objeto tangible como, por ejemplo, una tarjeta. Posteriormente, la verificación de la autenticidad de una persona se obtendría recurriendo a sus conocimientos, es decir, una contraseña secreta que, en teoría, solo esa persona debía conocer. No obstante, los avances tecnológicos han revelado la debilidad de estos métodos, obligando a los profesionales de esta competencia a buscar alternativas más robustas.

En este contexto, la biometría se presenta como una respuesta a este gran reto cuyo fin es fortalecer las defensas digitales en el ámbito de la ciberseguridad. Al utilizar diferentes características inherentemente personales, la biometría ofrece un método de autenticación avanzado que va un paso más allá en comparación con las contraseñas convencionales y los riesgos que presenta su uso, pues se ha demostrado que estas pueden verse fácilmente comprometidas. Por consiguiente, la incorporación de la biometría en cualquier sistema presenta numerosas ventajas significativas. Sin embargo, al mismo tiempo se han expuesto nuevas amenazas.

Actualmente, nuestra sociedad está haciendo frente a una situación en la que la usurpación de la identidad de una persona se puede producir de forma precisa. Esta amenaza no es solo teórica, puesto que la venta de datos biométricos en el mercado negro es ya una realidad [76].

El caso de Clearview AI sitúa la ética y la legalidad del uso de los datos biométricos como centro de debate. Esta compañía compartió con las fuerzas policiales americanas 30.000 millones de imágenes obtenidas de diversas redes sociales sin la autorización de los usuarios [27]. Esta noticia recalca la facilidad con la que se puede recopilar y hacer un uso indebido de los datos biométricos sin el consentimiento de las personas, lo que demuestra la necesidad de establecer un conjunto de regulaciones más precisas.

Por otro lado, los acontecimientos desarrollados a lo largo de este año vinculados con la empresa WorldCoin han ocasionado una gran controversia entre los usuarios que formaron parte del proyecto. A través de este se les ofreció una cantidad de dinero en forma de criptomonedas a cambio de que se les realizara un escaneo de su iris [62]. Esta polémica no solo demuestra la sensibilidad que tienen los datos biométricos, sino también el debate moral sobre el intercambio de información personal a cambio de una compensación económica [51].

Debido a los riesgos que conlleva el uso de la biometría, las diferentes Administraciones Públicas se han visto forzadas a regular su aplicación. En España, la legislación sobre la utilización de los datos biométricos está recogida bajo el Reglamento General de Protección de Datos, donde se establecen unas normas precisas para la protección de este tipo de información [11] que intensifican el cumplimiento del deber de las empresas sobre el tratamiento de este tipo de datos.

Por otra parte, conforme a la normativa publicada por el RGPD cualquier recogida y procesamiento de datos biométricos precisa la conformidad explícita de las personas [43]. Adicionalmente, la Agencia Española de Protección de Datos sancionará a aquellas organizaciones que impongan el uso de la biometría como control de acceso sin proporcionar otras posibilidades [26]. Son casos como los mencionados anteriormente los que han resaltado la importancia de mantener el equilibrio entre los avances tecnológicos y la protección de los derechos humanos.

1.2. Motivación

En un mundo cada vez más conectado como el nuestro, la sociedad es más consciente de la importancia que tiene la seguridad de la información de carácter personal. Desde este punto de vista, la aplicación de la biometría ha cambiado la manera en la que se autentican las personas y, asimismo, ha ocasionado progresos significativos en términos de seguridad.

Por lo tanto, la biometría se formula como una alternativa adecuada para potenciar la seguridad en una gran variedad de situaciones. Sin embargo, es esencial tener en cuenta que, junto con los últimos avances en tecnología, la seguridad de algunos métodos de identificación biométrica, que son ampliamente usados por diferentes usuarios, ha sido puesta en duda de forma significativa. Por consiguiente, es en este contexto cuando se plantean interrogantes sobre la fiabilidad de estos mecanismos de autenticación.

En este sentido, la búsqueda constante de nuevas soluciones para mejorar la confianza de las personas hacia la privacidad en el uso de esta tecnología se ha convertido en un propósito fundamental en el diseño de las técnicas de reconocimiento biométrico. Esto presenta un constante desafío para los profesionales del sector de la ciberseguridad debido a la complejidad de los elementos que influyen en la privacidad de este tipo de datos. Además, estas soluciones deberán poder adaptarse al dinamismo que caracteriza al mundo tecnológico. Dado el impacto que tienen en la sociedad, es relevante analizar estos riesgos y la manera de mitigarlos, puesto que el uso de la biometría es el presente, no el futuro.

¿Hasta qué punto son seguros estos métodos de autenticación? ¿Por qué se debe confiar en ellos? ¿Los sistemas biométricos son realmente la mejor solución que se necesita? Este tipo de preguntas son algunas de las que me he planteado a la hora de elegir el tema para mi Trabajo de Fin de Grado. Por este motivo, este documento se centrará en una investigación sobre el funcionamiento de los métodos biométricos más utilizados, como son el reconocimiento de las huellas dactilares y el reconocimiento facial en su estado actual, teniendo en cuenta de las necesidades de los usuarios. Además, se investigará cuáles son los retos más importantes que hacen frente este tipo de tecnologías. En otras palabras, la comprensión de estos desafíos permitirá evaluar la eficacia de los sistemas biométricos vigentes.

1.3. Objetivos

El principal objetivo de este proyecto es explorar la realidad de los sistemas de reconocimiento biométrico modernos para encontrar una respuesta a la pregunta: ¿Hasta qué punto las tecnologías de autenticación biométrica proporcionan la capacidad de identificar a una persona de manera única y segura? Además, se profundizará en los retos a los que se enfrentan este tipo de sistemas. Para ello, es necesario establecer una serie de objetivos teóricos específicos. Cabe destacar que estos objetivos no solo definirán los hitos que deberán lograrse durante el transcurso de esta investigación, sino que también garantizarán un planteamiento sistemático.

Se va a profundizar en la operatividad de las técnicas biométricas más populares actualmente. Es decir, se investigará la forma en la que funcionan estas tecnologías en diversas aplicaciones. Además, se estudiará la implicación que ha supuesto su uso en términos de precisión y seguridad. Por ello, es necesario cumplir con los siguientes objetivos:

- Definir la naturaleza de los datos biométricos utilizados en los sistemas de reconocimiento para comprender las propiedades de este tipo de información abarcando aspectos como su impacto en el rendimiento de un sistema de reconocimiento biométrico moderno.

- Analizar el desarrollo tecnológico en la captura y procesamiento de datos biométricos. Se examinarán los progresos en el mecanismo de los dispositivos evaluando cómo estas mejoras han impactado en la exactitud y la fiabilidad del sistema.

- Estudiar las fortalezas y debilidades de las técnicas de comparación de muestras biométricas. Se llevará a cabo un análisis comparativo de diferentes métodos de identificación biométrica, enfatizando sus beneficios, limitaciones y utilidad en diferentes contextos.

- Analizar la incorporación de técnicas biométricas en dispositivos Android, evaluando la utilización de la API BiometricPrompt para la integración de estos métodos de autenticación, considerando aspectos como su simplicidad de uso además de su seguridad.

- Identificar las amenazas de la biometría como método de autenticación. Se investigarán los riesgos asociados con el uso de estos métodos de identificación evaluando la efectividad de las medidas de seguridad actuales.

Finalmente, se ha determinado un conjunto de objetivos personales que contribuirán al desarrollo individual debido a que se considera que representan diferentes aspiraciones en áreas que se quiere mejorar el conocimiento:

- Poner en práctica los conocimientos adquiridos en la carrera incorporándolos en un proyecto teórico que aborda problemas que existen en el ámbito de la ciberseguridad de la sociedad actual.

- Explorar áreas complejas de la seguridad y privacidad de datos, además de obtener experiencia en la gestión de proyectos de investigación que requieren una planificación e implementación rigurosa.

- Fomentar la capacidad de transmitir las conclusiones técnicas obtenidas en la investigación de forma clara, tanto en la defensa oral, como en la memoria escrita.

1.4. Estructura de la memoria

En esta sección se presenta la organización del contenido de la memoria en una serie de capítulos teniendo en cuenta la metodología de la guía docente de la asignatura Trabajo de Fin de Grado adaptándola a este proyecto:

Capítulo 1: Introducción. Ofrece una contextualización del tema del proyecto en relación con la ciberseguridad. Además, se describe la motivación para llevarlo a cabo, así como los objetivos que se buscan lograr junto con la estructura del mismo.

Capítulo 2: Planificación del proyecto. Se detallará la planificación del proyecto teniendo en cuenta las diferentes fases existentes en la investigación, describiendo la metodología ágil utilizada y el plan para la gestión de riesgos.

Capítulo 3: Marco teórico. Se llevará a cabo una explicación detallada de los conceptos teóricos claves para una correcta comprensión del proyecto por parte del lector. Además, se realizará una investigación de los tipos de sistemas biométricos que se usan actualmente en el área de la ciberseguridad, detallando las diferentes aplicaciones y estándares empleados.

Capítulo 4: Reconocimiento de huellas digitales. Se presentan los conceptos clave para entender el funcionamiento de la biometría asociada a la huella dactilar. Se describirá con detalle el proceso completo del reconocimiento biométrico desde la captura de la huella hasta la comparación de las muestras. Por último, se analizará la seguridad de estos sistemas ofreciendo contramedidas efectivas.

Capítulo 5: Reconocimiento facial. Se abordará de forma minuciosa el funcionamiento completo del reconocimiento facial. Asimismo, se describirán tanto las técnicas como los algoritmos utilizados en cada fase del proceso. Para concluir, se realizará una evaluación de la seguridad de este tipo de sistemas.

Capítulo 6: Tecnologías biométricas aplicadas a dispositivos Android. Se examinará cómo en la actualidad la autenticación biométrica se integra en dispositivos Android, haciendo énfasis en el uso de la API BiometricPrompt. Se explicará en profundidad de qué forma esta API facilita el uso de estas técnicas de reconocimiento mejorando la seguridad.

Capítulo 7: El reto de la privacidad en la biometría. Se evaluarán las distintas amenazas que podrían poner en riesgo la privacidad de los usuarios que utilizan estos sistemas. Adicionalmente, se determinará el marco legal vinculado al empleo de este tipo de sistemas incluyendo a su vez una perspectiva ética que subrayará la relevancia de salvaguardar la privacidad de los datos sensibles.

Capítulo 8: Conclusiones. Se presentan las conclusiones obtenidas en el estudio, así como las futuras líneas de investigación.

Capítulo 2

Planificación del proyecto

Este capítulo detalla la metodología que se va a utilizar para realizar esta investigación. Adicionalmente, se presenta la planificación del proyecto identificando los potenciales riesgos que están asociados a su ejecución.

2.1. Metodología ágil

En la planificación de este proyecto se ha decidido que la metodología ágil que mejor se ajusta al desarrollo de este tipo de investigaciones es el marco de referencia Kanban. El término japonés *Kanban* hace referencia a un tablero visual. Este marco de trabajo se trata de un método visual de gestión de proyectos que está basado en el concepto *pull* [30]. Cuando se empieza un proyecto, los miembros del equipo deben elaborar una lista de tareas pendientes. A continuación, los integrantes deberán ir extrayendo actividades de esa lista para moverlas al apartado de trabajo.

Esta metodología se implementa a través de tableros Kanban dispuestos en diferentes columnas, donde cada una de ellas representa una etapa del proyecto. En este caso, las columnas que se utilizarán son *To do, In progress* y *Done*. Por otro lado, las tareas se representan a través de tarjetas visuales que van recorriendo las tres columnas hasta que su ejecución finalice [31].

En este contexto, la elección de esta metodología se debe principalmente por la posibilidad que ofrece para poder optimizar el flujo de trabajo [63], así como su flexibilidad, permitiendo adaptarse a cualquier cambio que surja en el proyecto. Otra de sus ventajas es la colaboración continua con el tutor del TFG al tener la oportunidad de consultar el flujo de trabajo en su totalidad. Gracias a este método es posible gestionar de forma eficaz y adaptativa las diferentes tareas que sean necesarias en el proyecto. Además, con el uso de la metodología Kanban se puede obtener información en tiempo real sobre la productividad de cada integrante que forma parte del equipo, proporcionando una visión clara del estado del TFG en todo momento.

2.1.1. Principios del desarrollo Kanban

La metodología Kanban fue aplicada por primera vez en el desarrollo software por el autor David J. Anderson. Su objetivo era mejorar el flujo de trabajo, aumentando al mismo tiempo la productividad y la calidad obtenida en el producto final.

Anderson afirma que para poder lograr este propósito en el desarrollo de cualquier proyecto es necesario seguir estos cuatro principios [63]:

- **Empezar con lo que estás haciendo en este momento:** No se debe efectuar ningún cambio en el proceso existente de forma inmediata. Los cambios que sean necesarios se realizarán de forma gradual a un ritmo adecuado a cada caso específico.
- **Conseguir una mejora continua a través del cambio evolutivo:** Es necesario realizar pequeñas variaciones incrementales en vez de modificaciones drásticas que podrían provocar dificultades en el entorno de trabajo del equipo.
- **Promover los actos de liderazgo:** Es imprescindible que exista un ambiente de confianza para que cualquier persona perteneciente al equipo se sienta cómoda para aportar ideas nuevas basadas en una explicación lógica.
- **Respetar las responsabilidades individuales:** Los integrantes del equipo deberán respetar tanto los roles como las responsabilidades de sus compañeros para eliminar el miedo al cambio.

Por otro lado, en esta metodología existen tres prácticas fundamentales que se deberían aplicar en cualquier proceso Kanban con el fin de optimizar el resultado del proyecto [63]:

- **Visualizar el flujo de trabajo:** Hay que intentar hacer visible lo invisible. La representación visual del trabajo ayuda a determinar el estado actual de las tareas para poder identificar posibles problemas.
- **Limitar el WIP - *Work in Progress*:** Reduciendo el trabajo que está activo, se anima a las personas a terminar primero la actividad que están haciendo antes de empezar una nueva. De esta forma, si se restringe el número de tareas activas se podrá controlar mejor los recursos que están disponibles, evitando así la ociosidad de los miembros del equipo.
- **Mejora continua del ciclo de vida:** Facilita aplicar pequeños cambios a un ritmo mediante el cual el equipo pueda adaptarse fácilmente.

En conclusión, estos principios junto con las buenas prácticas están pensadas para poder adaptarse de forma correcta al funcionamiento de esta metodología ágil y aprovechar así todos sus beneficios.

2.2. Adaptación Kanban al proyecto

En este proyecto se considera importante utilizar la metodología Kanban debido a que favorece tener una visión clara de las diferentes tareas existentes en cada estado que forma parte del desarrollo del proyecto. Además, se elige este marco de trabajo debido a su flexibilidad para que los miembros del equipo se adapten a los cambios que puedan ir surgiendo en el desarrollo del proyecto de forma fácil.

Adicionalmente, la importancia de implementar este tipo de metodología se debe a que existe un conocimiento previo sobre ella, ya que la empresa donde se está trabajando la usa en su día a día. De esta forma, se garantiza una buena aplicación práctica lo que aumentará la capacidad de gestionar correctamente el proyecto obteniendo al final un resultado exitoso.

Es importante señalar que en la adaptación de este marco de trabajo que se va a llevar a cabo en este Trabajo de Fin de Grado, se va a realizar un seguimiento periódico por parte del tutor, lo que permitirá obtener al estudiante una retroalimentación continua de los avances en el proyecto.

Por otro lado, para el desarrollo de este proyecto se utilizará la aplicación gratuita Trello para poder optimizar la gestión del proyecto en base a la metodología Kanban. Se ha elegido esta opción no solo por su sencilla interfaz, sino también por la posibilidad que ofrece de mantener una supervisión de las actividades tanto desde el ordenador como desde un dispositivo móvil. Adicionalmente, es posible compartir el tablero dedicado al proyecto con el tutor para que ambos puedan tener acceso a él.

A continuación, se muestra una imagen del tablero junto con los diferentes estados por los que irán pasando las tareas que se usará durante el desarrollo de este proyecto.

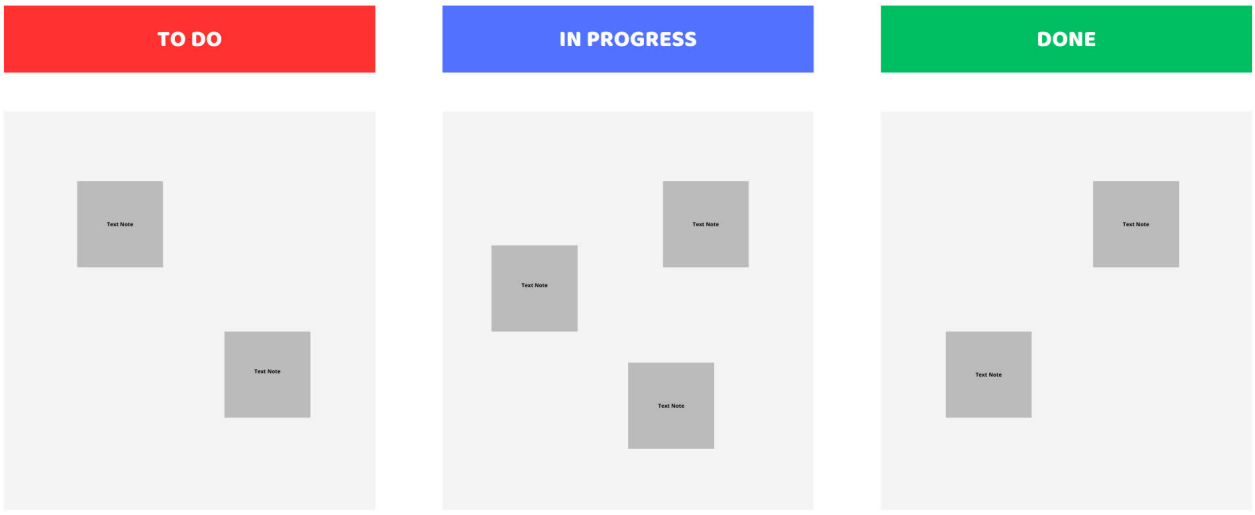

Figura 2.1: Tablero Kanban que se usará en el TFG

2.3. Planificación

Para asegurar el éxito de este proyecto se ha diseñado una planificación inicial dividiendo la investigación en siete fases diferentes, cada una de las cuales se enfocará en un periodo de la investigación concreto. Cada una de estas fases se realizará de forma secuencial siguiendo un enfoque en cascada. Por consiguiente, este modelo garantizará un desarrollo ordenado del estudio, ya que es fundamental que una etapa se finalice antes de poder pasar a la siguiente. Además, este plan está adaptado a lo establecido en la guía docente [73] del Trabajo de Fin de Grado de la Escuela de Ingeniería Informática de la Universidad de Valladolid, donde se establece que esta asignatura está formada por 12 créditos ECTS, lo que se corresponde aproximadamente a 300 horas de trabajo por parte del alumno.

2.3.1. Fases

A continuación, en la tabla 2.1 se proporciona una estructura que refleja el esfuerzo requerido para la correcta realización de este proyecto favoreciendo una gestión apropiada del tiempo y los recursos necesarios para el correcto desarrollo del mismo.

Tabla 2.1: Planificación inicial del proyecto

Fases del proyecto	Fecha inicio	Fecha fin	Días totales
Fase cero			
Puesta en marcha	01/03/2024	31/03/2024	30
Fase uno			
Introducción	01/04/2024	08/04/2024	7
Planificación	09/04/2024	05/05/2024	26
Marco teórico	06/05/2024	30/06/2024	55
Fase dos			
Reconocimiento de huellas digitales	01/07/2024	18/08/2024	48
Fase tres			
Reconocimiento facial	19/08/2024	16/11/2024	58
Fase cuatro			
El reto de la privacidad en la biometría	17/11/2024	03/12/2024	16
Fase cinco			
Tecnologías biométricas aplicadas a dispositivos Android	04/12/2024	13/12/2024	9
Fase seis			
Conclusiones	14/12/2024	15/12/2024	1

2.4. Gestión de riesgos

La complejidad de las tecnologías biométricas junto con los desafíos propios de la ciberseguridad hacen que la correcta gestión de los riesgos sea una parte esencial para conseguir un resultado favorable en el proyecto. También, de esta forma se garantiza con altas probabilidades la finalización del TFG dentro de los plazos establecidos reduciendo el impacto de las posibles interrupciones que puedan ir surgiendo.

Por todo ello, después de realizar la planificación inicial de la investigación, es necesario identificar, analizar y mitigar cualquier tipo de riesgo potencial que pueda ocurrir durante el transcurso del trabajo.

Según el Instituto de Gestión de Proyectos, se considera que un riesgo es la probabilidad de que un evento específico, en caso de que ocurra, tenga un efecto negativo en uno o varios objetivos del proyecto [71]. Al analizar los posibles riesgos existentes es determinante tener en consideración su posibilidad de ocurrencia, así como su posible impacto en el desarrollo del proyecto. Por ese motivo, con el fin de minimizar las consecuencias negativas de estos es esencial que este proyecto disponga de un plan estratégico de gestión de riesgos para minimizar su repercusión en la planificación del mismo.

En consecuencia, para el plan de gestión de riesgos que se ha diseñado se ha considerado imprescindible incluir los siguientes cuatro factores [9]:

- **Probabilidad:** Indica la posibilidad de que el riesgo ocurra categorizando los diferentes valores en bajo, medio y alto.

- **Impacto:** Denota la magnitud del alcance que tendría un riesgo si se llega a concretar y se pondera como bajo, medio o alto.

- **Plan de mitigación:** Refleja los procedimientos que se deberán llevar a cabo para reducir la probabilidad de que se produzcan esos riesgos.

- **Plan de contingencia:** Expone las acciones cuya aplicación es necesaria tan pronto como el riesgo se produzca con el objetivo de disminuir su efecto.

En conclusión, es importante enfatizar que la incorporación proactiva de un plan para la gestión de los riesgos favorece el cumplimiento de los objetivos del proyecto, además de aumentar la capacidad del alumno para afrontar las dificultades que puedan surgir en un futuro. De esta forma, se podrá realizar de forma continúa las actividades planificadas, incrementando la posibilidad de finalizar el proyecto dentro del plazo decretado.

Riesgo 01			
Título	Falta de disposición por parte del alumno		
Descripción	En vista de la extensión del proyecto, la disposición del alumno puede verse alterada, lo que puede exigir modificaciones en la planificación de la investigación.		
Probabilidad	Media	**Impacto**	Alto
Plan de mitigación	Compaginar de forma equilibrada el trabajo con el desarrollo del proyecto.		
Plan de contingencia	Planificar las tareas con un margen de tiempo adecuado respecto al tiempo ideal de duración, además de evaluar la opción de solicitar días libres en el trabajo.		

Tabla 2.2: Riesgo 01 - Falta de disposición por parte del alumno

Riesgo 02			
Título	Fallos hardware o software en el equipo de trabajo		
Descripción	Con este tipo de fallos técnicos podría ser necesario tener que reparar el equipo, lo que provocaría interrupciones importantes en el desarrollo del proyecto.		
Probabilidad	Media	**Impacto**	Medio
Plan de mitigación	Realizar el proyecto utilizando una plataforma online como Overleaf. Adicionalmente, realizar copias de seguridad del documento de la memoria regularmente.		
Plan de contingencia	Reparar, o en su defecto, reemplazar los componentes dañados. Durante ese tiempo utilizar otro equipo que esté disponible.		

Tabla 2.3: Riesgo 02 - Fallos hardware o software en el equipo de trabajo

Riesgo 03			
Título	Retraso en las comunicaciones con el tutor		
Descripción	Dado que gran parte del TFG se desarrollará en verano, podrían existir problemas para recibir retroalimentación del tutor, lo que influiría en la planificación del proyecto.		
Probabilidad	Alta	**Impacto**	Alto
Plan de mitigación	Usar diferentes medios de comunicación como Teams o correo electrónico para estar en contacto con el tutor y resolver las posibles dudas.		
Plan de contingencia	Dado el caso de que haya dificultades en el contacto con el tutor, se planificará las tareas para poder ir avanzando en otras áreas del proyecto que no requieran su ayuda.		

Tabla 2.4: Riesgo 03 - Retraso en las comunicaciones con el tutor

Riesgo 04			
Título	Enfermedad del alumno		
Descripción	El alumno que realiza el TFG puede no estar disponible en un plazo indefinido de tiempo debido a una causa médica, ocasionando un retraso en los plazos estimados.		
Probabilidad	Baja	**Impacto**	Alto
Plan de mitigación	Diseñar un cronograma flexible incluyendo márgenes de tiempo para eventos inesperados que puedan suceder.		
Plan de contingencia	En caso de que el alumno enferme, se le comunicará la situación al tutor lo antes posible para analizar los plazos de entrega para priorizar las tareas más importantes.		

Tabla 2.5: Riesgo 04 - Enfermedad del alumno

Riesgo 05			
Título	Estimación errónea en la duración de cada tarea		
Descripción	Si se realiza una planificación errónea en la estimación del tiempo necesario en alguna de las tareas podría afectar a la fecha de finalización inicial del TFG.		
Probabilidad	Media	**Impacto**	Alto
Plan de mitigación	Llevar a cabo una división del proyecto en tareas más pequeñas y detalladas, para poder evaluar cuidadosamente la duración de cada una de ellas.		
Plan de contingencia	Priorizar las actividades más importantes para el éxito del proyecto. Además, si es necesario se dedicará más tiempo del necesario para finalizar el TFG en el plazo establecido.		

Tabla 2.6: Riesgo 05 - Estimación errónea en la duración de cada tarea

Riesgo 06			
Título	Modificación de los objetivos del proyecto		
Descripción	Durante el desarrollo del TFG pueden aparecer cambios inesperados en los objetivos del proyecto provocando un desvío en el enfoque del trabajo afectando al plan inicial.		
Probabilidad	Media	**Impacto**	Alto
Plan de mitigación	Mantener una comunicación clara con el tutor para garantizar que los objetivos iniciales están bien definidos. Además, analizar los cambios antes de implementarlos.		
Plan de contingencia	Si en algún momento los objetivos sufren algún cambio se actualizará la planificación reasignando recursos según sea necesario para cumplir con la fecha límite de entrega.		

Tabla 2.7: Riesgo 06 - Modificación de los objetivos del proyecto

Riesgo 07			
Título	Dificultades con la metodología elegida		
Descripción	Una vez se haya escogido la metodología que se va a usar, pueden existir dificultades en su implementación lo cual podría tener un impacto en el éxito final del proyecto.		
Probabilidad	Baja	**Impacto**	Alto
Plan de mitigación	Analizar minuciosamente las referencias bibliográficas existentes para elegir la metodología más apropiada para este tipo de estudio, además de consultarlo con expertos.		
Plan de contingencia	Se deberá tener preparada una metodología alternativa para poder implementarla si la primera opción no resulta ser productiva.		

Tabla 2.8: Riesgo 07 - Dificultades con la metodología elegida

Riesgo 08			
Título	No tener acceso a bibliografía especializada		
Descripción	En algún momento durante el desarrollo del TFG pueden existir dificultades para acceder a libros o artículos que estén especializados en el tema del proyecto.		
Probabilidad	Media	**Impacto**	Alto
Plan de mitigación	Antes de iniciar el proyecto, llevar a cabo una búsqueda exhaustiva de este tipo de bibliografía para asegurar que se podrá tener acceso a los recursos necesarios.		
Plan de contingencia	En el supuesto de no encontrar las referencias necesarias, se consultará con el tutor o con otros profesores que estén especializados para poder disponer de fuentes alternativas.		

Tabla 2.9: Riesgo 08 - No tener acceso a bibliografía especializada

Capítulo 3

Marco teórico

En este capítulo se facilitará al lector una primera aproximación a los conceptos básicos que integran la biometría. De esta manera, se analizarán aspectos como sus propiedades, tipos, funcionamiento y aplicaciones, entre otros, todo ello desde un punto de vista panorámico. Finalmente, se proporcionará una descripción de los estándares biométricos esenciales, así como las principales organizaciones de estandarización que se responsabilizan de la regulación del uso de esta tecnología.

3.1. Definición de la biometría

La biometría ha sido definida como la tecnología necesaria que analiza un conjunto de métodos y técnicas para la identificación de personas de forma inequívoca utilizando tanto las características biológicas y morfológicas, como los diferentes aspectos del comportamiento propios de cada individuo [21].

Por otra parte, según el *National Institute of Standards and Technology*, la biometría se relaciona específicamente con la medición y el análisis estadístico de las características de los datos biológicos [69]. Más concretamente, en el ámbito de las tecnologías de la información se utiliza para autenticar y verificar diversas características del cuerpo humano.

Este método de reconocimiento está diseñado para imitar el complejo proceso que realiza el ser humano al identificar a familiares o amigos en función de sus características personales como su apariencia o voz [35]. Del mismo modo que el cerebro puede reconocer inmediatamente una cara familiar entre una multitud, los métodos de reconocimiento biométrico utilizan algoritmos sofisticados para poder analizar y comparar entre identidades que perteneces a diferentes individuos.

3.2. Tipos de biometría para el control de acceso

En el estudio de los diferentes tipos de biometría que existen en la actualidad, estos se pueden dividir en dos grandes grupos. En otras palabras, estas dos categorías comprenden las diversas formas de analizar las características humanas para autenticar la identidad de una persona.

Biometría estática: Características físicas

La biometría estática se enfoca en el análisis de las características fisiológicas propias de un ser humano que se caracterizan por el hecho de que no se modifican con el paso del tiempo. Este tipo de rasgos distintivos se pueden capturar de forma precisa y reproducible [15][16][37]. Cabe destacar que esta investigación se centrará en el estudio de los siguientes tipos:

- **Huella dactilar:** Se trata del método de identificación más antiguo que se ha registrado [37]. Las huellas dactilares de una persona poseen pequeños surcos, llamados minucias, formados por líneas que constituyen patrones únicos en cada persona [37]. Estos patrones son la base del reconocimiento dactilar.

- **Características faciales:** Estos métodos tienen como objetivo identificar a las personas analizando sus rasgos faciales únicos. Utilizan algoritmos complejos que permiten analizar y comparar aspectos como la estructura o la forma del rostro, así como sus proporciones como, por ejemplo, la distancia entre los ojos [37].

Biometría dinámica: Características de comportamiento

La biometría dinámica, por otra parte, consiste en el estudio de las propiedades de la forma de comportarse de cada individuo. A diferencia de las anteriores, estas características pueden sufrir ligeras variaciones a lo largo del tiempo [15][16][37]. A pesar de ello, se considera que son lo suficientemente diferenciales para que se puedan usar con fines de autenticación. A continuación, se presentan algunos ejemplos de este tipo:

- **Firma manuscrita online:** Se trata de una técnica que constata la identidad de una persona mediante su firma digital. Esta hace uso de dispositivos como pantallas táctiles para captar no solo la forma de la firma, sino también elementos como la presión ejercida sobre la pantalla o la velocidad de escritura [37].

- **Voz:** Estos sistemas utilizan redes neuronales que se entrenan para que sean capaces de aprender a reconocer voces. Esto se lleva a cabo a través de sofisticados algoritmos que evalúan la similitud entre las muestras. El reconocimiento es más complejo debido al ruido ambiental. Pese a ello, estos sistemas tienen una ventaja, ya que solo es necesario un micrófono de calidad por lo que el coste del dispositivo no es muy elevado [37].

3.3. Propiedades que deben tener los rasgos biométricos

Cualquier característica que se quiera utilizar en los métodos de reconocimiento biométrico debe de tener una serie de propiedades que permitan garantizar la eficacia y la seguridad de cualquier sistema de autenticación que haga uso de este tipo de tecnología. Pero, ¿qué aspectos debe cumplir un rasgo de este tipo para que se considere distintivo? Según la guía publicada por el INCIBE, cualquier rasgo biométrico, ya sea físico o de conducta, puede ser utilizado como característica biométrica solo si cumple con las siguientes propiedades [37]:

1. **Universalidad**

   Todas las personas tienen que presentar esa misma característica. Esta condición garantiza que el sistema de autenticación pueda ser utilizado por cualquier individuo sin exclusiones.

2. **Singularidad**

   El rasgo biométrico debe ser único para cada individuo, permitiendo de este modo una distinción clara entre diferentes sujetos.

3. **Permanencia en el tiempo**

   La característica biométrica debe ser lo suficientemente invariable en el tiempo y en diversas condiciones ambientales para poder garantizar que se obtiene una identificación consistente. Esto indica que este tipo de atributos no van a verse modificados en el transcurso de la vida de una persona.

4. **Cuantificación**

   La característica utilizada por el sistema de autenticación se tiene que poder medir de forma cuantitativa, garantizando que se puedan capturar de manera efectiva y repetible en una gran variedad de condiciones y escenarios.

Por otro lado, se debe agregar que desde el punto de vista funcional de los sistemas de reconocimiento biométrico existe otro conjunto de criterios que se deberán satisfacer para que estos sean eficientes. En primer lugar, es necesario que generen un alto rendimiento y, al mismo tiempo, garanticen un nivel de precisión óptimo que minimice los posibles errores que puedan surgir durante el proceso del reconocimiento. Asimismo, es esencial que los usuarios adopten este tipo de tecnologías en su día a día para poder mejorar su experiencia de uso. Finalmente, este tipo de tecnologías deberán ser lo más seguras posible y altamente resistentes al robo de identidad [37].

3.4. Tipos de sistemas biométricos

En función del uso que se quiera hacer de la biometría, se pueden distinguir principalmente dos tipos de sistemas: los sistemas de identificación y los sistemas de autenticación. Cabe destacar que ambos tipos de sistemas desempeñan un papel esencial en la ciberseguridad actual, a pesar de que difieren en su enfoque de aplicación.

Sistemas de Identificación

Los sistemas de identificación biométrica tienen como principal objetivo determinar la identidad de una persona sobre la base de un conjunto de datos biométricos. El procedimiento que siguen este tipo de sistemas consiste en comparar la muestra de los rasgos biométricos de un usuario con los múltiples registros almacenados previamente de forma segura en una base de datos. En este caso, no es necesario obtener una identificación previa del usuario en cuestión. Con esto se quiere decir que la única información que se recoge durante el proceso es una muestra biométrica, sin requerir un nombre de usuario ni ningún otro tipo de datos [37].

Por ello, se considera que este es un proceso de uno a muchos donde el sistema debe ser capaz de identificar de forma única a un individuo entre una multitud. Es decir, este tipo de sistemas deberán responder con precisión a la pregunta: *¿Quién eres?*

Sistemas de Verificación

En contraste, es preciso que los sistemas de verificación tengan la capacidad necesaria para demostrar que un usuario específico en el sistema es realmente quien dice ser. En dicho sistema, el usuario deberá introducir una prueba de identidad como puede ser el nombre de usuario y su contraseña, además del rasgo biométrico. Posteriormente, el sistema será el responsable de procesar estos datos y compararlos con la muestra que está almacenada para ese identificador concreto [37].

A diferencia de los anteriores, la verificación es un proceso uno a uno debido a que únicamente se deberán comparar dos muestras. Se obtendrá un resultado positivo si el usuario es auténtico y, por el contrario, se obtendría un resultado negativo en el caso de que el usuario se trate de un impostor. En este caso, estos sistemas son los encargados de responder a la pregunta: *¿Eres tú quién dice ser?*

3.5. Funcionamiento de los sistemas biométricos

A pesar de las singularidades que se presentan en cada caso dependiendo de la modalidad biométrica que se utilice, todos estos sistemas tienen un funcionamiento básico común.

En este punto, conviene subrayar que este proceso se detallará más adelante. Sin embargo, la operatividad de cualquier sistema de autenticación comienza con un primer proceso fundamental: la captura de los datos. En esta etapa, la información biométrica de la persona es recopilada mediante el uso de una tecnología adecuada a cada modelo biométrico, garantizando un nivel alto de precisión. Una vez que finaliza esta fase, los datos son procesados exhaustivamente por el sistema para, posteriormente, almacenarlos de forma segura, creando de este modo un perfil único para cada individuo. Por último, cada autenticación se compara con los registros previamente almacenados, obteniendo como resultado una identificación rápida y rigurosa [37].

3.6. Aplicaciones de la biometría en la ciberseguridad

La seguridad biométrica se define como la aplicación de la biometría para proteger y salvaguardar instalaciones, dispositivos o datos sensibles [74]. Por lo tanto, tomando en consideración lo mencionado, en la última década la biometría ha experimentado un notable desarrollo y su aplicación engloba múltiples aspectos tanto de la vida diaria como profesional de las personas, independientemente de si se utiliza como única forma de autenticación o se combina con otros métodos.

En primer lugar, en el ámbito gubernamental esta tecnología es ampliamente utilizada, ya que permite poder identificar a delincuentes. Asimismo, cabe destacar su importancia a la hora de monitorizar a las personas en eventos sociales.

Por otro lado, en el marco laboral la aplicación de los métodos biométricos destacan especialmente en la supervisión del acceso físico ya sea a edificios o a áreas restringidas. Su utilización también es relevante en el control de acceso lógico a sistemas o información confidencial, ya sea reemplazando o complementando a las técnicas tradicionales como contraseñas y tarjetas de acceso.

Por lo que se refiere al mundo del comercio, la biometría se usa para autentificar transacciones online brindando una mayor seguridad frente a las falsificaciones, al mismo tiempo que se mejora la experiencia del cliente al eliminar la necesidad de memorizar claves o llevar consigo tarjetas físicas.

Debido a la creciente digitalización, en el área de las finanzas cada vez es más popular hacer uso de la biometría con el objetivo de prevenir el fraude o la suplantación de identidad, considerándose un método mucho más adecuado que los convencionales. El ejemplo de aplicación que más se utiliza es el desbloqueo de dispositivos móviles a través del reconocimiento facial, lo que remarca la integración de este tipo de tecnologías en la vida cotidiana de las personas.

Para finalizar, la identificación biométrica mediante el reconocimiento facial que se lleva a cabo en los aeropuertos agiliza el flujo de pasajeros, pues facilita el control de acceso [17]. De la misma manera, el empleo de datos biométricos en los puntos de control refuerza la seguridad y defensa internacional al colaborar en la lucha contra el terrorismo y la delincuencia.

3.7. Modelos de uso de los sistemas biométricos

En consonancia a lo expuesto anteriormente, el reconocimiento biométrico se fundamenta en verificar la autenticidad de la identidad de un individuo. Es decir, este mecanismo conlleva aportar una muestra del dato biométrico necesario para, posteriormente, realizar una comparación con la muestra original almacenada en el sistema.

Es por este motivo que en el presente, existen tres enfoques que se consideran fundamentales en la aplicación de esta técnica:

- **Autenticación estática:** Este tipo implica en llevar a cabo una única verificación de identidad de la persona. Este proceso se efectúa habitualmente durante el acceso a una estancia o en el primer inicio de sesión del usuario [52].

  Si bien se considera que este método es importante para proteger el control de acceso, no avala la seguridad continua de la sesión la cual puede ser vulnerable por hackers experimentados.

- **Autenticación activa:** En este caso, conlleva que la persona se autentique una segunda vez después de que haya iniciado sesión en el sistema [52].

  Con esta técnica, la capacidad de descubrir el secuestro de sesión mejora significativamente en caso de que estos eventos sucedan antes de que el usuario vuelva a autenticarse [52]. En otras palabras, el sistema tiene la capacidad de reconocer esta situación, así como mitigar el riesgo que implica antes de que el atacante logre explotar el acceso que ha conseguido.

- **Autenticación continua:** En este método, la identidad del usuario se verifica varias veces después de haber iniciado sesión, lo que puede ocurrir periódicamente, después de una actividad específica o en intervalos de tiempo previamente establecidos [52].

  A pesar de que este modo minimiza considerablemente la posibilidad de que un hacker aproveche una vulnerabilidad, cabe la posibilidad de que se pueda aumentar la carga de procesamiento en el sistema de autenticación [52].

  Por ello, es necesario utilizar un enfoque equilibrado aplicando un intervalo de revalidación que sea relativamente pequeño, pero suficiente para reducir los costes de rendimiento.

En definitiva, implementar métodos de verificación sofisticados robustece la seguridad durante toda la sesión. Esto proporcionará una salvaguarda mucho más dinámica contra el acceso no autorizado. De este modo, se enfatiza un compromiso íntegro con la seguridad, adecuándose a las amenazas en constante evolución.

3.8. Estructura general del reconocimiento biométrico

Para que pueda funcionar correctamente, un sistema biométrico automatizado de reconocimiento debe llevar a cabo una serie de fases que garanticen no solo la fiabilidad, sino también la robustez del proceso. Estos estadios abarcan desde la adquisición de la característica biométrica hasta la del resultado de la identificación final. Cada uno de ellos se ha diseñado y perfeccionado a lo largo de los años con la finalidad de reducir al mínimo los posibles fallos, a la vez que se incrementa la precisión del sistema.

Captura de la característica biométrica

La primera fase del funcionamiento de un sistema de reconocimiento es la captura del rasgo biométrico que se quiera utilizar haciendo uso de uno de los dispositivos específicos para esta tarea ya sean sensores o cámaras. El propósito de estos sensores es captar con la mayor fidelidad posible las características propias tanto de las huellas dactilares como de los rostros humanos, las cuales serán un elemento clave en la siguiente fase.

Procesamiento y extracción de atributos

Tras la captura de la muestra, las técnicas de procesamiento de datos biométricos evalúan la calidad de la imagen obtenida con el fin de asegurar que se ajusta a los requisitos necesarios para que el sistema la considere válida. Posteriormente, la imagen es sometida a diferentes tratamientos para uniformar factores como, por ejemplo, la iluminación o la orientación. Se debe agregar que en este punto ya es factible extraer los atributos biométricos del individuo.

Comparación de muestras y toma de decisiones

En el transcurso de los años se han desarrollado múltiples algoritmos responsables de examinar la semejanza entre la muestra del individuo almacenada en la base de datos y aquella imagen que ha capturado el sistema. Es esta comparación la que integra el contenido de esta etapa. Finalmente, teniendo en consideración todo lo detallado anteriormente, el sistema concluirá el resultado final del reconocimiento.

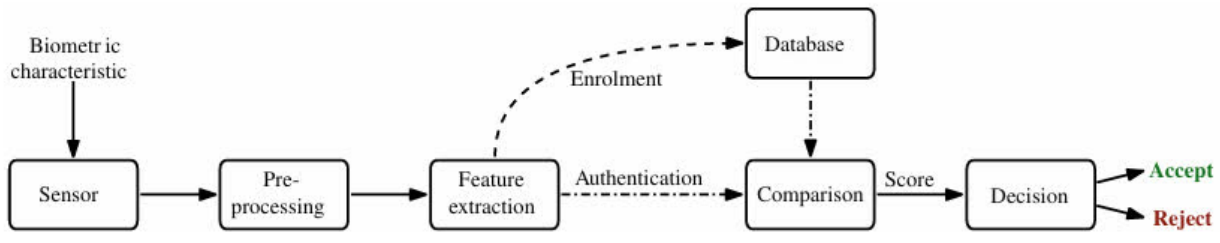

Figura 3.1: Visión general del funcionamiento de un sistema de reconocimiento biométrico [59]

3.9. Evaluación de rendimiento de un sistema biométrico

El rendimiento de un sistema de autenticación biométrico se calibra principalmente por su capacidad para tomar decisiones rigurosas en lo referente a aceptar o rechazar la coincidencia de una muestra de una característica biométrica dentro de una población determinada. Por consiguiente, es esencial comprender que es en este proceso donde reside el éxito o el fracaso de las técnicas biométricas. Para poder entender y optimizar el rendimiento de este tipo de sistemas, se emplean las siguientes métricas comúnmente utilizadas en la industria tecnológica:

- **Tasa de Falsas Aceptaciones (FAR):** Denota la tasa de error procedente de determinar que dos datos biométricos de individuos diferentes pertenecen a la misma persona [52]. Este hecho se considera un fallo crítico del sistema, puesto que de esta forma, se podría estar posibilitando un acceso no autorizado a un posible atacante.

- **Tasa de Falsos Rechazos (FRR):** Expresa la frecuencia con la que el sistema rechaza de forma incorrecta dos muestras biométricas de la misma persona distinguiéndolas como si se trataran de diferentes individuos [52]. Este tipo de imprecisiones pueden provocar problemas de usabilidad causando una gran frustración en los usuarios, lo que podría conllevar un rechazo de estas tecnologías.

- **Tasa de Fallos de Captura (FTCR) y Tasa de Fallos de Inscripción (FTER):** Estas métricas examinan la habilidad del sistema para capturar los datos biométricos, extraer las características particulares de cada uno de ellos y registrarlas correctamente en los sistemas de almacenamiento [52].

Es importante destacar que las tasas FAR y FRR están vinculadas entre sí [52]. Esto se debe a que ambas dependen del umbral de aceptación que se haya instaurado en el diseño del sistema. Adaptar este valor es fundamental para que el sistema sea más o menos resistente al ruido que experimentan las muestras recogidas. Por esta razón, el principal objetivo es encontrar un equilibrio entre la robustez del sistema y la comodidad de los usuarios.

3.10. Estandarización de la terminología biométrica

En el mundo de la biometría, disponer de un vocabulario preciso y estandarizado es esencial para evitar imprecisiones, sobre todo cuando se colabora en ámbitos internacionales. Existen conceptos que dependiendo del contexto de uso pueden derivar en diversas interpretaciones. Además, la falta de claridad en estos aspectos puede ocasionar equivocaciones a la hora de desarrollar, implementar y regular cualquier sistema barométrico. Es por ello que se considera necesario hacer una aclaración sobre el tipo de terminología que será utilizada a lo largo del proyecto.

Con el objetivo de hacer frente a este desafío, entidades como la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) se han enfocado en elaborar una serie de estándares relacionados con la biometría, entre los que destaca el *ISO Vocabulary for Biometrics* [40]. Este glosario ofrece definiciones rigurosas para promover una comprensión coherente de los diferentes términos empleados en este sector, minimizando así las confusiones entre las diversas partes involucradas. La utilización de un lenguaje común es fundamental para asegurar la compatibilidad entre diversos sistemas biométricos, evitando discordancia en términos técnicos y normativos.

Asimismo, estos estándares desempeñan un rol crucial al compatibilizar las terminologías empleadas por los fabricantes, científicos y juristas asegurando una mayor coherencia y eficiencia en el uso de los mismos. De esta forma, los desarrolladores pueden diseñar sistemas interoperables, los investigadores pueden utilizar un marco conceptual común y los juristas pueden crear una legislación vinculada a estas tecnologías. En otras palabras, el uso de un mismo lenguaje no solo optimiza el intercambio de ideas entre las partes implicadas, sino que también fomenta la confianza de los usuarios al simplificar su aplicación en diversos contextos.

3.11. Tipo de datos procesados en un sistema biométrico

Los sistemas de reconocimiento biométrico gestionan una gran variedad de información asociada a los rasgos tanto físicos, como de comportamiento de las personas. Este conjunto de datos es sometido a múltiples transformaciones divididas en fases, hasta que se convierten en un formato práctico que permite llevar a cabo los procesos de autenticación o identificación de manera eficiente.

En conformidad con el estándar ISO/IEC 2382-37:2022 [40], es esencial entender el tipo de información biométrica utilizada en estos sistemas, abarcando desde la captura inicial hasta las últimas etapas de almacenamiento y la posterior comparación. Este criterio ha fortalecido la fiabilidad en la implementación de los sistemas biométricos. A continuación, se desglosarán los conceptos clave que juegan un papel fundamental en este ámbito.

3.11.1. Dato biométrico

Este término hace referencia a una muestra biométrica o una agrupación de ellas como parte de cualquier fase del proceso de reconocimiento. Esto abarca desde la adquisición inicial hasta las plantillas biométricas empleadas en los procesos de análisis comparativo final. Como ejemplo, una imagen facial obtenida por un sensor representa datos biométricos en su forma más básica, que luego serán examinados para extraer sus características o elaborar plantillas. Este concepto destaca que este tipo de información no está claramente relacionada con una identidad concreta hasta que se procesan por el sistema.

3.11.2. Característica biométrica

En base al estándar, estas características se consideran atributos biológicos y de conducta propios de una persona que son esenciales para poder obtener características únicas y repetibles, las cuales son cruciales en el proceso de reconocimiento. Estas propiedades son la clave de los sistemas biométricos, facilitando la diferenciación precisa entre diferentes personas.

Concretamente, la composición de una huella dactilar o las proporciones geométricas de un rostro no solo posibilitan realizar comparaciones efectivas, sino que también sirven como fundamento para la elaboración de plantillas biométricas.

3.11.3. Datos en crudo frente a las muestras biométricas

De acuerdo con la norma, los denominados datos en crudo son las muestras adquiridas durante el proceso de captura. Se trata de aquellos datos que recoge el sensor biométrico, sin la aplicación de ningún tipo de procesamiento o modificación. Un claro ejemplo de esto podría ser una fotografía capturada por una cámara. Pese a que son determinantes para el funcionamiento del sistema, requieren de un posterior tratamiento para poder ser usados correctamente en las siguientes etapas.

En cuanto a las muestras biométricas, son las representaciones, ya sean digitales o analógicas, de los atributos biométricos antes de que se lleve a cabo la extracción de características. Estas son una variante procesada de los datos en crudo específicamente para el posterior análisis. Su calidad es vital para asegurar la precisión y la efectividad del sistema. Por ello, es habitual que en esta fase se apliquen diferentes técnicas de control de calidad garantizando que en las siguientes etapas se trabaje solo con aquellos datos que sean fiables.

3.11.4. Atributos biométricos frente a plantillas biométricas

Los atributos biométricos son un conjunto de números o etiquetas obtenidos a partir de las muestras biométricas a través de sofisticados algoritmos. El objetivo de estos datos es representar aquellas características únicas del individuo. Los atributos biométricos son datos que establecerán la base sobre la cual se elaboran las plantillas biométricas.

Por otro lado, las plantillas biométricas son un conjunto de atributos biométricos almacenados de forma digital. Estas plantillas se elaboran con el objetivo de facilitar la comparación, además de salvaguardar la integridad de la información biométrica. En contraste con los datos en crudo, estas no conservan información original, sino que ofrecen una representación optimizada utilizada en el proceso de comparación.

3.12. Principales estándares biométricos

Tal y como se ha mencionado anteriormente, uno de los aspectos más relevantes que garantizan la seguridad y precisión en los sistemas biométricos es la existencia de lo que se conoce como estándares, entendidos estos como un conjunto de normas desarrolladas por expertos con el fin de regular los protocolos que fundamentan esta materia.

El estándar **ISO/IEC 19794**, base de la biometría moderna, define los formatos que se deben utilizar en el intercambio de datos biométricos como huellas dactilares, imágenes faciales o firmas manuscritas indistintamente del fabricante o la tecnología utilizada.[66]. Estas normas son primordiales para asegurar la interoperabilidad, además de la calidad de la recopilación y el almacenamiento de datos biométricos.

Por otra parte, el estándar **ISO/IEC 24745:2022** se enfoca en la protección de los datos biométricos durante el almacenamiento y la transmisión [67]. Es decir, suministra una serie de pautas para administrar de forma segura este tipo de datos con el fin de evitar el acceso no autorizado, asegurando así la privacidad de los usuarios.

Otro estándar importante es el **ISO/IEC 30107-1:2023**. Este se focaliza en establecer métodos para calibrar la resistencia de un sistema biométrico frente a ataques de suplantación de identidad conocidos como ataques de presentación [68]. Dichos ataques implican proporcionar características biométricas falsas al sistema para evadir la autenticación. De esta forma, se aumenta la confianza para adoptar esta tecnología en aplicaciones sensibles.

En definitiva, el cumplimiento de los estándares biométricos es esencial para asegurar la integridad y confidencialidad de la información que utilizan estas tecnologías. Estos reglamentos proporcionan una base sólida para facilitar la integración y la confianza en las técnicas de autenticación avanzadas. Por consiguiente, la adopción de estos estándares es crucial para afrontar los retos de ciberseguridad, garantizando un futuro digital seguro.

Capítulo 4

Reconocimiento de huellas digitales

El propósito de este capítulo es brindar al lector un enfoque integral y crítico del reconocimiento dactilar. Se investigará la evolución de esta tecnología a lo largo de la historia, analizando el funcionamiento de este tipo de sistemas. Conjuntamente, se discutirán los límites y desafíos de estos métodos, además de llevar a cabo un estudio de la seguridad de estos sistemas de autenticación evaluando su impacto en la privacidad de los usuarios.

4.1. Introducción

Desde la antigüedad, diversas partes del cuerpo humano se han utilizado como elementos de identificación de personas, así lo evidencian los extraordinarios descubrimientos arqueológicos [25]. Siglos más tarde, las huellas dactilares se convirtieron en un método de identificación oficialmente aceptado en investigaciones científicas y procedimientos legales.

Actualmente, la identificación dactilar se ha convertido en la función biométrica más utilizada en el mercado a medida que el uso de sensores de huellas dactilares en diferentes dispositivos y sistemas de seguridad aumenta de forma vertiginosa. Conforme a los recientes informes del sector, se espera que el mercado mundial de este tipo de sensores tenga un valor de 9.540 millones de dólares en el año 2024 [39] debido a la gran cantidad de información que se puede obtener de cada dactilograma.

En el transcurso de los años, los avances tecnológicos han hecho posible que el reconocimiento basado en las huellas dactilares no solamente sea más preciso, sino también más accesible para el usuario final. Debido a ello, la popularidad de esta tecnología enfatiza su relevancia actual, además de suscitar nuevos interrogantes sobre su papel en el futuro de la protección de la identidad de las personas, exponiendo el siguiente interrogante: ¿Hasta qué punto estamos dispuestos a sacrificar nuestra privacidad por la comodidad y seguridad que brindan estos sistemas biométricos?

4.2. La evolución de la dactiloscopia en el tiempo

El método de reconocimiento basado en las huellas dactilares se denomina dactiloscopia, siendo este un término derivado de las palabras griegas *daktylos* (dedo) y *skopein* (estudiar) [64]. La dactiloscopia ha experimentado una gran evolución desde las técnicas primitivas hasta el diseño de los complejos sistemas biométricos actuales. Este trayecto a través de la historia es una demostración de la sagacidad del ser humano para concebir nuevas soluciones confiables en relación con la identificación de individuos. A lo largo de la historia, su desarrollo ha estado marcado por los progresos científicos y tecnológicos que han potenciado su precisión, adecuándose continuamente a las necesidades de la sociedad.

4.2.1. Antigüedad

La larga historia del uso de las huellas dactilares como identificadores biométricos se registra por primera vez en la antigüedad. Los descubrimientos arqueológicos demuestran la certeza de que su praxis existió desde el año 6000 a.C. En especial, la cultura china es distinguida por ser pionera en la utilización de impresiones de crestas de fricción como medio de identificación [13].

Por otro lado, son de particular interés los fragmentos de cerámica caracterizados por poseer huellas dactilares que probablemente fueron utilizados por los alfareros de Oriente Medio para rubricar sus trabajos. No obstante, estas impresiones no necesariamente identifican a un individuo, sino que pueden servir como una marca distintiva de aquellos que las crearon.

Asimismo, la historia de las diferentes dinastías chinas abarca numerosos ejemplos del uso de huellas dactilares. Se han descubierto algunos documentos de este periodo que contienen las huellas dactilares del autor, lo que manifiesta el uso temprano de este método para corroborar la autenticidad del documento. Paralelamente, se han hallado tablillas de bambú con este tipo de huellas que se utilizaban en investigaciones de robos [23].

4.2.2. Siglos XVII - XVIII: Primeros logros científicos

Durante el transcurso de estos siglos, tuvo lugar una gran revolución científica, es decir, fue una época marcada por relevantes descubrimientos en diferentes disciplinas. Es, en este sentido, cuando se iniciaron las primeras investigaciones científicas sobre la piel humana.

Nehemiah Grew, denominado como el «padre de la fisiología vegetal», fue el precursor en el análisis dactilar detallando los diversos modelos y patrones existentes en las huellas dactilares. En el año 1684, Grew publicó *The Description and Use of the Pores in the Skin of the Hands and Feet*, el primer estudio científico sobre la morfología de las crestas y poros de las huellas dactilares [23].

Al mismo tiempo, el anatomista italiano Marcello Malpighi, fue el primer investigador en esclarecer la importancia del significado evolutivo de las crestas de fricción de las manos haciendo uso de los microscopios que habían sido recientemente inventados. En reconocimiento a este autor, la capa de la piel llamada estrato de Malpighi fue nombrada de esta forma gracias a su trabajo en el campo [13] .

Pese a que las crestas de fricción han sido el foco de investigación de diversos científicos a lo largo de los años, la singularidad como propiedad de este rasgo biométrico en Europa no fue reconocida hasta el año 1788 gracias al médico alemán J. C. A. Mayer. En su trabajo llamado *Anatomical Copperplates with Appropriate Explanations* dio a conocer una minuciosa representación gráfica de los diferentes patrones existentes en este tipo de crestas. Adicionalmente, estableció un hito trascendental en la historia de la biometría gracias a la siguiente afirmación: "Aunque la disposición de los procesos de la piel nunca es la misma en dos personas, en algunas personas las similitudes son aún mayores". Con esta aserción, Mayer fue el primer científico en dejar constancia de la singularidad de las huellas que poseen las yemas de los dedos[13].

4.2.3. Siglo XIX: Auge de la dactiloscopia en el ámbito científico

Este siglo es considerado un periodo marcado por destacados progresos en la percepción y aplicación de las huellas dactilares con el objetivo de reconocer a un individuo. En el transcurso de estos años, esta característica biométrica ha sido utilizada en diferentes campos desde la medicina hasta la ciencia forense.

En el año 1823, el Doctor Johannes Evangelista Purkinje, un reputado profesor en la Universidad de Breslau, presentó en su escrito *Commentary on the Physiological Examination of the Organs of Vision and the Cutaneous System*, una categorización de la morfología de las huellas de los dedos en nueve tipos diferentes, proporcionando a cada uno de ellos un nombre basándose en la estructura de las minucias [13]. Cabe destacar que las investigaciones llevadas a cabo hasta principios del siglo XIX condujeron a dos deducciones fundamentales que, hasta el día de hoy, han contribuido a generar una base consolidada en el reconocimiento biométrico: la inexistencia de dos huellas iguales en individuos distintos y la no variación de este tipo de patrones a lo largo de la vida del individuo.

Unos años más tarde, Sir William Herschel, un administrador británico para la East India Company, llevó a la práctica otro acontecimiento histórico en la dactiloscopia de este siglo. En la década de 1850 inició el uso de la huella de la mano con el fin de autentificar los contratos de la empresa. A pesar de que en un principio implementó este método por prevención, su uso ostentó la eficacia a la hora de verificar la identidad de los trabajadores [13].

Por otro lado, el Dr. Henry Faulds, un médico misionero en la India y Japón, también jugó un papel importante en la historia de la biometría. Fue pionero en Europa por publicar en 1880 en la revista Nature un artículo llamado "On the Skin-Furrows of the Hand", argumentando que las huellas dactilares vistas en la escena del crimen podrían usarse para identificar a los delincuentes, lo que estableció las bases de su aplicación en el ámbito de la criminología [23].

En 1892, Francis Galton, primo de Charles Darwin, fue el autor del primer libro destinado plenamente a la investigación de este rasgo biométrico llamado *Finger Prints*. En él, Galton determina los fundamentos básicos como la unicidad y la permanencia en el tiempo de las huellas. Adicionalmente, detalló las pequeñas estructuras existentes en las huellas, lo que actualmente se denominan minucias [23].

El pináculo del trabajo de investigación del siglo XIX en el ámbito de las huellas dactilares lo protagonizó Juan Vucetich. Nacido en Croacia, inmigró a Argentina donde comenzó su carrera como estadístico en el Departamento Central de Policía en La Plata. Fue allí donde, basándose en los estudios de Galton, diseñó un sistema de clasificación dactiloscópico. Así, catalogó las huellas dactilares otorgando letras y números a los tipos de patrones existentes [23].

Vucetich, en 1892, puso en práctica su innovador sistema en una investigación criminal en el célebre "Caso Rojas". Una mujer llamada Francisca Rojas mató a sus dos hijos para posteriomente hacerse un corte en la garganta. Ella acusó a un hombre llamado Velázquez de ser responsable de este suceso. Sin embargo, Vucetich pudo evidenciar que la señora Rojas asesinó a los dos niños con base en una huella ensangrentada hallada en la escena del crimen. La resolución de este caso no solo demostró la eficacia del sistema, sino que también fue importante por su reconocimiento y aceptación mundial [13].

En 1904, Vucetich anunció la publicación del libro llamado *Dactiloscopia Comparada* en la que especificó al detalle el funcionamiento de su sistema. Esta obra representó un gran medio de información que se aplicaría durante los próximos años en las ciencias forenses [23].

En conclusión, se puede determinar que este siglo sirvió de base para la aplicación vanguardista en la identificación de personas a través de las huellas dactilares.

4.2.4. Siglo XX: Consolidación científica de la dactiloscopia

El siglo XX supuso el comienzo de un periodo de consolidación y aplicación de las características biométricas, como son las huellas dactilares, considerándolas una herramienta esencial para la identificación penal y civil. Durante estos años, se perfeccionó la ciencia del reconocimiento de huellas dactilares y tuvo lugar el desarrollo de nuevos métodos que aumentaron su precisión y eficiencia.

En 1901, se instauró el primer archivo de huellas dactilares en Scotland Yard en Londres, lo que supuso un acontecimiento importante en la organización y almacenamiento de un gran número de tarjetas que contenían muestras de este rasgo biométrico [23].

Durante los primeros años de este siglo, concretamente en 1903, el uso de este rasgo biométrico también se implantó en Estados Unidos cuando el sistema penitenciario de Nueva York empezó a registrar las huellas dactilares de los prisioneros. Años más tarde, en 1915, se fundó la primera organización profesional dedicada a la dactiloscopia en Oakland denominada Asociación Internacional para la Identificación Criminal [23].

A partir de mediados de siglo, el progresivo aumento tanto del número de arrestos como de las cifras de los delitos cometidos ocasionaron un nuevo punto de inflexión para los investigadores, quienes empezaron a cuestionar la productividad de los sistemas tradicionales para almacenar información. Este hecho fomentó la necesidad de desarrollar un nuevo método más efectivo que fuera capaz de procesar grandes cantidades de datos [23].

Finalmente, en la década de 1960 y 1970, debido al desarrollo de los ordenadores se presentaron nuevas oportunidades en la digitalización de las huellas dactilares de las personas. Esta evolución desembocó en la instauración del *Automated Fingerprint Identification System (AFIS)*, el cual transformó la forma en la que se analizaban estos rasgos biométricos [23].

4.3. Morfología de las huellas dactilares humanas

Actualmente, las huellas dactilares son consideradas algo más que meras marcas en la piel, son herramientas esenciales en el mundo moderno. El reconocimiento basado en ellas se fundamenta en la complejidad de las crestas de fricción. Por ello, en este apartado se detallará la formación de este rasgo biométrico, así como su clasificación en diferentes categorías.

4.3.1. Estructura de la piel

La piel es el órgano más grande del cuerpo humano y presenta una gran complejidad no solo en su estructura interna, sino también en la fisonomía única de las minucias presentes en las yemas de los dedos. Estas crestas de fricción junto con los poros posibilitan que los dedos se adhieran a diferentes superficies, de la misma forma que los pliegues aumentan la elasticidad de la piel [46].

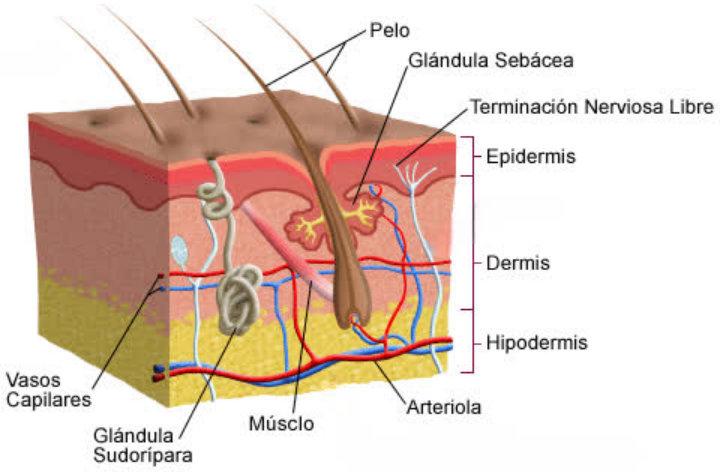

Figura 4.1: Corte transversal de la piel humana. [32]

La anatomía de la piel consta de tres capas fundamentales como se puede apreciar en la Figura 4.1: la epidermis, la dermis y la hipodermis. Cada una de estas capas realiza una función importante en el organismo humano.

La capa más externa llamada epidermis está compuesta fundamentalmente por queratinocitos, los cuales a su vez están formados por filamentos de queratina proporcionando una barrera física frente a patógenos externos, la radiación ultravioleta o la pérdida de agua debido a la evaporación. La epidermis se divide en diferentes subcapas que contribuyen con la regeneración constante de la piel, asegurando su elasticidad y resiliencia respecto a numerosos factores. Esta cualidad regenerativa y protectora hace de esta capa una parte esencial del cuerpo humano [46].

La dermis, conocida como la capa de tejido, se sitúa bajo la epidermis. Esta capa contiene una extensa red de vasos sanguíneos que ayudan a regular la temperatura corporal. La dermis está constituida principalmente por dos estratos. El primero de ellos se denomina dermis reticular y es un tejido conectivo que comprende una gran cantidad de colágeno. Por otro lado, la dermis papilar está formada por las papilas dérmicas y estas se caracterizan por su maleabilidad [46].

Finalmente, la hipodermis, también denominada tejido subcutáneo, es la capa cutánea más profunda. Está conformada esencialmente por tejido adiposo, el cual funciona como una reserva clave de energía. Además, se encarga de la absorción de los golpes disminuyendo la gravedad de los daños en otros tejidos u órganos durante el traumatismo. La consistencia de este tejido puede verse alterada debido a diferentes factores como el sexo del individuo, la edad o la genética, y ello produce la disparidad en el espesor de la piel [46].

4.3.2. Evolución embrionaria de las huellas dactilares

La formación de las crestas de fricción se produce en el transcurso de los dos primeros trimestres del crecimiento del feto humano. Sin embargo, si bien la evolución de todas ellas sigue la misma secuencia de fases, la duración de estas puede alterarse entre diferentes individuos.

Este proceso se inicia con el desarrollo de la mano aproximadamente en la sexta semana posteriormente a la fecundación del óvulo. Entre la sexta y séptima semana de embarazo, las membranas formadas por tejido cartilaginoso que se sitúan entre los dedos comienzan a desaparecer. Además, es en este periodo cuando comienza la formación de las denominadas almohadillas volares en las yemas de los dedos, como las que se pueden observar en la Figura 4.2. Estas prologan su crecimiento hasta la décima semana modificando su tamaño o aspecto [23].

En torno a la décima o undécima semana de la gestación, estas almohadillas empiezan a desaparecer desinflándose. En esta fase se materializa la formación de las crestas de fricción primarias. Este proceso es ocasionado por la fragmentación de las células basales que se encuentran en la epidermis. Esta misma fragmentación aumenta en las zonas centrales de las almohadillas volares desarrollándose, de esta forma, crestas superficiales en la epidermis [23].

Figura 4.2: Almohadilla volar en una mano fetal. [75]

Desde la semana decimoquinta hasta la decimoséptima semana del embarazo, se produce el inicio de la formación de las crestas secundarias. Estas son pequeñas crestas que se conforman en los valles situados entre las crestas primarias. El desarrollo de las huellas dactilares está influenciado por la tensión formada cuando las almohadillas volares retroceden, provocando que la piel se extienda y se oprima [23].

Finalmente, alrededor de la semana 25 se completa la formación de las crestas de fricción, las cuales persistirán invariables a lo largo de la vida de esa persona [23]. Cabe destacar que estos patrones se crean en las yemas de los dedos, además de alargarse a las manos y pies aportando una morfología que es clave en la identificación biométrica.

4.3.3. Clasificación de los patrones de las huellas dactilares

Las huellas dactilares presentes en las yemas de los dedos poseen múltiples patrones únicos formados en el transcurso del desarrollo del feto y no varían con el paso del tiempo a no ser que se produzca daños significativos en la piel. La habilidad de identificar y categorizar estos patrones ha posibilitado el diseño de sistemas de reconocimiento biométrico sofisticados. Actualmente, existen tres tipos que son reconocidos universalmente:

Arcos

Los arcos son la categoría de patrones menos frecuente en las personas, solo está presente en el 5 % de las huellas dactilares de las personas. Este modelo se asemeja a los arcos propios del ámbito de la arquitectura. En este patrón, las líneas de las crestas de fricción comienzan en un lado del dedo para, posteriormente, elevarse en el centro y volver a bajar por el otro lateral. Este patrón se divide en dos grandes tipos: arcos lisos y arcos de carpa.

Los primeros se distinguen por tener un arco suave cuyo trazo se presenta de forma homogénea a lo largo de la huella. Mientras, en el segundo tipo el arco muestra en el centro una pendiente con una mayor inclinación conformando una cúspide. Es precisamente por este motivo por el que reciben su nombre [23].

Figura 4.3: Subtipos del patrón arco [37]

Espiral

Este tipo de patrón se identifica por la forma circular que poseen las líneas de las crestas y se hallan en alrededor del 30 o 35 % de la población. Estos patrones se descomponen en cuatro subclases, cada una de ellas con rasgos propios. Los *plain whorl* se distinguen por la presencia de un centro claramente definido con líneas alrededor formando círculos concéntricos. En cambio, los *Double-loop whorls* se componen por dos bucles que, cuando se unen, forman una estructura similar a un yin-yang, como se puede observar en la Figura 4.4. Por otro lado, los *central pocket loop whorl* se caracterizan por poseer una espiral mucho más suave con un número menor de circunferencias alrededor. Finalmente, los *accidental whorl* se tratan de una fusión de dos o más tipos detallados anteriormente [23].

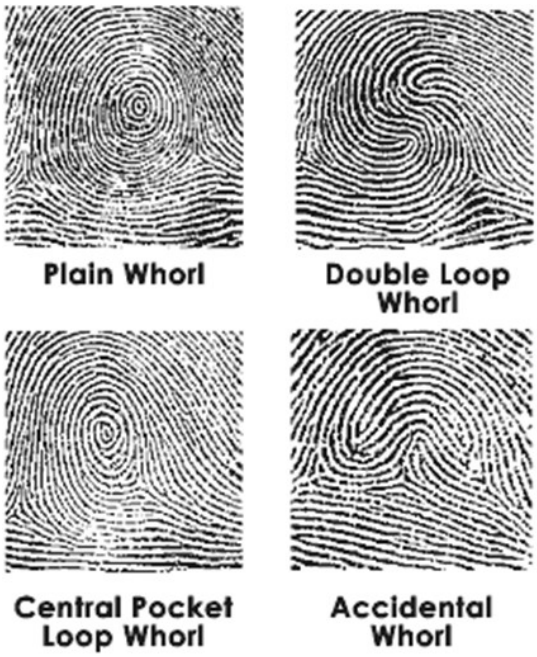

Figura 4.4: Subtipos del patrón espiral [49]

Bucle

El patrón de bucle, también denominado lazo, es el más habitual entre los individuos con una representación aproximada del 60-70 %. Estos bucles se particularizan debido a que las líneas de las crestas de fricción entran por el borde de la yema del dedo, crean una curvatura con forma de U cerca del núcleo y finalmente salen por el mismo lado por el que entraron [23].

En este caso, hay dos tipos de bucles esenciales: bucle izquierdo y bucle derecho. La diferencia entre ambas clases es la dirección que presentan las crestas de fricción. En el bucle izquierdo, las líneas entran por el lado izquierdo de la traza, se curvan alrededor del núcleo y luego salen por el mismo lado izquierdo. Sin embargo, en el bucle derecho las crestas entran por la derecha, forman un arco similar y salen, nuevamente, por la derecha.

Figura 4.5: Subtipos del patrón bucle [37]

En conclusión, la categorización de las huellas dactilares es un procedimiento esencial en el reconocimiento biométrico, puesto que posibilita tanto la organización como el análisis preciso de patrones que presentan una gran complejidad. Mediante su clasificación en estos tres modelos junto con sus correspondientes variantes, se consigue una sistematización que favorece la comparación de diferentes huellas y garantiza la mayor exactitud posible. Esta perspectiva enfatiza la importancia del uso de un método científico en la adquisición de las huellas dactilares.

Adicionalmente, la clasificación de las huellas no solo aporta beneficios en la identificación de individuos, sino que también desempeña un papel importante en la instauración además del mantenimiento de bases de datos que almacenen este rasgo biométrico a gran escala, lo que posibilitaría ser utilizadas por las fuerzas de seguridad a nivel mundial.

Dicho en otros términos, la identificación precisa de este tipo de patrones facilitará realizar búsquedas eficientes permitiendo comparar en pocos minutos una nueva huella dactilar con millones de muestras almacenadas de forma segura. Es por esto que este hecho tiene implicaciones importantes en la resolución de delitos y la prevención del fraude, lo que subraya la importancia de la continua investigación en el ámbito de la dactiloscopia para avalar la seguridad de los ciudadanos.

4.4. Evolución técnica en la captura de huellas dactilares

La tecnología de adquisición de huellas dactilares ha evolucionado significativamente a lo largo de los años, partiendo desde los primeros métodos, en los que las huellas dactilares se estampaban a mano en papel utilizando tinta, hasta los complejos sensores modernos. Esta transformación se ha caracterizado por grandes progresos no solo en términos de precisión, sino también en un aumento de la seguridad de los sistemas biométricos. Dicho de otro modo, estas mejoras optimizan la calidad de la imagen extraída, además de posibilitar la miniaturización de estos sistemas, lo que permite ampliar sus aplicaciones.

4.4.1. Clasificación de escáneres

Los escáneres que se utilizan para capturar las huellas dactilares se pueden catalogar conforme a la cantidad de dedos que son capaces de procesar simultáneamente. Esta clasificación es esencial para establecer los requisitos del sistema en términos de velocidad de procesamiento y robustez.

- **Escáneres de un solo dedo:** Este tipo de sensor está diseñado para poder capturar imágenes de un solo dedo a la vez. Se utilizan en aplicaciones que precisan mantener un equilibrio entre el coste de fabricación, su tamaño y la facilidad de uso personal. Sin embargo, al limitar su potencial se podría comprometer la precisión en el reconocimiento de huellas dactilares [47].

- **Escáneres de múltiples dedos:** A diferencia del anterior, este sensor es capaz de capturar imágenes de varios dedos de una misma mano a la vez. Esta clase de escáneres es muy útil en entornos que demandan un mayor grado de protección. De este modo, estos sistemas garantizan un análisis biométrico completo reduciendo la probabilidad de que ocurran errores en el proceso de identificación. No obstante, su complejidad implica un encarecimiento en los costes, además de incrementar considerablemente su tamaño [47].

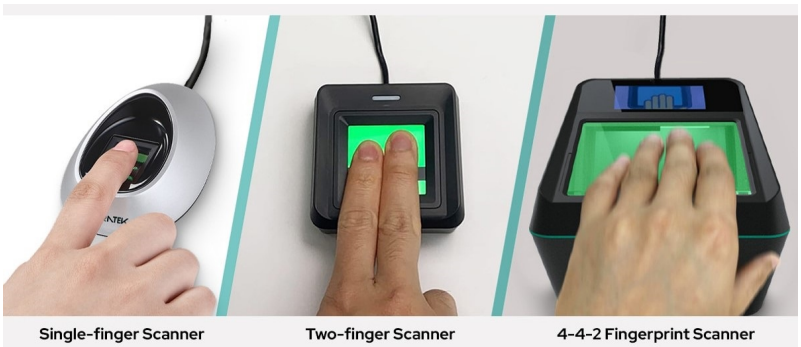

Figura 4.6: Tipos de escáneres de huellas dactilares [7]

4.4.2. Adquisición de huellas dactilares manualmente

La captura de huellas dactilares de forma manual es considerado un método fundamental en el desarrollo de los primeros pasos del campo del reconocimiento biométrico. Esto involucra la recogida de las muestras de las crestas de fricción manualmente sin la utilización de dispositivos digitales. Pese a su antigüedad, esta técnica es esencial en circunstancias concretas como, por ejemplo, en el ámbito de la criminología.

Este método de impresión tradicional inicia manchando la piel del dedo con tinta negra. Posteriormente, se ejerce una pequeña presión en el dedo sobre el papel para, finalmente, digitalizar la muestra por medio de un escáner de papel [47]. Este proceso requiere no solo la precisión de la captura inicial de las huellas dactilares, sino también el posterior almacenamiento y digitalización de estas. Si se realiza correctamente, esto garantiza que la calidad de la imagen perdure durante mucho más tiempo, lo cual es esencial en algunas aplicaciones de la identificación biométrica como en el ámbito penal, entre otros.

Sin embargo, en el registro de huellas dactilares por inyección de tinta existe la posibilidad de que las imágenes capturadas contengan áreas en las que falta información sobre las minucias de las crestas de fricción. Este hecho puede verse provocado por diversos factores como el uso de muy poca o demasiada tinta, hacer poca presión sobre el papel o realizar movimientos bruscos que puedan emborronar la imagen final [47].

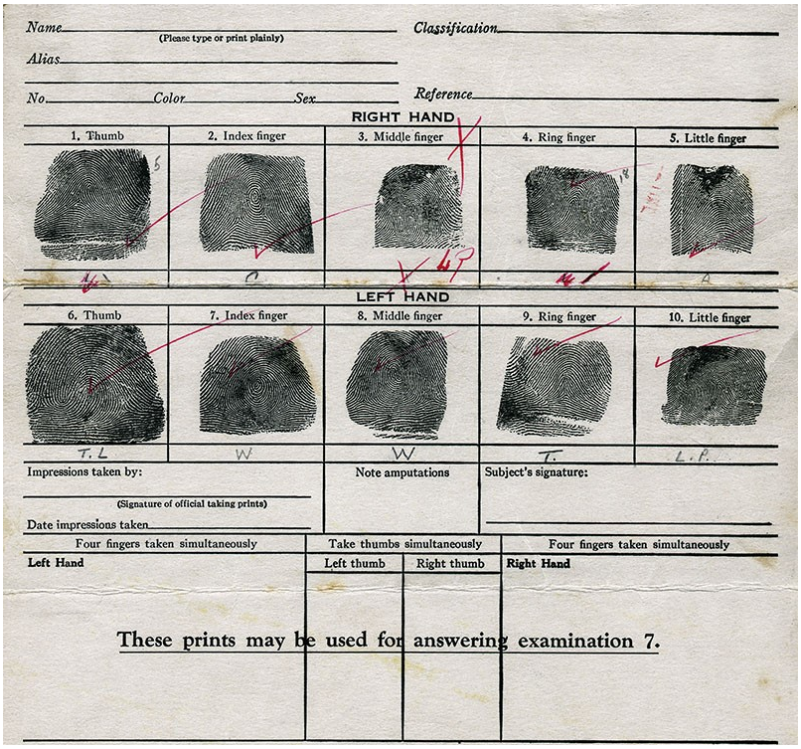

Figura 4.7: Ejemplo de una ficha policial con las huellas adquiridas con la técnica de la tinta [8]

4.4.3. Adquisición de huellas dactilares electrónicamente

El progreso de la tecnología de captura de huellas dactilares ha revolucionado el mundo de la biometría, proporcionando mejoras significativas en la velocidad y precisión de la adquisición de datos biométricos. En contraposición de las técnicas convencionales que requieren el seguimiento de procesos dificultosos, este tipo de escaneo captura las huellas en tiempo real con un gran nivel de detalle. A causa de estos avances, el rendimiento de los sistemas de verificación de identidad se ha optimizado notablemente.

4.4.3.1. Sensores ópticos

Los sensores ópticos se basan en la proyección de luz sobre el dedo para, después, analizar cómo esta se refleja y así capturar imágenes precisas de las minucias. A continuación, se detallan las distintas tecnologías utilizadas en los sistemas de capturas ópticos:

- **Frustrated Total Internal Reflection - FTIR:** Se trata de la técnica de adquisición de imágenes más antigua que se utiliza en la actualidad. En estos sistemas, para capturar la imagen, el dedo se coloca sobre la superficie de un prisma. Cuando este toca la parte superior del prisma, las crestas entran en contacto con la superficie, pero las ranuras permanecen a cierta distancia. De esta forma, la luz que entra en el prisma será totalmente reflejada en los valles, mientras que en la zona de las crestas será absorbida. Esta desigualdad presente en el reflejo de la luz origina un contraste donde las crestas se muestran oscuras, a diferencia de los valles que se muestran claros. Finalmente, la luz que se refleja es capturada por un sensor CCD o CMOS, dando como resultado una imagen digital de la huella dactilar. No obstante, estos sistemas pueden experimentar distorsiones geométricas como, por ejemplo, la distorsión trapezoidal, además de presentar problemas en casos concretos donde la piel del dedo esté seca y no se produzca suficiente contacto con la superficie del cristal [47].

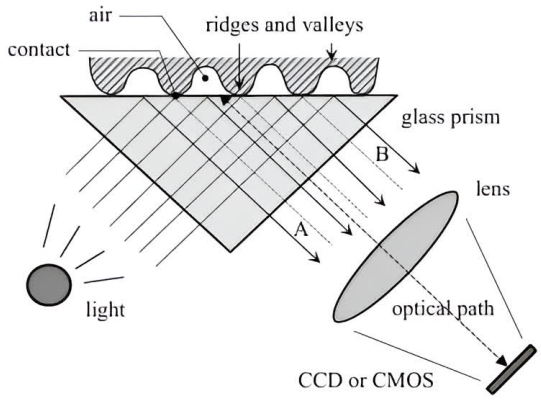

Figura 4.8: Funcionamiento del sensor FTIR [47]

- **FTIR con un conjunto de prismas:** Este sistema es una variación del sensor FTIR clásico. En lugar de usar un único prisma, este método utiliza una serie de prismas más pequeños ubicados de forma contigua. Esta modificación en el diseño del sensor ha permitido reducir su tamaño, a pesar de que la calidad de la imagen adquirida pueda resultar peor. Aunque exista este inconveniente, emplear este tipo de prismas resulta útil en lugares donde el espacio es limitado [47].

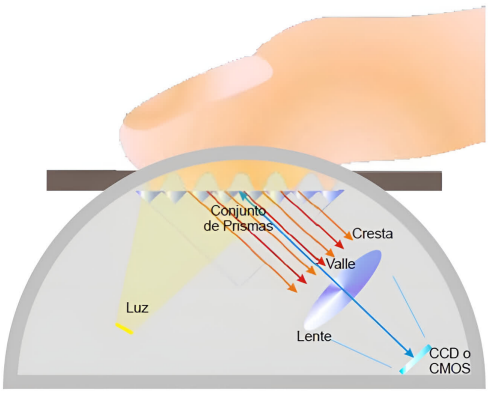

Figura 4.9: Funcionamiento del sensor FTIR con un conjunto de prismas [48]

- **Fibra óptica:** La aplicación de fibras ópticas es una alternativa a los métodos anteriores que ofrece reducir aún más el tamaño del dispositivo final al reemplazar los prismas y la lente por una pletina de fibras ópticas.

  En este caso, el dedo está en contacto directo con uno de los lados de la pletina. En contraste con los mecanismos FTIR, el sensor CCD o CMOS están unidos por el otro lateral de la pletina sin necesidad de utilizar una lente. Esta disposición aporta un diseño mucho más comprimido que otras tecnologías con un coste de producción elevado [47].

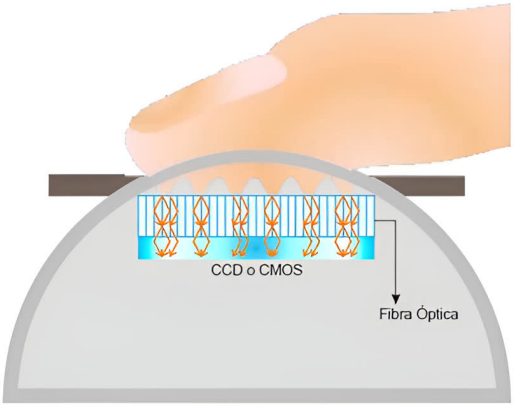

Figura 4.10: Funcionamiento del sensor de fibra óptica [48]

- **Electro-óptico:** Estos dispositivos están formados por dos capas: la superior incluye un polímero que, cuando se polariza aplicando un voltaje adecuado, emitirá luz dependiendo del voltaje que se emplee. Nuevamente, debido a que las crestas entran en contacto con el polímero y los valles no, se producen diferencias de potencial entre zonas al variar la cantidad de luz emitida. Por otro lado, la segunda capa se compone de fotodiodos que, cuando reciben la luz que se emite, la transforman en una imagen digitalizada. A pesar de la importante reducción de tamaño que se obtiene con ellos, la calidad de la imagen capturada es inigualable a la obtenida gracias al sensor FTIR [47].

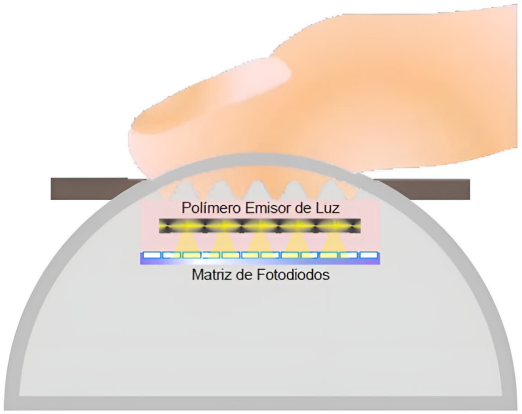

Figura 4.11: Funcionamiento del sensor electro-óptico [48]

4.4.3.2. Sensores de estado sólido

El principal motivo por el cual se diseñaron los sensores de estado sólido fue para solventar los inconvenientes asociados con el tamaño y el coste de fabricación, pues se consideraban los motivos que impedían el acogimiento masivo de estos sistemas de reconocimiento. Estos sensores están formados por numerosos píxeles, siendo cada uno de ellos un reducido sensor por sí mismo. Acto seguido, se describen las tecnologías utilizas para convertir el patrón de las huellas dactilares en señales eléctricas:

- **Capacitivos:** Actualmente, se trata de una de las tecnologías más utilizadas entre los sensores de silicio. Este tipo de sensores están formados por una lámina de condensadores que está integrada en un chip. Esta estructura posibilita que se originen pequeñas cargas eléctricas entre la superficie del dedo y las placas. La dimensión de estas cargas puede verse alterada en función de la distancia existente entre la superficie del dedo y las pletinas, dando como resultado distintos patrones de capacitancia que se corresponden al conjunto de crestas y valles propios de las huellas dactilares.

  Al contrario que en los sensores ópticos, en los capacitivos es complicado engañarlos utilizando una foto de la huella, ya que se debe tener en cuenta que estos dispositivos miden distancias, lo que implica que solo son capaces de capturar superficies tridimensionales.

El principal beneficio de este tipo de sensores es la posibilidad de adaptar los parámetros eléctricos. Este hecho favorece afrontar diferentes condiciones cutáneas de la piel como dedos excesivamente húmedos o secos. Sin embargo, requieren una limpieza regular, ya que la acumulación de grasa y suciedad pueden reducir la calidad de la imagen obtenida [47].

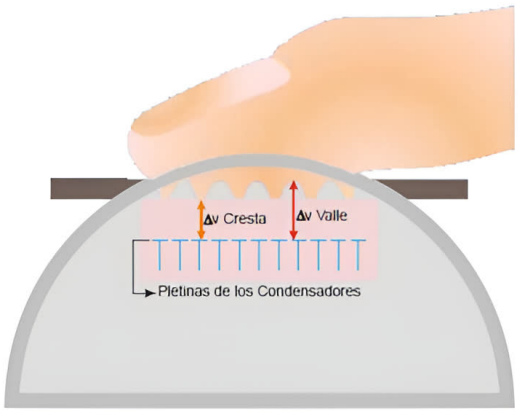

Figura 4.12: Funcionamiento del sensor capacitivo [48]

- **Térmico:** Estos sensores están compuestos por materiales piroeléctricos que producen electricidad a partir de variaciones en la temperatura. Se mantienen a temperaturas altas a través del calentamiento eléctrico para poder aumentar la disparidad de temperatura entre la superficie del sensor y la huella dactilar. En el momento en el que el dedo se apoye en el sensor, las crestas que están en contacto directo con la superficie provocarán una diferencia de temperatura distinta a la de los valles que se encuentran una distancia mayor del sensor. Es esta diferencia de temperatura lo que permite que se genere la imagen digital de la huella. No obstante, esta imagen se desvanece rápidamente cuando se alcanza el equilibrio térmico [47].

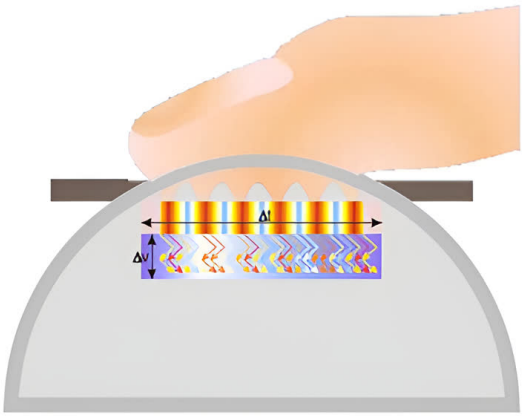

Figura 4.13: Funcionamiento del sensor térmico [48]

- **Campo eléctrico:** Este dispositivo está formado por un anillo conductor que genera una sinusoidal de radiofrecuencia, además de una serie de antenas que reciben las señales producidas por el anillo y moduladas por la morfología de la piel del dedo. Para su correcto funcionamiento, el dedo debe estar simultáneamente en contacto tanto con el sensor como con el anillo. Mediante esta técnica se pueden capturar imágenes precisas basadas en la modulación de la señal generada por las diferentes estructuras de la piel, proporcionando un mayor nivel de seguridad frente al uso de dedos artificiales [47].

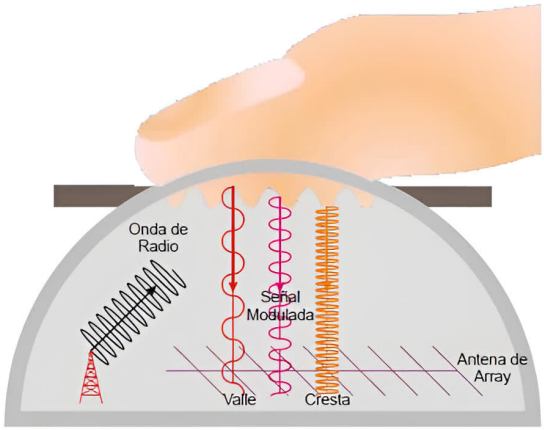

Figura 4.14: Funcionamiento del sensor de campo eléctrico [48]

- **Pizoeléctrico:** La superficie de este tipo de sensores está constituida por un dieléctrico no conductor que genera una pequeña señal eléctrica cuando se les somete a una presión con el dedo, lo que se denomina efecto piezoeléctrico. Por ende, la intensidad de esta corriente depende de la presión ejercida sobre la superficie del sensor. De nuevo, la diferencia de distancias entre las crestas y los valles de las huellas dactilares es desigual, lo que se convierte en presiones diferentes y, por consiguiente, en variaciones de corriente. Los sensores pizoeléctricos tienen una gran desventaja, ya que no son tan susceptibles para poder detectar diferencias pequeñas en la presión, por lo que se convierten en dispositivos que se pueden falsificar fácilmente [47].

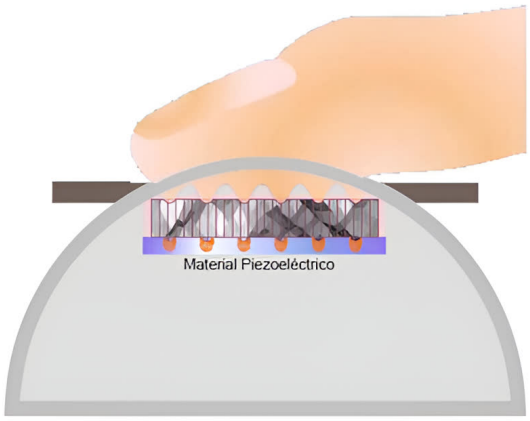

Figura 4.15: Funcionamiento del sensor pizoeléctrico [48]

4.4.3.3. Sensores ultrasónicos

El proceso de capturar una huella dactilar haciendo uso de sensores ultrasónicos se puede considerar como una ecografía. Este proceso implica enviar señales acústicas hacia el dedo para posteriormente registrar los diferentes ecos que se produzcan. Este dispositivo está formado por dos elementos: un transmisor que es el encargado de crear las señales sonoras y un receptor que detecta las respuestas obtenidas cuando las señales rebotan en la superficie de la huella. Es decir, el eco se utiliza para calcular la profundidad de la huella y poder así determinar la estructura de la cresta de fricción. Se ha demostrado que este método es resistente a la acumulación de suciedad y grasa en los dedos, de manera que permite adquirir imágenes de buena calidad. Sin embargo, es una tecnología realmente costosa de fabricar [47].

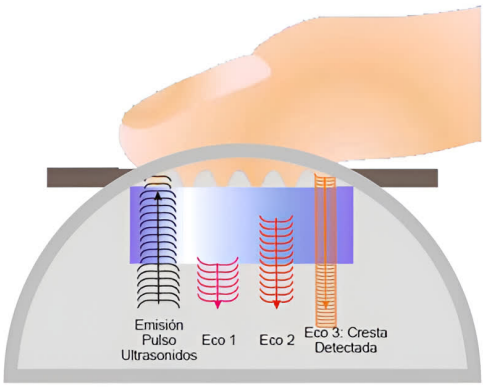

Figura 4.16: Funcionamiento del sensor ultrasónico [48]

4.5. Extracción de las características de las huellas

Después de que se haya capturado una imagen de calidad de la huella dactilar del individuo utilizando el tipo de sensor adecuado en cada contexto de aplicación, el siguiente paso que se debe llevar a cabo en el reconocimiento biométrico es la extracción de las características propias de las crestas de fricción. Este proceso es esencial, ya que involucra distinguir y procesar las singularidades de la huella. Este tratamiento de los datos biométricos es crucial para posteriormente realizar una correcta comparación con las muestras almacenadas en el sistema.

4.5.1. Proceso de segmentación

La segmentación es la etapa previa a la extracción de las características. El propósito es disgregar el área que contiene información valiosa sobre la huella de aquello que forma el fondo de la imagen capturada [41]

Como resultado de este proceso, se optimizará la calidad de los datos biométricos antes de procesarlos para avalar que los atributos extraídos procedan solamente de la huella y no de zonas intrascendentes que podrían incluir ruido o errores en la identificación final del usuario.

En vista de que las huellas dactilares están constituidas por diferentes patrones de líneas, esta segmentación no se puede realizar de forma eficaz utilizando métodos convencionales de umbralización. Para poder definir los límites de la imagen, este tipo de técnicas se fundamentan en la intensidad de los píxeles, por lo que no se consideran adecuados para separar ambas áreas a causa de la complejidad de las crestas de fricción. En cambio, en el presente, la segmentación de las huellas dactilares se lleva a cabo con procedimientos muchos más sofisticados que tienen en consideración la morfología específica de las crestas de las huellas [41]

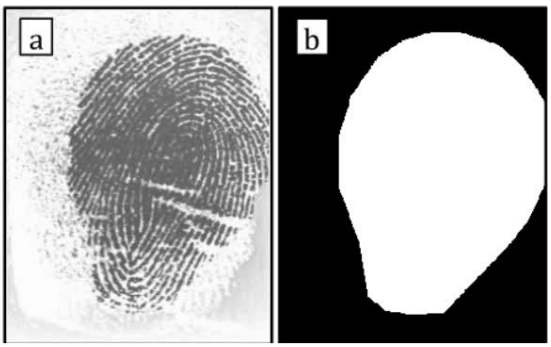

Figura 4.17: Segmentación de una huella dactilar [20]

4.5.2. Detección de singularidades

La detección de características se basa en identificar correctamente elementos clave como espirales o arcos, que son propios de las crestas de fricción. Esta localización es decisiva dado que simplifica la siguiente etapa, que es la coincidencia y comparación de muestras.

Gran parte de los planteamientos detallados en las fuentes bibliográficas de la biometría para detectar estas singularidades se basan en la orientación de la imagen adquirida de la huella dactilar que simboliza la dirección de las líneas de las crestas en cada punto.

La técnica más conocida para ello se sustenta en el índice de Poincaré. Este enfoque se realiza con cálculos matemáticos sobre las desemejanzas de orientación entre los elementos que son contiguos en los trazos de las huellas. Es común que estas diferencias representen la existencia de estas características. [41]

El primer paso para calcular este índice es fraccionar la imagen de la huella en una matriz con forma cuadrada donde cada elemento plasma el ángulo de la cresta en ese bloque de la figura. Para cada bloque ubicado en la posición (i,j), los ángulos de los bloques vecinos se evalúan para establecer la forma en la que cambian de dirección en torno a ese bloque central.

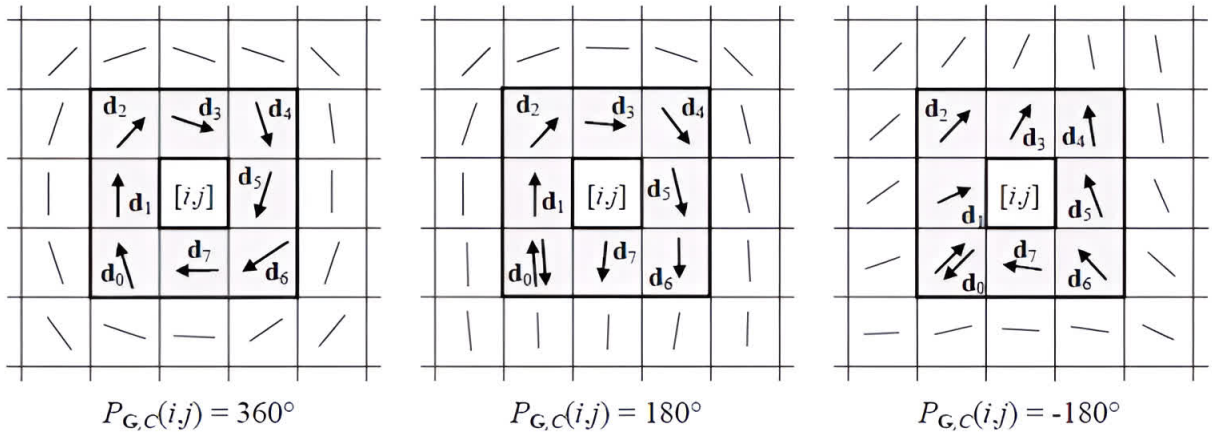

Figura 4.18: Cálculo del índice de Poincaré [65]

Es decir, el índice de Poincaré del bloque (i, j), que se expresa como P(i,j), se computa sumando los ángulos de los elementos adyacentes a ese bloque céntrico. Si el resultado obtenido es 360º denota que existe una característica del tipo espiral, mientras que si el resultado es 180º hay una espiral. Sin embargo, si el resultado da cero, eso significa que en ese bloque no se encuentra ninguna singularidad.

4.5.3. Mejora de la calidad de la imagen a través de la binarización

Con el fin de potenciar el rendimiento de los algoritmos de extracción de los puntos característicos es necesario analizar imágenes con la mejor calidad posible. Por este motivo, la mejora de la imagen adquirida consiste en incrementar el contraste de las minucias de las crestas.

Este paso es importante porque en muchas ocasiones las huellas dactilares obtenidas pueden ser de mala calidad debido a factores externos como la condición de la piel del dedo o complicaciones relacionadas con el sistema, como las interferencias que sufren los sensores.

Uno de los métodos más utilizados para conseguir este aumento de calidad es el filtrado contextual, cuyas propiedades se ajustan a la estructura de la huella. Dicho de otra manera, en lugar de utilizar un único filtro para toda la imagen, se aplica un tipo diferente dependiendo del área que se esté mejorando. En el ámbito de la biometría, un tipo de filtro muy popular para mejorar las huellas dactilares es el filtro Gabor. [41]

A continuación, se efectúa la binarización de la imagen. Este proceso aplicado a las huellas dactilares implica transformar la imagen que ha sido capturada en una escala de grises a una imagen binaria, es decir, cuyos colores solo sean blanco y negro [29]

4.5.4. Extracción de las minucias

Finalmente, el último paso de este proceso sería la extracción de las minucias. Sin embargo, este proceso necesita que la imagen de la huella sea sometida a un procesamiento de reducción del grosor de las líneas de las crestas a un solo píxel [41].

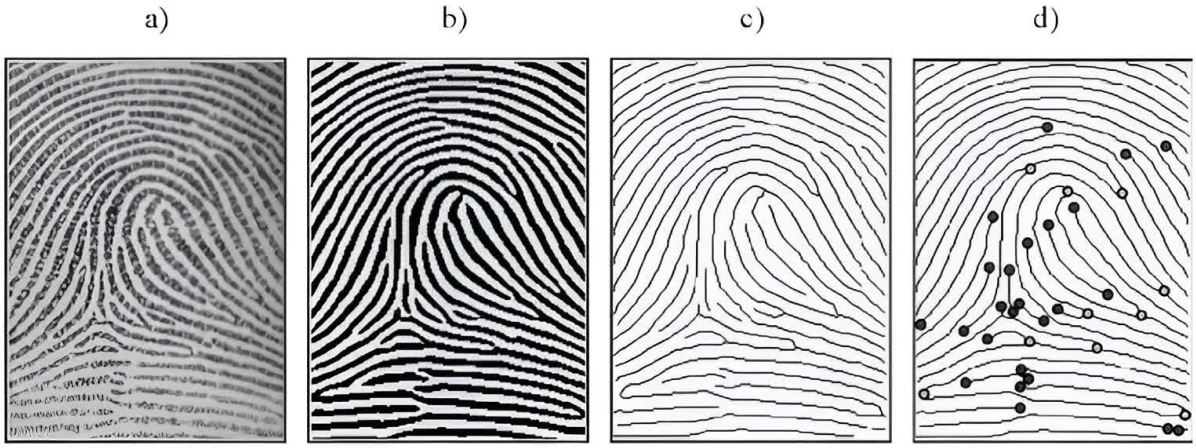

Figura 4.19: a) Imagen después de la segmentación; b) Proceso de mejora y binarización; c) Adelgazamiento; d) Extracción de minucias [41]

Es relevante resaltar que algunos autores han presentado diferentes métodos para extraer minucias directamente de la imagen representada en escala de grises sin que haya pasado por el proceso de la binarización. Este enfoque previene la posible pérdida de información relevante que puede producirse en la ejecución de este proceso con imágenes que tengan una calidad menor [41]

4.6. Comparación de huellas dactilares

Comparar un rasgo biométrico tan complejo como resulta una huella dactilar es un desafío debido a la gran variación intraclase que presentan las huellas de un mismo dedo, lo que puede llevar a que dos huellas del mismo dedo sean consideradas dispares en un sistema de reconocimiento biométrico debido a factores externos como movimientos de rotación o traslación.

Para resolver este inconveniente, los expertos en la industria de la biometría hacen uso de métodos detallados cuando se trata de precisar si dos crestas de fricción pertenecen al mismo dedo. Este procedimiento comprende aspectos como la evaluación de la composición global del patrón y la correspondencia cualitativa y cuantitativa de las minucias, así como la relación entre ellos [47].

El proceso de la coincidencia de huellas dactilares es una de las fases más importantes, pues involucra realizar una comparación de la imagen de la huella capturada con la muestra que está almacenada en el sistema con el fin de verificar la identidad de una persona, por lo que cualquier error en esta etapa puede tener graves consecuencias. Es por ello que el éxito de las técnicas de comparación depende en gran medida de la calidad de las huellas dactilares adquiridas, así como de la eficacia del algoritmo empleado para compararlas. En consecuencia, en esta etapa se debe hacer frente a los siguientes desafíos por causa de la variabilidad inherente propia de las huellas dactilares [52]:

- **Desplazamientos y rotaciones:** Cabe la posibilidad de que los usuarios ubiquen el dedo en una posición o ángulo en el sensor de forma diferente cada vez que se identifiquen. Esto puede resultar en que una parte de la huella esté fuera de la zona de captura, reduciendo el tamaño de la imagen captada. Este inconveniente es difícil de resolver en aquellos sensores que disponen de áreas de captura pequeñas. En estos casos, cualquier cambio, por pequeño que sea, puede provocar coincidencias inexactas.

- **Presión ejercida y condiciones de la piel:** La presión que se hace con los dedos sobre el sensor, del mismo modo que el estado de la piel, tales como humedad, sequedad o grasa, pueden afectar a la calidad de la imagen adquirida por el sistema.

- **Ruido introducido por el sensor:** Los sensores de este tipo de sistemas pueden insertar ruido en las imágenes obtenidas dificultando obtener una comparación precisa de muestras. Ejemplos de ruido pueden ser residuos de huellas anteriores que permanezcan en la superficie del sensor.

- **Distorsión no lineal:** Las crestas de fricción propias de las huellas son estructuras tridimensionales que se distorsionan cuando se proyectan sobre una imagen bidimensional. Esta deformación se debe a la elasticidad de la piel que puede deformarse de muchas maneras diferentes al ejercer presión en el sensor. Esta variación en la forma puede obstaculizar la comparación de las huellas debido a que una misma huella puede presentarse con diferentes imágenes.

En los últimos años, se han desarrollado diversas técnicas para comparar huellas dactilares, cada una de ellas diseñada para afrontar la complejidad asociada a este proceso. Estos métodos se pueden dividir en distintas categorías en consonancia con el planteamiento utilizado. Las más frecuentes son las basadas en correlación de imágenes o en las minucias, al igual que las que se centran en las características de las crestas de fricción.

En los sistemas modernos, la mayoría de estas técnicas funcionan correctamente en el supuesto de que las imágenes de las huellas dactilares que se le proporcionen sean de buena calidad. No obstante, la capacidad de operar con muestras de baja calidad o huellas parciales es un desafío para los investigadores de este ámbito.

4.6.1. Técnicas basadas en la correlación entre imágenes

Los métodos basados en correlación se enfocan en calcular la correlación cruzada entre la muestra de la huella del usuario almacenada en el sistema y la imagen capturada por el mismo con el fin de maximizarla. Este proceso se basa en la superposición de dos imágenes de muestras de las huellas dactilares para poder computar la correlación existente entre los diferentes píxeles. En concreto, consiste en aplicar rotaciones en la imagen capturada sobre la muestra para analizar la similitud en cada punto hasta conseguir una alineación entre ambas imágenes que sea óptima. Cuanto mayor sea el valor de correlación, la semejanza entre las huellas que se están comparando será mayor [41].

Pese a que aparentan ser técnicas sencillas, este tipo de procesado requiere un elevado coste de computación debido al gran número de operaciones que sería necesario realizar en un intervalo de tiempo pequeño. Por otro lado, la aplicación directa de esta técnica no suele aportar resultados que se consideren aceptables. Esto se debe a los desafíos, detallados anteriormente, que enfrentan este tipo de algoritmos.

Para poder superar estas dificultades, se han diseñado nuevas variaciones de este método como, por ejemplo, el cómputo de la correlación local en zonas específicas del patrón de las huellas o la correlación en el dominio de Fourier, que aumentan el rendimiento del proceso [41].

4.6.2. Técnicas basadas en minucias

Las técnicas basadas en minucias son consideradas el método más eficiente en la comparación de huellas dactilares, siendo actualmente las más utilizadas. Se fundamentan en comparar las singularidades propias de las crestas de fricción. En este proceso se extraen las minucias de las dos muestras de huellas para almacenarlas como un conjunto de puntos en un plano bidimensional. En este caso, cada minucia está representada como $m = (x, y, \theta)$, donde (x, y) simbolizan las coordenadas de la ubicación de la minucia y θ es el ángulo que representa la orientación en ese punto concreto. Este cambio en el enfoque transforma la comparación de huellas en un problema de coincidencia de patrones de puntos [41].

En este caso, es fundamental realizar una alineación previa de las muestras de las huellas para poder obtener una comparación precisa. Esto implica efectuar movimientos de desplazamiento y rotación de una de las dos imágenes para conseguir que las minucias estén lo más próximas posible entre ellas.

Para llevar a cabo este proceso, uno de los algoritmos más frecuentes es la transformada de Hough que se utiliza en la coincidencia global de singularidades basándose en la detección de picos en un espacio de parámetros. En contraposición al método de correlación, esta técnica facilita una forma más estructurada de comparar huellas dactilares, ya que se centra en la coincidencia de puntos decisivos en lugar de en la correlación general de imágenes [41].

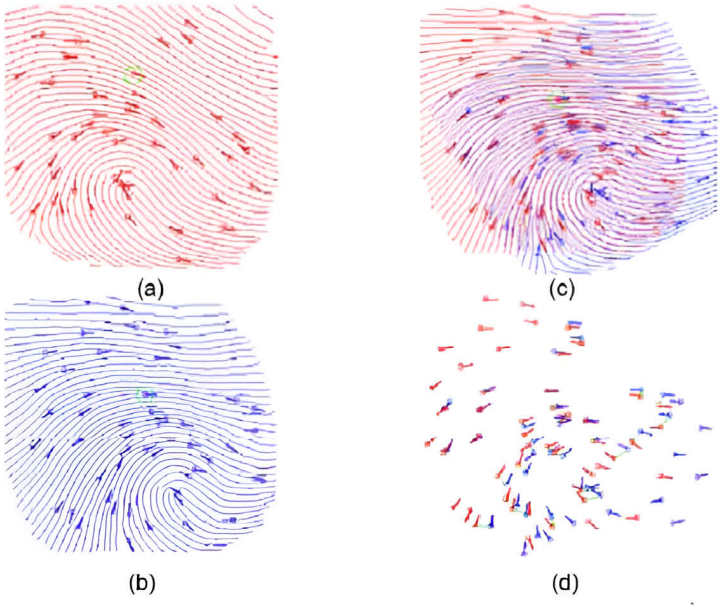

Figura 4.20: Técnica de comparación basada en minucias: a) y b) Muestras de las huellas a comparar; c) Proceso de alineación; d) Detección de minucias [65]

Existen algunos autores que han recomendado el uso de métodos de coincidencia de minucias basados en la estructura local de la huella que está caracterizada por tener propiedades invariantes con respecto a transformaciones globales, como son los movimientos de traslación y rotación, por lo que se ha determinado que son más adecuadas para realizar la comparación sin necesidad de tener que alinear previamente las muestras. No obstante, la comparación de huellas dactilares basada exclusivamente en características locales disminuye la cantidad de información disponible para llevar a cabo este proceso [41].

En conclusión, para diseñar un algoritmo que se fundamente en este tipo de técnicas es necesario mantener un equilibrio entre el uso de las coincidencias locales, que ofrecen una mayor simplicidad y menor carga computacional, pero presentan una menor capacidad de distinción entre huellas frente a las coincidencias globales, que son mucho más complejas, pero prometen una alta discriminabilidad.

4.6.3. Técnicas basadas en características generales de las minucias

Este tipo de métodos surgieron como una alternativa en aquellos casos en los que el sistema de reconocimiento obtiene imágenes de baja calidad de la característica biométrica, lo que puede dificultar la extracción de los pequeños detalles de estas. Sin embargo, este tipo de patrones disponen de otras características más generales como pueden ser la orientación o la textura, que pueden ser analizadas de forma más segura [41].

Actualmente, existen una serie de características alternativas que se emplean en la comparación de huellas dactilares. Uno de los métodos más favorable es el análisis de las relaciones espaciales y las propiedades geométricas de las crestas de fricción, así como de las características relacionadas con la forma.

Adicionalmente, los poros ubicados en la piel de la yema del dedo proporcionan un nivel alto de discriminación a pesar de que requieren sensores de alta resolución para poder examinarlos, lo que aumenta significativamente su coste. Por otro lado, existe una variación de estas técnicas todavía en fase de investigación que se basa en la información que se puede extraer acerca de las texturas de la piel.

Finalmente, se han planteado en estudios recientes la combinación de la utilización de las técnicas basadas en minucias junto con el análisis de otro tipo de características con el objetivo de mejorar el rendimiento en términos de precisión de los sistemas de reconocimiento biométrico [41].

En relación con lo expuesto anteriormente, la comparación de huellas dactilares, si bien es la clave para el éxito de las tecnologías biométricas, debe anteponerse a los desafíos relacionados con la variabilidad inherente propia de estas características.

En consecuencia, los sistemas automatizados modernos se han impuesto a muchos de estos obstáculos por medio de técnicas sofisticadas de análisis de datos. Sin embargo, desarrollar un sistema de reconocimiento biométrico exige mantener un equilibrio entre la precisión de la captura de imágenes y la robustez de los algoritmos para garantizar un rendimiento óptimo, incluso en aquellos entornos operacionales complejos.

4.7. Evaluación de seguridad de los sistemas de reconocimiento basados en huellas dactilares

En estos últimos años, los sistemas de autenticación biométrica, cuyo funcionamiento se basa en las huellas dactilares, se han reafirmado convirtiéndose en uno de los métodos de verificación de identidad más frecuentes y fiables en virtud de la singularidad de las crestas de fricción en el transcurso del tiempo.

No obstante, del mismo modo que cualquier otra tecnología, estos tipos de sistemas no están libres de la posibilidad de que se exploten vulnerabilidades. Es por esta razón que evaluar su seguridad es fundamental para poder minimizar los riesgos a los que se exponen, puesto que estos mismos riesgos podrían poner en compromiso la integridad del proceso de autenticación.

En esta sección se llevará a cabo un análisis de las amenazas esenciales que afrontan los sistemas de reconocimiento basados en huellas dactilares, clasificando los diferentes tipos de ataques y estudiando la eficiencia de las contramedidas propuestas para proteger estos sistemas de un posible fraude o de accesos no autorizados.

4.7.1. Tipos de fallos en los sistemas basados en huellas

Las vulnerabilidades que aparecen en el diseño de estos sistemas no solo repercuten en el acceso de los usuarios que son legítimos, sino que también podrían manifestarse brechas de seguridad que pueden ser aprovechadas por un atacante. En el presente, existen dos tipos principales de errores que pueden afectar al correcto funcionamiento de estos sistemas:

- **Denegación de servicio (DoS):** La denegación de servicio, un error en el que se bloquea el acceso a usuarios lícitos, puede provocar bloqueos parciales o fallas totales del sistema. Este tipo de fallos no solo influyen en la experiencia de uso del usuario, sino que también pueden tener consecuencias catastróficas en aplicaciones críticas, como en el ámbito bancario o en la sanidad pública. Estos pueden ser provocados por errores internos del sistema u ocasionados intencionalmente por un hacker, cuyo objetivo es comprometer el sistema para obtener un beneficio [47].

- **Intrusiones:** Este fallo supone una amenaza aún más grave en el momento en el que una persona externa obtiene un acceso no autorizado al sistema. Las consecuencias de un ataque exitoso pueden resultar ser nefastas, desde la modificación de datos confidenciales hasta la revelación de información personal. En contraposición a las claves tradicionales, las huellas dactilares no se pueden modificar en caso de ser comprometidas. Este hecho las hace un objetivo para los piratas informáticos más experimentados [47].

El equilibrio entre la prevención de una denegación de servicio y la protección contra intrusiones en los sistemas de autenticación basados en huellas dactilares es complejo, pues en ocasiones los dos propósitos pueden entrar en conflicto entre sí. Por una parte, la implementación de medidas de prevención de intrusiones, como una autenticación multifactor, pueden mejorar la seguridad del sistema, pero, simultáneamente, se pueden aumentar el número de falsos rechazos. Por otro lado, facilitar el proceso de autenticación para perfeccionar la usabilidad de los usuarios puede desembocar en que el sistema sea más vulnerable frente a los ataques de intrusión.

4.7.2. Ataques directos a partir de huellas latentes

En los sistemas de autenticación basados en la adquisición de huellas dactilares de la yema de los dedos, un ataque directo hace referencia a que no es necesario tener un conocimiento exhaustivo de la operatividad interna del sistema. En otros términos, un atacante únicamente requiere tener acceso al sensor de captura de huellas para, posteriormente, utilizar un dato biométrico falso con la finalidad de engañar al sistema, simplificando así la metodología para llevar a cabo el ataque de forma exitosa. Los ataques partiendo de las huellas dactilares latentes son un ejemplo perfecto de un ataque directo.

Estos representan un serio riesgo, ya que posibilitan obtener un acceso no autorizado a través de aquellas huellas que las personas dejan fortuitamente en diferentes superficies. Este tipo específico de huellas se pueden encontrar en muchos objetos que se usan en la vida diaria como, por ejemplo, las pantallas táctiles. El proceso de adquisición de la muestra ficticia, también denominado *gummy finger*, es crucial para la eficacia del ataque. Con este propósito, existen dos escenarios fundamentales:

- **Con cooperación:** Con la colaboración del usuario, este sitúa su dedo de manera legítima sobre un material moldeable para obtener el negativo de la huella dactilar. A continuación, este molde se recubre con silicona para fabricar la huella falsa. [33].
- **Sin cooperación:** En este caso, el atacante capturará la huella latente que permanece en la superficie del sistema de reconocimiento haciendo uso de un conjunto especial de herramientas. El siguiente paso será su digitalización para aumentar su calidad aplicando técnicas de procesamiento de imágenes. Por último, se imprimirá en un PCB que se utilizará como molde para la creación de la huella artificial [33].

Este tipo de ataques han sido evaluados por el investigador Javier Galbally, quien para ello utilizó diferentes tipos de sensores de captura de huellas, concretamente los ópticos, capacitivos y térmicos. En estos estudios pudo comprobar que la eficacia del ataque se fundamenta en su mayoría en la calidad de la imagen obtenida, así como en la tecnología empleada en el sensor.

Figura 4.21: Ejemplos de imágenes de huellas de buena calidad que se utilizaron en la evaluación de los ataques directos [33]

Analizando los resultados de las pruebas que realizó llegó a la conclusión de que los sensores ópticos son los más sensibles a esta clase de ataques, puesto que el efecto de la refracción de la luz tanto en la yema del dedo, como en el material del dedo ficticio son muy parecidos. Sin embargo, los sensores térmicos, que dependen de las desigualdades de temperatura entre las crestas y los valles de las muestras que en la silicona no se perciben, son más robustos aunque no inmunes. Es por ello que, a pesar de que se aplique calor al dedo ficticio antes de situarlo en el sensor, se obtendrían unas imágenes de baja calidad. De forma similar ocurre con los sensores capacitivos en los cuales es necesario procesar previamente el dedo artificial con un material conductor para optimizar la calidad de la imagen resultante [33].

En definitiva, Galbally demostró que las condiciones de la imagen de la huella dactilar en términos de calidad de sus píxeles repercute directamente en la probabilidad de que un ataque tenga éxito.

4.7.3. Ataques indirectos Hill-Climbing

Los ataques indirectos de la categoría hill-climbing simbolizan otra seria amenaza para este tipo de sistemas, especialmente aquellos cuyo funcionamiento se basa en las técnicas de minucias. Al contrario que en los ataques directos donde se emplean datos biométricos falsos para lograr un acceso no autorizado, este tipo de ataques son mucho más complejos. Estos tienen como objetivo transformar progresivamente una serie de minucias sintéticas hasta conseguir que el sistema los reconozca como huellas dactilares válidas, permitiendo una intrusión exitosa.

El proceso de funcionamiento de este ataque comienza con la generación aleatoria de un conjunto de muestras compuestas por características sintéticas. Estas muestras iniciales se envían al sistema para poder seleccionar aquella muestra que obtenga una mayor puntuación en el algoritmo de comparación de huellas.

Según este resultado, el atacante realizará cambios adicionales en lo que respecta a su orientación o la incorporación o eliminación de pequeñas minucias. Estas modificaciones solo se almacenan en caso de que mejoren la puntuación obtenida por el sistema. El proceso se repite hasta que la estimación excede el umbral establecido o se llega al número máximo de iteraciones permitidas [33].

Las conclusiones obtenidas por Javier Galbally evidencian que la eficiencia de estos ataques se somete a diferentes factores. Estos incluyen el número de muestras iniciales originadas y el número de iteracciones que debe realizar el algoritmo, así como la región de interés (ROI), utilizada para restringir la localización de las minucias.

Se ha demostrado que el uso de un ROI, el cual identifica la región con mayor probabilidad de encontrar minucias, aumenta en gran medida la posibilidad de que un ataque tenga éxito al reducir la cantidad de iteraciones que son necesarias [33].

4.7.4. Protección frente a potenciales ataques

La correcta aplicación de contramedidas para proteger los sistemas de autenticación basados en huellas dactilares es fundamental si se desea garantizar la integridad y confidencialidad de datos o bienes. Considerando que estos sistemas son vulnerables a una gran heterogeneidad de ataques, tanto directos como indirectos, es extremadamente importante llevar a la práctica medidas preventivas eficaces con el fin de reducir lo máximo posible la probabilidad de que se produzcan violaciones de seguridad en el sistema.

Una de las principales medidas preventivas es la detección de vivacidad, cuyo propósito es diferenciar las muestras de huellas dactilares que son reales de aquellas que son adulteradas, como es el caso de los *gummy finger* usados en los ataques directos. Este protocolo se fundamenta en examinar aspectos inherentes de la piel localizada en la yema de los dedos. En particular, se estudian características como el sudor, la elasticidad o el flujo sanguíneo, las cuales no son fáciles de reproducir en una prótesis ficticia. En la investigación llevada a cabo por Galbally se ha demostrado que este método es una herramienta eficaz para prevenir ataques directos. Sin embargo, la eficacia de este tipo de contramedida depende en su mayor parte del tamaño de la base de datos que se utilice, el material de las prótesis o el tipo del sensor [33].

Otro método destacado es cuantificar las coincidencias en el sistema de verificación. Esta técnica funciona limitando la precisión de la puntuación obtenida en el proceso de comparación de huellas, lo que hace que el éxito en los ataques indirectos, como el hill-climbing, sea mucho más complejo de conseguir. De esta forma, se reduce significativamente la cantidad de información que un atacante puede obtener del sistema para modificar las plantillas que usará en la siguiente fase del algoritmo. Una consecuencia de esta medida es que se incrementa la cantidad de interacciones que se requieren para que el ataque sea fructífero [33].

Por último, se debe tener en cuenta el almacenamiento y la transmisión seguros de cualquier dato biométrico. Se recomienda que las muestras de huellas dactilares se cifren tanto cuando se almacenan en una base de datos, como cuando se transmiten para evitar que los atacantes intercepten o alteren esa información. Por otro lado, se deberán llevar a cabo auditorías periódicas con el objetivo de identificar actividades sospechosas, así como implementar tecnologías de acceso multifactor, creando nuevas capas de protección de activos.

Capítulo 5

Reconocimiento facial

La finalidad de este capítulo es proporcionar al lector una comprensión global y realista de los sistemas biométricos basados en el reconocimiento facial. Se profundizará en la evolución de este tipo de tecnología a lo largo de la historia, investigando la operatividad de estos sistemas. Asimismo, se explorarán los desafíos y los límites asociados, además de realizar un análisis en profundidad de la seguridad que brindan estos sistemas, destacando su impacto en la privacidad de los usuarios.

5.1. Introducción

El reconocimiento facial ha pasado de ser un elemento utilizado en las películas de ciencia ficción a considerarse una de las técnicas biométricas más prestigiosas de la actualidad. Desde su despliegue en dispositivos móviles, hasta su aplicación en complejos sistemas de seguridad, la capacidad que poseen de identificar a un individuo basándose únicamente en una imagen de su rostro ha transformado por completo la forma en la que se implementan los controles de acceso modernos. Es por ello que esta técnica desempeña una función fundamental en las interacciones que se realizan en el día a día en el mundo digital.

En vista de los últimos avances de la tecnología, el uso del reconocimiento facial se ha extendido a diversas áreas. En el sector de la seguridad pública, su aplicación se ha ampliado significativamente. Así lo evidencia la adopción del reconocimiento facial automático por parte de la Policía Nacional, que lo han utilizado en las investigaciones de delitos obteniendo, de este modo, un gran éxito en la identificación de delincuentes [54]. Debido a este auge, los usuarios comienzan a plantearse cuestiones primordiales en cuanto a la precisión de estos sistemas o los sesgos existentes en los algoritmos.

En otros términos, en los últimos años el impacto de esta tecnología está siendo cuestionado. ¿Las personas son realmente conscientes del alcance que tienen este tipo de sistemas y su repercusión en el futuro? Si bien es imposible negar que simplifican muchas actividades que se llevan a cabo en la vida cotidiana, ¿qué precio están dispuestos a pagar los usuarios por la privacidad de sus datos biométricos? ¿En qué medida puede esta sofisticada tecnología preservar su correcto funcionamiento?

5.2. La revolución del reconocimiento facial durante las últimas décadas

Durante los siglos XX y XXI, el reconocimiento facial ha sufrido un verdadero desarrollo, desde ser considerada un concepto experimental hasta transformarse en una herramienta esencial en el presente. Este progreso ha sido posible gracias al aumento en la capacidad de procesamiento de información, al igual que por el crecimiento que ha experimentado la inteligencia artificial. Desde su implementación en pequeños dispositivos a la integración en la seguridad ciudadana, el reconocimiento facial ha cambiado la forma de interacción entre las personas y la tecnología. Ahora bien, ¿cómo se ha logrado llegar a este punto? ¿Cuáles son los acontecimientos que han causado esta revolución? La historia de estos sistemas biométricos evidencia una trayectoria repleta de innovación, retos y una gran repercusión en la vida diaria de las personas.

5.2.1. Década de 1960: Principios innovadores

Los primeros intentos de automatizar el proceso del reconocimiento facial los realizó en 1964 Woodrow Wilson Bledsoe, un matemático e informático americano, quien fomentó el desarrollo del primer sistema que podía catalogar imágenes de rostros humanos. Esto se consiguió utilizando una tableta RAND, es decir, un dispositivo electrónico que permitía registrar las coordenadas de veinte rasgos faciales concretos como, por ejemplo, la distancia entre los ojos o las dimensiones de la boca a través de un lápiz óptico y pulsos electromagnéticos.

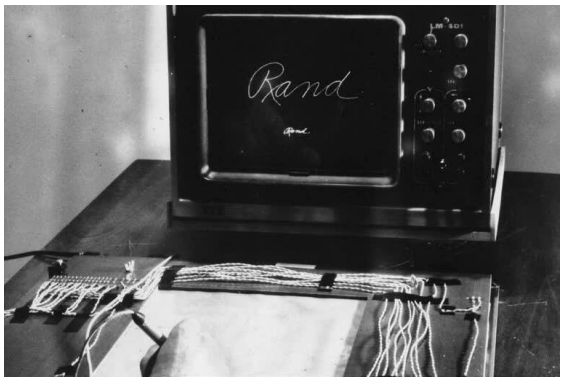

Figura 5.1: La tableta RAND en la que se probó el primer sistema de reconocimiento facial [19]

No obstante, este proyecto no tuvo mucho éxito a causa de las limitaciones tecnológicas de aquella época. Bledsoe se dio cuenta de que la complicación del reconocimiento facial residía en diferentes factores como las grandes variaciones en la rotación e inclinación de la cabeza o las expresiones faciales. Pese a ello, este descubrimiento estableció las bases para el uso próximo de esta tecnología biométrica, dando paso a un largo periodo de perfeccionamiento y progresos [38].

5.2.2. Década de 1970: Primeros avances en la automatización

Durante los años 70, el objetivo de conseguir un reconocimiento facial automático empezó a adquirir popularidad debido a los progresos alcanzados en la identificación de patrones. Científicos como Goldstein, Harmon y Lesk mejoraron el sistema original ampliando 21 nuevos marcadores tales como el color del pelo o el grosor de los labios [58].

A pesar de esta progresión, la tecnología que se empleaba no era vanguardista. Es decir, este sistema afrontaba nuevas limitaciones debido a la ausencia de una base de datos adecuada para realizar las pruebas necesarias para poder perfeccionarlo. En definitiva, este sistema de reconocimiento facial dependía excesivamente de la participación de operarios en el proceso de registro de las medidas faciales, lo que limitaba tanto su precisión como su adaptabilidad a gran escala.

5.2.3. Década de 1980: La aparición de la inteligencia artificial

Esta década afrontó avances significativos en las técnicas del reconocimiento facial impulsados por los progresos conseguidos en el ámbito del aprendizaje automático y la inteligencia artificial. Concretamente, en el año 1987, Sirovich y Kirby diseñaron un sistema capaz de codificar un rostro humano alineado con menos de cien valores. Este hallazgo instauró las bases para la aplicación del análisis de componentes principales, también denominado PCA, una técnica que permite trabajar con un conjunto de datos faciales amplio reduciendo su dimensionalidad. De esta forma, mediante el álgebra lineal se facilita la interpretación de imágenes de rostros faciales [58].

5.2.4. Década de 1990: Desarrollo del método Eigenfaces

En 1991, Alex Pentland y Matthew Turk, profesores del Instituto Tecnológico de Massachusetts, dieron a conocer el primer ejemplo exitoso de la tecnología de reconocimiento facial denominado Eigenfaces [72]. Este método, fundamentado en el PCA, revolucionó la biometría, pues utilizaba el análisis estadístico para identificar aquellos rasgos faciales más importantes, mejorando notablemente la precisión en la identificación de personas [38].

Con el propósito de seguir desarrollando esta tecnología, en el año 1998, la *Defense Advanced Research Projects Agency* (DARPA) incentivó el programa de tecnología de reconocimiento facial FERET.

Este proyecto formó una base de datos compleja con 2.400 imágenes extraídas de 850 individuos que se convirtió en la principal fuente de información para el mundo académico, así como para la industria biométrica. Esto posibilitó el desarrollo de futuros sistemas de reconocimiento facial automático, más precisos y fiables [38].

5.2.5. Década de 2000: Fomento del *Face Recognition Grand Challenge*

A principios de esta década, en 2005, se promovió el conocido *Face Recognition Grand Challenge*, un importante acontecimiento cuyo objetivo fue la expansión de nuevas tecnologías del reconocimiento facial, además de mejorar las existentes. Asimismo, este reto motivó a la comunidad científica a resolver los desafíos que enfrentaban este tipo de sistemas en esta época.

En vista de que las bases de datos de pruebas aumentaban su tamaño y heterogeneidad, los investigadores encontraron nuevas dificultades que pusieron a prueba su capacidad para garantizar su correcto funcionamiento en la vida real [38].

5.2.6. Década de 2010: El auge del reconocimiento facial

Con el avance del Deep Learning en 2011, aumentó el diseño de nuevos sistemas de reconocimiento facial. Debido a los nuevos métodos que utilizaban redes neuronales, estos sistemas comienzan a aprender de forma autónoma, optimizando su funcionamiento con cada nueva muestra añadida a las bases de datos [38].

Unos años más tarde, en 2014, la empresa Facebook publicó el algoritmo llamado DeepFace, alcanzando aproximadamente el 97 % de precisión, lo que transformó por completo este tipo de técnicas biométricas. Este logro permitió a la red social reconocer rostros de forma eficaz en su plataforma [38].

Otro de los grandes hitos se produjo en el año 2017 con el lanzamiento del iPhone X por parte de Apple, convirtiéndose en el primer dispositivo móvil de la compañía que utilizaba de forma segura la tecnología de reconocimiento facial llamada FaceID. Este hecho no solo promulgó el uso de esta técnica en pequeños dispositivos, sino que, además, lo puso a disposición de millones de personas a nivel mundial, lo que marcó el inicio de su uso universalizado.

5.3. Dificultades en el reconocimiento facial automático

El método biométrico basado en el reconocimiento facial de forma automática, si bien se ha ido investigando en el transcurso de estos últimos 50 años, continúa haciendo frente a diferentes problemas que restringen su efectividad y precisión. Uno de los mayores desafíos que deben enfrentar estos sistemas en la actualidad es la denominada «maldición de la dimensionalidad» que hace referencia a la gran cantidad de imágenes para entrenar al algoritmo de comparación necesarias para categorizar un rostro con una gran granularidad. No obstante, esto no es lo único que obstaculiza que el proceso del reconocimiento tenga éxito [24].

Es bien conocido que el rostro humano no es rígido por lo que su apariencia y forma pueden sufrir variaciones bajo la influencia de distintos factores tanto intrínsecos como extrínsecos. Se considera que los factores intrínsecos son aquellos que están relacionados con la naturaleza física de la cara. Es decir, comprenden desemejanzas entre diferentes individuos como, por ejemplo, el sexo o la etnia, o entre la misma persona como la edad, expresiones faciales o el uso de complementos como gafas. Por otro lado, los factores extrínsecos como la iluminación de la estancia, el ángulo de captura de la cámara o la resolución de la imagen desempeñan un papel fundamental en la apariencia de un rostro [24].

Está demostrado que estos aspectos influyen negativamente en el correcto rendimiento de los sistemas de reconocimiento facial. Fundamentalmente, se han determinado cuatro factores que deberán ser abordados en cualquier técnica de reconocimiento de rostros [24]:

- Algunas de las técnicas en 2D propuestas solo cuando hay cambios moderados en la iluminación, mientras que su rendimiento se reduce significativamente cuando hay grandes alteraciones en las condiciones lumínicas.
- Las alteraciones en la postura, como por ejemplo la rotación de la cabeza, también influyen en el reconocimiento facial debido a que introducen distorsiones en la imagen adquirida. Este problema se vuelve aún más grave cuando los dispositivos de captura modifican el ángulo más allá del rango de visión para el que está diseñado el sistema.
- En ocasiones, incluso cuando se captura la imagen del rostro desde la perspectiva correcta, cualquier cambio exagerado en la expresión facial pueden provocar que se produzca una identificación errónea.
- La última dificultad tiene que ver con las transformaciones faciales que se producen con el paso del tiempo, ya que estos cambios no se ocasionan de forma lineal. Por este motivo, esta cuestión es mucho más difícil de afrontar en el diseño de un algoritmo.

En conclusión, estos desafíos reflejan las limitaciones técnicas, así como prácticas que enfrenta el reconocimiento facial en situaciones del mundo real, donde las variaciones en las condiciones dificultan desarrollar una implementación de esta tecnología precisa y confiable.

5.4. El rostro como identidad biométrica

En el ámbito de la biometría se ha demostrado que cada tecnología presenta sus propias limitaciones ya sea en los sensores o en el algoritmo de comparación. Así lo demuestra el reconocimiento del iris, una técnica realmente precisa, pero sin aceptación a nivel mundial a causa de los últimos acontecimientos con empresas mundialmente conocidas. Asimismo, los métodos basados en huellas dactilares, si bien son confiables, no se consideran adecuados en aquellos entornos donde el usuario prefiere no interactuar directamente con el sistema. Ante tales circunstancias, el reconocimiento facial se ha convertido en una solución ecuánime que ofrece una perfecta combinación entre fiabilidad y sencillez de uso [24].

Desde un punto de vista cognitivo, el rostro es una de las características biométricas más utilizadas por las personas para identificar a los demás. De hecho, el reconocimiento facial es una habilidad que se estimula a partir de los pocos meses de nacimiento. Por este motivo, los sistemas biométricos de este tipo pretenden reproducir este proceso natural fundamentándose en atributos físicos como la forma de los ojos y las cejas o la boca [24].

A pesar de que esta actividad puede parecer sencilla para los seres humanos, resulta un procedimiento complicado para un sistema informático. Detectar y reconocer rostros en una imagen arbitraria implica determinar la presencia de una cara para, posteriormente, poder identificar al individuo a la que pertenece.

Con el propósito de lograr este objetivo, científicos de diversos campos como la psicología y la informática han estado años trabajando conjuntamente para recrear la capacidad humana de reconocer rostros utilizando sistemas automáticos de reconocimiento facial.

5.4.1. Psicología cognitiva del reconocimiento facial

Identificar rostros humanos es un proceso complejo que implica el uso de diversas regiones del cerebro. Por esa razón, el reconocimiento facial se considera un área esencial de investigación en el ámbito de la psicología cognitiva, ciencia cuyo núcleo de estudio son estos mismos procesos mentales que integran la habilidad fundamental de interacción social. Así, comprenderlos en profundidad es imprescindible para diseñar sistemas precisos basados en esta característica biométrica.

Durante décadas se ha estudiado cómo el cerebro procesa las caras, determinando finalmente que es una red cortical de la vía ventral visual la que se encarga del procesamiento facial [14]. Adicionalmente, se ha concluido que este tipo de reconocimiento presenta una naturaleza jerárquica que inicia con la identificación de rasgos faciales elementales y termina con un reconocimiento de aquellas características faciales propias de cada individuo. Esta última fase se conoce como procesamiento holístico.

Desde el punto de vista del crecimiento de una persona, los infantes en un principio efectúan un procesamiento featural, centrándose en partes representativas de la cara como la boca o los ojos. No obstante, al mismo tiempo que el individuo crece va aprendiendo a realizar un procesamiento configural de los rasgos faciales, en otros términos, se comienza a apreciar las relaciones espaciales entre diferentes elementos de la cara. Por último, en la edad adulta, el cerebro comienza a funcionar de forma integral percibiendo el rostro como un conjunto [24].

Por otro lado, en el área de la neurofisiología se ha demostrado que el reconocimiento facial, así como la percepción de las expresiones emocionales son procesadas por diferentes sistemas neurofisiológicos. Este hecho permite a una persona hacer una distinción independiente entre quién es un individuo, es decir su identidad facial, y qué es lo que siente en un momento determinado. Esto significa que teóricamente se puede identificar a una persona sin tener en consideración sus emociones, y viceversa [24].

Esta separación de funciones ha supuesto importantes repercusiones en lo que respecta a la computación. Por lo tanto, como consecuencia de este hallazgo, se ha desarrollado un método a través del cual una aplicación tiene la capacidad de determinar un reconocimiento de identidad sin requerir un análisis previo de las expresiones emocionales. Sin embargo, pese a esta disociación, los estudios muestran que subsiste un conjunto de neuronas que sugieren cierta interacción entre ambos procesos [24].

En definitiva, los resultados expuestos no solo mejoran el conocimiento acerca del reconocimiento de rostros, sino que también proporcionan una base sólida para perfeccionar los sistemas de reconocimiento facial automático en función de cómo nuestros cerebros realizan estas funciones cognitivas.

5.4.2. Clasificación de los rasgos faciales

El proceso mediante el cual se reconoce un rostro humano se fundamenta en la interpretación de un conjunto de diferentes rasgos faciales que se pueden categorizar según su nivel de detalle en diferentes grupos de forma similar que en el caso de las huellas dactilares. Estos comprenden desde características generales hasta los pequeños detalles, permitiendo así una identificación precisa de una persona entre una multitud [42].

Nivel 1: Características generales

Los rasgos categorizados en este nivel incluyen todas aquellas características que son sencillamente reconocibles. Estos abarcan elementos de la forma geométrica de la cara, el color de la piel o características demográficas como el sexo o el origen étnico. Este primer grupo posibilita realizar diferenciaciones rápidas como distinguir entre un rostro femenino o masculino. Otro claro ejemplo es la diferencia existente entre un rostro redondo y corto y otro que pueda ser largo y delgado. Tal es su recognoscibilidad que este tipo de rasgos se pueden extraer fácilmente incluso en imágenes con una resolución baja.

Nivel 2: Características concretas

Este tipo de rasgos físicos engloban componentes estructurales del rostro, centrándose en atributos representativos como los ojos, la nariz o la boca, además de sus proporciones y sus relaciones espaciales. Este nivel es clave para llevar a cabo un reconocimiento facial preciso, pues se basa en una evaluación detallada de la morfología del rostro. Para poder captar estos detalles es necesario que el sistema sea capaz de obtener imágenes con una resolución mayor con el fin de determinar correctamente la ubicación de estos elementos. En el diseño de un sistema de reconocimiento biométrico, estos rasgos distintivos se representan a través de descriptores geométricos.

Nivel 3: Microdetalles de la piel

Los detalles clasificados en este nivel integran características no estructuradas y únicas localizadas en la superficie de la piel, como pueden ser cicatrices, pecas o lunares, así como alguna alteración en la coloración de la piel. Este tipo de rasgos son sustanciales en los casos en los que las características globales y locales son consideradas insuficientes para distinguir dos personas con rasgos físicos semejantes, como podría suceder con gemelos idénticos. Este último nivel ha permitido que la tecnología del reconocimiento facial se imponga sobre los límites de los dos primeros niveles, garantizando una mayor rigurosidad en la identificación del individuo.

En resumen, el reconocimiento facial es un proceso complejo que requiere realizar un análisis tomando en consideración diversos niveles de peculiaridades. Esta clasificación ha posibilitado que estos sistemas identifiquen con exactitud a sujetos con rasgos comunes, con atributos prácticamente iguales o con características singulares. Al unificar esta jerarquía de información biométrica es posible optimizar los sistemas de reconocimiento facial para adecuarlos a una gran variedad de aplicaciones.

5.5. Evolución tecnológica en la captura de rostros

El reconocimiento facial se constituye como uno de los métodos biométricos más sofisticados, cuya efectividad radica en gran parte en las condiciones de la tecnología utilizada para capturar las imágenes del rostro. Un aspecto fundamental en la evolución de estos sistemas de identificación ha sido la asequibilidad de cámaras compactas de alta resolución, ideales para ser incorporadas en una amplia gama de dispositivos. En la última década, la tecnología detrás de las cámaras digitales ha experimentado un importante desarrollo en términos de densidad de píxeles o de velocidad de obturación. En la actualidad, se ha logrado diseñar sensores con un tamaño reducido y económicos, lo que permite que incluso los dispositivos móviles logren realizar fotografías con una resolución alta.

Este tipo de cámaras proporcionan un extenso abanico de diversas calidades de imagen que están influenciadas por diferentes factores tecnológicos. Estos incluyen la utilización en el proceso de identificación de una imagen estática o, en su defecto, de un vídeo. Avanzando en el estudio, se van a analizar los tipos de sensores empleados en la captura de imágenes conjuntamente con su impacto en el reconocimiento facial.

5.5.1. Sensores 2D: La base del reconocimiento facial tradicional

Típicamente, la operatividad de este tipo de sistemas biométricos se basaba en cámaras que captaban imágenes bidimensionales, también denominadas imágenes estáticas. Estos sensores se establecieron como el modelo referente de sistemas de reconocimiento facial. Se utilizaban con el objetivo de realizar fotografías desde una perspectiva frontal, lo que permitía analizar la morfología del rostro para identificar al individuo [42].

No obstante, aquellos sistemas biométricos que emplean un sensor 2D están expuestos a una serie de importantes límites. Los cambios en la luminosidad de la estancia, al igual que la perspectiva en la orientación de la cámara pueden influenciar significativamente la resolución de las imágenes capturadas, repercutiendo en la exactitud del proceso de identificación. Asimismo, cabe destacar que, debido a que los rostros son una figura tridimensional, estos sensores no tienen la capacidad de reflejar todas las características faciales, por lo que ciertos rasgos quedan ocultos en función del ángulo utilizado en el proceso. Con el propósito de resolver este último inconveniente, se suelen utilizar varias cámaras para capturar el rostro desde diferentes ángulos, minimizando así las complicaciones relacionadas con el posicionamiento de la cara [42].

Por otro lado, para afrontar las otras dificultades mencionadas, en especial la variación en la condición lumínica, se han diseñado otro tipo de dispositivos denominados cámaras de infrarrojo cercano o cámaras NIR por sus siglas en inglés. Al utilizar una luz infrarroja invisible para el ojo humano, estos sensores posibilitan captar imágenes en situaciones caracterizadas por una escasa luminiscencia o, incluso, de noche [42]. Un ejemplo del funcionamiento de este tipo de cámaras se puede observar en la Figura 5.2.

Figura 5.2: Imágenes faciales capturadas con una cámara NIR en diferentes longitudes de onda [42]

En contraste con esta evolución tecnológica, los sistemas de reconocimiento facial con sensores 2D disponen de un alcance operativo limitado, aproximadamente de uno a dos metros. En contextos en los que la persona está situada a una distancia mayor, la calidad de la imagen adquirida se reduce considerablemente, lo que podría provocar errores en el proceso de reconocimiento. Para solucionar este impedimento se han adoptado dos estrategias: utilizar métodos de alta resolución y el uso de cámaras PTZ. Este tipo de cámaras, conocidas por sus siglas como Panorámica, Inclinación y Zoom, tienen la capacidad de acercar o alejar la imagen de forma dinámica con el objetivo de ajustar la distancia al sensor para obtener la mejor resolución posible. Sin embargo, el campo de visión se disminuye significativamente si se aumenta demasiado el zoom. En otras palabras, para optimizar el proceso de reconocimiento se desarrolló un sistema que utiliza conjuntamente una cámara estática que proporciona una visión más amplia del escenario, junto con una cámara PTZ que se encarga de capturar imágenes de alta calidad de los individuos de interés [42].

5.5.2. Sensores 3D: Captura de imágenes más precisa

Los sensores tridimensionales han supuesto un gran progreso tecnológico en el reconocimiento facial, imponiéndose a las restricciones de los sensores 2D, principalmente en lo referente a las diferencias de posición, expresiones faciales o condiciones lumínicas. Todos estos obstáculos se derivan de la ocultación de rasgos característicos de la cara, considerados esenciales en la identificación de sujetos. Por este motivo, se impulsó el desarrollo de sensores más sofisticados capaces de proporcionar imágenes faciales mucho más completas y detalladas [42].

En la actualidad, se han diseñado dos importantes sistemas de reconocimiento facial en 3D. Por un lado, los escáneres láser tienen una gran reputación debido a su precisión en la adquisición de imágenes, pues crean un modelo tridimensional idéntico de la cara, denominado escaneo 2.5D, que captura la cabeza en un ángulo de aproximadamente 120º. En consecuencia, para obtener un modelo facial completo se deben combinar entre tres y cinco sensores ubicados en diferentes perspectivas. Este tipo de sistemas suelen tener una estructura poligonal para optimizar el proceso de la captura de la imagen. A pesar de que los cambios de posición pueden afectar al modelo 3D obtenido, se considera que estas alteraciones son mínimas, por lo que no generan apenas impacto en el resultado del reconocimiento [42].

Figura 5.3: Modelo 3D de un rostro humano real [60]

Las cámaras estereográficas, por otro lado, posibilitan la adquisición de imágenes en tiempo real, pero se produce una ligera pérdida en términos de precisión en comparación con los escáneres láser. Sin embargo, al contrario de lo que ocurría con los sensores anteriores, estos se han convertido en sistemas mucho más resistentes a las alteraciones en la luz o perspectiva. Es por ello que estos sistemas son perfectos para aquellos entornos donde se necesita una exactitud alta [42].

Es importante señalar que, pese a lo expuesto anteriormente, los sistemas basados en sensores 3D no están exentos de dificultades en su implementación. La captura de imágenes en tres dimensiones exige más tiempo, además de originar ficheros de gran volumen, lo que aumenta el requisito de disponer de mejores recursos de procesamiento y almacenamiento. Otra desventaja asociada a este tipo de tecnología es el alto coste de los sensores de imágenes 3D, que puede ser un impedimento para su adopción en diferentes aplicaciones a nivel mundial.

5.5.3. Secuencias de vídeo: Innovación en el reconocimiento facial dinámico

Los sistemas cuyo funcionamiento consiste en el análisis de secuencias de vídeo se presentan como una nueva opción de identificación facial dinámica al poder capturar imágenes de objetos en movimiento en tiempo real. Este tipo de cámaras son capaces de obtener múltiples imágenes por segundo, siendo este un método que ha generado gran interés principalmente en las ya habituales cámaras de vigilancia, donde el reconocimiento facial automático es clave para identificar personas en tiempo real [42].

Una gran ventaja de los sistemas de vídeo es la habilidad de escoger el fotograma idóneo de un individuo entre miles de imágenes y así permitir seleccionar solo aquellas imágenes que tengan una resolución alta, por ejemplo, con una postura lo más frontal posible. Esta característica es importante en aquellas situaciones donde la persona no siempre está situada enfrente de la cámara.

Por otra parte, se debe agregar que el hecho de que el coste de los sensores de secuencias de vídeo sea cada vez menor ha hecho posible que esta tecnología sea más asequible, además de rentable en una gran pluralidad de aplicaciones [42].

A pesar de las ventajas mencionadas, las cámaras de vídeo generan imágenes con una calidad menor comparada con los sensores 2D estáticos dado que tienen que procesar un gran conjunto de datos transmitidos desde el sensor al dispositivo de procesamiento. En estos casos, es habitual utilizar técnicas de comprensión de vídeo, lo que puede provocar una reducción en la calidad de la imagen adquirida influenciando el resultado del reconocimiento. No obstante, los sistemas de vídeo siguen siendo fundamentales, primordialmente en aquellas circunstancias en las que se requiere realizar un seguimiento continuo de una persona en concreto [42].

5.6. Reconocimiento facial a partir de imágenes en 2D

La tecnología de reconocimiento facial basada en imágenes en 2D ha emergido como una de las innovaciones biométricas más exploradas en los últimos años. Esta técnica, que se centra en la captura de imágenes bidimensionales, ha dado pie a la creación de soluciones de reconocimiento altamente efectivas en diversas áreas. Desde la protección de dispositivos móviles hasta la vigilancia en lugares públicos, su versatilidad es innegable. Además, brinda a los usuarios un equilibrio entre velocidad y exactitud, todo ello sin la necesidad de invertir mucho dinero para poder usarla. Sin embargo, a pesar de la evolución vertiginosa de las tecnologías 3D y la creciente búsqueda de soluciones más exactas, el reconocimiento facial en 2D continúa destacándose como una poderosa herramienta.

5.6.1. Métodos utilizados en la detección de rostros

La localización de rostros es el punto de partida del proceso de reconocimiento facial dado que implica reconocer la existencia de una cara, ya sea en una imagen estática o en un vídeo, para su posterior evaluación. Con este procedimiento se pretende aislar la región donde se encuentra el rostro de la persona eliminando el fondo o cualquier otro elemento que pueda dificultar el reconocimiento. Esta etapa es muy relevante, puesto que un error supondrá un impacto directo en el rendimiento del sistema. La ausencia de una detección exacta ocasionaría que la identificación biométrica no se considere confiable. Por esta razón, es esencial comprender cómo funcionan este tipo de técnicas.

5.6.1.1. Algoritmo Viola-Jones

El algoritmo de detección de rostros propuesto por Paul Viola y Michael Jones, célebre por su idoneidad para funcionar en tiempo real de forma rigurosa y con exactitud, es una de las técnicas fundamentales en el reconocimiento facial. Este planteamiento fue el precursor en el ámbito de la detección de objetos, implicando su uso en el procesamiento de imágenes faciales a causa de sus eficientes implementaciones disponibles en librerías como OpenCV.

El proceso da comienzo con la realización de una inspección de la imagen obtenida por el sistema, fragmentándola en las denominadas ventanas de detección de diversos tamaños. En cada una de ellas, este algoritmo concluye la existencia de una cara utilizando un conjunto de clasificadores. Estos se basan en los filtros Haar que posibilitan captar los cambios de intensidad entre las distintas regiones del rostro [42].

Los filtros Haar son formas rectangulares que seccionan la imagen en áreas oscuras y claras. Estos filtros pueden combinarse en diferentes tamaños como se puede observar en la Figura 5.4. El objetivo de este algoritmo es determinar la diferencia entre la suma de las intensidades de los píxeles de ambas regiones para poder identificar rasgos faciales. Así, por ejemplo, en el

caso de un rostro humano, se puede utilizar un filtro con tres campos para detectar tanto los ojos como la nariz. Esto es porque los ojos tienden a ser más oscuros que la nariz y el uso de este tipo de filtro ayuda a resaltar estas diferencias. No obstante, aplicar un único filtro no es idóneo para detectar rostros con precisión, de modo que este algoritmo utiliza un conjunto de filtros de diferentes tamaños en cada ventana de detección [42].

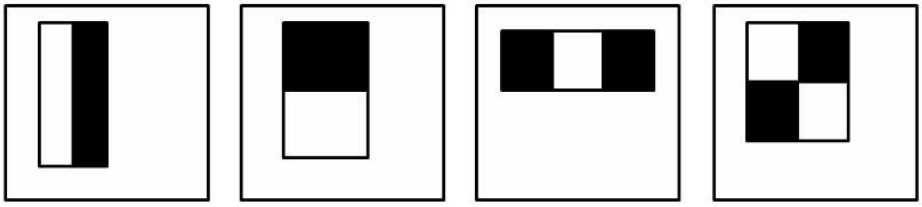

Figura 5.4: Tipos de filtros Haar utilizados en la detección de rostros [42]

A fin de optimizar este procedimiento y disminuir el coste computacional, se emplea un procesado de datos en cascada. En la etapa inicial, el algoritmo utiliza un subgrupo de filtros para eliminar rápidamente aquellas regiones de la imagen que no engloban una cara, agilizando así el proceso de detección. En la medida en que se avanza en el desarrollo de los estadios, se aplican filtros y clasificadores más potentes para confirmar la existencia de un rostro en la imagen [42].

El algoritmo Viola-Jones usa dos de los filtros Haar más eficientes, los cuales se pueden ver en la Figura 5.5, para prescindir de alrededor del 60 % de las zonas que no presentan rostros. El primer filtro enfatiza que habitualmente la zona de los ojos es más oscura que las mejillas. Por otro lado, el segundo filtro destaca el contraste entre el puente de la nariz, que suele ser más brillante, y el área de los ojos, que se caracteriza por ser más oscura [42]. Estos patrones simples, pero eficaces ayudan al algoritmo a identificar rápidamente rostros, lo que reduce significativamente los falsos positivos antes de aplicar filtros más complejos.

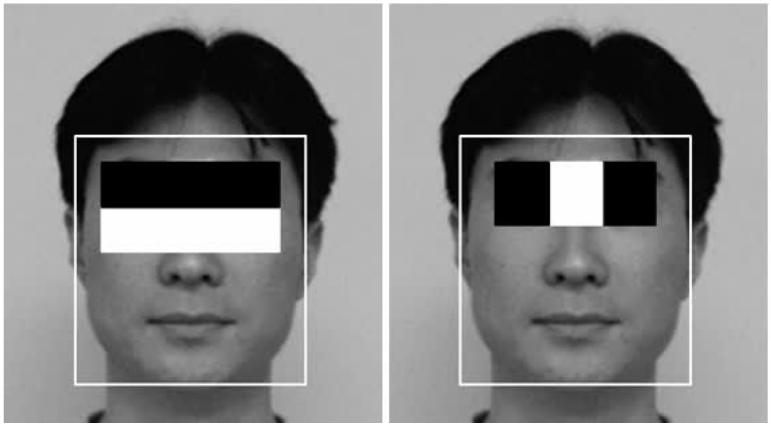

Figura 5.5: Las dos características más discriminativas de tipo Haar superpuestas en una imagen real capturada por un sistema de reconocimiento facial [42]

5.6.1.2. Métodos basados en características faciales

Las técnicas fundamentadas en características tienen como objetivo reconocer rasgos faciales propios de las personas, para luego determinar la presencia de una cara en la imagen. En función de estos rasgos, se desarrollan modelos estadísticos para describir la relación existente entre ellos que permitirán corroborar la existencia de un rostro. Si bien estos métodos son útiles, pueden ser influenciados por la luz o la oclusión, reduciendo así la calidad de las características extraídas. Actualmente, se han propuesto diferentes planteamientos. Estos se detallarán a continuación.

5.6.1.2.1. Análisis realizado a bajo nivel

Este tipo de estudio es uno de los enfoques más elementales. Consiste en utilizar las diferentes propiedades específicas de los píxeles, como, por ejemplo, la información sobre el color. Se trata de una técnica que no es compleja debido a que hace uso directamente de la información contenida en la imagen, lo que lo convierte en un método rápido y eficaz para identificar rostros. Sin embargo, en vista del análisis llevado a cabo a bajo nivel, las características extraídas pueden ser ambiguas.

Bordes

La utilización de bordes en la localización surge de las primeras investigaciones en este campo de la biometría. Estos bordes permiten trazar aquellas partes importantes de un rostro. Cabe destacar que este enfoque se ha ido perfeccionando con el transcurso del tiempo hasta llegar a utilizar operadores matemáticos como Sobel o Marr-Hildreth para delimitar los cambios de intensidad en la imagen. En esta aproximación, los bordes deben estar etiquetados y emparejados con un modelo de la cara para garantizar que las detecciones sean correctas [24].

Escala de grises

Los distintos tonos de grises ofrecen un método eficaz para detectar rasgos faciales. Comúnmente, las características faciales como las cejas, las pupilas de los ojos o los labios son más oscuras que el resto de la zona facial, y este hecho es lo que los hace más fáciles de identificar. Es importante señalar que el procesamiento de las imágenes capturadas por el sistema por medio de operaciones de contraste favorece la detección de estas áreas [24].

Información sobre el color

A diferencia de la escala de grises, el análisis del color es una poderosa herramienta para la detección facial. En esta estrategia, se utilizan diversos modelos de color como RGB o YIQ para desacoplar la piel del fondo de la imagen. Adicionalmente, la tonalidad de la piel constituye un grupo compacto en el espacio cromático, lo que la hace bastante uniforme entre las personas, inclusive cuando se tienen en cuenta las diferentes razas.

Por consiguiente, este criterio es resistente a cambios en la luz y los sensores, de modo que este proceso es óptimo cuando las condiciones son adversas [24].

Movimiento

En los casos en los que el sistema utilice secuencias de vídeo, la evaluación del movimiento es valiosa para detectar caras. Métodos como valorar la diferencia existente entre fotogramas de un mismo vídeo pueden desacoplar el rostro que esté moviéndose de los fondos estáticos [24].

5.6.1.2.2. Modelos de formas activas

Los modelos de formas activas se conforman como una herramienta que posibilita la extracción de las singularidades faciales. En contraposición a otros métodos, estos reproducen el aspecto físico de una persona de forma realista. Es decir, estos modelos se adaptan de manera flexible a las particularidades que presenta una imagen, como son las variaciones en el brillo, moldeándose progresivamente para representar con precisión las características del rostro. En los últimos años, se han desarrollado tres clases de modelos de formas activas utilizados en la extracción de rasgos faciales [24].

En primer lugar, los contornos dinámicos, también conocidos en inglés como *snakes*, se aplican generalmente con el propósito de localizar los límites de la cabeza. Sin embargo, pueden encontrar ciertos desafíos al intentar inferir detalles más complejos. Para resolver estas restricciones se diseñaron los modelos deformables avanzados que incorporan puntos de control para asegurar la armonía en la silueta del rostro. Por otro lado, en aquellas situaciones que son más particulares, como es el caso de los ojos, se usan plantillas deformables que garantizan obtener un ajuste más preciso. A pesar de ello, su implementación es más compleja [24].

5.6.2. Técnicas de reconocimiento facial

El reconocimiento biométrico ha emergido como una de las técnicas biométricas más revolucionarias de los últimos años. Tras ella, se ocultan sofisticados algoritmos junto con métodos matemáticos que hacen posible reconocer rostros con gran precisión. Con la finalidad de entender su extraordinario potencial, al igual que los retos que debe hacer frente, es fundamental explorar los diversos métodos que se han utilizado con el paso del tiempo.

Esta sección del capítulo se adentrará en un análisis detallado de los métodos más destacados en el proceso del reconocimiento facial, organizándolos en diferentes categorías clave. Se profundizará en los principios teóricos que sustentan cada una de ellas, además de enfatizar en qué forma estas metodologías han potenciado la exactitud y rapidez en la identificación de un individuo en diversos contextos de aplicación.

Al explorar en detalle cada técnica, se revelará cómo los progresos en campos como el análisis de imágenes o el aprendizaje automático han abierto nuevas puertas, superando así las barreras que en el pasado obstaculizaban el reconocimiento facial. Debido al constante avance de la tecnología, es crucial considerar los dilemas éticos, así como las preocupaciones de los usuarios acerca de su privacidad que pueden surgir a raíz de su adopción.

En resumen, este estudio brindará al lector una visión clara no solo de las técnicas de reconocimiento facial, sino también de las repercusiones que ya están generando y lo continuarán haciendo en nuestra sociedad, abriendo un nuevo camino para innovaciones futuras.

5.6.2.1. Métodos holísticos basados en la apariencia

Estas metodologías basadas en la apariencia convierten el reconocimiento facial en una cuestión de análisis de espacio, permitiendo la aplicación de diversas técnicas estadísticas para abordar esta evaluación de manera innovadora. Entre las diversas técnicas, resalta su idoneidad para operar con imágenes de baja resolución. Además, se caracteriza por su rápida implementación, lo que permite su integración en sistemas en tiempo real.

No obstante, presentan una serie de desafíos a considerar. Una dificultad a tener en cuenta es que, para obtener resultados óptimos, es necesario contar con un número significativo de muestras durante la etapa de entrenamiento. Asimismo, elementos como la variación en la iluminación, la postura adoptada y la expresión facial juegan un papel fundamental en el resultado final. Según el enfoque utilizado, la magnitud de estos inconvenientes puede variar significativamente.

5.6.2.1.1. Análisis de componentes principales. Eigenfaces

La innovadora técnica de Eigenfaces, fundamentada en el análisis de componentes principales, también conocida por sus siglas en inglés como PCA, ha dejado una huella indeleble en el campo del reconocimiento facial y se ha convertido en una de las estrategias más destacadas y transformadoras. Este enfoque revela un subespacio lineal que transforma las complejas imágenes faciales, compuestas por millones de píxeles, en un espacio de características más reducido siendo más fácil de manejar [41].

El proceso se inicia al calcular la matriz de la covarianza utilizando una colección de imágenes de entrenamiento. Este análisis da origen a una serie de vectores propios, conocidos como *eigenfaces*, que constituyen las direcciones esenciales de variación presentes en esos datos. En este método, las caras se describen a través de vectores de características, aunque no se basan en las formas comunes como los ojos o la boca. Al proyectar las imágenes de los rostros en este particular subespacio de características, se generan vectores que permiten no solo clasificar, sino también equiparar las caras utilizando diversas métricas de distancia [24].

Un elemento clave de este método es que los primeros componentes principales representan una cantidad notable de varianza, lo que les otorga una gran relevancia en el análisis. Por poner un ejemplo, los tres primeros *eigenvectores* tienen la capacidad de captar más del 75 % de la variabilidad presente en los datos de entrenamiento. Esto implica que al proyectar la información en este espacio de dimensiones reducidas se preserva la mayor parte de la información valiosa necesaria para el reconocimiento facial. Esta característica dota al sistema de la capacidad de identificar rostros bajo diversas condiciones de luz y con distintas expresiones, garantizando una identificación precisa y confiable. No obstante, al incrementar la cantidad de *eigenvectores* empleados, la exactitud del reconocimiento se eleva, dado que se logra captar una mayor cantidad de rasgos faciales significativos [24].

En resumen, esta técnica ha marcado un hito fundamental en el análisis de rostros, ofreciendo un razonamiento matemático robusto que permite simplificar la complejidad de los datos y potenciar el proceso de identificación facial. No obstante, su susceptibilidad a los cambios en la iluminación, así como a las distintas expresiones y posturas, puede impactar de manera notable la exactitud del reconocimiento. Asimismo, al centrarse en maximizar la varianza total, no asegura una diferenciación efectiva entre los diversos tipos de rostros. Por otra parte, su desempeño está ligado a la diversidad del conjunto de imágenes de entrenamiento. Estas limitaciones han sido el motor que ha impulsado la creación de enfoques adicionales, diseñados para enfrentar estos retos de una manera más precisa.

5.6.2.1.2. Análisis discriminante lineal. Fisherfaces

El análisis discriminante lineal (siendo LDA sus siglas en inglés), al contrario que otros enfoques como el PCA que priorizan la maximización de la varianza total de los datos, se orienta hacia la separación de clases. Su objetivo es determinar la relación más efectiva entre la variabilidad entre las diferentes clases y aquella que se encuentra dentro de cada clase, logrando así una diferenciación óptima. La habilidad de esta técnica para destacar las distinciones entre diferentes conjuntos de datos la convierte en una herramienta ideal para el reconocimiento facial [24].

A pesar de ello, cuando se intenta utilizar el método LDA en el análisis de imágenes faciales aparece un obstáculo recurrente: la cantidad de imágenes que se emplean en el entrenamiento suele ser inferior al número de píxeles que componen cada imagen. Esta discrepancia da lugar a que la matriz de dispersión intraclase resulte singular, lo que complica la implementación directa de LDA. Para superar esta restricción, se emplea una fusión entre los métodos PCA y LDA. En primer lugar, se utiliza el análisis de componentes principales para simplificar la complejidad de los datos y evitar el dilema de la singularidad. Posteriormente, se lleva a cabo el análisis discriminante lineal en este nuevo subespacio reducido. Este enfoque combinado ha probado una notable mejora en los resultados del reconocimiento facial, superando las capacidades del PCA utilizado de forma independiente [41].

Uno de los progresos más destacados es la implementación de Fisherfaces, un método que, en contraste con Eigenfaces, se enfoca en localizar un subespacio lineal concreto para cada clase.

A través del algoritmo LDA se logra un equilibrio perfecto, ya que maximiza la dispersión entre distintas clases de rostros, mientras que a la vez minimiza la variabilidad dentro de cada clase. Este hecho lo posiciona como una alternativa destacada frente a Eigenfaces, especialmente en situaciones donde se presentan cambios significativos en la iluminación y en las expresiones faciales [24]. En esencia, esta combinación potencia la exactitud en el reconocimiento, particularmente en contextos donde las características distintivas de cada clase son fundamentales. Este enfoque garantiza que los rostros de un mismo grupo se reúnan con gran cercanía, mientras que se logra una separación nítida entre las diferentes clases, facilitando así una identificación efectiva.

5.6.2.2. Métodos analíticos basados en modelos

Los métodos analíticos fundamentados en modelos constituyen una estrategia avanzada en el ámbito del reconocimiento facial. Estos enfoques se centran en comprender la compleja estructura junto con la dinámica de los rostros humanos, utilizando procedimientos matemáticos y geométricos. En concreto, estas metodologías extraen rasgos biométricos únicos de las imágenes, analizando detalles como la separación ocular, la amplitud nasal y las dimensiones de la boca con el fin de llevar a cabo un adecuado reconocimiento. A diferencia de los enfoques que se focalizan en la apariencia, estos exigen un entendimiento más profundo de las imágenes, lo que, a su vez, los convierte en procesos más lentos y complejos. Sin embargo, su notable resistencia a los cambios en la orientación, las expresiones faciales y las fluctuaciones en las condiciones de luz los hace una alternativa más confiable en entornos complejos y en constante movimiento.

5.6.2.2.1. Correspondencia entre agrupaciones de grafos elásticos

El método denominado en inglés *Elastic Bunch Graph Matching* se fundamenta en la creación de un esquema de conexiones que utiliza grafos para capturar la esencia de cada rostro. Estos grafos, en su estructura dinámica, reflejan los rasgos únicos de cada individuo, permitiendo así una representación detallada de las características faciales. Además, se configuran como una red geométrica que enlaza nodos posicionados en lugares distintivos y emblemáticos del rostro, tales como los ojos, las comisuras de los labios y otros puntos esenciales que definen la expresión facial. Como se puede apreciar en la Figura 5.6, estos nodos se entrelazan por medio de aristas que trazan las conexiones geométricas entre las diversas características del rostro [41].

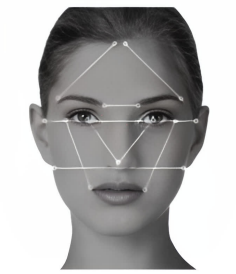

Figura 5.6: Grafo utilizado en el método EBGM [56]

Se usan coeficientes de onda de Gabor para capturar las características locales de cada nodo. Estos se encargan de codificar la información a través de una variedad de orientaciones y frecuencias, ofreciendo una representación detallada. Así, se pueden obtener matices locales que resultan sustanciales para diferenciar entre los diversos rostros. La fortaleza de este método reside en su versatilidad que permite abordar las variaciones geométricas presentes en las imágenes faciales. Gracias a ello, es posible modificar la estructura del grafo con el fin de adaptarse a las distintas expresiones y posiciones relativas de los puntos clave de la cara en cada momento [41].

Durante el reconocimiento, la imagen capturada por el sistema se transforma en un grafo que se contrasta con los que están almacenados. La semejanza entre estos grafos establece el grado de correspondencia, mientras que la opción más precisa señala la identidad de la persona.

Esta metodología fusiona datos locales minuciosos con una visión global de las interacciones geométricas entre las características faciales creando, de esta manera, un método sólido y adaptable a diversas situaciones [41].

5.7. Reconocimiento facial a partir de imágenes 3D

En las últimas dos décadas, la tecnología del reconocimiento facial basado en imágenes 3D ha surgido como una opción más precisa y, por lo tanto, más confiable, superando así a los métodos convencionales cimentados en imágenes bidimensionales. Numerosos estudios han puesto de relieve la impactante capacidad de los sistemas 3D para adaptarse a cambios en la postura y la iluminación, demostrando su versatilidad y eficacia en entornos dinámicos. Este hecho quedó claro tras las conclusiones obtenidas por parte del Face Recognition Vendor Test de 2002, que puso de manifiesto las carencias de las técnicas bidimensionales. No obstante, en aquel instante, los métodos en 3D aún carecían de una validación sólida, lo que se debía a la escasez de bases de datos accesibles. Por este motivo, con el propósito de impulsar la investigación, en 2006 el National Institute of Standards and Technology dio un gran paso al presentar el *Face Recognition Grand Challenge*. Esta iniciativa incorporó bases de datos de imágenes en dos y tres dimensiones que han marcado un hito en el avance del reconocimiento facial. En otras palabras, estas bases de datos han abierto la puerta a un examen más exhaustivo de los algoritmos de reconocimiento facial en el ámbito tridimensional [44].

5.7.1. Particularidades del procesamiento previo al análisis

Antes de analizar imágenes en 3D, es importante realizar un procesamiento de forma adecuada para mejorar la calidad de los datos que se van a evaluar. Esto es fundamental para llevar a cabo con éxito la extracción de características y la ejecución de los algoritmos de reconocimiento facial. De esta manera, los pasos básicos en esta etapa son:

Eliminación de ruido

En esta etapa, el objetivo es erradicar lo máximo posible el ruido utilizando diferentes técnicas. Una forma común de tratar la imagen es aplicando un filtro de mediana que sustituye el valor de cada píxel por el promedio de los valores de los píxeles cercanos. Con ajustes en los algoritmos, ha mostrado ser efectivo en imágenes tridimensionales. Asimismo, se emplea la técnica de interpolación para completar las zonas vacías de las imágenes. En concreto, la interpolación cúbica es una variante muy eficaz para este propósito, aunque requiere de una gran capacidad de procesamiento [52].

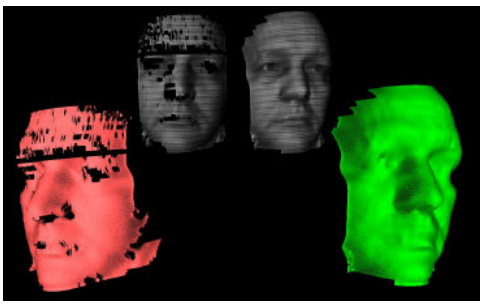

Figura 5.7: Efectos del ruido en la imagen adquirida. A la izquierda un modelo 3D con una gran cantidad de ruido. A la derecha, el mismo modelo después del proceso de la eliminación del ruido. [61]

Operaciones morfológicas

Este tipo de operaciones son fundamentales en el preprocesamiento, pues permiten estudiar la forma de la superficie de las imágenes. En estos casos, se utiliza un elemento estructural que se desplaza por la imagen equiparando los píxeles de su alrededor. En la actualidad, la erosión y la dilatación son las dos operaciones morfológicas clave. Por un lado, la erosión hace más pequeñas determinadas áreas de la imagen al eliminar píxeles, mientras que la dilatación las hace más grandes al agregar píxeles [52].

En definitiva, es importante realizar un tratamiento previo para mejorar la calidad de las imágenes adquiridas y minimizar así posibles errores antes de aplicar los algoritmos de reconocimiento.

5.7.2. Técnicas sofisticadas de reconocimiento facial en 3D

Estas técnicas tienen como finalidad incrementar la exactitud así como la fiabilidad, especialmente en aquellas situaciones complejas donde hay cambios en la postura y las expresiones de la persona o la luz. Como consecuencia, estos métodos mejorados utilizan tecnología avanzada para adquirir y evaluar los rasgos faciales, lo que resulta en un mayor rendimiento en diversas aplicaciones.

5.7.2.1. Detección de puntos de referencia

El procedimiento para detectar puntos de referencia en imágenes faciales tridimensionales se realiza utilizando un método que localiza ocho puntos importantes en la anatomía de la cara del individuo: ambos extremos de los ojos, la punta de la nariz, las dos comisuras de los labios y el mentón. Estos puntos se organizan en tres grupos en función del modelo que se utilicen: FLM8 (Facial Landmark Model), que incluye los ocho puntos completos; y FLM5L y FLM5R, que hacen referencia solo a los cinco puntos que son visibles en los lados izquierdo y derecho del rostro. Estos modelos están diseñados para posibilitar que al menos cinco puntos de referencia sean visibles en las imágenes que se capturan desde ángulos laterales, haciéndolos útiles en circunstancias donde no es posible capturar todo el rostro [44].

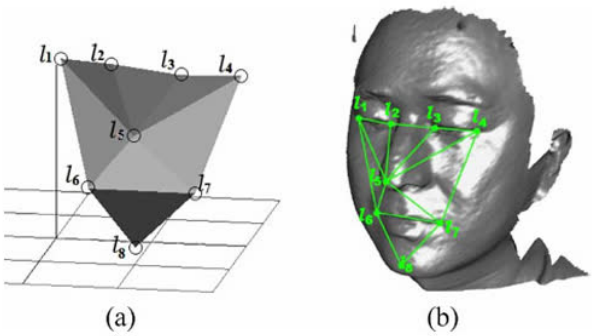

Figura 5.8: a) Representación de un modelo 3D, b) Ese mismo modelo superpuesto en una imagen facial [44]

Este proceso inicia con la recopilación de posibles puntos candidatos, extraídos de un mapa de índices, el cual sea crea a partir de las imágenes en 3D de rostro. En este mapa, los picos marcan puntos potenciales localizados en zonas como la punta de la nariz o el mentón, a diferencia de los valles que se relacionan con los límites de los ojos y la boca. Posteriormente, los puntos que han sido seleccionados en la etapa anterior se organizan y se analizan en relación con su influencia haciendo uso de cinco plantillas a las que se aplican movimiento de rotación. La semejanza entre dos imágenes se evalúa a través de un coeficiente de correlación lineal normalizado [44].

5.7.2.2. Ajuste de modelo deformable simétrico

En esta vertiente del reconocimiento facial en tres dimensiones, la adaptación de modelos flexibles se ha convertido en la clave para capturar la esencia de los rostros con la máxima precisión, transformando simples imágenes faciales en representaciones vívidas y detalladas. No obstante, cuando este tipo de datos disponen de ciertas áreas de la cara ocultas por la posición o la calidad, es crucial aplicar métodos que permitan abordar estas carencias. A continuación, se presenta una técnica centrada en la simetría facial que genera resultados exactos incluso cuando se trabaja con información incompleta.

La adaptación de este modelo deformable se fundamenta en la integración de un ajuste simétrico diseñado para abordar la falta de información en las imágenes de caras. En la actualidad, es posible gestionar por separado tanto la parte izquierda, como la derecha de un modelo facial. Como resultado, este enfoque se basa en la armonía innata del rostro humano, eludiendo la necesidad de realizar una gran cantidad de cálculos computacionales en las zonas donde los datos capturados puedan ser escasos [44].

Durante este procedimiento, al calibrar el escaneo facial catalogado como perteneciente al extremo izquierdo, la adaptación se lleva a cabo exclusivamente en esa mitad del rostro. Posteriormente, se replica en el lado derecho para reproducir la estructura de la cara de manera simétrica. En las imágenes del lateral derecho, el proceso se lleva a cabo de forma inversa: se ajusta el lado derecho y se refleja en el izquierdo. De esta forma y tal y como ya se ha mencionado, esta metodología garantiza una adaptación total [44].

5.8. Evaluación de seguridad de los sistemas de reconocimiento facial

La robustez del reconocimiento facial es un pilar esencial que garantiza su rigor generando confianza en un amplio espectro de aplicaciones. Con la creciente incorporación de esta clase de sistemas en una variedad de ámbitos, desde la banca hasta los dispositivos móviles, se vuelve imprescindible desentrañar los riesgos que conllevan su utilización.

Esta tecnología no está exenta de amenazas que podrían ser aprovechadas por posibles atacantes, poniendo en jaque la confidencialidad de los usuarios. Las intrusiones que se benefician de diferentes vulnerabilidades pueden abrir la puerta a accesos no autorizados, y ello destaca la urgencia de implementar ingeniosas estrategias de defensa.

Dentro de este panorama, resulta fundamental analizar no solo las vulnerabilidades más relevantes de estos sistemas, sino también las contramedidas que son necesarias implementar para poder mitigarlas. Por consiguiente, en esta sección se evaluarán los riesgos, al igual que las tácticas de protección diseñadas para optimizar la seguridad de los sistemas de reconocimiento facial, buscando siempre un equilibrio entre la eficacia y la seguridad.

5.8.1. Ataque Hill-Climbing indirecto

El ataque Hill-Climbing es una estrategia sofisticada que se emplea con frecuencia para sacar provecho de las debilidades de los sistemas de reconocimiento facial. Esto se logra a través de un proceso de ajuste iterativo de las plantillas sintéticas que busca eludir las defensas de seguridad de manera eficiente. Este ataque se encuentra su fundamento en beneficiarse de las puntuaciones de similitud que proporciona el sistema, utilizando esta información para ajustar las plantillas hasta alcanzar una coincidencia óptima. Con el paso del tiempo, distintos

investigadores han presentado pluralidad de estrategias para abordar este ataque. Entre ellas se encuentra el innovador enfoque de Mohanty, quien propuso un método basado en modelos para la reconstrucción de imágenes faciales a partir de las puntuaciones de coincidencia. No obstante, uno de los desafíos más significativos de esta técnica es la necesidad de contar con un amplio conjunto de imágenes faciales auténticas.

En este escenario, el ataque de Hill-Climbing Bayesiano surge como una alternativa más efectiva. En contraposición a otros enfoques, este algoritmo se sustenta en la teoría bayesiana para personalizar una serie de plantillas generales, ajustándolas a las particularidades de un grupo de individuos específicos que se encuentran más próximos al objetivo del ataque. Esta habilidad para ajustarse es lo que le confiere una ventaja única frente a otros métodos, permitiendo su uso en sistemas biométricos que funcionan con vectores de características de longitud constante y que, además, producen puntuaciones de similitud [33].

El investigador Javier Galbally ha puesto a prueba este tipo de ataque en dos sistemas de identificación facial: uno que utiliza el clásico método de Eigenfaces y otro que emplea una técnica más sofisticada basada en Modelos de Mezcla Gaussiana (GMM).

5.8.2. Funcionamiento del ataque Hill-Climbing bayesiano

Este algoritmo adopta una estrategia iterativa que recuerda a otros métodos de Hill-Climbing, donde se crean plantillas sintéticas que se refinan progresivamente dependiendo de las puntuaciones de similitud adquiridas en cada paso del proceso. Sin embargo, el verdadero punto distintivo se encuentra en la aplicación de la teoría bayesiana, que permite personalizar las plantillas de una amplia gama de usuarios para ajustarlas de manera más precisa a un grupo específico que se asemeja al objetivo del atacante. La definición del algoritmo se basa en tres parámetros primordiales [33] :

- **N:** La cantidad de plantillas seleccionadas de la distribución general para calcular las puntuaciones de similitud. Estas plantillas sirven como base sobre la cual se construirán nuevas plantillas en las siguientes iteraciones.
- **M:** La cantidad de plantillas elegidas que han obtenido las puntuaciones más altas para realizar los cálculos en la distribución local. Es importante destacar que se debe cumplir que M <N.
- α**:** El coeficiente de ajuste que determina la manera en que se ponderan las plantillas elegidas para transformar la distribución a nivel global. Este parámetro puede oscilar entre los valores [0,1].

La clave de este algoritmo reside en su habilidad para adaptarse a las particularidades del sistema objetivo sin requerir imágenes auténticas. Esta versatilidad se mantiene intacta, siendo irrelevante la característica biométrica analizada.

5.8.3. Aplicación del ataque en sistemas de reconocimiento facial

Este tipo de ataque fue evaluado en dos sistemas de identificación de rostros distintos. Se eligieron estos sistemas en concreto para poder analizar cómo se desempeñan estos ataques en técnicas biométricas que emplean vectores de características de longitud constante y que generan puntuaciones de similitud reales. En consecuencia, este enfoque resalta la versatilidad y la capacidad de ajuste del algoritmo ante diversas técnicas de reconocimiento facial.

Sistema basado en Eigenfaces

Este sistema utiliza la conocida técnica de Análisis de Componentes Principales para simplificar las imágenes faciales, convirtiéndolas en vectores de características que facilitan una comparación eficaz entre rostros. Se emplean imágenes faciales recortadas a un tamaño de 64x80 píxeles para entrenar un espacio vectorial, asegurando que se preserve el 80 % de la varianza en las características.

En los experimentos realizados por Galbally, el ataque logró eludir la seguridad de más del 85 % de los casos, dejando al descubierto la fragilidad de los sistemas basados en Eigenfaces ante este tipo de amenazas. Esto se atribuye, en parte, a las características intrínsecas de este tipo de sistemas que simplifican las imágenes al reducirlas a un espacio de menor dimensiones. Esta transformación permite al algoritmo explorar y ajustar de manera más ágil las plantillas faciales sintéticas en un proceso iterativo [33].

Sistema basado en Modelos de Mezcla Gaussiana (GMM)

El innovador sistema de evaluación transforma las imágenes de tamaño 64×80 en bloques pequeños de 8×8, añadiendo una superposición de 4 píxeles tanto en horizontal como en vertical. Este proceso se traduce en obtener como resultado 285 bloques.

Posteriormente, se extraen 15 coeficientes de la transformada discreta del coseno a partir de cada bloque, y estos se convierten en los vectores de características. El ataque sobre este sistema resultó ser sorprendentemente eficaz, alcanzando una tasa de éxito comparable a la del sistema PCA, comprometiendo el 86 % de los usuarios atacados. A pesar de la intricada naturaleza del sistema, el algoritmo Hill-Climbing demostró su potencial al crear plantillas sintéticas altamente efectivas sin recurrir a imágenes reales, lo que garantizó que el ataque mantuviera su eficacia en este contexto [33].

En definitiva, ambas tecnologías de reconocimiento facial revelaron sus vulnerabilidades ante este modelo de ataque Hill-Climbing. A pesar de las variaciones en la manera en que se presentan y comparan las imágenes faciales, la esencia cíclica de la estrategia de ataque logró un notable éxito en la mayoría de los escenarios analizados. Este análisis subraya la urgencia y necesidad de implementar estrategias más robustas con el fin de reforzar la seguridad de los sistemas de reconocimiento facial ante estas amenazas emergentes.

5.8.4. Contramedidas propuestas para este tipo de ataques

Una de las estrategias más investigadas para mitigar estos ataques es la cuantización de puntuaciones. Esta técnica se presenta como una solución eficaz para restringir la cantidad de información que un atacante puede obtener a partir de las puntuaciones de similitud que el sistema proporciona.

La cuantización de las puntuaciones implica restringir la exactitud de los valores que el sistema suministra, lo que a su vez disminuye las posibilidades del atacante para explotar mínimas diferencias en las puntuaciones a lo largo de las diferentes iteraciones del ataque Hill-Climbing. Al convertirlas en valores discretos, se genera un grado de incertidumbre que complica el ajuste exacto de las plantillas sintéticas. Esto no solo retarda la progresión del ataque, sino que también eleva el número de intentos requeridos para lograr un resultado exitoso [33].

En aquellos sistemas cuyo funcionamiento se basa en Eigenfaces, los ensayos realizados por Galbally con diversas escalas de cuantización revelaron un fenómeno curioso: conforme el tamaño de la cuantización aumentaba, la eficacia del ataque se desvanecía. A pesar de ello, el ataque logró alcanzar una tasa de éxito del 16.5 %. Esto sugiere que, si bien la cuantización de puntuaciones puede mitigar la eficacia del ataque, no resulta ser una solución infalible por sí misma. Además, los amplios intervalos de cuantización impactan de manera adversa en el Equal Error Rate (EER) del sistema, generando un difícil equilibrio entre la seguridad y el rendimiento. Esto se traduce en un aumento en los errores, tanto a la hora de permitir el acceso a impostores como al rechazar a personas legítimas [33].

De forma análoga, en el sistema fundamentado en GMM, los diversos incrementos en los pasos de cuantización hicieron que la eficacia del ataque disminuyera. Sin embargo, logró mantener una notable tasa de éxito del 81 % incluso con el mayor ajuste evaluado. Esto indica que a pesar de que la cuantización actúa como un escudo frente a posibles ataques, el algoritmo Hill-Climbing mantiene su capacidad para perfeccionar las plantillas con eficacia decisiva. En contraste, el sistema GMM demostró una robustez significativa frente a ataques que emplean pasos de cuantización más reducidos, logrando así una mayor armonía entre la seguridad y la eficiencia [33].

5.8.5. Recomendaciones para las contramedidas propuestas

Pese a que la cuantización de puntuaciones ha demostrado ser funcional en cierta medida, las pruebas llevadas a cabo en ambos sistemas revelan que, por sí misma, esta estrategia no basta para erradicar plenamente la eficacia de los ataques Hill-Climbing fundamentados en la teoría bayesiana. Aunque se puede limitar la eficiencia del ataque requiriendo más intentos para poder penetrar en el sistema, el algoritmo mantiene una valiosa fortaleza que le permite eludir esta defensa en numerosas ocasiones [33].

Por este motivo, es aconsejable integrar la cuantización de puntuaciones con diversas tácticas de seguridad. Esto incluye la identificación de patrones de ataque, como múltiples intentos infructuosos que presenten pequeñas variaciones en las plantillas. También se sugiere establecer umbrales de seguridad adaptables, además de implementar técnicas que identifiquen e impidan el uso de plantillas que sean demasiado parecidas entre sí. Estos enfoques complementarios potenciarán la resistencia del sistema reduciendo, de esta forma, la probabilidad de sufrir ataques exitosos [33].

En conclusión, esta medida preventiva se presenta como una herramienta valiosa en la batalla contra los ataques Hill-Climbing, aunque se considera que no es una solución absoluta. Por ello, es fundamental integrar este mecanismo dentro de un marco más amplio que entrelace diversas estrategias de seguridad con el propósito de salvaguardar adecuadamente los sistemas de reconocimiento facial frente a esta creciente amenaza.

Capítulo 6

Tecnologías biométricas aplicadas a dispositivos Android

Este capítulo tiene como propósito ofrecer al lector un análisis sobre la integración de las técnicas biométricas en el desarrollo de aplicaciones móviles para dispositivos Android. Desde este punto de vista, se detallará el funcionamiento de una de las APIs que está disponible en este contexto para llevar a cabo la implementación de diferentes funciones de reconocimiento biométrico. En las siguientes páginas se investigará de qué forma esta tecnología fortalece la seguridad, optimizando de forma simultánea la experiencia de uso de las personas.

6.1. Introducción

En el competitivo mundo de los dispositivos móviles, el sistema operativo Android se ha impuesto obteniendo un porcentaje del mercado con el valor de 71.77 % en el año 2024, de acuerdo a un estudio reciente realizado por StatCounter [70]. Este liderato implica la existencia de millones de dispositivos Android, que abarcan desde móviles económicos hasta aquellos de gama alta, usados en cualquier parte del planeta. Esta magnitud, junto con la incorporación de tecnologías innovadoras como la biometría, ha ocasionado que este sistema operativo se alce como uno de los más eficaces. Así, estos sistemas, desarrollados para maximizar la experiencia del usuario permitiendo una mayor personalización, se han convertido en un medio para satisfacer las novedades del mercado tecnológico.

Por otro lado, la biometría como técnica de reconocimiento ha evolucionado significativamente desde el inicio de su desarrollo. Como consecuencia, hoy en día, gracias a los numerosos proyectos que han promovido su progreso y perfección, se ha logrado incorporar esta tecnología a múltiples entornos. En otras palabras, el hecho de investigar cómo se aplican estas técnicas en el sistema operativo propiedad de Google es una elección que se fundamenta en su relevancia en el mercado actual.

En concreto, en Android existe una interfaz llamada BiometricPrompt que ha posibilitado a los programadores integrar de una forma efectiva la identificación biométrica tanto a través de las huellas dactilares, como del rostro del usuario. Esta API fue diseñada para simplificar la incorporación de este tipo de funcionalidad garantizando, al mismo tiempo, una robusta seguridad. Es por este motivo que a lo largo de este capítulo se detallará el funcionamiento de la misma con el propósito de demostrar que su implementación es mucho más sencilla de lo que se puede pensar a priori.

6.2. Evolución histórica del sistema operativo Android

En 2003, el sistema operativo conocido mundialmente como Android fue diseñado por Andy Rubin, Nick Sears, Rich Miner y Chris White, en el seno de Android Inc., una empresa fundada por estos mismos emprendedores dedicada al desarrollo de software que, posteriormente, en el año 2005, fue adquirida por Google. En sus inicios, este proyecto fue pensado para optimizar la experiencia de uso en las cámaras digitales [22]. No obstante, los desarrolladores supieron reconocer rápidamente el auge del mercado de los dispositivos móviles. Como consecuencia, solo dos años después fue presentada al mercado la primera versión beta de Android, marcando el comienzo de uno de los mayores éxitos tecnológicos.

Poco después, en el año 2008, se publicó la primera versión oficial incorporada en el dispositivo HTC Dream. Esta proporcionaba funciones muy básicas como la integración de las aplicaciones propias de Google entre las que se puede señalar, por ejemplo, Gmail. En caso de que el usuario quisiera adquirir otro tipo de aplicaciones o juegos se puso en marcha Android Market, un antecedente a lo que hoy se conoce como Play Store. Esto permitió a los desarrolladores recaudar dinero por sus aplicaciones, marcando un importante punto de inflexión a partir del cual se incorporaron elementos cada vez más innovadores. Un claro ejemplo de ello es la versión llamada Cupcake, que integró un teclado virtual en la pantalla táctil del dispositivo [22].

En la década de 2010, los desarrolladores de Android consolidaron el dominio de este sistema operativo en el mercado tecnológico. Ello fue debido a la implementación de mejoras clave como la fluidez de movimiento en la pantalla o una gran transformación de la interfaz de usuario. Al mismo tiempo, el uso de este SO se expandió hacia otro tipo de dispositivos como tablets o relojes inteligentes.

En resumen, el progreso técnico de Android subraya su potente dominio en el área de los dispositivos móviles, además de su habilidad para incorporar de forma eficaz y rápida nuevas tecnologías, como podría ser el caso hoy en día de la Inteligencia Artificial. Asimismo, estos avances han demostrado que está diseñado para satisfacer las necesidades dinámicas de un mundo que está en constante cambio.

6.3. Arquitectura de la API

La API BiometricPrompt ha sido desarrollada para poder llevar a cabo un reconocimiento biométrico en diversas aplicaciones móviles. Así, fue creada para fortalecer la seguridad de estos procesos y simplificar el uso de una combinación de varios métodos biométricos, como son las huellas digitales o el reconocimiento facial, a través de una interfaz única. El objetivo es centralizar la gestión de la utilización de los distintos sensores biométricos que tiene un dispositivo. Asimismo, brinda una implementación sólida en términos de privacidad utilizando criptografía. A continuación, se pueden observar los diferentes componentes que forman esta arquitectura.

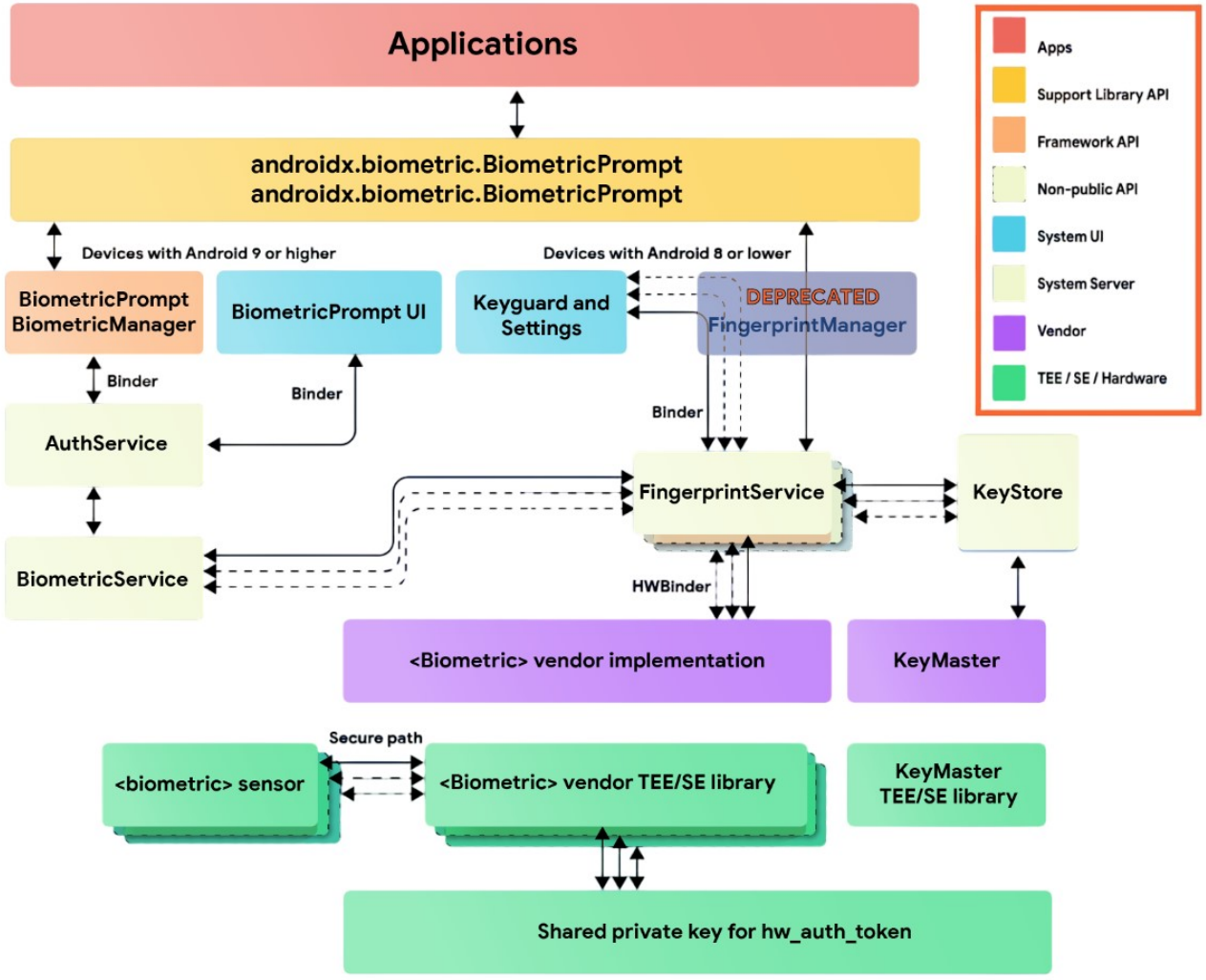

Figura 6.1: Arquitectura de la API BiometricPrompt [2]

Esta API creada para su uso en dispositivos Android representa una solución óptima para la incorporación de este tipo de autenticación. Como se puede comprobar en la capa superior de la Figura 6.1, la aplicación deberá implementar la API androidx.biometric.BiometricPrompt para hacer uso de los nuevos servicios disponibles a partir de Android 9 Versión Pie, con el fin de interactuar con los servicios del sistema, como el AuthService, mediante el mecanismo de comunicación Binder. Esta interfaz de comunicación garantiza que la transmisión de datos se realice de forma segura. Por otro lado, el componente BiometricPrompt UI proporciona al usuario final una interfaz visual personalizable para solicitar los datos biométricos.

Por último, en la capa inferior de la arquitectura, los componentes KeyStore, junto con las bibliotecas TEE protegen el procesamiento de estos datos con la ayuda de la criptografía, ejecutando el proceso en un entorno protegido. El diseño por parte de los proveedores de los sensores biométricos específicos asegura la captura fiable de las características biométricas del individuo. En conclusión, la decisión de analizar el funcionamiento de esta API se debe a que gracias a su diseño se permite ejecutar la autenticación biométrica con un alto grado de seguridad ajustando su uso a diversos dispositivos y versiones del sistema operativo.

6.3.1. Principal funcionamiento de la API

¿De qué manera los sistemas biométricos consiguen reconocer y confirmar la identidad de una persona? La clave reside en la conformación de las dos etapas fundamentales [42]:

Enrolamiento

En esta etapa inicial, el sistema recoge por primera vez los datos biométricos del individuo. Esta información es sometida a un proceso de análisis exhaustivo con el objetivo de obtener los atributos más significativos. En este punto, cabe destacar que estos datos no son almacenados por completo, es decir, solo se preserva el conjunto de características más relevantes que posibilitan marcar la diferencia entre la identidad de una persona de la de los demás, mientras que los datos en crudo se eliminan.

Por consiguiente, el elemento resultante de este proceso es una plantilla biométrica exclusiva, que se almacena en una base de datos y se convierte en la referencia para futuras comparaciones. Es imprescindible que esta configuración se realice en el TEE, componente clave que se detallará más adelante, lo que garantiza un almacenamiento seguro.

Reconocimiento

En la segunda etapa, el individuo intenta autenticarse en el dispositivo presentando de nuevo la misma característica biométrica que se registró previamente, la cual será capturada por el sistema haciendo uso de mecanismos específicos, como son escáneres y cámaras, en función del tipo de característica biométrica que se esté evaluando. Esta es minuciosamente analizada en

el TEE para extraer las mismas cualidades significativas que se recopilaron durante la primera fase, lo que asegura una coherencia en la evaluación.

Posteriormente, esta nueva información se contrasta con la plantilla almacenada con anterioridad para identificar al individuo. Esta equiparación se lleva a cabo mediante algoritmos de coincidencia de patrones, desarrollados para evaluar la semejanza entre ambas muestras. Por último, se informa a la aplicación del resultado que se ha obtenido del reconocimiento.

En la actualidad, es necesario que cualquier dispositivo gestione de forma segura la información biométrica de un usuario. En este sentido, todo el proceso de identificación se deberá ejecutar en el denominado Entorno de Ejecución Confiable (TEE), un entorno que se ha desarrollado en el propio dispositivo para ejecutar código de forma segura y aislada del resto de elementos que forman parte de la arquitectura. Gracias a este componente, en ninguna fase de este proceso existe la posibilidad de que este tipo de datos sean compartidos con la aplicación o sean utilizados por procesos que no están autorizados para ello. Es decir, todo el proceso se realizará exclusivamente dentro del TEE.

6.3.2. Extracción de datos privados en un entorno seguro

En el sistema operativo Android, y en particular en el uso de esta API, el tratamiento de los datos es mucho más seguro cuando se hace uso del componente KeyStore. A continuación, se detalla el flujo de trabajo que se lleva a cabo entre el sistema biométrico y este elemento:

1. **Establecer el uso de la autenticación biométrica para las claves secretas**

   El primer paso es determinar que la autenticación biométrica sea obligatoria para poder tener acceso a la clave secreta mediante la función setUserAuthenticationRequired(true). Esta función obliga a utilizar este tipo de autenticación cuando se quiera acceder a las claves secretas.

2. **Solicitar información relacionada con la clave secreta**

   En el momento en el que la aplicación requiera acceder a datos que estén salvaguardados por la clave secreta, el sistema deberá mostrar un cuadro de diálogo para solicitar al usuario que presente sus datos biométricos.

3. **Comprobación en el TEE**

   En este punto, el sensor transmitirá de manera fiable la información biométrica capturada hacia el TEE. Es importante señalar que las aplicaciones externas no podrán consultar esta transacción. Una vez lleguen los datos al TEE, se tratan para contrastarlos con la plantilla almacenada.

4. **Creación del token de autenticación de hardware (HAT)**

   Si el resultado de la comparación es correcto, se produce un token de autenticación de hardware. Este contiene un código de autenticación de mensajes basado en hash (HMAC), cuya función es garantizar factores como la integridad y la veracidad de la transacción.

5. **Desbloqueo de la clave secreta**

   El componente KeyMaster, en el momento en el que reciba el valor HAT, tendrá la capacidad de verificar su autenticidad y desbloquear así la clave secreta. Este mecanismo asegura que únicamente se desbloquee la clave en caso de que la autenticación sea exitosa, brindando una capa extra de seguridad.

6. **Realizar un callback a la aplicación que necesita la autenticación**

   El último paso de este proceso es ejecutar un callback a la aplicación que está esperando el resultado del reconocimiento. Esto permitirá al usuario poder hacer uso de la aplicación.

Como última consideración, los sistemas basados en Android introducen una capa de seguridad extra desactivando las claves privadas vigentes que están vinculadas a este tipo de autenticación cada vez que se configure una nueva identidad biométrica en el dispositivo. Se ha comprobado que este método impide que un posible atacante añada una nueva credencial para obtener acceso a la información privada que está protegida. En el supuesto de que esto suceda, las claves secretas no se podrán utilizar, por lo que los datos asociados a ellas no estarán disponibles.

6.4. Evaluación de la seguridad biométrica en Android

Con el objetivo de asegurar que la tecnología es compatible con Android, cualquier implementación biométrica deberá satisfacer los criterios que se han determinado en el Documento de Definición de Compatibilidad. En este informe se analiza la seguridad de la integración del reconocimiento biométrico en los dispositivos a través de dos factores decisivos [3]:

- **Seguridad arquitectónica:** Esta pauta evalúa la capacidad de proteger los datos biométricos en el hipotético caso de que se produzca un compromiso del kernel del sistema o de la plataforma. Un sistema es clasificado como seguro si estos ataques no posibilitan el acceso a los datos biométricos en crudo, ni permiten la inyección de datos sintéticos que puedan afectar al funcionamiento de la autenticación. Esto asegura que el reconocimiento sea robusto respecto a ataques externos.

- **Rendimiento de la seguridad biométrica:** Este criterio se mide con base en diferentes métricas especializadas, cuya finalidad es determinar la capacidad de estos sistemas para soportar distintos tipos de ataques, a la vez que reducen al mínimo los fallos en el reconocimiento. Se considera que estos indicadores son fundamentales para avalar que el uso de las tecnologías biométricas sea seguro. En el caso del sistema operativo Android se emplean tres medidas concretas.

  - **Tasa de aceptación de suplantación de identidad (SAR):** Es una métrica incorporada a partir de la versión 9 de Android. La finalidad es analizar lo fuerte que es un sistema biométrico ante un ataque de presentación física. Es decir, se mide la probabilidad de que una tecnología biométrica admita una muestra válida registrada previamente. Un ejemplo claro es el de la biometría por voz, métrica que evaluaría las probabilidades que tendría un atacante de acceder al dispositivo utilizando una grabación de voz del usuario legítimo.

  - **Tasa de aceptación de impostores (IAR):** Evalúa la posibilidad de que el dispositivo admita como válida una muestra biométrica falsa. Este parámetro es fundamental para medir la robustez ante ataques de *spoofing*.

  - **Tasa de aceptación falsa (FAR):** Calcula la frecuencia con la que un sistema de este tipo aprueba el acceso de forma errónea a una persona no autorizada.

En resumen, el desempeño de la seguridad en el ámbito de la autenticación biométrica en dispositivos Android se fundamenta en unos criterios robustos válidos para la mayoría de los métodos biométricos que se utilizan hoy en día. No obstante, cabe destacar que la tasa IAR no está diseñada para ser utilizada de forma general en cualquier modalidad. Adicionalmente, Android colabora con los suministradores tanto del hardware como del software biométrico realizando pruebas exhaustivas de seguridad para garantizar que estos sistemas se ajusten a los estándares establecidos en términos de seguridad y calidad.

6.5. Flujo del proceso de la autenticación biométrica

El proceso del reconocimiento biométrico mediante la API BiometricPrompt se desglosa en cinco etapas clave. En primer lugar, es imprescindible comprobar si el dispositivo que se está usando es compatible con la autenticación biométrica. En el momento en el que se ha verificado, se establece las funciones de retorno para manejar los diferentes eventos existentes en el proceso. Posteriormente, se define la configuración del prompt biométrico. Después, se procede con la autenticación permitiendo al usuario presentar la característica biométrica que se vaya a utilizar. Por último, se procesa el resultado de dicha autenticación gestionando las futuras acciones en función de si el resultado fue exitoso o no.

Figura 6.2: Flujo del proceso de la autenticación biométrica [12]

En los siguientes apartados se explicará de forma detallada cómo llevar a cabo estas fases usando el lenguaje de programación Java.

6.6. Guía para la implementación de BiometricPrompt

La API BiometricPrompt ha sido desarrollada para proporcionar flexibilidad en la adaptación de diferentes métodos biométricos con una gran facilidad de uso. A lo largo de esta sección, se proporcionará un manual que detalla los pasos fundamentales para implementar esta API [4].

6.6.1. Añadir las dependencias necesarias al proyecto

Para empezar a implementar esta API, el primer paso es incorporar las dependencias imprescindibles para su correcto funcionamiento. Esto se realiza en el fichero build.gradle a nivel de aplicación del proyecto. Para ello, es necesario localizar la sección de las dependencias para añadir la siguiente línea:

```
dependencies {

implementation "androidx.biometric:biometric:1.1.0"

}
```

En este caso, se ha decidido utilizar la versión estable de la API publicada en 2021. Sin embargo, en caso de que el desarrollador decida utilizar la última versión disponible de la interfaz, este dato se puede consultar en el siguiente enlace [5].

6.6.2. Declarar los tipos de autenticación soportados por la app

El segundo paso es establecer los métodos de autenticación que admitirá la aplicación que se está desarrollando. Para ello, es preciso utilizar la interfaz BiometricManager.Authenticators. Esta tiene la capacidad de detectar qué opciones de reconocimiento serán accesibles para el usuario en función de las características hardware de sus dispositivos, así como sus preferencias a la hora de autenticarse.

Tipos de autenticación disponibles en la API

En este contexto se ofrece al desarrollador poder incorporar las siguientes alternativas. Es importante destacar que esta elección se fundamenta en los requisitos de seguridad que se hayan establecido para el diseño de la aplicación:

- **BIOMETRIC_STRONG** Cualquier método biométrico disponible en el dispositivo que cumpla con los requisitos de la Clase 3 definida en el CDD de Android [6].

- **BIOMETRIC_WEAK** Cualquier método biométrico disponible en el dispositivo que cumpla con los requisitos de la Clase 2 definida en el CDD de Android [6].

- **DEVICE_CREDENTIAL** Hace referencia al uso de credenciales que no estén relacionadas con la biometría, como podrían ser un PIN o un patrón. No obstante, se recomienda su uso exclusivamente en combinación con alguno de los dos anteriores.

Proceso de configuración

El siguiente paso es configurar el cuadro de diálogo que usará la API. En otras palabras, se definirá la pantalla de autenticación de usuario, los textos que van a aparecer en la pantalla y los métodos de autenticación que va a soportar. A continuación, se muestra el fragmento de código que se debe de usar para poder establecer las opciones que va a disponer el usuario de la aplicación:

```
// Permitimos al usuario autenticarse utilizando biometría
// o una credencial en la pantalla de bloqueo (PIN, patrón...)
promptInfo = new BiometricPrompt.PromptInfo.Builder()
    .setTitle("Autenticación biométrica")
    .setSubtitle("Autentícate utilizando el sensor biométrico")
    .setAllowedAuthenticators(BIOMETRIC_STRONG | DEVICE_CREDENTIAL)
    .build();
```

6.6.3. Verificar la disponibilidad del sistema para utilizar biometría

Una vez se han establecido los tipos de autenticación que van a ser soportados en la aplicación, es esencial comprobar si estos van a estar presentes en el dispositivo que está utilizando el usuario. Para este paso, se utilizará la función canAuthenticate() de la clase BiometricManager. Este será el encargado de analizar si las técnicas definidas anteriormente están disponibles en el dispositivo. El método retorna un valor que informa de las condiciones de los soportes para la biometría que se pueden usar.

Por otra parte, el primer caso señala que la biometría está disponible y se puede continuar con el proceso y el segundo caso supone que el equipo no cuenta con ningún tipo de hardware biométrico, por lo que se deben elegir otros métodos de autenticación. Mientras, el cuarto caso indica que el dispositivo tiene el hardware necesario, pero está indisponible por algún error. Finalmente, el último caso significa que se debe registrar una credencial que sea compatible.

```
BiometricManager biometricManager = BiometricManager.from(this);

switch (biometricManager.canAuthenticate(BIOMETRIC_STRONG |
   DEVICE_CREDENTIAL)) {

    case BiometricManager.BIOMETRIC_SUCCESS:
        Log.d("MY_APP_TAG", "Se puede autenticar en la aplicación
           con biometría.");
        break;
    case BiometricManager.BIOMETRIC_ERROR_NO_HARDWARE:
        Log.e("MY_APP_TAG", "El dispositivo no dispone de sensores
           biométricos.");
        break;
    case BiometricManager.BIOMETRIC_ERROR_HW_UNAVAILABLE:
        Log.e("MY_APP_TAG", "Las funciones biométricas no están
           disponibles actualmente.");
        break;
    case BiometricManager.BIOMETRIC_ERROR_NONE_ENROLLED:
        // Solicitar al usuario que configure unas credenciales
           nuevas
        final Intent enrollIntent = new Intent(Settings.
           ACTION_BIOMETRIC_ENROLL);
        enrollIntent.putExtra(Settings.
           EXTRA_BIOMETRIC_AUTHENTICATORS_ALLOWED,
                BIOMETRIC_STRONG | DEVICE_CREDENTIAL);
        startActivityForResult(enrollIntent, REQUEST_CODE);
        break;
}
```

6.6.4. Mostrar la solicitud de autenticación al usuario

Cuando el desarrollador tiene la certeza de que el dispositivo dispone de la tecnología necesaria para utilizar la biometría, el siguiente paso es mostrar por pantalla una solicitud para que el usuario pueda presentar sus credenciales biométricas. Sobre la base de la configuración del cuadro de diálogo que se ha hecho al inicio, esta solicitud tendrá la apariencia que se puede observar en la Figura 6.3.

Figura 6.3: Ejemplo del cuadro de diálogo configurado para solicitar las credenciales biométricas

En primer lugar, es necesario crear una nueva instancia de la clase BiometricPrompt, que será la encargada de gestionar toda la parte de interacción con el usuario, permitiendo, de esta forma, definir callbacks para poder gestionar lo que ocurrirá dependiendo del resultado de la autenticación. Posteriormente, es necesario configurar los tres métodos definidos en la interfaz AuthenticationCallback. El primero se debe ejecutar en caso de que ocurra algún tipo de error durante la autenticación, entre los que se puede mencionar el caso en el que los sensores no estén disponibles. El parámetro errorCode identificará el problema, mientras que el parámetro errString indica el mensaje que describe el error de forma más detallada. Por último, unificando toda esta información, se le mostraría al usuario una ventana emergente explicando el error que ha recibido. Por otro lado, el segundo método se ejecutará en los casos en los que la autenticación biométrica haya sido exitosa, a diferencia del tercer método que se utilizará cuando esta haya sido fallida.

En resumen, el flujo de trabajo tiene como fin establecer el funcionamiento de los métodos que son imprescindibles para gestionar los diferentes tipos de eventos asociados al proceso de autenticación, diseñar la apariencia del cuadro de diálogo y, finalmente ejecutar el método que permitirá al usuario autenticarse.

```
@Override
protected void onCreate(Bundle savedInstanceState) {
    biometricPrompt = new BiometricPrompt(MainActivity.this,
            executor, new BiometricPrompt.AuthenticationCallback()
               {

        @Override
        public void onAuthenticationError(int errorCode,
                @NonNull CharSequence errString) {
            super.onAuthenticationError(errorCode, errString);
            Toast.makeText(getApplicationContext(),
                "Error de autenticación: " + errString, Toast.
                   LENGTH_SHORT)
                .show();
        }

        @Override
        public void onAuthenticationSucceeded(
                @NonNull BiometricPrompt.AuthenticationResult
                   result) {
            super.onAuthenticationSucceeded(result);
            Toast.makeText(getApplicationContext(),
                "¡Autenticación exitosa!", Toast.LENGTH_SHORT).show
                   ();
        }

        @Override
        public void onAuthenticationFailed() {
            super.onAuthenticationFailed();
            Toast.makeText(getApplicationContext(), "Autenticación
               fallida",
                Toast.LENGTH_SHORT)
                .show();
        }
    });

    promptInfo = new BiometricPrompt.PromptInfo.Builder()
        .setTitle("Autenticación biométrica")
        .setSubtitle("Autentícate utilizando el sensor biométrico")
        .build();

    Button biometricLoginButton = findViewById(R.id.biometric_login
       );
    biometricLoginButton.setOnClickListener(view -> {
            biometricPrompt.authenticate(promptInfo);
    });}
```

6.7. Ventajas del uso de la API BiometricPrompt

El enfoque que han utilizado los desarrolladores de Android en el funcionamiento de esta API presenta diferentes ventajas que se especificarán en esta sección. Se considera que estos factores garantizan una experiencia de uso fiable.

- **Ofrece una seguridad sofisticada:** La utilización de entornos de ejecución seguros, como es el caso del elemento TEE, asegura que tanto los datos sensibles, como las claves se administren únicamente dentro de estos componentes, reduciendo así el riesgo de una posible filtración o exposición de esta información.

- **Uso de operaciones criptográficas:** El diseño de esta API permite asociar la criptografía con el reconocimiento biométrico. Esto implica que la información sensible solo sea accesible después de que el usuario legítimo realice una autenticación correcta. Este hecho proporciona un nivel superior de seguridad en aquellas aplicaciones que gestionen transacciones importantes.

- **Garantía de maximizar la privacidad del usuario:** El tratamiento de la información biométrica exclusivamente en el TEE, sin que haya terceros que tengan acceso, garantiza que el individuo tenga el control sobre el uso de sus datos personales. Asimismo, este método se ajusta a los estándares que regulan este tipo de usos.

- **Uso simplificado:** Los desarrolladores de Android han ofrecido a otros programadores una API que es sencilla de incorporar a cualquier aplicación, teniendo en cuenta las dificultades asociadas a estos métodos de reconocimiento. Igualmente, una gran ventaja de esta API es el soporte a diversas técnicas biométricas, como son las huellas dactilares o el reconocimiento facial, ajustándose a las características de cada dispositivo.

En conclusión, esta interfaz de programación de aplicaciones ha conseguido unificar aspectos clave como la seguridad y la privacidad utilizando la criptografía, maximizando, de esta forma, la simplicidad de su uso. Ello ha permitido en la actualidad poder efectuar un reconocimiento biométrico proporcionando unos altos estándares de protección. En pocas palabras, BiometricPrompt se ha convertido en un recurso esencial en el sistema operativo Android.

Capítulo 7

El reto de la privacidad en la biometría

Este capítulo tiene como objetivo brindar al lector un acercamiento a la privacidad en el ámbito de la biometría. En un mundo digital en el que los datos personales son capturados, analizados y almacenados de forma masiva, este tema cobra una gran relevancia. Por esta razón, este estudio se propone explorar de qué manera las tecnologías biométricas, concebidas para verificar identidades con un alto grado de seguridad, pueden generar importantes dilemas en materia de privacidad para los usuarios. Del mismo modo, se profundizará en la delgada línea que existe actualmente entre salvaguardar datos sensibles y los peligros asociados a su exposición, enfatizando en la importancia de desarrollar soluciones tecnológicas que sean tanto éticas como responsables.

7.1. Introducción

Hoy en día, las huellas dactilares o el rostro son aspectos que nos diferencian como individuos. A pesar de que hace no muchos años no se planteaban estos problemas, cada vez es más frecuente el uso de estos rasgos con fines maliciosos, haciendo que el ataque a la privacidad digital de los usuarios forme parte de una inquietante realidad. Por ello, como dos caras de la misma moneda, los sistemas biométricos fueron concebidos en un primer lugar para proporcionar facilidad de uso y seguridad y, sin embargo, actualmente presentan una grave amenaza para la protección de datos de carácter personal.

La biometría ha revolucionado nuestra relación con la tecnología, convirtiendo el cuerpo humano en la herramienta perfecta para poder acceder a dispositivos y garantizar la defensa de la información personal. No obstante, esta evolución plantea una compleja disyuntiva tanto de carácter ético como técnica: ¿pueden las personas estar seguras de que su información biométrica está a salvo de una filtración de datos o de usos ilícitos? A diferencia de una contraseña tradicional que se puede modificar con un simple clic, ¿qué ocurre cuando lo que se ve amenazado es tu propia identidad biométrica?

Incidentes de seguridad que han tenido lugar en 2024, como la filtración de datos de una compañía dedicada al reconocimiento facial, ponen de manifiesto lo frágiles que resultan ser este tipo de sistemas ante posibles amenazas [18] pues en este caso cientos de miles de registros, incluyendo información biométrica, fueron expuestos. Por ende, este tipo de sucesos revelan un nuevo peligro: las singularidades de una persona se han convertido en el nuevo objetivo de muchos delincuentes cibernéticos.

Dados lo recientes desafíos que ha enfrentado esta tecnología, en los últimos años se han presentado nuevas propuestas destinadas a superarlos. Así, de acuerdo con el análisis reciente llevado a cabo por Blaine Frederick [28], el horizonte de la biometría se perfila bajo el lema «prioridad a la privacidad». Esto conlleva la aplicación de diversas estrategias como la incorporación de medidas de seguridad desde el inicio del diseño del sistema o la utilización de técnicas avanzadas de anonimización, las cuales posibilitan el uso de la biometría sin poner en riesgo la identidad de las personas.

Tendiendo lo mencionado en cuenta, en este capítulo se analizará la biometría en términos de privacidad, una herramienta efectiva para fortalecer la seguridad, pero también un riesgo para los derechos fundamentales de los usuarios si no se administra correctamente. Durante el análisis, se explorarán las amenazas más relevantes que enfrentan los sistemas biométricos. Además, se investigarán las nuevas soluciones y normativas en desarrollo que pretenden mantener un equilibrio adecuado entre la seguridad y la privacidad, proporcionando un contexto ético que preserve los derechos primordiales de las personas.

7.2. Amenazas asociadas a los sistemas biométricos

Muchas personas consideran que la biometría ofrece una solución infalible para proteger sus datos personales, sin embargo, la suplantación de identidad mediante técnicas avanzadas es un problema real. Así, las amenazas vinculadas a estos sistemas son sumamente vanguardistas, así como preocupantes. En la Figura 7.1 se muestra la clasificación de los diferentes tipos de ataques existentes en la actualidad que podrían poner en riesgo un sistema biométrico. En los siguientes apartados se detallará cómo estos riesgos influyen en la privacidad, además de en la credibilidad en una tecnología que aparentaba ser confiable. ¿Hasta qué punto se considera segura la biometría?

7.2.1. Tipos de ataques realizados por un adversario

Teniendo en cuenta el amplio ámbito del reconocimiento biométrico, los ataques actuales no representan ofensas comunes: son operaciones rigurosamente elaboradas para sacar el máximo beneficio posible. Con este fin, los atacantes detectan y aprovechan cualquier vulnerabilidad del sistema [42].

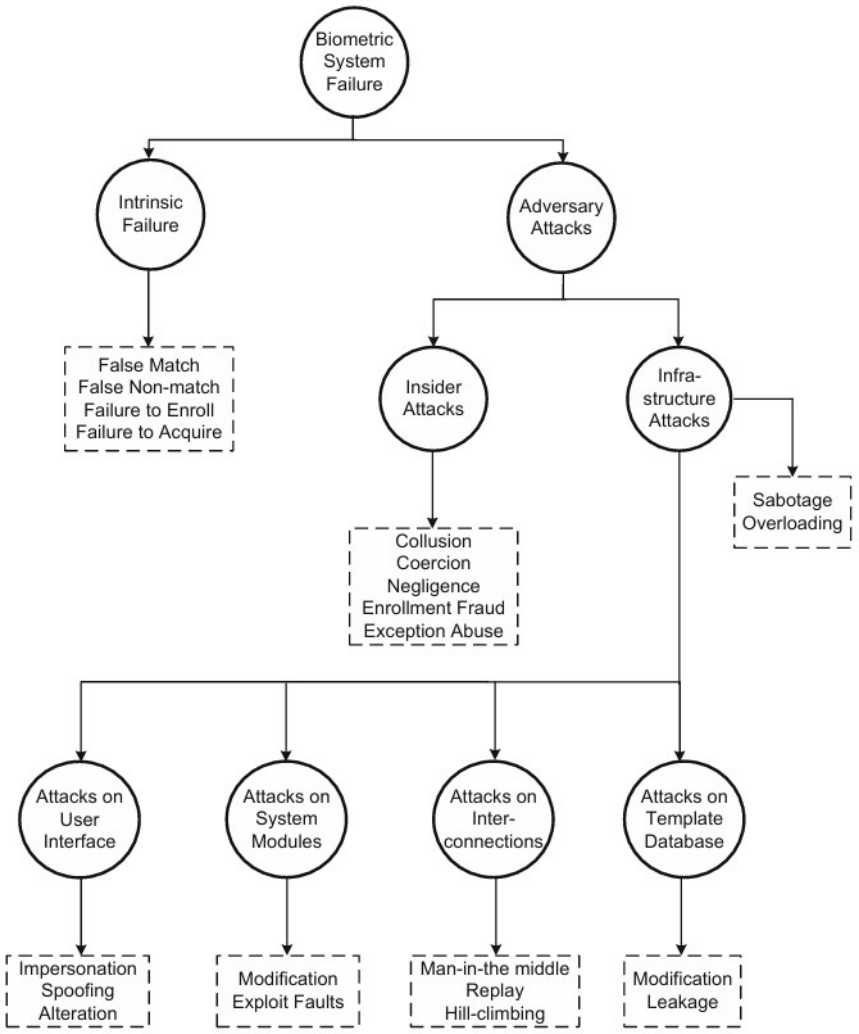

Figura 7.1: Clasificación de los ataques que se pueden llevar a cabo en un sistema biométrico [42]

7.2.1.1. Ataques internos

Estos ataques se caracterizan por beneficiarse de las diferentes interacciones entre una persona autorizada y el sistema. Un claro ejemplo de estos son las que llevan a cabo los administradores con el propósito de gestionar los usuarios, monitorear el apropiado uso del sistema o adaptar los diversos parámetros de seguridad a los requisitos establecidos.

- **Colusión:** Son los casos en los que un usuario con autorización realiza acciones maliciosas intencionalmente de forma individual o con ayuda externa a cambio de una recompensa económica. Un ataque de esta naturaleza tendría un grave impacto en el sistema al tratarse de un usuario con privilegios y con la capacidad de modificar la mayor parte de los módulos que componen el sistema. En este contexto, es complicado defenderse, pues la única protección posible consiste en proporcionar una buena formación, así como monitorizar la actividad de los usuarios para identificar lo antes posibles patrones anómalos.

- **Coerción:** En contraposición al anterior, en estos supuestos un atacante fuerza a los administradores a actuar de forma malintencionada, probablemente por medio de intimidación física o extorsión. En estas situaciones, es esencial localizar de forma segura estas situaciones sin poner en peligro a los usuarios legítimos.

- **Negligencia:** Una persona con intenciones malignas podría sacar provecho de los descuidos de los usuarios con privilegios para eludir la seguridad del sistema. Una acción común en muchos empleados es no cerrar la sesión correctamente después realizar operaciones críticas. Asimismo, se considera una negligencia permitir a personas no identificadas acceder al entorno de trabajo. Por lo tanto, una forma de reducir los efectos de esta amenaza es recordar de forma continúa las pautas que se deben seguir en cada puesto de trabajo y, así mermar estas posibles vulnerabilidades.

- **Fraude de identidad:** El oponente podría registrarse en el sistema de forma ilícita proporcionando sus características biométricas junto a unas credenciales fraudulentas. La solución para prevenir este tipo de ataques implica comparar las características biométricas del nuevo usuario con las características de la totalidad de los usuarios registrados con el objetivo de identificar un registro duplicado, procedimiento que se conoce como deduplicación de datos. No obstante, representa un desafío considerable en caso de que el número de personas presentes en el sistema sea muy alto.

7.2.1.2. Ataques a la infraestructura del sistema

Este tipo de ataques están orientados a atacar las principales debilidades técnicas del sistema, afectando a los diversos módulos de funcionamiento, así como a las vías de comunicación que los conectan entre sí. Sin embargo, en la actualidad se dispone de una variedad de configuraciones físicas a la hora de implementar estos sistemas, lo que repercute en la forma en la que se explotan dichas vulnerabilidades, además de en las medidas requeridas para reducir su impacto [42].

- **Interfaz de usuario:** Estos ataques se enfocan en la interacción preliminar entre el individuo y el dispositivo. Un caso frecuente es la impersonación, en el que una persona intenta suplantar a un usuario válido. Otro ejemplo es la denominada ofuscación, en la que un atacante altera intencionalmente sus características biométricas con el fin de impedir ser reconocido. Por último, se encuentran los ataques de *spoofing* que consisten en presentar un dato biométrico falso, como pueden ser dedos hechos de silicona o fotografías, para burlar el sistema. Con el propósito de mitigar estos ataques, se han diseñado medidas preventivas entre las que se puede citar el detector de vitalidad, que abarca el análisis de aspectos como el pulso, la sudoración o el desplazamiento de los ojos.

- **Módulos del sistema:** Los módulos que componen cualquier sistema biométrico desde el sensor hasta la toma de decisiones pueden verse alterados mediante el uso de un software maligno o, incluso, a través de la explotación de las vulnerabilidades derivadas de fallos en su diseño. Concretamente, un atacante podría implantar un troyano obligando al extractor de características a producir plantillas incorrectas que posibiliten un acceso indebido. Otra técnica es alterar el valor del umbral de tolerancia con el propósito de que todas las entradas se consideren legítimas. En otras palabras, estas ofensas tienen como finalidad amenazar la integridad del reconocimiento y son mitigados desarrollando exhaustivos test de calidad para los algoritmos utilizados.

- **Conexión entre los módulos:** Las vías de conexión entre los diversos bloques que forman el sistema son un blanco común para los atacantes. Por ejemplo, en el ataque conocido como *Man in the middle*, el objetivo es acceder a las comunicaciones entre estos módulos para alterar los datos que se intercambian, evitando que ninguno de los extremos lo descubran. Por otro lado, existen los *replay attack*, en los que un adversario podría disponer de los datos biométricos transferidos para, posteriormente, volverlos a reproducir. Este tipo de ataques pueden ser aplacados por medio de la implementación de un cifrado robusto, junto con un reconocimiento en tiempo real.

- **Bases de datos:** Las bases de datos constituyen un componente fundamental en estos sistemas y, por lo tanto, son extremadamente susceptibles a recibir ataques. Estas ofensas implican tanto la alteración de las plantillas, es decir, se reemplaza una válida por otra falsa, como el robo de las mismas con la intención de extraer los atributos biométricos. Estas últimas se utilizan para reproducir los rasgos mediante dedos o caretas artificiales para suplantar la identidad del individuo. En consecuencia, para preservar este componente es necesario aplicar una sólida encriptación de datos, además de implementar una base de datos descentralizada.

Como conclusión, la tecnología biométrica, si bien ofrece la promesa de transformar la manera en la que las personas se autentican, dista mucho de estar exenta de recibir ataques cibernéticos. Los errores humanos y las vulnerabilidades inherentes a la arquitectura de los sistemas, al igual que la creciente complejidad de los ataques que se llevan a cabo en la actualidad resaltan los riesgos asociados a su uso. Estas amenazas no solo comprometen la integridad de los datos, sino que, además, ponen en entredicho la credibilidad de una tecnología cuyo funcionamiento se fundamenta en un aspecto íntimo: nuestra identidad. No obstante, la comprensión de estos puntos débiles debería concebirse como una oportunidad desarrollar medidas de protección más robustas.

7.3. La privacidad: Un derecho esencial en la era digital

El marco normativo que rige el derecho a la privacidad en el contexto de las tecnologías biométricas representa un pilar imprescindible en la preservación de los derechos ante los desa-

fíos que se presentan ante el rápido progreso tecnológico experimentado en la última década. La privacidad, considerada un derecho intrínseco de la personalidad de cada persona, es clave para asegurar la protección de la información biométrica, que tiene una naturaleza distintiva y persistente en el tiempo.

En España, este derecho se fundamenta en el artículo 18 de la Constitución España que determina la protección de los datos personales y la garantía de los derechos digitales. Este artículo es desarrollado en la Ley Orgánica 3/2018 que, a su vez, se ajusta al Reglamento General de Protección de Datos dictaminado por la Unión Europea y vigente desde el año 2018. En él, se establece que es necesario someter a los datos biométricos a una protección más intensa, así como a controles estrictos respecto a su necesidad y proporcionalidad. De esta manera, su procesamiento únicamente es legal en ciertas circunstancias y contando siempre con la autorización expresa de la persona interesada. En el ámbito biométrico, la LOPDGDD instaura medidas complementarias, como la obligación de llevar a cabo valoraciones de impacto. Dichas evaluaciones tienen el objetivo de facilitar la identificación y reducción de potenciales infracciones. Por otro lado, el derecho europeo compele a las organizaciones que trabajen con sistemas biométricos a la implantación de mecanismos apropiados para resguardar esta información frente a posibles accesos no permitidos o usos inapropiados.

No obstante, el crecimiento vertiginoso que están experimentando las técnicas biométricas comporta la necesidad de llevar a cabo revisiones periódicas de la legislación al respecto. Esto es con la pretensión de evitar lagunas legales en cuestiones que empiezan a tomar forma actualmente, como son el reconocimiento en lugares públicos o el uso de la Inteligencia Artificial en estos sistemas biométricos, pues son situaciones que pueden dar lugar a vulneraciones de diversos derechos humanos y, concretamente, el derecho a la intimidad y privacidad, protagonista de este capítulo, se podría ver afectado desde numerosas perspectivas.

7.4. Impacto ético del uso del reconocimiento biométrico

Es indudable que la adopción de métodos de identificación biométrica innovadores, pese a ser indiscutiblemente valiosos en diversos campos, ha dado lugar a significativos debates morales sobre los límites de estas técnicas y su repercusión en la vida de los usuarios, pues estos sistemas no solo podrían tener un impacto negativo en la privacidad de las personas, sino que también influyen en aspectos como la igualdad o la libertad. No obstante, el estudio de estos efectos sobrepasa las cuestiones técnicas o jurídicas al ser un aspecto subjetivo que debe verse valorado por los propios usuarios, valoración que tiene su fundamento en las interacciones diarias con la tecnología, así como en los principios que reinan la moral de cada individuo.

Como ya se ha mencionado en numerosas veces, una de las preocupaciones éticas más importantes hoy en día es la vulnerabilidad que entraña la información biométrica. La inevitable imposibilidad de modificar este tipo de datos implica, en caso de uso indebido, serias consecuencias para las personas afectadas. ¿Qué ocurriría con nuestra libertad si no podemos tener control sobre la forma en que se usan nuestros rasgos más singulares?

Por otro lado, la aceptación de esta tecnología por parte de la sociedad difiere notablemente en función de cada país. Así, en naciones desarrolladas, como el caso de España, donde se dispone de una amplia legislación dirigida a proteger y asegurar los derechos fundamentales, existe una creciente desconfianza hacia su uso. Son cada vez más los usuarios que manifiestan su preocupación respecto a la posibilidad de que implante una vigilancia intrusiva. En cambio, en países tercermundistas estas técnicas son recibidas con entusiasmo al constituir un medio que brinda un acceso seguro a servicios básicos como son transacciones bancarias o votaciones electorales. Esta disparidad de opiniones destaca la magnitud ética que conlleva la utilización de estos sistemas.

Otra cuestión relevante sobre la implementación de estas técnicas es el incremento de la brecha social que estas pueden llegar a ocasionar. Según estudios recientes realizados por el NIST, los mecanismos de reconocimiento facial han demostrado tener sesgos demográficos en la identificación de individuos de determinadas etnias, como sería el caso de personas africanas o asiáticas [34]. Ello contribuiría a la generación de estereotipos y comportamientos discriminatorios en los ámbitos donde estos se utilizan. Adicionalmente, se ha puesto a prueba el concepto de la privacidad. La realidad es que actualmente es posible realizar una identificación masiva de personas en tiempo real [55], un hecho que difumina la frontera entre lo privado y lo público. En este contexto, surge el siguiente interrogante: ¿es posible conciliar el uso de las técnicas biométricas y la privacidad de los usuarios?

Esta reflexión debe finalizar remarcando la importancia de disponer de un marco legislativo que asegure la protección de los derechos humanos, así como evitar usos maliciosos de estas técnicas analizadas. No solo el desarrollo de las tecnologías biométricas, sino también su aplicación, debería llevarse a cabo cumpliendo los principios de transparencia y responsabilidad. Dicho en otras palabras, ¿qué tipo de sociedad queremos crear? ¿Una en la cual la tecnología nos ayude a ser más libres o una donde sea un obstáculo que la restrinja? Solo mediante un compromiso equilibrado entre lo ético y lo técnico se podrá garantizar que estos sistemas logren facilitar la vida a las personas de forma segura.

Capítulo 8

Conclusiones

8.1. Conclusiones

El objetivo principal de este proyecto consistía en investigar el estado de los sistemas modernos utilizados en la autenticación biométrica con la finalidad de precisar hasta qué punto estas tecnologías son capaces de reconocer de manera única y segura a un individuo. Por ello, a lo largo de las diversas etapas del estudio se ha analizado los progresos tecnológicos, además de los desafíos éticos, de aceptación social y los relativos a la protección de la privacidad que estos originan, consiguiendo, de esta manera, satisfacer los propósitos establecidos al inicio de este proyecto.

Inicialmente, el marco teórico permite al lector obtener una mayor comprensión de la biometría, pues en él se realiza una explicación de los conceptos básicos que se utilizan a lo largo del resto del estudio. Así, a través de este primer capítulo se ha conseguido definir la naturaleza de los datos biométricos de forma accesible. De igual forma, se ha logrado discernir sus propiedades más primordiales. Por lo tanto, se ha alcanzado con éxito el primer objetivo.

En lo referente a los apartados que analizan el reconocimiento de huellas digitales y rostros, se ha llevado a cabo un estudio comparativo de la evolución histórica de ambos métodos biométricos, profundizando en el progreso que han sufrido respecto a las técnicas más convencionales. De esta forma, se ha documentado de forma detallada el desarrollo tecnológico en los sensores de captura de datos biométricos, así como el funcionamiento de las técnicas de procesamiento de estos datos, junto con los sofisticados algoritmos de comparación patrones. Gracias a este análisis, se ha podido determinar que la exactitud de estos sistemas ha aumentado de manera significativa a causa de las constantes innovaciones en las técnicas utilizadas. No obstante, cada uno de estos métodos presentan debilidades concretas que se podrían resumir en: en relación con el reconocimiento de huellas dactilares, el desempeño podría verse influenciado por elementos externos, como el sudor en las yemas de los dedos o la colocación incorrecta del dedo en el sensor, mientras que en el reconocimiento facial, los inconvenientes generalmente están asocia-

dos con la distancia y el ángulo del rostro en la cámara, así como la gran variabilidad de las expresiones faciales que puede tener una persona. Asimismo, es importante señalar que también se observaron puntos débiles comunes a ambos métodos, entre los que se puede mencionar el margen de error existente en la precisión del reconocimiento debido a factores claves en este proceso, como la calidad de los datos adquiridos. Como consecuencia, se puede afirmar que se ha logrado cumplir tanto el segundo de los objetivos marcados, en concreto, la evaluación del desarrollo tecnológico en la captura y procesamiento de datos biométricos, sus mejoras y su fiabilidad, como el tercero, basado en el análisis de las fortalezas y debilidades de las técnicas de comparación de muestras biométricas.

Por otro lado, la evaluación de la implementación de este tipo de técnicas de autenticación en dispositivos con un sistema operativo Android ha evidenciado la simplicidad de su incorporación en el desarrollo de cualquier aplicación móvil. En especial, se ha demostrado que el uso de la API BiometricPrompt facilita a los desarrolladores integrar estos métodos de autenticación de manera segura. Por ende, el propósito número cuarto se da por satisfecho.

En lo que respecta a las amenazas de la biometría como método de reconocimiento, aspectos como la adquisición, conservación y tratamiento de la información biométrica sensible se han revelado como protagonistas de importantes riesgos que abarcan desde la filtración de datos, hasta la suplantación de identidad. Esto, junto con el hecho de que la efectividad de la biometría ocasionalmente no es perfecta, ha provocado que se generen dudas sobre su capacidad para integrarse en escenarios que requieren una máxima precisión en la autenticación. En lo que a esto respecta, si bien la biometría ha sido incorporada en campos como la supervisión en los aeropuertos o las finanzas, su utilización debe limitarse a situaciones que estén rigurosamente justificadas. Asimismo, es fundamental asegurar que la gestión del uso de este tipo de datos esté en poder de cada persona y no en manos de las organizaciones. Es por ello que se ha llegado a la conclusión de que las medidas de seguridad que se utilizan en la actualidad no en todas las ocasiones han resultado ser adecuadas para mitigar dichas amenazas, lo que enfatiza la relevancia de instaurar normativas rigurosas, además de emplear una perspectiva ética en el diseño de estos sistemas. Teniendo en cuenta todo lo mencionado anteriormente, se puede asegurar que se ha garantizado la consecución del quinto de los objetivos propuestos, relativo a la identificación de las amenazas y riesgos que derivan del uso de estas técnicas.

Es importante añadir las conclusiones que se han obtenido tomando en consideración la totalidad de esta investigación acerca del interrogante que ha guiado este proyecto desde su inicio y que ahora se recuerda: ¿Hasta qué punto las tecnologías de reconocimiento biométrico son capaces de identificar a un individuo de manera única y segura? En los últimos años, se ha demostrado que la biometría se presenta como una opción para autenticar a las personas de forma única, mucho más segura que los métodos tradicionales. No obstante, al igual que cualquier otro tipo de tecnología, las técnicas biométricas no están libres de tener vulnerabilidades. A pesar de su fiabilidad, siguen existiendo amenazas que deberán ser tratadas de forma adecuada. Por ello, los usuarios deben ser conscientes de estos peligros y estar dispuestos a aceptarlos dentro ciertos límites razonables.

Como última cuestión, personalmente este proyecto me ha brindado la posibilidad de utilizar los conocimientos que he ido obteniendo a lo largo de la carrera en el abordaje de esta

problemática tan significativa en el campo de la ciberseguridad. Además, he visto fortalecidas mi capacidad no solo de planificación, sino también de gestión de problemas derivados de un estudio de este calibre. Todo ello evidencia que la biometría forma parte de nuestro presente y que, indudablemente, su progreso continuará en un futuro, junto con otras técnicas emergentes. Por ello, es necesario seguir investigando sobre las mismas e impulsar su desarrollo, pues la tecnología debe ser capaz de adaptarse al dinamismo que gobierna nuestra sociedad.

8.2. Líneas futuras de investigación

El ámbito de la biometría es una parte de la tecnología que experimenta una evolución continua, teniendo que enfrentarse a retos tanto técnicos como éticos, lo que justifica la necesidad de desarrollar nuevas soluciones. Es por ello que en esta sección se enumeran algunas de las múltiples direcciones futuras que podría tomar este ámbito de estudio:

1. **Uso de la Inteligencia Artificial para detectar ataques de *spoofing* o *deepfakes*:** Las vulnerabilidades de las tecnologías biométricas que fundamentan su uso en las huellas dactilares ante ataques de suplantación es un problema crítico. Estos ataques, cuyo objetivo es conseguir acceso a través de la creación de muestras biométricas falsas como los dedos de silicona, son cada vez más sofisticados. En este contexto, la IA ha surgido como una nueva solución para minimizar la posibilidad de éxito de estos ataques, ya que se podrán diseñar nuevas técnicas para diferenciar entre muestras reales de aquellas que son falsas.

   Por otra parte, los *deepfakes* han supuesto un reto considerable para los desarrolladores de estos sistemas. Estos ataques utilizan imágenes o secuencias de vídeos ficticios extremadamente realistas para eludir la seguridad del sistema y obtener un acceso no autorizado. En este caso, la IA va a jugar un papel muy importante permitiendo identificar anomalías al llevar a cabo un análisis exhaustivo en las texturas, el color o los movimientos de este tipo de muestras.

2. **Modalidades biométricas avanzadas:** El futuro de la biometría no se reducirá a los métodos tradicionales, como las huellas digitales o el rostro. Existen nuevas modalidades emergentes, aunque todavía se encuentren en desarrollo, que pretenden incrementar el tipo de características que pueden utilizarse para autenticar a una persona de forma robusta, mejorando así la seguridad en aquellos escenarios que requieren un alto nivel de protección.

   Ritmo cardíaco: En los últimos años se ha estudiado la frecuencia y el ritmo de los latidos del corazón y se ha puesto en evidencia que existen singularidades en cada persona. Este nuevo método podría incorporarse en dispositivos como smartwatches, ampliamente usados actualmente en todo el mundo.

Olor: El aroma corporal de las personas ha sido investigado para poder comprobar en qué medida es identificable y consistente en el tiempo, haciendo una distinción de otro tipo de olores que provienen del uso de perfumes o jabones. Sin embargo, la utilización del olor necesita desarrollar complejos sistemas que sean capaces de detectar estos aromas para su análisis.

En conclusión, la biometría es un ámbito que actualmente se encuentra en continuo desarrollo, afrontando nuevos retos tanto técnicos como éticos que generan la necesidad de desarrollar soluciones innovadoras de forma constante. La implementación de estas perspectivas de investigación futuras promete aumentar de manera significativa la seguridad y la precisión del funcionamiento de los sistemas biométricos. Por todo ello, estas propuestas no solo reforzarán el proceso de reconocimiento, así como la protección de datos sensibles, sino que además darán lugar a nuevas oportunidades para la incorporación de la tecnología biométrica en distintos escenarios, contribuyendo a crear un futuro más seguro.

Glosario

A

amenazas

Circunstancia o evento con el potencial de impactar negativamente en las operaciones, activos o empleados de una organización a través de un sistema de información. Asimismo, es la probabilidad de explotar con éxito una vulnerabilidad particular de un sistema de información.. 4

atacante

Persona con acceso a información privilegiada, que actúa con intención maliciosa para comprometer un sistema.. 50

autenticación

Acción mediante la cual se demuestra a otra persona o sistema que un individuo es quien realmente dice que es, mediante un documento, una contraseña, rasgo biológico etc.. 2

B

biometría

Método de reconocimiento de personas basado en sus características fisiológicas o de comportamiento. Para la identificación del individuo es necesario que los rasgos o características analizadas sean de carácter universal, ser lo suficientemente distintas a las de otra persona, permanecer de forma constante e invariante en el individuo con el paso del tiempo y además, poder ser medida.. 1

C

confidencialidad

Principio esencial en la seguridad de la información que garantiza el nivel de secreto necesario de la información y de su tratamiento para protegerla contra su divulgación no autorizada durante su almacenamiento o transmisión.. 1

contramedidas

Medidas de protección establecidas para cumplir con los requisitos de seguridad, en términos de confidencialidad, integridad y disponibilidad, especificados para un sistema de información. Estas pueden incluir elementos de seguridad, restricciones de gestión, seguridad del personal y seguridad de las estructuras físicas, áreas y dispositivos.. 5

contraseña

Forma de autenticación de un usuario, a través de una clave secreta, para controlar el acceso a algún recurso o herramienta. En caso de que no se proporcione la clave correcta no se le permitirá el acceso a dichos elementos.. 2

crestas de fricción

Protuberancias que se desarrollan en la piel formando patrones únicos en los dedos y las palmas de las manos y los pies. Estas son responsables de la fricción que posibilita a las personas poder agarrar y manipular objetos con precisión.. 27

D

Deep Learning

Conjunto de algoritmos propios del *machine learning* que utilizan redes neuronales para simular el complejo proceso de toma de decisiones que lleva a cabo el cerebro humano. . 57

F

fiabilidad

Capacidad de un sistema o componente para funcionar en las condiciones establecidas durante un periodo de tiempo determinado.. 3

G

grafos

Diagrama que representa mediante puntos y líneas las relaciones entre pares de elementos y que se usa para resolver problemas lógicos, topológicos y de cálculo combinatorio.. 71

H

hackers

Persona que realiza actividades delictivas en la red contra personas o sistemas informáticos, pudiendo provocar daños económicos o reputacionales mediante el robo o exfiltración de información, deterioro de *software* o *hardware*, fraude y extorsión. Casi siempre se tratan de actos que están orientados a la obtención de fines económicos.. 20

huella latente

Huella imperceptible que se forma al tocar una superficie, producto de los residuos naturales de la piel como el sudor, los aceites y otros componentes. Para poder visualizar y analizar este tipo de huellas, generalmente se necesitan técnicas de revelado especializadas, como el uso de polvos, sustancias químicas o luz ultravioleta. Se utilizan comúnmente en investigaciones forenses para poder identificar a personas en lugares donde se ha producido un delito. Estas son tratadas para poder ser comparadas con los registros de huellas dactilares almacenadas en bases de datos, de manera que se puedan asociar con posibles sospechosos.. 51

I

identificación

Acción mediante la cual se le dice a otra persona o sistema quiénes somos.. 3

IEC

International Electrotechnical Commission. Se dedican al desarrollo y publicación de estándares internacionales para todas las tecnologías eléctricas, electrónicas y relacionadas. Estos campos se agrupan bajo el nombre de ”electrotecnología”.. 23

impacto

La magnitud del daño que cabe esperar como resultado de las consecuencias de la divulgación no autorizada de información, la modificación no autorizada de información, la destrucción no autorizada de información o la pérdida de información o de disponibilidad del sistema de información.. 26

INCIBE

Instituto Nacional de Ciberseguridad de España. 17

integridad

La seguridad de que los datos, ya sean personales o relativos a una organización, son precisos, completos, coherentes y confiables en todas las etapas de su ciclo de vida. Esto significa que la información permanece sin cambios, tanto si está en reposo como en movimiento, y no ha sido modificada por individuos no autorizados de manera accidental o intencional.. 1

intrusión

Acción realizada por un atacante de forma malintencionada para acceder a una red, sistema, dispositivo o aplicación sin autorización para poder obtener información confidencial o realizar actividades maliciosas. Pueden ocurrir de varias formas, como por ejemplo a través de malware, phishing, hacking o ingeniería social.. 50

ISO

International Organization for Standardization. Se dedican a la creación de normas o estándares para asegurar la calidad, seguridad y eficiencia de diversos productos y servicios.. 23

M

minucias

Particularidades únicas y específicas presentes en los patrones de las yemas de los dedos. Son esenciales para poder identificar huellas dactilares de distintas personas con gran precisión.. 16

mitigar

Proceso de implementación de medidas y estrategias para reducir el impacto o la probabilidad de que una amenaza o vulnerabilidad afecte a los sistemas de información y redes. 20

morfología

Área de la biología que estudia la forma de los seres orgánicos y las modificaciones o transformaciones que experimenta.. 27

P

polariza

Restringir en una dirección las vibraciones de una onda transversal, como la luz u otras radiaciones electromagnéticas.. 39

polímero

Compuesto químico, natural o sintético, formado por polimerización y que consiste fundamentalmente en unidades estructurales repetidas.. 39

R

riesgo

Medida del grado en que una entidad se ve amenazada por una circunstancia o evento, y suele ser en función de los impactos adversos que se producirían si el suceso ocurriera y la probabilidad de ocurrencia.. 10

ruido

Perturbación o señal anómala que se produce en los sistemas de transmisión de datos. Es decir, es todo tipo de señal que no fue enviada desde la fuente, pero, por estar presente dentro de la señal transmitida y con niveles perceptibles, perturba la recepción de ésta.. 22

S

sensor

Dispositivo que está capacitado para detectar acciones o estímulos externos y responder en consecuencia transmitiendo la información de forma adecuada. Estos mecanismos pueden transformar las magnitudes físicas o químicas en magnitudes eléctricas.. 24

sesión

Se produce cuando un usuario accede a un sistema o servicio. Durante la sesión, se establece una comunicación bidireccional permitiendo la transferencia de datos y la interacción con diferentes aplicaciones. Una sesión en el ámbito de redes informáticas, es el período de tiempo durante el cual se mantiene activa una conexión utilizando una capa de sesión de un protocolo de red. . 20

suplantación de identidad

Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o delito.. 19

U

usabilidad

Grado en que un producto puede ser utilizado por usuarios específicos para alcanzar objetivos concretos con eficacia, eficiencia y satisfacción en un contexto de uso específico.. 50

V

vulnerabilidad

Debilidad o fallo de un sistema que puede ser aprovechado con fines maliciosos. Normalmente mediante un programa que se denomina *exploit*. Cuando se descubre, el desarrollador del *software* o *hardware* lo solucionará publicando una actualización de seguridad del producto.. 20

Bibliografía

[1] Carlos J. Álvarez. «¿Por qué están aumentando los casos de ciberataque en España?» En: *Expansión* (mayo de 2024). [Online] (Última vez accedido: 18/06/2024). URL: https://www.expansion.com/empresas/2024/05/30/66584a5fe5fdeac9698b457f.html.

[2] Biometría. [Online] (Última vez accedido: 11/12/2024). URL: https://source.android.com/docs/security/features/biometric?hl=es.

[3] Medición de la seguridad de desbloqueo biométrico. [Online] (Última vez accedido: 07/12/2024). URL: https://source.android.com/docs/security/features/biometric/measure?hl=es.

[4] Cómo mostrar un diálogo de autenticación biométrica. [Online] (Última vez accedido: 10/12/2024). URL: https://source.android.com/docs/compatibility/cdd?hl=es.

[5] Biometric. [Online] (Última vez accedido: 07/12/2024). URL: https://developer.android.com/jetpack/androidx/releases/biometric?hl=es-419#1.1.0.

[6] Documento de definición de compatibilidad de Android. [Online] (Última vez accedido: 07/12/2024). URL: https://source.android.com/docs/compatibility/cdd?hl=es.

[7] Aratek. «Biometric Devices 101: Definition and Examples». En: *Aratek Biometric Post* (sep. de 2022). [Online] (Última vez accedido: 02/08/2024). URL: https://www.aratek.co/news/biometric-devices-definition-and-examples.

[8] Juan José Sánchez Arreseigor. «Las huellas dactilares, el arma perfecta de la policía para identificar personas». En: *Historia National Geographic* (mar. de 2020). [Online] (Última vez accedido: 02/08/2024). URL: https://historia.nationalgeographic.com.es/a/huellas-dactilares-arma-perfecta-policia-para-identificar-personas_12745.

[9] Team Asana. «¿En qué consiste un registro de riesgos? Guía para gerentes de proyectos». En: *Asana* (feb. de 2024). [Online] (Última vez accedido: 29/04/2024). URL: https://asana.com/es/resources/risk-register.

[10] Aselcom. «El futuro y las tendencias en ciberseguridad para 2024». En: *Aselcom* (ene. de 2024). [Online] (Última vez accedido: 06/04/2024). URL: https://aselcom.com/blog/actualidad/el-futuro-y-las-tendencias-en-ciberseguridad-para-2024.

[11] Grupo Atico34. «Datos biométricos y protección de datos RGPD». En: *Grupo Atico34* (jun. de 2024). [Online] (Última vez accedido: 18/06/2024). URL: https://protecciondatos-lopd.com/empresas/datos-biometricos-rgpd/.

[12] Implementing Biometric Authentication in Java Android. [Online] (Última vez accedido: 10/12/2024). URL: https://blog.atul-sharma.com/implementing-biometric-authentication-in-java-android-bf8aa2f4d762.

[13] Jeffery G. Barnes. «El Libro de Refencia de las Huellas Dactilares». En: ed. por Departamento de Justicia de los Estados Unidos. Instituto Nacional de Justicia. Cap. Historia.

[14] Bir Bhanu y Ajay Kumar. *Deep Learning for Biometrics. Advances in Computer Vision and Pattern Recognition*. Springer, ago. de 2017.

[15] Ayelet Biger-Levin. «Behavioral Biometrics vs Static Biometrics: Dynamic Fraud Detection Explained». En: *BioCatch Blog Channel* (oct. de 2020). [Online] (Última vez accedido: 09/05/2024). URL: https://www.biocatch.com/blog/behavioral-biometrics-vs-static-biometrics-fraud-detection.

[16] Biosys. «Sistemas biométricos». En: *Biosys* (dic. de 2023). [Online] (Última vez accedido: 09/05/2024). URL: https://www.biosys.es/sistemas-biometricos/#:~:text=Biometr%C3%ADa%20din%C3%A1mica%20(que%20recoge%20la,del%20paso%20y%20conducta%20gestual..

[17] European Data Protection Board. «Reconocimiento facial en aeropuertos: las personas deben tener el máximo control sobre los datos biométricos». En: *EDPB* (mayo de 2024). [Online] (Última vez accedido: 05/06/2024). URL: https://www.edpb.europa.eu/news/news/2024/facial-recognition-airports-individuals-should-have-maximum-control-over-biometric_es.

[18] Pablo Bobadilla. «Violación masiva de datos vinculada al reconocimiento facial: privacidad en riesgo». En: *Ciberprisma* (mayo de 2024). [Online] (Última vez accedido: 17/11/2024). URL: https://ciberprisma.org/2024/05/16/violacion-masiva-de-datos-vinculada-al-reconocimiento-facial-privacidad-en-riesgo/.

[19] Olivia López Bueno. «Reconocimiento facial: cómo nació de una tableta de la década del 60». En: *La Nación* (ago. de 2020). [Online] (Última vez accedido: 20/08/2024). URL: https://www.lanacion.com.ar/tecnologia/reconocimiento-facial-como-nacio-tableta-decada-del-nid2421334/.

[20] Raffaele Cappelli. «Unveiling the Power of Simplicity: Two Remarkably Effective Methods for Fingerprint Segmentation». En: *ResearchGate* (ene. de 2023). [Online] (Última vez accedido: 10/08/2024). URL: https://www.researchgate.net/publication/376729616_Unveiling_the_Power_of_Simplicity_Two_Remarkably_Effective_Methods_for_Fingerprint_Segmentation.

[21] CCN CERT. «Glosario - CCN CERT». En: *CCN CERT* (ago. de 2015). [Online] (Última vez accedido: 07/05/2024). URL: https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html.

[22] Christian Collado. «Versiones de Android: de la primera a la última versión del sistema operativo de Google». En: *La Vanguardia* (oct. de 2024). [Online] (Última vez accedido: 06/12/2024). URL: https://www.lavanguardia.com/andro4all/android/versiones-android-historia.

[23] Hillary Moses Daluz. *Fundamentals of Fingerprint Analysis*. Ed. por CRC Press. CRC Press, 2018.

[24] Asit Kumar Datta, Madhura Datta y Pradipta Kumar Banerjee. *Face Detection and Recognition: Theory and Practice*. Chapman y Hall/CRC, nov. de 2015.

[25] Laura Benito Díez. «Biometría para saber el sexo de los artistas de la Prehistoria». En: *LB Paleorama* (dic. de 2016). [Online] (Última vez accedido: 02/07/2024). URL: https://arqueologiaenred.paleorama.es/2016/12/biometria-para-saber-el-sexo-de-los.html.

[26] FinReg360. «La AEPD sanciona por requerir la huella dactilar como identificador de acceso». En: *FinReg360* (feb. de 2024). [Online] (Última vez accedido: 06/04/2024). URL: https://finreg360.com/alerta/la-aepd-sanciona-por-requerir-la-huella-dactilar-como-identificador-de-acceso/.

[27] Alex Suárez Font. «Clearview AI entregó 30.000 millones de fotos de Facebook y otras redes a la Policía en EE.UU.» En: *La Vanguardia* (abr. de 2023). [Online] (Última vez accedido: 06/04/2024). URL: https://www.lavanguardia.com/tecnologia/20230405/8876104/clearview-ai-entrego-30-000-millones-fotos-facebook-redes-policia.html.

[28] Blaine Frederick. «Why the future of biometrics must be privacy-first for widespread scaling and adoption». En: *Biometric Update* (oct. de 2024). [Online] (Última vez accedido: 17/11/2024). URL: https://www.biometricupdate.com/202410/why-the-future-of-biometrics-must-be-privacy-first-for-widespread-scaling-and-adoption.

[29] Mario Rodríguez García. «Reconocimiento parcial de huellas dactilares mediante Redes Neuronales Artificiales». Tesis de mtría. Universidad de Valladolid, 2017.

[30] Kanban Guides. «Kanban Guide en español». En: *Kanban Guides* (dic. de 2020). [Online] (Última vez accedido: 17/04/2024). URL: https://kanbanguides.org/enespanol/.

[31] Dmitry Gurendo. «Software Development Life Cycle (SDLC). All About Kanban Model». En: *XB Software* (jul. de 2015). [Online] (Última vez accedido: 17/04/2024). URL: https://xbsoftware.com/blog/software-development-life-cycle-sdlc-all-about-kanban/.

[32] Stanford Children's Health. «Anatomía de la piel». En: *Stanford Children's Health* (nov. de 2022). [Online] (Última vez accedido: 17/07/2024). URL: https://www.stanfordchildrens.org/es/topic/default?id=anatomy-of-the-skin-85-P04436.

[33] Javier Galbally Herrero. «Vulnerabilities And Attack Protection In Security Systems Based On Biometric Recognition». Tesis doct. Universidad Autónoma de Madrid, 2009.

[34] Aaron Holmes. «La tecnología de reconocimiento facial tiene sesgos raciales, según un nuevo estudio». En: *Business Insider* (dic. de 2019). [Online] (Última vez accedido: 30/11/2024). URL: https://www.businessinsider.es/tecnologia-reconocimiento-facial-tiene-sesgos-raciales-550473.

[35] INCIBE. «Biometría: amenazas, riesgos y vulnerabilidades». En: *INCIBE Blog* (mar. de 2024). [Online] (Última vez accedido: 07/05/2024). URL: https://www.incibe.es/empresas/blog/biometria-amenazas-riesgos-y-vulnerabilidades#:~:text=Dicho%20de%20otro%20modo%2C%20la,su%20forma%20de%20andar%2C%20etc..

[36] INCIBE. «Nadia Calviño destaca la contribución de INCIBE a posicionar España como el 4º país en ciberseguridad». En: *Sala de prensa INCIBE* (oct. de 2023). [Online] (Última vez accedido: 05/04/2024). URL: https://www.incibe.es/incibe/sala-de-prensa/nadia-calvino-destaca-la-contribucion-de-incibe-posicionar-espana-como-el-4o.

[37] INCIBE. «Tecnologías biométricas aplicadas a la ciberseguridad». En: *INCIBE* (2016). [Online] (Última vez accedido: 09/05/2024). URL: https://www.dcd.es/ebooks/guia_tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf.

[38] Adjabi Insaf y A. Ouahabi. «Past, Present, and Future of Face Recognition: A Review». En: *Research Gate* (jul. de 2020). [Online] (Última vez accedido: 20/08/2024). URL: https://www.researchgate.net/publication/343162886_Past_Present_and_Future_of_Face_Recognition_A_Review.

[39] Mordor Intelligence. «Tamaño del mercado de sensores de huellas dactilares y análisis de participación tendencias de crecimiento y pronósticos (2024-2029)». En: *Mordor Intelligence* (2024). [Online] (Última vez accedido: 02/07/2024). URL: https://www.mordorintelligence.com/es/industry-reports/global-fingerprint-sensor-market.

[40] ISO. «ISO/IEC 2382-37:2022 - Biometrics». En: *ISO* (mar. de 2022). [Online] (Última vez accedido: 28/06/2024). URL: https://www.iso.org/standard/73514.html.

[41] Anil K. Jain, Patrick Flynn y Arun A. Ross. *Handbook of Biometrics*. Ed. por Springer London Ltd. Springer London Ltd, 2007.

[42] Anil K. Jain, Arun A. Ross y Karthik Nandakumar. *Introduction to Biometrics*. Springer, nov. de 2011.

[43] Kelio. «Datos biométricos en la RGPD. ¿Es legal en 2024 fichar con biometría?» En: *Kelio Blog* (mar. de 2024). [Online] (Última vez accedido: 06/04/2024). URL: https://www.kelio.es/recursos/blog/465-datos-biometricos-en-rgpd-es-legal-2024-ficharcon-biometria.html.

[44] Stan Z. Li y Anil K. Jain. *Handbook of Face Recognition*. Springer, mar. de 2005.

[45] Gregg Lindemulder y Matt Kosinski. «¿Qué es la ciberseguridad?» En: *Think IBM* (ago. de 2024). [Online] (Última vez accedido: 05/04/2024). URL: https://www.ibm.com/es-es/topics/cybersecurity.

[46] Alice V. Maceo. «El Libro de Refencia de las Huellas Dactilares». En: ed. por Departamento de Justicia de los Estados Unidos. Instituto Nacional de Justicia. Cap. Anatomía y fisiología de la cresta de fricción en la piel adulta.

[47] Davide Maltoni et al. *Handbook of Fingerprint Recognition*. Ed. por Springer London Ltd. Springer London Ltd, 2009.

[48] Rubén Juste Meco. «Módulo de Identificación Biométrica Mediante Huellas Dactilares para Sistemas Empotrados». Tesis de mtría. Universidad Carlos III, 2010.

[49] Brendan Murphy. «Unit 4: Fingerprints 4.3 Classification of Fingerprints». En: *SlidePlayer* (2016). [Online] (Última vez accedido: 23/07/2024). URL: https://slideplayer.com/slide/10500160/.

[50] Fabio Natalucci, Mahvash S. Qureshi y Felix Suntheim. «Las crecientes amenazas cibernéticas, una grave preocupación para la estabilidad financiera». En: *IMF Blog* (abr. de 2024). [Online] (Última vez accedido: 21/04/2024). URL: https://www.imf.org/es/Blogs/Articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability.

[51] Laura Negro. ««Dejarte escanear el iris a cambio de criptomonedas es como vender tu alma al diablo»». En: *El Norte de Castilla* (mar. de 2024). [Online] (Última vez accedido: 06/04/2024). URL: https://www.elnortedecastilla.es/valladolid/dejarte-escanear-iris-cambio-criptomonedas-vender-alma-20240302195017-nt.html.

[52] Mohammad S. Obaidat, Issa Traore e Isaac Woungang. *Biometric-Based Physical and Cybersecurity Systems*. Ed. por Springer London Ltd. Springer London Ltd, 2018.

[53] Álvaro Olloqui. «España es uno de los países de Europa que más ciberataques sufre: pérdidas de 30.000 millones». En: *La Razón* (abr. de 2024). [Online] (Última vez accedido: 21/04/2024). URL: https://www.larazon.es/espana/espana-uno-paises-europa-que-mas-ciberataques-sufre-perdidas-30000-millones_202404196622859e8e6602000170ebc
html.

[54] Manuel G. Pascual. «La Policía española ya usa en sus investigaciones un sistema automático de reconocimiento facial». En: *El País* (mayo de 2024). [Online] (Última vez accedido: 19/08/2024). URL: https://elpais.com/tecnologia/2024-05-28/la-policia-espanola-ya-usa-en-sus-investigaciones-un-sistema-automatico-de-reconocimiento-facial.html.

[55] Manuel G. Pascual. «Los miedos de los expertos sobre el nuevo sistema de reconocimiento facial de la policía española: vigilancia masiva, pérdida de anonimato y borrado de datos». En: *El País* (ene. de 2023). [Online] (Última vez accedido: 30/11/2024). URL: https://elpais.com/tecnologia/2023-01-10/los-miedos-de-los-expertos-sobre-el-nuevo-sistema-de-reconocimiento-facial-de-la-policia-espanola-vigilancia-masiva-perdida-de-anonimato-y-borrado-de-datos.html.

[56] Sara Domínguez Pavón. «Reconocimiento facial mediante el Análisis de Componentes Principales (PCA)». Tesis de mtría. Universidad de Sevilla, 2017.

[57] PWC. «La IA generativa preocupa a una gran mayoría de consumidores, aunque el 50 % confía en ella para las tareas de menor riesgo». En: *Sala de prensa PWC* (jun. de 2024). [Online] (Última vez accedido: 18/06/2024). URL: https://www.pwc.es/es/sala-prensa/notas-prensa/2024/ia-generativa-preocupacion-consumidores.html.

[58] Li Qinjun. «Facial Recognition Technology: A Comprehensive Overview». En: *Francis Academic Press* (2023). [Online] (Última vez accedido: 21/08/2024). URL: https://francis-press.com/papers/11241.

[59] Christian Rathgeb et al. *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks*. Springer, ene. de 2022.

[60] *Reconocimiento facial tridimensional*. [Online] (Última vez accedido: 11/10/2024). 2021. (Visitado 01-09-2024).

[61] Marcos Rodrigues y Lyuba Alboul. «3D modelling and recognition». En: *Research Gate* (2006). [Online] (Última vez accedido: 10/11/2024). URL: https://www.researchgate.net/publication/228960393_3D_modelling_and_recognition.

[62] Trinidad Rodríguez. «Worldcoin y el escándalo del escaneo de iris en España: cotiza en máximos históricos». En: *20 Minutos* (mar. de 2024). [Online] (Última vez accedido: 06/04/2024). URL: https://www.20minutos.es/tecnologia/actualidad/cuanto-vale-worldcoin-espana-escaneo-iris-5226624/.

[63] Bhaskar S. «What is Kanban? A Beginner's Guide!» En: *Nimblework* (abr. de 2024). [Online] (Última vez accedido: 30/04/2024). URL: https://www.nimblework.com/kanban/what-is-kanban/.

[64] J. M. Sadurní. «La dactiloscopia, la ciencia de las huellas dactilares». En: *Historia National Geographic* (ago. de 2021). [Online] (Última vez accedido: 04/07/2024). URL: https://historia.nationalgeographic.com.es/a/dactiloscopia-ciencia-huellas-dactilares_17133.

[65] Gustavo Francisco Sanz. «Desarrollo de un Sistema de Reconocimiento de Huella Dactilar Para Apicaciones Match-On-Card». Tesis de mtría. Universidad Autónoma de Madrid, jul. de 2009.

[66] Internacional Organization for Standardization. «ISO/IEC 19794-1:2011». En: *ISO* (2024). [Online] (Última vez accedido: 28/06/2024). URL: https://www.iso.org/standard/50862.html.

[67] Internacional Organization for Standardization. «ISO/IEC 24745:2022». En: *ISO* (2022). [Online] (Última vez accedido: 28/06/2024). URL: https://www.iso.org/standard/75302.html.

[68] Internacional Organization for Standardization. «ISO/IEC 30107-1:2023». En: *ISO* (2023). [Online] (Última vez accedido: 28/06/2024). URL: https://www.iso.org/standard/83828.html.

[69] National Institute of Standards y Technology. «Glossary - CSRC - NIST Computer Security Resource Center». En: *NIST* (abr. de 2024). [Online] (Última vez accedido: 07/05/2024). URL: https://csrc.nist.gov/glossary/term/biometrics.

[70] StatCounter. «Mobile operating system market share worldwide». En: *StatCounter GlobalStats* (jun. de 2024). [Online] (Última vez accedido: 06/12/2024). URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202406-202406-map.

[71] Anastasia Stsepanets. «Gestión de riesgos en un proyecto: todo lo que debería saber iniciando y realizando proyectos». En: *GanttPRO Project Management Blog* (jul. de 2023). [Online] (Última vez accedido: 29/04/2024). URL: https://blog.ganttpro.com/es/planificacion-gestion-riesgos-proyecto/.

[72] Matthew Turk y Alex Pentland. «Eigenfaces for Recognition». En: *MIT Press* (1991). [Online] (Última vez accedido: 31/10/2024). URL: https://direct.mit.edu/jocn/article/3/1/71/3025/Eigenfaces-for-Recognition.

[73] Universidad de Valladolid. «Guía docente del trabajo de fin de grado (Mención en Tecnologías de la Información)». En: *UVa* (sep. de 2023). [Online] (Última vez accedido: 24/04/2024). URL: https://apps.stic.uva.es/guias_docentes/uploads/2023/545/46977/1/Documento.pdf.

[74] Viafirma. «¿Qué es la seguridad biométrica?» En: *Viafirma* (nov. de 2021). [Online] (Última vez accedido: 05/06/2024). URL: https://www.viafirma.com/es/seguridad-biometrica/.

[75] Kasey Wertheim. «El Libro de Refencia de las Huellas Dactilares». En: ed. por Departamento de Justicia de los Estados Unidos. Instituto Nacional de Justicia. Cap. Embriología y morfología de la piel de las crestas de fricción.

[76] Matt Williams. «NordVPN: How to Protect Biometric Data from Cybercriminals». En: *MVPro Media* (ago. de 2023). [Online] (Última vez accedido: 06/04/2024). URL: https://mvpromedia.com/nordvpn-how-to-protect-biometric-data-from-cybercriminals/.