Sistema de control de acceso con reconocimiento facial para el mejoramiento de la seguridad y eficiencia de softwares implementados

Carlos Daniel Cardona Tamayo

Director

Ing. Javier Medina Cruz

Universidad Nacional Abierta y a Distancia -UNAD

Escuela de Ciencias Básicas Tecnología e Ingeniería -ECBTI

Tecnología en Desarrollo de Software

2025

Agradecimientos

A Dios, por su amor infinito y su favor constante desde el primer día de estudio hasta este momento, otorgándome la fortaleza necesaria para completar este proyecto de grado.

Al Ingeniero Javier Medina Cruz, por sus valiosas correcciones y orientación en el desarrollo de este proyecto, quien ha sido un pilar fundamental en este proceso.

Al Ingeniero Nevardo Alonso Ayala, por su apoyo y guía a lo largo de cada etapa de este proyecto.

A mis compañeros de curso, quienes han sido parte esencial de mi crecimiento académico y profesional durante todo el proceso educativo.

De manera especial, a mis padres, por su amor incondicional, su constante apoyo y ánimo, que han sido una fuente de motivación invaluable en este camino.

Resumen

El proyecto "Sistema de Control de Acceso con Reconocimiento Facial para el Mejoramiento de la Seguridad y Eficiencia de Software Implementados" tiene como objetivo desarrollar un sistema innovador que emplee el reconocimiento facial para optimizar la seguridad y eficiencia en entornos que requieran control de acceso. Este sistema combina tecnologías de programación de alto nivel, como React para el frontend y Python para el backend, junto con herramientas de código abierto como face_recognition y opencv-python, para implementar algoritmos avanzados de aprendizaje profundo. A través de una metodología estructurada que incluye la definición de requisitos, diseño del sistema, implementación y pruebas exhaustivas, se busca ofrecer una solución robusta, escalable y ética, que reduzca costos, incremente la precisión y mejore la experiencia del usuario en aplicaciones de control de acceso. El sistema logra administrar eficazmente los rostros asociados a un cliente, proporcionando un control de acceso confiable y adaptable a entornos que demanden altos estándares de seguridad.

Palabras clave: Control de acceso, reconocimiento facial, softwares implementados.

Abstract

The project "Access Control System with Facial Recognition for Improving Security and Efficiency of Implemented Software" aims to develop an innovative system that uses facial recognition to optimize security and efficiency in environments requiring access control. This system combines high-level programming technologies, such as React for the frontend and Python for the backend, along with open-source tools like face_recognition and opencv-python, to implement advanced deep learning algorithms. Through a structured methodology that includes requirement definition, system design, implementation, and thorough testing, the goal is to provide a robust, scalable, and ethical solution that reduces costs, increases accuracy, and improves user experience in access control applications. The system effectively manages the faces associated with a client, providing reliable access control that can be adapted to environments demanding high security standards.

Keywords: Access control, facial recognition, implemented software

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Introducción

El control de acceso es un elemento clave en la gestión de seguridad de diversas organizaciones, desde empresas hasta instituciones públicas. La tecnología de reconocimiento facial ha surgido como una solución innovadora para la identificación y verificación de personas, utilizando características biométricas únicas. Sin embargo, su implementación plantea desafíos técnicos, como la privacidad de los usuarios, la equidad en los algoritmos y la precisión en condiciones variadas.

Este proyecto aborda estos desafíos desarrollando un sistema de control de acceso con reconocimiento facial que combina React y Python. A través de herramientas de código abierto y algoritmos avanzados, el sistema está diseñado para operar en entornos diversos, con un enfoque en la seguridad, escalabilidad y eficiencia, el sistema se propone como una solución integral para mejorar la gestión de acceso en múltiples contextos.

Justificación

Las técnicas desarrolladas para reconocimiento facial se pueden clasificar en dos grupos: basadas en la apariencia, basadas en modelos, cada una de ellas cuenta con sus propios desafíos técnicos en donde el criterio para su uso depende del contexto donde van a ser aplicadas. De esta manera el control de acceso aporta una relevancia en el ámbito del reconocimiento facial utilizando herramientas de programación de alto nivel donde a su vez presenta una serie de desafíos técnicos y de diseño que deben abordarse cuidadosamente para garantizar la seguridad, eficiencia y usabilidad del sistema. De acuerdo con lo anterior, se toma como referencia a Acuña (2019) la visión por computador en conjunto con el campo del aprendizaje profundo de crecimiento rápido aumenta el desafío de lograr soluciones sostenibles y no tan costosas para diseñar un sistema que permita atacar el problema de un control adecuado de acceso del personal. Con base a esto se tienen en cuenta una serie de características las cuales fomentan posibles soluciones en el ámbito expuesto anteriormente, algunas de las características más esenciales del control de acceso son: la protección de activos permite un control exacto del personal sin necesidad de presencia de supervisores para el registro de los ingresos y salida de los empleados, reemplazo de guardas y personal de seguridad.

Por otra parte, en el área tecnológica del reconocimiento facial se entiende como "un mecanismo de identificación o verificación de identidad de un individuo que utiliza su rostro o rasgos faciales" (p. 5) a su vez, se ignora o subestima el hecho de que el empleo de sistemas digitales para el rastreo, registro o identificación de individuos en situaciones de riesgo o vulnerabilidad representa graves amenazas a su privacidad y seguridad, por ejemplo, En el año 2016, Martínez, Neal y otros individuos presentaron una demanda legal contra SNAPCHAT, INC., alegando que la compañía recolectaba información personal de sus usuarios mediante la

función de filtros con tecnología de reconocimiento facial (TRF) sin su previo consentimiento, como lo exige la Ley de Privacidad de la Información Biométrica de Illinois (BIPA). Sin embargo, este caso no llegó a ser juzgado en un tribunal.

Cualquiera sea el caso, este estudio se justifica sobre varios puntos, pues el propósito es contribuir al desarrollo de un software que permita crear el control de acceso diversas organizaciones, realizando un reconocimiento facial y generando que la información sea transmitida y adquirida con el fin de generar un análisis de los datos obtenidos por las herramientas del software a implementar.

Objetivos

Objetivo General

Desarrollar un sistema de control de acceso basado en reconocimiento facial utilizando React para la interfaz de usuario y Python para el backend, que permita una autenticación segura y eficiente en entornos basados en seguridad física donde se requiera control de acceso.

Objetivos Específicos

Investigar y seleccionar los algoritmos y técnicas más adecuadas para el reconocimiento facial en tiempo real.

Implementar un módulo de reconocimiento facial que compare los rostros detectados mediante cámara web, con las imágenes almacenadas en la base de datos.

Desarrollar un backend robusto en Python que gestione la lógica de negocio, la autenticación de usuarios y la gestión de datos.

Diseñar e implementar una interfaz de usuario intuitiva y receptiva utilizando el marco de trabajo React.

Planteamiento Problema

Es importante comprender que los sistemas de control de acceso en un contexto variado, como compañías, centros educativos y entidades públicas actualmente carecen de sesgos raciales y de género en el reconocimiento facial, es decir que están entrenados con datos que carecen de diversidad, según Perez & Madrid (2021) “Los sistemas de aprendizaje profundo se basan en la extracción de patrones. Identifican combinaciones, incluso muy sutiles, entre los datos empleados. El uso de modelos opacos puede causar un problema de discriminación oculto, y también un problema de perpetuación de esa discriminación”. Esto refleja que, la causa, podría originarse en la falta de diversidad en los datos de entrenamiento, generando resultados discriminatorios que afectan negativamente a ciertos grupos poblacionales. Por consiguiente, en contexto a nivel internacional Raji y Fried (como se citó en Perez & Madrid 2021) artículo titulado como “una encuesta sobre la evaluación del reconocimiento facial” encontró que,

“Debido a la enorme demanda de datos del Aprendizaje Profundo, se han obtenido las imágenes frecuentemente sin conocimiento ni consentimiento de los interesados. Esto ha dado lugar a conjuntos de datos llenos de problemas: fotos de menores, etiquetas racistas y sexistas e iluminación y calidad no uniforme”. (p.2).

Se puede decir que, es importante implementar regulaciones, adoptar prácticas éticas y evaluar los sesgos son medidas necesarias para garantizar un desarrollo responsable y equitativo de esta tecnología. Así mismo, tomando como referencias los contextos nacionales e internacionales las problemáticas relacionadas con el tratamiento de datos personales y el mal manejo por las entidades, puede causar un riesgo para los usuarios teniendo en cuenta que, la fiabilidad del reconocimiento facial no es absoluta y el uso del reconocimiento facial plantea preocupaciones éticas relacionadas con la privacidad, la vigilancia y el sesgo algorítmico por eso

es importante diseñar el sistema de manera que respete la privacidad de los usuarios, minimice la vigilancia excesiva y mitigue el potencial de sesgo en los algoritmos de reconocimiento facial. Según un proyecto implementado por Transmilenio (transporte público de la ciudad de Bogotá) Barrera (2023) “Este software permite hacer el reconocimiento facial y tomar las fotografías, que luego se cotejan con la base de datos de la institución. Después se genera una alerta verde o roja a los uniformados para que realicen la captura en el lugar” (p.1) Ahora bien es importante resaltar, el concepto de protección de datos y sus marcos regulatorios, CEPAL (2024) “se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes” (p.1) En ese sentido, el buen uso de los datos personales facilita a las empresas de seguridad una automatización del tiempo, disminuyendo los delitos como el robo, reducción de costos entre otros.

A nivel internacional, el reglamento General de Protección de Datos, constituye una base importante de la protección de datos en la Unión Europea. Este marco legal establece las normas que rigen el tratamiento de datos personales y su libre circulación, con el objetivo primordial de salvaguardar los derechos y libertades fundamentales de las personas, especialmente el derecho a la protección de sus datos personales. Según Moreano J.A.C (2017) “el reconocimiento facial es una herramienta muy importante en el medio en tanto permite identificar a través de ciertas características a un individuo, aunque

a veces resulta beneficioso el reconocimiento facial, no se debe olvidar que el mal uso del reconocimiento facial afecta de gran manera al desarrollo del individuo”. (p.2) Por lo tanto, la tecnología de reconocimiento facial ha experimentado avances considerables, no se puede considerar infalible. Los sistemas basados en la tecnología de reconocimiento facial generan resultados expresados en similitudes, entre las dos imágenes faciales comparadas. El análisis de

estos resultados puede ser complejo, ya que dependen de los procesos de cálculo específicos de cada sistema y algoritmo. De acuerdo con lo anterior, la tecnología de reconocimiento facial, a pesar de sus avances, no está exenta de limitaciones. Su eficacia se ve afectada por diversos factores externos, como la iluminación, la postura del sujeto o su edad. Estos factores pueden generar resultados erróneos, conocidos como falsos negativos y falsos positivos, que pueden tener consecuencias significativas en diversos ámbitos, como la seguridad y la privacidad.

Es importante tener en cuenta estas limitaciones al evaluar la implementación de sistemas de reconocimiento facial y considerar medidas para mitigar su impacto, como la implementación de protocolos de control de calidad y la capacitación del personal involucrado en su uso. Un ejemplo es un artículo publicado por La Corporación de Radio y Televisión Española (RTVE, 2023) donde se expone el caso de la empresa de inteligencia artificial Clearview detrás de una de las herramientas de reconocimiento facial más empleada en Estados Unidos y que permite identificar a alguien, casi instantáneamente, a partir de una foto, si bien existen diversos métodos para enfrentar este problema, como el procesamiento de imágenes para filtrar cuidadosamente rostros de un conjunto amplio de imágenes en diferentes entornos, o las soluciones empresariales de alto rendimiento disponibles, la accesibilidad a estas opciones se ve limitada por su elevado costo. En algunos casos, se requieren grandes cantidades de datos para validar los rostros de numerosos usuarios. Es a partir de este panorama que este trabajo de grado se pregunta

¿Qué desafíos técnicos y de diseño deben abordarse al desarrollar un sistema de control de acceso basado en reconocimiento facial utilizando herramientas de programación de alto nivel?

Marco Teórico

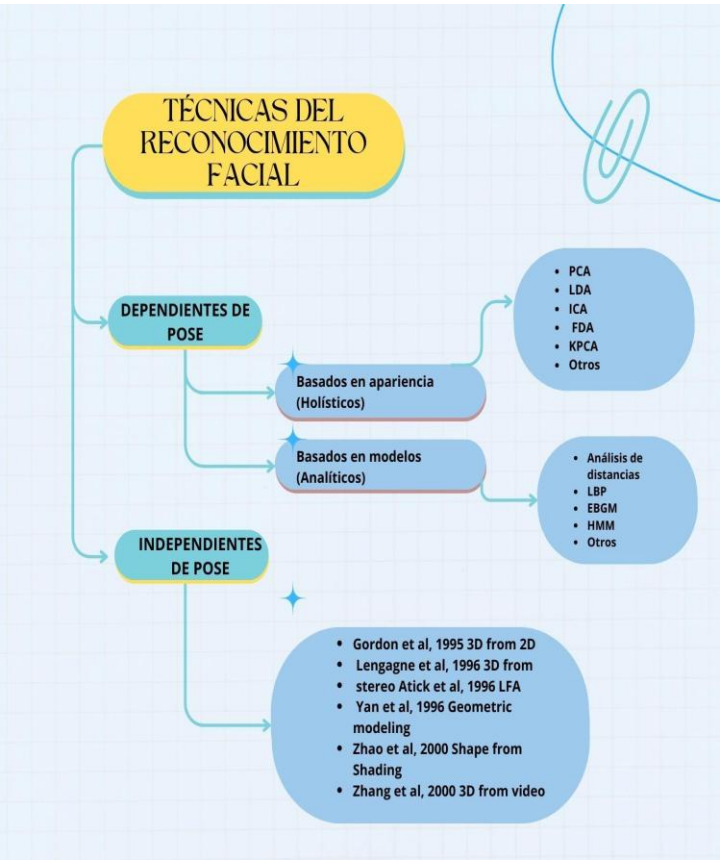
En este apartado se exponen los aspectos teóricos que se desarrollan en esta investigación, en primer lugar, se relaciona el concepto de técnicas para el reconocimiento facial, luego control de acceso y su tipología, herramientas de reconocimiento facial.

Técnicas para el Reconocimiento Facial

Es importante resaltar que el concepto de reconocimiento facial se define como la capacidad de todos los individuos de reconocer formas básicas de expresión afectiva, la cual se muestra en los rostros de las personas y se constituyen por 6 emociones básicas (Russell, 1994; Saracco, 2012), estas emociones básicas incluyen miedo, enojo, sorpresa, alegría, tristeza y asco. Ahora bien, en el ámbito tecnológico el reconocimiento facial supera las capacidades de las tecnologías de identificación presentes en celulares y computadoras, las cuales se basan en el reconocimiento de personas en fotos. Su aplicación para la identificación y validación de personas tiene el potencial de agilizar el control de acceso a edificios corporativos y gubernamentales. Otro concepto relacionado al ámbito tecnológico del reconocimiento facial, Salazar & Orozco (2016) proponen que “El reconocimiento facial es un sistema para la identificación de personas por medio de imágenes, las cuales pueden ser tomadas anteriormente o adquiridas en un sistema de tiempo real”. lo anterior permite comprender que, el éxito del reconocimiento facial depende de la comprensión de diversos factores, ya que las variables externas pueden afectar significativamente el procesamiento de la imagen. Además, la elección de la técnica de reconocimiento adecuada es crucial para optimizar el rendimiento del sistema. Teniendo en cuenta lo anterior, se expondrán las técnicas del reconocimiento facial y su conceptualización.

Figura 1

Técnicas del reconocimiento facial



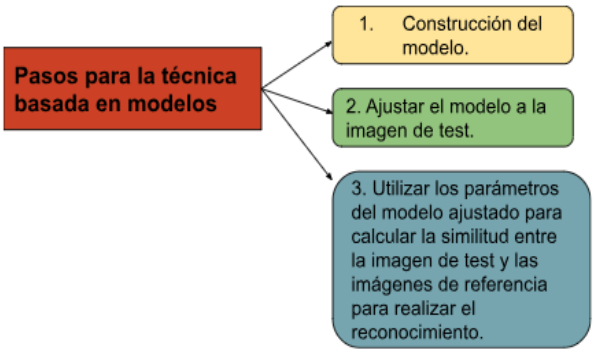
Nota. La figura muestra las técnicas de reconocimiento facial. *Fuente.* Elaboración propia (2024)

Tabla 1

Las Técnicas del Reconocimiento Facial y su Conceptualización

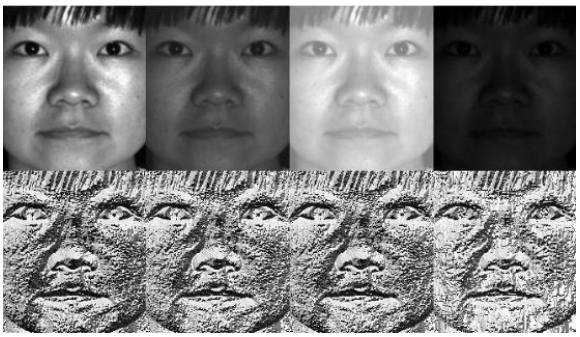
Técnicas de Reconocimiento Facial	Características
Técnicas Basadas en la Apariencia (Holísticos)	Aplican diferentes técnicas estadísticas sobre la textura de la imagen para obtener información significativa Las técnicas basadas en la apariencia se dividen en: **PCA (Principal Component Analysis)** Es una técnica que permite transformar un conjunto de datos de alta dimensión en un subespacio de menor dimensión, conservando la mayor cantidad de información posible. En el contexto del reconocimiento facial, esto significa que se puede representar cada rostro como un vector con menos dimensiones, sin perder información importante para su identificación.  Nota. La figura muestra la técnica PCA (Principal Component Analysis) . Fuente: Dominguez y Martin (2017). **Linear Discriminant Analysis** Derivado del PCA, es una técnica que combina

	PCA con Análisis Discriminante Lineal (LDA) para el reconocimiento facial. Esta técnica logra mayor robustez frente a cambios de iluminación, pero tiene un costo computacional más elevado.  Nota. La figura muestra la tecnica Linear Discriminant Analysis. Fuente: Dominguez y Martin (2017). **Frecuency Domain Analysis** No dependen de datos de entrenamiento y cuentan con algoritmos eficientes para una implementación sencilla y de bajo costo computacional.
Técnicas Basadas en Modelos (Analíticos)	Estos métodos se enfocan en la creación de un modelo facial preciso y sensible a las variaciones en los rostros humanos, permitiendo una detección precisa de las expresiones y características faciales. Es decir que, obtienen información tanto de la forma como de la textura del rostro para identificar patrones únicos En estos sistemas, el algoritmo está familiarizado con el objeto de que debe representar, en este caso, una cara humana. Su objetivo es alinear la imagen facial real con un modelo predefinido. Para lograrlo, se emplea un proceso de tres pasos.



Nota. La figura muestra los pasos para la técnica basada en modelos. Fuente: Elaboración propia (2024).

LBP: El descriptor Local Binary Pattern (LBP) es ampliamente reconocido por su capacidad para describir texturas a nivel local con gran precisión. Su uso se ha extendido a diversas aplicaciones en el ámbito del procesamiento de imágenes y el reconocimiento de patrones.

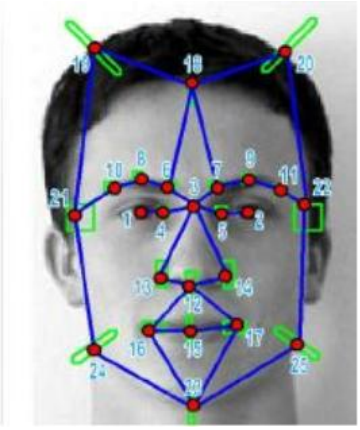


Nota. La figura texturas a nivel local con gran precisión. Fuente: Dominguez y Martin (2017).

EBGM Elastic Bunch Graph Matching

El reconocimiento facial basado en puntos de interés surge como una técnica innovadora que se aleja del enfoque tradicional de analizar la cara en su totalidad. Esta técnica se centra en identificar y

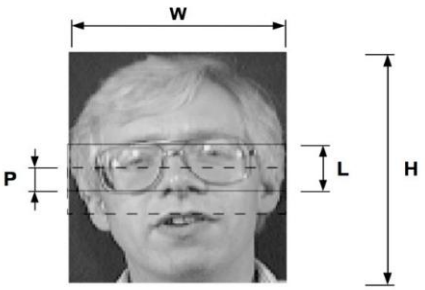
utilizar puntos clave en el rostro, explotando la similitud topológica que estos comparten entre diferentes individuos.



Nota. La figura muestra la técnica facial basado en puntos de interés. Fuente: Dominguez y Martin (2017).

Hidden Markov Models (HMMs)

Los Modelos Ocultos de Markov (HMMs) han demostrado ser una herramienta eficaz para el reconocimiento facial, ofreciendo robustez frente a variaciones de iluminación, expresión y orientación facial. Esta característica los convierte en una alternativa atractiva a los métodos holísticos tradicionales.



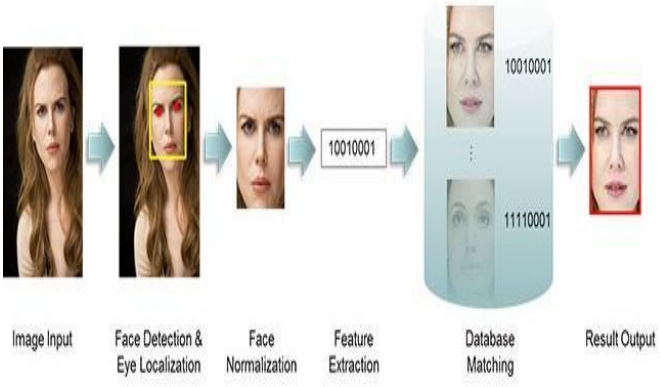
Nota. La figura muestra Los Modelos Ocultos de Markov (HMMs). Fuente: Dominguez y Martin (2017).

Nota. La tabla muestra las técnicas del reconocimiento facial y su conceptualización. Fuente: Elaboración propia (2024).

Así mismo, los autores del libro "*Modern Deep Learning and Advanced Computer Vision*" de Thomas Binford, Jagadeesh Kumar, J, Ruby, J. Lepika, J. Tisa y J. Nedumaan describen las cuatro fases o los cuatro módulos que integran una solución de reconocimiento facial y que se esquematizan en la siguiente figura:

Figura 2

Cuatro módulos que integran una solución de reconocimiento facial



Nota. La figura muestra los cuatro módulos que integran una solución de reconocimiento facial.

Fuente. Gavilán, J (2021).

Las distintas etapas del proceso emplean algoritmos especializados basados en técnicas de aprendizaje profundo como las redes neuronales convolucionales. Estos algoritmos pueden implementarse en módulos o incluso en soluciones independientes.

Control de Acceso y su Tipología

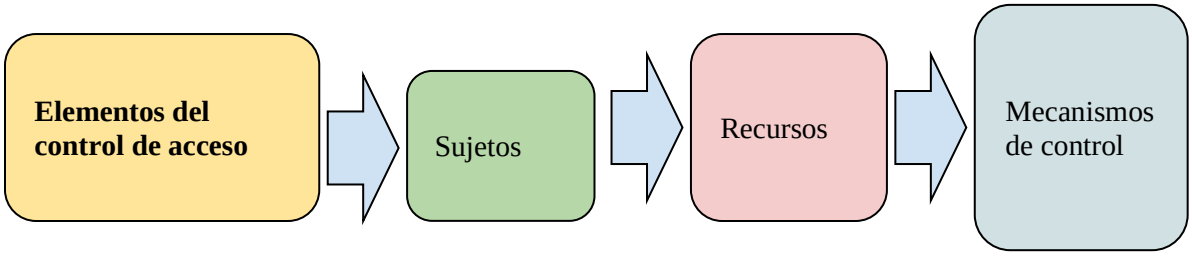
Revisando el concepto de control de acceso y su literatura Pacheco, J & Chavez, J (2023) Proponen que “se refiere a un conjunto de medidas que tienen como objetivo proteger determinados recursos de usuarios no autorizados”. (p. 2). Estos recursos pueden ser físicos, como instalaciones, dispositivos o información digital. El objetivo del control de acceso es proteger estos recursos de accesos no autorizados, ya sea para prevenir daños, robos o simplemente para mantener la privacidad y confidencialidad.

Otro concepto revisado es el de, Morales et al. (2022) “representa una gran herramienta en cuestiones de seguridad, puesto que se reforzarán los procesos manuales de control de acceso, limitando la entrada a personas ajenas” (p.5) Por lo anterior, el control de acceso constituye una de las alternativas más considerables ya que garantiza la seguridad y previene el acceso de personas no autorizadas a ciertos recursos y lugares.

A continuación, se exponen en la figura los elementos que identifican el control de acceso.

Figura 3

Elementos del control de acceso



Nota. La figura muestra los elementos del control de acceso. *Fuente.* Elaboración propia (2024).

Además, es importante describir los elementos del control de acceso demostrados en la figura anterior:

Sujetos: Pueden ser personas, dispositivos, programas o cualquier otra entidad capaz de solicitar acceso.

Recursos: Los objetos o información a los que se intenta acceder, pueden ser archivos, bases de datos, dispositivos, instalaciones físicas o cualquier otro recurso que se necesite proteger.

Mecanismos de control: Los medios por los cuales se verifica y se permite o deniega el acceso. Estos mecanismos pueden incluir contraseñas, tokens de seguridad, biometría, controles físicos o cualquier otra forma de verificar la identidad y autorización del sujeto.

Así mismo, Montoya, J & Restrepo, Z (2013) describen desde una perspectiva organizacional al control de acceso como “La gestión de identidades y control de acceso, IAM por sus siglas en inglés, es una solución que permite realizar la gestión del ciclo de vida de las identidades y controlar el acceso a los diferentes recursos, con el objetivo de

mitigar riesgos, reducir costos y permitir que el negocio evolucione de manera segura y flexible" (p.23). De acuerdo con lo anterior, se resalta un elemento como lo son los mecanismos de control, estos en los ambientes laborales permiten detectar y reconocer el rostro buscando siempre disminuir costos y optimizar recursos para que el producto llegue a los usuarios de pequeñas, medianas y grandes empresas (Pérez León & Rojas Arévalo, 2019).

Tipos de Control de Acceso

Existen diferentes tipos de control de acceso, cada uno con sus propias características y aplicaciones:

Para facilitar la visualización de las técnicas más prevalentes en los estudios analizados, se elaboró una representación gráfica que clasifica las técnicas empleadas en cada publicación. De esta manera, se permite identificar de forma clara y concisa las técnicas que han recibido mayor atención por parte de los investigadores en este campo.

Tabla 2

Tipología y técnicas de control de acceso

Técnicas de Control de Acceso	Características
Técnica de Control de Acceso Basada en Roles (RBAC)	Esta técnica se basa en establecer roles a los que se les asignan los permisos de acceso; una vez creados, a los usuarios se le asignan los roles correspondientes a la organización, para que de esta manera puedan acceder a la información adecuada (Ghazal et al., 2020)
Técnica de Control de Acceso Re Cifrado Proxy	Mediante el proxy se busca en esta técnica establecer políticas de control de acceso detalladas y que permitan decisiones de revocación de consentimiento, tal y como lo usaron en su modelo los autores (Thein & Vasupongayya, 2019).
Técnica de Atributos de Control de Acceso Basado en Políticas (CP-ABE)	Esta técnica consiste en asignar a cada usuario un conjunto de atributos en términos de claves secretas, las cuales se asignan según su cargo y el nivel de acceso que deben tener de acuerdo con las políticas establecidas por las autoridades de atributos de la organización, permitiendo el descifrado solo a

	aquellos que posean el conjunto de atributos que coincida con dicha política (Gupta et al., 2023).
Técnica de Control de Acceso Basada en Ontologías (ODAC)	Esta técnica propuesta por (Kiran & Nalini, 2020) se centra en el control de acceso a los datos de unidad de almacenamiento en la nube, manteniendo una política de permisos para los usuarios, y a su vez ayudándose de la técnica de reconocimiento seguro (SAT) para el autenticado del acceso a dichos datos.
Técnica Enigmático Estándar de Cifrada Diagonal (EDES)	Este modelo propuesto busca encriptar la información almacenada en la nube eficazmente, haciendo uso de estándares de encriptación diagonal basado en un generador de claves, buscando de esta manera que la información de la nube no sea un punto vulnerable para la información de una organización.
Técnica Blockchain Habilitada para Control de Acceso (ACE-BC)	Esta técnica se centra en el cifrado basado en atributos del usuario, en la cual el mecanismo de control de acceso es el encargado de limitar el acceso de usuarios no autorizados, de manera similar a la técnica CP-ABE. La diferencia radica en que la técnica de cifrado en este caso

	es blockchain,) mejora el índice de confidencialidad considerablemente.
Marco de Control de Accesos PICO	PICO es el nombre de un marco que utiliza IoT para el control de acceso, el cual preserva la privacidad en escenarios IoT haciendo uso de información incompleta. Este marco permite a los dispositivos evaluar los riesgos de privacidad asociados con las políticas de divulgación, y así determinar hasta qué punto se puede divulgar.

Nota. Información tomada del artículo titulado: Control de accesos en seguridad de la información: Una revisión sistemática de las técnicas actuales (2023).

Por tal motivo, la protección de los datos mediante el control de acceso constituye una tarea crucial para las organizaciones que priorizan la seguridad de su información confidencial.

Por esta razón, las técnicas mencionadas anteriormente ofrecen beneficios y aplicaciones prácticas en sus respectivos enfoques, es importante destacar que son propuestas relativamente nuevas en el ámbito del control de accesos. Debido a su reciente desarrollo, aún no han logrado una amplia adopción por parte de las organizaciones, a pesar de su potencial para superar las limitaciones de las técnicas tradicionales. No obstante, su relevancia en el panorama de la seguridad informática es innegable, y se espera que su uso y reconocimiento continúen creciendo a medida que maduren y se consoliden en este campo.

Herramientas de Reconocimiento Facial

Las herramientas de reconocimiento facial se utilizan en una amplia variedad de aplicaciones, como la seguridad, el control de acceso, la vigilancia y la autenticación. También se están explorando nuevas aplicaciones en áreas como la atención al cliente, el marketing y la educación. Según Zapatero, D (2016) "propone desarrollar un sistema de reconocimiento facial, por medio del uso de técnicas de aprendizaje profundo, a partir de la obtención de fotografías tomadas de la red social Instagram, usando Web Scraping, contando con la aprobación del dueño para dicha extracción". (p.337) Por lo tanto, las herramientas de reconocimiento facial son una tecnología poderosa con una amplia gama de aplicaciones potenciales. Esta tecnología ha experimentado un rápido desarrollo en los últimos años, gracias a los avances en inteligencia artificial y aprendizaje automático.

Además, la evolución tecnológica trae consigo nuevos retos para la detección de rostros, como la velocidad de reconocimiento, la iluminación variable, el desenfoque, el ruido, los cambios en los rasgos faciales y el uso de accesorios. (Chihaoui, 2016). A continuación, se describirán el funcionamiento de las herramientas de reconocimiento facial y sus respectivas características.

Funcionamiento de las Herramientas de Reconocimiento Facial

El proceso de reconocimiento facial se puede dividir en los siguientes pasos:

Detección de Rostros. El primer paso es detectar la presencia de rostros en una imagen o vídeo. Esto se puede hacer utilizando algoritmos de visión por computadora que buscan características faciales como los ojos, la nariz y la boca. Ahora bien, un ejemplo de la detección de rostros es el algoritmo de detección de rostros implementado en libreria dlib, según García del Prado, N et alt (2017) “Este detector está basado en un clasificador que utiliza características basadas en una variante de histogramas de gradientes orientados (HOG) extraídas de ventanas deslizantes de tamaño fijo operando sobre pirámides de imágenes”. (p. 978).

Figura 4

Detector de ojos

Nota. La figura muestra detector de ojos. Fuente: Domínguez y Martin (2017).

Extracción de Características. Una vez que se detecta un rostro, se extraen características únicas del mismo. Estas características pueden incluir la forma de la nariz, los ojos, la boca y la mandíbula, así como la distancia entre diferentes puntos faciales. De acuerdo con, Ibarra, J & Paredes, K (2018) “Estos métodos están orientados a la construcción de modelos del rostro humano a partir de características geométricas (características invariantes) que

permitan establecer diferencias faciales entre un rostro y otro". (p.286). Por lo cual, al detectar estas características, cada una se analiza como un patrón individual (con sus propias propiedades únicas).

Figura 5

Extracción de características

Nota. La figura muestra extracción de características. *Fuente.* Dominguez y Martin (2017).

Normalización de Características. Las características extraídas se normalizan para que sean comparables entre sí, independientemente de la iluminación, la posición o la expresión facial. Para Carrero, D et alt (2010) "el objetivo de los métodos de normalización y de extracción de características consiste en localizar de forma precisa las regiones faciales. Estos métodos se pueden agrupar en dos familias" (p.2).

Figura 6

Normalización de características

Nota. Información tomada del artículo titulado: Prestaciones de la Normalización del Rostro en el Reconocimiento Facial (2010). *Fuente.* Elaboración propia.

Decisión. La herramienta de reconocimiento facial toma una decisión sobre la identidad de la persona en función de la similitud entre la representación del rostro y las entradas de la base de datos. Según Domínguez, S (2017) “Finalizada la extracción de características se llega a la última fase, cuyo objetivo es determinar qué imagen del conjunto de entrenamiento es más parecida a la imagen de test, a partir de sus representaciones mediante las eigenfaces (sus proyecciones)”. (p.32). Es decir que, el reconocimiento facial, se busca la proyección de las imágenes de entrenamiento que tenga la mayor similitud con la proyección de la imagen capturada por la cámara.

Tipos de Herramientas de Reconocimiento Facial

Existen dos tipos principales de herramientas de reconocimiento facial:

Basadas en el Análisis de Características. Estas herramientas analizan las características faciales de una imagen o vídeo para crear una representación matemática del rostro. Esta representación se puede comparar con una base de datos de rostros conocidos para identificar a la persona.

Basadas en Deep Learning. Estas herramientas utilizan redes neuronales artificiales para aprender a reconocer rostros. Las redes neuronales se entrenan con una gran cantidad de imágenes de rostros etiquetados para aprender a identificar las características faciales que son distintivas de cada persona. De acuerdo con Muñiz, A (2018) “Este enfoque propone modelar abstracciones de alto nivel de los datos empleando para ello arquitecturas compuestas por un elevado número de capas de transformaciones que pueden ser tanto lineales como no lineales. Se trata de una idea inspirada en la arquitectura y funcionamiento del cerebro humano y, por ello, estas técnicas reciben también el nombre de redes neuronales artificiales (RNAs)”. (p.8). Esto quiere decir que, las técnicas de Deep Learning han revolucionado el campo de la inteligencia artificial al introducir la posibilidad de entrenar arquitecturas neuronales profundas, es decir, modelos complejos con un gran número de capas. Esta capacidad representa un avance significativo en comparación con las técnicas clásicas de aprendizaje automático.

Metodología

Técnicas de Recolección de Información

La metodología que se plantea para esta investigación es de carácter cuantitativo con diseño o herramienta experimental, según Hernández Sampieri, se caracteriza por los siguientes elementos:

Técnica

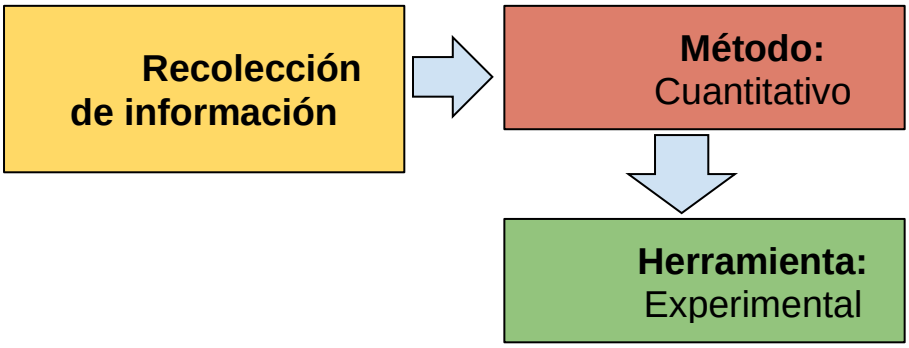
Cuantitativo. El método cuantitativo de investigación es un enfoque sistemático para recopilar, analizar e interpretar datos numéricos a fin de comprender y explicar fenómenos del mundo real. Se basa en la medición y el uso de técnicas estadísticas para establecer relaciones entre variables y extraer conclusiones generalizables.

Herramienta

Experimental. La herramienta experimental es un elemento fundamental en la investigación, particularmente en el método cuantitativo con enfoque experimental. Se refiere a los instrumentos, recursos y procedimientos que se utilizan para manipular variables y recolectar datos.

Figura 7

Elementos de recolección de información del proyecto



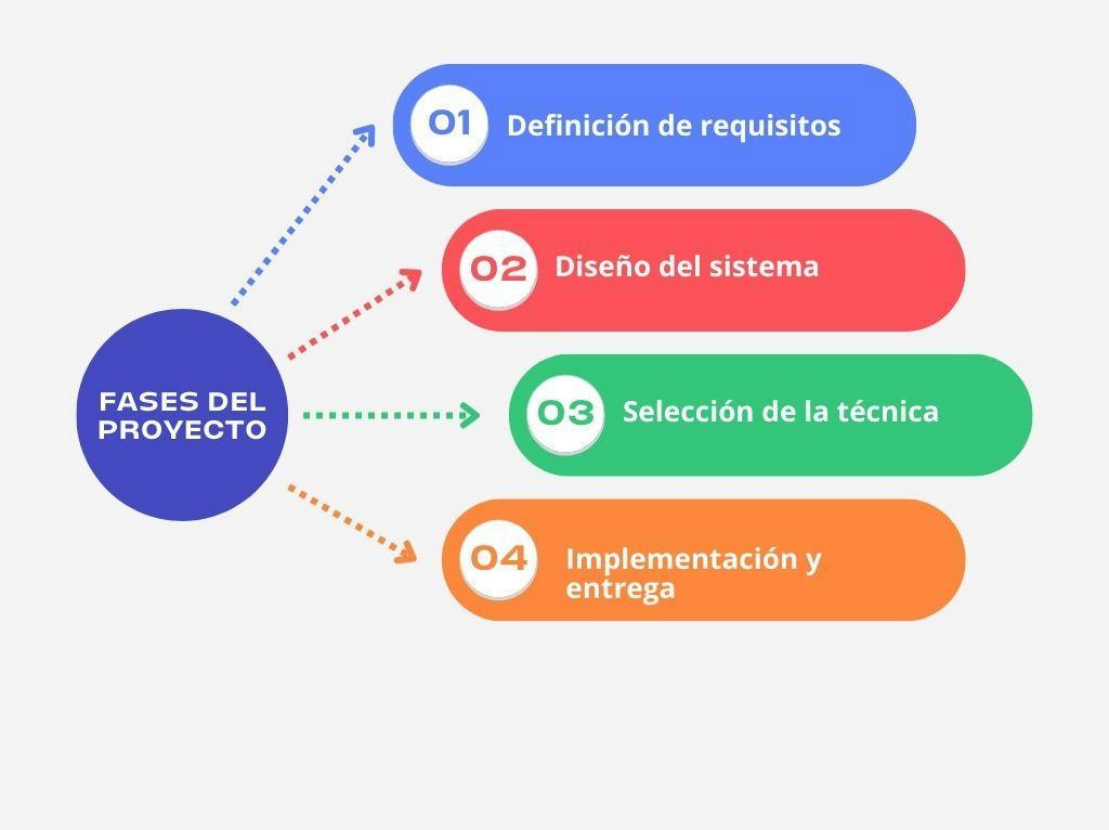
Nota. La figura muestra los elementos de recolección de información del proyecto. *Fuente*. Elaboración propia (2024).

Fases del Proyecto

El desarrollo del proyecto se divide en cuatro fases, cada una con actividades específicas que se ejecutan en orden cronológico, tal como se muestra en la figura, para alcanzar los objetivos establecidos.

Figura 8

Fases del proyecto



Nota. La figura muestra las fases del proyecto. *Fuente*. Elaboración propia (2024).

Fase 1: Definición de Requisitos

En esta fase se identifican y documentan los requisitos funcionales y no funcionales del sistema de reconocimiento facial. Se realizan entrevistas con los usuarios finales para determinar sus necesidades específicas, como el número de usuarios a registrar, las condiciones de iluminación en las que se utilizará el sistema, la precisión requerida en la identificación y el tiempo máximo de respuesta.

El usuario es un actor clave en esta fase, definiendo las características que el sistema debe tener.

La participación de los usuarios es fundamental para el éxito del sistema de reconocimiento facial. Por esta razón, se ha identificado y clasificado a los principales grupos de usuarios que interactuarán con el sistema.

Además, se incluyen tres actividades importantes que permiten la evidencia al desarrollo de esta fase.

Actividad 1

Establecer los criterios para el acceso al sistema, teniendo en cuenta lo siguientes aspectos:

Usuarios del Sistema

Tabla 3

Usuarios del sistema

Tipo de Usuario	Rol en el Sistema	Necesidades Específicas
Administrador	Configura el sistema, gestiona usuarios, define parámetros de reconocimiento.	Alta seguridad, flexibilidad en la configuración, informes detallados.
Clientes	Utiliza el sistema para tareas diarias como control de acceso, verificación de identidad. Beneficiario directo del sistema, como empleado, cliente o visitante.	Interfaz intuitiva, rapidez en la identificación, alertas personalizables.
Usuario	Utiliza el sistema para tareas diarias como control de acceso, verificación de identidad.	Seguridad, privacidad, facilidad de uso.

Nota. La tabla muestra los usuarios del sistema. *Fuente.* Elaboración propia (2024).

Requerimientos Funcionales

Los requerimientos funcionales, plasmados en la tabla, establecen las bases para el desarrollo del sistema, definiendo su comportamiento y alcance.

Tabla 4

Requerimientos funcionales

N°	Requerimiento Funcional	Rol del Usuario	Descripción
1	Iniciar sesión	Administrador	El administrador debe poder iniciar sesión en el sistema.
2	Registrar usuario	Administrador	El administrador debe poder registrar nuevos usuarios (administradores).
3	Registrar un cliente	Cliente	El cliente debe poder registrar nuevos clientes.
4	Capturar la imagen a través de una cámara web	Rostros	El software debe poder capturar su imagen utilizando la cámara web del dispositivo.
5	Guardar la información en la base de datos	Administrador	El sistema debe guardar la información de los usuarios y sus imágenes en una base de datos.
6	Guardar la imagen capturada de los usuarios en una carpeta	Rostros	El sistema debe guardar las imágenes capturadas de los usuarios en una carpeta específica.
7	Realizar el reconocimiento facial	Administrador	El sistema debe poder realizar el reconocimiento facial de los estudiantes.
9	El reconocimiento facial permitirá reconocer en tiempo real al usuario.	Usuarios/ clientes	El usuario/ cliente debe ser reconocido en tiempo real por el sistema.
10	Verificar si el usuario es correcto.	Administrador	El administrador debe poder verificar si el usuario

			identificado por el sistema es el correcto.
11	Listar Usuarios	Administrador	El administrador debe poder visualizar una lista de todos los usuarios registrados en el sistema.
13	Listar clientes	Usuario	El usuario debe poder visualizar una lista de todos los clientes registrados en el sistema.

Nota. La tabla muestra requerimientos funcionales. Fuente: Elaboración propia (2024).

Especificaciones de los Requerimientos

La tabla presenta un listado detallado de los requisitos funcionales que el sistema debe cumplir para satisfacer las necesidades y expectativas de los usuarios y clientes. Este documento es esencial para garantizar que el desarrollo del sistema se alinea con los objetivos del proyecto.

Tabla 5

Especificaciones de los requerimientos

Id Req.	Requerimiento	Descripción Detallada	Prioridad	Estimación (horas)
01	Iniciar sesión	El sistema debe permitir a un administrador iniciar sesión utilizando sus credenciales.	Alta	16
02	Registrar usuario	El sistema debe permitir a un administrador crear nuevos usuarios con diferentes roles y permisos.	Alta	16
03	Registrar cliente	El sistema debe permitir a un usuario registrar nuevos cliente, incluyendo la captura de su imagen facial.	Alta	64
04	Capturar imagen facial	El sistema debe capturar la imagen facial de un usuario utilizando una cámara web y almacenarla en la base de datos.	Alta	48
05	Almacenar información en base de datos	El sistema debe almacenar la información de los usuarios y clientes (incluyendo imágenes faciales) en una base de datos para su posterior análisis y comparación.	Alta	32
06	Almacenar imágenes en dataset	El sistema debe almacenar las imágenes faciales capturadas en un dataset para entrenar el modelo de reconocimiento facial.	Alta	48
07	Comparar rostros	El sistema debe comparar la imagen facial capturada en tiempo real con las imágenes almacenadas en la base de datos para calcular un porcentaje de similitud.	Alta	72

09	Identificar usuarios/clientes	El sistema debe identificar al usuario/cliente en tiempo real basándose en la comparación de rostros.	Alta	64
010	Validar identidad	El sistema debe validar la identidad del usuario comparando el rostro capturado con el rostro registrado.	Alta	48
011	Permitir ingreso según similitud	El sistema debe permitir el ingreso del usuario/cliente si el porcentaje de similitud supera un umbral predefinido.	Alta	56
012	Listar usuarios	El sistema debe permitir a un usuario visualizar una lista de todos los clientes registrados.	Media	16
013	Listar clientes	El sistema debe permitir a un administrador visualizar una lista de todos los usuarios registrados.	Media	16

Nota. La tabla muestra las especificaciones de los requerimientos. Fuente: Elaboración propia (2024).

Requerimientos no Funcionales del Software

Además de los requerimientos funcionales, que definen las funcionalidades del sistema, es necesario considerar los requerimientos no funcionales. Los requerimientos no funcionales describen las características generales del software, como su desempeño, seguridad y usabilidad. Estos requerimientos, a diferencia de los funcionales, no especifican qué debe hacer el sistema, sino cómo debe hacerlo. En la tabla se detallan los atributos de calidad que el software debe poseer para garantizar su éxito.

Tabla 6

Requerimientos no funcionales del software

N°	Requerimiento No Funcional	Usuario	Descripción
1	Base de datos	Administrador	Define el tipo de base de datos, su estructura y las operaciones que se realizarán sobre ella (por ejemplo, SQL Server, MySQL).
2	Usabilidad	usuario y cliente	Especifica los criterios de facilidad de uso de la interfaz, como la intuitividad, la consistencia y la accesibilidad.
3	Rendimiento	Administrador	Establece los niveles de respuesta del sistema, como tiempos de carga de páginas, tiempos de respuesta a consultas y capacidad de manejo de carga.
4	Seguridad	Administrador	Define las medidas de seguridad necesarias para proteger la información del sistema, como autenticación, autorización, cifrado y protección contra ataques.
5	Eficiencia	Usuario/Cliente	Especifica la optimización de los recursos del sistema, como el uso de la CPU y la memoria, para garantizar un funcionamiento rápido y eficiente.
6	Confidencialidad	Administrador	Establece las medidas para proteger la privacidad de los datos, como el control de acceso y la gestión de permisos.
7	Integridad	Administrador	Garantiza la precisión, consistencia y completitud de los datos almacenados en el sistema.
8	Disponibilidad	Administrador	Define el tiempo de funcionamiento del sistema y los procedimientos para restaurar el servicio en caso de fallas.

Nota. La tabla muestra los Requerimientos no funcionales del software. *Fuente.* Elaboración propia (2024).

Actividad 2

Autenticación de Usuarios

En este proceso de verificación de la identidad de un usuario mediante la comparación de credenciales presentadas con las almacenadas en una base de datos. Los métodos de autenticación pueden ser basados en conocimiento (contraseñas). Al iniciar sesión, el usuario proporciona sus credenciales, que son procesadas por el sistema. Si las credenciales son válidas, se genera una sesión de usuario y se concede el acceso a los recursos autorizados. En caso contrario, se muestra un mensaje de error y se deniega el acceso. A continuación, se muestra un ejemplo de esta actividad en la plataforma Face Recognition.

Portal Web del Administrador

Repositorio

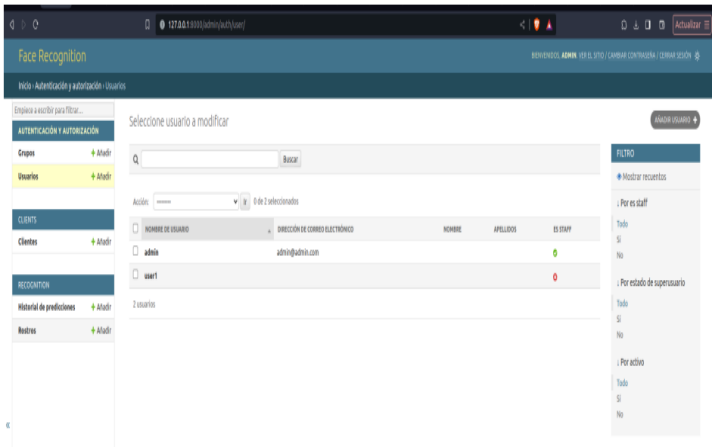
https://github.com/danitamay0/face-recognition

El sistema solicita al usuario que proporcione sus nombres, apellidos, correo electrónico y tres fotografías de su rostro para completar el proceso de registro, como se muestra a continuación:

Usuarios

Figura 9

Usuarios face- recognition

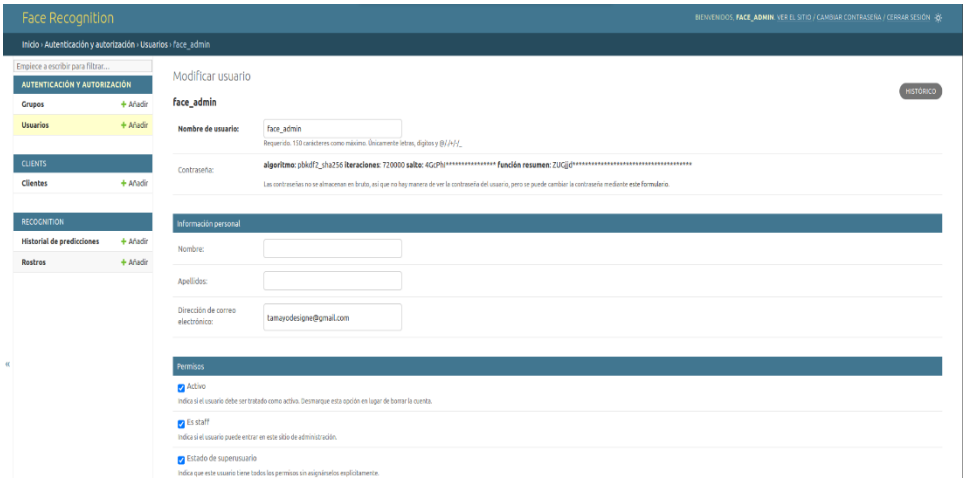


Nota. La figura muestra los Usuarios face- recognition. *Fuente.* Elaboración propia (2024).

En la vista de usuarios, se presenta una lista de los registros almacenados en el sistema. La tabla principal muestra información relevante como el nombre del usuario, la dirección de correo electrónico y la propiedad "ES STAFF", que indica si un usuario tiene permisos para acceder al sistema. Adicionalmente, se incluye una sección de filtros que permite buscar usuarios según las propiedades Staff, Superusuario y Activo. También se dispone de un buscador específico para localizar usuarios por nombre de usuario.

Figura 10

Detalle usuario – Portal Web Administrador



Nota. La figura muestra el detalle de un Usuario face- recognition. *Fuente.* Elaboración propia (2024).

Al seleccionar un usuario de la lista, se abre el módulo de detalle de usuarios, donde se muestra toda la información asociada al registro. En esta sección, es posible realizar actualizaciones en:

Nombre de Usuario

Información Personal. Incluye nombres, apellidos y dirección de correo electrónico.

Sección de Permisos. Activo: Indica si el usuario debe ser tratado como activo. Si no, esta opción puede desmarcarse en lugar de eliminar la cuenta.

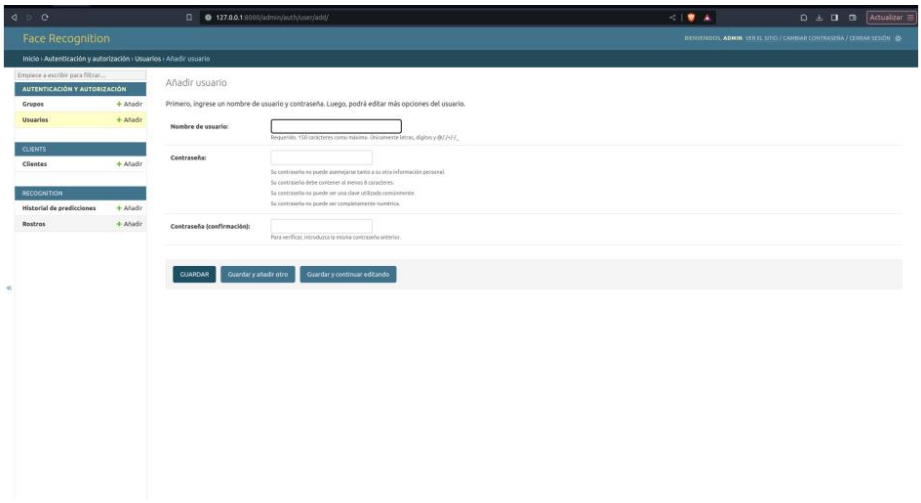
Es Staff: Señala si el usuario tiene acceso al sitio de administración.

Estado de Superusuario. Indica que este usuario tiene todos los permisos sin necesidad de asignarlos explícitamente.

Esta funcionalidad permite gestionar los datos y permisos de los usuarios de forma eficiente y detallada.

Usuario -Crear

Figura 11 *Usuario- crear face- recognition*



Nota. La figura muestra usuario- crear face- recognition. *Fuente.* Elaboración propia (2024).

El módulo de creación de usuarios presenta un formulario con los siguientes campos:

Nombre de usuario: Requiere validación para asegurar que el texto tenga un máximo de 150 caracteres y esté compuesto únicamente por letras, dígitos y los símbolos permitidos (@, ., +, -, _).

Contraseña y Confirmación de contraseña: Ambas contraseñas deben coincidir y cumplir con criterios de seguridad, incluyendo:

Un mínimo de 8 caracteres.

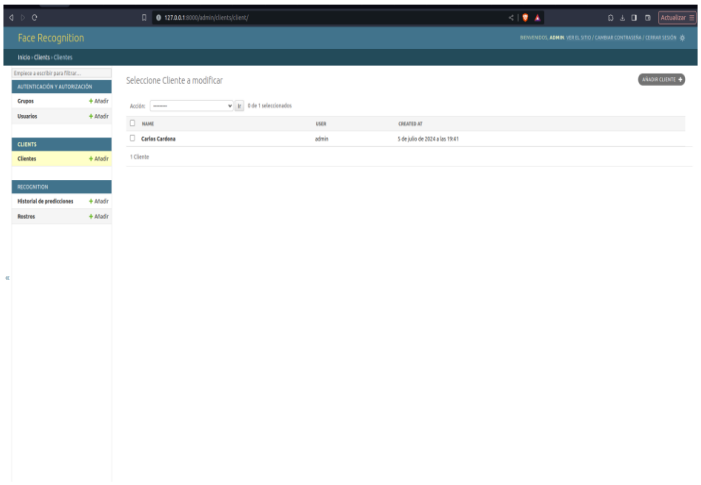
No ser completamente numérica.

Este enfoque garantiza la integridad de los datos y refuerza la seguridad del sistema.

Clientes

Figura 12

Clientes face- recognition



Nota. La figura muestra clientes face- recognition. *Fuente.* Elaboración propia (2024).

En la vista de clientes, se presenta una lista con los registros almacenados en el sistema. La tabla principal muestra información relevante, como:

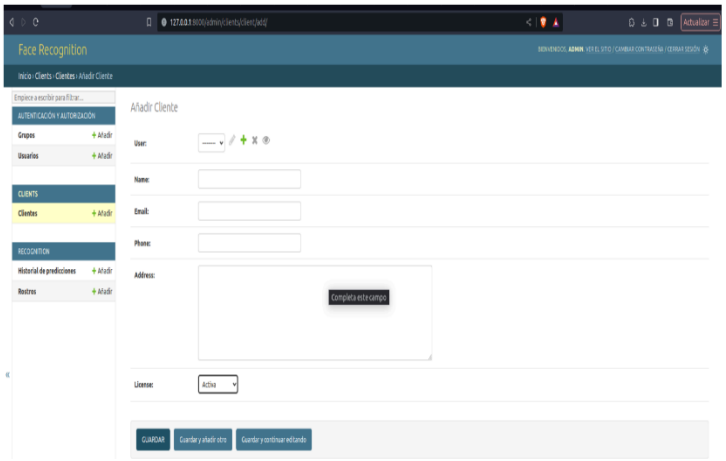
Nombre del cliente.

Usuario asignado al cliente.

Fecha de creación del registro.

Este módulo permite listar y visualizar de manera organizada todos los clientes registrados en el sistema, facilitando su gestión.

Figura 13
Clientes crear Portal Web Administrador



Nota. La figura muestra el formulario para crear clientes face- recognition. *Fuente.* Elaboración propia (2024).

El módulo "Crear Cliente" permite gestionar la creación de nuevos clientes en el sistema, los cuales podrán ser vinculados a usuarios existentes y configurados para participar en el sistema de reconocimiento facial. Este formulario asegura que solo los clientes con licencias activas puedan utilizar el reconocimiento facial.

Campos del formulario

Usuario: Campo seleccionable (dropdown). Con la lista de usuarios previamente registrados en el sistema.

Email

Teléfono (Phone)

Dirección (Address)

Licencia (License), campo seleccionable (dropdown).

Opciones disponibles

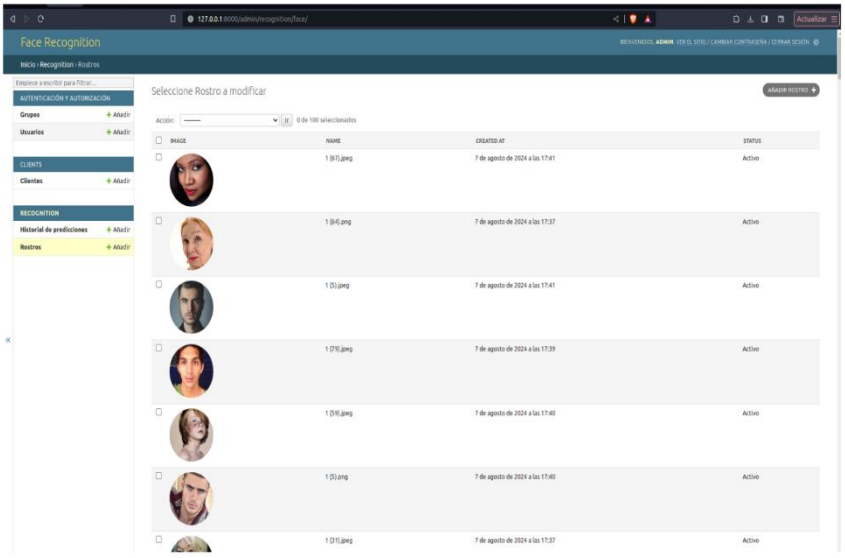
Pendiente: Cliente en proceso de registro o aprobación.

Activa: Cliente autorizado para reconocimiento facial.

Desactivada: Cliente sin autorización para usar el sistema.

Rostros

Figura 14
Rostros - Lista de registros Portal Web Administrador



Nota. La figura muestra el listado de rostros almacenados. *Fuente*. Elaboración propia (2024).

El módulo de lista de “Rostros" ofrece una vista general de todos los rostros registrados en el sistema. Proporciona detalles clave que permiten identificar y gestionar los registros de manera eficiente. Este módulo está diseñado para facilitar la administración y verificación de los datos almacenados en el sistema de reconocimiento facial.

Elementos mostrados en la lista

Imagen principal: Miniatura de la imagen principal del rostro registrado.

Nombre asignado al rostro en el momento de su registro.

Fecha de creación: Muestra la fecha y hora en la que el rostro fue registrado en el sistema.

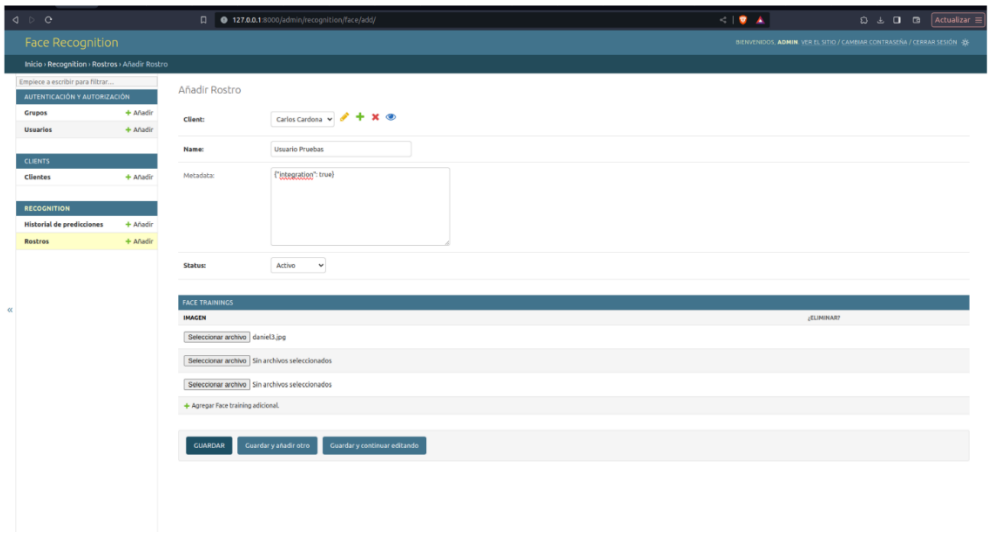
Estado (Status):

Activo: El rostro está habilitado para ser utilizado en el reconocimiento facial.

Inactivo: El rostro no está habilitado para reconocimiento facial.

Rostros

Figura 15
Rostros - Crear Portal Web Administrador



Nota. La figura muestra el formulario para crear rostros. *Fuente.* Elaboración propia (2024).

El módulo "Añadir Rostro" permite registrar nuevos rostros en el sistema de reconocimiento facial, asociándolos a un cliente existente y proporcionando información esencial para garantizar la precisión y efectividad del reconocimiento. Este formulario asegura que los datos requeridos para el entrenamiento y operación del sistema sean consistentes y suficientes.

Campos del formulario

Cliente (Client): Lista desplegable que muestra los clientes registrados en el sistema. Es obligatorio.

Nombre (Name): Campo de texto para identificar el rostro. Es obligatorio.

Metadata: Campo tipo JSON para guardar información no estructurada adicional asociada al rostro. Es opcional.

Estado (Status): Lista desplegable con opciones de "Activo" e "Inactivo". Es obligatorio.

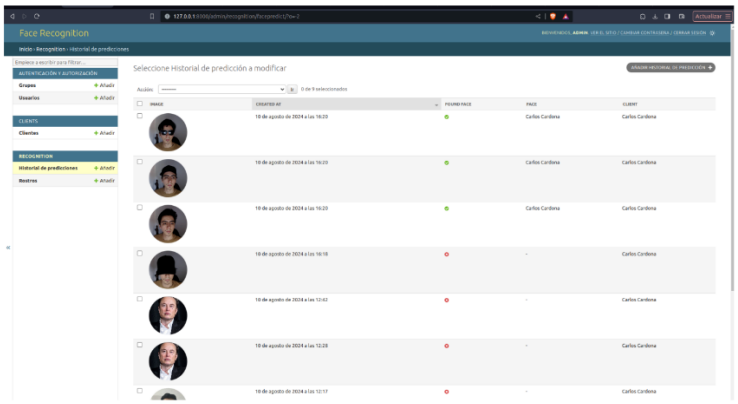
Lista de Imágenes: Campo para subir archivos en formatos .png, .jpg, o .jpeg. Se requieren al menos 3 imágenes, esto es necesario para mejorar la presición del algoritmo.

Una vez se guarda el registro, se extraen los códigos faciales de cada imagen usando la red neuronal de **face_recognition** y se guardan en la base de datos.

Rostros

Figura 16

Historial de predicciones Portal Web Administrador



Nota. La figura muestra el reporte de las predicciones que se han realizado. *Fuente*. Elaboración propia (2024).

El módulo de Historial de predicciones presenta una lista con todos los intentos realizados en el reconocimiento facial. La tabla incluye la siguiente información:

Imagen Capturada. Muestra la imagen utilizada para intentar la predicción.

Fecha de Creación. Indica cuándo se generó el registro.

Found Face. Señala si se encontró un rostro previamente creado y relacionado en la predicción.

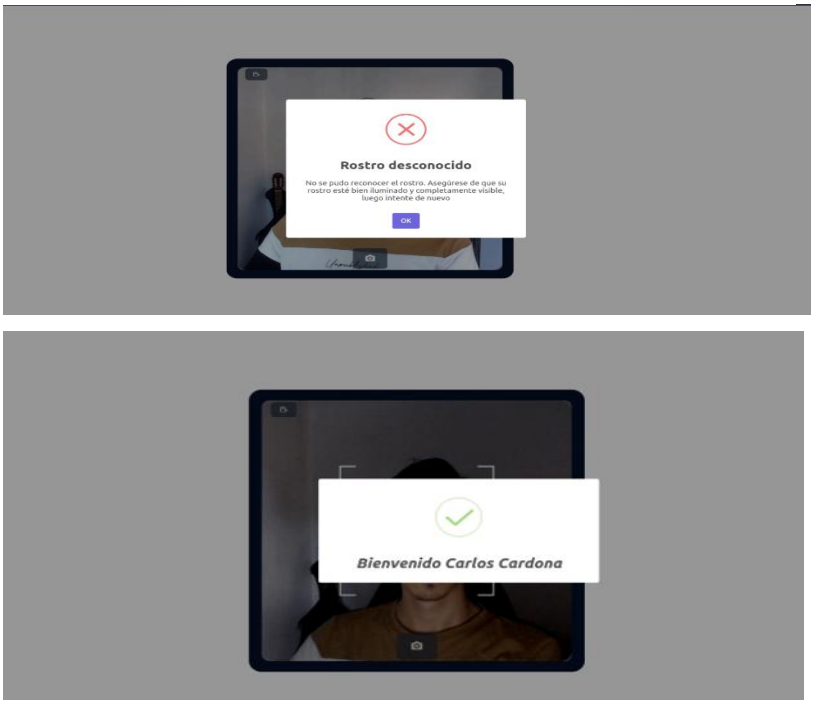
Face. Nombre del rostro asociado a la predicción.

Client. Cliente al que pertenece el rostro encontrado.

Este módulo facilita el seguimiento y análisis de las predicciones realizadas, proporcionando un registro detallado de los intentos y sus resultados.

Figura 17

Implementación de reconocimiento facial



Nota. La figura muestra componente de reconocimiento facial exitosamente. *Fuente*. Elaboración propia (2024).

El componente de reconocimiento facial realiza una integración a través de una API REST utilizando el endpoint /faces/recognition-knn/ del administrador de rostros. Este endpoint procesa la clasificación del rostro capturado por la cámara, compara el rostro con los registros existentes y, si encuentra una coincidencia, devuelve la información correspondiente. En el caso de una clasificación exitosa, el componente frontend muestra el nombre del usuario identificado.

Análisis de las Especificaciones de los Requerimientos Funcionales

Actividad 3

Antes de iniciar el desarrollo del sistema, se realizó un análisis detallado de los requerimientos funcionales prioritarios. Este análisis permitió identificar las funcionalidades esenciales que el software debe ofrecer para satisfacer las necesidades del cliente. Los resultados de este análisis se plasmaron en un documento de especificaciones técnicas, el cual sirve como guía para el equipo de desarrollo.

Requerimiento Funcional 1, Iniciar Sesión

Tabla 7

Requerimiento funcional 1, Iniciar Sesión

Código	Nombre	Prioridad	Descripción	Usuario	Entradas	Proceso	Salidas
1	Iniciar sesión	Alta	Permitir el acceso al sistema a un usuario registrado.	Administrador	Usuario, Contraseña	Verificar credenciales en la base de datos. Si son válidas, otorgar acceso al sistema.	Usuario Autentificado

Nota. La tabla muestra los Requerimientos no funcionales del software. *Fuente*. Elaboración propia (2024).

Nota: Se han priorizado los siguientes requerimientos para garantizar que el sistema cumpla con los objetivos establecidos.

Requerimiento Funcional 2, Registrar Usuario

Tabla 8

Requerimiento funcional 2, Registrar usuario

Código	Nombre	Prioridad	Descripción	Usuario	Entradas	Proceso	Salidas
2	Registrar Usuario	Alta	Permitir la creación de un nuevo usuario en el sistema y su almacenamiento en la base de datos.	Administrador	Nombres, Apellidos, Nombre de usuario (único), Contraseña	Validar datos de entrada, almacenar en la base de datos, enviar notificación de confirmación (opcional).	Nuevo usuario registrado en la base de datos, notificación al usuario (opcional).

Nota. La tabla muestra Requerimiento funcional 2, Registrar usuario. *Fuente*. Elaboración propia (2024).

Requerimiento Funcional 3, Reconocimiento Facial

Tabla 9

Requerimiento funcional 3, Reconocimiento facial

Código	Nombre	Prioridad	Descripción	Usuario	Entradas	Proceso	Salidas
3	Reconocimiento Facial	Alta	Identificar si un usuario está registrado en la base de datos.	Usuario Final	Imágenes faciales en tiempo real capturadas por la cámara web.	Comparar las imágenes capturadas con las plantillas faciales almacenadas en la base de datos.	Nombre completo del estudiante si se encuentra registrado, mensaje de "Usuario desconocido" si no se encuentra.

Nota. La tabla muestra Requerimiento funcional 3, Reconocimiento facial. *Fuente.* Elaboración propia (2024).

Actividad 4

Determinación de la instrumentación y herramientas de software para el sistema de reconocimiento facial.

Metodología de Reconocimiento Facial

El reconocimiento facial es una tecnología que utiliza los rasgos faciales para identificar a las personas de manera única. A continuación, el proceso de desarrollo del modelo de reconocimiento facial se estructura en dos fases principales: entrenamiento y ejecución. La fase de entrenamiento, dividida en dos etapas, implica la creación y el ajuste del modelo utilizando un conjunto de datos de entrenamiento. La fase de ejecución, que abarca dos etapas adicionales, consiste en la aplicación del modelo entrenado a nuevas imágenes para identificar rostros. Ambas fases están interrelacionadas y siguen una secuencia, como se muestra en la figura.

Tabla 10

fase de extracción de códigos faciales

Fase de Extracción de Códigos Faciales	Número de Etapas	Descripción
	1	Elaboración del DataSet
	2	Entrenamiento de la red neuronal artificial

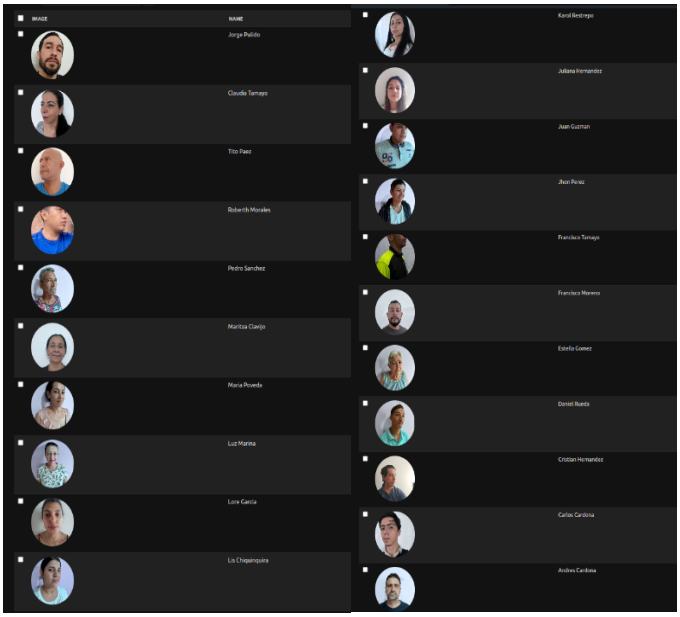
Nota. La tabla muestra fase de extracción de códigos faciales. Fuente: Elaboración propia (2024).

Etapa 1: Elaboración del DataSet.

En la etapa de elaboración del Dataset, se lleva a cabo la recopilación de una cantidad significativa de imágenes faciales de alta calidad. Asimismo, Estas imágenes son procesadas y etiquetadas para crear un conjunto de datos balanceado y representativo, que incluirá variaciones en expresiones faciales, iluminación, poses y condiciones ambientales, por lo tanto, este DataSet será utilizado para entrenar y evaluar el modelo de reconocimiento facial.

Figura 18

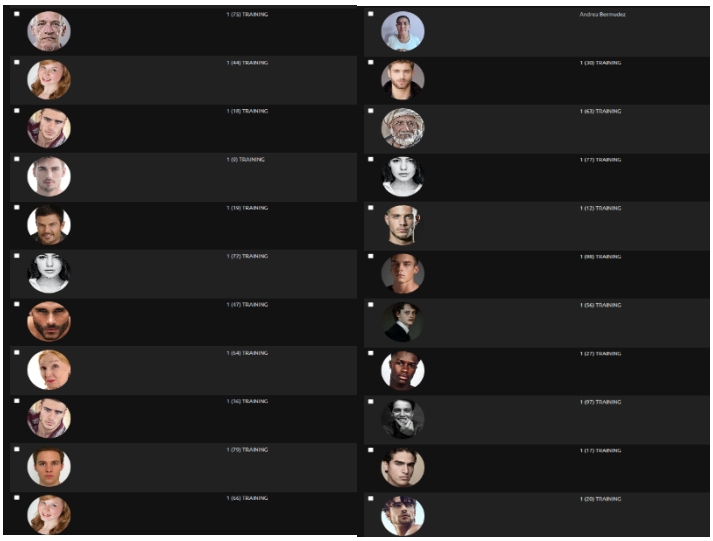
Elaboración del DataSet



Nota. La figura muestra la elaboración del DataSet. *Fuente.* Elaboración propia (2024).

Figura 19

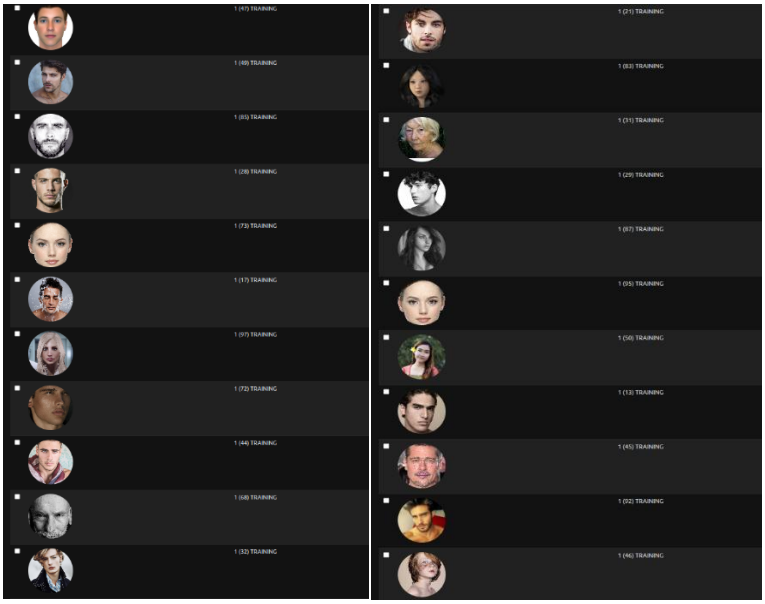
Elaboración del DataSet1



Nota. La figura muestra la elaboración del DataSet1. *Fuente.* Elaboración propia (2024).

Figura 20

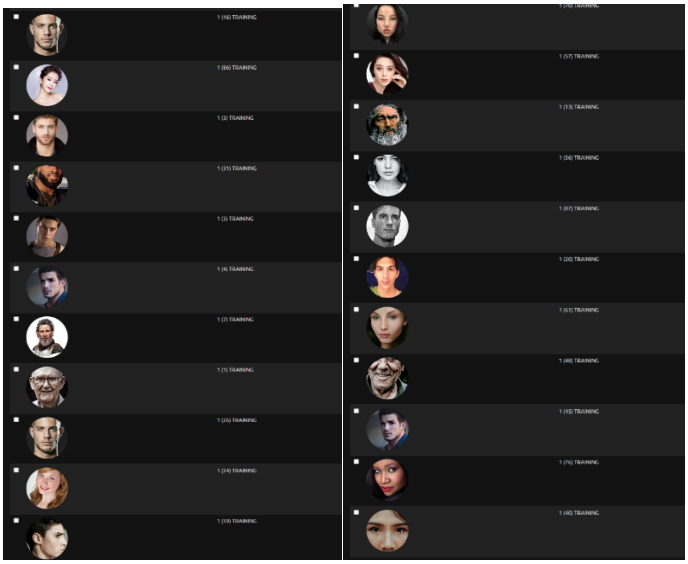
Elaboración del DataSet2



Nota. La figura muestra la elaboración del DataSet2. *Fuente*. Elaboración propia (2024).

Figura 21

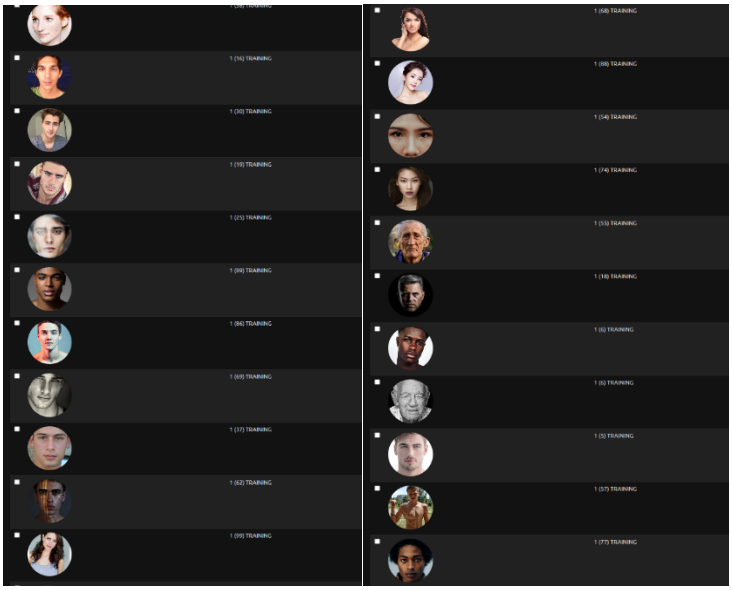
Elaboración del DataSet3



Nota. La figura muestra la elaboración del DataSet3. *Fuente*. Elaboración propia (2024).

Figura 22

Elaboración del DataSet3

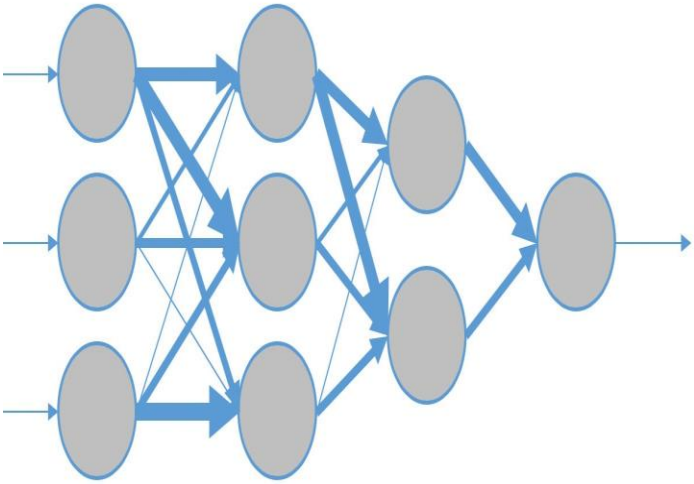


Nota. La figura muestra la elaboración del DataSet3. *Fuente*. Elaboración propia (2024).

La calidad de un sistema de reconocimiento facial depende en gran medida de la calidad y diversidad de los datos utilizados para entrenarlo. La figura muestra la creación de un conjunto de datos faciales variado, con múltiples imágenes por persona tomadas desde distintos ángulos y bajo diferentes condiciones, incluyendo oclusiones. Este tipo de dataset garantiza que el modelo sea capaz de reconocer rostros en una amplia variedad de situaciones reales, mejorando así su precisión y robustez.

Figura 23

Ejemplo red neuronal



Nota. La figura muestra ejemplo red neuronal. *Fuente*. Elaboración propia (2024).

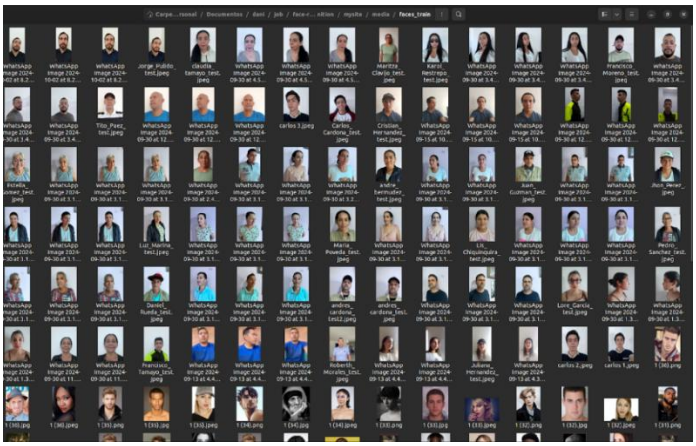
El entrenamiento de una red neuronal para la detección de rostros es un proceso fundamental. Para que una red neuronal pueda identificar rostros de manera precisa y confiable, es necesario entrenarla con un conjunto de datos que incluya una gran cantidad de imágenes, tanto de rostros como de objetos no faciales, capturadas en diferentes escenarios y condiciones de iluminación. Esta diversidad de datos permitirá a la red aprender a extraer las características distintivas de un rostro y a descartar aquellas que no son relevantes. Una vez entrenada, la red podrá detectar rostros en imágenes reales con un alto grado de precisión.

Las imágenes que servirán para entrenar el algoritmo corresponden a aquellas que fueron almacenadas en la etapa 1. La figura adjunta muestra la forma en que estas imágenes están organizadas y estructuradas dentro del conjunto de datos.

Formato de las Imágenes para el Entrenamiento de los Algoritmos

Figura 24

Formato de las imágenes para el entrenamiento de los algoritmos



Nota. La figura muestra formato de las imágenes para el entrenamiento de los algoritmos.

Fuente. Elaboración propia (2024).

Descripción de las Imágenes Tal y Como Se Especifica en el Registro

Figura 25

Descripción de las imágenes tal y como se especifica en el registro

Nota. La figura muestra descripción de las imágenes tal y como se especifica en el registro.

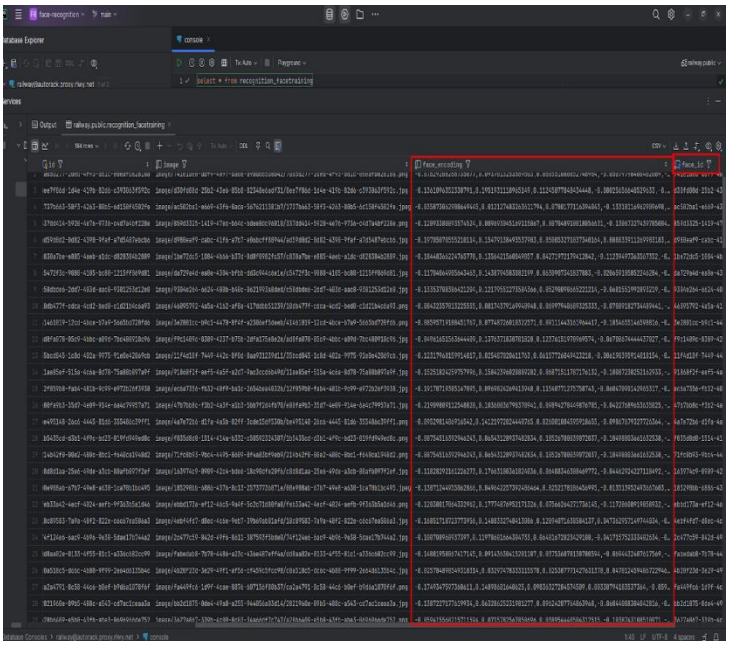
Fuente. Elaboración propia (2024).

La figura ilustra la estructura de almacenamiento de las imágenes, especificando que cada imagen se ubica en un directorio con un nombre único en formato JPG o JPEG, requisitos indispensables para el procesamiento por parte del algoritmo.

Registros de los Códigos Faciales

Figura 26

Registros de los códigos faciales



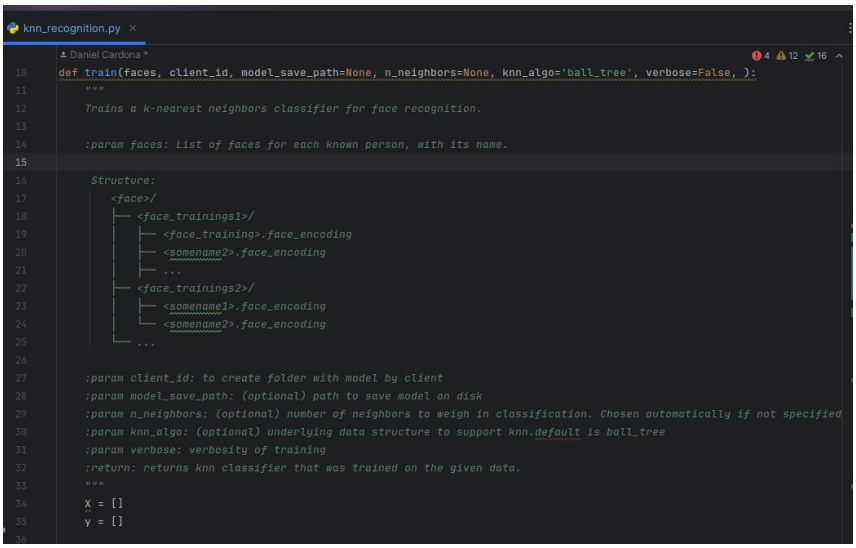
Nota. La figura muestra registros de los códigos faciales *Fuente.* Elaboración propia (2024).

Una vez procesadas las imágenes se generan los registros de los códigos faciales en la base de datos asociados al rostro de la persona almacenada en las fases previas.

Entrenamiento de la Red Neuronal en Python -1

Figura 27

Entrenamiento de la red neuronal en Python -1



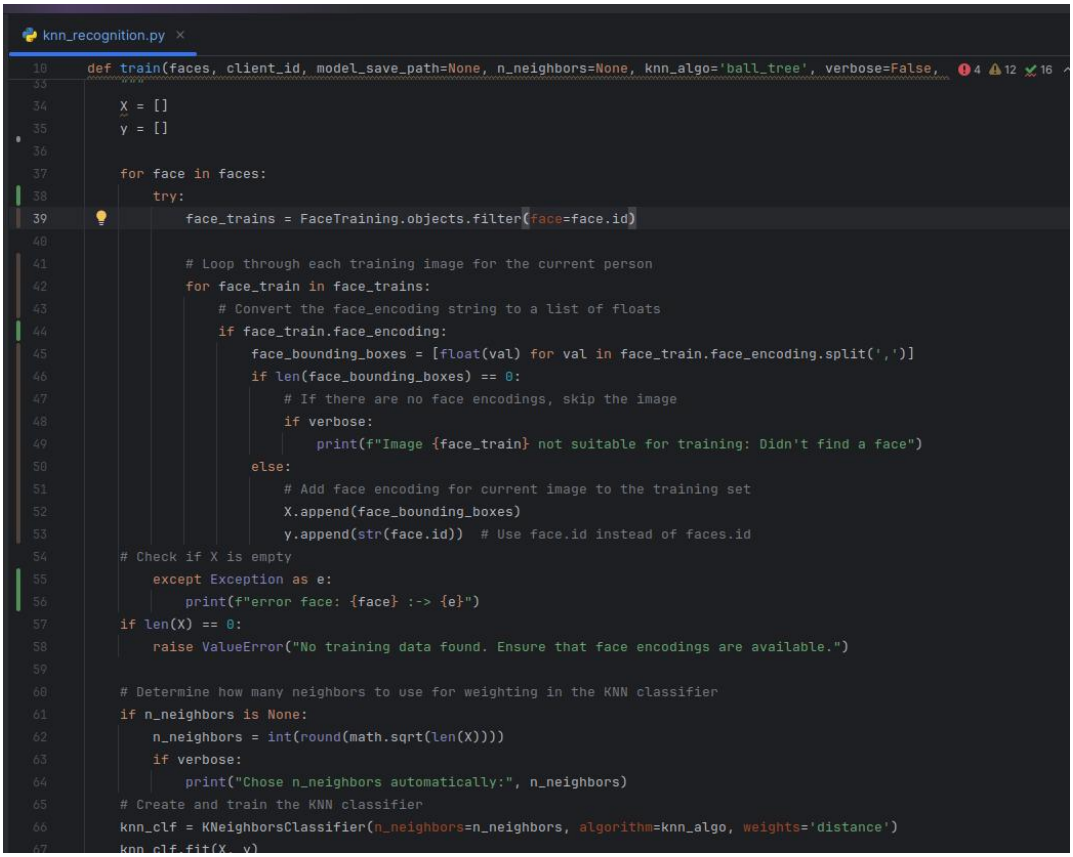
Nota. La figura muestra entrenamiento de la red neuronal en Python -1. *Fuente.* Elaboración propia (2024).

La función knn_recognition utiliza los códigos faciales extraídos por la red neuronal de la librería face_recognition, los cuales se almacenan en la base de datos y son asociados a un cliente. Estos códigos se emplean para entrenar un modelo de clasificación K-Vecinos (KNN). Con el modelo entrenado, es posible analizar y clasificar un nuevo rostro en función de los datos previamente registrados, identificando a qué cliente pertenece el rostro más cercano según el algoritmo KNN. Esto permite un reconocimiento facial eficiente y basado en los datos históricos del sistema.

Entrenamiento de la Red Neuronal en Python -2

Figura 28

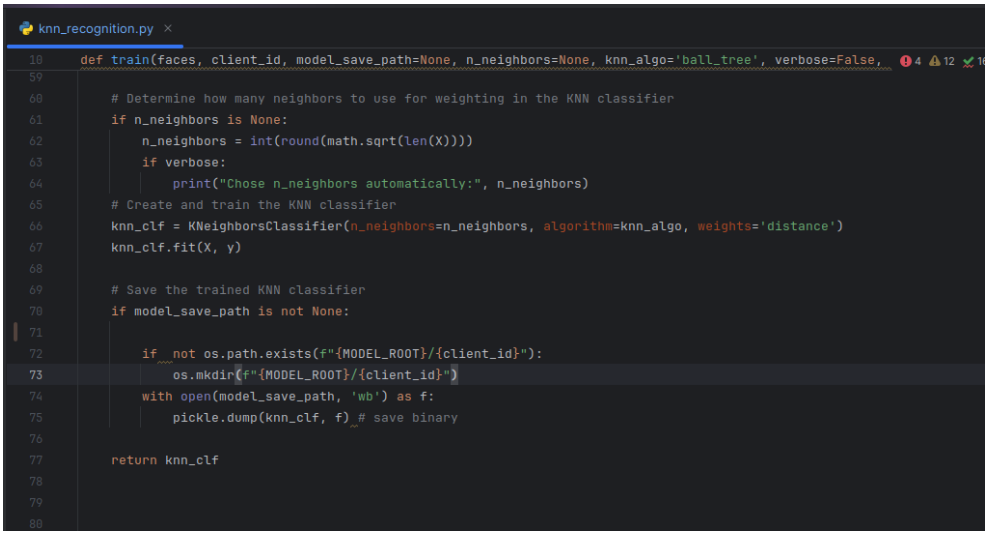
Entrenamiento de la red neuronal en Python -2



Nota. La figura muestra ejemplo red neuronal. *Fuente*. Elaboración propia (2024).

Figura 29

Ejemplo red neuronal



Nota. La figura muestra ejemplo red neuronal. *Fuente*. Elaboración propia (2024).

Entrenamiento de Modelo de Machine KNeighborsClassifier Python -3

Las figuras, muestra las líneas de código para el entrenamiento de la red, los cuales se explican a continuación:

Se realizo entrenamiento a 21 rostros conocidos, 127 rostros desconocidos al finalizar el aprendizaje se obtuvo el modelo entrenado como se evidencia en la figura, con los modelos almacenados.

Fase 2: Diseño del Sistema

Se elabora la arquitectura del sistema, incluyendo la identificación de los módulos principales (adquisición de imágenes, preprocesamiento, extracción de características, clasificación, base de datos), la definición de las interfaces entre ellos y la especificación

de los requisitos de hardware y software. Se crean diagramas de flujo y diagramas de clases para visualizar la estructura del sistema.

Actividad 1

Elaboración de un diseño arquitectónico integral del sistema

Identificación de Componentes Principales: Definir los componentes clave que conforman el sistema, como módulos de captura de imágenes, algoritmos de reconocimiento facial, bases de datos de usuarios, etc. Detallar las funcionalidades y responsabilidades de cada componente.

Modelado de Interacciones: Establecer las relaciones y dependencias entre los componentes del sistema.

Representar gráficamente las interacciones y el flujo de datos entre los componentes.

Describir los protocolos de comunicación utilizados para la interacción entre componentes.

Definición de Interfaces: Especificar las interfaces que permiten la comunicación entre los componentes del sistema.

Definir los formatos de datos, los métodos de comunicación y las reglas de interacción para cada interfaz.

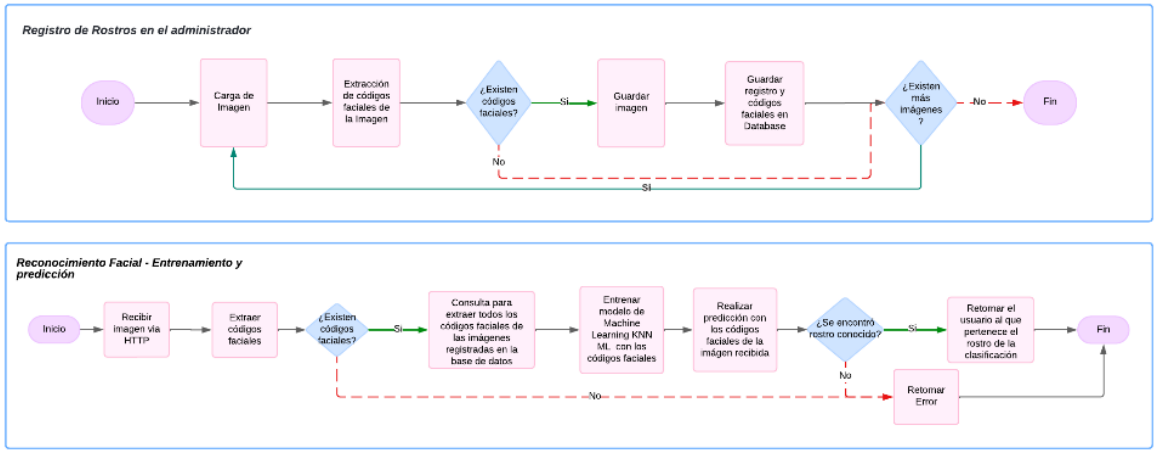
Documentar claramente las especificaciones de las interfaces para facilitar su implementación.

A continuación, se muestran los pasos para el desarrollo del diseño del sistema de reconocimiento facial usando face recognition.

Pasos para la Creación del Diseño del Sistema de Reconocimiento Facial

Figura 30

Pasos para la creación del diseño del sistema de reconocimiento facial



Nota. La figura muestra pasos para la creación del diseño del sistema de reconocimiento facial.

Fuente. Elaboración propia (2024).

Imágenes de Muestra. Para construir un detector de objetos, es fundamental contar con una variedad de imágenes que representen diferentes condiciones y perspectivas. Por lo tanto, las muestras positivas deben mostrar el objeto de interés en distintas poses, tamaños y entornos, mientras que las muestras negativas deben incluir objetos similares o fondos complejos que puedan confundir al clasificador. A continuación, se muestra una tabla con las cuatro muestras necesarias.

Tabla 11

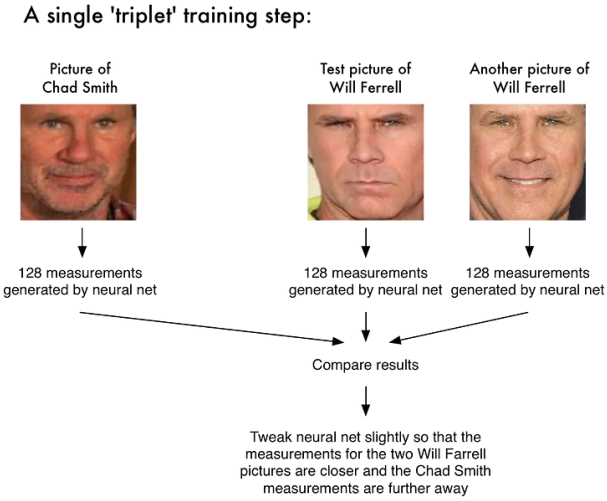
Tipo de muestra

Tipo de Muestra	Uso
Positivas para entrenamiento	Generación del clasificador
Negativas para entrenamiento	Generación del clasificador
Positivas para prueba	Evaluación del clasificador
Negativas para prueba	Evaluación del clasificador

Nota. La tabla muestra tipo de muestra. *Fuente*. Elaboración propia (2024).

Por lo tanto, para la extracción de características de cada objeto son aplicando ciertas funciones que permiten la representación y descripción de los objetos de interés en la imagen. Además, los filtros con bases Haar, realizan una codificación de diferencia de intensidades en la imagen, generando características de contornos, puntos y líneas, mediante la captura de contraste entre regiones como se muestra en la figura.

Figura 31
Tres imágenes para entrenamiento de red neuronal



Nota. La figura muestra 3 rostros que se van a comparar basado en los 128 códigos faciales.

Fuente. Geitgey, A. (2020).

Actividad 2

Creación de un esquema de base de datos para la gestión de información de usuarios e imágenes faciales.

Definición de Entidades

Identificar las entidades principales que se almacenarán en la base de datos, como usuarios, imágenes faciales y registros de acceso.

Definir los atributos de cada entidad, incluyendo tipos de datos, restricciones y relaciones entre entidades.

Tabla 12

Definición de entidades

Entidad	Descripción	Atributos clave	Relaciones
auth_user	Usuario autenticado en el sistema	id_usuario, nombre_usuario, correo_electronico, contrasena_hash, fecha_creacion, rol	1:N con face_training (un usuario puede tener muchas imágenes de entrenamiento)
clientes	Cliente del sistema (puede o no ser un usuario autenticado)	id_cliente, nombre_cliente, empresa, contacto	1:N con face (un cliente puede tener muchas imágenes faciales)
face	Imagen facial	id_face, imagen, fecha_captura, calidad_imagen	1:1 con face_training (una imagen facial solo puede estar asociada a un entrenamiento), N:1 con clientes (muchas imágenes pueden pertenecer a un cliente)
face_training	Imagen facial utilizada para entrenar el modelo	id_face_training, id_usuario, id_face, etiqueta, fecha_entrenamiento	N:1 con auth_user (muchas imágenes de entrenamiento pueden pertenecer a un usuario), 1:1 con face (una imagen de entrenamiento solo puede usar una imagen facial)

Nota. La tabla muestra la definición de entidades. *Fuente.* Elaboración propia (2024).

Modelado de Relaciones

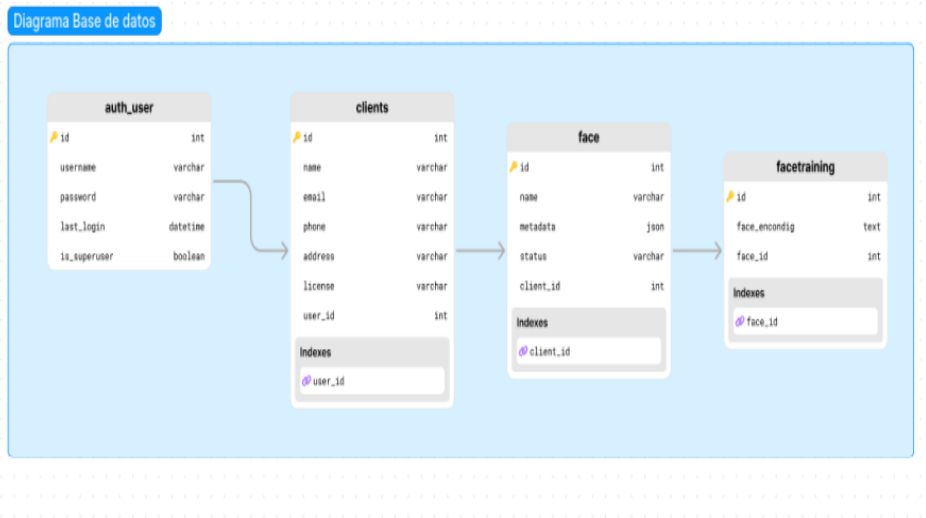
Establecer las relaciones entre las entidades de la base de datos.

Utilizar un modelo de datos adecuado, como el modelo entidad-relación (E-R), para representar las relaciones entre entidades.

Definir las claves primarias, claves foráneas y otras restricciones de integridad de datos.

Figura 32

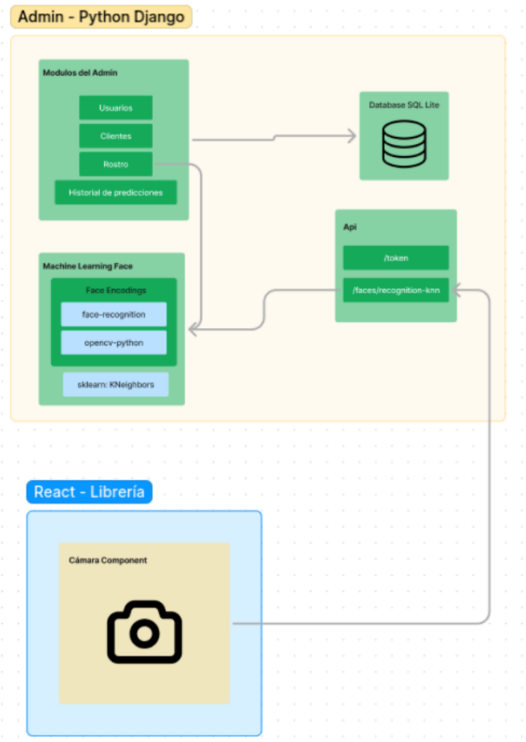
Diagrama base de datos



Nota. La figura muestra el diagrama base de datos. *Fuente.* Elaboración propia (2024).

Figura 33

Diagrama admin-python django



Nota. La figura muestra el diagrama admin-python django. *Fuente.* Elaboración propia (2024).

Diagrama de Clases

El diagrama de clases presentado en la Figura proporciona una visión general de la estructura del sistema de gestión de inventario. Cada clase representa un concepto del mundo real, como producto, almacén o proveedor. Se describen cada una de las clases respecto a: nombre, descripción, atributos, métodos y relaciones.

Clase Tipo de Usuario

Tabla 13

Clase tipo de usuario

Elemento	Descripción
Nombre	Usuario
Tipo	Clase
Descripción	Representa la información de los usuarios que tendrán acceso al sistema.
Atributos	id Usuario: Identificador único del usuario. Nombre: Nombre completo del usuario. Clave: Contraseña del usuario.
Métodos	Insertar: Agrega un nuevo registro de usuario a la base de datos. Actualizar: Modifica los datos de un usuario existente en la base de datos. Eliminar: Elimina un registro de usuario de la base de datos.

Nota. La tabla muestra Clase tipo de usuario. *Fuente.* Elaboración propia (2024).

Fase 3: Selección de la Técnica

Se evalúan y comparan diferentes algoritmos de clasificación: máquina de soporte vectorial (SVM), KVecinos (KNN), a su vez se utiliza la librería open source de Python: face recognition en función de su precisión, velocidad, escalabilidad y capacidad de adaptación a las condiciones específicas del proyecto. También, se selecciona el algoritmo que mejor se ajusta a los requerimientos técnicos y presupuestarios. Por lo tanto, se resaltan las siguientes dos fases La fase de ejecución, que abarca dos etapas adicionales, consiste en la aplicación del modelo entrenado a nuevas imágenes para identificar rostros. Ambas fases están interrelacionadas y siguen una secuencia, como se muestra en la tabla.

Tabla 14

Fase de ejecución

Fase de Ejecución	3	Reconocimiento facial
	4	Análisis de los resultados

Nota. La tabla muestra la fase de ejecución. Fuente: Elaboración propia (2024).

Actividad 1

Evaluación de algoritmos de reconocimiento facial para la verificación de identidad.

Selección de Algoritmos

Identificar y seleccionar algoritmos de reconocimiento facial con características y capacidades relevantes para el proyecto.

Análisis Comparativo

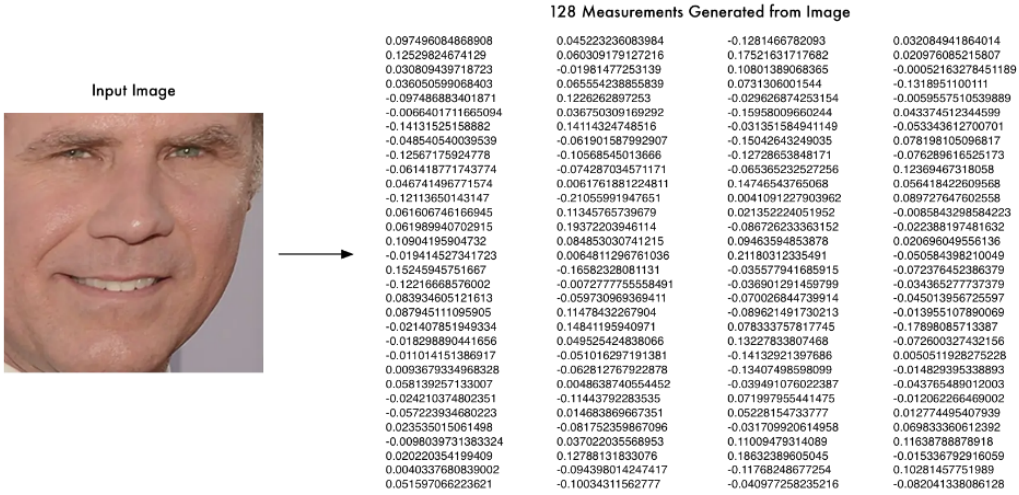
Realizar una comparación detallada de los algoritmos seleccionados, evaluando su rendimiento en diferentes escenarios y condiciones.

Utilizar métricas de evaluación adecuadas, como la tasa de reconocimiento facial (FRR), la tasa de falsos positivos (FAR) y la tasa de falsos negativos (FNR).

Fase de Ejecución

La fase de ejecución abarca dos etapas clave: reconocimiento y análisis de resultados. El reconocimiento facial se lleva a cabo utilizando el algoritmo Haar Cascade en face recognition, que se detallara a continuación.

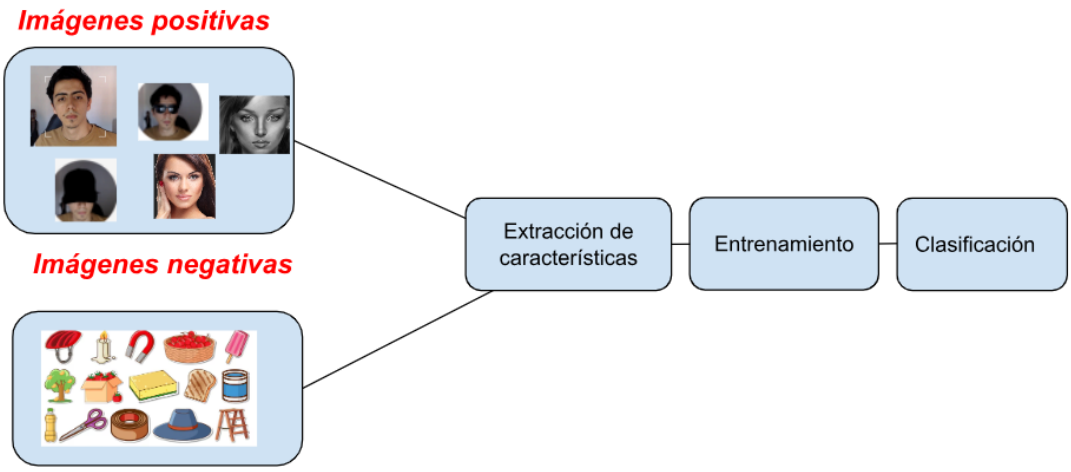
Figura 34
Extracción de códigos faciales



Nota. La figura muestra la extracción de los códigos faciales. *Fuente.* Geitgey, A. (2020).

Figura 35

Diagrama extracción de características reconocimiento facial



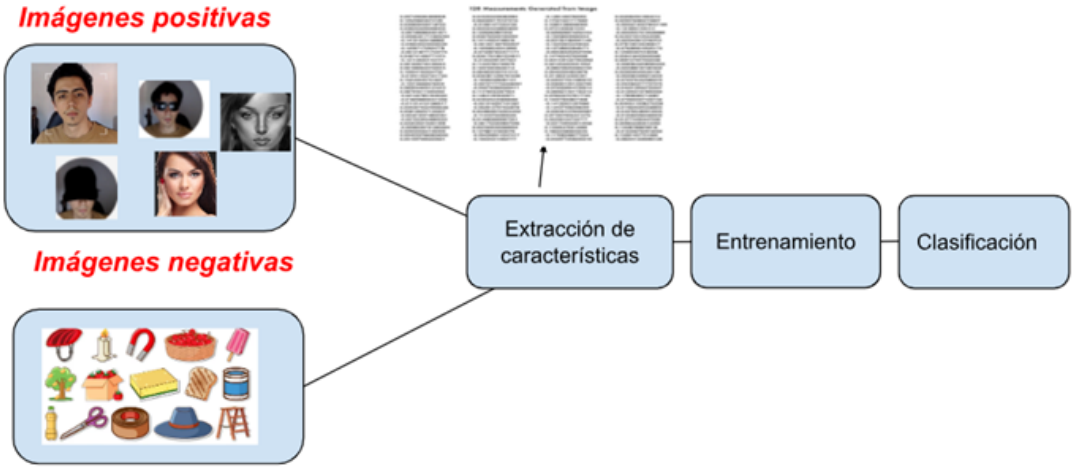
Nota. La figura muestra el diagrama extracción de características reconocimiento facial. *Fuente.* Elaboración propia (2024).

Desarrollo de un Sistema de Reconocimiento Facial

El entrenamiento de un clasificador de rostros es un proceso iterativo que requiere de una gran cantidad de datos. Tal como se observa en la figura, el entrenamiento de un clasificador de rostros requiere de una amplia base de datos compuesta por imágenes que contengan rostros (positivas) y por imágenes que no los contengan (negativas). Esta diversidad de imágenes permite al clasificador aprender a identificar las características distintivas de un rostro y a discriminarlo de otros objetos.

Figura 36

Diagrama entrenamiento de un clasificador de rostros



Nota. La figura muestra el diagrama entrenamiento de un clasificador de rostros. Fuente: Elaboración propia (2024).

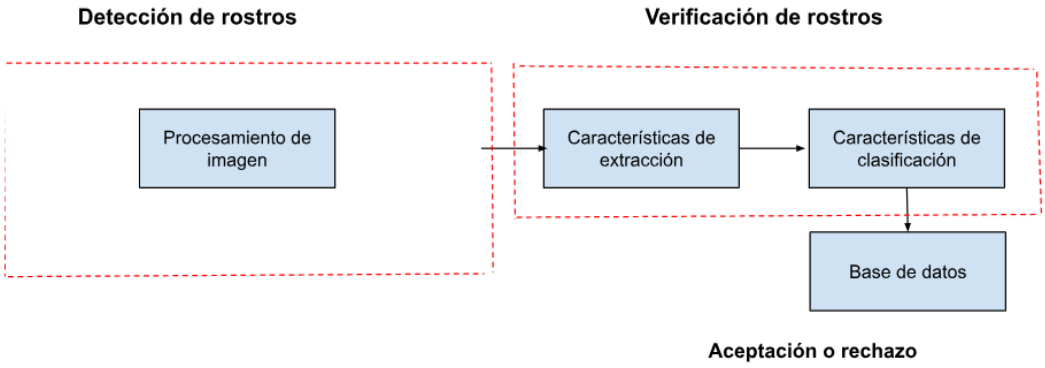
La figura describe el proceso de entrenamiento de un detector de rostros. Se inicia con un conjunto de datos de entrenamiento que incluye imágenes con y sin rostros. A partir de estas imágenes, se extraen características de Haar, que son utilizadas para entrenar una cascada de clasificadores. Esta cascada permite evaluar de manera jerárquica las regiones de interés, descartando aquellas que no cumplen con las características de un rostro y reteniendo solo las que son más probables de corresponder a un rostro.

Sistema de Reconocimiento Facial Basado en Dos Niveles para el Reconocimiento Facial: Detección y Verificación de rostros

La verificación facial es un proceso de comparación uno a uno, donde se confirma la identidad de una persona al cotejar su rostro con una imagen de referencia. La identificación, por otro lado, es un proceso de búsqueda uno a N, donde se busca una coincidencia en una base de datos de múltiples rostros.

Figura 37

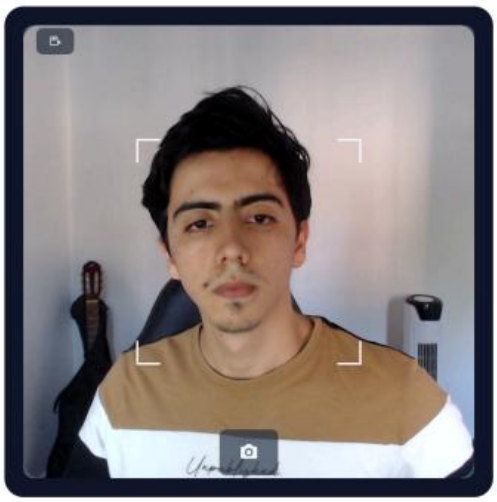
Diagrama proceso de comparación uno a uno



Nota. La figura muestra el diagrama proceso de comparación uno a uno. Fuente: Elaboración propia (2024).

Figura 38

Ejemplo de detección de rostros en face- recognition



Nota. La figura muestra el ejemplo de detección de rostros en face- recognition. *Fuente*. Elaboración propia (2024).

Ejemplo de Detección de Rostros

En la figura, se evidencia como face recognition logra detectar un rostro, mientras que ignora el fondo de la imagen u otros objetos que estén presentes dentro de ella.

Actividad 2

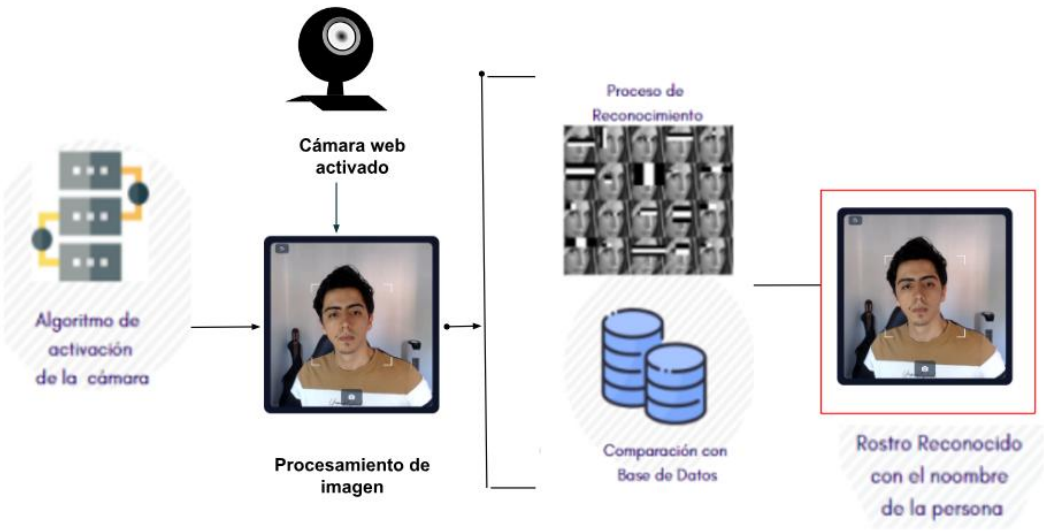
Determinar y analizar los rasgos distintivos de cada técnica de reconocimiento facial.

Reconocimiento Facial

Mediante la implementación de Python y la librería face-recognition-lib, se lleva a cabo un proceso de análisis de las características faciales en tiempo real. Esto permite identificar y verificar la identidad de las personas captadas por la cámara.

Figura 39

Diagrama pasos para el análisis de características faciales



Nota. La figura muestra el diagrama pasos para el análisis de características faciales (2024).

Fuente: Elaboración propia (2024).

Análisis de los Resultados

Se realiza diferentes pruebas con relación a los tipos planteados que son: rostro sin mascarilla y sin lentes, rostro con mascarilla sin lentes, rostro con lentes y mascarilla, rostro con lentes sin mascarilla. Estas pruebas se clasifican por tipo para analizar el porcentaje de reconocimiento de cada uno de ellos, de manera que a través de la aplicación del Deep Learning cumpla un porcentaje de precisión aceptable al reconocer e identificar el rostro de las personas, incluyendo las restricciones que sean causados por mascarillas o lentes que reduce los rasgos faciales para un mejor reconocimiento.

Fase 4: Implementación y Entrega

En la fase de implementación y entrega, se realizan pruebas en el entorno de producción para garantizar su correcto funcionamiento y la mediación de la precisión, la velocidad y la seguridad del sistema en una variedad de situaciones y condiciones.

Actividad 1

Desplegar el sistema en el entorno de producción y realizar pruebas finales para asegurar que funcione según lo esperado.

Validación del Rendimiento

Durante las pruebas finales, se ejecutan diversos escenarios y casos de uso para evaluar el rendimiento del sistema en diferentes condiciones. Esto incluye medir métricas como tiempos de respuesta, utilización de recursos y tasas de error.

Detección y Resolución de Errores. Cualquier error o defecto descubierto durante las pruebas se documenta, analiza y prioriza cuidadosamente para su resolución.

Elaboración del Conjunto de Testing

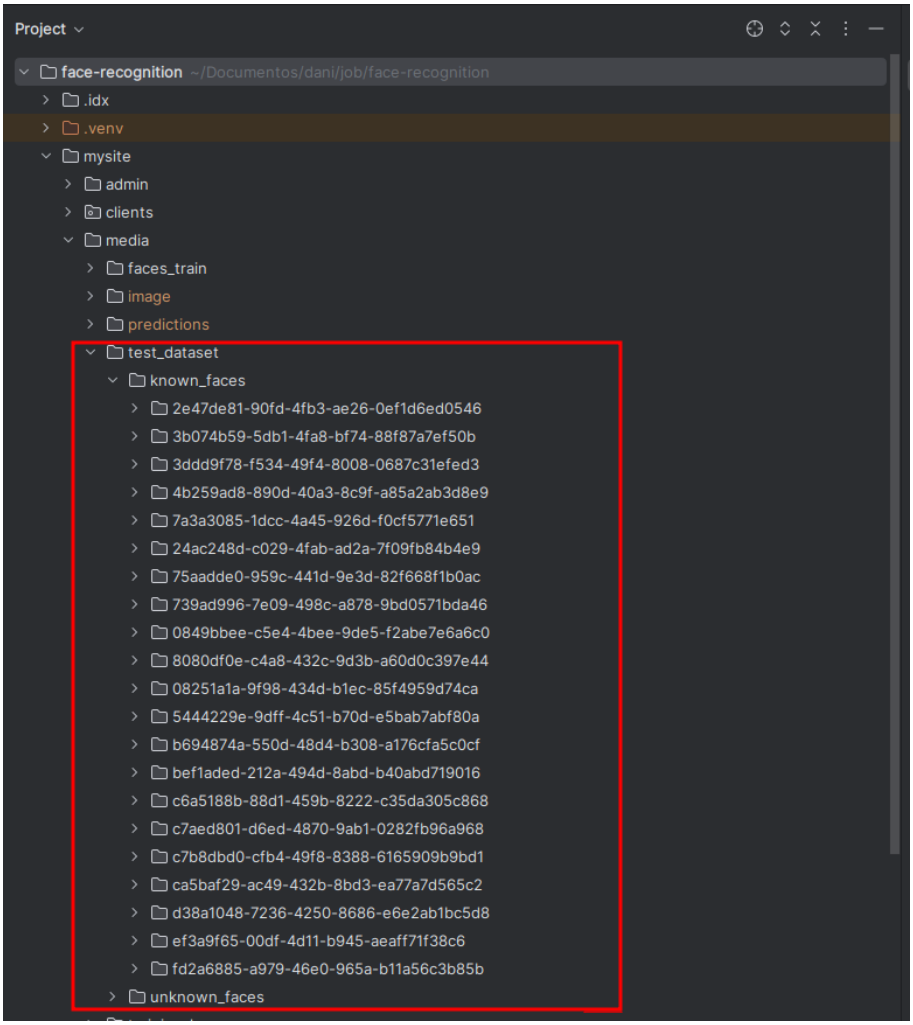
Para el análisis de los resultados, se construyó el conjunto de datos de prueba, dividido en dos categorías: rostros conocidos y rostros no conocidos. La estructura de carpetas consta de dos directorios principales. En el directorio "known_faces" se encuentran subcarpetas que corresponden al ID de cada rostro, lo que permite comparar la predicción y verificar si es correcta. Las imágenes utilizadas para los rostros conocidos incluyen fotografías de la misma persona en diferentes contextos: diferente ropa, rostro sin gorra ni lentes, rostro con gorra y sin lentes, y rostro sin gorra, pero con lentes.

En el segundo directorio, "unknown_faces", se almacenan imágenes de rostros que no están registrados en el sistema, y el resultado esperado es que el software no realice ningún reconocimiento sobre estos rostros.

Estas pruebas se clasifican por tipo para analizar el porcentaje de reconocimiento de cada uno de ellos, de manera que a través de la aplicación del Deep Learning cumpla un porcentaje de precisión aceptable al reconocer e identificar el rostro de las personas, incluyendo las restricciones que sean causados por mascarillas o lentes que reduce los rasgos faciales para un mejor reconocimiento.

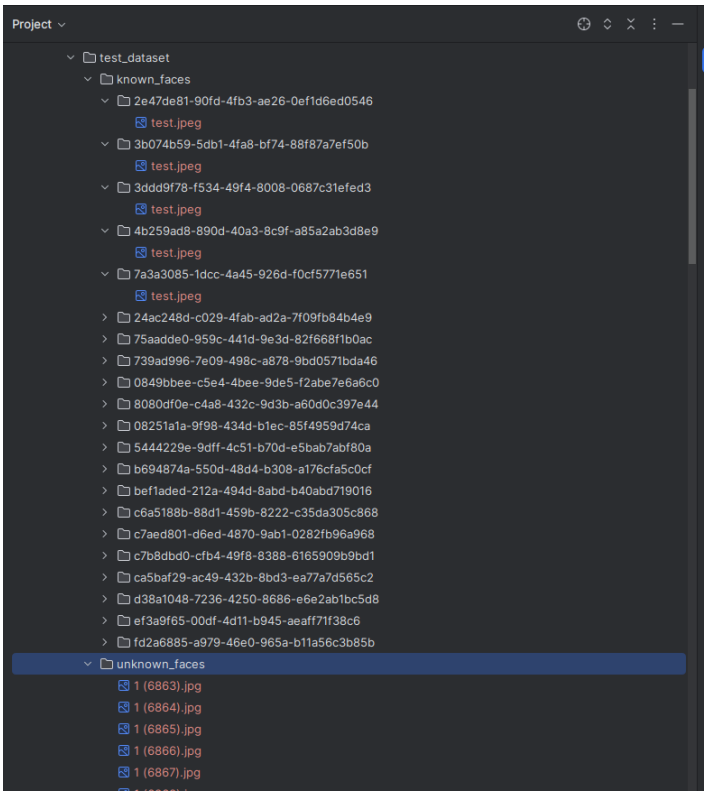
Figura 40

Pruebas conjunto testing



Nota. La figura muestra Pruebas conjunto testing en face recognition. *Fuente.* Elaboración propia (2024).

Figura 41
Pruebas conjunto testing2



Nota. La figura muestra Pruebas conjunto testing2 en face recognition. *Fuente*. Elaboración propia (2024).

Para el procesamiento y pruebas del sistema de reconocimiento facial, se utilizaron imágenes de rostros desconocidos provenientes de un conjunto de datos público. Las imágenes fueron obtenidas del siguiente dataset de Kaggle:

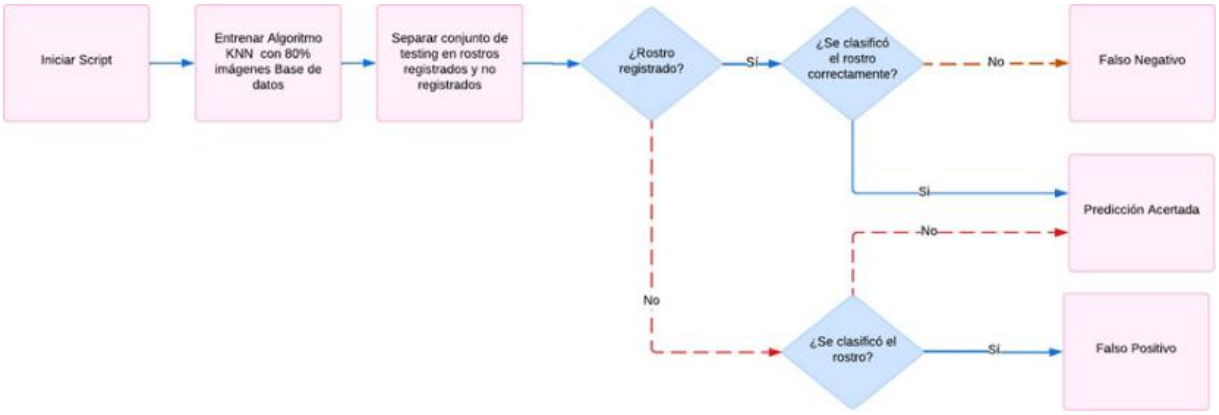
Fuente de Datos: https://www.kaggle.com/datasets/ashwingupta3012/human-faces

Licencia: CC0 (Dominio Público)

Este conjunto de datos contiene imágenes bajo una licencia CC0, lo que permite su uso libre para análisis y pruebas sin restricciones de derechos de autor.

Figura 42

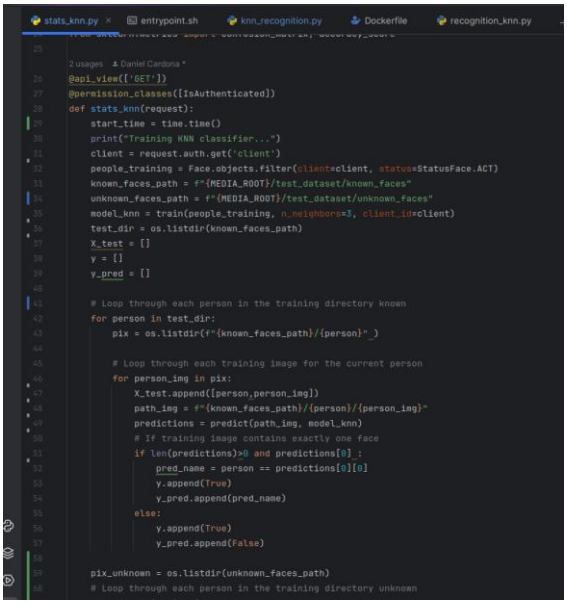
Diagrama de flujo de entrenamiento y testing



Nota. Diagrama de flujo de entrenamiento y testing (2024). *Fuente*. Elaboración propia (2024).

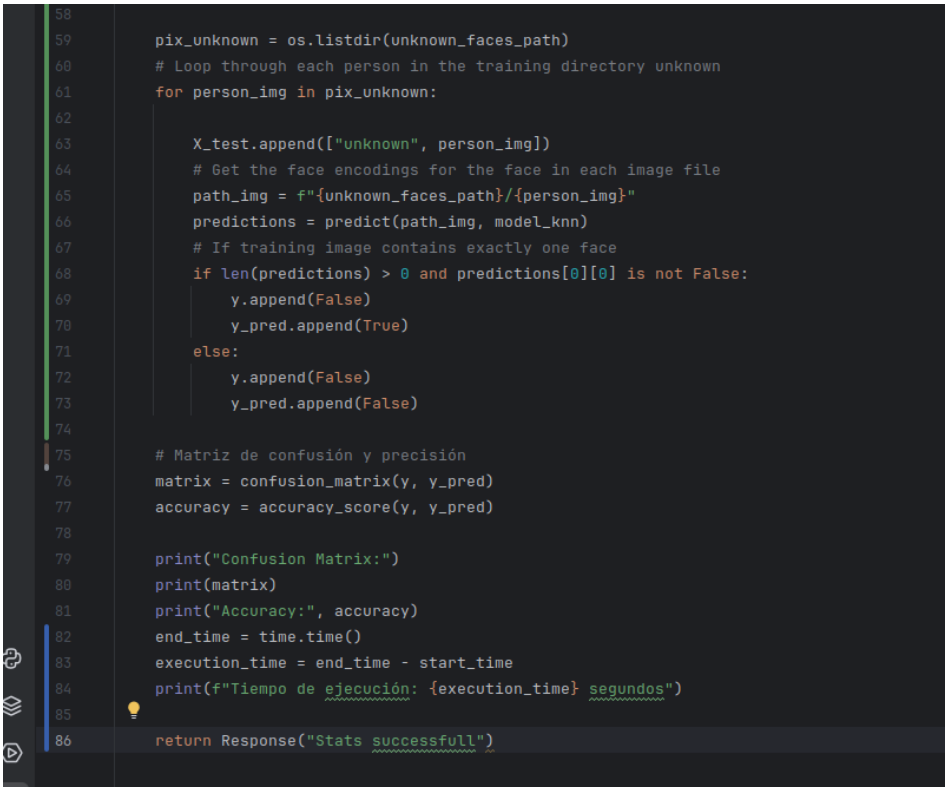
Figura 43

Fase de evaluación del algoritmo Python -2



```
stats_knn.py | entrypoint.sh | knn_recognition.py | Dockerfile | recognition_knn.py

2 usages  ▲ Daniel Cardona *
@api_view(['GET'])
@permission_classes([IsAuthenticated])
def stats_knn(request):
    start_time = time.time()
    print("Training KNN classifier...")
    client = request.auth.get('client')
    people_training = Face.objects.filter(client=client, status=StatusFace.ACT)
    known_faces_path = f"{MEDIA_ROOT}/test_dataset/known_faces"
    unknown_faces_path = f"{MEDIA_ROOT}/test_dataset/unknown_faces"
    model_knn = train(people_training, n_neighbors=3, client_id=client)
    test_dir = os.listdir(known_faces_path)
    X_test = []
    y = []
    y_pred = []

    # Loop through each person in the training directory known
    for person in test_dir:
        pix = os.listdir(f"{known_faces_path}/{person}")

        # Loop through each training image for the current person
        for person_img in pix:
            X_test.append([person,person_img])
            path_img = f"{known_faces_path}/{person}/{person_img}"
            predictions = predict(path_img, model_knn)
            # If training image contains exactly one face
            if len(predictions)>0 and predictions[0]:
                pred_name = person == predictions[0][0]
                y.append(True)
                y_pred.append(pred_name)
            else:
                y.append(True)
                y_pred.append(False)

    pix_unknown = os.listdir(unknown_faces_path)
    # Loop through each person in the training directory unknown
```

Nota. La figura muestra la fase de evaluación del algoritmo Python -2. *Fuente.* Elaboración propia (2024).



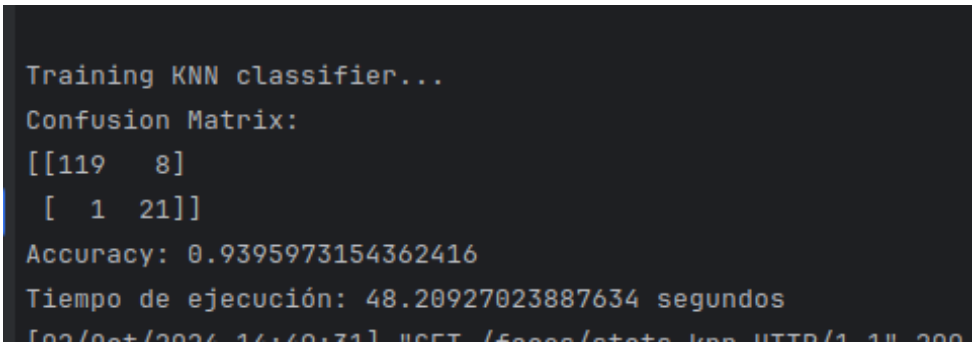
```
    pix_unknown = os.listdir(unknown_faces_path)
    # Loop through each person in the training directory unknown
    for person_img in pix_unknown:

        X_test.append(["unknown", person_img])
        # Get the face encodings for the face in each image file
        path_img = f"{unknown_faces_path}/{person_img}"
        predictions = predict(path_img, model_knn)
        # If training image contains exactly one face
        if len(predictions) > 0 and predictions[0][0] is not False:
            y.append(False)
            y_pred.append(True)
        else:
            y.append(False)
            y_pred.append(False)

    # Matriz de confusión y precisión
    matrix = confusion_matrix(y, y_pred)
    accuracy = accuracy_score(y, y_pred)

    print("Confusion Matrix:")
    print(matrix)
    print("Accuracy:", accuracy)
    end_time = time.time()
    execution_time = end_time - start_time
    print(f"Tiempo de ejecución: {execution_time} segundos")

    return Response("Stats successfull")
```

Nota. La figura muestra la fase de evaluación del algoritmo Python -2. Fuente: Elaboración propia (2024).

Resultados

Figura 44

Resultados Fase de evaluación del algoritmo Python -2



```
Training KNN classifier...
Confusion Matrix:
[[119   8]
 [  1  21]]
Accuracy: 0.9395973154362416
Tiempo de ejecución: 48.20927023887634 segundos
```

Nota. La figura muestra los Resultados fase de evaluación del algoritmo Python -2. *Fuente*. Elaboración propia (2024).

Tabla 15

Tabla de matriz de confusión del resultado de la evaluación del algoritmo

	Predicción Correcta	Predicción Incorrecta
Real True	21	1
Real False	119	8

Nota. La tabla muestra matriz de confusión del resultado de la evaluación del algoritmo (2024).

El Porcentaje de Éxito (accuracy): 93,95%

Teniendo en cuenta los resultados y datos anteriores se puedes analizar lo siguiente:

La matriz de confusión es una herramienta fundamental para evaluar el desempeño de modelos de clasificación, como el sistema de reconocimiento facial que estás evaluando. Por lo tanto, cada celda de la matriz representa una combinación de la clase real y la clase predicha por el modelo.

Verdaderos Positivos (VP): 21 casos en los que el modelo predijo correctamente que una persona era la que realmente era.

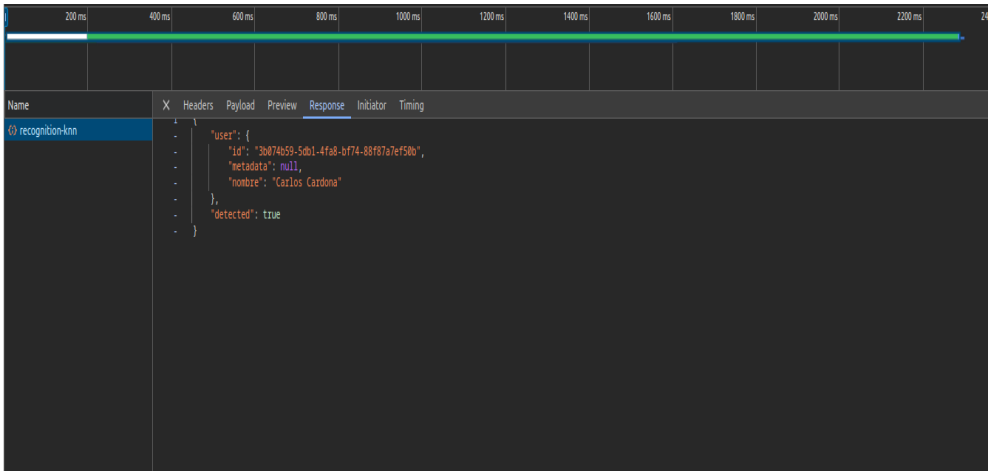
Falsos Positivos (FP): 1 casos en los que el modelo predijo erróneamente que una persona era la que realmente era, cuando no lo era.

Falsos Negativos (FN): 8 casos en los que el modelo predijo erróneamente que una persona no era la que realmente era, cuando sí lo era.

Verdaderos Negativos (VN): 119 casos en los que el modelo predijo correctamente que una persona no era la que realmente era.

Figura 45

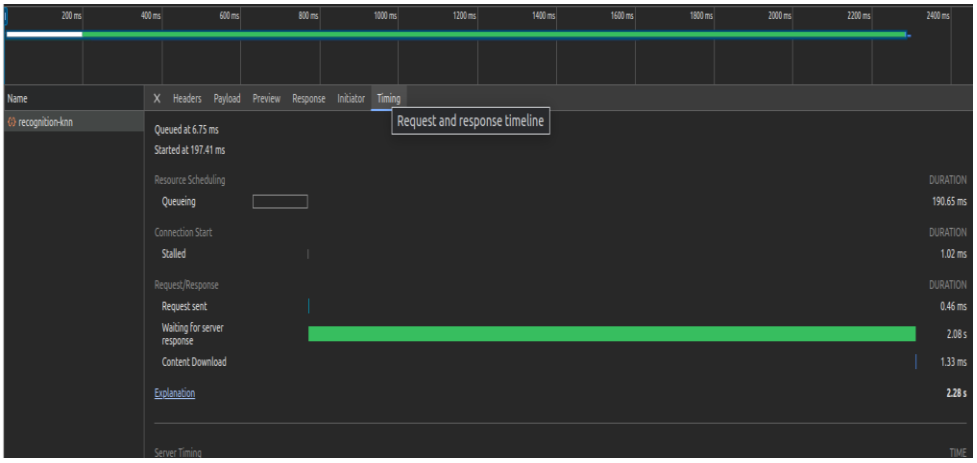
Evaluación de tiempo de respuesta del algoritmo para identificar un rostro



Nota. La figura muestra la Evaluación de tiempo de respuesta del algoritmo para identificar un rostro. Fuente: Elaboración propia (2024).

Figura 46

Evaluación de tiempo de respuesta del algoritmo para identificar un rostro



Nota. La figura muestra la Evaluación de tiempo de respuesta del algoritmo para identificar un rostro. Fuente: Elaboración propia (2024).

Resultado 2.08 Segundos

Un tiempo de respuesta de 2.08 segundos para el algoritmo de detección facial es adecuado en términos de rendimiento general, pero su eficiencia debe evaluarse dentro del contexto específico de la aplicación y del hardware utilizado. En este caso, el sistema fue implementado y probado en el servicio en la nube Railway, utilizando una máquina con recursos limitados:

Memoria: 4 GB

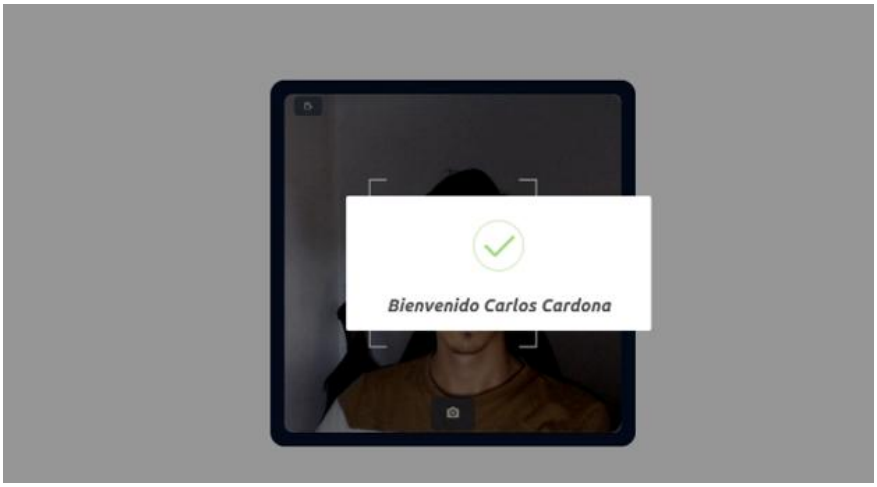
CPU: 4 vCPU

Estas especificaciones de hardware ofrecen un entorno adecuado para pruebas y aplicaciones de baja a moderada demanda, pero pueden no ser óptimas para aplicaciones en tiempo real o de alta concurrencia, donde se requieren tiempos de respuesta aún más bajos. Las limitaciones de recursos en Railway afectan el rendimiento del algoritmo, especialmente en tareas intensivas como la detección y el reconocimiento facial en imágenes de alta resolución o con múltiples rostros.

Evaluar el tiempo de respuesta en este contexto permite entender mejor el impacto de los recursos de hardware en el rendimiento del sistema y plantea la posibilidad de optimizar o escalar el hardware en función de los requerimientos específicos de la aplicación final.

Figura 47

Tiempo de respuesta



Nota. La figura muestra tiempo de respuesta del algoritmo para identificar un rostro. *Fuente.*

Elaboración propia (2024).

Conclusiones

El objetivo principal de este trabajo se basó en, desarrollar un sistema de control de acceso basado en reconocimiento facial utilizando React para la interfaz de usuario y Python para el backend, que permita una autenticación segura y eficiente en entornos basados en seguridad física donde se requiera control de acceso. Además, este proyecto ha permitido identificar las técnicas más adecuadas para abordar los desafíos inherentes a la detección de rostros en imágenes. Los resultados obtenidos demuestran la eficacia de la metodología propuesta, contribuyendo al avance en el campo del reconocimiento de patrones.

Por lo tanto, se puede concluir que:

En primer lugar, para el entrenamiento del modelo se aplicó el proceso típico de clasificación en máquinas de aprendizaje (machine learning) en identificación de una muestra de 21 personas voluntarias para el desarrollo del proyecto cada uno con 4 fotografías en diferentes escenarios teniendo un total de 84 fotografías. Asimismo, para la segunda muestra del entrenamiento del modelo, se registraron 79 imágenes de rostros diferentes de la base de datos Human faces.

En el reconocimiento facial se utilizó la librería Face recognition y para evaluar este modelo se utilizó la matriz de confusión con dos clasificaciones de personas conocidos y no conocidos, donde se le da una etiqueta a cada uno de estos, finalmente se obtuvo un 93,95% de éxito, evaluando el tiempo de respuesta del algoritmo para identificar un rostro teniendo como resultado 2.08 Segundos.

De acuerdo con el análisis con base en los resultados con la aplicación de la matriz de confusión, se concluyó que la elaboración del sistema de reconocimiento facial es exacto y preciso con un porcentaje del 93 % con el reconocimiento facial.

Los aportes de este proyecto se presentan mediante un método eficaz para la detección de rostros, utilizando la biblioteca OpenCV y face recognition, demostrando la viabilidad de la propuesta a través de una implementación práctica y una evaluación exhaustiva.

Los resultados obtenidos muestran que el sistema es capaz de detectar rostros con alta precisión y en tiempo real, lo que lo convierte en una herramienta valiosa para diversas aplicaciones. Sin embargo, es importante reconocer que el sistema aún puede ser mejorado en términos de robustez frente a variaciones en la iluminación, expresiones faciales y oclusiones. Futuras investigaciones podrían explorar la integración de técnicas de aprendizaje profundo para mejorar el rendimiento del sistema y ampliar su rango de aplicaciones.

Referencias Bibliográficas

Basel, A. (2023). *Faces Detection Using Haar Cascade*. https://medium.com/@baselanaya/faces-detection-using-haar-cascade-3e175aef84f5

Carrero, D., Ruíz, B., Puente, L., & Poza, M. J. (2010). *Prestaciones de la Normalización del Rostro en el Reconocimiento Facial.* Actas de Las V Jornadas de Reconocimiento Biométrico de Las Personas.

CEPAL (2024). *Sobre la protección de los datos*.https://biblioguias.cepal.org/c.php?g=495473&p=4398118#:~:text=La%20protecci%C3%B3n%20de%20datos%20se,y%20de%20corregir%20las%20inexactitudes.

Chihaoui, A. E. A *Survey of 2D Face Recognition Techniques*. Computers, vol. 5(No 4), Art. No 4. doi:doi: 10.3390/computers5040021.

Corporación de Radio y Televisión Española (RTVE) (2023). *Si estás en las redes, Clearview AI tiene tu cara*. https://www.rtve.es/noticias/20231107/clearview-posee-red-reconocimiento-facial-venden-datos/2456767.shtml

Domínguez Pavón, S. (2017). *Reconocimiento facial mediante el Análisis de Componentes Principales (PCA).* https://idus.us.es/handle/11441/66514

García del Prado, N., González Castro, V., Alegre Gutiérrez, E., & Fidalgo Fernández, E. (2017). *Comparación de métodos de detección de rostros en imágenes digitales.* Actas de las XXXVIII Jornadas de Automática.

Geitgey, A. (2020). The world's simplest facial recognition api for Python and the command line. URL: https://github. com/ageitgey/face recognition

Ghazal, R., Malik, A., Qadeer, N., Raza, B., Shahid, A., & Alquhayz, H. (2020). *Intelligent Role-Based Access Control Model and Framework Using Semantic Business Roles in Multi-Domain Environments.*

Gupta, R., Kanungo, P., Dagdee, N., Madhu, G., Sahoo, K., Jhanjhi, N. Z., . . . AlZain, M. (2023). *Secured and Privacy-Preserving MultiAuthority Access Control System for Cloud-Based Healthcare Data Sharing*. https://doi.org/10.3390/ s23052617

Hernández Sampieri R. (2010). *Metodología de la Investigación* 5 Ed: ISBN 978- 607-15-0291-9, p.700

Ibarra-Estévez, J., & Paredes, K. (2018). *Redes neuronales artificiales para el control de acceso basado en reconocimiento facial*. revistapuce.

Montoya S., J. A., y Restrepo R., Z. (2013). *Gestión de identidades y control de acceso desde una perspectiva organizacional.* Ingenierías USBMed, 3(1), 23–34. https://doi.org/10.21500/20275846.261

Morales Castro, C., Zozaya Salas, R. G., Torres Balcazar, A., Rojo López, A., Paz Cruz, M., Velázquez Montes, O., & Soto Morales, C. M. (2022). *Prototipo de un Sistema Biométrico para Control de Acceso.* Congreso Internacional de Investigacion Academia Journals, 14(9), 1549–1553.

Moreano, J. A. C., Pulloquinga, R. H. M., Lagla, G. A. F., Chisag, J. C. C., & Pico, O. A. G. (2017). *Reconocimiento facial con base en imágenes.* Revista Boletín Redipe, 6(5), 143-151.

Muñiz, A. G. (2018). *Aplicaciones de técnicas de inteligencia artificial basadas en aprendizaje profundo (deep learning) al análisis y mejora de la eficiencia de procesos industriales*. *Universidad de Oviedo*.

Pacheco, J., Chavez, J., & De Los Santos, A. M. (2023). *Control de accesos en seguridad de la información: Una revisión sistemática de las técnicas actuales.* Revista Campus, 28(36), 163–176. https://doi-org.bibliotecavirtual.unad.edu.co/10.24265/campus.2023.v28n36.01

Pérez León, E. V., & Rojas Arévalo, D. I. (2019). *Impacto de la inteligencia artificial en las empresas con un enfoque global*. Lima-Peru: UPCC.

Pérez y Madrid, A. (2021). *El reconocimiento facial es un superpoder. Cómo te afectará y por qué deberías conocerlo.* Dykinson. https://e-archivo.uc3m.es/rest/api/core/bitstreams/72be4448-72cf-4638-a6bc-cd3c5541c7f8/content

Russell, J. (1994). *Is there universal recognition of emotion from facial expression?Areviewof cross-culturalstudies.Psychological bulletin*, 115, 102–141.

Salazar Carvajal, C. B., & Orozco Alzate, S. (2016). *Diseño de un sistema biométrico de reconocimiento facial en tiempo real.* https://repositorio.utp.edu.co/items/0cb9db3d-6fc2-4078-a987-7038a8730cad

Zapatero Olmedillo, D. (2016). *Herramienta de reconocimiento facial de emociones en Android.* https://oa.upm.es/44722/