Diseño de una alarma con inteligencia artificial para fortalecer la seguridad de los hogares estrato 2 y 3 de Bogotá

Daniel Steven Garcia Triana

Programa de Ingeniería de Software, Fundación Universitaria Compensar

Proyecto fin de grado

Oscar Andrés Acosta Villamil

2023

Esta obra está bajo una Licencia Creative Commons Atribución-NoComercial-CompartirIgual 4.0 Internacional.

Tabla de contenido

Resumen 8

Abstract 9

Introducción 10

Formulación del problema 11

Planteamiento del problema 12

Objetivos 14

Objetivó general 14

Objetivos específicos 14

Justificación 15

Estado del arte 17

Antecedentes 23

Análisis de contexto del proyecto y de la entidades y comunidades beneficiarias 27

Marco teórico 28

Inteligencia artificial 28

Inteligencia 28

Redes Neuronales Artificiales. 29

Deep Learning 30

Capa de Convolución 30

Marco Conceptual 32
Algoritmo 32
Base de datos 32
Controlador 32
Microcontroladores 33
Bot 33
Arduino IDE 34
Open Cv 34
EigenFace 34
FisherFace 35
LBPH 35
Metodología 36
Tipo de investigación 36
Fuentes de información para el estudio 36
Población y muestra 37
Cronograma de actividades 38
Análisis de entradas principales de las casas estrato 2 de Bogotá 39
Requerimientos del controlador 44
Controladores 45
Esp32 CAM 45

Raspberry pi 4 Modelo B 47

Selección de controlador 48

Presupuesto 49

Etapa 1: Creación de la base de datos 50

Etapa 2: Preparación de los datos 51

Etapa 3: Entrenamiento 52

Etapa 4: Test de los modelos de reconocimiento facial 55

Etapa 5: Reentrenamiento y Test de los modelos de reconocimiento facial 61

Resultados 64

Escenario de prueba 64

Diseño de la alarma 67

Esquema 67

Bot de Telegram 68

Arquitectura propuesta 70

Diagrama caso de uso 71

Diseño físico propuesto 72

Discusión 74

Referencias 76

Anexos 84

Tabla de tablas

Tabla 1 17

Tabla 2 18

Tabla 3 19

Tabla 4 20

Tabla 5 21

Tabla 6 22

Tabla 7 38

Tabla 8 44

Tabla 9 44

Tabla 10 49

Tabla 11 57

Tabla 12 59

Tabla 13 60

Tabla 14 62

Tabla 15 62

Tabla 16 63

Tabla 17 65

Tabla 18 66

Tabla de figuras

Figura 1 29

Figura 2 31

Figura 3 39

Figura 4 40

Figura 5 41

Figura 6 42

Figura 7 43

Figura 8 46

Figura 9 47

Figura 10 48

Figura 11 50

Figura 12 51

Figura 13 52

Figura 14 53

Figura 15 54

Figura 16 55

Figura 17 56

Figura 18 58

Figura 19 60

Figura 20 61

Figura 21 64

Figura 22 65

Figura 23 67

Figura 24..... 68

Figura 25..... 70

Figura 26..... 71

Figura 27..... 72

Figura 28..... 73

Figura 29..... 84

Figura 30..... 85

Resumen

En este documento se presenta información sobre el robo de viviendas como una problemática que afecta a los ciudadanos de Bogotá, y el cómo la seguridad privada y la inteligencia artificial se han ido complementando para hacer frente al hurto en hogares, haciendo énfasis en los beneficios y en las falencias que presentan hoy en día. Esta investigación plantea una solución basada en el diseño de una alarma con inteligencia artificial, que está enfocada al reconocimiento facial, que permite la identificación de personas en tiempo real y que generará reportes a través de mensajes en el celular, con esto se busca brindar una alternativa más ecónoma, pero igualmente precisa que permitirá fortalecer la seguridad en las residencias de Bogotá. En este proyecto se probaron 3 modelos de inteligencia artificial para el reconocimiento de imágenes, basados en “redes neuronales convolucionales”, estos fueron: EigenFaces, FisherFace y LBPH. En el documento se exponen y se sustentan los resultados obtenidos por parte de los métodos de inteligencia artificial, en los cuales se obtuvieron resultados satisfactorios para la realización del diseño que tendrá la alarma, finalmente se presentan las conclusiones basadas en los objetivos formulados.

Palabras clave: inteligencia artificial, redes neuronales convolucionales, reconocimiento facial, seguridad privada, hurto a viviendas.

Abstract

This document presents information on home burglary as a problem that affects the citizens of Bogotá, and how private security and artificial intelligence have complemented each other to deal with home theft, emphasizing the benefits and shortcomings that they present today. This research proposes a solution based on the design of an alarm with artificial intelligence, which is focused on facial recognition, which allows the identification of people in real time and which will generate reports through messages on the cell phone, this seeks to provide a cheaper alternative, but equally accurate to strengthen security in residences in Bogotá. In this project, 3 artificial intelligence models for image recognition were tested, based on "convolutional neural networks", these were: EigenFaces, FisherFace and LBPH. In the document the results obtained by the artificial intelligence methods are exposed and supported, in which satisfactory results will be obtained for the realization of the design that the alarm will have, finally the conclusions are presented based on the formulated objectives.

Keywords: artificial intelligence, convolutional neural networks, facial recognition, private security, home burglary.

Introducción

La contratación de servicios de seguridad privada ha ido en aumento y es que según la Superintendencia de Vigilancia y Seguridad Privada de Colombia en su informe indicadores financieros (2021) desde los últimos tres años se reportó un incremento en los ingresos operacionales de este sector correspondiente a 3’171.595 pesos colombianos, esto solo en empresas de vigilancia y seguridad privada, paralelamente una encuesta de Percepción y Victimización de Bogotá (2022) realizada por la cámara de comercio de esta ciudad, arrojo que Colombia hoy día enfrenta una de las tasas más altas de delincuencia, donde la modalidad de hurto a viviendas presenta un incremento progresivo.

En el desarrollo de este documento de investigación se abordaron diferentes estudios dirigidos al uso de inteligencia artificial con reconocimiento facial como herramienta para la mitigación de robos a viviendas. Luego de ello se realiza un análisis de la estructura de las casas estrato 2 y 3 de la ciudad de Bogotá, asiendo principal enfoque en la entrada de la vivienda, con el objetivo de diseñar un dispositivo con reconocimiento facial que pueda identificar cada persona que entra en el recinto, informando si es una persona no identificada o si es reconocida por los habitantes, esto se logra al haber desarrollado y probado tres algoritmos que permiten el reconocimiento facial haciendo uso de redes neuronales convolucionales, también se tuvo en consideración la calidad de imagen que proporciona el dispositivo ESP-32 y la distancia máxima permitida para la toma de imágenes.

Formulación del problema

¿Cómo fortalecer la seguridad de los hogares bogotanos a través de una alarma que haga uso de inteligencia artificial para el reconocimiento facial de personas, para que permita reducir los índices de robo a viviendas en la ciudad?

Planteamiento del problema

Según la OEA los grupos delictivos corresponden a un conjunto de 3 o más personas que se ponen de acuerdo con el fin de cometer uno o más delitos con el propósito de obtener un beneficio, generalmente económico (OEA, 2009). En la mayoría de los casos se suele asociar a los grupos delictivos con el trágico de estupefacientes, sin embargo, poco se habla de aquellos grupos organizados que se dedican al robo de viviendas, y es que según un reporte por parte del Canal 1 (2021) en la mitad del año 2021 en Colombia se registraron 13.109 hurtos a viviendas, lo que quiere decir que diariamente se cometían 81 asaltos a hogares.

Con base en la encuesta de Percepción y Victimización de Bogotá (2022) realizada por la cámara de comercio de esta ciudad, se puede decir que la capital de Colombia hoy día enfrenta una de las tasas más altas de delincuencia, aunque es cierto que ha disminuido respecto al 2020 aún sigue siendo superior a la tasa del 2019. Por otro lado, tenemos que, el principal delito es la modalidad de hurto a personas seguido por el hurto a viviendas, pero cabe aclarar que este último ha ido en aumento y aunque el hurto a personas sigue siendo el principal delito esta ha ido decayendo.

Según información recopilada por la Corporación Excelencia en la Justicia (CEJ) para el año 2022 con corte al 30 de junio se habían registrado más de 14.000 hurtos a viviendas, con un promedio de 80 casos diarios (CEJ, 2022), donde tenemos que el 41% fueron realizados bajo la modalidad del “factor oportunidad”, modalidad que consiste en aprovecharse de descuidos de los ciudadanos ya sea dejar una puerta o ventanas abiertas Mientras que un 32% se atribuye al forcejeo de cerraduras o el uso de llaves clonadas y un 17% se atribuyen a otros métodos. (infobae, 2023), esto da a entender que principalmente los delincuentes acceden a las viviendas

por la entrada principal ya sea por un descuido de algún habitante de la residencia o por el uso de técnicas y/o herramientas que les permiten vulnerar la cerradura.

Una de las tácticas que usan estos grupos “consiste en dibujar en alguna parte, no muy visible, de la casa determinadas marcas específicas que indican varias situaciones sobre esta; tales como que sus habitantes se encuentran de vacaciones, que esa casa ya ha sido atracada o que es perfecta para llevar a cabo el atraco.”(Metrocuadrado, 2021); Una vez identificada la casa en la cual se va a cometer el delito los delincuentes usan una técnica llamada Bumpíng, la cual consiste en abrir la cerradura sin la llave del propietario y sin la necesidad de forzar la cerradura.

Objetivos

Objetivó general

Diseñar una alarma que haga uso de reconocimiento facial para la identificación de personas, y con base en ello envié notificaciones por medio de un bot de Telegram, usando tecnología de código abierto. Para mejorar la seguridad en los hogares Bogotanos.

Objetivos específicos

- Determinar los requerimientos del sistema basado en las condiciones de acceso a las viviendas estrato 2 y 3 de la ciudad Bogotá, y con base en ello, elegir el controlador (placa de desarrollo) que se utiliza en la alarma.
- Evaluar tres inteligencias artificiales de reconocimiento facial (EigenFace, FisherFace y LBPH) de la librería OpenCV, mediante pruebas de simulación de escenarios, donde se medirá el índice de precisión y la confiabilidad de los datos.
- Sintetizar en un diseño la integración de la inteligencia artificial junto con el modelo de la alarma, que permita el reconocimiento de personas y él envió de notificaciones por medio de un bot de Telegram.

Justificación

El columnista Jordi Sabate del medio informativo consumoClaro (Sabaté, 2015) en un reportaje cuenta su experiencia con el uso de un sistema de alarmas que implemento es su hogar, el relata que en un principio estas alarmas domesticas funcionaban bastante bien, pues era un medio de disuasión para las personas malintencionadas, le brindaba una sensación de seguridad mientras no estaba en casa y la respuesta era rápida, sin embargo, el cabo de un tiempo comenzó a experimentar fallos en el sistema, pues encontró que la alarma se disparaba sin motivo aparente, las personas encargadas de alertar a las autoridades se demoraban en contactar con el propietario y con la policía. Después de consultar con otras personas que hacían uso de sistemas de alarmas, conoció más historias como la suya encontrando que en ocasiones la central de policía se llegaba a saturar motivo de las falsas alarmas. En conclusión, el determinó que contar con sistemas de seguridad domestico era importante, sin embargo, había cosas que mejorar y optimizar.

Teniendo en cuanta los índices de hurto en las residencias de la ciudad de Bogotá y los problemas en los sistemas de alarmas hogareños, se desea diseñar un sistema de seguridad que hace uso inteligencia artificial con reconocimiento facial con el fin de identificar delincuentes que han venido afectando a la población en general, para dicho sistema se cuenta con:

- Una inteligencia artificial enfocada en el reconocimiento facial que hace uso de redes neuronales convolucionales, las cuales permiten encontrar patrones en las imágenes para luego clasificarlos.
- Esp 32-Cam, es un dispositivo que cuenta con una cámara y conectividad Wifi, cabe resaltar que es económico y fácil de programar, por tanto, reduce los costos finales de la alarma. (Álvarez, 2022)

- Sensor de movimiento PIR, que mediante una lente de Fresnel ofrece un alcance de detección de movimiento de 6 metros de distancia. (Gonzáles, 2017)

Este proyecto busca mejorar la detección de intrusos, pues la IA se encargará de determinar el tipo de amenaza y avisará al propietario, quien determinará la acción a seguir, ya sea llamar a la autoridad o no, según el escenario que se presente, sin embargo, quedará evidencia del intruso a través de las fotografías que el dispositivo tome.

Estado del arte

Para la elaboración del estado del arte se decidió trabajar por medio de fichas que contendrían información relevante de otros trabajos de investigación relacionados con el uso de inteligencia artificial dentro de sistemas de seguridad privada, la cuales se presentan a continuación:

Tabla 1

Ficha 1 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
1	Servicios de video vigilancia hogareño con soporte de inteligencia artificial	Britti, Gonzalo	1/7/2021	Argentina	Universidad de San Andrés. Escuela de Negocios	http://hdl.handle.net/10908/18682

Resumen	Conclusión
Este artículo explora la posibilidad de transformar los servicios de seguridad privada con una gran fuerza laboral especializada en sistemas alimentados por tecnología de inteligencia artificial. En particular, se intenta trabajar la seguridad en las casas. Para ellos, la propuesta de valor de un servicio de video vigilancia con un componente de análisis de video estaría dirigida a automatizar tareas que tradicionalmente son realizadas por humanos. (Britti, Gonzalo, 2021).	Durante el desarrollo de este trabajo se planteó y estudió un modelo de negocio de video vigilancia domiciliaria basado en innovaciones tecnológicas. Se discute acerca de las capacidades técnicas, es decir, si con los avances técnicos y tecnológicos actuales es posible desarrollar un producto o servicio con estas capacidades requeridas para realizar las operaciones requeridas. Finalmente se puede constatar es que no solo existe la tecnología, sino que se han desarrollado las capacidades necesarias para posibilitar una aplicación como la propuesta en el artículo. (Britti, Gonzalo, 2021).

Tabla 2

Ficha 2 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
2	Desarrollo de un prototipo de Sistema de Domótica enfocado en la seguridad de una vivienda mediante una aplicación de Inteligencia Artificial en visión por computadora, en la ciudad de Guayaquil	Carrillo Delgado, Ronnie Eduardo Arias Maldonado, Jose Elías	1/9/2022	Guayaquil, Ecuador	Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales	http://repositorio.ug.edu.ec/handle/redug/65267

Resumen	Conclusión
El trabajo presenta un prototipo que permite monitorear y administrar apartamentos, centrados en la seguridad de la ciudad de Guayaquil, el principal problema es el factor criminal y la forma en que se desarrolla constantemente, lo que lleva a una gran cantidad de discusiones. Las razones pueden ser la falta de trabajo, las consecuencias de la pandemia Covid-19, entre otros, debido a este problema de investigación se plantea como objetivo mitigar este problema en la ciudad de Guayaquil mediante el desarrollo de un prototipo de sistema domótico que se enfoque en la seguridad del hogar mediante el uso de inteligencia artificial en visión por computadora y evaluación en el mismo nivel. (Eduardo, Elías, 2022)	Se presentó una propuesta adecuada con sus capacidades, apoyada en métodos, utilizada para generar una solución mediante prototipado que mejora las versiones anteriores. Se han obtenido resultados favorables más allá de un prototipo funcional que cubre las necesidades detectando armas e intrusos, mientras que los usuarios reciben alertas de peligro vía WhatsApp, reduciendo la probabilidad de ser hackeados. (Eduardo, Elías, 2022)

Tabla 3

Ficha 3 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
3	Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo	Ruano Ruano, Ildefonso	8/3/2022	España	Universidad de Jaén. Ingeniería de Telecomunicación	https://hdl.handle.net/10953.1/16437

Resumen	Conclusión
El proyecto ha desarrollado un sistema de seguridad de Internet de las Cosas (IoT) basado en Raspberry Pi y ha creado un prototipo funcional. Para implementar este sistema de seguridad se realizó un estudio preliminar de los medios de comunicación, tecnología y equipos necesarios para su funcionamiento. Además, se ha implementado un bot de Telegram para que los usuarios controlen de forma remota el sistema de seguridad. El sistema de seguridad incluye sensores y actuadores de todo tipo. Entre los sensores se encuentran un sensor de presencia infrarrojo pasivo y una cámara, y los accionamientos son una cerradura automática, botones, luces y parlantes. Además, la inteligencia artificial (IA) se implementa utilizando la cámara de entrada, lo que ayuda en el reconocimiento facial basado en la imagen capturada por una de las cámaras. (Eduardo, 2022)	El hecho de que el prototipo de seguridad esté programado íntegramente en Python demuestra la potencia y facilidad que caracteriza al lenguaje. Bibliotecas potentes como OpenCV, que se utiliza para proyectos de visión artificial, o scikit-learning, que se utiliza para el aprendizaje automático en el campo de la inteligencia artificial, se pueden implementar fácilmente en Python. Esta facilidad de uso proviene en parte de las comunidades activas detrás del idioma y muchas de estas librerías, lo que hace que recuperar información sea más rápido y eficiente. (Eduardo, 2022)

Tabla 4

Ficha 4 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
4	Reconocimiento y creación del modelo facial 3D mediante sistema de video aplicado a la seguridad usando inteligencia artificial.	Caba costales, Carlos Santiago Jara Chávez, Caroline Viviana	1/3/2018	Riobamba, Ecuador	Escuela Superior Politécnica de Chimborazo	http://dspace.espoch.edu.ec/handle/123456789/9198

Resumen	Conclusión
En este trabajo se desarrolló e implemento un sistema que reconoce y genera modelos tridimensionales de rostros que simulan cualquier tipo de entrada a un lugar en particular. El sistema consta de dos fases: la fase de registro de usuarios y la fase principal de ejecución del programa, en la que se reconoce y genera el modelo. Se utiliza un método de detección general basado en modelos faciales. Para verificar los datos de entrada, se utiliza un método de inteligencia artificial: lógica difusa, con un controlador difuso del tipo Mamdani y con un reductor central; esto se utiliza para verificar la similitud entre el usuario activo y la información almacenada en la base de datos. El filtro Gabor se utiliza para generar vectores específicos del usuario y la distancia euclidiana se utiliza para la comparación. Para mayor precisión, al momento de reconocer a una persona, se utilizan varias imágenes como entrada, tales como: una imagen general de la cara, ojos, boca, nariz, tanto de frente como de perfil. (Santiago, Viviana 2018)	Se implementó un sistema de reconocimiento para seguridad usando algoritmos de reconocimiento EBGM y 3DMM para modelado de rostros; Con la ayuda de algoritmos de inteligencia artificial, se permite el acceso sin posibilidad de errores de identificación, ya que en muchos casos las características de una persona suelen ser similares a las de otras, pero no debe ser en todo su rostro. (Santiago, Viviana 2018)

Tabla 5

Ficha 5 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
5	Diseño de un sistema de control domótico y video vigilancia supervisado por un teléfono móvil	Guerra Ruiz, Felipe	1/6/2014	Lima, Perú	Pontificia universidad católica del Perú	http://hdl.handle.net/20.500.12404/5375

Resumen	Conclusión
En este trabajo de investigación se segmento en diferentes capítulos en el primer capítulo se examina el problema que aborda el proyecto, el cual es la inseguridad ciudadana. En el segundo capítulo se proporciona una breve descripción de las tecnologías utilizadas en el desarrollo del sistema. En el tercer capítulo se formula los objetivos de diseño y proporciona enfoques iniciales para el sistema diseñado. En el cuarto capítulo se describe cada componente y fase de diseño de un sistema de domótica y videovigilancia, desglosado en segmentos. Finalmente, en el quinto capítulo se evalúa los costos del sistema para demostrar si el sistema puede tener cabida como solución al problema de delincuencia de nuestro país. (Felipe, 2014)	El diseño de sistema basado en el trabajo puede desplegarse en el ámbito de una red de área local debido a que tiene requerimientos de ancho de banda muy bajos y no requiere servidores con alta potencia de cómputo o instalación de múltiples elementos complejos. Lo que lo hace viable para su implementación en hogares de no muy altos recursos. (Felipe, 2014)

Tabla 6

Ficha 6 del estado del arte

Ficha	Título	Autor(es)	Año de publicación	Ciudad, País	Editor	Enlace
6	Implementación de una red neuronal de convolución para el reconocimiento de poses en imágenes de rostros	Paul Méndez, Julio Ibarra	19/12/2014	Quito, Ecuador	ACI Avances en ciencias e ingenierías	https://doi.org/10.18272/aci.v6i2.167

Resumen	Conclusión
Este artículo de investigación estudia el uso de redes neuronales convolucionales para el reconocimiento de imágenes de posiciones faciales horizontales no planas. Se propone una implementación basada en la biblioteca de código abierto OpenCV para clasificar imágenes de rostros humanos según 7 poses predefinidas, se detalla la arquitectura de red y la estrategia de aprendizaje. (Julio. 2014)	La arquitectura final de la red neuronal consta de seis capas: una capa de entrada, tres capas convolucionales, una capa de submuestreo y una capa de salida tradicional totalmente conectada con activación sigmoidal. (Julio. 2014)

Antecedentes

Dentro de la bibliografía que se ha consultado para el desarrollo del proyecto, se ha encontrado diferentes documentos tanto tesis como investigaciones referentes a el uso de la inteligencia artificial como mecanismo de mejora en sistemas de seguridad, alarmas y el uso de las técnicas de inteligencia artificial.

- "Face Detection and Recognition System for Enhancing Security Measures Using Artificial Intelligence System" Este artículo señala la importancia del uso del reconocimiento facial en la mejora de los sistemas de seguridad a través de las diferentes capacidades que la inteligencia artificial brinda. (Engr et al., 2020)

- "Face Detection in Security Monitoring Based on Artificial Intelligence Video Retrieval Technology". Esta publicación señala la importancia de la inteligencia artificial en los sistemas de procesamiento de video y la facilidad que brindan estos algoritmos al momento de realizar procesos de reconocimiento facial. (Zuolin et al., 2020).

- "AI-empowered IoT Security for Smart Cities". Este artículo señala la importancia de la implementación de Inteligencia Artificial en los sistemas de IOT debido a las posibles fallas de seguridad que estos pueden presentar y así reducir las amenazas que pueden afectar el correcto funcionamiento de estos. (Zhihan et al., 2021).

- "Alarmas inteligentes en unidades de cuidados intensivos basadas en redes neuronales" donde el propósito es a través de la inteligencia artificial implementar

alarmas en el sector médico y así prevenir diferentes tipos de accidentes clínicos. (Jorge, 1999).

- “Fire alarm systems construction on artificial intelligence principles”, en este artículo encontramos una implementación de inteligencia artificial para un sistema de alarmas contra incendios. (Andreev et al., 2022).
- “Investigación aplicada al área de inteligencia artificial y desarrollo de un sistema experto”, es una investigación donde se desarrolla un sistema experto con la aplicación de algoritmos de inteligencia artificial en El Salvador. (Rudy et al., 2004)
- “Facial recognition technology and the growing power of artificial intelligence”. Artículo donde se muestra la forma en que los sistemas de reconocimiento facial e inteligencia artificial han surgido exponencialmente y lo impactante que han sido en la cotidianidad. (Chair, 2022)
- “Artificial intelligence in security: opportunities and implications”, este articulo cuenta la forma en que tecnologías como la inteligencia artifician se han adoptado en la actualidad llegando a ser muy importantes en escenarios como la seguridad. (Michael et al., 2021)
- “Sistema de reconocimiento facial con visión artificial para apoyar al ecu-911 con la identificación de personas en la lista de los más buscados”. Este proyecto de investigación se basa en la creación de un prototipo donde, con ayuda de los algoritmos de inteligencia artificial y reconocimiento facial, se facilite la

localización de personas identificadas como delincuentes en Ecuador y de esta forma mejorar los índices de seguridad. (Alex, 2017)

- "Planteamiento de un algoritmo para la identificación de posibles delincuentes mediante reconocimiento facial en la ciudad de Bogotá". En esta tesis de la Universidad Distrital se plantea el uso del reconocimiento facial y algoritmos de inteligencia artificial como herramienta para solucionar diferentes casos de delincuencia común en la ciudad de Bogotá y planteamientos a nivel de la infraestructura para la aplicación de esta. (Oscar, 2020)

- "Inteligencia artificial para gestión y atención de alarmas", donde se plantea la integración de un mecanismo de inteligencia artificial con el objetivo de gestionar distintas alarmas digitales en una planta petrolera y así prevenir diferentes riesgos en esta área. (Padilla, 2022)

- "Aplicación de inteligencia artificial como estrategia para la disminución del nivel de riesgo en seguridad residencial en el sector de Bocagrande (Cartagena de indias)". Esta tesis señala la importancia de estar a la vanguardia a nivel de tecnología potenciando la seguridad que pueden ofrecer las empresas de vigilancia al implementar algoritmos de inteligencia artificial, reconocimiento facial y biométrico. (Hugo, 2019)

- "Desarrollo de un prototipo de herramienta en entorno web que implemente técnicas de inteligencia artificial con fin de analizar tendencias de inseguridad", es un proyecto que a partir del uso de inteligencia artificial y redes neuronales busca

identificar y categorizar las actividades delictivas en Bucaramanga y así poder mejorar los esquemas de seguridad en el sector. (Cristhian, 2020)

- “Sistemas de seguridad basados en biometría”. Este artículo señala la importancia y utilidad que tienen los diferentes sistemas biométricos, reconocimiento facial y de voz en la seguridad y señala algunas características importantes a tener en cuenta cuando se implementan estos sistemas. (Cortés et al, 2010)

Análisis de contexto del proyecto y de la entidades y comunidades beneficiarias

Se determinó que, para la elaboración del diseño de la alarma y de la selección de la inteligencia artificial que más se ajuste a los requisitos y objetivos del proyecto, los alcances y limitaciones de la investigación, se deben ajustar teniendo como grupo objetivo del estudio las viviendas de estrato 2 de la ciudad de Bogotá.

Por tal motivo se toma como referencia el estudio de indicadores financieros de la Superintendencia de Vigilancia y Seguridad Privada de Colombia (2021) así como la encuesta de Percepción y Victimización de Bogotá (2022) realizada por la cámara de comercio de esta ciudad con relación a los factores sugeridos para determinar el problema como los son: percepción de seguridad, número de denuncias, incremento de hurtos a hogares e incremento en la seguridad privada.

Bogotá se cataloga como un enlace para identificar a las partes interesadas o involucradas, en este caso los dueños o habitantes de hogares estrato 2 y 3, y las empresas de seguridad privada, quitándole a la ciudad el foco principal del estudio, teniendo en cuenta siempre el propósito de la alarma el cual es fortalecer la seguridad de los hogares bogotanos estrato 2 y 3.

Marco teórico

Inteligencia artificial

Para poder definir lo que es la inteligencia artificial hay que comprender en primer lugar que es la inteligencia:

Inteligencia

Desde los antiguos filósofos griegos se ha entendido la inteligencia como la capacidad de: razonamiento, adaptarse a su entorno y la solución de problemas (Ardila, 2011), sin embargo, Margaret Ann Boden (profesora de investigación cognitiva en el departamento de informática de la Universidad de Sussex) en su libro "Inteligencia Artificial" declara que: "La inteligencia no es una dimensión única, sino un espacio profusamente estructurado de capacidades diversas para procesar la información"(Boden, 2017), dándonos a entender que la inteligencia también comprende las competencias psicológicas como lo son: la abstracción, el análisis, la síntesis, la coordinación motora, entre otras.

La inteligencia y la inteligencia artificial se pueden definir de la misma manera, pero esta última es aplicada a las máquinas, de tal forma que si tenemos un dispositivo inteligente sabremos que bajo un conocimiento previamente establecido este es capaz de abstraer, analizar y sintetizar la información y con base a ello tratar de dar una solución a un determinado problema. Dicho de otra manera, por Marvin Minsky: "La inteligencia Artificial es la ciencia de construir máquinas para que hagan cosas que, si las hicieran los humanos, requerirían inteligencia" (F. Escolano, 2003).

Redes Neuronales Artificiales.

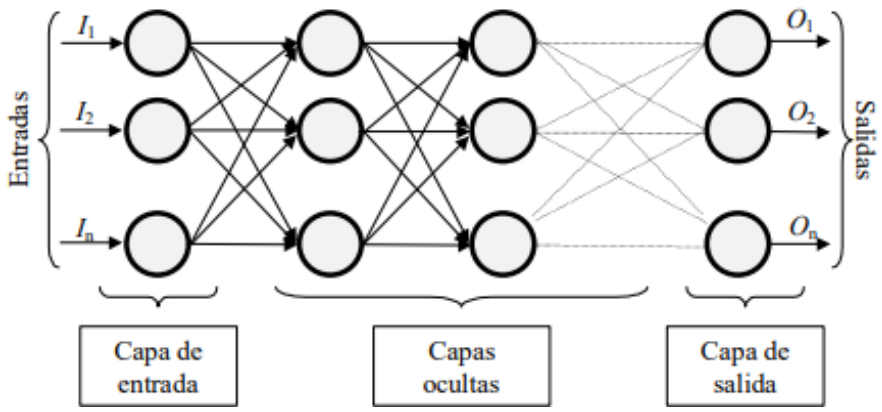
Una de las ramas más destacadas del campo científico de la Inteligencia Artificial corresponde a las Redes Neuronales Artificiales (RNAs) las cuales tratan de emular el comportamiento del cerebro humano, caracterizándose por el aprendizaje a través de la experiencia y la extracción de conocimiento genérico a partir de un conjunto de datos.(López & Fernández, 2008)

Las RNAs están diseñadas de tal manera que se asemejan lo más posible a una red neuronal humana, por tal motivo también se diseñaron un conjunto de unidades que se parecen a las neuronas biológicas, su función es realizar cálculos sencillos con datos proporcionados del mundo exterior o provenientes de otras neuronas, proporcionando así una salida única. Estas neuronas están distribuidas en tres capas:

- De entrada: donde se ingresa la información originaria del mundo exterior.
- Ocultas: se encargan de procesar la información.
- De salida: genera una respuesta.

Figura 1

Red neuronal artificial



Nota: ejemplo de una red neuronal artificial, fuente: (Ruiz et al., s. f.)

La figura 1 muestra un ejemplo de una RNA donde los círculos vendrían a ser las neuronas y las flechas representan las conexiones, así como el flujo de la información. Los datos ingresan por medio de la "capa de entrada", pasan a través de la "capa oculta" y salen por la "capa de salida". Cabe mencionar que la capa oculta puede estar constituida por varias capas.(Ruiz et al., s. f.)

Deep Learning

En español más conocido como aprendizaje profundo (AP) el Deep Learning es un conjunto de métodos para el entrenamiento de las redes neuronales artificiales, cabe aclarar que las RNAs comunes se componen de una o más capas ocultas, por otro lado, el AP hace referencia a que las RNAs que este entrena pueden contener cientos de capas ocultas, cada una con diferente tipo de neuronas.

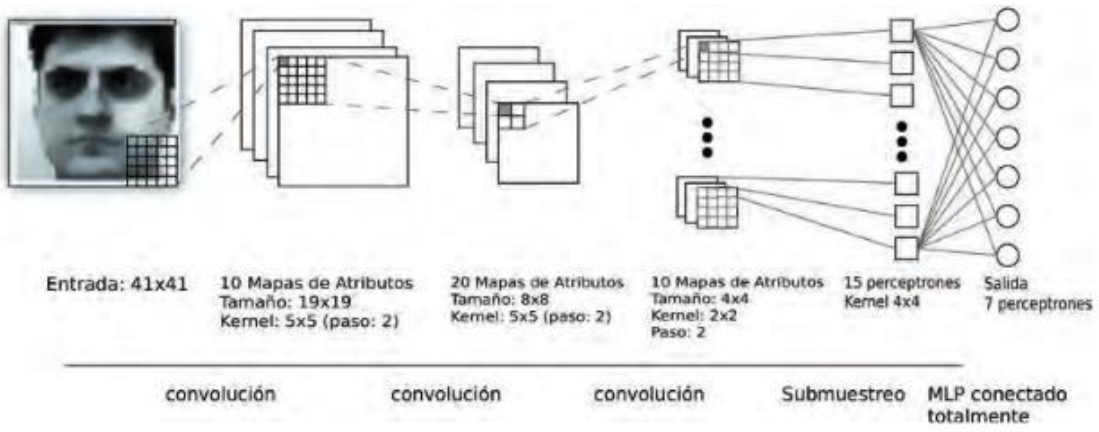
En el Deep Learning se hace uso de RNAs especiales conocidas como redes neuronales convolucionales, la diferencia de estas respecto a las convencionales radica en que la primera contiene dos capas ocultas especializadas en dos procesos: convolución y agrupación. (Sáez, 2019)

Capa de Convolución

Estas capas ocultas se ocupan de aprender patrones locales en ventanas pequeñas de dos dimensiones, alto por ancho. Son capas que sirven para detectar características visuales en las imágenes como líneas, bordes y gotas de color. Estas capas permiten aprender una propiedad de la imagen en un punto específico y ser capaz de reconocerla en cualquier lugar de la propia imagen. (Sáez, 2019)

Figura 2

Red neuronal de convolución



Nota: Arquitectura de la red neuronal de convolución, fuente: (Méndez & Ibarra, 2014)

La arquitectura final de la red neuronal está constituida de seis capas: entrada, tres capas de convolución, una capa de sub-muestreo y una capa de salida tradicional con conexión completa, con función de activación sig-moidal y el número de mapas que se resume en la Figura2. (Méndez & Ibarra, 2014)

Marco Conceptual

Algoritmo

Un algoritmo es una serie de pasos y secuencias lógicas que se utilizan para resolver un problema. Según Juan Carlos López Garcia en la guía "ALGORITMOS Y PROGRAMACIÓN" (2007) estable que desde los principios de los tiempos el ser humano se ha esforzado por abstraer la estructura de la solución a diversos problemas, con el fin de desarrollar un medio que les permita establecer una serie de procesos seguros, precisos y rápidos.

Base de datos

El libro "FUNDAMENTOS SOBRE LA GESTIÓN DE BASE DE DATOS" define una base de datos como: "un conjunto ordenado y estructurado de datos que representan una realidad objetiva y que están organizados independientemente de las aplicaciones" (2017), esto quiere decir que una base de datos es un repositorio donde se almacena información de manera ordenada, puede contener desde imágenes a archivos de texto.

Controlador

Un controlador es un dispositivo que se emplea para el gobierno de uno o varios procesos según el artículo Viviendas inteligentes (2005), se entiende mejor con un ejemplo, en el caso de un termostato cuando este a través de un sensor detecta un cambio en la temperatura, envía esta información al controlador, quien es el que se encarga de decidir que se va a hacer a continuación, ya sea aumentar o reducir la temperatura.

Microcontroladores

Un microcontrolador es un circuito integrado, en el que se puede grabar instrucciones para realizar una o varias tareas sencillas de manera repetitiva (Peña, 2020), aunque pueden funcionar de manera independiente se suelen encontrar varios de estos dispositivos en controladores.

Ethernet

"Ethernet es una red de comunicaciones de esquema abierto en su interconexión, su eficiencia en el intercambio de grandes volúmenes de información y al bajo coste de las interfaces requeridas en su implementación." (Juan, Javier, 2011) Dicho en otras palabras Ethernet es una estándar que permite a distintos dispositivos conectarse entre sí, siempre y cuando estén conectados por cable.

Cabecera GPIO

Las cabeceras o pines GPIO (General Purpose Input/Output) son elementos que Raspberry presento como interfaz de bajo nivel destinada a conectarse directamente con otros módulos de subsistemas. (Eugenio, 2017). Esto quiere decir que estos pines permiten la conexión de diferentes dispositivos como lo puede ser un sensor de movimiento y un controlador.

Bot

Un bot es una aplicación informática equipada con inteligencia artificial (IA) capaz de crear una conversación bidireccional entre humanos y máquinas (robots) a través de interfaces conversacionales o de chat. (Ávila et al., 2020). Esto quiere decir que un bot emplea un extenso algoritmo que está diseñado para contestar de una manera dependiendo de algún evento.

Arduino IDE

El entorno de desarrollo integrado o IDE de Arduino es una aplicación multiplataforma que se puede utilizar para escribir y cargar programas en placas Arduino y también aquellas que sean compatibles. (Peña, 2020), Sin embargo, tiene una comunidad activa que ha desarrollado núcleos gratuitos para que sea posible cargar programas en otros dispositivos.

Open Cv

"OpenCV (Open Source Computer Vision) es una popular biblioteca de visión por computadora iniciada por Intel en 1999. La biblioteca multiplataforma se enfoca en el procesamiento de imágenes en tiempo real e incluye implementaciones libres de patentes de los últimos algoritmos de visión por computadora." (Reconocimiento facial con OpenCV, s.f.)

Los algoritmos que están disponibles en la biblioteca Open Cv son:

EigenFace

EigenFace es conocido como el conjunto de vectores propios para el reconocimiento de rostros humanos se denominan caras propias. El término "Eigen" se refiere a un conjunto de vectores propios. La principal ventaja de este enfoque es que el conjunto de imágenes se puede representar utilizando una base que consiste en imágenes propias, cuyo tamaño es mucho más pequeño que el conjunto original. (caballero et al., 2017) esto quiere decir que el enfoque de reconocimiento facial de este modelo se basa en la captura de los cambios en un conjunto de imágenes faciales y usa esa información para codificar y comparar la totalidad de las imágenes faciales individuales.

FisherFace

Este es un método de reconocimiento facial que tiene en cuenta la iluminación y las expresiones faciales. Este es el responsable de la clasificación y reducción de facetas mediante el método FLD (Discriminant Linear Fisher). En este sentido, el análisis discriminante de Fisher intenta diseñar datos de tal manera que sus nuevas varianzas sean óptimas para la clasificación. (Esparza et al., 2015) en este caso en particular para el modelo es más importante centrarse en rasgos particulares y en las distintas variaciones de luz, de esta forma busca distanciar las fotografías de distintas personas, mejorando cada vez la precisión.

LBPH

“EL método de LBPH asigna etiquetas a cada uno de los pixeles de la imagen tomando en cuenta la distribución de los vecinos.” (Esparza et al., 2015)

Metodología

Tipo de investigación

Para el cumplimiento de los objetivos de este proyecto final de grado se hizo uso de una investigación mixta, que mantuvo un enfoque cuantitativo y cualitativo, ya que se manejaron distintas métricas de evaluación. La investigación cuantitativa se realiza cuando los datos recolectados son transformados en escalas numéricas y la investigación cualitativa cuando un conjunto de datos no puede ser sintetizado en números, sino que solamente puede ser representado en palabras o imágenes. (Julián, 2018) Un ejemplo de ello es el análisis que se realizó para este proyecto el cual examina las entradas principales a casas estrato 2 de Bogotá, dado que fue necesario tomar imágenes y medidas para la realización de este.

Para el análisis de la imágenes se utilizó el enfoque cualitativo ya que como menciona Frank Morales en su artículo tipos de investigación científica esta consiste en "caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciadores"(Goñi, 2014), en este caso en concreto permitió identificar los atributos que son fundamentales para el diseño de la alarma.

Fuentes de información para el estudio

Teniendo en cuenta lo anterior, durante el estudio se realizaron análisis, pruebas y comparaciones que sirvieron como base para la elaboración del diseño de la alarma, los resultados obtenidos se categorizaron como fuentes primarias, las cuales son:

- Análisis de entradas principales de las casas estrato 2 de Bogotá.
- Prueba de los tres modelos de reconocimiento facial.
- Comparación de alojamientos para servicios en la nube.

Durante el estudio se verificaron diferentes fuentes secundarias, cuyo origen se refiere a las poblaciones a ser consultadas como parte de este proceso, dentro de las fuentes tenemos:

- Encuesta de Percepción y Victimización de Bogotá (2022).
- Indicadores Financiaros del sector de Vigilancia y Seguridad Privada (2021).

Estas fuentes se obtuvieron por medio de las encuestas realizadas por la alcaldía mayor de Bogotá y la Superintendencia de Vigilancia y Seguridad Privada de Colombia, estas están disponibles en la página oficial de la cámara de comercio de Bogotá en el apartado de biblioteca digital y en la página se SuperVigilancia.gov.co del Ministerio de defensa del gobierno de Colombia.

Población y muestra

Ya que este proyecto presenta un diseño de una alarma para los hogares estrato 2 de la ciudad de Bogotá y debido a que la mayoría de personas no aceptaron el ingreso a sus viviendas, así como compartir información de estas, se trabajó con 5 casas estrato 2 de diferentes localidades de Bogotá como: Lisboa, bosa y candelaria a las cuales se obtuvo permiso por parte de los propietarios para tomar fotos y medidas.

Cronograma de actividades

Para determinar el tiempo que se tardara la elaboración de este proyecto de investigación se estableció trabajar con un diagrama de Gantt, ya que permitió visualizar los componentes básicos del proyecto y organizarlos en tareas más pequeñas y manejables. por ende, se define el periodo donde se empiezan a trabajar las actividades, así como la duración de estas (Eddie, 2023) El modelo es el siguiente:

Tabla 7

Cronograma de actividades

Actividades	Mes	1		2		3		4	
	Semanas	3 - 4	1 - 2	3 - 5	1 - 2	3 - 4	1 - 2		
Inicio									
Formulación y planteamiento del problema									
Objetivos									
Antecedentes y justificación									
Marco teórico									
Marco Conceptual									
Metodología de investigación									
Análisis casas									
Selección controlador									
Etapas para selección de IA									
Etapa 1: Creación base de datos									
Etapa 2: Preparación de los datos									
Etapa 3: Entrenamiento									
Etapa 4: Test									
Etapa 5: Reentrenamiento y test									
Diseño									
Diseño de la arquitectura									
Diseño del funcionamiento									
Diseño físico de la alarma									
Fin									

Nota: fuente, elaboración propia

Análisis de entradas principales de las casas estrato 2 de Bogotá

Para el análisis de tuvieron en cuenta 5 casas, en las que se hizo enfoque en la entrada principal, donde se tomaron medidas correspondientes a la distancia entre la puerta y la pared o en su defecto entre la puerta y la escalera, como se aprecia en la Figura 3, esto para determinar el alcance mínimo que tendrá la cámara de la alarma.

En la primera casa, la entrada contaba con acceso directo a las escaleras, ya que el primer piso es un local en arriendo, la distancia entre la escalera y la puerta es de 3 metros, no se apreció ninguna toma de corriente y ningún objeto relevante.

Figura 3

Casa 1



Nota: Conjunto de fotografías que muestran la entrada de la casa 1. Fuente: elaboración propia

En la segunda casa la entrada principal da acceso tanto al primer piso como al segundo, sin embargo, solo se tuvo en cuenta la entrada hacia el segundo piso, como se puede observar en la Figura 4, al igual que en la primera casa no hay presencia de tomas de corriente y de objetos relevantes como muebles.

Figura 4

Casa 2



Nota: Conjunto de fotografías que muestran la entrada de la casa2. Fuente: elaboración propia

La tercera casa solo tiene un piso por lo que no hay escaleras, la pared se encuentra a 5 metros de distancia, sin embargo, se puede apreciar una barra a 3.5 metros como se puede observar en la Figura 5, ducha barra es lo suficiente mente ancha para colocar objetos, además se identificaron varias tomas corrientes.

Figura 5

Casa 3

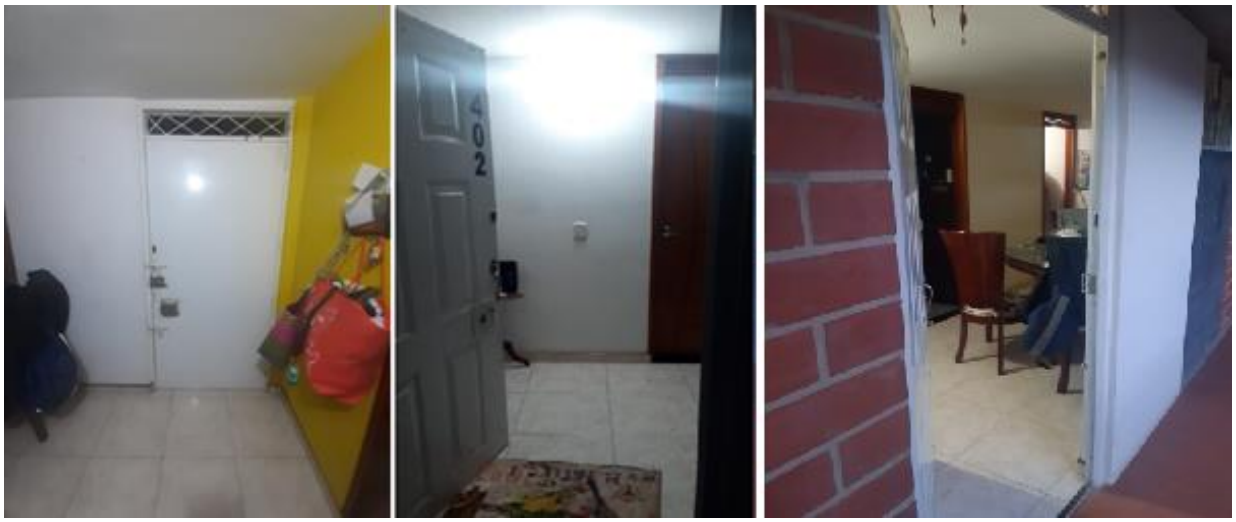


Nota: Conjunto de forografias que muestran la entrada de la casa3. Fuente: elaboración propia

En la cuarta casa pertenece a un conjunto cerrado, donde la estructura de las casas es igual. Esta casa tampoco posee acceso a un segundo piso por ende no hay escaleras, la pared se encuentra a 2 metros de distancia, también se puede apreciar una mesa cerca a la entrada como se puede observar en la Figura 6, además se identificaron varias tomas corrientes.

Figura 6

Casa 4



Nota: Conjunto de forografias que muestran la entrada de la casa 4. Fuente: elaboración propia

La quinta casa solo se analizó el primer piso, en donde se evidencio que respecto a las otras casas sin escalera tiene la pared más alejada de la puerta, encontrándose a 5 metros de distancia, también se puede apreciar varios elementos como una mesa a unos 4 metros con respecto a la entrada como se puede observar en la Figura 7, además se identificaron varias tomas corrientes.

Figura 7

Casa 5



Nota: Conjunto de forografias que muestran la entrada de la casa 5. Fuente elaboración propia

Para las casas se midió el alto de la puerta de la entrada, y en el caso de contar con escaleras se midió la distancia entre la puerta y el escalón donde la escalera alcanza los 1.71 metros de altura, ya que según la página DatosMundial.com (que recopila estudios científicos publicados por la NCS Risk Factor Collaboration y de la revista médica The Lacent) se presentan datos como la altura promedio de las personas en todos los países, en este caso se informa que la altura promedio de los hombres en Colombia es de 1,75 metros, con el fin de definir la atura en la que debería estar la alarma se utiliza este parámetro.

Las medidas tomadas se presentan a continuación:

Tabla 8

Tabla que muestra las medidas obtenidas

	Casa 1	Casa 2	Casa 3	Casa 4	Casa 5
Distancia entre la puerta y la pared	6.5 metros	4.2 metros	3.5 metros	2 metros	5 metros
Distancia entre la puerta y la escalera	3 metros	1 metro	n/a	n/a	n/a
Alto de la puerta	2 metros	1.9 metros	1.9 metros	1.8 metros	2 metros
Distancia entre la puerta el escalón que alcanza 1.71 metros de altura	4.96 metros	2.7 metros	n/a	n/a	n/a

Nota: fuente elaboración propia

Requerimientos del controlador

Con base al análisis realizado a 5 casas estrato 2 de la ciudad de Bogotá se permitió realizar una selección del controlador que se usaría como referencia para el diseño de la alarma con reconocimiento facial, para ello se definieron los siguientes requerimientos:

Tabla 9

Tabla de requerimientos del controlador

Requerimiento	Nombre	Descripción	Prioridad
RF1	Portabilidad	El dispositivo debe ser compacto de manera que no ocupe demasiado espacio y pueda colocarse en diferentes lugares.	Alta
RF2	Distancia de uso	El dispositivo debe poseer una cámara que permita una visualización de al menos 5 metros de distancia	Alta
RF3	Iluminación	El dispositivo debe poseer la manera de iluminar espacios oscuros.	Alta

RF4	Alimentación	El dispositivo debe poder alimentarse con una fuente que no requiera ser conectada a tomas de corriente.	Alta
RF5	Conexión WIFI	El dispositivo debe poseer la capacidad de conectarse a una red WIFI, preferiblemente sin cable Ethernet	Alta
RF6	Precio asequible	El dispositivo debe tener un precio asequible.	Alta
RF7	Sensor de movimiento	El dispositivo debe poseer un sensor de movimiento, o puertos que permitan acoplarle uno.	Alta

Controladores

En el siguiente apartado se presentan dos controladores que se usan habitualmente para la realización de proyectos de domótica enfocados en el reconocimiento facial, se hizo una comparación de los dos teniendo en cuenta el objetivo del proyecto de investigación, aparte de la eficiencia y el bajo coste para el diseño de una alarma con reconocimiento facial, que sea compacto y permita enviar imágenes por red Wifi, entre otros.

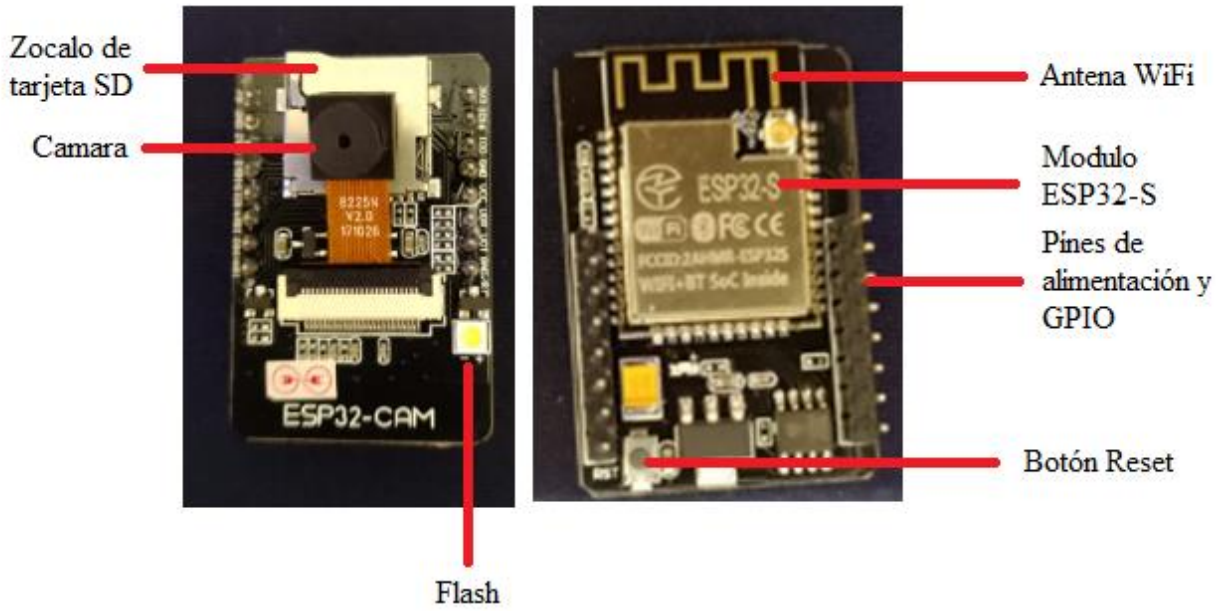
Esp32 CAM

Es un controlador que contiene una cámara OV2640 que tiene una visualización de 6 metros de distancia y una resolución de 1622×1200 px, Bluetooth, Wifi, lámpara de Flash, varios GPIO para conectar periféricos, también cuenta con una ranura para una tarjeta micro SD máximo de 4 GB que puede ser útil para almacenar imágenes tomadas con la cámara o almacenar otro tipo de archivos. Para la alimentación admite 5 voltios y tiene unas dimensiones de 40.5mm * 27mm *

4.5mm lo cual lo convierten en un dispositivo compacto. (Ernesto, 2020) Cuesta aproximadamente $40.000 pesos colombianos.

Figura 8

Aspecto del controlador Esp32cam

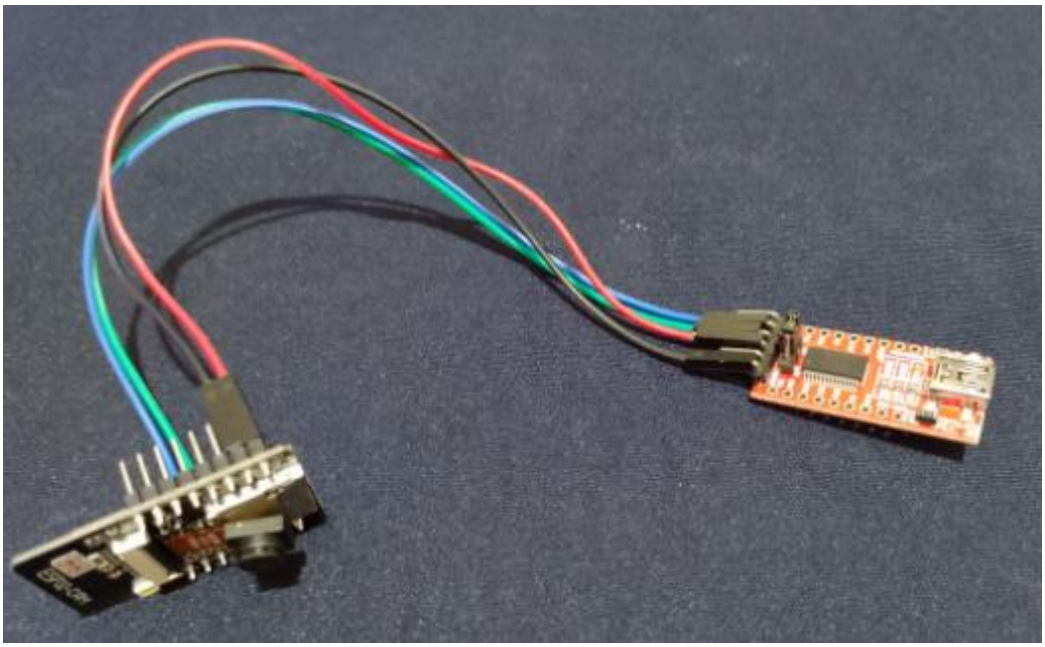


Nota: *Fuente elaboración propia*

Uno de los mayores defectos es que no cuenta con una interfaz USB para poder cargar el código directamente por lo que es necesario hacer uso de un programador FTDI como se muestra en la figura *, que nos permite programarlo con ayuda del IDE de Arduino.

Figura 9

Programdor FTDI conectado al modulo Esp32cam



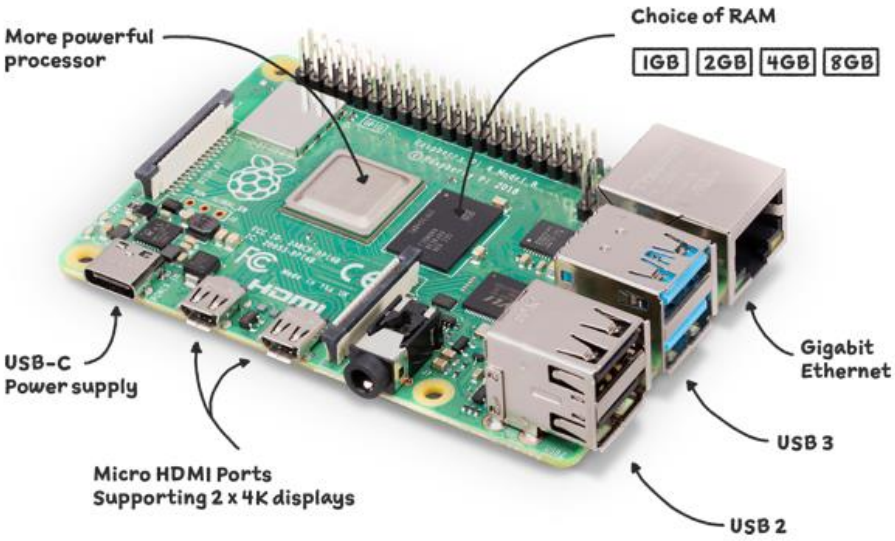
Nota: Fuente elaboración propia

Raspberry pi 4 Modelo B

Es una placa que cuenta con un procesador ARM, lo cual le permite realizar actividades que normalmente se llevan a cabo con un ordenador convencional, como crear documentos en Word y Excel, posee un puerto de cámara, conexión Bluetooth, Gigabit Ethernet, una cabecera GPIO de 40 pines para conectar periféricos, ranura para tarjeta micro SD que permite cargar el sistema operativo y almacenar archivos. Se puede alimentar a través de un conector Micro USB, soportando 5 voltios. Tiene unas dimensiones de 85mm * 56mm lo cual lo convierten en un dispositivo compacto. Cuesta aproximadamente 550.900 pesos colombianos. (Raspberry Pi, 2023)

Figura 10

Aspecto del controlador Raspberry Pi 4 Model B



Nota: La imagen indica los componentes del controlador Raspberry Pi 4 Modelo. Tomado de Raspberry Pi. (2023).

Selección de controlador

Para tomar la decisión del controlador que se usa en el proyecto se tuvo en cuenta los requerimientos previamente definidos, ver tabla 8, como el factor económico, la portabilidad y el aprovechamiento del hardware, en este caso tenemos que el Raspberry Pi ofrece más posibilidades ya que cuenta con varios puertos y permite hacer tareas que generalmente se hacen con un ordenador, y pese a que posee un puerto para conectar una cámara no la trae de fábrica, en cuanto a la portabilidad ambos ocupan un pequeño espacio. En el caso del ESP32-Cam este es más limitado y necesita de un programador FTDI para poder ser programado, sin embargo, trae de fábrica una cámara y posee los suficientes puertos para acoplarle un sensor de movimiento y

es considerablemente más económica que el Raspberry Pi, por tanto, la selección final corresponde al Esp32-Cam.

Presupuesto

Con base a la selección del controlador a utilizar se presenta una tabla, ver tabla *, que relaciona los costos del hardware que se presentaran en el diseño de la alarma:

Tabla 10

Costos del hardware

Elementos Alarma	Costos
Módulo Esp32-cam	40000
Batería 5v	10000
Sensor de movimiento PIR	10000
Programador FT	15000
Cables jumper	12000
Total	87000
Precio sin Programador FT	77000

El precio final es de 87000 pesos colombianos, sin embargo, en caso de querer desarrollar más de una alarma, se pude re utilizar el programador, por tanto, el coste del segundo y los posteriores seria de 77000.

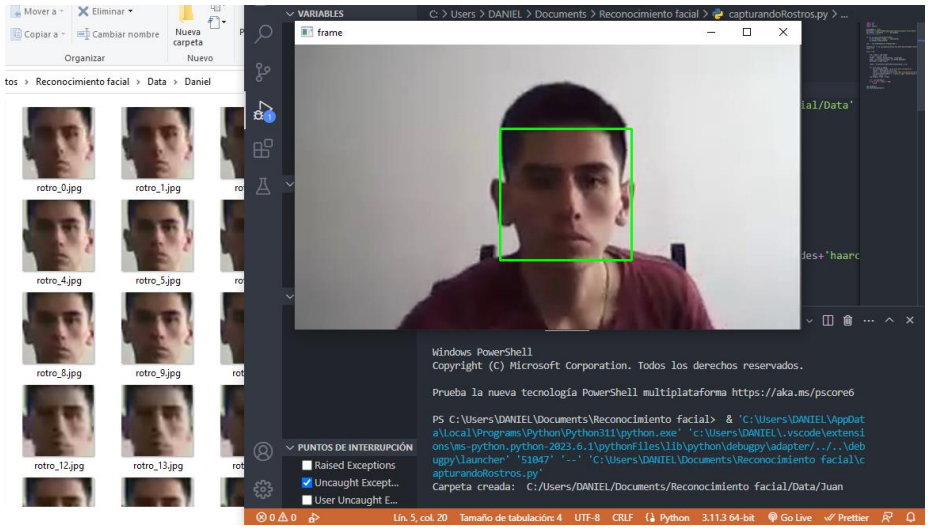
Etapa 1: Creación de la base de datos

Para el entrenamiento de los modelos se decidió construir un almacenamiento robusto, para que la inteligencia artificial tenga los suficientes recursos para que dado el momento pueda realizar un reconocimiento facial que logre superar el 95% de precisión. La configuración presentada en el diseño de cada capa del algoritmo ha sido verificada por un conjunto de prueba de dos bancos de imágenes, en el que se usaron 600 imágenes correspondiente a dos personas, guardando una estructura para almacenar los archivos que permita entrenar modelos en diferentes situaciones.

En el primer caso se decidió utilizar un video de una persona realizando diferentes movimientos de cabeza y gestos, este video fue echo con una cámara de 2 mega pixeles para asimilarlo a la calidad de imagen que tendría el dispositivo final que es de 5 mega pixeles.

Figura 11

Captura de imagen del almacendamiento de rostros por parte del algorimto

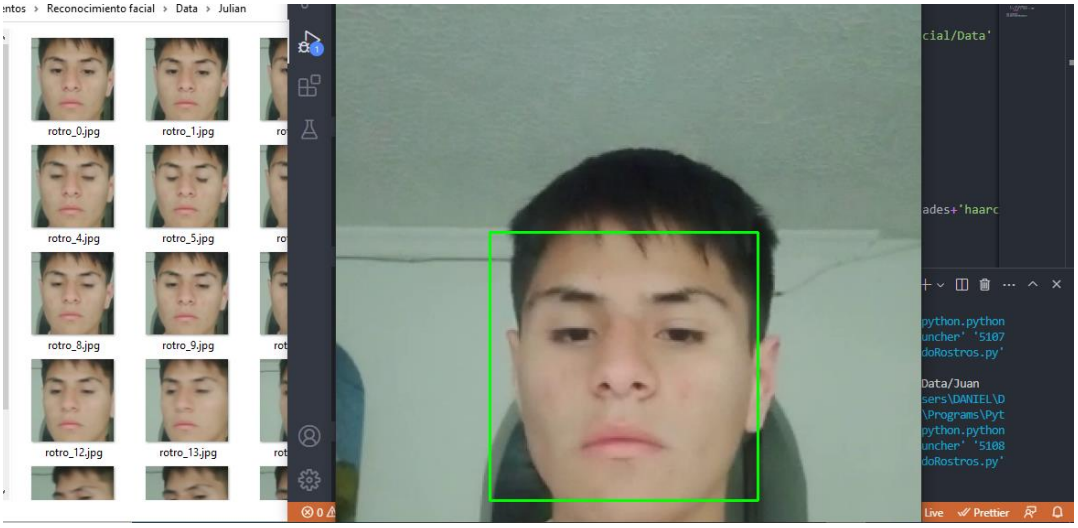


Nota: fuente, elaboración propia

En el segundo caso se decidió utilizar un video de una persona realizando diferentes movimientos de cabeza y gestos, este video fue echo con una cámara de 8 mega pixeles para determinar el impacto que tiene la resolución en cuanto al porcentaje de precisión.

Figura 12

Captura de imagen del almacendamiento de rostros por parte del algorimto



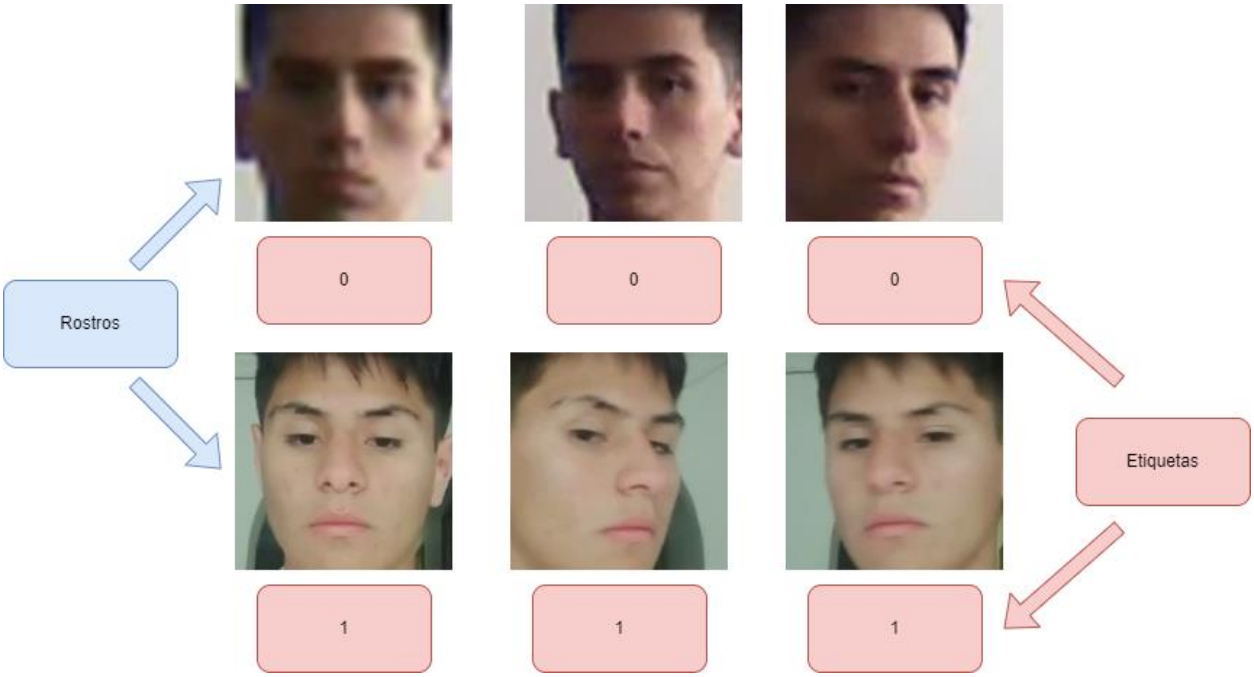
Nota: fuente, elaboración propia

Etapa 2: Preparación de los datos

Previo al entrenamiento de las inteligencias artificiales se optó por asociar una etiqueta a cada almacenamiento de imágenes, en este caso como se tenían dos depósitos correspondientes a cada escaneo que se realizado con OpenCV, ver figura 1 y 2, se optó por colocarle 0 y 1 como etiquetas respectivamente (ver figura 13), con el fin de que el algoritmo supiera que cada imagen corresponde a una persona distinta.

Figura 13

Modelo de asiganacion de etiquetas



Nota: fuente, elaboración propia

Etapa 3: Entrenamiento

Se empezó con el modelo Eigenfaces, para el enteramiento de este modelo es indispensable que las imágenes conserven el mismo tamaño, por eso en el proceso de captura de imágenes se utilizó la siguiente línea de código:

rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)

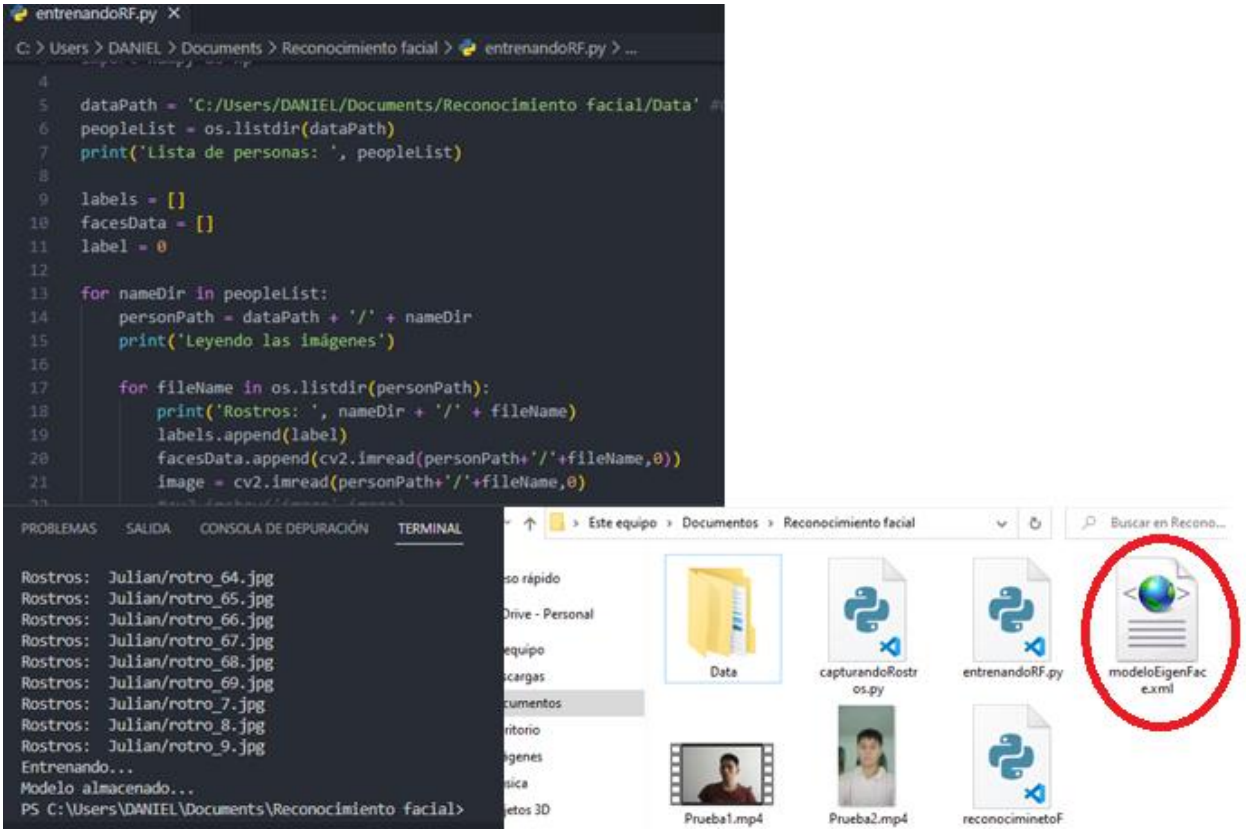
La cual indica al programa que las imágenes sean guardadas en una escala de 150 * 150, adicional a ello el modelo también requiere que las imágenes estén en escala de grises, por tanto, se implementó la siguiente línea de código al algoritmo:

cv2.rectangle(frame, (x,y),(x+w,y+h),(0,255,0),2)

Una vez ejecutado el código el programa procede a analizar todas las imágenes, para que finalmente proporcione un archivo xml de nombre “modeloEigenFace”, como se muestra a continuación:

Figura 14

Captura del modelo Eigenfaces entrenando y creando archivo xml



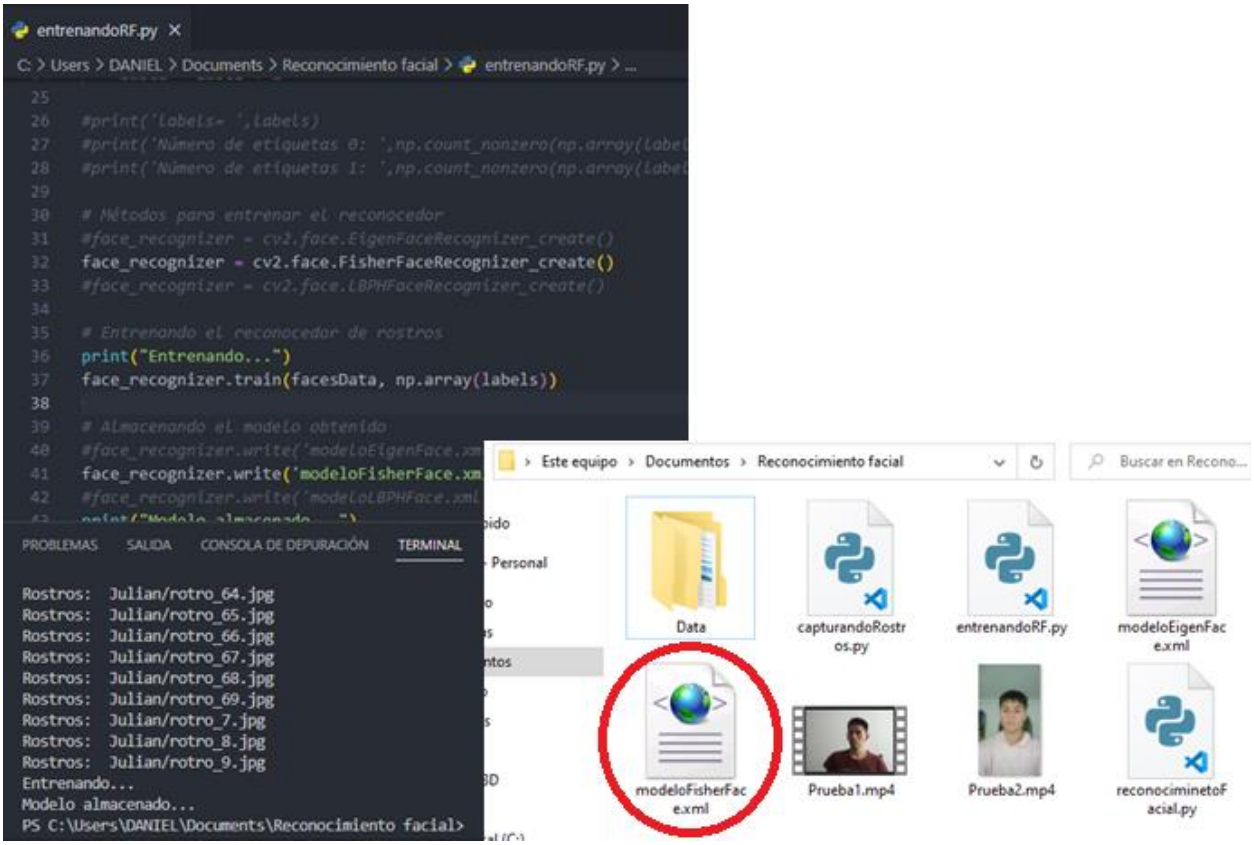
Nota: fuente, elaboración propia

Posterior mente el modelo Fisherfaces al igual que el anterior modelo, para el enteramiento es importante que las imágenes conserven el mismo tamaño, y que estas se encuentren en escala de grises. Una vez ejecutado el código el programa procede a analizar todas

las imágenes, para que finalmente proporcione un archivo xml de nombre “modeloFiserFace”, tal como se puede apreciar en la siguiente imagen:

Figura 15

Captura del modelo Fisherfaces entrenando y creando archivo xml



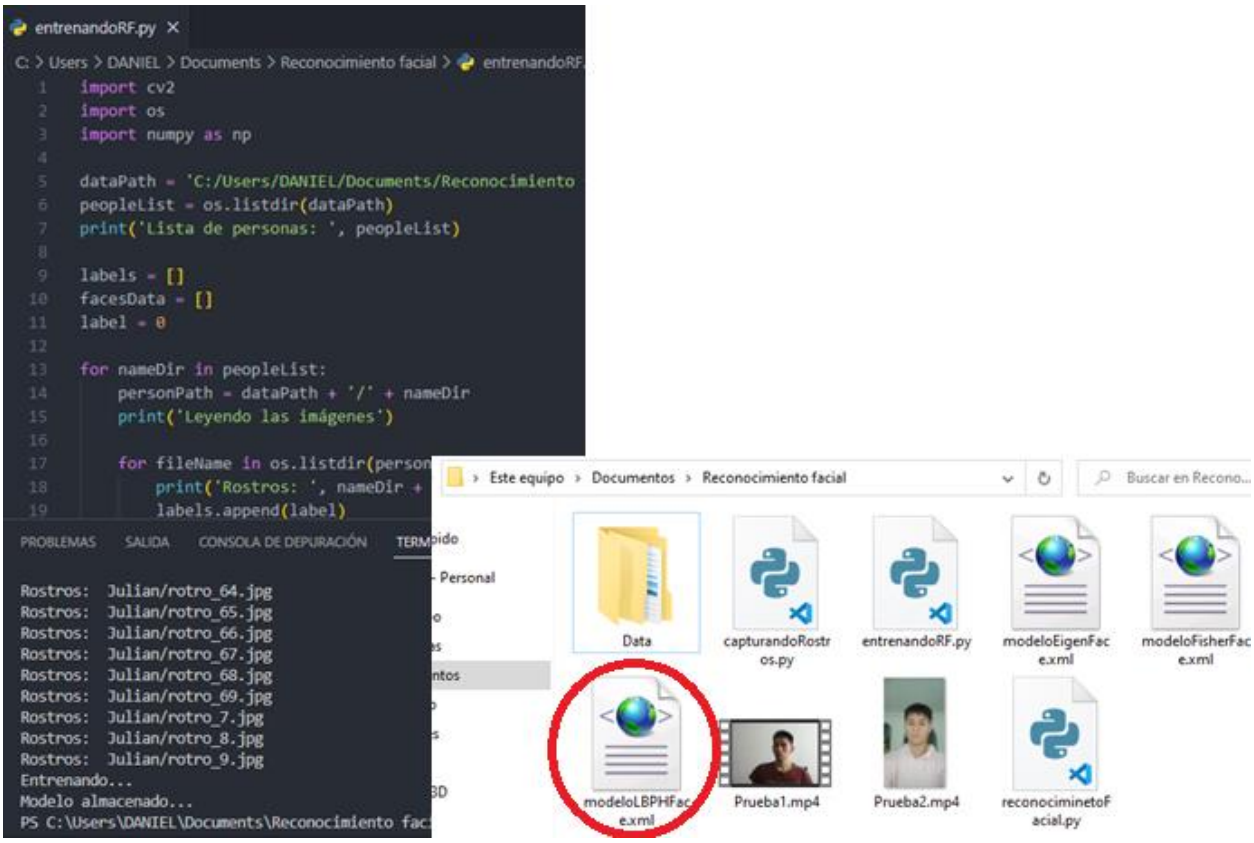
Nota: fuente, elaboración propia

Por último, el modelo LBPH al igual que los anteriores modelos, para el enteramiento es importante que las imágenes se encuentren en escala de grises, sin embargo, para este modelo las imágenes pueden tener distintos tamaños, pero dado que en la creación de datos se estableció un tamaño de 150 *150, no se probaron imágenes de distintos tamaños. Una vez ejecutado el código

el programa procede a analizar todas las imágenes, para que finalmente proporcione un archivo xml de nombre “modeloLBPHFace”, tal como se puede apreciar en la siguiente imagen:

Figura 16

Captura del modelo LBPH entrenando y creando archivo xml



Nota: fuente, elaboración propia

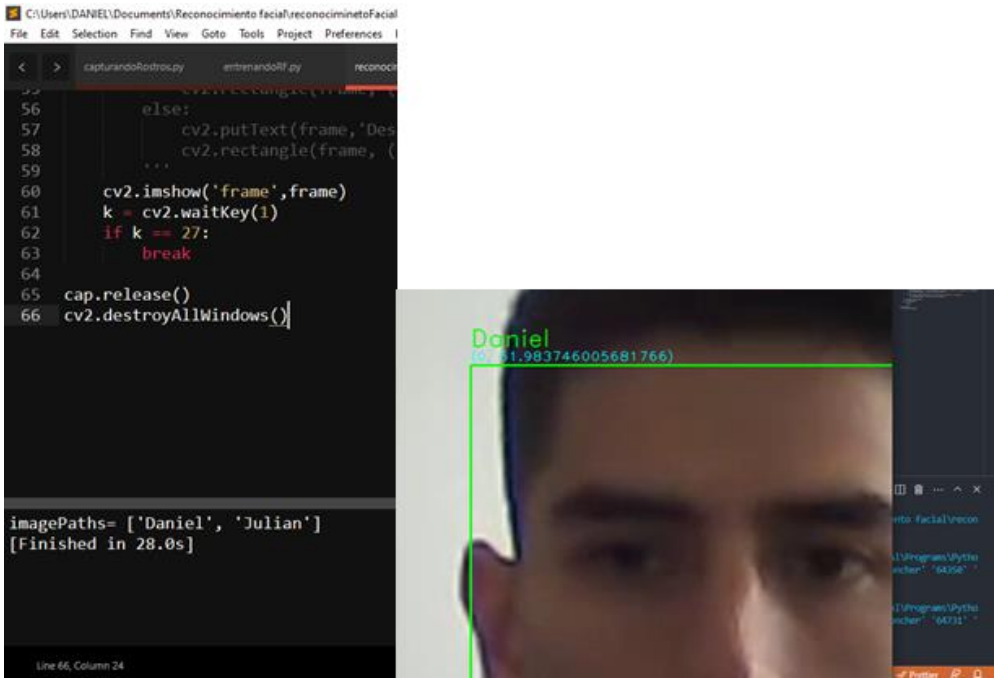
Etapa 4: Test de los modelos de reconocimiento facial

Para el primer Test se inició con el modelo EigenFace, primero se ejecutó con el video de prueba y se midió su valor de confianza, este valor aparece al lado derecho después del 0, como se ve en la figura 16. Este valor es de suma importancia pues entre más cercano este a cero mejor será el modelo, una vez ejecutado el modelo este resultado empezará a variar, por lo que es

importante tener en cuenta el valor más alto ya que este será el que se usará como referencia para el análisis de los demás videos.

Figura 17

Identificación de rostro por el modelo EigenFace



Nota: Captura del modelo Eigenface identificando un rosrto. Fuente: elaboracón propia

Para este modelo se analizaron cuatro videos, cada dos videos correspondían a una persona, en este caso a los sujetos Daniel y Julián, a continuación, se muestra los resultados obtenidos tras la ejecución del modelo EigenFace:

Tabla 11

Valores registrados en el test EigenFace

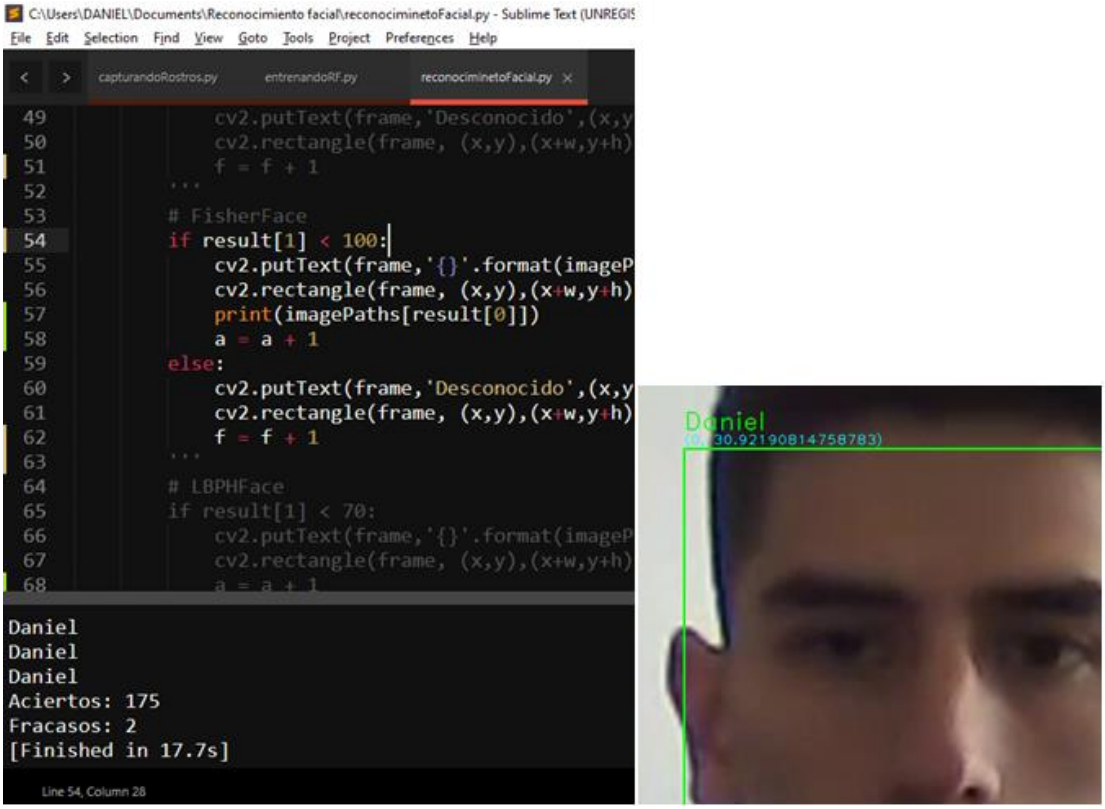
Modelo EigenFace				
	Daniel		**Julián**	
	Video 1	Video 2	Video 1	Video 2
Duración video	18 (s)	11(s)	3(s)	6(s)
Duración análisis	25.6 (s)	20.2(s)	6.9(s)	7.8(s)
Aciertos	177	250	5	0
Fracasos	0	29	14	25
Valor de confianza	5700	5700	6000	6000

En este caso se decidió aumentar el valor de confianza del segundo sujeto de prueba ya que el modelo no reconocía a la persona. Esto se debe a que los videos de Julián eran más cortos y tenían movimientos más bruscos, esto con el fin de simular como sería en una situación real la entrada de una persona a una vivienda. En el caso de Daniel los videos eran más prolongados y con movimientos más lentos, también el primer video era muy similar al que fue usado como medio de aprendizaje de la inteligencia artificial.

Para el Segundo Test se siguió con el modelo FasherFace, este se ejecutó con el video de prueba uno y se midió su valor de confianza, este valor aparece al lado derecho después del 0, como se ve en la figura 17. Este valor oscilaba entre los 30 y 100 tal como se puede apreciar en la figura 17:

Figura 18

Captura del modelo Fisherface identificando un rosrto



Nota: fuente, elaboración propia

Para este modelo se analizaron cuatro videos, cada dos videos correspondían a una persona, en este caso a los sujetos Daniel y Julián, a continuación, se muestra los resultados obtenidos tras la ejecución del modelo FisherFace:

Tabla 12

Resultados del modelo FisgerFace

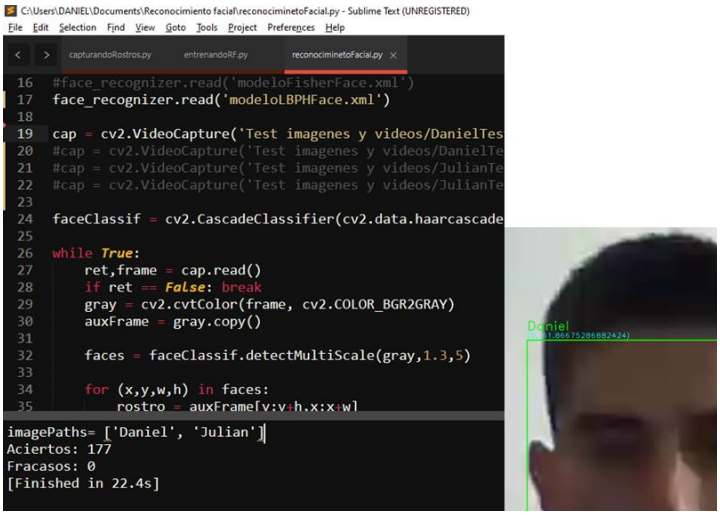
Modelo FisherFace				
	Daniel		**Julián**	
	Video 1	Video 2	Video 1	Video 2
Duración video	18 (s)	11(s)	3(s)	6(s)
Duración análisis	17.7 (s)	6.4(s)	1.9(s)	2.8(s)
Aciertos	175	248	0	0
Fracasos	2	31	19	25
Valor de confianza	100	100	100	100

Al igual que el anterior modelo en los videos de ‘Julián’ no lograba reconocerlo, pero adicionalmente lo marcaba erróneamente como si fuera ‘Daniel’. Respecto a los demás modelos presenta los peores valores pues en los videos 1 y 2 de Julián presenta los valores de fracasos más altos que cualquier otro. Lo único positivo de este modelo es que el análisis de reconocimiento de rostros lo hacía en menor tiempo, inclusive esteba por debajo de la duración de cada video.

Finalmente, el ultimo Test que se hizo fue con el modelo LBPH, este se ejecutó con el video de prueba uno y se midió su valor de confianza, este valor aparece al lado derecho después del 0, como se ve en la figura 17. Este valor oscilaba entre los 60 y 70 tal como se puede apreciar en la figura 18:

Figura 19

Captura del modelo LBPH identificando un rosrto



Nota: fuente, elaboración propia

Para este modelo se analizaron cuatro videos, cada dos videos correspondían a una persona, en este caso a los sujetos Daniel y Julián, a continuación, se muestra los resultados obtenidos tras la ejecución del modelo LBPH:

Tabla 13

Resultados del modelo LBPH

Modelo LBPH				
	Daniel		**Julián**	
	Video 1	**Video 2**	**Video 1**	**Video 2**
Duración video	**18 (s)**	**11(s)**	**3(s)**	**6(s)**
Duración análisis	**22.1 (s)**	**16.5(s)**	**3.5(s)**	**4.6(s)**
Aciertos	**177**	**230**	**0**	**0**
Fracasos	**0**	**49**	**19**	**25**
Valor de confianza	**70**	**70**	**70**	**70**

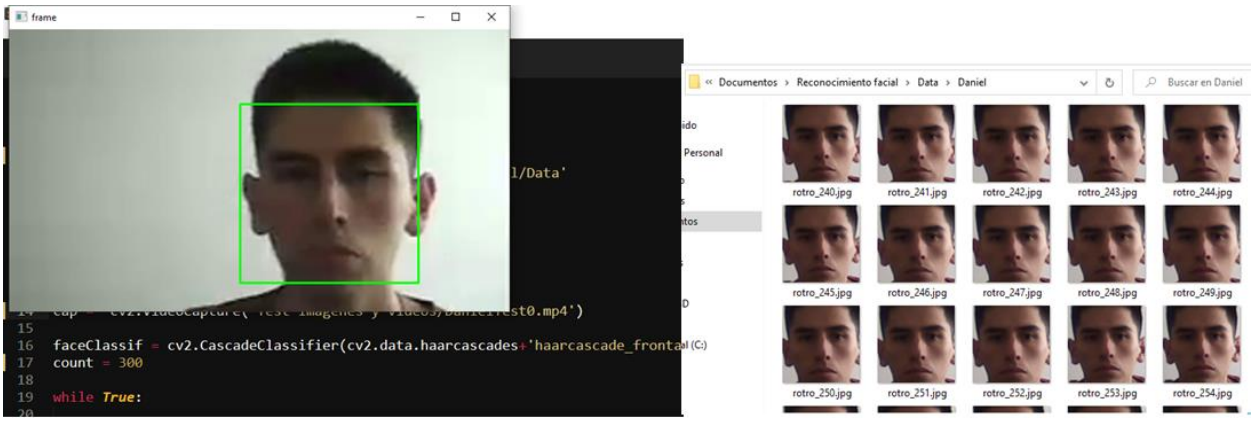
Al igual que los anteriores modelos en los videos de ‘Julian’ no lograba reconocerlo. Presenta valores muy parecido a los obtenidos por el modelo FisherFace.

Etapa 5: Reentrenamiento y Test de los modelos de reconocimiento facial

Debido a que los valores obtenidos en el primer test de cada modelo en su mayoría fueron erróneos, sobre todo con los videos de la persona ‘Julian’. Se decidió volver a entrenar cada modelo, para este entrenamiento se alimentó el banco de datos con más imágenes, para el caso de la data de ‘Daniel’ se agregaron 425 imágenes y para el caso de ‘Julian’ se agregaron 23 más. Como se muestra en la figura 19 a continuación:

Figura 20

Captura de imágenes



Nota: fuente, elaboración propia

Luego se reentrenaron los modelos y se pusieron a prueba nuevamente, dando los siguientes resultados para el modelo EigenFace:

Tabla 14

Resultados obtenidos por el modelo EigenFace

Modelo EigenFace				
	Daniel		**Julián**	
	Video 1	Video 2	Video 1	Video 2
Duración video	18 (s)	11(s)	3(s)	6(s)
Duración análisis	36.3 (s)	30.6(s)	13.7(s)	15(s)
Aciertos	177	279	18	25
Fracasos	0	0	1	0
Valor de confianza	4000	4000	4000	4000

En los resultados se nota una gran mejora en cuanto a los aciertos obtenidos por reconocer a la persona, tiendo un éxito del 100% en la mayoría de casos, solamente en uno presento un 5.26% de margen de error. También se puede apreciar que el valor de confianza se pudo reducir a 4000. Sin embargo, también se nota que duración del análisis era más del doble de la duración de los videos, incluso en algunos casos llegando a triplicar dicho valor.

En el caso del modelo FisherFace se presentaron los siguientes resultados:

Tabla 15

Resultado análisis con el modelo FisherFace

Modelo FisherFace				
	Daniel		**Julián**	
	Video 1	Video 2	Video 1	Video 2
Duración video	18 (s)	11(s)	3(s)	6(s)
Duración análisis	17.8 (s)	6.1(s)	1.8(s)	2.7(s)
Aciertos	177	279	18	24
Fracasos	0	0	1	1
Valor de confianza	10	10	10	10

Al igual que en el anterior modelo en los resultados se aprecia una gran mejora en cuanto a los aciertos obtenidos por reconocer a la persona, tiendo un índice de éxito que está por encima de 94% y en algunos casos alcanzo el 100%. También se puede apreciar que el valor de confianza se pudo reducir a 10, cabe resaltar que este es el valor más bajo de los tres modelos, lo que significa que su confiabilidad es mayor. Por otra parte, también se nota que la duración del análisis es menor no solamente a la duración del video, si no, con respecto a la prueba anterior de este modelo, dejándolo, así como el más rápido de los tres modelos.

En el caso del modelo LBPH se presentaron los siguientes resultados:

Tabla 16

Resultados del segundo test del modelo LPBH

Modelo LBPH				
	Daniel		**Julián**	
	Video 1	Video 2	Video 1	Video 2
Duración video	18 (s)	11(s)	3(s)	6(s)
Duración análisis	28.7 (s)	22.8(s)	5.8(s)	7(s)
Aciertos	177	279	6	24
Fracasos	**0**	**0**	**13**	**1**
Valor de confianza	**50**	**50**	**50**	**50**

Al igual que en los anteriores modelos los resultados presentan una gran mejoría en cuanto a los aciertos obtenidos por reconocer a la persona, sin embargo, en una prueba registro 31.5% de desacierto, lo que lo deja como el modelo más impreciso hasta el momento. También se puede apreciar que el valor de confianza se pudo reducir a 50, y al igual que el modelo EigenFace la duración del análisis se incrementa no solamente respecto a la duración del video, si no, con respecto a la prueba anterior de este modelo, llegando a duplicar la duración.

Resultados

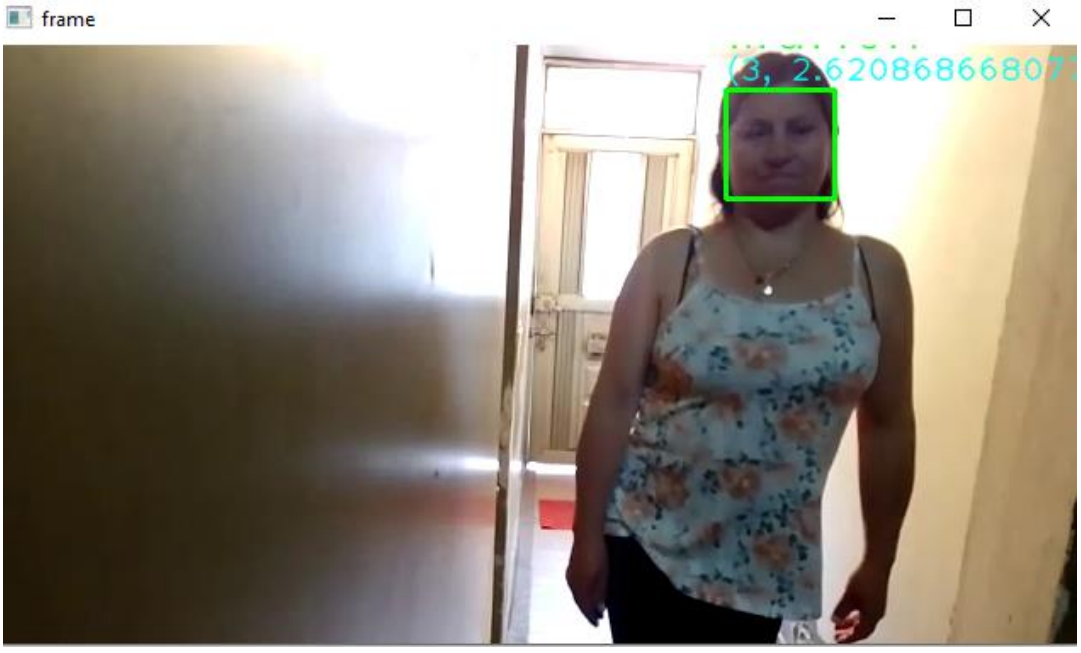
Escenario de prueba

En este apartado se presenta una simulación del comportamiento de la alarma en la que donde se pone a prueba las inteligencias artificiales con la presencia de una persona de la cual se posee imágenes en la base de datos y otra que no ha sido identificada. Para asimilarlo a un escenario real se usó la casa 1, ver fugara 21, y la cámara se colocó a una altura de 1.71 metros. Para esto proceso ya se contaba con una base de datos con 1000 imágenes y se utilizó el modelo FisherFace ya que fue el modelo con mayor índice de precisión.

A continuación, se muestra los resultados de la prueba con la persona registrada en la base de datos.

Figura 21

Reconocimiento positivo de una persona registrada



Nota: Se aprecia como el algoritmo reconoce a la persona, aunque no se alcanza a leer el color verde indica cual fue reconocida. Fuente: elaboración propia.

Tabla 17

Matriz de confusión persona identificada

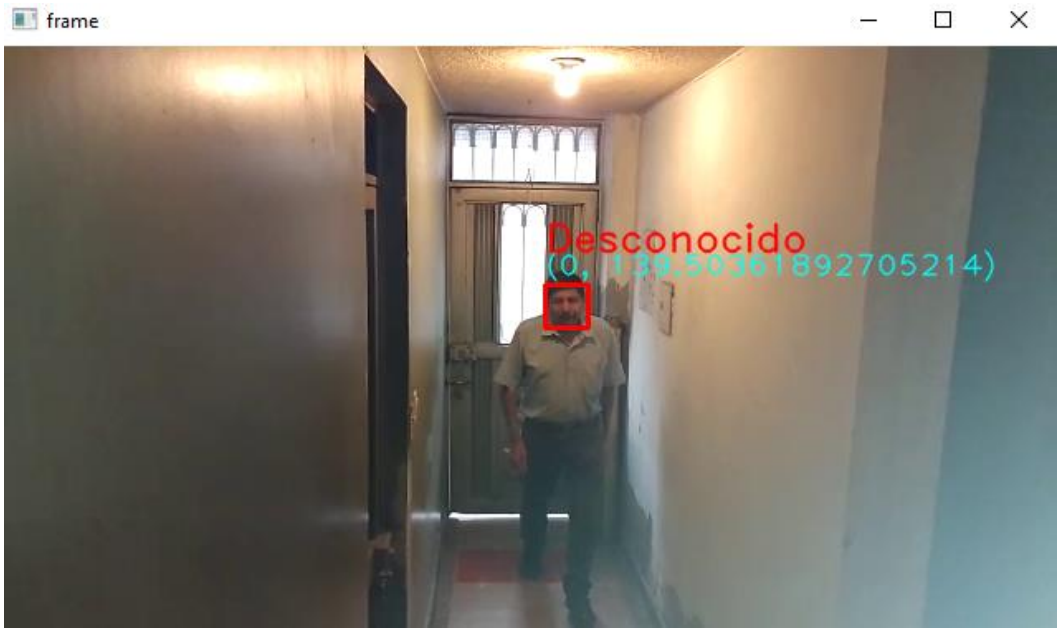
		Predicción	
		Positivo	Negativo
Actual	Positivo	13	0
	Negativo	0	0

El primer análisis demostró tener una precisión del 100%, pues como se aprecia en la matriz de confusión, el índice de predicción fue igual al obtenido por la inteligencia artificial.

Después, se muestra los resultados de la prueba con la persona que no está registrada en la base de datos.

Figura 22

Reconocimiento positivo de una persona no registrada



Nota: Se aprecia como el algoritmo identifica a la persona como desconocida. Fuente: elaboración propia.

Para el segundo análisis también se demostró tener una precisión del 100%, pues como se aprecia en la matriz de confusión (ver tabla 17), el índice de predicción fue igual al obtenido por la inteligencia artificial, ya que en este caso se esperaba que se identificara a la persona como desconocido, y la inteligencia artificial así lo hizo.

Tabla 18

Matriz de confusión persona no identificada

		Predicción	
		Positivo	Negativo
Actual	Positivo	0	0
	Negativo	11	0

Diseño de la alarma

Esquema

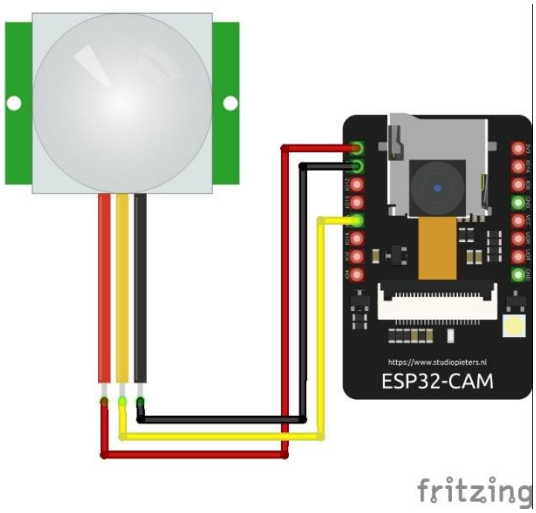
Para poder diseñar la alarma con reconocimiento facial objetivo, se utiliza como base el artículo de investigación: Sistema de seguridad con reconocimiento facial en módulo ESP32 (Álvarez & Bazá, 2022), en el que se muestra la construcción y el diseño de una alarma que toma fotos cuando detecta movimiento, el propósito fue mejorar el funcionamiento de dicho dispositivo al integrarle una inteligencia artificial que hace uso de reconocimiento facial para la identificación de personas, a la vez se le diseño una carcasa que permite colocarlo en paredes, escaleras u otros objetos, además que protege al dispositivo de golpes.

En el diseño se emplean 4 elementos, como se ven en la figura 23:

- Modulo Esp32-Cam
- Batería o pila de 5v
- 5 Cables jumper
- Sensor de movimiento PIR

Figura 23

Esquema para ESP32-CAM con sensor PIR



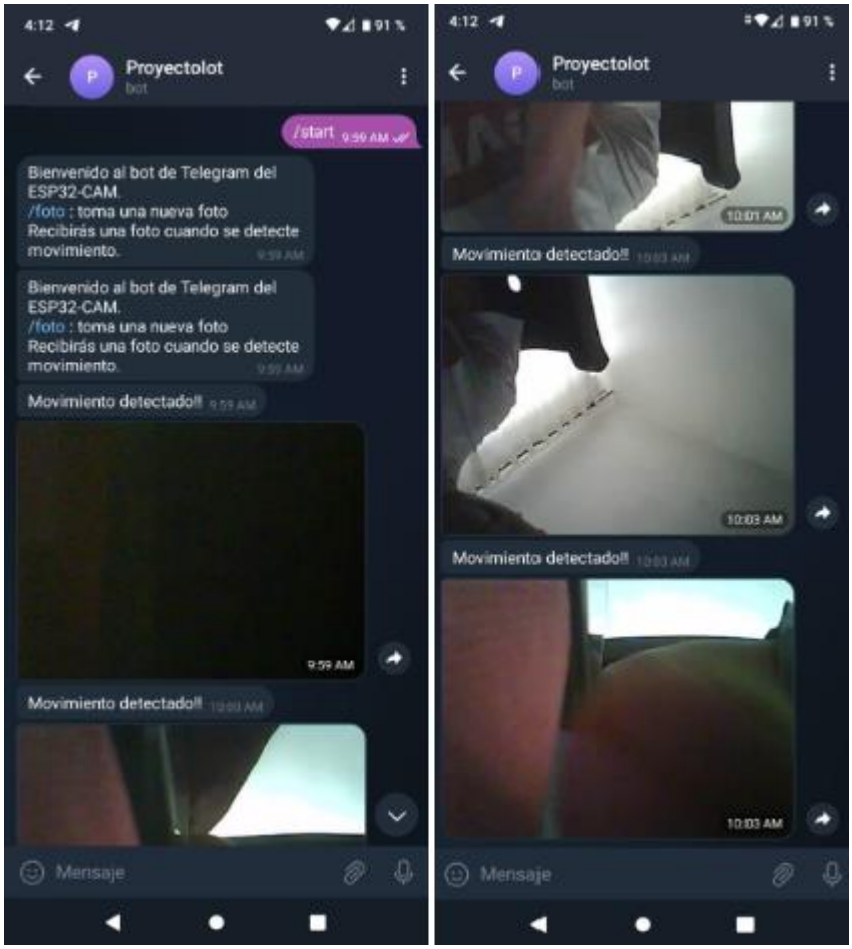
Nota: Adaptado de Diagrama de cableado para ESP32 y sensor PIR, por WillMakesTV, 2021, (https://www.hackster.io/WillMakesTV/discord-security-camera-with-an-esp32-7c4621)

Bot de Telegram

A continuación, se muestra la interacción que debe de tener la alarma con el bot de Telegram, pues cuando se detecte movimiento se enviara un mensaje de alerta, sin importar, si se realizaron movimientos bruscos enfrente del dispositivo, la interacción se muestra a continuación:

Figura 24

Interacción con el bot de Telegram



Nota: Se muestra las alertas al detectar movimiento. Fuente: elaboración propia

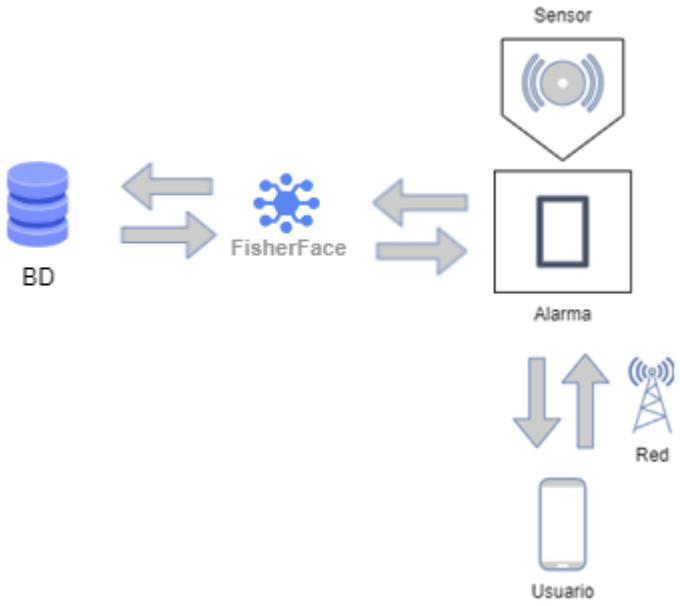
Como se puede apreciar en la imagen, se debe de iniciar con el comando “/start” luego el Bot muestra un mensaje de bienvenida, donde nos indica que es posible tomar fotos con el comando “/foto” o en su defecto cuando se detecte movimiento, pues automáticamente este tomara fotos. Sin importar la baja iluminación el bot detectara los movimientos fueran lentos o bruscos, como se aprecia en la figura 24, por cada movimiento tomaba una fotografía, sin embargo, cabe resaltar que estas se pueden demorar algunos segundos en ser tomadas y enviadas al celular.

Arquitectura propuesta

Teniendo en cuenta que se desea integrar una inteligencia artificial como parte del funcionamiento de una alarma son sensor de movimiento se diseña la arquitectura que debería de implementarse para lograr la integración de las dos herramientas, tal como se muestra en la figura 25, se implementara google drive como almacenamiento en la nube para la inteligencia artificial.

Figura 25

Arquitectura propuesta para la integración de la alarma con la IA



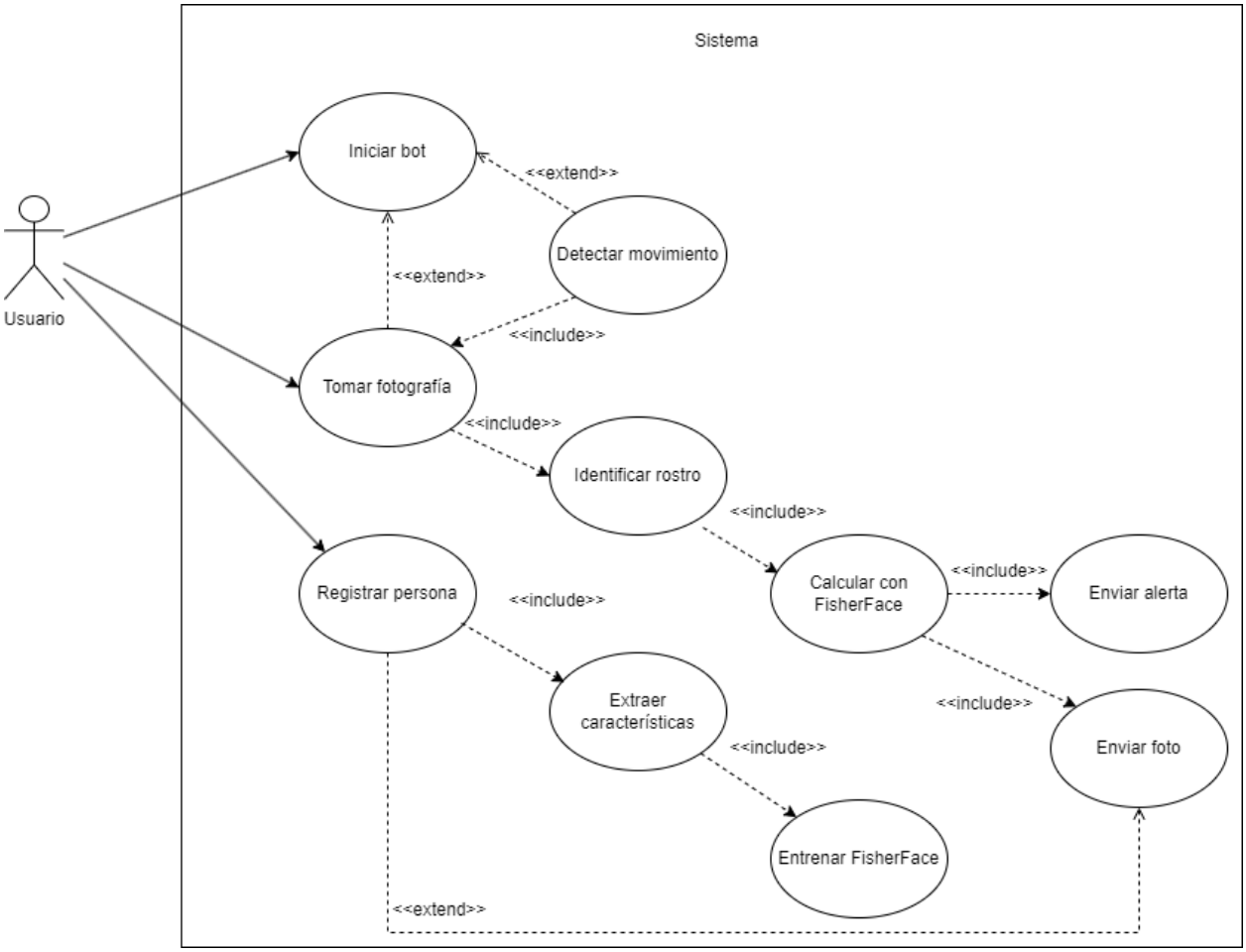
Nota: fuente elaboración propia

La figura 25 se muestra como funcionaria la alarma integrando la inelegancia artificial, en primer lugar, el sensor al detectar movimiento enviara una señal al dispositivo, este tomara fotos y la IA se encargará de analizarlas con base en la data almacenada y con base en ello enviara una respuesta, finalmente cuando esta respuesta llegue al dispositivo, este la enviara al usuario a través de la red WiFi.

Diagrama caso de uso

Figura 26

Diagrama caso se uso



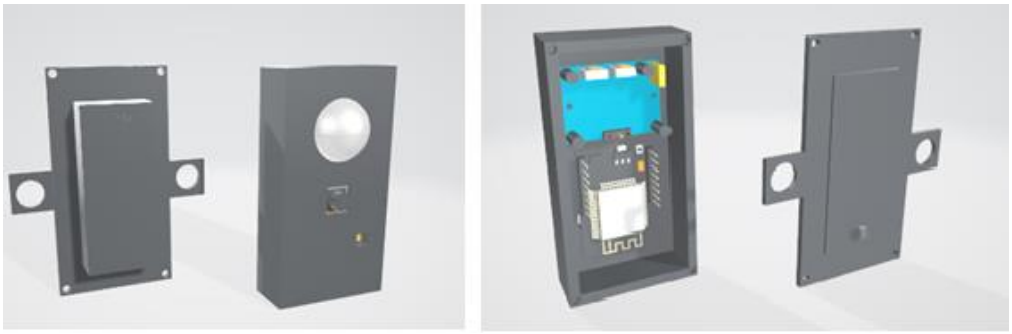
Nota: fuente, elaboración propia

Diseño físico propuesto

Debido a que la alarma tiene podrá colocarse en tanto en escaleras como en murtos a una altura de 1.71 metros, se diseñaron dos propuestas que se ajustaron a los estándares, los cuales indican que la alarma no puede estar alejada más de 6 metros de la entrada, con base en ello se presenta el primer modelo, en la figura 27:

Figura 27

Diseño propuesto para la cobertura de la alarma



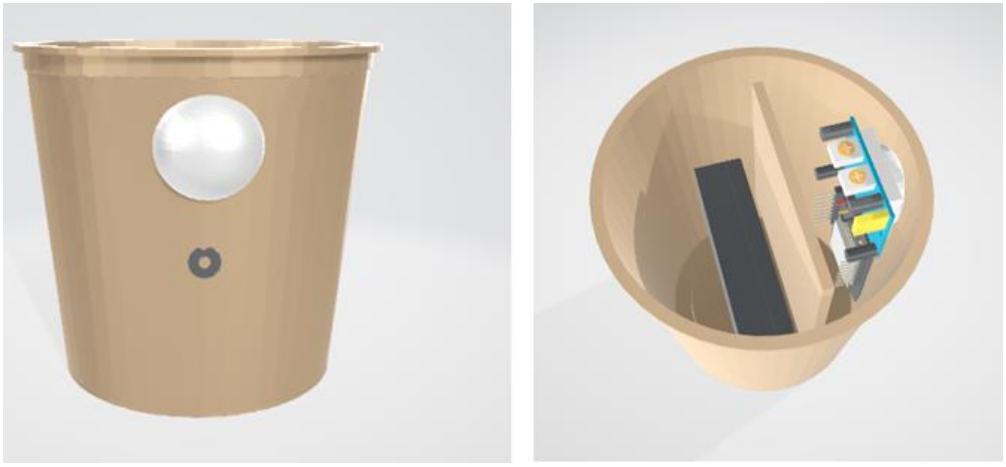
Nota: Diseño para ser colocado en una pared. Fuente: Elaboración propia

Este diseño pretende utilizar una caja de pilas como fuente de energía, que alimentara al ESP32-cam y al sensor Pir, dicha caja tendrá dos pestañas a los lados laterales para que sean atornilladas a una pared o mueble.

Como se encontró que muchas de las viviendas contaban con escaleras justo después de la entrada, se elaboró un diseño en forma de maceta que albergaría la alarma en su interior, además que permite el uso de una caja de pilas, así como la implementación de una batería, en cuanto a la fuente de alimentación, como se muestra en la figura 28.

Figura 28

Segundo diseño propuesto para la cobertura de la alarma



Nota: Diseño para ser colocado en una escalera. Fuente: Elaboración propia

Discusión

El diseño de una alarma que haga uso de reconocimiento facial se plantea como una solución a un problema social, como lo es el hurto a viviendas, a continuación, se reacciona a los resultados obtenidos luego del análisis de las casas estrado 2 de la ciudad de Bogotá y de los tres modelos de reconocimiento facial probados anteriormente:

1. En el análisis que se realizó a 5 casas estrato 2 de la ciudad de Bogotá, se encontraron diversos escenarios, pues hay casas donde la entrada principal conecta directamente con la escalera que va al segundo piso, mientras hay casas donde se encontraban paredes entre 5 y 4 metros de distancia con relación a la puerta, debido a esto se decidió elaborar dos diseños uno que está orientado a instalarse fijamente a una pared y otro que cuenta con una apariencia de maseta que permite colocarlo en cualquier espacio de la casa, por otra parte en el análisis se identificó que la mayoría de casas no tiene tomas de corriente en la entrada principal, por lo que, se optó que la alarma debería contar con una batería o un porta pilas.
2. De los tres modelos probados se evidencio que EigenFace se presenta inicialmente como el mejor de los tres en cuanto a precisión, pero su alto índice en el valor de confianza es por mucho el mayor de todos, lo que no es un buen indicio, por otro lado, luego de reentrenar todos los modelos FisherFace, no solo mejoro considerablemente su índice de aciertos si no que su índice de confianza es el más cercano a cero, lo que es un buen indicador, también su velocidad de respuesta logra ser superior respecto a los otros dos modelos. En conclusión, se decide dejar como inteligencia artificial para la

propuesta de diseño el modelo FisherFace, pero es necesario que cuente con al menos 600 imágenes para cada persona en el banco de datos, también es importante recalcar que el modelo mejorara con la variedad de entornos y de luz en las imágenes.

3. En primer lugar, se toma en cuenta un esquema previo de una alarma ESP32-cam que toma fotos cuando detecta movimiento, de acuerdo a los requerimientos y al diseño presentado en la figura 23, se establece la posibilidad de integrar una batería o una caja de pilas de 5 volteos, luego se muestra como debe de ser la interacción entre el usuario y el bot, donde a través de comandos simples como: /star, /foto, se podrá dar instrucciones a la inteligencia artificial, en el diseño de la arquitectura la inteligencia artificial estará almacenada en el dispositivo, pues no ocupa mucho espacio y ya que el ESP32-cam permite micro SD de hasta 4G, se considera que es lo suficiente para almacenar la data perteneciente a los habitantes del hogar. Como conclusión se alcanzaron los objetivos propuestos pues se logra crear el diseño de la alarma, que está compuesto, por un esquema, un diagrama de casos de uso, un diagrama de la arquitectura, el diseño de la interacción con el bot y dos diseños de carcasas para la alarma.

Referencias

A. Andreev, A Doronin, V Kachenkova, B Norov, and Z Mirkhasilova. (2022). Fire alarm systems construction on artificial intelligence principles. https://www.e3s-conferences.org/articles/e3sconf/pdf/2023/02/e3sconf_conmechydro2023_04028.pdf

Adrián Sáez de la Pascua. (enero, 2019). Deep Learning para el reconocimiento facial de emociones básicas.

Alex Fernando Graces Nuñez. (enero, 2017). SISTEMA DE RECONOCIMIENTO FACIAL CON VISIÓN ARTIFICIAL PARA APOYAR AL ECU-911 CON LA IDENTIFICACIÓN DE PERSONAS EN LA LISTA DE LOS MÁS BUSCADOS. https://repositorio.uta.edu.ec/bitstream/123456789/24490/3/Tesis_t1189ec.pdf

Álvarez Salvador, R., & Bazán Prieto, C. (2022). Sistema de seguridad con reconocimiento facial en módulo ESP32. Mare Ingenii, 4(1), 43–52. https://doi.org/10.52948/mare.v4i1.684

Ángel Pisco Gómez, Julio Johnny Regalado Jalca, Jimmy Gutiérrez García , Omar Quimis Sánchez, Kleber Marcillo Parrales, Javier Marcillo Merino. (2017). FUNDAMENTOS SOBRE LA GESTIÓN DE BASE DE DATOS. https://books.google.es/books?id=H0VBDwAAQBAJ&lpg=PA7&ots=fXl_SIvD1C&dq=que%20es%20una%20base%20de%20datos&lr&hl=es&pg=PA7#v=onepage&q=que%20es%20una%20base%20de%20datos&f=false

Britti, Gonzalo. (jul, 2021). Servicios de video vigilancia hogareño con soporte de inteligencia artificial. http://hdl.handle.net/10908/18682

Caba Costales, Carlos Santiago. Jara Chavez, Caroline Viviana (mar, 2018) Reconocimiento y creación del modelo facial 3D mediante sistema de video aplicado a la seguridad usando inteligencia artificial http://dspace.espoch.edu.ec/handle/123456789/9198

Cámara de Comercio de Bogotá. (2022). Encuesta de Percepción y Victimización de Bogotá. https://www.ccb.org.co/observatorio/content/download/296024/file/Encuesta%20de%20Percepci%C3%B3n%20y%20Victimizaci%C3%B3n%20Bogot%C3%A1%202022.pdf?inLanguage=esl-CO&version=1

Carlos H. Esparza Franco, Christian Tarazona Ospina, Esdras E. Sanabria Cuevas, Daniel A. Velazco Capacho. (2015). RECONOCIMIENTO FACIAL BASADO EN EIGENFACES, LBHP Y FISHERFACES EN LA BEAGLEBOARD-xM. https://ojs.unipamplona.edu.co/ojsviceinves/index.php/rcta/article/view/395/364

Carrillo Delgado, Ronnie Eduardo, Arias Maldonado, Jose Elías. (septiembre, 2022) Desarrollo de un prototipo de Sistema de Domótica enfocado en la seguridad de una vivienda mediante una aplicación de Inteligencia Artificial en visión por computadora, en la ciudad de Guayaquil. http://repositorio.ug.edu.ec/handle/redug/65267

CEJ. (octubre, 2022). En 2022 se redujeron los hurtos a residencias 9%. https://cej.org.co/infografias/en-2022-se-redujeron-los-hurtos-a-residencias-9/

Cristhian Javier Delgado Fonseca. (2020). DESARROLLO DE UN PROTOTIPO DE HERRAMIENTA EN ENTORNO WEB QUE IMPLEMENTE TÉCNICAS DE INTELIGENCIA ARTIFICIAL CON FIN DE ANALIZAR TENDENCIAS DE INSEGURIDAD. https://repository.unab.edu.co/bitstream/handle/20.500.12749/16757/2020_Tesis_Cristian_Javier_Delgado.pdf?sequence=1&isAllowed=y

Claudio Peña. (2020). Arduino ID: Domina la programación y controla la placa. https://books.google.es/books?id=Xgv2DwAAQBAJ&lpg=PP1&ots=vNFWCgQz2Y&dq=que%20es%20arduino%20IDE&lr&hl=es&pg=PT7#v=onepage&q=que%20es%20arduino%20IDE&f=false

CORTÉS OSORIO, JIMY ALEXANDER; MEDINA AGUIRRE, FRANCISCO ALEJANDRO; MURIEL ESCOBAR, JOSÉ A. (diciembre, 210). SISTEMAS DE SEGURIDAD BASADOS EN BIOMETRÍA. https://www.redalyc.org/articulo.oa?id=84920977016

Daniela Ramírez Ariza. (2022). ¡Asegure bien su casa! Casi 7.000 viviendas fueron robadas este año en Bogotá. Caracol Radio. https://caracol.com.co/2022/12/30/asegure-bien-su-casa-casi-7000-viviendas-fueron-robadas-este-ano-en-bogota/

Eddie Meardon. (2023). ¿Qué son los diagramas de Gantt? https://www.atlassian.com/es/agile/project-management/gantt-chart

Electrónica de una. (julio, 2022). Alarma con Esp32 CAM y Telegram, https://github.com/electrodeuna/alarm-esp32cam

Engr Muhammad Farshan Siddiqui, Wagas Ahmed Siddiqui, Awais Khan Jumani. (marzo, 2020). Face Detection and Recognition System for Enhancing Security Measures Using Artificial Intelligence System. https://www.researchgate.net/profile/Awais-Jumani/publication/340183601_Face_Detection_and_Recognition_System_for_Enhancing_Security_Measures_Using_Artificial_Intelligence_System/links/5e7cc982a6fdcc139c089bc4/Face-Detection-and-Recognition-System-for-Enhancing-Security-Measures-Using-Artificial-Intelligence-System.pdf

Ernesto Tolocka. (julio, 2020). Probando el streaming de video con ESP32-CAM y Arduino IDE. https://www.profetolocka.com.ar/2020/07/15/probando-el-streaming-de-video-con-esp32-cam-y-aduino-ide/

Eugenio López Aldea. (2017). Raspberry Pi Fundamentos y Aplicaciones. https://books.google.es/books?id=mo6fDwAAQBAJ&dq=que+es+una+cabecera+GPIO&lr=&hl=es&source=gbs_navlinks_s

F. Escolano Ruiz, M. Á. Cazorla Quevedo, M. I. Alfonso Galipienso, O. Colomina Pardo, and M. Á. Lozano Ortega, “Inteligencia artificial: modelos, técnicas y áreas de aplicación.” p. 370, 2003.

Franco Gabriel Caballero Julián, Martín Vidal Reyes, Antonia López Sánchez, Carlos Alberto Jerónimo Ríos. (2017). RECONOCIMIENTO FACIAL POR EL MÉTODO DE EIGENFACES. https://pistaseducativas.celaya.tecnm.mx/index.php/pistas/article/view/1068/878

Fúnez Fernández, Eduardo. (mar, 2022) Diseño de un sistema de seguridad en el hogar basado en IoT y creación de prototipo. https://hdl.handle.net/10953.1/16437

González Godoy, C. A., & Salcedo Parra, O. J. (2017). Sistema de seguridad para locales comerciales mediante Raspberry Pi, cámara y sensor PIR. Revista Virtual Universidad Católica Del Norte, (51), 175–193.

Goñi, A. A. (2014, octubre 2). Tipos de Investigación científica. Franck Morales. Antropología para Todos. https://antropologiaparatodos.wordpress.com/2014/10/02/tips-de-investigacion/

Guerra Ruiz, Felipe. (junio, 2014). Diseño de un sistema de control demótico y video vigilancia supervisado por un teléfono móvil. http://hdl.handle.net/20.500.12404/5375

Guillermo. (2022). ESP32-Cam: Subir fotos a Google Drive. https://www.gsampallo.com/2019/10/13/esp32-cam-subir-fotos-a-google-drive/

Hugo Alberto Pelaez Ramos. (2019). Aplicación de inteligencia artificial como estrategia para la disminución del nivel de riesgo en seguridad residencial en el sector de Bocagrande (Cartagena de indias). https://repository.unimilitar.edu.co/bitstream/handle/10654/36267/Pel%C3%A1ezRamos%20HugoAlberto2020%20.pdf?sequence=1&isAllowed=y

Infobae. (mayo, 2023). Más de 6.000 viviendas fueron robadas en Bogotá. https://www.infobae.com/america/colombia/2022/12/31/mas-de-6000-viviendas-fueron-robadas-en-bogota/#:~:text=De%20acuerdo%20con%20las%20cifras,viviendas%20en%20toda%20la%20ciudad.

Jorge Díaz Fernández. (1999). Alarmas inteligentes en unidades de cuidados intensivos basada en redes neuronales. https://oa.upm.es/664/1/09199919.pdf

José Francisco Ávila-Tomás, Eduardo Olano-Espinosa, César Minué-Lorenzo, Francisco Javier Martínez-Suberbiola, Blanca Matilla-Pardo, María Encarnación Serrano-Serrano, María Victoria Güeto-Rubio y Grupo Dej@lo. (julio, 2020). Dejal@Bot: Un chatbot aplicable en el tratamiento de la deshabituación tabáquica. https://www.riecs.es/index.php/riecs/article/view/196/275

Juan Ángel Gámiz Caro y Javier Gámiz Caro. (2011). Ethernet como soporte de sistemas de control en red. https://www.tecnicaindustrial.es/wp-content/uploads/Numeros/79/1248/a1248.pdf

Juan Carlos Lopez Garcia. (2007). ALGORITMOS Y PRIGRAMACIÓN. http://libros.metabiblioteca.org/handle/001/169

Julián Cárdenas (2018). Investigación cuantitativa. https://refubium.fu-berlin.de/handle/fub188/22407

Karen Barrero. (2023). Bogotá actualizo su censo inmobiliario para 2023 ¡Aquí los detalles! Alcaldía de Bogotá. https://bogota.gov.co/mi-ciudad/hacienda/bogota-actualizo-su-censo-inmobiliario-para-2023-aqui-los-detalles

Luis Felipe Herrera Quintero. (2005). Viviendas inteligentes. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-56092005000200006

Méndez Paul, Ibarra Julio. (2014). Implementación de una red neuronal de convolución para el reconocimiento de poses en imágenes de rostros https://doi.org/10.18272/aci.v6i2.167

Michael Coole, Deborah Evans, Jennifer Medbury. (mayo, 2021). ARTIFICIAL INTELLIGENCE IN SECURITY: OPPORTUNITIES AND IMPLICATIONS. https://www.asisonline.org/globalassets/foundation/documents/digital-transformation-series/ai-guidance-document-final.pdf

OEA. (2009, agosto 1). OEA - Organización de los Estados Americanos: Democracia para la paz, la seguridad y el desarrollo. http://www.oas.org/ios/glossarydetails.aspx?lang=es&type=0&id=19

Oscar Enrique Lopez Guevara. (2020). Planteamiento de un algoritmo para la identificación de posibles delincuentes mediante reconocimiento facial en la ciudad de Bogotá. https://repository.udistrital.edu.co/bitstream/handle/11349/27966/LopezGuevaraOscarEnrique2020.pdf?sequence=1&isAllowed=y

Padilla Trillos, Samuel Arturo. (junio, 2022). Inteligencia artificial para gestión y atención de alarmas. https://repository.javeriana.edu.co/handle/10554/63702

Pat Kelly, Chair. (octubre, 2022). FACIAL RECOGNITION TECHNOLOGY AND THE GROWING POWER OF ARTIFICIAL INTELLIGENCE. https://www.ourcommons.ca/Content/Committee/441/ETHI/Reports/RP11948475/ethirp06/ethirp06-e.pdf

R. Álvarez y C. Bazá. (2022). Sistema de seguridad con reconocimiento facial en módulo ESP32. https://cipres.sanmateo.edu.co/ojs/index.php/mi/article/view/684/605

Raspberry Pi. (2023). Buy a Rasberry Pi 4 Model B. https://www.raspberrypi.com/products/raspberry-pi-4-model-b/

Reconocimiento facial con OpenCV. (s.f). https://docs.opencv.org/4.2.0/da/d60/tutorial_face_main.html#tutorial_face_credits

Rudy Chicas, Hugo Contreras, Ruth Cortez, Danny Gutierrez. (2004). Inteligencia artificial para el desarrollo de un sistema experto. https://ri.ues.edu.sv/id/eprint/13463/1/Investigaci%C3%B3n%20aplicada%20al%20%C3%A1rea%20de%20inteligencia%20artificial%20y%20desaarrollo%20de%20un%20sistema%20experto.pdf

Sabaté, J. (2015, octubre 21). Alarmas domésticas anti-robos: ¿funcionan de verdad o solo tienen un efecto placebo? elDiario.es. https://www.eldiario.es/consumoclaro/ahorrar_mejor/alarmas-quejas-seguridad-privada-securitas-prosegur-tyco_1_2461168.html

Superintendencia de Vigilancia y Seguridad Privada. (2021). Indicadores Financieros del sector de Vigilancia y Seguridad Privada 2021.

https://www.supervigilancia.gov.co/publicaciones/9822/indicadores-financieros-del-sector-de-vigilancia-y-seguridad-privada-2021/

Zhihan Lv, Liang Qiao, Amit Kumar Singh, Qingjun Wang. (22 julio 2021). AI-empowered IoT Security for Smart Cities. https://dl.acm.org/doi/abs/10.1145/3406115

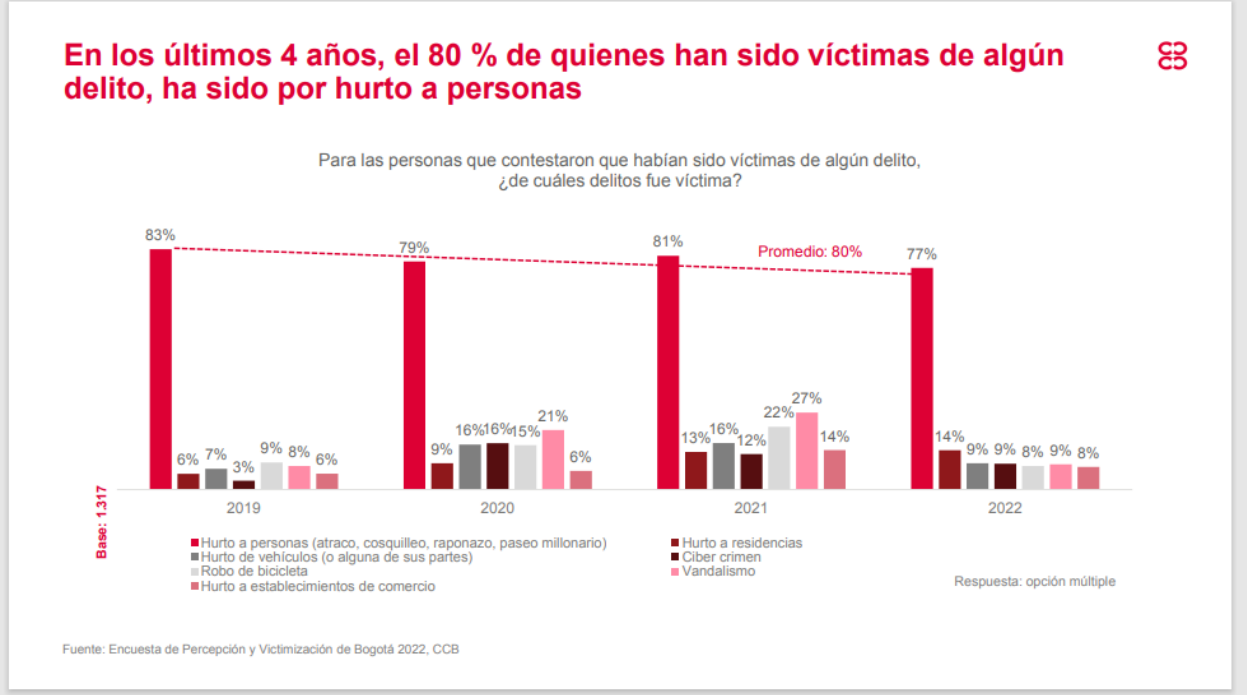
Zuolin Dong, Jiahong Wei, Xiayu Chen, Pengfei Zheng. (marzo, 2020). Face Detection in Security Monitoring based on Artificial Intelligence Video Retrieval Technology. https://www.researchgate.net/publication/340112248_Face_Detection_in_Security_Monitoring_Based_on_Artificial_Intelligence_Video_Retrieval_Technology

Anexos

A continuación, se comparte un fragmento de la Encuesta de Percepción y Victimización de Bogotá (2022) donde se puede evidenciar una gráfica que compara la variación de los delitos desde el año 2019 hasta el año 2022. Pese a que el índice de hurto a personas es el más alto se nota una reducción a través de los años, por otra parte, el segundo delito que más porcentaje presenta es el hurto a residencias, en contraste con el anterior este ha ido aumento a lo largo del tiempo, pues en el 2019 solo el 6% de los delitos correspondían a esta modalidad, sin embargo, para el año 2022 ya representa el 14%, lo que indica esta manera de delinquir va en aumento.

Figura 29

Grafica de delitos 2019 - 2022



Nota: Adaptado de "Encuesta de Percepción y Victimización de Bogotá" (p. 9), por Cámara de Comercio de Bogotá, 2022, Cámara de comercio de Bogotá

A continuación, se comparte un fragmento de los indicadores financieros del sector de vigilancia y seguridad privada 2021 donde se puede evidenciar una tabla que compara los ingresos operacionales de cada servicio de seguridad privada, desde el año 2019 hasta el 2021, en él se puede apreciar el incremento financiero que hay la seguridad privada, donde se puede concluir que hay una alta demanda por este tipo de servicios.

Figura 30

Grafica de ingresos del sector de seguridad privada 2019 - 2021

INGRESO OPERACIONALES DEL SECTOR			
Tipo de servicio	**2021**	**2020**	**2019**
COOPERATIVA DE VIGILANCIA Y SEGURIDAD PRIVADA	662.720	650.577	622.521
EMPRESA ARRENDADORA DE VEHÍCULOS BLINDADOS	114.100	94.192	86.672
EMPRESA ASESORA, CONSULTORA E INVESTIGADORA EN VIGILANCIA Y SEGURIDAD PRIVADA	49.311	53.801	65.889
EMPRESA BLINDADORA	386.663	316.404	332.328
EMPRESA DE TRANSPORTE DE VALORES	735.630	643.611	716.665
EMPRESA DE VIGILANCIA Y SEGURIDAD PRIVADA CON/SIN ARMAS	10.862.130	10.008.465	9.690.535
ESCUELA DE CAPACITACIÓN Y ENTRENAMIENTO EN VIGILANCIA Y SEGURIDAD PRIVADA	50.845	47.779	60.080
Total	**12.861.401**	**11.814.851**	**11.574.690**

Nota: Adaptado de "indicadores financieros del sector de vigilancia y seguridad privada 2021" (p. 3), por Superintendencia de Vigilancia y Seguridad Privada, 2021, SuperVigilancia