Sistema Inteligente De Reconocimiento Facial En Aerolíneas Usando CRISP-DM, Teoría de Autómatas y Programación Paralela Como Apoyo a La Seguridad y El Flujo de Pasajeros

Autor(es): Andres Mauricio Jaimes

1093589017

Brayan Danilo Sánchez Monroy

1091965055

Jorge Eduardo Ibarra Páez

1004903848

Informe presentado para aprobación curso Fundamentos de Ciencia de Datos

Universidad de Pamplona

Facultad de Ingenierías y Arquitectura

Ingeniería de Sistemas

2024

Villa del Rosario – Norte de Santander

**RESUMEN**

Este proyecto propone el desarrollo de un sistema de reconocimiento facial diseñado para aerolíneas, cuyo objetivo principal es optimizar los procesos de seguridad y el flujo de pasajeros. Basado en la metodología CRISP-DM, el estudio aborda la integración de técnicas avanzadas de visión por computadora, teoría de autómatas y programación paralela para la identificación biométrica rápida y precisa. La implementación de este sistema busca reducir el tiempo de espera y mejorar la experiencia del pasajero, aumentando a su vez la seguridad aeroportuaria. Se utilizarán datos biométricos obtenidos de bases públicas y capturados en tiempo real, procesados mediante redes neuronales convolucionales. Este enfoque también incorpora estrategias de limpieza y etiquetado de datos, asegurando la calidad y fiabilidad del modelo. Los resultados esperados incluyen un software escalable capaz de integrarse con sistemas de gestión de pasajeros y operar bajo condiciones exigentes de seguridad, promoviendo una operación más eficiente y segura en las aerolíneas.

Palabras clave: reconocimiento facial, CRISP-DM, aerolíneas, seguridad, flujo de pasajeros.

Contenido

[INTRODUCCION 5](#_Toc183353798)

[CAPÍTULO I 7](#_Toc183353799)

[1. EL PROBLEMA 7](#_Toc183353800)

[1.1 Planteamiento del Problema 7](#_Toc183353801)

[1.2 Formulación del Problema 9](#_Toc183353802)

[1.3 Objetivos 10](#_Toc183353803)

[1.3.1 Objetivo General del Proyecto 10](#_Toc183353804)

[1.3.2 Objetivos Específicos 10](#_Toc183353805)

[1.4 Justificación 11](#_Toc183353806)

[CAPITULO II 13](#_Toc183353807)

[2. ESTADO DEL ARTE 13](#_Toc183353808)

[2.1 Antecedentes 13](#_Toc183353809)

[2.2 Marco Referencial 17](#_Toc183353810)

[2.3 Marco Teórico 47](#_Toc183353811)

[2.4 Marco Conceptual 48](#_Toc183353812)

[2.5 Marco Legal 49](#_Toc183353813)

[CAPITULO III 51](#_Toc183353814)

[3. Metodología 51](#_Toc183353815)

[3.1 Fases de la Metodología 51](#_Toc183353816)

[3.2 Fases Detalladas 52](#_Toc183353817)

[3.3 Técnica de Programación Paralela 55](#_Toc183353818)

[3.4 Datos y Origen de los mismos 55](#_Toc183353819)

[3.5 Herramientas 60](#_Toc183353820)

[CAPITULO IV 61](#_Toc183353821)

[4. Análisis e Interpretación de Resultados 61](#_Toc183353822)

[4.1 Desarrollo e Interfaz Grafica 70](#_Toc183353823)

[CAPITULO V 86](#_Toc183353824)

[5. Conclusiones 86](#_Toc183353825)

[6. Bibliografía 88](#_Toc183353826)

# INTRODUCCION

El presente proyecto se centra en el desarrollo de un sistema de reconocimiento facial diseñado específicamente para su implementación en el ámbito de las aerolíneas. El propósito principal es optimizar los procesos de seguridad y agilizar el flujo de pasajeros mediante la automatización de la identificación biométrica.

Diversos estudios han demostrado que la implementación de sistemas de reconocimiento facial en entornos aeroportuarios puede reducir drásticamente los tiempos de espera en los controles de seguridad y facilitar la identificación de posibles amenazas. Como lo señalan Kumar, Singh y Singh (2021), "el reconocimiento facial ha demostrado ser una herramienta eficaz para mejorar la seguridad en los aeropuertos, al reducir significativamente el tiempo de procesamiento de los pasajeros y la tasa de falsos positivos" (p. 1). Asimismo, Zheng, Liu y Kan (2019) proponen un sistema de reconocimiento facial con alta precisión y robustez, demostrando el potencial de esta tecnología en entornos de vigilancia (Zheng, Liu, & Kan, 2019).

Más allá de los beneficios en términos de seguridad, el reconocimiento facial también puede mejorar significativamente la experiencia del pasajero. Al automatizar los procesos de identificación, se reducen las colas y los tiempos de espera, lo que se traduce en una mayor satisfacción de los viajeros.

Los procesos de identificación manual, basados en documentos, son lentos y propensos a errores. Este proyecto busca resolver este problema mediante el desarrollo de un sistema automatizado de reconocimiento facial que permita agilizar los procesos de embarque y control de acceso, al tiempo que se refuerzan los protocolos de seguridad.

Para desarrollar el sistema de reconocimiento facial, se seguirá la metodología CRISP-DM. Iniciamos comprendiendo las necesidades específicas de las aerolíneas y las regulaciones vigentes. Luego, recopilaremos y analizaremos datos biométricos de los pasajeros para entrenar nuestro modelo. Estos datos serán limpiados y preparados para garantizar su calidad. A continuación, desarrollaremos y entrenaremos modelos de reconocimiento facial, utilizando técnicas avanzadas como las redes neuronales convolucionales. Una vez entrenado el modelo, lo evaluaremos en condiciones reales para medir su precisión y confiabilidad. Finalmente, integraremos el sistema en los procesos existentes de la aerolínea, poniendo en marcha nuestra solución.

Para el entrenamiento y evaluación del sistema se utilizarán bases de datos de imágenes faciales de alta calidad, obtenidas de bases de datos públicas. Estos datos serán etiquetados manualmente para garantizar su precisión y consistencia.

El alcance de este proyecto abarca el desarrollo de un sistema de reconocimiento facial completo, desde la captura de imágenes faciales hasta la generación de alertas en caso de detección de una coincidencia. El producto final será un software escalable y adaptable, capaz de integrarse con diferentes sistemas de gestión de pasajeros y de operar en entornos de alta seguridad.

# CAPÍTULO I

# EL PROBLEMA

## Planteamiento del Problema

El reconocimiento facial se ha posicionado como una tecnología disruptiva con un potencial transformador en múltiples sectores. En el ámbito aeroportuario, su implementación promete agilizar los procesos de embarque, mejorar la seguridad y optimizar la experiencia del pasajero. Diversos estudios respaldan esta afirmación. Por ejemplo, según Kumar, Singh y Singh (2021), la adopción de sistemas de reconocimiento facial en aeropuertos ha demostrado reducir significativamente los tiempos de espera en los controles de seguridad, lo que se traduce en una mayor satisfacción de los usuarios. Asimismo, Zheng, Liu y Kan (2019) señalan que esta tecnología puede contribuir a la detección temprana de posibles amenazas, fortaleciendo así los protocolos de seguridad en entornos aeroportuarios.

Actualmente, los procesos de identificación en los aeropuertos se basan en gran medida en la verificación manual de documentos de identidad. Este método es susceptible a errores humanos, es lento y puede generar largas filas, lo que afecta negativamente la experiencia del pasajero. Si bien algunas aerolíneas han comenzado a implementar sistemas de reconocimiento facial, su adopción aún es limitada y no se ha generalizado en la industria.

La falta de un sistema de reconocimiento facial eficiente y ampliamente implementado en las aerolíneas genera una serie de problemas, como: Retrasos en los procesos de embarque; Las verificaciones manuales son lentas y generan cuellos de botella, especialmente en horas pico. Mayor riesgo de errores humanos; La verificación manual de documentos es propensa a errores, lo que puede llevar a la identificación errónea de pasajeros. Experiencia del pasajero deficiente; Las largas filas y los retrasos generan frustración y molestia en los viajeros. Vulnerabilidad a la seguridad; La verificación manual puede facilitar la suplantación de identidad y otros tipos de fraude.

Como afirma Kumar, Singh y Singh (2021), "la implementación de sistemas de reconocimiento facial en aeropuertos ha demostrado ser una herramienta eficaz para mejorar la seguridad y la eficiencia operativa". Nuestro proyecto se alinea con esta visión, buscando desarrollar una solución tecnológica que contribuya a transformar la experiencia de viaje en las aerolíneas.

El presente proyecto busca abordar la problemática de la ineficiencia y la falta de seguridad en los procesos de identificación de pasajeros en los aeropuertos, mediante el desarrollo de un sistema de reconocimiento facial innovador y robusto. Se plantea la necesidad de diseñar una solución que permita agilizar los procesos de embarque, reducir los errores humanos, mejorar la experiencia del pasajero y fortalecer los protocolos de seguridad, todo ello sin comprometer la privacidad de los usuarios.

## Formulación del Problema

¿Cómo puede un sistema de reconocimiento facial, desarrollado mediante la integración de CRISP-DM, Teoría de Autómatas y Programación Paralela, optimizar los procesos de seguridad y agilizar el flujo de pasajeros en las aerolíneas, ¿mejorando así la experiencia del viajero y fortaleciendo los protocolos de seguridad?

## Objetivos

### Objetivo General del Proyecto

Desarrollar un sistema de reconocimiento facial automatizado en aerolíneas usando CRISP-DM, Teoría de Autómatas y Programación paralela como apoyo a la seguridad y el flujo de pasajeros.

### Objetivos Específicos

Investigar los aspectos técnicos funcionales y éticos de las aerolíneas en la región haciendo énfasis en el tiempo requerido para cada uno de estos procesos identificando las falencias existentes.

Seleccionar las tecnologías y recursos necesarios para desarrollar el sistema de reconocimiento facial, basándose en la investigación y los requisitos definidos en el primer objetivo específico.

Desarrollar el sistema de reconocimiento facial de acuerdo con las especificaciones y tecnologías seleccionadas, implementando las funcionalidades requeridas para optimizar la seguridad y el flujo de pasajeros.

Evaluar el desempeño y la efectividad del sistema de reconocimiento facial mediante pruebas y análisis, asegurando que cumpla con los objetivos de optimización de seguridad y flujo de pasajeros.

## Justificación

Desde el punto de vista social, la implementación de un sistema inteligente de reconocimiento facial en aerolíneas responde a una creciente demanda social por mayor seguridad y eficiencia en los viajes aéreos. La sociedad actual busca soluciones tecnológicas que agilicen los procesos, reduzcan las filas y minimicen los riesgos de seguridad. Este proyecto se alinea con estas expectativas, ofreciendo una alternativa innovadora que contribuye a mejorar la experiencia del pasajero y a fortalecer los protocolos de seguridad en un contexto donde los actos terroristas y la delincuencia organizada son una preocupación constante. Además, el reconocimiento facial puede facilitar la identificación de personas buscadas, contribuyendo así a la seguridad nacional.

Desde el punto de vista académico, este proyecto se enmarca en una línea de investigación activa y en constante evolución, que busca desarrollar soluciones tecnológicas basadas en inteligencia artificial para resolver problemas del mundo real. La aplicación del reconocimiento facial en el ámbito aeroportuario representa un desafío académico interesante, ya que implica la integración de diversas disciplinas como la visión por computador, el aprendizaje automático, la ingeniería de software y la seguridad informática. Además, este proyecto puede generar nuevas preguntas de investigación y contribuir al avance del conocimiento en áreas como la biometría, la privacidad y la ética de la inteligencia artificial.

Desde el punto de vista metodológico, el proyecto propone una metodología rigurosa basada en CRISP-DM, que garantiza un enfoque sistemático y estructurado para el desarrollo del sistema. La utilización de la teoría de autómatas permite modelar de manera formal los procesos de reconocimiento facial y facilita la identificación de posibles errores o ineficiencias. Por otro lado, la programación paralela es esencial para procesar grandes volúmenes de datos de manera eficiente y en tiempo real, lo que es fundamental para aplicaciones como el reconocimiento facial en entornos dinámicos como los aeropuertos.

Desde el punto de vista práctico, la implementación de un sistema de reconocimiento facial en aerolíneas tiene un gran potencial para mejorar la eficiencia operativa y reducir costos. Al automatizar los procesos de identificación, se pueden reducir significativamente los tiempos de espera en los controles de seguridad, lo que permite a las aerolíneas aumentar su capacidad y mejorar la satisfacción de los pasajeros. Además, este sistema puede contribuir a prevenir el fraude y la suplantación de identidad, protegiendo así los activos de las aerolíneas y la seguridad de los pasajeros.

Desde el punto de vista de la línea de investigación, este proyecto se inscribe en una línea de investigación que busca desarrollar sistemas inteligentes capaces de interactuar con el mundo real de manera autónoma y eficiente. El reconocimiento facial es una de las tecnologías clave en este campo, y su aplicación en el ámbito aeroportuario representa un caso de estudio interesante para evaluar el desempeño de estos sistemas en entornos complejos y dinámicos.

# CAPITULO II

# ESTADO DEL ARTE

## Antecedentes

En el proyecto titulado "Aplicación de machine learning en un aeropuerto: reconocimiento facial y gestión de colas", el autor Víctor Piñón Rattia explora la implementación de algoritmos de aprendizaje automático para mejorar la eficiencia en aeropuertos. El estudio se enfoca en dos aplicaciones principales: el reconocimiento facial y la predicción del tiempo de espera en colas. Para el reconocimiento facial, se compararon dos enfoques, uno basado en edge computing y otro en computación en la nube usando la API de Face de Azure. Ambas opciones fueron implementadas en una Raspberry Pi para evaluar diferencias en tiempo de procesamiento y consumo energético. Los resultados mostraron que el modelo basado en la nube superó al modelo edge tanto en precisión de reconocimiento como en eficiencia energética, siendo la opción preferida en escenarios con conexión a internet estable.

En cuanto a la gestión de colas, se desarrolló una herramienta que predice los tiempos de espera utilizando datos públicos históricos. Se compararon varios algoritmos de aprendizaje automático para determinar cuál ofrecía los mejores resultados, optimizando finalmente el más efectivo. Los hallazgos fueron prometedores, sugiriendo que la implementación de esta tecnología podría mejorar significativamente la experiencia del usuario en los aeropuertos, reduciendo tiempos de espera y optimizando la asignación de recursos. Este proyecto demuestra el potencial de las tecnologías de machine learning para abordar problemas de gestión y logística en el entorno aeroportuario, proponiendo un avance significativo hacia la automatización y eficiencia en la industria de la aviación.

El artículo "Estrategia de innovación y transformación digital para optimizar el aeropuerto de Bilbao" se centra en implementar tecnologías avanzadas para mejorar la eficiencia y experiencia del pasajero en el aeropuerto de Bilbao. El estudio destaca el uso de la automatización y el Internet de las Cosas (IoT) como pilares fundamentales para esta transformación digital. Mediante la implementación de sensores inteligentes y sistemas automatizados, se busca optimizar la gestión de recursos y operaciones aeroportuarias, incluyendo el manejo de equipajes y la gestión de flujos de pasajeros. La digitalización de procesos es vista no solo como un medio para mejorar la eficiencia operativa, sino también como una herramienta para ofrecer una experiencia de usuario más ágil y satisfactoria, reduciendo los tiempos de espera y facilitando el acceso a información en tiempo real.

Además, el proyecto enfatiza la importancia de una conectividad intermodal eficiente, integrando el aeropuerto con otros sistemas de transporte para facilitar el movimiento de pasajeros. La implementación de soluciones de inteligencia artificial y análisis de datos permite prever picos de demanda y ajustar los recursos en consecuencia, mejorando así la planificación y respuesta operativa. Se considera esencial el uso de plataformas digitales que permitan a los pasajeros realizar un seguimiento de su viaje y acceder a servicios personalizados. Este enfoque integral no solo busca optimizar las operaciones internas del aeropuerto, sino también mejorar la conectividad y experiencia general del pasajero, posicionando al aeropuerto de Bilbao como un referente en innovación tecnológica en la industria aeronáutica.

El artículo titulado "Estrategia para la implementación de herramientas con reconocimiento facial en los Sistemas Integrados de Emergencias y Seguridad (SIES)" explora la viabilidad de integrar tecnologías de reconocimiento facial en sistemas de videovigilancia en Colombia para mejorar la seguridad ciudadana. El estudio destaca que, aunque en Colombia ya existen numerosas cámaras de seguridad, tanto públicas como privadas, su integración y uso efectivo para reconocimiento facial aún están en desarrollo. Se sugiere que la implementación de esta tecnología puede optimizar la gestión de recursos humanos y mejorar la eficacia en la identificación y captura de personas de interés. El estudio se basa en experiencias internacionales de países como China, Emiratos Árabes Unidos y Reino Unido, donde estas tecnologías han demostrado su utilidad en diversos contextos de seguridad.

El documento subraya la necesidad de un marco regulatorio claro que permita el uso adecuado de estas tecnologías, respetando la privacidad y los derechos de los ciudadanos. En particular, se resalta la importancia de establecer normativas para la gestión de datos y la protección de la privacidad, inspirándose en modelos europeos y americanos. Además, se propone que las autoridades locales y nacionales colaboren para la financiación y despliegue de estas herramientas, integrando tanto cámaras de vigilancia públicas como privadas en un sistema unificado que pueda ser utilizado por la Policía Nacional. Este enfoque permitiría una respuesta más rápida y eficiente ante incidentes de seguridad, fortaleciendo el servicio de policía y mejorando la seguridad en áreas urbanas y rurales de Colombia.

El artículo "Digitalización y automatización en el aeropuerto El Dorado" examina las estrategias y tecnologías implementadas para optimizar la gestión de operaciones y mejorar la experiencia de los pasajeros en este aeropuerto colombiano, especialmente a raíz de los desafíos presentados por la pandemia de COVID-19. Entre las medidas destacadas se encuentran la adopción de tecnologías de Big Data y sistemas de monitoreo en tiempo real para analizar el flujo de pasajeros y predecir aglomeraciones, permitiendo una respuesta rápida y eficiente para mejorar la movilidad y reducir tiempos de espera. Se enfatiza la necesidad de digitalización a través del uso de sensores de movimiento, cámaras de alta definición y quioscos de auto-servicio, que permiten una mayor automatización y autosuficiencia en procesos como el check-in y el despacho de equipaje.

El estudio también menciona la implementación de sistemas de autogestión de equipaje, lo cual reduce significativamente las filas y tiempos de espera, y el control de migración automático mediante tecnologías biométricas y códigos QR. Estas innovaciones buscan no solo cumplir con las normativas de bioseguridad sino también mejorar la eficiencia operativa y la satisfacción del pasajero. La integración de estas tecnologías convierte al aeropuerto El Dorado en un modelo a seguir para la modernización aeroportuaria en la región, mostrando cómo la adopción de soluciones digitales puede transformar la infraestructura y operaciones tradicionales en sistemas más ágiles, seguros y centrados en el usuario.

El artículo “Tecnología de reconocimiento facial y sus riesgos en los derechos humanos” aborda la tensión entre la implementación de tecnologías de reconocimiento facial impulsadas por inteligencia artificial y los derechos fundamentales garantizados en el sistema de derechos humanos. A través de un análisis cualitativo-inductivo de diversas fuentes, estudios de caso y legislaciones, se examina cómo los sistemas de visión artificial utilizados en estas herramientas interactúan con el derecho penal, especialmente en las etapas de indagación e investigación. Los hallazgos revelan que el uso de reconocimiento facial en estas etapas del proceso penal plantea riesgos significativos para las garantías de un debido proceso y el principio de no discriminación.

## Marco Referencial

A continuación, se presentan los estudios previos que sirven como referencia para abordar los desafíos actuales en el reconocimiento facial. En 2021, Alfattama, Kanungo y Bisoy desarrollaron una solución innovadora para mejorar los sistemas de reconocimiento facial ante la creciente problemática de la autenticación facial en entornos donde las personas usaban mascarillas, un reto que se intensificó durante la pandemia de COVID-19. Su enfoque se basó en el uso de los modelos MTCNN y VGGF, los cuales permitieron optimizar el reconocimiento facial en imágenes parcialmente ocluidas, logrando una precisión del 90% en rostros donde solo se capturaba la mitad superior. Esta mejora es especialmente relevante en aplicaciones de seguridad en aeropuertos y otros lugares públicos, donde la identificación de los usuarios se veía afectada por las mascarillas, poniendo de relieve la importancia de adaptar estos sistemas a nuevas condiciones de uso para mantener su eficacia y fiabilidad.

En 2021, Raiu, Vidyasree y Patel presentaron un enfoque innovador para mejorar la precisión de los sistemas biométricos multimodales en el contexto de la identificación de pasajeros en aeropuertos, especialmente ante los desafíos derivados de la pandemia de COVID-19. Dado que el uso de mascarillas dificulta el reconocimiento facial, propusieron una solución que combina rasgos biométricos contactless, como el iris y las huellas dactilares. Utilizando técnicas avanzadas de aprendizaje profundo, como el autoencoder esparso, lograron reducir la dimensionalidad de los datos extraídos, lo que mejora tanto la precisión como la eficiencia del sistema. Esta propuesta busca no solo fortalecer la seguridad de los pasajeros, sino también fomentar un viaje más seguro y eficiente en un entorno donde la demanda de seguridad y fluidez en los terminales aéreos sigue creciendo.

En 2021, Arafah, Achmad, Indrabayu y Areni llevaron a cabo una investigación enfocada en la identificación facial en personas que usan velo, un escenario relevante en la seguridad aeroportuaria, especialmente para el rastreo de sospechosos de terrorismo. Utilizando imágenes obtenidas a través de cámaras de CCTV en áreas de inspección de pasajeros, aplicaron técnicas avanzadas de procesamiento de imágenes como el método Histogram of Oriented Gradients (HOG) para la extracción de características y el algoritmo Multi-class Support Vector Machine (MSVM) para la clasificación. A pesar de las oclusiones causadas por el velo, el sistema alcanzó un 75.08% de precisión. Este estudio destaca la importancia de mejorar los algoritmos de reconocimiento facial en situaciones donde parte del rostro está cubierto, especialmente en contextos críticos como la seguridad aeroportuaria.

En 2021, Sehrawat presentó un análisis detallado sobre el uso de patrones de iris como un medio infalible para la identificación en el ámbito forense. En su artículo, destaca cómo el reconocimiento biométrico, basado en características individuales como el iris, ha demostrado ser altamente eficaz en contextos de alta seguridad, como aeropuertos y centrales nucleares. Debido a su unicidad y dificultad para ser replicado, el iris se ha posicionado como una herramienta esencial en sistemas biométricos que buscan asegurar el acceso solo a personas autorizadas. Esta tecnología no solo mejora la seguridad, sino que también tiene aplicaciones importantes en la identificación de intrusos en instalaciones críticas. El trabajo de Sehrawat subraya tanto las ventajas como las limitaciones actuales de esta técnica y sus futuras aplicaciones en el campo forense.

En 2021, Maheswari, Aluvalu y Chennam exploraron el uso de algoritmos de aprendizaje automático para el análisis de expresiones faciales, un campo con aplicaciones en medicina, educación, entretenimiento y análisis forense. El análisis de expresiones faciales se realiza después del reconocimiento facial y depende de la extracción eficiente de características faciales. El uso de algoritmos de aprendizaje automático y profundo ha demostrado ser crucial para clasificar y analizar de manera precisa las expresiones, especialmente en entornos donde no es posible la comunicación verbal. Este estudio discute cómo los algoritmos de ML y DL pueden aplicarse a imágenes y videos, y cómo el análisis de expresiones es fundamental en áreas como la interacción humano-computadora y el comportamiento humano en zonas de alta concurrencia, como los aeropuertos. Además, se hace un análisis comparativo de algoritmos supervisados y no supervisados para la clasificación de imágenes y su efectividad en la recuperación de datos de bases de imágenes faciales.

En 2021, Stevens presentó un análisis sobre la identificación de personas en aeropuertos durante el control de pasaportes, destacando el desarrollo de estándares internacionales interoperables para documentos de viaje y los avances tecnológicos que facilitan el procesamiento rápido y efectivo de la información de los pasajeros. Este trabajo pone especial énfasis en los desafíos actuales que enfrentan los controles fronterizos debido a la amenaza de impostores de identidad y el uso creciente de la tecnología de reconocimiento facial en los puntos de Control Fronterizo Automatizado (ABC). Aunque la tecnología ha avanzado considerablemente, Stevens subraya que el papel del personal humano sigue siendo crucial en la verificación de la identidad y nacionalidad de los viajeros, lo que implica una adecuada selección, formación y monitoreo del desempeño de estos trabajadores.

En 2021, Rakib et al. presentaron un marco seguro denominado DeepHealth, diseñado para gestionar certificados de salud mediante el uso de IoT médico, blockchain y aprendizaje profundo. Este sistema fue desarrollado en respuesta a la necesidad de reducir la transmisión del COVID-19, proporcionando una solución para monitorear el estado de salud de las personas y generar certificados seguros basados en su estado diario. El marco incluye almacenamiento biométrico de usuarios, utilizando blockchain para asegurar los datos y un sistema de reconocimiento facial basado en aprendizaje profundo, en el que las características faciales se vinculan a un código QR que contiene el estado de salud del usuario. El sistema permite a supermercados, centros comerciales y aeropuertos consultar el estado de salud de las personas mediante cámaras instaladas y una aplicación distribuida. El ciclo completo de gestión del certificado de salud, desde su creación hasta el almacenamiento y la visualización dinámica, está cubierto por este sistema seguro, preservando la privacidad y facilitando su uso en diferentes escenarios de verificación.

En 2021, Fasfous et al. desarrollaron BinaryCoP, un clasificador basado en redes neuronales binarias (BNN) para predecir el uso correcto y la posición de mascarillas faciales, dirigido a dispositivos edge. Este trabajo se enfoca en la necesidad de controlar el uso de mascarillas durante la pandemia de COVID-19, especialmente en espacios interiores como aeropuertos, edificios corporativos y áreas comerciales. Utilizando redes neuronales convolucionales (CNNs), BinaryCoP clasifica la correcta colocación de mascarillas en tiempo real, garantizando que el procesamiento se realice en el dispositivo edge, sin comunicación con servidores en la nube, para preservar la privacidad de los datos.

El sistema fue implementado en un acelerador FPGA integrado, que permite ejecutar operaciones binarias de alto rendimiento a velocidades de hasta 6400 cuadros por segundo con un consumo de energía de aproximadamente 2W, adecuado para entornos con múltiples cámaras y puertas de control de acceso rápido. En modo de espera, el consumo de energía se reduce a 1.65W, optimizando la duración de la batería del dispositivo. BinaryCoP alcanzó una precisión del 98% en la clasificación de cuatro posiciones de uso de mascarillas utilizando el conjunto de datos MaskedFace-Net. Además, se utilizó el método Grad-CAM para asegurar que el algoritmo generalizara correctamente las características relevantes, considerando una amplia diversidad de estructuras faciales, tonos de piel y tipos de mascarilla.

En su estudio de 2021, Lad, Mishra y Rajagopalan realizaron un análisis comparativo de arquitecturas de redes neuronales convolucionales (CNN) para la detección en tiempo real de mascarillas faciales durante la pandemia de COVID-19. Este sistema busca automatizar la verificación del uso de mascarillas en espacios públicos, algo que es difícil de realizar manualmente. En su investigación, compararon tres arquitecturas de CNN: Sequential bi-layered CNN, VGG-16 CNN, y MobileNetV2 CNN. De estas, MobileNetV2 mostró el mejor desempeño, alcanzando una precisión del 99.2% en la detección de mascarillas. La solución propuesta puede implementarse utilizando dispositivos IoT y cámaras en lugares públicos como estaciones de tren, aeropuertos, parques, escuelas y oficinas, para garantizar que las personas sigan las directrices de uso de mascarillas. Este sistema es particularmente útil en el período posterior al brote, cuando el monitoreo de grandes multitudes es esencial para evitar una nueva propagación del virus.

En 2021, Wang, Zhao y Chen desarrollaron un enfoque innovador para la detección del uso de mascarillas durante la pandemia de COVID-19, combinando técnicas de aprendizaje transferido y un sistema de aprendizaje amplio. Este método se estructura en dos etapas: la primera utiliza un modelo transferido que integra Faster R-CNN con InceptionV2 para identificar regiones potenciales donde se están usando mascarillas, mientras que la segunda etapa se enfoca en la verificación precisa del uso de mascarillas mediante un sistema de aprendizaje amplio entrenado para clasificar las imágenes en dos categorías. Los autores también introdujeron un nuevo conjunto de datos denominado WMD, que contiene 7804 imágenes con un total de 26403 mascarillas, abarcando diversas escenas. Los resultados experimentales demostraron que el enfoque propuesto alcanza una precisión general del 97.32% en escenas simples y del 91.13% en escenas más complejas, superando los métodos comparados. Este estudio subraya la efectividad de su método híbrido en la detección precisa de mascarillas, lo que resulta crucial para el monitoreo en lugares públicos como hospitales y aeropuertos durante la pandemia.

Mohammed Aarif K. O., Mohamed Yousuff C., Mohammed Hashim C., Durga P., Divya G., Ayeshwariya D., Fathima Asfeeya S., y Sivakumar P. (2021) presentan un enfoque innovador para la detección de rostros enmascarados y la prevención de fraudes, utilizando una combinación de Gabor wavelets y redes neuronales convolucionales profundas (CNN). En respuesta a los desafíos que presenta la pandemia de COVID-19, su método aborda la limitación de los sistemas tradicionales de reconocimiento facial que se ven afectados por el uso de mascarillas. El enfoque propuesto extrae características del rostro no enmascarado mediante Gabor wavelets y las integra con características aprendidas por CNN para crear un vector de características más robusto. La metodología fue evaluada utilizando cuatro conjuntos de datos de referencia y un conjunto de datos manualmente preparado, logrando una precisión media del 97%. Este avance es particularmente relevante para aplicaciones en el control de acceso, seguridad facial y verificación en entornos como escuelas, oficinas y estaciones de transporte.

Khan, N., y Efthymiou, M. (2021) examinan el uso de la tecnología biométrica en los aeropuertos, centrando su estudio en el Programa de Entrada y Salida Biométrica del Departamento de Seguridad Nacional de EE.UU. (DHS). Este programa, implementado por la Oficina de Aduanas y Protección Fronteriza (CBP), utiliza el Sistema de Verificación de Viajeros (TVS) para confirmar biométricamente la identidad de los viajeros y su entrada o salida, mejorando la capacidad para detectar documentos fraudulentos y estancias prolongadas con visa. El estudio analiza la implementación del programa en el Aeropuerto de Dublín, incluyendo las puertas de embarque con reconocimiento facial, y evalúa los resultados de las pruebas piloto en Dublín y otros aeropuertos estadounidenses. Entre los desafíos identificados se encuentran la falta de apoyo de las partes interesadas, una baja tasa de coincidencia biométrica, problemas de infraestructura y conectividad, preocupaciones sobre la privacidad de los viajeros y una fuerte dependencia de las aerolíneas. Se presentan recomendaciones y soluciones para superar estos problemas y avanzar en la implementación de la tecnología biométrica en el entorno aeroportuario.

Ishihara, K., Yamada, H., Otani, T., Sasamoto, T., Inoue, J., e Ishikawa, M. (2021) presentan el sistema Face Express, un nuevo procedimiento de embarque que utiliza el sistema de reconocimiento facial de NEC en el Aeropuerto Internacional de Narita. Con Face Express, los pasajeros registran su imagen facial y pueden completar los procedimientos en el aeropuerto, incluidos el check-in de equipaje, el paso por el control de seguridad y el embarque, sin necesidad de mostrar su pasaporte ni tarjeta de embarque. Este sistema permite procedimientos de check-in sin contacto y sin fricciones. El artículo discute las dificultades para demostrar la precisión del reconocimiento facial en el proyecto del sistema "One ID" del Aeropuerto Internacional de Narita, la importancia de ajustar la calidad de las imágenes para cada ubicación de instalación, el diseño para realizar un "ritmo de caminata" y los esfuerzos para coordinarse con diversas partes interesadas relacionadas con las operaciones existentes.

Bindemann, M. (2021) en su libro Forensic Face Matching: Research and Practice ofrece una visión exhaustiva sobre la identificación de personas en contextos forenses, como el control de pasaportes, en fronteras, en investigaciones policiales y en juicios criminales. El texto examina el proceso de comparación de imágenes faciales, conocido en entornos forenses como "comparación de imágenes faciales" y como "coincidencia de rostros no familiares" en la ciencia cognitiva. Reúne conocimientos de expertos en psicología, derecho y práctica forense para abordar problemas como los impostores de identidad y cómo la variabilidad dentro de la persona y la similitud entre personas, influenciadas por factores como la calidad de la imagen, la dirección de la iluminación y el ángulo de visión, afectan la identificación.

El libro presenta un marco para desarrollar una teoría cognitiva de la coincidencia de rostros y analiza las habilidades de coincidencia de rostros de observadores no entrenados, revisores faciales, examinadores faciales y super-reconocedores. Además, revisa las diferencias individuales entre observadores, el aprendizaje y entrenamiento para el reconocimiento y coincidencia de rostros, y la selección de personal. También considera los criterios de admisibilidad de las pruebas de coincidencia de rostros en entornos legales, enfocándose en aspectos como la relevancia, la prohibición de pruebas de opinión y la fiabilidad. El libro explica conceptos clave relevantes para los algoritmos automáticos de reconocimiento facial en aeropuertos e investigaciones policiales, como las redes neuronales convolucionales profundas, la biometría y la interacción humano-computadora. Finalmente, aborda las nuevas amenazas de seguridad en forma de disfraces de máscaras hiperrealistas y su impacto en la identificación de personas en entornos aplicados y de laboratorio.

Zhang, E. (2021) presenta un modelo de aprendizaje profundo de transferencia en tiempo real para la detección de mascarillas faciales en el Integrated Communications, Navigation and Surveillance Conference (ICNS). Con el aumento de la pandemia de COVID-19, el uso de mascarillas en áreas públicas se ha vuelto crucial para prevenir la transmisión del coronavirus. Sin embargo, los métodos actuales de supervisión del uso de mascarillas son en su mayoría humanos, lo que resulta difícil de ejecutar eficazmente en lugares de alta densidad y de rápido movimiento como aeropuertos y transporte público. Zhang desarrolla un sistema automatizado de detección de mascarillas faciales utilizando el API de aprendizaje profundo Keras y la plataforma de código abierto TensorFlow. El modelo emplea redes neuronales convolucionales profundas (DCNN) entrenadas con una base de datos de aproximadamente 12,000 imágenes de rostros, con una división de 50-50 entre rostros con y sin mascarilla.

El software de detección de mascarillas DCNN logró una precisión de validación del 98%. Además, se utilizan técnicas de visión por computadora de OpenCV, como la detección facial y los contornos, para identificar la ubicación de los rostros. El DCNN se combina con esta aplicación para lograr una detección en tiempo real mediante la identificación de personas y la verificación de si llevan una mascarilla. El artículo también explora la implementación y aplicaciones potenciales del modelo de detección facial a través de la conexión de cámaras en áreas de monitoreo para notificar a los oficiales. Dado que los países están desarrollando regulaciones sobre el uso de mascarillas, la detección automática de mascarillas faciales se presenta como una aplicación clave para ayudar en la supervisión gubernamental y garantizar el cumplimiento de las regulaciones en áreas públicas susceptibles de transmisión.

Perpetuini, D., Filippini, C., Cardone, D., & Merla, A. (2021) ofrecen una visión general de los exámenes basados en imágenes térmicas infrarrojas durante emergencias pandémicas en el International Journal of Environmental Research and Public Health. La tecnología de imágenes térmicas infrarrojas (IRI) se utiliza para monitorear la temperatura de la piel humana de manera no invasiva, y su capacidad para detectar fiebre ha sido fundamental durante emergencias epidémicas pasadas y la pandemia actual de COVID-19. Sin embargo, la evaluación de fiebre por sí sola no es específica para la infección por SARS-CoV-2. El artículo revisa cómo se ha empleado la IRI en epidemias recientes, destacando tanto las potencialidades como las limitaciones de esta tecnología para contener contagios. Se analiza la aplicación de métodos automáticos para el reconocimiento facial y la evaluación de fiebre, así como el desempeño de la IRI en la detección masiva en aeropuertos y hospitales. Además, se proporciona una visión general de nuevos métodos de aprendizaje automático para el análisis de datos IRI, orientados a identificar enfermedades respiratorias.

Ullah, S., Partheeban, N., Sriramulu, S., Soni, R. K., Gupta, S., y Daniel, A. (2021) presentan un sistema de detección de mascarillas faciales adaptado para enfrentar la pandemia de COVID-19 en el Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking. Dado el impacto global de la pandemia y las nuevas normativas de salud, los autores desarrollaron un sistema basado en OpenCV y TensorFlow que utiliza una red neuronal convolucional (CNN) para identificar si las personas llevan mascarilla en lugares públicos como templos y aeropuertos. El sistema, que integra cámaras de vigilancia, analiza imágenes en tiempo real para detectar la presencia o ausencia de mascarillas, alertando sobre violaciones a las normas de seguridad y promoviendo el cumplimiento de los protocolos sanitarios. La solución propuesta no solo facilita la supervisión en tiempo real, sino que también mejora la seguridad en entornos públicos al garantizar que las personas sigan las directrices establecidas para mitigar la propagación del virus.

Mas adelante en el tiempo Nassr y Al-Khafaji (2021) en el artículo “Designing a system for identifying persons using 3D images” publicado en International Journal of Nonlinear Analysis and Applications, Alwahab, presentan un sistema innovador para la identificación de personas mediante imágenes 3D. Dado el creciente desafío en la seguridad de la información y la proliferación de cámaras de vigilancia en lugares como bancos y aeropuertos, el sistema propuesto aborda las complejidades del reconocimiento facial al registrar características faciales tridimensionales, como el tamaño y la posición de los rasgos faciales, para mejorar la precisión del reconocimiento. La tecnología empleada permite una identificación precisa y rápida sin la necesidad de extensas sesiones de entrenamiento para los técnicos, y destaca por su facilidad de uso en comparación con otras técnicas biométricas. Este sistema, desarrollado utilizando Matlab, promete ofrecer resultados rápidos y exactos en el campo de la seguridad mediante un análisis detallado y automático de las imágenes faciales.

En el artículo “Face recognition system for criminal identification using deep metric learning” presentado en AIP Conference Proceedings (2022), Sowmeya y Karthik (2022) abordan la aplicación de sistemas de reconocimiento facial para la identificación de criminales mediante el aprendizaje métrico profundo. Este estudio se centra en la mejora de los sistemas de reconocimiento facial para aplicaciones críticas como la identificación de delincuentes en investigaciones criminales. Utilizando redes neuronales convolucionales (CNN) y la biblioteca de reconocimiento facial Dib, el sistema propuesto facilita una identificación más precisa y confiable de los delincuentes. Este enfoque no solo optimiza la detección en contextos de alta seguridad como bancos y aeropuertos, sino que también apoya a las fuerzas policiales en la investigación de delitos graves.

En el artículo “A Critical Scrutiny of ConvNets (CNNs) and Its Applications: Review” publicado en SN Computer Science (2022), Shanmuganathan y Nalini examinan exhaustivamente los métodos actuales para la identificación de objetos, con un enfoque en las redes neuronales convolucionales (ConvNets o CNNs). El estudio revisa la literatura existente desde 1993 y destaca cómo los CNNs se han convertido en una herramienta prevalente en la identificación facial y en diversas aplicaciones comerciales y de seguridad. Los CNNs se utilizan en aeropuertos para la verificación de seguridad, en bancos para pagos sin contacto, en la atención médica para el chequeo y diagnóstico de pacientes, en el comercio minorista para mejorar la experiencia del cliente, y en educación para la identificación de estudiantes. El artículo también aborda problemas de privacidad y las implicaciones comerciales de estas tecnologías, proporcionando una visión crítica sobre sus enfoques y aplicaciones actuales.

En el artículo “OneDetect: A Federated Learning Architecture for Global Soft Biometrics Prediction” presentado en la 2022 International Conference on Intelligent Systems and Computer Vision, Hassan e Izquierdo abordan el desarrollo de tecnologías de seguridad avanzadas en respuesta al aumento de amenazas y terrorismo. Propongan una arquitectura de aprendizaje federado denominada OneDetect, diseñada para ofrecer un sistema de verificación de identidad único y global utilizando biometría suave, como el género, la edad y la etnicidad. Este enfoque federado protege la privacidad de los datos de cada cliente mientras mejora continuamente el sistema de verificación. La arquitectura emplea el dataset MMV Pedestrian, recopilado en un entorno similar a un aeropuerto, y utiliza EfficientNetB3 para entrenamiento y predicción. Este sistema promete una identificación fluida en aeropuertos, puertos y otros lugares públicos, contribuyendo a una seguridad más eficaz y generalizada.

En el artículo “Face Mask Detection: A Deep Learning Concept” presentado en la 3rd International Conference on Intelligent Engineering and Management (ICIEM 2022), Saini, Bharadwaj y Gupta exploran el desarrollo de un programa para la detección de mascarillas faciales utilizando conceptos de aprendizaje profundo y visión por computadora. En respuesta a la pandemia de COVID-19, el programa, implementado con OpenCV y Keras/TensorFlow, se enfoca en detectar mascarillas en imágenes y vídeos en tiempo real. El modelo utiliza el detector de un solo disparo (SSD) por su precisión y velocidad, y se basa en MobileNetV2 para facilitar su integración en dispositivos embebidos como Google Coral y Raspberry Pi. Los resultados muestran una eficiencia del 100% con una precisión del 99% en pruebas, demostrando la eficacia del sistema para garantizar el cumplimiento de medidas de seguridad en lugares públicos como aeropuertos, estaciones de tren, oficinas y mercados.

En el artículo “FaceHack: Attacking Facial Recognition Systems Using Malicious Facial Characteristics”, publicado en IEEE Transactions on Biometrics, Behavior, and Identity Science, Sarkar, Benkraouda, Krishnan, Gamil y Maniatakos exploran las vulnerabilidades de los sistemas de reconocimiento facial ante ataques maliciosos. Los autores demuestran que las Redes Neuronales Profundas (DNNs), comúnmente empleadas en estos sistemas, pueden ser manipuladas mediante características faciales específicas que actúan como desencadenantes para ataques encubiertos. Estos ataques pueden implementarse en sistemas de reconocimiento facial en tiempo real, utilizando filtros de redes sociales o mediante movimientos naturales de los músculos faciales. La investigación valida la efectividad de estos ataques y confirma que los desencadenantes son indetectables por los mecanismos de defensa y detección actuales. Este trabajo destaca las serias amenazas que representan las vulnerabilidades en los sistemas de reconocimiento facial, desde aplicaciones en redes sociales hasta controles biométricos en aeropuertos.

El artículo “A PLS-SEM Neural Network for Understanding Computer Vision Technical. Apply to Gender Classification System” de Duc y Viet, publicado en el Journal of Engineering Science and Technology Review (2022), propone un enfoque novedoso para el reconocimiento de género facial utilizando una combinación de modelos de análisis. Primero, el estudio emplea el método Local Binary Pattern y K-Nearest Neighbor para desarrollar una aplicación de reconocimiento de género facial con una base de datos de 6000 imágenes, logrando una precisión del 95.4%. Posteriormente, se utiliza un modelo de dos capas para analizar encuestas sobre la aceptación de la tecnología de reconocimiento de género facial. Este enfoque combina el modelado de ecuaciones estructurales parciales (PLS-SEM) y redes neuronales artificiales (ANN) para obtener resultados más precisos que el SEM tradicional. El estudio también evalúa la relación entre la aceptación tecnológica y la calidad del sistema de información, utilizando ANN para clasificar los factores predictivos importantes con alta precisión. Los hallazgos confirman que el enfoque combinado de PLS-SEM y ANN mejora la precisión de las predicciones en comparación con el SEM.

El artículo “Face recognition with a hyperbolic metric classification model” de Trpin y Boshkoska, presentado en el 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO 2022), explora el uso del métrico hiperbólico Poincaré para la clasificación en sistemas de reconocimiento facial. Los sistemas de reconocimiento facial, cada vez más comunes en tecnologías como teléfonos inteligentes y control automatizado de pasaportes en aeropuertos, generan grandes volúmenes de datos fotográficos. Este estudio investiga cómo el métrico Poincaré, típico en geometría hiperbólica, puede mejorar el algoritmo de k Vecinos Más Cercanos (k-NN). Los resultados mostraron que el uso del métrico Poincaré combinado con el filtro Edge ofrece los mejores resultados en la clasificación de imágenes para pequeños valores de k (hasta cinco) cuando se aplica al método de Aprendizaje de Vecinos Más Cercanos con Gran Margen (LMNN). Esta metodología demuestra ser efectiva para gestionar y clasificar grandes conjuntos de imágenes faciales.

El artículo “Face Recognition System with 2D Anti-Spoofing” de Savanth et al., presentado en la IEEE World Conference on Applied Intelligence and Computing (AIC 2022), aborda la creciente preocupación por la seguridad en los sistemas de reconocimiento facial frente a ataques de suplantación. Este estudio propone un sistema de reconocimiento facial con características de anti-suplantación, utilizando la arquitectura de red neuronal ResNet50 para entrenar el modelo. El sistema incorpora detección de parpadeo ocular para mitigar ataques de foto y reflexión de luz para contrarrestar ataques de video. La propuesta se implementa en un prototipo de hardware que combina estas funciones, ofreciendo una solución robusta contra intentos de fraude que podrían comprometer la seguridad en edificios o instalaciones críticas. El trabajo destaca la necesidad de fortalecer la tecnología de reconocimiento facial para mantener su eficacia frente a ataques sofisticados.

El artículo “Realtime Facial Emotion Detection Using Machine Learning” de Brintha et al., presentado en la International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES 2022), propone una solución innovadora para mejorar la detección de emociones faciales en tiempo real. Este sistema está diseñado para asistir a los oficiales antidrogas en la identificación de sospechosos en aeropuertos, donde el tráfico de drogas es una preocupación creciente. La solución implica la instalación de software en cámaras de CCTV que captura y analiza las expresiones faciales de las personas, notificando a los oficiales sobre posibles sospechosos basándose en sus emociones. El enfoque también tiene aplicaciones en robótica, proporcionando un mecanismo de soporte valioso para diversas tareas de identificación emocional.

En su trabajo titulado “Feature Selection Based on Machine Learning Algorithms: A Weighted Score Feature Importance Approach for Facial Authentication”, Ghoualmi y Benkechkache (2022) abordan la selección de características en sistemas de autenticación facial biométrica. Dado que esta tecnología se ha vuelto parte integral de nuestras vidas en áreas como la seguridad y la investigación forense, el estudio propone un novedoso enfoque basado en la combinación de puntajes de importancia de características generados por diferentes modelos de machine learning. Utilizan un algoritmo genético (GA) como optimizador para combinar estos puntajes y reducir el tamaño de las características, mejorando así la eficiencia del sistema en tiempo real. Sus resultados, probados en la base de datos Fetch Olivetti Faces, muestran un aumento en la precisión del 93.5% al 95.62% y una reducción significativa del tamaño de las características de 4096 a 964.

En el artículo “Comparative Analysis of Face Mask Detection Models”, Chauhan et al. (2022) presentan una comparación de diferentes modelos de detección de mascarillas faciales, un tema crucial en la lucha contra la pandemia de COVID-19. Utilizando datasets como el Real World Masked Face Dataset (RMFD) y otro disponible en Kaggle, los autores recopilaron imágenes de personas usando mascarillas reales, además de generar imágenes sintéticas al editar fotos de rostros sin mascarilla. Este enfoque permite que los modelos aprendan los detalles específicos de las mascarillas, mejorando la precisión de la detección. La aplicación de visión por computadora y la inteligencia artificial en esta área busca abordar problemas de distanciamiento social en lugares de alta afluencia, como aeropuertos y oficinas, contribuyendo al control del virus.

El artículo “Facial Recognition Based Workplace Security System Using LBPH Algorithm” de Gaurav Srivastav y Richa Singh (2022). Aborda la implementación de un sistema de reconocimiento facial para mejorar la seguridad en lugares de trabajo y hogares. Utilizando el algoritmo Local Binary Pattern Histogram (LBPH), se desarrolló y probó un modelo de reconocimiento facial en tiempo real, enfocado en las variaciones de características faciales, poses, ángulos e iluminación. El modelo obtuvo una precisión superior al 85% bajo condiciones de iluminación variables, demostrando su efectividad en comparación con otros métodos como Eigenface y Fisherface. Los autores sugieren que este tipo de sistema es ideal para la vigilancia en áreas concurridas, calles y aeropuertos, destacando su robustez en diferentes condiciones de iluminación.

El artículo “Convolution Neural Network Approach for Facial Mask Detection” de Irish C. Juanatas y Roben A (2023). Juanatas presenta una técnica de detección de mascarillas faciales basada en Redes Neuronales Convolucionales (CNN). En respuesta a la pandemia de COVID-19 y la necesidad de cumplir con los protocolos de salud, este estudio utiliza el modelo You Only Look Once (YOLO) v8 para clasificar imágenes en tres categorías: con mascarilla, sin mascarilla y uso inadecuado de mascarilla. La automatización de este proceso tiene aplicaciones en lugares como aeropuertos, hospitales, lugares de trabajo y espacios públicos, contribuyendo a la salud y seguridad pública. El modelo alcanza una precisión promedio (mAP) del 88.2% en 300 épocas, con una tasa de precisión del 96.2%, lo que muestra un rendimiento excepcional en la identificación de mascarillas. Sin embargo, el estudio destaca una tasa de recall del 73.3%, indicando la necesidad de mejorar la detección de todos los casos positivos.

El artículo "Safety, Security and Privacy in Future Airport Terminals: A System Theory Perspective" analiza los desafíos de seguridad, protección y privacidad en los aeropuertos del futuro debido a la digitalización y el uso de biometría y reconocimiento facial. Se explora cómo la eliminación de barreras físicas entre pasajeros nacionales e internacionales podría generar preocupaciones en términos de seguridad. Desde una perspectiva de teoría de sistemas, se identificaron más de 250 interacciones potencialmente peligrosas entre usuarios, controladores y sistemas automatizados, y más de 100 escenarios disruptivos relacionados. Estos resultados proporcionan una base para los requisitos y restricciones en la implementación de nuevos conceptos operativos en terminales de aeropuertos.

El artículo "Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Models" de Zolfi A, et al (2023), explora cómo las máscaras adversariales pueden desafiar los modelos de reconocimiento facial (FR) en entornos reales. Durante la pandemia de COVID-19, el uso generalizado de mascarillas protectoras reveló que los modelos basados en aprendizaje profundo mantenían un rendimiento sobresaliente, lo que llevó a la comunidad de investigación a investigar la robustez de estos sistemas frente a ataques adversariales. Este trabajo presenta un ataque físico de perturbación universal adversarial (UAP) aplicado a máscaras faciales, en forma de un patrón cuidadosamente diseñado. Los experimentos demostraron que este ataque redujo drásticamente la capacidad del sistema de reconocimiento facial para identificar correctamente a los participantes, con una tasa de éxito de identificación del 3.34%, en comparación con al menos el 83.34% de otras máscaras evaluadas. Este enfoque ofrece nuevas perspectivas para vulnerar modelos de FR en el mundo real.

En el artículo “To Improve the Identification of Images Using LBPH in Machine Learning” presentado en la 2023 1st International Conference on Intelligent Computing and Research Trends, Kumar Shukla et al. (2023) exploran la mejora de los sistemas de identificación facial utilizando Local Binary Patterns (LBP). El estudio destaca la aplicación de redes neuronales convolucionales (CNN) para mejorar la precisión en la identificación facial en tiempo real, a pesar de variaciones en la postura, el estado de ánimo y la resolución de las imágenes. El sistema propuesto integra técnicas avanzadas para la detección y reconocimiento facial, actualizando automáticamente las bases de datos de entrenamiento y clasificación. Este enfoque tiene aplicaciones potenciales en la vigilancia de aeropuertos, terminales de autobuses y otros espacios públicos, contribuyendo a la reducción de actividades criminales mediante un sistema de seguridad más eficiente y preciso.

El artículo "Understanding User Perception of Biometric Privacy in the Era of Generative AI" de Srinivasan S (2023), analiza cómo la combinación de la biometría y la inteligencia artificial generativa está transformando la tecnología, al mismo tiempo que plantea preocupaciones sobre la privacidad y seguridad de los datos biométricos. A través de una encuesta realizada a residentes de los EAU, se examinaron factores demográficos como edad, género, nivel educativo y competencia tecnológica en relación con la frecuencia de uso de la autenticación biométrica (huellas dactilares, reconocimiento facial, etc.). El estudio también aborda preocupaciones sobre el mal uso de datos biométricos y la necesidad de obtener un consentimiento explícito antes de recopilar dichos datos. Aunque no se encontró una relación significativa entre las variables demográficas y las preocupaciones de privacidad, sí se observó una correlación estadísticamente significativa entre el uso de la autenticación biométrica y la conciencia sobre los riesgos de privacidad, así como el conocimiento de tecnologías emergentes como la IA generativa y los deepfakes.

El artículo "Robust Multi-Bio-Metric Authentication Framework in Face and Iris recognition" de Gianto L, et al (2023), presenta un marco de autenticación biométrica robusto que combina el reconocimiento facial y de iris. Los sistemas biométricos proporcionan un nivel de seguridad superior en comparación con métodos tradicionales como contraseñas o PINs, y se utilizan en una amplia gama de aplicaciones, desde transacciones financieras hasta control de acceso en aeropuertos. El estudio aborda las limitaciones de los sistemas biométricos basados en un solo rasgo, que no son adecuados para aplicaciones altamente seguras. Para resolver estas limitaciones, los autores proponen un sistema biométrico multimodal que utiliza múltiples características físicas y conductuales para la autenticación del usuario, como el color de ojos, género, y otras características "suaves". El sistema propuesto mejora la autenticación del usuario y la seguridad sin comprometer la velocidad.

El artículo "Real-Time Masked Face Recognition in the Wild with few shots" de Bagwan, Gupta y Thiagale (2023), aborda el desafío del reconocimiento facial con mascarilla (MFR) en tiempo real, un problema que se ha vuelto relevante tras la pandemia debido al uso generalizado de mascarillas en lugares públicos como aeropuertos y hospitales. A pesar de los avances en el reconocimiento facial tradicional, el MFR sigue siendo complicado debido a la oclusión de gran parte del rostro por la mascarilla. Los autores proponen un enfoque basado en el aprendizaje con pocas muestras (Few-Shot Learning, FSL), utilizando una combinación de los conjuntos de datos Labeled Faces in the Wild (LFW) y Masked LFW (MLFW), junto con un conjunto de datos aumentado que incluye transformaciones de cara a mascarilla y viceversa. El modelo propuesto mejora la precisión del MFR en un 10%, alcanzando una tasa de precisión del 87.52% utilizando FaceNet512, en comparación con métodos previos. Además, el sistema logra tiempos de inferencia tan bajos como 0.024 segundos, lo que lo hace apto para aplicaciones en tiempo real.

El estudio realizado por Josphineleela et al. (2023) aborda la detección eficiente y precisa del uso de mascarillas en áreas concurridas mediante el uso de algoritmos de aprendizaje automático. La pandemia de COVID-19 ha subrayado la importancia de las mascarillas como medida preventiva para frenar la propagación del virus. A pesar de la disminución en los casos, el uso de mascarillas sigue siendo crucial en diversos entornos, como aeropuertos, hospitales y otros lugares públicos. Este estudio presenta un sistema basado en aprendizaje profundo para identificar eficazmente a las personas que no utilizan mascarillas de manera adecuada. La investigación destaca cómo esta tecnología puede mejorar la seguridad en contextos masivos, proporcionando una herramienta valiosa para el cumplimiento de las normativas de salud y seguridad. La solución propuesta ofrece una manera de mantener el control en escenarios públicos, garantizando una mayor adherencia a las medidas preventivas (Josphineleela, Vekariya, Bharathidasan, Alfurhood, Kumar, & Tripathi, 2023).

Priya et al. (2023) exploran el uso de la autenticación impulsada por inteligencia artificial (IA) para mejorar la seguridad en hogares inteligentes. En su investigación, se centran en los sistemas de gestión de visitantes basados en reconocimiento facial, destacando su eficacia en comparación con métodos tradicionales como CCTV. El estudio sugiere que los sistemas de gestión de visitantes, que utilizan reconocimiento facial para identificar y autenticar a las personas, pueden ser una solución segura y rentable para la seguridad del hogar. Estos sistemas emplean redes neuronales convolucionales para analizar características faciales y gestionar la seguridad sin necesidad de dispositivos adicionales. La integración de estas tecnologías en hogares y otros entornos está en constante expansión, proporcionando una solución innovadora y práctica para la gestión de acceso y la prevención de intrusiones (Priya, Gopinath, Mohamed Ashif, & Yadeshwaran, 2023).

Kumar Shukla et al. (2023) investigan la mejora en la identificación de imágenes utilizando el método Local Binary Patterns (LBP) en el contexto del aprendizaje automático. Su estudio se enfoca en la implementación de un sistema de identificación facial en tiempo real que integra variaciones en la postura, el estado de ánimo y la resolución de imágenes. El trabajo destaca cómo el uso de redes neuronales convolucionales (CNN) y la actualización continua de bases de datos pueden optimizar el proceso de detección y reconocimiento facial. Esta tecnología se aplica en sistemas de vigilancia en lugares públicos como aeropuertos y terminales de autobuses, contribuyendo a la reducción de actividades criminales y mejorando la seguridad en estos entornos (Kumar Shukla, Kumar Tripathi, Kumar, Prakash, & Kumar Singh, 2023).

Nidhi y Verma (2023) ofrecen una revisión exhaustiva sobre el reconocimiento de emociones faciales, una técnica crucial para interpretar el estado emocional de una persona a partir de sus expresiones. El artículo destaca la importancia de los sistemas basados en inteligencia artificial para implementar en áreas de alta seguridad como estaciones de autobuses, ferrocarriles, aeropuertos y estadios, ayudando a las fuerzas de seguridad a identificar amenazas potenciales. A través de un análisis detallado de métodos tradicionales y de aprendizaje profundo, los autores comparan distintos modelos y conjuntos de datos, identificando ventajas y desventajas en su rendimiento. La revisión también aborda las lagunas en la literatura actual y propone futuras direcciones para la investigación en el campo del reconocimiento de emociones faciales (Nidhi & Verma, 2023).

Syed Musthafa et al. (2024) exploran el uso de la tecnología de reconocimiento facial impulsada por inteligencia artificial para mejorar la búsqueda de personas desaparecidas. El artículo propone un método que utiliza algoritmos de IA para comparar las imágenes de personas desaparecidas con el video en tiempo real capturado por cámaras de seguridad. Este enfoque incluye la recopilación de información sobre la persona desaparecida, la creación de una base de datos de fotos faciales y el uso de algoritmos de IA para realizar coincidencias con la filmación en vivo. La tecnología de redes neuronales convolucionales (CNN) es destacada por su eficacia en la identificación y clasificación de imágenes, demostrando resultados prometedores en la detección de personas desaparecidas. La metodología propuesta tiene el potencial de acelerar y mejorar la precisión de las búsquedas, aumentando las probabilidades de reencuentros exitosos (Syed Musthafa et al., 2024).

Railkar et al. (2024) presentan un sistema de reconocimiento criminal utilizando tecnologías de reconocimiento facial y detección basadas en aprendizaje profundo. El artículo destaca cómo las tecnologías de reconocimiento facial, especialmente los sistemas basados en redes neuronales convolucionales (CNN), se están aplicando en la seguridad y vigilancia para la identificación de delincuentes. Estas tecnologías se utilizan en establecimientos como bancos y aeropuertos para mejorar la eficiencia en la detección de sospechosos. El estudio sugiere que, para mejorar la precisión en la identificación de criminales, es necesario contar con grandes volúmenes de datos y que las técnicas actuales de CNN deben adaptarse para abordar desafíos específicos, como la identificación en contextos de alta seguridad. El sistema propuesto busca asistir a las fuerzas policiales en la detección de delincuentes mediante el uso de algoritmos de aprendizaje profundo para el reconocimiento de imágenes en plataformas web (Railkar et al., 2024).

Fysh et al. (2024) investigan el impacto de las distracciones en el proceso de identificación facial en entornos visuales simulados, utilizando un entorno virtual de aeropuerto. El estudio explora cómo la presencia de estímulos irrelevantes, como otras personas en el fondo, afecta la precisión y velocidad de la identificación de rostros. A pesar de que la mayoría de los estudios previos se han realizado en entornos altamente controlados, este estudio utiliza un entorno más realista y encuentra que, en general, las personas en el fondo no afectan la precisión de la identificación facial. Sin embargo, la inmersión en realidad virtual (VR) revela que una multitud enfadada en el fondo retrasa la velocidad de emparejamiento sin afectar la precisión. Los resultados tienen implicaciones teóricas y prácticas importantes para el diseño de sistemas de reconocimiento facial en situaciones reales (Fysh et al., 2024).

Chougule et al. (2024) proponen un enfoque innovador basado en redes generativas adversariales (GAN) para mejorar la resolución de imágenes faciales, una tarea crucial en aplicaciones de visión por computadora como la seguridad y la detección de emociones. A pesar de los avances en sistemas de reconocimiento facial basados en aprendizaje profundo, la identificación precisa de rostros en imágenes de baja resolución sigue siendo un desafío. El artículo presenta una arquitectura generadora estilo U-Net que utiliza conexiones de salto entre las capas del codificador y decodificador para preservar las características faciales de las imágenes de entrada, evitando la generación de imágenes completamente nuevas. El modelo propuesto ha demostrado generar imágenes de alta resolución más similares a las originales en comparación con modelos de creación de imágenes de alta resolución existentes, mejorando la precisión en la detección de rostros (Chougule et al., 2024).

Çavşi Zaim, Yılmaz y Yolaçan (2024) proponen un sistema de reconocimiento de género utilizando aprendizaje profundo basado en la computación cuántica. En sistemas biométricos, como los utilizados en aeropuertos y bancos, las imágenes digitales son clave para la autenticación. Aunque los sistemas biométricos mejoran la seguridad, enfrentan desafíos prácticos, especialmente en la clasificación de datos biométricos según características como género. Las redes neuronales convolucionales (CNN) han demostrado ser efectivas en el análisis facial, pero pueden tener dificultades con grandes volúmenes de datos. El estudio introduce la Red Neuronal Cuántica Convolucional (QCNN) como una solución alternativa en un entorno de computación cuántica, comparando su rendimiento con el de CNN en términos de tiempo y precisión. Los resultados muestran una precisión del 92% para QCNN frente al 90% para CNN, con tiempos de procesamiento de 128.85 segundos para QCNN y 832.30 segundos para CNN, respectivamente (Çavşi Zaim, Yılmaz, & Yolaçan, 2024).

Ouassam, Dabachine, Hmina y Bouikhalene (2024) abordan la mejora de la eficiencia y seguridad en los procesos de control de pasaportes en aeropuertos utilizando el modelo de detección de objetos R-CNN. La optimización en tiempo real de estos procedimientos puede incrementar significativamente la eficiencia y seguridad de los controles. El artículo propone la implementación de algoritmos de inteligencia artificial, como reconocimiento de caracteres, reconocimiento facial y algoritmos predictivos, para automatizar el proceso. La metodología incluye el uso del modelo R-CNN para detectar objetos relacionados con pasaportes en imágenes en tiempo real capturadas por cámaras de control de pasaportes. Los autores describen el proceso paso a paso, que abarca la preprocesación, el entrenamiento y la prueba del modelo R-CNN, su integración en el sistema de control de pasaportes, y la evaluación de su precisión y velocidad. Los resultados muestran una mejora significativa en la reducción de errores, demoras y costos asociados en comparación con métodos anteriores (Ouassam, Dabachine, Hmina, & Bouikhalene, 2024).

Malla, Vemuri, Nagalli, Abhishek y Anjali (2024) examinan el desafío de distinguir entre rostros generados por inteligencia artificial y rostros reales. La creciente capacidad de las tecnologías de IA para crear rostros artificiales indistinguibles de los reales plantea preocupaciones significativas, especialmente en sistemas de seguridad que dependen del reconocimiento facial. El artículo aborda cómo los sistemas actuales pueden enfrentar dificultades para diferenciar entre un "deep-fake" de alta calidad y un rostro real, lo cual es crítico en puntos de control de seguridad, como en los aeropuertos. La investigación destaca la necesidad de enfoques de aprendizaje automático que sean adaptativos y capaces de identificar eficazmente rostros fraudulentos en medio de una amplia gama de rostros reales y generados artificialmente. Los resultados del estudio enfatizan la importancia de desarrollar sistemas de inteligencia artificial robustos y confiables para enfrentar estas amenazas emergentes, asegurando su eficacia en funciones críticas donde la realidad y la ficción se entremezclan (Malla, Vemuri, Nagalli, Abhishek, & Anjali, 2024).

Kavitha, Hemalatha, Raja, Sripriya y Yokeshwaran (2024) abordan la necesidad emergente de sistemas automatizados para la detección de mascarillas faciales, especialmente en el contexto de la pandemia de COVID-19. Su investigación presenta un sistema innovador de reconocimiento de mascarillas utilizando redes neuronales convolucionales (CNNs). Este enfoque de aprendizaje profundo se basa en una arquitectura CNN que permite la extracción de características faciales distintivas para identificar si un individuo está usando una mascarilla. El algoritmo propuesto se entrena con un conjunto de datos amplio que incluye imágenes de personas tanto con mascarillas como sin ellas. La tecnología desarrollada promete mejorar la seguridad, la atención sanitaria y la seguridad pública, con aplicaciones potenciales en la implementación de regulaciones sobre el uso de mascarillas en aeropuertos, hospitales, escuelas y transporte público. Los resultados destacan la importancia de contar con soluciones automatizadas para el cumplimiento de normas de salud pública y la protección durante situaciones pandémicas (Kavitha, Hemalatha, Raja, Sripriya, & Yokeshwaran, 2024).

Anagnostopoulou, Tolikas, Spyrou, Akac y Kappatos (2024) presentan una herramienta de toma de decisiones diseñada para gestionar flujos de pasajeros en terminales de aeropuertos. Su estudio introduce un modelo de simulación que permite explorar diversas estrategias de manejo de multitudes, las cuales pueden ser actualizadas según las necesidades específicas de cada terminal. Este enfoque busca ayudar a los gestores aeroportuarios a mitigar riesgos potenciales y evaluar estrategias para el manejo de multitudes. El objetivo principal es reducir los factores de riesgo asociados con el hacinamiento y minimizar los tiempos de espera de los pasajeros, con el fin de ofrecer una experiencia de viaje segura y satisfactoria. La congestión en áreas específicas de la terminal puede dificultar el movimiento libre de los pasajeros, incrementar el riesgo de accidentes, problemas de seguridad e interrupciones en el servicio, además de generar frustración y conflictos entre los pasajeros. Según los resultados obtenidos, la optimización de las rutas de los pasajeros mediante soluciones tecnológicas modernas se destaca como la estrategia más prometedora para gestionar un aeropuerto capaz de manejar 800 pasajeros por hora (Anagnostopoulou, Tolikas, Spyrou, Akac, & Kappatos, 2024).

## Marco Teórico

El reconocimiento facial se ha convertido en una herramienta esencial en la mejora de la seguridad en los aeropuertos y en la optimización de los procesos de verificación de identidad. Este proceso se basa en el análisis de características biométricas únicas, como las facciones faciales, que permiten identificar a una persona con un alto nivel de precisión. Las tecnologías de reconocimiento facial actuales se sustentan en algoritmos avanzados de aprendizaje automático y visión por computadora, que permiten extraer y comparar patrones específicos de rostros humanos para determinar coincidencias. Estas aplicaciones han probado ser eficaces en entornos de alta seguridad, como los controles de inmigración y acceso a zonas restringidas en aeropuertos.

La metodología CRISP-DM (Cross-Industry Standard Process for Data Mining) se ha consolidado como un estándar en proyectos de ciencia de datos por su flexibilidad y enfoque iterativo en la resolución de problemas. Esta metodología está compuesta por seis fases que guían el proceso desde la comprensión del negocio hasta la implementación de modelos, facilitando así la integración de técnicas de minería de datos en proyectos como el reconocimiento facial. Al aplicar CRISP-DM en el contexto de este proyecto, se garantiza un enfoque estructurado para abordar los retos de análisis y modelado de datos que permitan la identificación precisa y rápida de los pasajeros, mejorando la experiencia de usuario y la seguridad en el aeropuerto.

La teoría de autómatas proporciona una base sólida para el análisis y modelado de sistemas que requieren reconocimiento de patrones y toma de decisiones basadas en entradas definidas. En el caso de los sistemas de reconocimiento facial, los autómatas se pueden emplear para interpretar las secuencias de datos faciales y validar las identificaciones de manera eficiente. La programación paralela, por su parte, permite procesar grandes volúmenes de datos de manera simultánea, mejorando la rapidez en la verificación de identidad. La combinación de estas tecnologías hace posible un sistema de reconocimiento facial robusto y ágil, alineado con las necesidades de seguridad y eficiencia en el contexto aeroportuario.

## Marco Conceptual

Reconocimiento facial: El reconocimiento facial es una tecnología que permite la identificación o verificación de una persona mediante el análisis de sus características faciales. Este proceso implica la captura de imágenes faciales y la extracción de características clave, como la distancia entre los ojos, la forma de la nariz y el contorno de la mandíbula, para generar un "mapa facial" que se compara con otros registros en una base de datos.

Metodología CRISP-DM: La metodología CRISP-DM (Cross-Industry Standard Process for Data Mining) es un enfoque estructurado en seis fases utilizado en proyectos de ciencia de datos y minería de datos. Las fases incluyen la comprensión del negocio, comprensión de los datos, preparación de los datos, modelado, evaluación e implementación. En el contexto del reconocimiento facial en aeropuertos, CRISP-DM orienta el proceso de desarrollo del sistema, asegurando una alineación entre los objetivos del negocio y los resultados del análisis de datos.

Autómatas y programación paralela: Un autómata es un modelo matemático que representa un sistema mediante estados y transiciones entre estos, utilizado en la computación para resolver problemas de reconocimiento de patrones y procesos secuenciales. La programación paralela permite la ejecución simultánea de varias tareas, lo cual es fundamental en aplicaciones de procesamiento de imágenes y datos a gran escala. La integración de autómatas y programación paralela en este proyecto asegura una rápida respuesta en la identificación de pasajeros, atendiendo así a los requerimientos de eficiencia y seguridad en el ámbito aeroportuario.

## Marco Legal

El presente proyecto se enmarca en el cumplimiento de la Ley 1581 de 2012, la cual regula la protección de datos personales en Colombia, considerando los datos biométricos como sensibles. De acuerdo con esta ley, es obligatorio garantizar la recolección, almacenamiento y tratamiento de datos bajo el principio de confidencialidad y consentimiento informado. En este sentido, se debe obtener la autorización explícita de los pasajeros para el uso de su información facial, explicando claramente su finalidad, relacionada con la mejora en la seguridad y flujo aeroportuario. Este marco legal asegura que los derechos de los titulares de los datos, como el acceso, actualización y supresión, sean respetados, en concordancia con los principios de proporcionalidad y transparencia.

Asimismo, el sistema debe alinearse con la Circular Externa 002 de 2015 de la Superintendencia de Industria y Comercio, que establece pautas para la implementación de videovigilancia en espacios públicos y privados. Dicha regulación obliga a informar a los usuarios sobre la captura de sus imágenes mediante avisos visibles y establece la necesidad de restringir el tratamiento únicamente a datos necesarios para cumplir con las finalidades declaradas. Además, en cumplimiento de la Ley 1621 de 2013, se garantiza que el uso de tecnologías biométricas respete los derechos humanos y sea proporcional a los objetivos de seguridad que busca alcanzar el proyecto.

Por último, en cuanto al software desarrollado, este estará protegido por la Decisión Andina 351 de 1993 y la Ley 23 de 1982, que garantizan los derechos de autor sobre la creación intelectual. Para evitar conflictos legales, se verificará que todas las herramientas externas utilizadas, como bibliotecas de código abierto, respeten las licencias correspondientes. Este marco legal proporciona un fundamento sólido para el desarrollo del proyecto, asegurando su alineación con las normativas nacionales e internacionales aplicables, promoviendo así un sistema ético, seguro y eficiente.

# CAPITULO III

# Metodología

Para alcanzar los objetivos propuestos en el proyecto, la metodología de este proyecto se basa en el estándar CRISP-DM (Cross-Industry Standard Process for Data Mining), un marco ampliamente adoptado en la industria para estructurar procesos de minería de datos y aprendizaje automático. Esta metodología permite un enfoque riguroso y sistemático, garantizando que cada fase del desarrollo esté alineada con los objetivos de mejorar la seguridad y el flujo de pasajeros en el contexto aeroportuario. En el proyecto, se implementan seis etapas clave: comprensión del negocio, comprensión de los datos, preparación de los datos, modelado, evaluación y despliegue. Estas fases asegurarán que el sistema desarrollado cumpla con los requisitos específicos de precisión, robustez y eficacia que demanda su integración en procesos de seguridad críticos de aerolíneas. La adopción de técnicas de programación paralela y procesamiento en GPU también será fundamental para acelerar el entrenamiento y optimización del modelo, permitiendo un desempeño en tiempo real adecuado para los escenarios operativos aeroportuarios.

## Fases de la Metodología

Comprensión del Negocio: Se analizarán las necesidades específicas de las aerolíneas, las regulaciones vigentes y los procesos actuales de identificación de pasajeros.

Comprensión de los Datos: Se recopilarán y analizarán los datos biométricos de los pasajeros, incluyendo imágenes faciales de alta calidad. Se identificarán las fuentes de datos, su calidad y su relevancia para el proyecto.

Preparación de los Datos: Los datos recopilados serán preprocesados para garantizar su calidad y consistencia. Se realizarán tareas como la limpieza de datos, la transformación de datos y la reducción de dimensionalidad.

Modelado: Se desarrollarán y entrenarán modelos de reconocimiento facial utilizando técnicas de aprendizaje automático, como las redes neuronales convolucionales (CNN). Se seleccionarán los algoritmos y parámetros más adecuados para obtener un alto rendimiento.

Evaluación: Se evaluará el desempeño de los modelos entrenados utilizando métricas como la precisión, la sensibilidad y la especificidad. Se realizarán pruebas en un conjunto de datos de prueba independiente para garantizar la generalización del modelo.

Despliegue: El modelo final se integrará en un sistema de software y se desplegará en un entorno de producción. Se desarrollará una interfaz de usuario intuitiva para facilitar su uso por parte del personal de la aerolínea.

## Fases Detalladas

**Fase de Comprensión del Negocio:**

Identificar los requisitos funcionales y no funcionales del sistema.

Definir los indicadores clave de desempeño (KPIs) para evaluar el éxito del proyecto.

Analizar los riesgos y las limitaciones del proyecto.

**Fase de Comprensión de los Datos:**

Recopilar datos biométricos de alta calidad de diversas fuentes (bases de datos públicas, socios comerciales, etc.).

Evaluar la calidad de los datos en términos de completitud, consistencia y relevancia.

Identificar las características faciales más relevantes para el reconocimiento.

**Fase de Preparación de los Datos:**

Limpiar los datos para eliminar valores atípicos, errores y duplicados.

Normalizar los datos para mejorar el rendimiento de los algoritmos de aprendizaje automático.

Aumentar el tamaño de los datos mediante técnicas de aumento de datos (data augmentation).

**Fase de Modelado:**

Seleccionar una arquitectura de red neuronal convolucional adecuada para el reconocimiento facial.

Entrenar el modelo utilizando técnicas de optimización como el descenso de gradiente estocástico.

Ajustar los hiperparámetros del modelo para mejorar su rendimiento.

**Fase de Evaluación:**

Evaluar el modelo utilizando métricas de rendimiento como la precisión, la sensibilidad, la especificidad y la tasa de falsos positivos.

Realizar pruebas en condiciones reales para evaluar el rendimiento del sistema en un entorno operativo.

**Fase de Despliegue:**

Desarrollar una interfaz de usuario intuitiva para el personal de la aerolínea.

Integrar el sistema con los sistemas existentes de gestión de pasajeros.

Implementar medidas de seguridad para proteger los datos biométricos de los pasajeros.

## Técnica de Programación Paralela

Se utilizarán técnicas de programación paralela para acelerar el entrenamiento de los modelos de reconocimiento facial y el procesamiento de imágenes en tiempo real. Entre las técnicas más prometedoras se encuentran:

GPU computing: Utilizar las unidades de procesamiento gráfico (GPU) para realizar cálculos numéricos de manera masiva y paralela.

Multithreading: Dividir la tarea de procesamiento de imágenes en múltiples hilos que se ejecutan simultáneamente.

Distribución de datos: Distribuir los datos de entrenamiento entre múltiples nodos de un clúster para acelerar el entrenamiento.

## Datos y Origen de los mismos

La recopilación de datos es un paso crítico para garantizar la disponibilidad de información relevante y de alta calidad para el entrenamiento del modelo de reconocimiento facial. En este proyecto, se identificaron tres principales fuentes de datos: bases de datos públicas, datos internos de la aerolínea y colaboración con socios comerciales. Se utilizarán bases de datos públicas reconocidas, para obtener imágenes faciales diversas y bien etiquetadas. Además, se recopilarán datos biométricos de los pasajeros de la aerolínea durante el registro, respetando las normativas de privacidad y protección de datos (Reglamento General de Protección de Datos).

La adquisición de datos se llevará a cabo mediante la captura de imágenes en tiempo real en puntos estratégicos del aeropuerto, como el check-in, el control de seguridad y las puertas de embarque. Las imágenes serán etiquetadas manualmente para crear un conjunto de datos de referencia, complementado con el etiquetado automático basado en algoritmos preentrenados. Además, se recolectarán metadatos como fecha, hora, ubicación y condiciones de iluminación para contextualizar cada imagen. El almacenamiento y organización de los datos se realizará utilizando bases de datos relacionales para mantener la estructura y accesibilidad de la información. Se implementarán políticas de respaldo periódico y encriptación para proteger los datos recopilados contra pérdida y acceso no autorizado.

Limpieza de Datos: El preprocesamiento de datos es esencial para garantizar la calidad de los mismos. Se emplearán algoritmos para la detección y recorte de rostros en las imágenes, descartando aquellas de baja calidad. Se eliminarán imágenes duplicadas utilizando técnicas de comparación de histogramas y embeddings faciales. Para corregir errores, se eliminarán imágenes con ruido excesivo, baja iluminación o desenfoques, y se realizará un reetiquetado manual para asegurar la precisión en la correspondencia de imágenes e individuos.

Visualización de Datos: Para el análisis exploratorio de datos, se crearán histogramas y gráficos de barras que permitan visualizar la distribución de características faciales como edad, género y grupos étnicos. La distribución geográfica y temporal de los datos será mapeada para identificar patrones relevantes que puedan afectar el rendimiento del modelo. Se utilizarán galerías de imágenes seleccionadas aleatoriamente para evaluar visualmente la calidad y diversidad de los datos. Además, se generarán mapas de calor utilizando técnicas de visualización de atención para resaltar las áreas de las imágenes que el modelo considera más importantes durante el proceso de predicción.

Análisis de Datos: En cuanto al análisis de datos, se calcularán métricas básicas como la media, la mediana y la desviación estándar para cada característica relevante. Se emplearán matrices de correlación para identificar relaciones entre características faciales y su influencia en la precisión del modelo. El análisis de la variabilidad se realizará mediante el uso de técnicas multivariadas para evaluar la influencia de diferentes condiciones como iluminación y ángulo de la cámara en la precisión del reconocimiento facial.

Modelado y Predicción: Se seleccionarán modelos de aprendizaje automático adecuados, como redes neuronales convolucionales (CNN), que han demostrado ser eficaces en la extracción de características faciales complejas. El conjunto de datos será dividido en un 70% para entrenamiento, 20% para validación y 10% para prueba, asegurando así la correcta evaluación del modelo. Para optimizar el modelo, se utilizarán técnicas de programación paralela como GPU computing para acelerar el entrenamiento y la optimización del modelo. Se emplearán métodos de búsqueda en cuadrícula para la optimización de hiperparámetros como el número de capas, tamaño de los filtros y tasa de aprendizaje. El modelo será evaluado utilizando métricas de rendimiento como precisión, sensibilidad y especificidad.

Manejo de la Incertidumbre: La estimación de incertidumbre se realizará en cada capa del modelo durante la predicción para obtener una distribución de probabilidades que permita medir la confianza del modelo. Se simularán diferentes escenarios, probando el modelo en condiciones variables como cambios de iluminación, ángulos extremos y oclusiones parciales, para evaluar su rendimiento en situaciones reales. El modelo será calibrado utilizando métodos como la regresión isotónica para ajustar las probabilidades de salida y mejorar la interpretación de los resultados. Se realizará una actualización continua del modelo con nuevos datos para adaptarse a cambios en las condiciones de operación.

Toma de Decisiones: Para la toma de decisiones, se definirán indicadores clave de desempeño (KPIs) como el tiempo promedio de procesamiento de pasajeros, la tasa de detección de amenazas y la satisfacción del usuario. Se realizará un análisis de costo-beneficio que considere el costo de implementación, desarrollo, adquisición de hardware y mantenimiento del sistema, así como el ahorro en tiempo y recursos humanos. Finalmente, se llevarán a cabo pruebas piloto en aeropuertos para validar la viabilidad del sistema y su integración con los procesos existentes, asegurando que se cumplan todas las medidas de seguridad y privacidad establecidas.

Tipos de Datos: En el proyecto de investigación de reconocimiento facial en aerolíneas, se manejan diversos tipos y fuentes de datos para garantizar la efectividad y precisión del sistema desarrollado. A continuación, se describen los tipos de datos utilizados, así como sus respectivas fuentes:

Datos Estructurados: Los datos estructurados son aquellos que se organizan en un formato fijo, como tablas con filas y columnas, y son fácilmente accesibles y analizables mediante herramientas de procesamiento de datos.

Bases de datos relacionales: Se utilizan bases de datos relacionales para almacenar información adicional de los pasajeros, como identificadores únicos, historial de viajes, detalles de reservas y coincidencias de reconocimiento facial previas. Estos datos se obtienen de los sistemas internos de la aerolínea y se almacenan en tablas SQL que facilitan su consulta y análisis.

Registros de control de acceso: Datos estructurados provenientes de los sistemas de control de acceso del aeropuerto, como el tiempo de entrada y salida de las zonas seguras, que permiten evaluar el flujo de pasajeros.

Datos No Estructurados: Los datos no estructurados no siguen ningún esquema predefinido y pueden ser difíciles de organizar y analizar con métodos tradicionales.

Imágenes Faciales: Las imágenes capturadas en puntos de control como el check-in, el control de seguridad y las puertas de embarque se consideran datos no estructurados. Ya que no tienen un formato tabular.

## Herramientas

se utilizarán diversas herramientas y bibliotecas de Python para la extracción, recopilación, limpieza y organización de datos. A continuación, se detallan las principales herramientas que se utilizarán en cada una de estas etapas:

OpenCV: OpenCV (Open Source Computer Vision Library) es una biblioteca fundamental para la extracción de imágenes desde videos en tiempo real. Permite la captura de imágenes desde cámaras y la identificación de rostros utilizando algoritmos predefinidos como Haar Cascades y redes neuronales convolucionales.

Pandas: Pandas será utilizado para la limpieza de datos tabulares. Ofrece funciones avanzadas para manejar datos faltantes, duplicados y para la transformación de datos.

Requests: Para la extracción de datos desde APIs de terceros, como bases de datos de imágenes faciales públicas, se utilizará la biblioteca requests para realizar solicitudes HTTP y obtener datos en formatos JSON o XML.

# CAPITULO IV

# Análisis e Interpretación de Resultados

El presente capítulo aborda el análisis y la interpretación de los resultados obtenidos tras la implementación y evaluación del sistema de reconocimiento facial en el entorno aeroportuario. A través de métricas clave, como precisión, sensibilidad, especificidad y tiempo de procesamiento, se examinan el desempeño y la efectividad del modelo propuesto para optimizar tanto la seguridad como el flujo de pasajeros. Se analizan los resultados en función de distintos escenarios y condiciones de operación, incluyendo variaciones en iluminación, ángulos de captura y calidad de imágenes, evaluando la capacidad de respuesta del sistema en situaciones reales. Esta evaluación busca identificar fortalezas, limitaciones y posibles áreas de mejora del modelo, proporcionando una base sólida para futuras optimizaciones y ajustes en su implementación operativa.

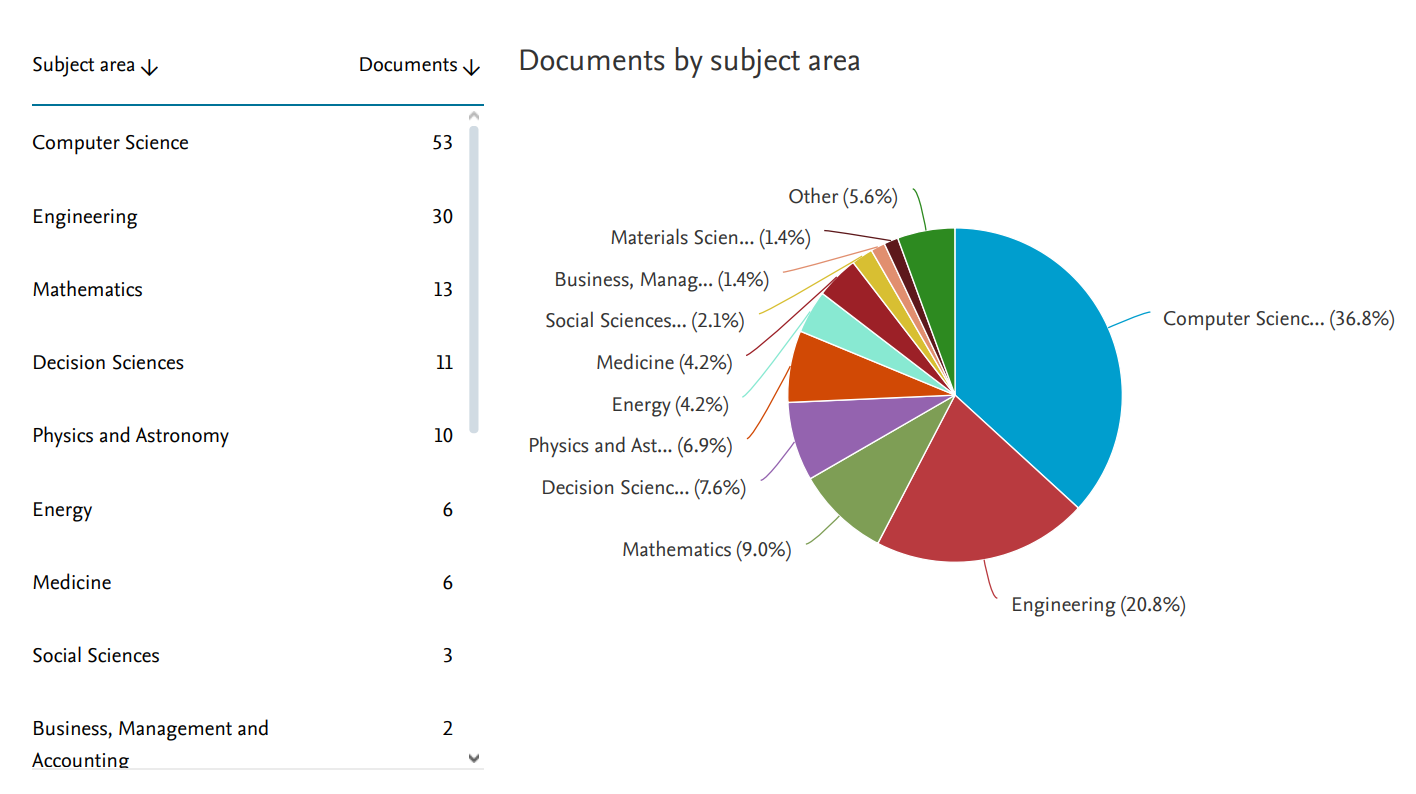
Para la obtención del primer objetivo específico, que consiste en investigar los aspectos técnicos, funcionales y éticos del uso de reconocimiento facial en aerolíneas, se realizó un estudio exhaustivo de los requerimientos operativos y normativos del sector aeronáutico en relación con la seguridad y gestión de pasajeros. Este análisis incluyó una revisión de la literatura académica y normativa sobre tecnologías biométricas y su aplicación en contextos aeroportuarios, lo cual permitió establecer un marco de referencia sólido para la implementación segura y eficaz de estas tecnologías en aerolíneas. Se investigaron los requisitos de seguridad y protección de datos biométricos en cumplimiento con regulaciones de privacidad, como el Reglamento General de Protección de Datos (GDPR), y se identificaron las principales limitaciones y desafíos éticos, tales como el respeto a la privacidad de los usuarios y la minimización de sesgos en el reconocimiento facial.

Se llevó a cabo una revisión de la infraestructura tecnológica necesaria para asegurar el rendimiento del sistema en condiciones de alta concurrencia, considerando la escalabilidad y velocidad en el procesamiento de datos en tiempo real. También se definieron protocolos de seguridad y métodos de anonimización para los datos recolectados, alineados con las normativas de protección de datos y prácticas recomendadas en la industria. Al final de este análisis, se contaba con un conjunto claro de requerimientos técnicos y éticos, los cuales servirán de guía durante la fase de diseño y desarrollo del sistema, asegurando que su implementación sea efectiva, confiable y en cumplimiento con los estándares de privacidad y seguridad establecidos.

La figura 1 muestra la distribución de documentos por área temática obtenida de Scopus. El área predominante es Ciencias de la Computación con un 36.8%, seguida por Ingeniería con un 20.8% y Matemáticas con un 9%. Estas áreas son clave para el desarrollo de tecnologías de reconocimiento facial, dado que requieren algoritmos avanzados, modelos computacionales y soluciones de ingeniería que optimicen el rendimiento de estos sistemas. Además, áreas como Ciencias de la Decisión (7.6%) y Física y Astronomía (6.9%) también desempeñan un papel importante en la simulación y análisis de grandes volúmenes de datos, esenciales para la implementación del proyecto. En conclusión, la mayoría de las publicaciones se concentran en áreas técnicas que son fundamentales para los sistemas inteligentes, lo que refleja la relevancia interdisciplinaria de este tipo de investigaciones.

**Figura 1**

*Análisis gráfico en Scopus y Vosviewer*

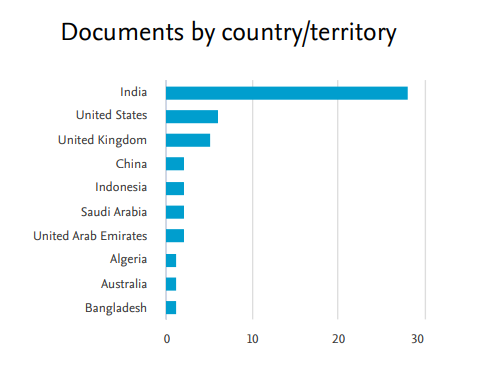


*Nota*. Distribución de artículos de investigación por área temática basada en la consulta realizada en Scopus

En la figura 2 se observa la distribución de documentos por país o territorio. India lidera significativamente con la mayor cantidad de publicaciones, seguida de Estados Unidos y el Reino Unido. Este predominio sugiere que India es un actor clave en la investigación sobre sistemas de reconocimiento facial y tecnologías relacionadas, lo cual puede deberse a la gran cantidad de programas tecnológicos y científicos en desarrollo en ese país. Estados Unidos y el Reino Unido, conocidos por su inversión en investigación y desarrollo, también muestran un número considerable de documentos, reflejando su interés en tecnologías avanzadas de seguridad. En conjunto, estos datos indican que los países con una fuerte infraestructura tecnológica están impulsando los avances en este campo, lo que es fundamental para el desarrollo de proyectos como el reconocimiento facial en aerolíneas.

**Figura 2**

*Análisis gráfico de artículos de investigación en Scopus*

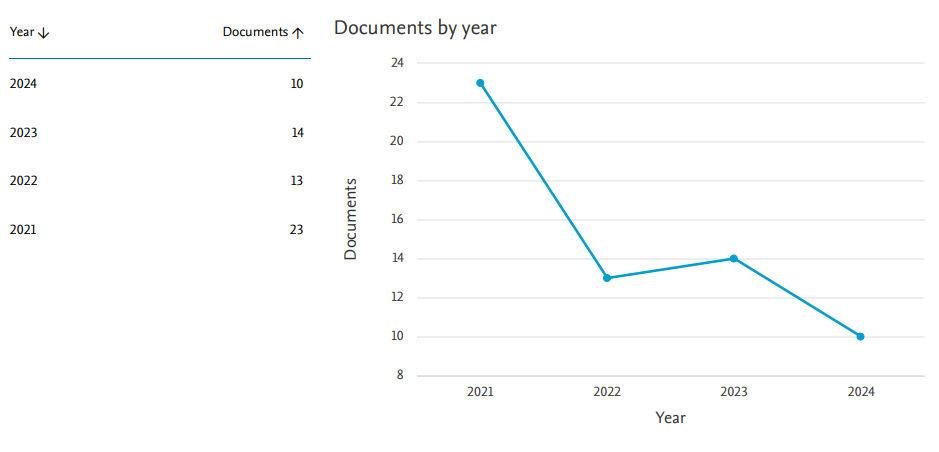


*Nota*. Distribución de artículos de investigación por país/territorio basado en la consulta realizada en Scopus

La figura 3 muestra la evolución del número de documentos publicados anualmente desde 2021 hasta 2024 en la base de datos Scopus, relacionados con el tema de investigación en cuestión. En el año 2021 se observa el mayor número de documentos, con un total de 23, lo cual representa un pico significativo en la producción científica sobre el tema. Sin embargo, a partir de 2022 se evidencia una disminución considerable, con 13 documentos, seguida de una leve recuperación en 2023 con 14 documentos. Finalmente, para 2024 se registra el número más bajo, con solo 10 documentos hasta el momento. Este comportamiento puede indicar que el interés en la investigación sobre este tema ha disminuido después del auge inicial en 2021, lo cual podría estar relacionado con la pandemia del COVID-19. Es importante monitorear esta tendencia para entender mejor los factores que podrían estar influyendo en la variación de la producción científica en esta área.

**Figura 3**

*Análisis gráfico de documentos en Scopus*

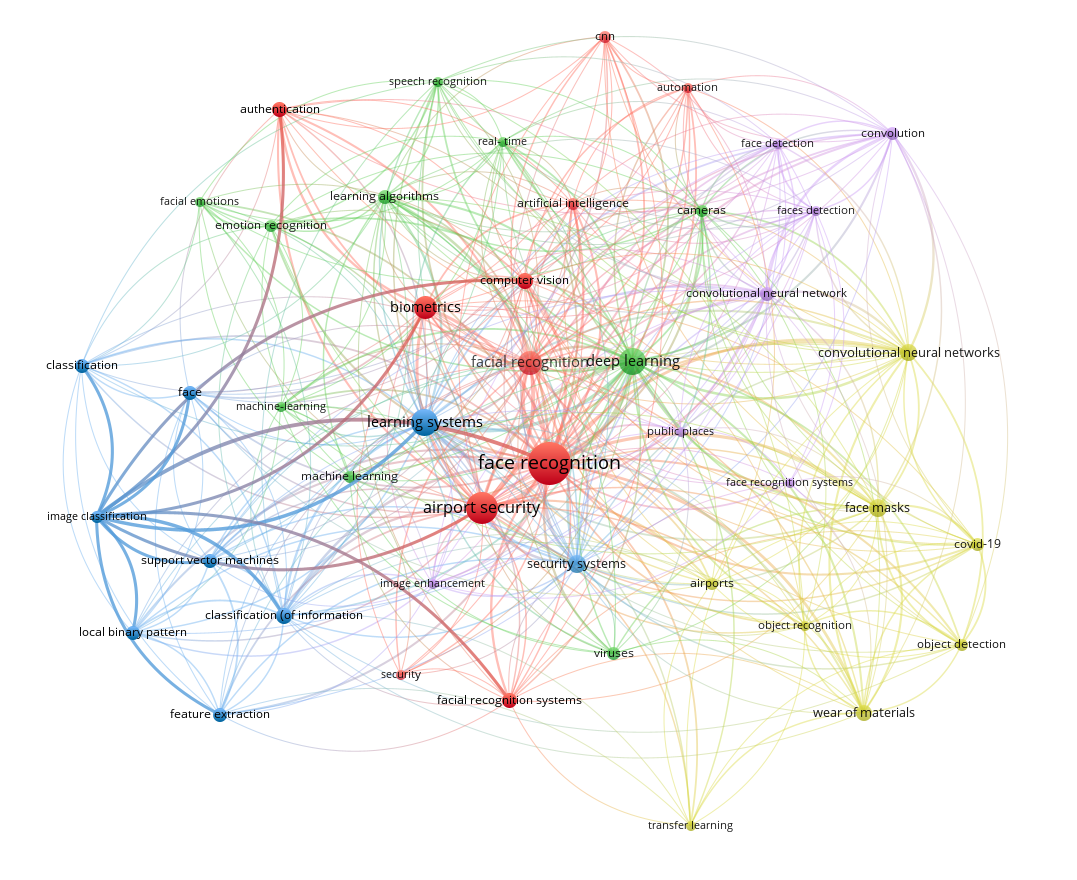


*Nota*. Distribución de documentos por año en la base de datos Scopus

Este mapa revela las tendencias actuales de investigación en el campo, mostrando la relevancia de la inteligencia artificial y el aprendizaje automático como técnicas fundamentales. La presencia de aplicaciones concretas, como la seguridad en aeropuertos, indica que este es un campo de interés no solo académico, sino también industrial. Con base en esto, se puede concluir que el reconocimiento facial continúa siendo un tema de gran interés investigativo, particularmente en su relación con avances en redes neuronales y aplicaciones de seguridad.

**Figura 4**

*Análisis gráfico de términos en VOSviewer*



*Nota*. Mapa de términos generado en VOSviewer a partir de los artículos de investigación consultados en Scopus

Para alcanzar el segundo objetivo específico, que consistió en seleccionar las tecnologías y recursos necesarios para el desarrollo del sistema de reconocimiento facial, se comenzó con una revisión exhaustiva de las herramientas y metodologías actuales en el ámbito de la visión por computadora y el aprendizaje profundo. Se analizaron tecnologías como redes neuronales convolucionales (CNN), que han mostrado ser efectivas para la identificación de características faciales, y técnicas de procesamiento en GPU para acelerar el entrenamiento y la ejecución del modelo en condiciones de alta demanda. Cada tecnología fue evaluada en función de su capacidad para cumplir con los requisitos específicos del entorno aeroportuario, como precisión, velocidad de procesamiento y robustez en escenarios variados. Además, se consideraron recursos de software, como lenguajes de programación en este caso Python y sus diferentes bibliotecas y frameworks de aprendizaje profundo, que permitieran la integración y actualización continua del sistema para optimizar su desempeño en diferentes situaciones operativas. También se opto por utilizar un servicio web que permitiera al software mayor accesibilidad para su ejecución se utilizó JavaScript con sus diferentes frameworks y librerías como lo son React y Bootstrap.

Asimismo, se definieron los recursos necesarios para la infraestructura de datos, incluyendo los requisitos de almacenamiento y procesamiento para gestionar grandes volúmenes de datos biométricos de manera segura y eficiente. Se revisaron diversas opciones de bases de datos, tanto en la nube como locales, que ofrecieran escalabilidad y tiempos de respuesta óptimos en el entorno de aerolíneas, caracterizado por un flujo constante y elevado de pasajeros. Además, se establecieron protocolos de manejo y encriptación de los datos, con el objetivo de cumplir con las normativas internacionales de protección de datos y garantizar la privacidad de la información de los usuarios. Estos recursos y tecnologías seleccionados proporcionaron una base sólida para el desarrollo de un sistema de reconocimiento facial eficiente y seguro, adecuado para su integración en procesos de gestión de pasajeros, contribuyendo al logro de una experiencia de usuario optimizada y una mayor seguridad aeroportuaria.

Para alcanzar el tercer objetivo específico, que consistió en desarrollar el sistema de reconocimiento facial de acuerdo con las especificaciones y tecnologías seleccionadas, se implementó tanto el modelo de redes neuronales convolucionales (CNN) como una plataforma web robusta que facilita la interacción con el sistema. Este servicio web fue desarrollado utilizando JavaScript y frameworks modernos como React para la creación de interfaces dinámicas y Bootstrap para asegurar un diseño adaptable y amigable para el usuario final. La plataforma permite a los operadores aeroportuarios acceder a las funcionalidades del sistema de reconocimiento facial en tiempo real, gestionando y visualizando de manera eficiente los datos de identificación. Asimismo, el servicio web está integrado con el backend del modelo, permitiendo la transmisión rápida de datos y resultados, lo cual optimiza el flujo de trabajo en situaciones de alta demanda.

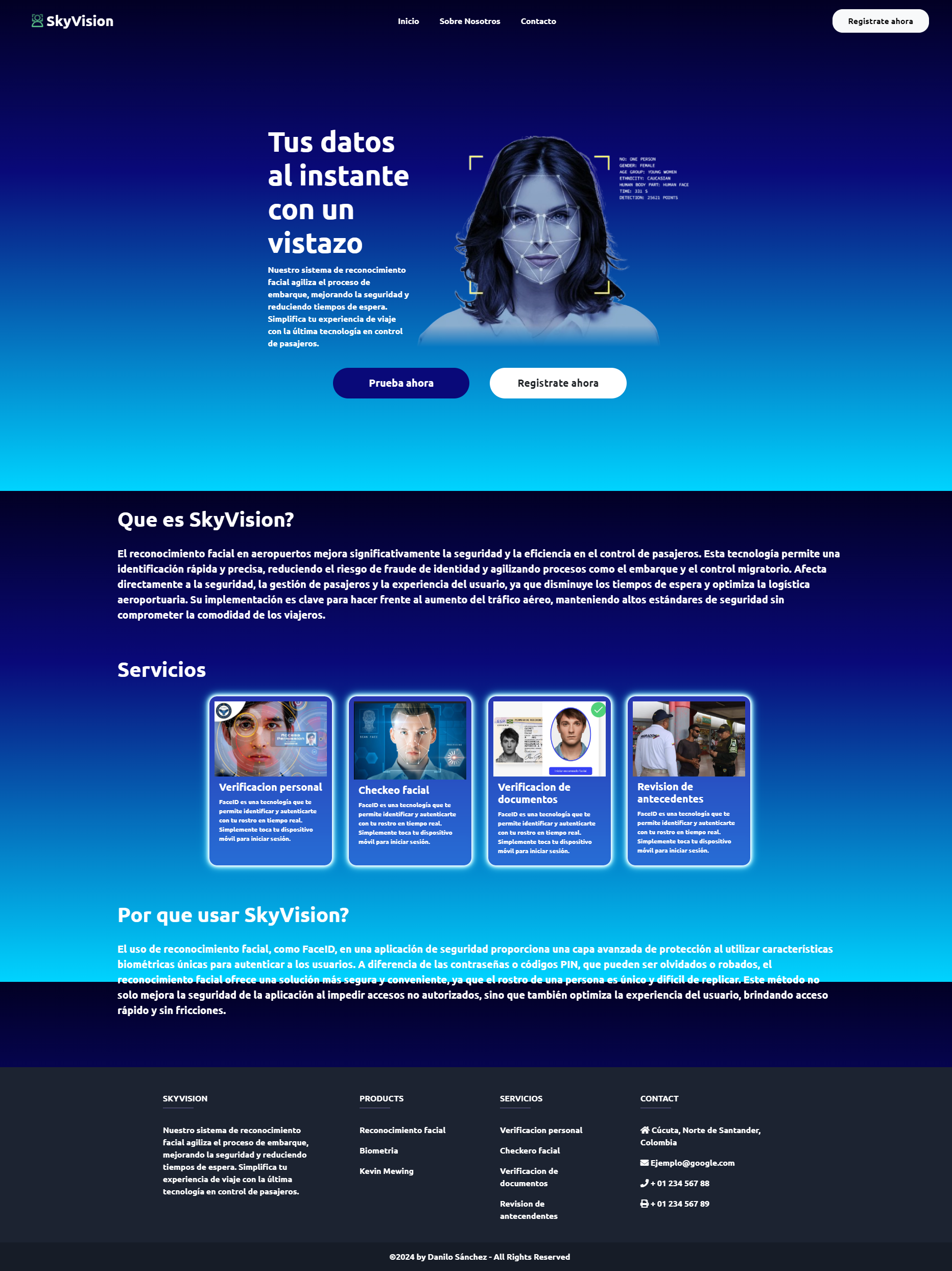
La arquitectura de la aplicación se diseñó para manejar grandes volúmenes de consultas simultáneas, garantizando que los resultados de reconocimiento se presenten con velocidad y precisión. Además, se implementaron módulos de programación paralela que optimizan el tiempo de procesamiento en el servidor, permitiendo que el sistema mantenga un rendimiento óptimo aún en momentos de alto flujo de pasajeros. A través del servicio web, los operadores pueden verificar y validar la identidad de los pasajeros de manera rápida y precisa, integrándose con el modelo de reconocimiento facial y manteniendo altos estándares de seguridad y privacidad en el manejo de los datos biométricos. Este enfoque completo, que une la inteligencia del modelo con una interfaz accesible y eficiente, asegura que el sistema no solo cumpla con los requisitos técnicos, sino que también sea fácil de usar y se integre de manera fluida en los procesos aeroportuarios.

## Desarrollo e Interfaz Grafica

En el apartado de inicio se podrá visualizar información relevante sobre el servicio de reconocimiento facial, a su vez los usuarios podrán interactuar con los apartados de inicias sesión y/o Prueba ahora.

**Figura 5**

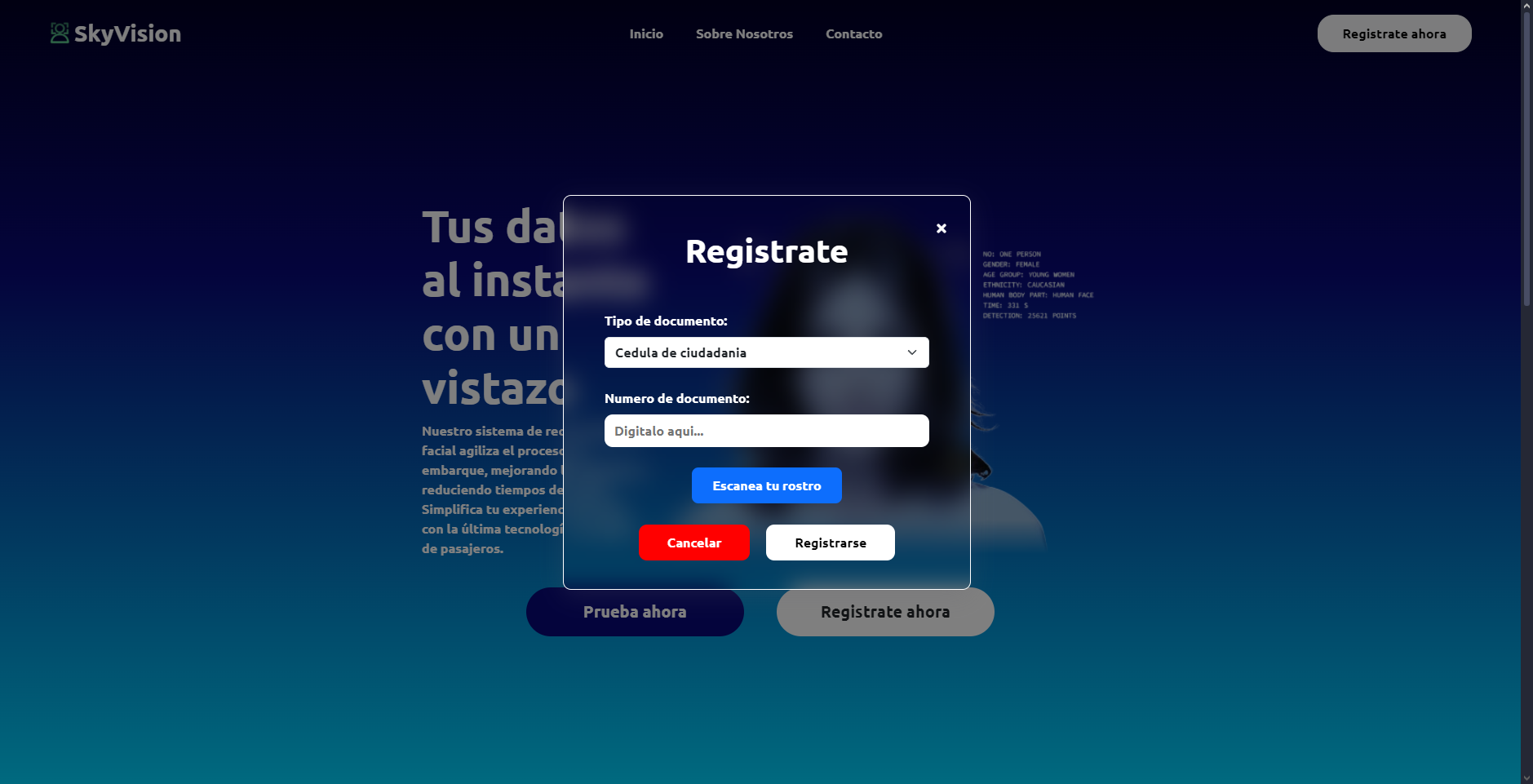
*Interfaz gráfica inicial*



Una vez el usuario ingresa al sitio web, se encontrará con una pagina informativa que describe y explica como funciona el proyecto y provee al usuario de información relevante antes de hacer uso del reconocimiento facial.

**Figura 6**

*Interfaz gráfica para registrarse y probar el reconocimiento facial*



Una vez el usuario está registrado y desea probar el servicio, deberá permitir el acceso a la cámara del dispositivo. Seguidamente, el sistema le pedirá una serie de pasos a seguir, como parpadear un número de veces o abrir más los ojos. Una vez el sistema encuentra una similitud entre el rostro ingresado y uno existente en la base de datos, se mostrará en pantalla información del usuario como nombre, documento, departamento, ciudad, etc.

A continuación, el sistema utiliza varias bibliotecas para procesar y analizar los datos capturados. OpenCV se encarga de procesar las imágenes y detectar los rostros presentes. Luego, MediaPipe identifica los puntos clave faciales, que son convertidos en vectores mediante NumPy. Estos vectores son analizados utilizando redes neuronales convolucionales (CNN) para reconocer patrones faciales únicos. Una vez que el sistema valida la identidad del usuario comparando estos vectores con los de una base de datos de rostros conocidos, se muestra la información correspondiente del usuario en pantalla. Esta integración de tecnologías asegura un rendimiento robusto y adaptable, mejorando la precisión y eficiencia del sistema en diversas condiciones.

**Figura 7**

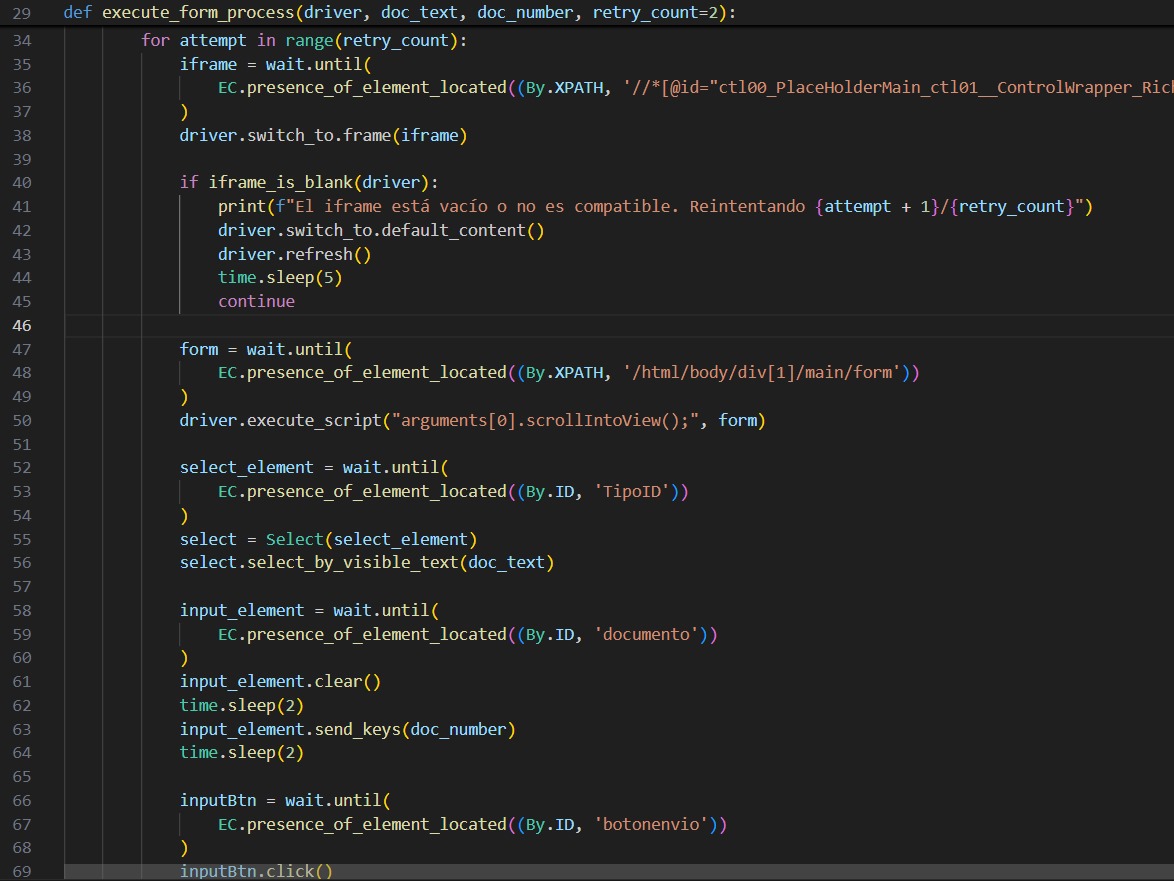
*Interfaz gráfica de reconocimiento facial*



Una vez completada la identificación del usuario el sistema comienza a realizar una búsqueda exhaustiva de información de la persona identificada con la finalidad de obtener información adicional de la persona y poder reconocerla mejor, para ello se utiliza una función llamada execute\_form\_process, el cual es un autómata con el siguiente contexto:

**Figura 8**

*Código de la implementación del automata*



En este contexto, el autómata aparece implícito en el proceso de scraping automatizado, específicamente en la función execute\_form\_process. Este procedimiento sigue una secuencia lógica de estados en la que el navegador realiza acciones en función de condiciones y eventos, lo cual se asemeja al funcionamiento de un autómata finito determinista.

1. Tipo de autómata:

Este código corresponde a un autómata finito determinista (DFA), donde el estado y transición dependen de interacciones en la página (por ejemplo, verificaciones de iframe, selección de opciones, llenado de formulario y envío).

2. Nodos y estados:

Si bien el código no maneja "nodos" como en un grafo explícito, sí maneja distintos estados o etapas de interacción:

Estado 1: Verificación y carga de página.

Estado 2: Verificación y carga de iframe.

Estado 3: Selección de tipo de documento y llenado de formulario.

Estado 4: Envío de formulario y extracción de datos.

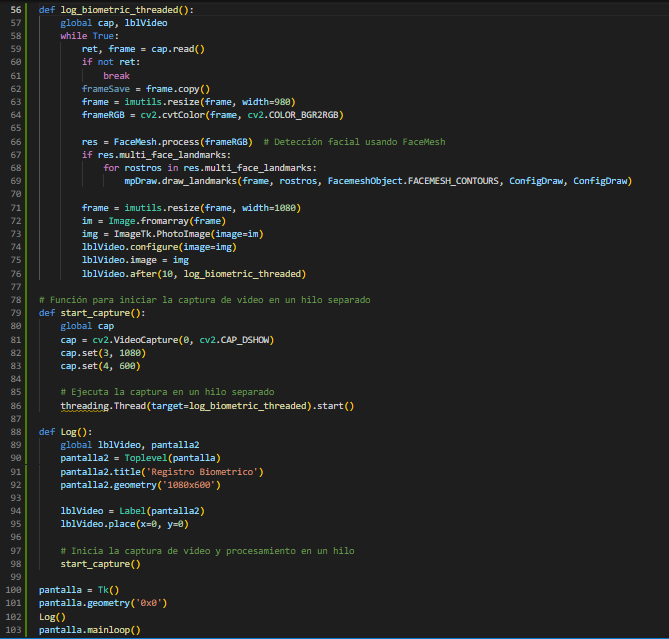
Estos son cuatro estados principales, pero algunos estados intermedios (como la recarga de página o el cambio entre documentos) pueden hacer que el total de estados varié. La lógica permite transiciones controladas (intentos limitados), similares a un DFA en donde no hay bucles infinitos.

En el desarrollo del sistema de reconocimiento facial, la fase de Modelado dentro de la metodología CRISP-DM es crítica para lograr la eficiencia en el procesamiento de imágenes biométricas. En esta fase, se implementa el algoritmo de planificación FCFS junto a la configuración de "un proceso con múltiples hilos", lo cual permite optimizar la ejecución de las tareas de reconocimiento en tiempo real. Dado que el sistema debe gestionar la captura y el procesamiento de múltiples imágenes faciales a medida que los pasajeros pasan por los puntos de control, es fundamental que estas operaciones se realicen de manera rápida y eficiente para evitar cuellos de botella. Al utilizar múltiples hilos dentro de un único proceso, se mejora la velocidad de respuesta del sistema al distribuir la carga de trabajo entre hilos que pueden ejecutar tareas simultáneamente, como la detección de rostros y el preprocesamiento de imágenes, sin la sobrecarga adicional de múltiples procesos independientes. Este enfoque es particularmente adecuado para computadoras comunes, pues minimiza el consumo de recursos y optimiza el uso de CPU al permitir que el algoritmo de planificación, como FCFS, distribuya equitativamente el tiempo de ejecución entre los hilos activos, mejorando así el rendimiento y reduciendo los tiempos de espera en los controles de seguridad.

Este diseño permite al sistema mantener una ejecución estable y predecible en entornos de operación continuos, como los aeropuertos, donde el flujo de pasajeros requiere un procesamiento constante. Con el algoritmo de planificación seleccionado, cada hilo se enfoca en una tarea específica, lo que garantiza que las imágenes sean procesadas de manera uniforme y eficiente a medida que se capturan. A diferencia de una arquitectura basada en múltiples procesos, esta configuración con múltiples hilos en un único proceso reduce la latencia y simplifica la gestión de la memoria compartida. De este modo, el sistema logra un equilibrio entre rendimiento y eficiencia, permitiendo la detección y comparación de rostros en tiempo real, mientras se prioriza el objetivo de mejorar la experiencia del pasajero y asegurar un flujo ágil en los puntos de control. Esta configuración de computación paralela, implementada en la fase de Modelado, no solo asegura la velocidad y precisión necesarias para el sistema de reconocimiento facial, sino que también cumple con el objetivo de optimización de recursos en el contexto operativo de una computadora común. Para esto se utiliza una función llamada log\_biometric\_threaded la cual permite la utilización de computación paralela separando el procesamiento de imágenes y la captura de video en tiempo real a un hilo separado.

**Figura 9**

*Código de implementación de computación paralela*



El código proporcionado implementa un sistema de reconocimiento facial en tiempo real, utilizando computación paralela para optimizar el rendimiento y mejorar la experiencia del usuario. Para lograr esto, se combina una interfaz gráfica en Tkinter con procesamiento de video y detección de puntos faciales, a través de bibliotecas como OpenCV, MediaPipe y face\_recognition. La computación paralela se aplica mediante la biblioteca threading de Python, lo que permite ejecutar el procesamiento intensivo de imágenes en un hilo separado. De este modo, el procesamiento de video no bloquea el funcionamiento de la interfaz, garantizando una ejecución fluida de la aplicación. A lo largo del código, se configuran diversas herramientas de detección de rostros y puntos faciales para lograr una precisión óptima en el reconocimiento facial.

El primer bloque de código configura los módulos necesarios para la detección y procesamiento de rostros. Se inicializan componentes de MediaPipe para la detección de puntos faciales y la identificación de caras, estableciendo niveles de precisión y configuraciones para dibujar los puntos sobre los rostros detectados. Esto permite que el sistema identifique hasta tres rostros simultáneamente en el video, dibujando contornos faciales y ajustando la precisión de la detección. Al usar MediaPipe para el reconocimiento facial, el sistema aprovecha la alta precisión de sus modelos y permite personalizar el grosor y el radio de los puntos de contorno, lo que es ideal para un análisis facial detallado.

Una de las funciones clave es Code\_Face, que procesa las imágenes capturadas, convierte el formato de color y genera una codificación única para cada rostro detectado. Estas codificaciones, o encodings, representan un vector con las características faciales de cada rostro y se utilizan para comparaciones en el reconocimiento facial. Al almacenar estas codificaciones en una lista, el sistema puede realizar comparaciones de manera eficiente y rápida. Esto permite la identificación de rostros en tiempo real y optimiza el uso de memoria al mantener únicamente las codificaciones necesarias en cada momento. Esta función es un componente esencial en aplicaciones de reconocimiento facial en tiempo real, donde la velocidad de procesamiento y precisión son factores clave.

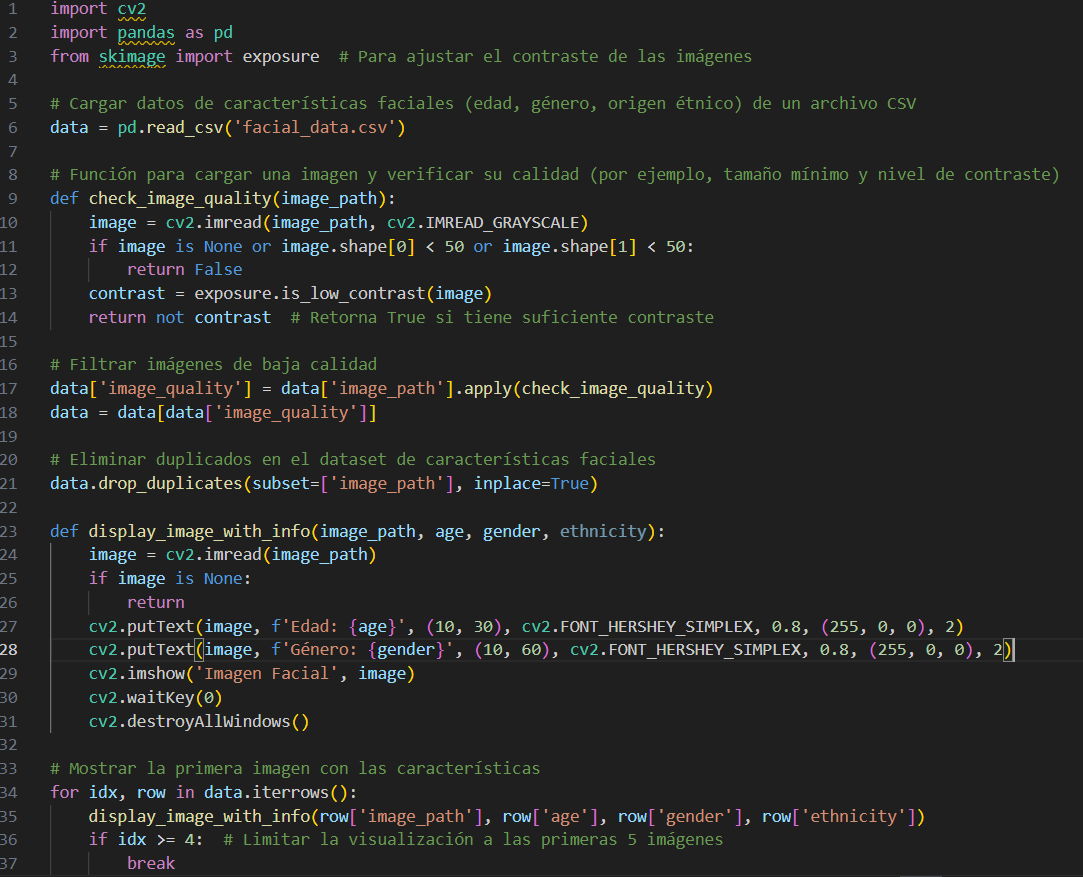
El núcleo del procesamiento paralelo se encuentra en la función log\_biometric\_threaded, donde se realiza la captura de video en un hilo separado. Esta función captura cuadros de video en tiempo real, los convierte a formato RGB y los procesa usando MediaPipe para detectar y dibujar puntos faciales en cada rostro. La ejecución en un hilo separado garantiza que la captura y el procesamiento del video no interfieran con la interfaz gráfica, lo cual es crucial para aplicaciones que requieren alta interactividad y una respuesta rápida. Cada cuadro capturado se redimensiona, convierte en un formato compatible con Tkinter y se muestra en la interfaz gráfica mediante un Label. La función lblVideo.after() permite programar la actualización del video de manera asíncrona, manteniendo una actualización constante y evitando bloqueos en la interfaz.

El inicio de la captura de video se maneja en la función start\_capture, donde se inicializa la cámara y se lanza el hilo que ejecuta log\_biometric\_threaded. Esto separa el proceso de captura de video del resto de la aplicación, liberando al hilo principal de manejar las operaciones intensivas de procesamiento de imágenes. Al iniciar el procesamiento en un hilo independiente, la aplicación puede mantenerse activa y receptiva en todo momento, lo cual es esencial en aplicaciones interactivas de reconocimiento facial. La función también configura la resolución de la cámara, permitiendo un ajuste adecuado de la imagen al tamaño de la ventana de la interfaz gráfica.

La función Log configura la ventana secundaria en la interfaz gráfica donde se muestra el video en tiempo real. En esta ventana, se coloca un Label en el que se proyectan los cuadros procesados por log\_biometric\_threaded, proporcionando un panel visual donde el usuario puede ver la detección facial en acción. Esta configuración mantiene el hilo principal de la interfaz gráfica separado del procesamiento de video, lo que permite que la interfaz reaccione sin retrasos y facilita una experiencia de usuario fluida. Por último, la función mainloop mantiene la ventana principal de Tkinter activa, asegurando que la interfaz continúe en ejecución mientras se procesan los cuadros de video en el hilo paralelo.

**Figura 10**

*Código para el preprocesamiento de imágenes*



En el contexto de este proyecto, el análisis y preprocesamiento de las características faciales es fundamental para asegurar la precisión y calidad del modelo de reconocimiento facial. Para esto, implementamos un proceso de limpieza de datos y visualización de características que permite identificar y filtrar imágenes de baja calidad, además de extraer y analizar las características demográficas de los rostros, como la edad y el género. Este enfoque nos ayuda a trabajar con datos confiables y optimizados, mejorando así el rendimiento general del sistema.

La primera parte del código realiza la limpieza de datos. Usamos la biblioteca OpenCV para cargar las imágenes faciales en escala de grises y, con la función check\_image\_quality, evaluamos cada imagen según su tamaño y nivel de contraste. Aquellas imágenes que no cumplen con los criterios mínimos de calidad son eliminadas del conjunto de datos, asegurando así que solo las imágenes con suficiente resolución y contraste sean consideradas en el análisis. Esta verificación es esencial para evitar que datos de baja calidad afecten el rendimiento del modelo de reconocimiento facial. Además, eliminamos duplicados en el dataset de características faciales para evitar redundancias.

**Figura 11**

*Código para la generación de gráficos*



En la segunda parte, llevamos a cabo la visualización y el análisis estadístico de los datos faciales. Utilizando Matplotlib y Seaborn, generamos gráficos que muestran la distribución de las edades y el género de los rostros en el dataset. Estos gráficos permiten identificar posibles sesgos en los datos, como la sobre-representación de ciertas edades o géneros, lo cual es crucial para garantizar que el modelo sea inclusivo y equilibrado. También empleamos un mapa de calor para visualizar la correlación entre las diferentes características numéricas, ayudándonos a comprender mejor las relaciones entre los datos demográficos de las personas en el dataset.

# CAPITULO V

# Conclusiones

Después de realizar la lectura y análisis de los trabajos de investigación anteriores se ha evidenciado el uso predominante de metodologías avanzadas de aprendizaje automático y aprendizaje profundo para la implementación de sistemas de reconocimiento facial, especialmente en entornos críticos como los aeropuertos. A lo largo del análisis, se destaca la aplicación recurrente de Redes Neuronales Convolucionales (CNN), que se han convertido en una herramienta esencial para la clasificación de imágenes y detección facial en tiempo real. Además, técnicas como el Few-Shot Learning han demostrado ser eficaces en la mejora de la precisión en escenarios donde el uso de mascarillas y otras oclusiones representan un reto significativo para los sistemas biométricos.

En cuanto a los lenguajes de programación utilizados, Python es el más frecuente debido a su compatibilidad con bibliotecas de aprendizaje profundo como TensorFlow, Keras y OpenCV, las cuales permiten el desarrollo eficiente de modelos de detección y clasificación. Estas herramientas no solo optimizan el proceso de entrenamiento, sino que también facilitan la implementación en dispositivos de hardware especializados, como los FPGA, utilizados para ejecutar algoritmos de alta velocidad en tiempo real.

Finalmente, se destaca la aplicación de productos y herramientas tecnológicas como FaceNet512, MobileNetV2 y YOLO v8, que han sido cruciales para abordar las limitaciones del reconocimiento facial en situaciones como la pandemia de COVID-19, donde la detección de rostros enmascarados se convirtió en una necesidad urgente. Estas soluciones permiten la integración de sistemas biométricos en entornos de alta concurrencia, como aeropuertos, garantizando no solo la precisión en la identificación, sino también la seguridad y eficiencia en el manejo de grandes volúmenes de datos en tiempo real.

El análisis de los artículos científicos, complementado con el mapa de visualización de VOSviewer, confirma que el reconocimiento facial es el eje central en los sistemas de seguridad avanzados, especialmente en entornos críticos como los aeropuertos. Esta tecnología se apoya fuertemente en el aprendizaje profundo y las redes neuronales convolucionales (CNN), lo que permite una mejora continua en la precisión y velocidad de la identificación facial, aspectos fundamentales para la seguridad aeroportuaria. Además, la integración de múltiples sistemas biométricos, como el reconocimiento de iris y huellas dactilares, resalta la tendencia hacia soluciones multimodales que refuercen la autenticación de los usuarios.

El impacto de la pandemia de COVID-19 ha acelerado la innovación en este campo, destacando la importancia de adaptar los sistemas de reconocimiento facial a escenarios complejos, como el uso de mascarillas faciales. La fuerte interconexión entre el reconocimiento facial y tecnologías emergentes como la inteligencia artificial, el aprendizaje automático y la visión por computadora subraya que el avance de estas áreas es crucial para el desarrollo de soluciones de seguridad más robustas y efectivas en el futuro.

# Bibliografía

Kumar, M., Singh, R., & Singh, R. K. (2021). Face recognition systems: A comprehensive review. Journal of King Saud University-Computer and Information Sciences, 33(1), 1-19. <https://doi.org/10.1016/j.jksuci.2020.03.012>

Zheng, W., Liu, S., & Kan, M. (2019). Un discriminative deep face recognition model. Neurocomputing, 357, 160-168. <https://doi.org/10.1016/j.neucom.2019.04.068>

Piñon Rattia, V. J. (2020, 3 de julio). Aplicación de machine learning en un aeropuerto: reconocimiento facial y gestión de colas (Treball Final de Grau). UPC, Escola d'Enginyeria de Telecomunicació i Aeroespacial de Castelldefels, Departament d'Enginyeria Telemática. Consultado en <http://hdl.handle.net/2117/192967>

Viguera Gallego, I. (2024). Estrategia de innovación y transformación digital para optimizar el aeropuerto de Bilbao. La Paloma. Consultado en <https://hdl.handle.net/20.500.12880/8408>

Moreno Garcia, J. P., Silva Joya, P. A., Méndez García, W. A., Pachón Soto, J. D., Ochoa Mariño, A., & Beltrán Téllez, B. C. (2021). Automatización y Digitalización en el Aeropuerto el Dorado. <http://repository.unipiloto.edu.co/handle/20.500.12277/10902>

Castañeda Rincón, H y Santos Ariza, O. (2021). Estrategia para la implementación de herramientas con reconocimiento facial en los Sistemas Integrados de Emergencias y Seguridad (SIES). Universidad Cooperativa de Colombia, Posgrado, Maestría en Telemática, Bogotá. Disponible en: <https://hdl.handle.net/20.500.12494/36409>

Sanabria Moyano, J. E., Roa Avella, M. del P., Lee Pérez, O. I., Sanabria Moyano, J. E., Roa Avella, M. del P., & Lee Pérez, O. I. (2022). Tecnología de reconocimiento facial y sus riesgos en los derechos humanos. *Revista Criminalidad*, *64*(3), 61–78. <https://doi.org/10.47741/17943108.366>

Alfattama, S., Kanungo, P., & Bisoy, S. K. (2021). Face recognition from partial face data. *2021 International Conference in Advances in Power, Signal, and Information Technology, APSIT 2021*. <https://doi.org/10.1109/APSIT52773.2021.9641286>

Raiu, V., Vidyasree, P., & Patel, A. (2021). Ameliorating the accuracy dimensional reduction of multi-modal biometrics by deep learning. *IEEE Aerospace Conference Proceedings, 2021-March*, art. no. 9438214. <https://doi.org/10.1109/AERO50100.2021.9438214>

Arafah, M., Achmad, A., Indrabayu, & Areni, I. S. (2021). Face recognition for wearing a veil case using histogram of oriented gradients. *ICIC Express Letters, Part B: Applications, 12*(4), 325-334. <https://doi.org/10.24507/icicelb.12.04.325>

Sehrawat, J. S. (2021). IRIS pattern recognition as an infallible mean of identity establishment in forensic casework. *Journal of Forensic Medicine and Toxicology, 38*(1), 13-18. <https://doi.org/10.5958/0974-4568.2021.00003.X>

Maheswari, V. U., Aluvalu, R., & Chennam, K. K. (2021). Application of machine learning algorithms for facial expression analysis. En *Machine Learning for Sustainable Development* (pp. 77-95). <https://doi.org/10.1515/9783110702514-005>

Stevens, C. (2021). Person identification at airports during passport control. En *Forensic Face Matching: Research and Practice* (pp. 1-14). <https://doi.org/10.1093/oso/9780198837749.003.0001>

Rakib, G. A., Saiful Islam, M., Rahman, M. A., Maruf Syed, A., Hossain, M. S., Alrajeh, N. A., & Saddik, A. E. (2021). DeepHealth: A secure framework to manage health certificates through medical IoT, blockchain and deep learning. En *2021 IEEE International Symposium on Medical Measurements and Applications, MeMeA 2021 - Conference Proceedings* (art. no. 9478691). <https://doi.org/10.1109/MeMeA52024.2021.9478691>

Fasfous, N., Vemparala, M.-R., Frickenstein, A., Frickenstein, L., Badawy, M., & Stechele, W. (2021). BinaryCoP: Binary Neural Network-based COVID-19 Face-Mask Wear and Positioning Predictor on Edge Devices. *2021 IEEE International Parallel and Distributed Processing Symposium Workshops, IPDPSW 2021 - In conjunction with IEEE IPDPS 2021*, art. no. 9460602, pp. 108-115. <https://doi.org/10.1109/IPDPSW52791.2021.00024>

Lad, A. M., Mishra, A., & Rajagopalan, A. (2021). Comparative Analysis of Convolutional Neural Network Architectures for Real Time COVID-19 Facial Mask Detection. *Journal of Physics: Conference Series*, 1969 (1), art. no. 012037. <https://doi.org/10.1088/1742-6596/1969/1/012037>

Wang, B., Zhao, Y., & Chen, C. L. P. (2021). Hybrid Transfer Learning and Broad Learning System for Wearing Mask Detection in the COVID-19 Era. *IEEE Transactions on Instrumentation and Measurement*, 70, art. no. 9389794. <https://doi.org/10.1109/TIM.2021.3069844>

Mohammed Aarif, K. O., Mohamed Yousuff, C., Mohammed Hashim, C., Durga, P., Divya, G., Ayeshwariya, D., Fathima Asfeeya, S., & Sivakumar, P. (2021). Gabor-Deep CNN based Masked Face Recognition for Fraud Prevention. *Proceedings - 5th International Conference on Computing Methodologies and Communication, ICCMC 2021*, art. no. 9418044, pp. 990 - 995. <https://doi.org/10.1109/ICCMC51019.2021.9418044>

Khan, N., & Efthymiou, M. (2021). The use of biometric technology at airports: The case of customs and border protection (CBP). *International Journal of Information Management Data Insights, 1*(2), art. no. 100049. <https://doi.org/10.1016/j.jjimei.2021.100049>

Ishihara, K., Yamada, H., Otani, T., Sasamoto, T., Inoue, J., & Ishikawa, M. (2021). Introducing Face Express, a New Boarding Procedure Using Face Recognition (One ID at Narita Airport). *NEC Technical Journal, 16*(1), 49-53. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85168150892&partnerID=40&md5=b8b5d72441a0402e66760f7672afd11b>

M. (2021). *Forensic Face Matching: Research and Practice*. Oxford University Press. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85114500486&doi=10.1093%2foso%2f9780198837749.001.0001&partnerID=40&md5=4d9d9e162fad9f86ac0bd98b171ac892>

Zhang, E. (2021). A real-time deep transfer learning model for facial mask detection. *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, art. no. 9441582. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85107541487&doi=10.1109%2fICNS52807.2021.9441582&partnerID=40&md5=8883e5175b729781779349198739cf0f>

erpetuini, D., Filippini, C., Cardone, D., & Merla, A. (2021). An overview of thermal infrared imaging-based screenings during pandemic emergencies. *International Journal of Environmental Research and Public Health, 18*(6), art. no. 3286, pp. 1-12. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85102757345&doi=10.3390%2fijerph18063286&partnerID=40&md5=9df2021fcbc10e15df5298176258a69f>

Ullah, S., Partheeban, N., Sriramulu, S., Soni, R. K., Gupta, S., & Daniel, A. (2021). Identifying and Analyze the Face Mask Detection for the Person during Covid. *Proceedings - 2021 3rd International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*, pp. 2036-2040. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85127007654&doi=10.1109%2fICAC3N53548.2021.9725678&partnerID=40&md5=4c9557ae5e05899d6cecd169a08ca122>

Alwahab, S. A., Nassr, H. J., & Al-Khafaji, B. J. (2021). Designing a system for identifying persons using 3d images. *International Journal of Nonlinear Analysis and Applications*, 12(2), 2477-2481. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85118148665&doi=10.22075%2fijnaa.2021.5391&partnerID=40&md5=8efeaf813da90d0226181e35925c1443>

Kumar Shukla, R., Kumar Tripathi, P., Kumar, A., Prakash, V., & Kumar Singh, D. (2023). To Improve the Identification of Images Using LBPH in Machine Learning. *2023 1st International Conference on Intelligent Computing and Research Trends, ICRT 2023*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85163883454&doi=10.1109%2fICRT57042.2023.10146722&partnerID=40&md5=7a05d2ed0eec4fa5283a9d2fa9250099>

Sowmeya, V., & Karthik, R. Jaya (2022). Face recognition system for criminal identification using deep metric learning. *AIP Conference Proceedings, 2393*, art. no. 020066. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85131182821&doi=10.1063%2f5.0074484&partnerID=40&md5=bff0371fdcf093f86278920c00450db7>

Shanmuganathan, M., & Nalini, T. (2022). A Critical Scrutiny of ConvNets (CNNs) and Its Applications: Review. *SN Computer Science, 3*(6), art. no. 460. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85139486937&doi=10.1007%2fs42979-022-01359-8&partnerID=40&md5=ee94e1278c700e81a6b3360594c44b89>

Hassan, B., & Izquierdo, E. (2022). OneDetect: A Federated Learning Architecture for Global Soft Biometrics Prediction. *2022 International Conference on Intelligent Systems and Computer Vision, ISCV 2022*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85134290659&doi=10.1109%2fISCV54655.2022.9806101&partnerID=40&md5=5ac8f05ddd3d82b4d8a59c3e5387cb86>

Saini, K., Bharadwaj, S., & Gupta, V. (2022). Face Mask Detection: A Deep Learning Concept. *Proceedings of 3rd International Conference on Intelligent Engineering and Management, ICIEM 2022*, pp. 437 - 441. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85136969675&doi=10.1109%2fICIEM54221.2022.9853014&partnerID=40&md5=337589697c026ce74d061b0a86e7e4c4>

Sarkar, E., Benkraouda, H., Krishnan, G., Gamil, H., & Maniatakos, M. (2022). FaceHack: Attacking Facial Recognition Systems Using Malicious Facial Characteristics. *IEEE Transactions on Biometrics, Behavior, and Identity Science, 4*(3), pp. 361 - 372. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85135299723&doi=10.1109%2fTBIOM.2021.3132132&partnerID=40&md5=ae6622fe4660528a5899dd027a5e4b0e>

Duc, M. L., & Viet, Q. N. K. (2022). A PLS-SEM Neural Network for Understanding Computer Vision Technical. Apply to Gender Classification System. *Journal of Engineering Science and Technology Review, 15*(5), pp. 77 - 89. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85149817953&doi=10.25103%2fjestr.155.11&partnerID=40&md5=42b60e9f2b10ae39f97f7c35fa902613>

Trpin, A., & Boshkoska, B. M. (2022). Face recognition with a hyperbolic metric classification model. *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology, MIPRO 2022 - Proceedings*, pp. 317 - 320. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85133930303&doi=10.23919%2fMIPRO55190.2022.9803771&partnerID=40&md5=791f859245bd9f134cacb859eb643a1a>

Savanth, A. S., Manish, K. G. R., Narayan, P., Nikhil, M. L., & Gokul, V. G. (2022). Face Recognition System with 2D Anti-Spoofing. *Proceedings - 2022 IEEE World Conference on Applied Intelligence and Computing, AIC 2022*, pp. 226 - 230. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85137778582&doi=10.1109%2fAIC55036.2022.9848909&partnerID=40&md5=54130f0482820e8475b7fa1ec911209e>

Brintha, N. C., Narayana, J. A., Jaswanth, G. L. V. S., Chandrapal, G. J., & Venkat, D. (2022). Realtime Facial Emotion Detection Using Machine Learning. *Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2022*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141535799&doi=10.1109%2fICSES55317.2022.9914318&partnerID=40&md5=29667f26634ffe581b1c393e95af6d27>

Ghoualmi, L., & Benkechkache, M. E. A. (2022). Feature Selection Based on Machine Learning Algorithms: A Weighted Score Feature Importance Approach for Facial Authentication. *3rd International Informatics and Software Engineering Conference, IISEC 2022*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85146366916&doi=10.1109%2fIISEC56263.2022.9998240>

Chauhan, A., Khurana, L., Avinashwar, Singh, P., Diwakar, M., & Tripathi, A. (2022). Comparative Analysis of Face Mask Detection Models. *Lecture Notes in Electrical Engineering*, 915, 57-63. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85138766009&doi=10.1007%2f978-981-19-2828-4_6>

Srivastav, G., & Singh, R. (2022). Facial Recognition Based Workplace Security System Using LBPH Algorithm. *AIP Conference Proceedings*, 2555, art. no. 040008. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85141820202&doi=10.1063%2f5.0124629>

Juanatas, I. C., & Juanatas, R. A. (2023). Convolution Neural Network Approach for Facial Mask Detection. *GCCE 2023 - 2023 IEEE 12th Global Conference on Consumer Electronics*, pp. 1152-1155.<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85179761142&doi=10.1109%2fGCCE59613.2023.10315441>

de Lima, I. J. (2023). Safety, security and privacy in future airport terminals: a system theory perspective. *Transportation Research Procedia*, 72, pp. 2503-2509. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85182943050&doi=10.1016%2fj.trpro.2023.11.756>

Zolfi, A., Avidan, S., Elovici, Y., & Shabtai, A. (2023). Adversarial Mask: Real-World Universal Adversarial Attack on Face Recognition Models. *Lecture Notes in Computer Science (LNAI)*, 13715, pp. 304-320. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85151061277&doi=10.1007%2f978-3-031-26409-2_19>

Srinivasan, S. (2023). Understanding User Perception of Biometric Privacy in the Era of Generative AI. *4th International Conference on Communication, Computing and Industry 6.0*, C216 2023.<https://www.scopus.com/inward/record.uri?eid=2-s2.0-85186516536&doi=10.1109%2fC2I659362.2023.10430931>

Bagwan, S.M.R., Gupta, G., Thigale, S.B. (2023). Robust Multi-Bio-Metric Authentication Framework in Face and Iris recognition. *2023 2nd International Conference for Innovation in Technology, INOCON 2023*. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85158002758&doi=10.1109%2fINOCON57975.2023.10100996>

Gunturi, S.K., Alugubelly, M., Jayabalan, M., Aggarwal, S. (2023). Real-Time Masked Face Recognition in the Wild with few shots. *Proceedings - International Conference on Developments in eSystems Engineering, DeSE*, pp. 303 - 310. <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85189372390&doi=10.1109%2fDeSE60595.2023.10469038>

Josphineleela, R., Vekariya, V., Bharathidasan, B., Alfurhood, B. S., Kumar, V. P., & Tripathi, V. (2023). The most efficient and accurate face mask detection in crowded area using machine learning algorithm. *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, 937-942. <https://doi.org/10.1109/ICACITE57410.2023.10182832>

Priya, P., Gopinath, B., Mohamed Ashif, M., & Yadeshwaran, H. S. (2023). AI powered authentication for smart home security—A survey. *Lecture Notes in Networks and Systems, 719*, 227-237. <https://doi.org/10.1007/978-981-99-3758-5_21>

Kumar Shukla, R., Kumar Tripathi, P., Kumar, A., Prakash, V., & Kumar Singh, D. (2023). To improve the identification of images using LBPH in machine learning. *2023 1st International Conference on Intelligent Computing and Research Trends (ICRT 2023)*. <https://doi.org/10.1109/ICRT57042.2023.10146722>

Nidhi, & Verma, B. (2023). From methods to datasets: A detailed study on facial emotion recognition. *Applied Intelligence, 53*(24), 30219–30249. <https://doi.org/10.1007/s10489-023-05052-y>

Syed Musthafa, A., Dinesh, S., Dinesh Kumar, K., Jeeva, C., & Madesh, S. (2024). Digital vigilance: AI solutions in the quest for missing persons using face recognition with deep learning algorithms. *2nd International Conference on Artificial Intelligence and Machine Learning Applications: Healthcare and Internet of Things (AIMLA 2024)*. <https://doi.org/10.1109/AIMLA59606.2024.10531327>

Railkar, Y., Pawar, S., Pise, R., Nasikkar, A., & Patil, P. (2024). Criminal recognition system. *2024 International Conference on Emerging Smart Computing and Informatics (ESCI 2024)*. <https://doi.org/10.1109/ESCI59607.2024.10497321>

Fysh, M. C., Baker, E., Rockett, J., Allen, J., McCall, C., Burton, A. M., & Bindemann, M. (2024). Queues, crowds, and angry mobs: Face identification under distraction in a virtual airport. *Quarterly Journal of Experimental Psychology, 77*(6), 1169-1178. <https://doi.org/10.1177/17470218231203939>

Chougule, A., Kolte, S., Chamola, V., & Hussain, A. (2024). A novel generative adversarial network-based super-resolution approach for face recognition. *Expert Systems, 41*(8), e13564. <https://doi.org/10.1111/exsy.13564>

Çavşi Zaim, H., Yılmaz, M., & Yolaçan, E. N. (2024). Design of gender recognition system using quantum-based deep learning. *Neural Computing and Applications, 36*(4), 1997-2014. <https://doi.org/10.1007/s00521-023-09213-5>

Ouassam, E., Dabachine, Y., Hmina, N., & Bouikhalene, B. (2024). Improving the efficiency and security of passport control processes at airports by using the R-CNN object detection model. *Baghdad Science Journal, 21*(2), 524-536. https://doi.org/10.21123/bsj.2023.8546

Malla, J., Vemuri, H., Nagalli, S., Abhishek, S., & Anjali, T. (2024). The analysis of neural network models to distinguish AI generated faces from real faces. *Procedia Computer Science, 233*, 295-306. https://doi.org/10.1016/j.procs.2024.03.219

Kavitha, T., Hemalatha, S., Raja, B. S., Sripriya, R., & Yokeshwaran, D. (2024). Protective face mask recognition using deep learning techniques. *Proceedings of the 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS 2024)*, 375-381. https://doi.org/10.1109/ICC-ROBINS60238.2024.10533900

Anagnostopoulou, A., Tolikas, D., Spyrou, E., Akac, A., & Kappatos, V. (2024). The analysis and AI simulation of passenger flows in an airport terminal: A decision-making tool. *Sustainability (Switzerland)*, 16(3), 1346. https://doi.org/10.3390/su160301346