UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN
MENCIÓN: ELECTRÓNICA Y AUTOMATIZACIÓN
Resolución: RPC-SO-09-No.265-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título del proyecto:
Inteligencia artificial para videovigilancia y control de acceso
Línea de Investigación:
Ciencias de la Ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Ingeniería, industria y construcción
Autor/a:
Ángel Alberto Idrobo Vivar
Tutor/a:
Mgs. René Ernesto Cortijo Leyva

Quito – Ecuador

2023

APROBACIÓN DEL TUTOR

Yo, **René Ernesto Cortijo Leyva**, con C.I: **1719010108** en mi calidad de Tutor del proyecto de investigación titulado: **Inteligencia artificial para videovigilancia y control de acceso,**

Elaborado por: **Ángel Alberto Idrobo Vivar**, de C.I: **0603035650**, estudiante de la Maestría: **ELECTRÓNICA Y AUTOMATIZACIÓN**, resolución: **RPC-SO-09-No.265-2021**, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., 4 de septiembre de 2023

RENE ERNESTO CORTIJO LEYVA

Firmado digitalmente por RENE ERNESTO CORTIJO LEYVA
Fecha: 2023.10.06 18:13:39 -05'00'

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Ángel Alberto Idrobo Vivar, con C.I: **0603035650**, autor/a del proyecto de titulación denominado: **Inteligencia artificial para videovigilancia y control de acceso**. Previo a la obtención del título de Magister en: **ELECTRÓNICA Y AUTOMATIZACIÓN.**

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., 4 de septiembre de 2023

Firmado electrónicamente por:
ANGEL ALBERTO
IDROBO VIVAR

Firma

Tabla de contenidos

APROBACIÓN DEL TUTOR	2
DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE	3
INFORMACIÓN GENERAL	1
Contextualización del tema	1
Problema de investigación	2
Objetivo general	3
Objetivos específicos	3
Vinculación con la sociedad y beneficiarios directos:	3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO	5
1.1. Contextualización general del estado del arte	5
1.2. Proceso investigativo metodológico	9
CAPÍTULO II: PROPUESTA	10
2.1. Fundamentos teóricos aplicados	10
2.1.1. Cámaras de videovigilancia	10
2.1.2. Sistemas de control de acceso	11
2.1.3. Control de acceso mediante reconocimiento facial	14
2.1.4. Inteligencia artificial	15
2.1.5. Redes neuronales convolucionales (CNN)	18
2.1.6. Detección de armas mediante inteligencia artificial (IA)	21
2.2. Descripción de la propuesta	22
2.3. Validación de la propuesta	28
2.4. Matriz de articulación de la propuesta	30
2.5. Análisis de resultados. Presentación y discusión.	33
CONCLUSIONES	33
RECOMENDACIONES	34
BIBLIOGRAFÍA	35

Índice de tablas

Tabla 1 Herramientas tecnológicas a emplear. 28

Tabla 2 Descripción de perfil de validadores. 41

Tabla 3 Criterios de valuación 41

Tabla 4 Evaluación según importancia y representatividad 42

Tabla 5 Matriz de articulación. 43

Tabla 6 Datos de personas desconocidas en el sistema. 51

Tabla 7 Personas habitantes del hogar. 52

Índice de figuras

Figura 1 Cámaras de videovigilancia. 10
Figura 2 Control de acceso basado en tarjetas RFID. 11
Figura 3 Control de acceso basado en biometría. 12
Figura 4 Control de acceso basado en reconocimiento facial. 13
Figura 5 Control de acceso basado en reconocimiento de voz. 14
Figura 6 Usos de la inteligencia artificial. 16
Figura 7 Esquema de una CNN. 20
Figura 8 Flujo funcional del sistema de videovigilancia y control de acceso. 25
Figura 9 Configuración PuTTY. 30
Figura 10 Terminal de Raspberry. 31
Figura 11 Prueba de reconocimiento facial. 32
Figura 12 Conteo para puerta abierta. 32
Figura 13. Configuración para el tópico 33
Figura 14 Imágenes para el entrenamiento del modelo de inteligencia artificial. 34
Figura 15 Detección de armas 35
Figura 16 Reconocimiento de placa vehicular.. 36
Figura 17 Conversión de imagen a binario para fácil detección de la placa vehicular. 36
Figura 18 Negativo de la imagen binarizada. 37
Figura 19 Identificación de los dígitos correspondientes a la placa vehicular 37
Figura 20 Impresión en pantalla de los dígitos obtenidos de la detección de placas. 38
Figura 21 Plataforma Telegram para el envío de notificaciones de alerta. 39
Figura 22 *Reconocimiento facial de uno de los habitantes del domicilio.* 46
Figura 23 Pausa de 5 segundos para evitar falsos positivos en reconocimiento facial. 46
Figura 24 Simulación de una persona sospechosa ante la cámara de videovigilancia 47
Figura 25 Detección de persona desconocida 48
Figura 26 Notificación de alerta en la plataforma de Telegram. 48
Figura 27 Notificaciones enviadas por el sistema a Telegram. 49
Figura 28 Detección de dígitos de la placa de un vehículo. 50
Figura 29 Análisis en el sistema para reconocimiento de placas. 50
Figura 30 Control de acceso de vehículo al estar registrado en base de datos. 51

INFORMACIÓN GENERAL

Contextualización del tema

En la actualidad se ha incrementado el uso de sistemas con inteligencia artificial para diferentes ámbitos, como son en el área educativa, empresarial, industrial y también en el área de seguridad, mediante esto uno de los principales indicios para utilizar inteligencia artificial se desarrolla en la videovigilancia.

La inteligencia artificial en la videovigilancia busca poder realizar acciones previamente cargadas en un algoritmo para poder reconocer desde intrusos o personas no autorizadas hasta el accionamiento de actuadores que permitan el ingreso de las personas autenticadas o enviar una alerta si se encuentra ante una posible actividad delictiva.

Muchas empresas, hogares, y locales están comenzando a implementar sistemas que utilicen inteligencia artificial para vigilar su espacio ya sea de domicilio o de trabajo, y así poder tener un control de lo que sucede a su alrededor y tomar medidas referentes a la información obtenida mediante un sistema de videovigilancia aplicando técnicas de IA.

En el barrio Eloy Alfaro perteneciente a la ciudad de Shushufindi provincia de Sucumbíos, se encuentra el domicilio para instalar el sistema de videovigilancia con inteligencia artificial. Es una casa individual, la misma que cuenta también con un departamento de arrendamiento, en la parte exterior tienen un portón que permite el ingreso al domicilio. La actual propiedad no cuenta con un sistema de videovigilancia instalado, y tampoco cuenta con algún otro medio de seguridad, por lo cual es propenso a sufrir diversas acciones delictivas, al no tener videovigilancia no se tiene una monitorización de las personas que se encuentran en sus inmediaciones o intentan ingresar al domicilio, tampoco se verifica a las personas que ingresan al departamento de arriendo ya sean estos familiar o amigos de los inquilinos o a su vez personas que se hacen pasar por alguno de ellos, esto ha influido que en ocasiones anteriores se evidencie intentos de ingreso de gente no autorizada o personas ajenas a las se les fue entregado el departamento, provocando problemas como la pérdida de diferentes artículos que se encontraban dentro de la propiedad. Al usar un sistema de videovigilancia se elimina la presencia permanente de una persona que cuide el hogar y al momento de aplicar técnicas de inteligencia artificial se puede realizar reconocimiento facial de las personas que se acerquen al portón y determinar si puede ingresar o no al domicilio.

Problema de investigación

La sociedad actual, se enfrenta a una alarmante escalada de la delincuencia en todo el país, esto ha generado mucha inseguridad tanto en los espacios públicos como en los privados, ya que delincuentes intentan ingresar a los domicilios con el fin de saquear pertenencias de valor, secuestrar a personas inocentes o en el peor de los casos atentar contra su integridad. Esta preocupante situación se traduce en una sensación de vulnerabilidad para todas las personas de bien que ya ni en su propio domicilio pueden sentirse a salvo. (Mella, 2023)

En el barrio Eloy Alfaro perteneciente a Shushufindi también se ha evidenciado un incremento en el número de actos delictivos en los últimos meses, por lo cual no ha sido inmune a esta problemática. Esto ha generado en la población un sentimiento de vulnerabilidad y de inseguridad debido a factores como peleas en las calles, robos a mano armada, y en gran medida el ingreso ilegal de personas a diversos domicilios del sector, lo que ha influido significativamente en la disminución de la tranquilidad y bienestar de los moradores creando una necesidad de cuidar sus negocios y propiedades.

El domicilio personal ubicado en el barrio Eloy Alfaro, carece de un sistema de videovigilancia, lo que conlleva a diversos peligros significativos para sus residentes, ya que, al no contar con una cámara de seguridad no se puede realizar una monitorización de las inmediaciones de la propiedad, esta vivienda queda expuesta a diversas amenazas mencionadas previamente. Pero no obstante según la problemática actual del sector no basta solo con un sistema de videovigilancia sino también aplicar técnicas de inteligencia artificial al mismo, ya que la ausencia de este sistema representa una limitación significativa en su seguridad ya que no se puede activar o enviar una notificación cuando personas no reconocidas están merodeando el sector, y no se cuenta con un acceso automático con el reconocimiento de los habitantes del hogar. De igual forma ayuda a que no se necesite una persona constantemente monitoreando las cámaras.

Por todo lo expuesto anteriormente es indispensable implementar un sistema de videovigilancia que además incorpore inteligencia artificial para generar alertas cuando personas sospechosas se encuentran en las inmediaciones del hogar y en caso contrario cuando se encuentren los residentes fuera del domicilio se pueda activar su ingreso, también que se pueda tener una monitorización del entorno del hogar en tiempo real sin la necesidad de tener constantemente una persona presente revisando las cámaras de la vivienda.

Objetivo general

Desarrollar un sistema de videovigilancia y control de acceso mediante inteligencia artificial para resguardar la seguridad del domicilio personal.

Objetivos específicos

Contextualizar los fundamentos teóricos sobre inteligencia artificial.

Determinar los elementos electrónicos para el sistema de videovigilancia.

Desarrollar el algoritmo de inteligencia artificial mediante Python.

Validar el correcto funcionamiento del sistema aplicado en el domicilio.

Vinculación con la sociedad y beneficiarios directos:

Representa un aporte social, ya que, al implementar un sistema de videovigilancia con inteligencia artificial en el domicilio, este contribuirá a mejorar la seguridad y protección de los residentes del hogar, así como también del entorno cercano. Además, al ser un sistema completamente nuevo en la zona este generará interés y conciencia en los otros residentes del barrio Eloy Alfaro sobre la importancia de tener una videovigilancia en el hogar en la época actual donde existe tanta inseguridad. Al implementar este sistema de inteligencia artificial para videovigilancia se espera reducir significativamente el riesgo al que se exponen los habitantes del hogar, en comparación con otras viviendas en el sector, ya que mediante una vigilancia constante y efectiva los delincuentes y personas malintencionadas se verán disuadidos de intentar acceder a la propiedad. La presencia de este sistema en el domicilio actúa como un elemento disuasorio en el sentido de que los delincuentes reconsiderarán sus acciones y se verán disuadidos de ingresar a una propiedad con un sistema de videovigilancia con técnicas de inteligencia artificial.

Además de los beneficiarios directos que vienen siendo los residentes del hogar, la implementación de este sistema de videovigilancia también tiene cierta incidencia con la comunidad. Se prevé que, una vez instalado el sistema en el domicilio establecido, se lleve a cabo una socialización con los dirigentes del barrio en donde se les hará conocer el funcionamiento y aplicación de este sistema, con el fin que, al validar su funcionamiento, lleguen a fomentar en los habitantes del barrio Eloy Alfaro el cuestionamiento sobre el tema y con ello la inclinación por conocer o adquirir este tipo de sistemas de seguridad. La divulgación de los resultados de este sistema también se logrará con la ayuda de redes sociales, lo que fomentará un sentido de comunidad informada y comprometida con el tema de la seguridad en sus barrios.

Así mismo, es fundamental compartir la investigación y resultados con la comunidad científica con el propósito de dar a conocer nuestra investigación, como también, que sirva de guía y base para futuros estudios investigativos y experimentales. Para lograrlo, se planea redactar un artículo científico el cual se pretende sea aprobado para la publicación en revistas de tecnología, seguridad y ciencias de la computación, asegurando de esa manera que el estudio realizado tenga un alcance a una comunidad compuesta por expertos y profesionales

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

En el ámbito de la seguridad y la tecnología, la combinación de videovigilancia e inteligencia artificial ha emergido como una evolución significativa en la forma en que se abordan los desafíos de supervisión y prevención. Por este motivo se han desarrollado diversos proyectos con este enfoque, a continuación, se muestran varias fuentes que han sido de gran ayuda y sustento para la elaboración del proyecto.

La revista Scielo publica el 1 de Junio del 2023, (Cataño-Añazco et al., 2023) un trabajo titulado La inteligencia artificial y la videovigilancia en la predicción y detección de delitos en espacio-tiempo: una revisión sistemática, desarrollado por Hernán Barragán, Kevin Cataño, Mauricio Sevincha y Obed Vargas, en este proyecto se exponen los delitos que se han incrementado en Bogotá, utilizan una metodología de enfoque descriptivo-cualitativo ya que realizaron su investigación en diferentes fuentes académicas en donde se determinó la importancia de la inteligencia artificial aplicado a la video-vigilancia para la predicción de delitos. Usaron algoritmos de inteligencia artificial enfocados en espacio-tiempo para predecir y detectar puntos críticos de la delincuencia en la ciudad, este método de inteligencia artificial se enfoca principalmente en una ayuda para la vigilancia policial ya que proporciona la identificación de lugares en donde se manifiesta un mayor número de incidentes. La inteligencia artificial aplica redes neuronales para la detección de puntos críticos de la delincuencia, estos algoritmos se implementaron en diversos delitos como varios robos suscitados en California, de este medio empírico se estableció que tiene una efectividad del 73,9% en la videovigilancia. Según los datos obtenidos del proyecto usando métodos inteligentes presentan que es de gran ayuda a la hora de la detección de crímenes en tiempo y espacio, pero que aún se deben realizar más investigaciones para medir de una mejor manera su eficacia. Este proyecto presenta una ayuda importante al momento de entender el enfoque de la inteligencia artificial usando redes neuronales a los medios de seguridad existentes en el mercado, y que se debe manejar de la mejor manera para evitar fallos al momento de aplicarla en videovigilancia.

Otro estudio importante para el presente proyecto fue realizado en la Universidad de San Andrés, (Britti, 2021) con el tema denominado Servicios de video vigilancia hogareño con soporte de inteligencia artificial, realizado por Gonzalo Britti en donde se presenta la utilización de una inteligencia artificial mediante aprendizaje profundo (deep learning), que es una técnica de aprendizaje automático que utiliza redes neuronales, realizan el estudio enfocándose en la base de datos de personas sospechosas y las redes de contactos de confianza, para la

videovigilancia aplican cámaras de venta en el mercado, estaciones de proceso y todo lo referente al sistema de vigilancia ya que el software con inteligencia artificial puede ser aplicado a todos estos dispositivos sin ningún problema. En el software que propone el autor se desarrolla el reconocimiento facial y una distinción con anomalías de detección, aquí se enfoca en que el sistema "pre conoce" la fisionomía de un rostro, entonces si al momento de la detección se determina una anomalía que impide la detección del rostro, este debe meta-entrenarse para entender los comportamientos que no hayan sido enfocados en el algoritmo o estén fuera de lugar. El autor usa una arquitectura denominada Edge Computing que se enfoca en optimizar el tiempo de respuesta al momento de realizar un reconocimiento facial y también en la optimización del volumen de datos usados en el sistema. También realizan el análisis de este sistema como puede ser adoptado y que tenga un impacto de negocio acorde a su implementación y su acoplamiento con las comunicaciones IoT y 5G, logrando así incrementar el sistema en cada hogar. Uno de los principales aspectos que se tomaron de este proyecto fue que es posible realizar una intervención tecnológica en el área de seguridad mediante cámaras ya que se compone de diversos parámetros como la tecnología que se encuentra ampliamente comercial en el mercado.

El tema de proyecto de fin de grado publicado en la Universidad Politécnica de Madrid, (Gutiérrez Santamarta, 2021) llamado "Videovigilancia IA" realizado por Diego Gutiérrez que fue implementado en un edificio de la ciudad de Madrid, desarrolla la creación de un sistema de inteligencia artificial, en donde utilizan cámaras IP para acceder a su contenido en tiempo real mediante la dirección que tiene cada una de las cámaras en la red local, aquí interviene directamente la inteligencia artificial al momento de marcar a las personas que aparezcan en las cámaras con el objetivo de asignarle un identificador el cual no se repetirá y realizar su seguimiento en el lugar que fue implementado el sistema. Utilizaron el sistema de TinyYOLO v2.7 el cual es un modelo ya existente para la detección de personas, y mediante la realización de un algoritmo se desarrolló el enfoque para el tracking de las personas. La arquitectura que se plantea en este proyecto es el del cliente-servidor, un cliente son los diversos dispositivos que interactúan con el sistema de videovigilancia mientras que el servidor compone toda columna vertebral del sistema enfocándose en la recolección y procesamiento de los datos. El autor concluye que el proyecto fue de gran eficiencia para el edificio y se ha implementado la mayor parte del tracking de personas que se movilizan dentro de la propiedad y que algunas funciones no se han podido implementar dejando abierta para futuros proyectos. Esta investigación aporta en gran medida al trabajo de investigación en la forma en que se puede utilizar cámaras IP para poder obtener su contenido y así aplicar las técnicas de reconocimiento facial al mismo,

también nos presenta algoritmos ya establecidos y que pueden ser una pauta importante para el proyecto del presente trabajo.

Amores Heredia (Amores, 2017), publica su proyecto titulado "Reconocimiento de imágenes en frames de vídeo utilizando redes neuronales". En primer lugar, se enfoca en utilizar el software Matlab, específicamente la herramienta AlexNet Toolbox, la cual es una herramienta para la creación de redes neuronales. Aquí, realiza el entrenamiento en las últimas 3 capas de la red, permitiendo que el algoritmo clasifique únicamente personas y vehículos. Además, el algoritmo es capaz de eliminar el fondo del video para un procesamiento más efectivo de los frames. Para lograr todo esto, utiliza redes neuronales convolucionales (CNN) con el propósito de clasificar las diversas imágenes reconocidas como parte de una secuencia de cuadros obtenidos de un video. Dicho video se obtuvo mediante una cámara de videovigilancia. El autor empleó un total de aproximadamente 300 imágenes para entrenar la red neuronal. Luego, creó una base de datos para las imágenes, divididas en secciones correspondientes a autos y personas. Posteriormente, llevó a cabo una prueba de efectividad del algoritmo, obteniendo un 100% de eficiencia en la clasificación de los frames. Realizaron diversas pruebas durante un período de 3193 segundos, en las cuales evidenciaron el reconocimiento y clasificación de las personas y autos que pasaban por el área cubierta por la cámara de videovigilancia, logrando una precisión del 100% en la "Mini-Batch Accuracy". Este proyecto aporta en términos de cómo crear un modelo de inteligencia artificial mediante programación, así como en la forma de segmentar en frames los videos capturados por una cámara de videovigilancia para posteriormente llevar a cabo el reconocimiento de los objetos presentes en ellos.

Según un estudio realizado en la Universidad Tecnológica Israel (Changotasig Yánez, 2023), las redes neuronales convolucionales son consideradas como una forma de red neuronal debido a su configuración estratificada. Operan descomponiendo las imágenes que son sometidas a análisis, esto con el propósito de modificarlas y generar distintas resoluciones. Este proceso tiene como objetivo destacar los atributos elementales de las imágenes, como brillo y bordes, junto con otras propiedades únicas de cada imagen.

Un estudio importante para el presente proyecto fue realizado en la Escuela Superior Politécnica de Chimborazo (Caba Costales & Jara Chávez, 2018), denominado “Reconocimiento y creación del modelo facial 3D mediante sistema de video aplicado a la seguridad usando inteligencia artificial”, realizado por Carlos Caba y Caroline Jara en la ciudad de Riobamba, en el cual se presenta la creación de un modelo de inteligencia artificial aplicando lógica difusa, la misma que se enfoca en el tipo Mamdani y deffuzificador centroide, con lo cual se usa para

poder determinar la similitud existente entre el usuario y la información almacenada en la base de datos, los autores utilizan filtros Gabor para la elaboración de los vectores que representa los rostros de las personas. Al momento de tener más precisión el sistema de inteligencia artificial tiene el ingreso de diversos parámetros como imágenes del rostro total, nariz, ojos y fotos de perfil y mediante distancia euclidiana realizan las comparaciones. Utilizaron MySQL como el gestor de base de datos y usaron elementos electrónicos como Arduino para la comunicación con el software de Matlab y realizar el modelado facial en 3D. Las pruebas de funcionamiento los realizaron en base a la norma ISO 9126 en donde determinaron que el sistema tiene un porcentaje de funcionalidad del 84% de igual forma tiene un 84% de usabilidad y por último cuenta con un 80% de eficiencia. Los autores concluyen que al utilizar un algoritmo de inteligencia artificial para la selección del usuario se evitan errores de identificación, por lo cual expresan que se debe tomar en consideración el tiempo de respuesta para que el algoritmo no genera falsos positivos. Este proyecto aporta en la investigación referente a los elementos electrónicos que se pueden usar y el sistema de reconocimiento facial para obtener el reconocimiento de personas.

En este contexto, se requiere la implementación de un sistema de videovigilancia aplicando técnicas de inteligencia artificial, para realizar el reconocimiento facial de las personas que se acerquen al domicilio y realizar alguna acción según la información obtenida mediante el algoritmo de IA. La información presentada en los trabajos es relevante para poder seleccionar las cámaras óptimas para la video-vigilancia, así como seleccionar el mejor sistema de inteligencia artificial para este caso.

Según plantea un estudio realizado en la Universidad Tecnológica Israel (Guerrero Moreno, 2017), la implementación de sistemas de videovigilancia genera un notable fortalecimiento del control y la seguridad en entornos. Esta tecnología posibilita una supervisión constante, independientemente de la ubicación del usuario. Ya sea a través de dispositivos móviles, computadoras fijas o portátiles, e incluso en pantallas de televisores domésticos, se puede mantener un monitoreo continuo. Un beneficio primordial radica en la mejora de la seguridad, y todo esto sin requerir la contratación de personal adicional. La habilidad de vigilar las instalaciones de manera continua durante las 24 horas del día actúa como un disuasivo ante posibles actividades delictivas y ofrece una respuesta inmediata en caso de incidentes. Esta rapidez en la respuesta resulta esencial para mitigar los intentos de robo u otras situaciones de emergencia.

1.2. Proceso investigativo metodológico

En el presente trabajo se propone el desarrollo de un sistema de videovigilancia mediante inteligencia artificial, a través de una investigación científica en donde interviene la investigación aplicada y tecnológica, tal como indica (Esteban Nieto, 2018)

Para llevar a cabo correctamente esta investigación se aplica el método de investigación documental ya que se realiza una revisión bibliográfica y hemerográfica, ayudando así a obtener una revisión documental de diversos casos de estudio referente al tema planteado, haciendo un análisis de las tecnologías utilizadas para poder seleccionar las herramientas necesarias para el desarrollo del presente proyecto.

Los datos recopilados incluyen detalles técnicos específicos sobre los equipos de hardware y software necesarios, así como las condiciones de operación requeridas para implementar la solución tecnológica más apropiada para las condiciones del sistema.

Para establecer el algoritmo de inteligencia artificial se utilizó el método de investigación cualitativa, a través de la revisión en diferentes fuentes información referente al tema, para definir el método adecuado para la videovigilancia con inteligencia artificial, y de igual forma conocer los datos de los elementos electrónicos a ser utilizados, se usó la técnica de observación no participante, ya que de esta manera se puede saber qué acción realiza el cierto procesamiento de los datos en el algoritmo y poder empezar a dilucidar cómo funcionará la inteligencia artificial.

Finalmente, la metodología que se ha optado por plantear para la evaluación de los resultados de este proyecto se basa en la realización de un enfoque sistemático y riguroso capaz de identificar fallos. El proceso comienza con la selección de una muestra de fotografías en las que se incluya diversas situaciones de videovigilancia y control de acceso, dichas imágenes serán identificadas respectivamente y empleadas para desarrollar y a su vez entrenar un modelo de inteligencia artificial utilizando lenguaje de programación Python. La validación del sistema se llevará a cabo mediante pruebas métricas de precisión, para posteriormente, efectuar la aplicación del sistema en un entorno real en donde se pueda recopilar datos y con ello evaluar su funcionamiento. La evaluación además incluirá análisis estadísticos para medir la eficacia de la detección de situaciones sospechosas a través del reconocimiento de personas que posean una base experimental de datos en donde se evalúe también márgenes de error e intervalos de confianza.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

Para el desarrollo del presente proyecto es necesario conocer las definiciones de los elementos a utilizar, así como también las tecnologías con las cuales se trabajará para la construcción del sistema.

2.1.1. Cámaras de videovigilancia

Las cámaras de videovigilancia son dispositivos electrónicos los cuales cumplen la función de capturar imágenes en tiempo real, para realizar una monitorización de un lugar determinado, estas cámaras cumplen un papel importante en el área de seguridad, ya que ayudan a la prevención de delitos o en otros casos al reconocimiento de delincuentes. Como se observa en la figura 1, hay diferentes tipos de cámaras de video las cuales pueden ser de diferentes tipos, ya sean analógicas, digitales, cámaras ip entre otras. (Tipos de cámara de vigilancia para casa, 2021)

Las cámaras de videovigilancia desempeñan un papel fundamental en la seguridad al disuadir delitos, facilitar investigaciones criminales y gestionar emergencias. A lo largo del tiempo, han evolucionado desde sistemas analógicos a digitales, con mejoras en resolución y funcionalidades como visión nocturna y térmica. Estas mejoras han fortalecido su eficacia en la prevención y respuesta a situaciones de riesgo, contribuyendo a la seguridad pública y la gestión de espacios.

Figura 1
Cámaras de videovigilancia.

Nota: El gráfico representa los diferentes tipos de cámaras de videovigilancia existentes en el mercado. Tomado de (*Tipos de cámara de vigilancia para casa*, 2021)

2.1.2. Sistemas de control de acceso

Un sistema de control de acceso es una solución tecnológica que está netamente diseñada para regular y controlar el acceso de individuos a una cierta ubicación física, como un domicilio, edificio, institución, área restringida o instalación. El objetivo principal de estos sistemas es mejorar la seguridad y controlar quién tiene acceso a un determinado lugar.

Un sistema de control de acceso es un dispositivo que, basándose en la validación previa de identidad, facilita la entrada a un recurso específico. Hay diversas modalidades para llevar a cabo el control de acceso. Por ejemplo, existen enfoques basados en software que exigen la introducción de una contraseña, así como sistemas que emplean huellas dactilares y reconocimiento facial, entre otras opciones. (Villegas, s. f.)

Existen varios tipos de sistemas de control de acceso, cada uno diseñado para satisfacer necesidades específicas en función de la seguridad y la comodidad. Algunos de los sistemas de control más conocidos son:

Basados en tarjetas o tarjetas RFID

Estos sistemas utilizan tarjetas físicas o etiquetas RFID (identificación por radiofrecuencia) para permitir o denegar el acceso. Los usuarios presentan sus tarjetas a lectores de tarjetas para autenticarse.

El sistema de control de acceso basado en RFID incluye todas las características del sistema convencional de control de acceso, pero además posibilita el tránsito rápido de Múltiples individuos al mismo tiempo, al mismo tiempo que registra automáticamente los datos personales de cada persona que ingresa o vende. Cuando una persona con una tarjeta RFID cruza la puerta, el sistema recopila de manera automática la información de la tarjeta sin necesidad de intervención manual, lo que simplifica considerablemente la administración del control de acceso. («RFID Para La Gestión Del Control de Acceso Que Le Gustaría Saber», s. f.)

Figura 2
Control de acceso basado en tarjetas RFID.

Nota: El gráfico representa el acceso mediante tarjeta RFID. Tomado de («RFID Para La Gestión Del Control de Acceso Que Le Gustaría Saber», s. f.)

Biometría

Estos sistemas se basan en características físicas únicas de los usuarios, como huellas dactilares, iris, reconocimiento facial o voz, para autorizar el acceso. Son altamente seguros debido a la singularidad de las características biométricas.

La voz, el patrón del iris ocular, las huellas dactilares e incluso las características vocales son atributos únicos para cada individuo. Esto posibilita la identificación de empleados de manera inequívoca y segura. Además, permite habilitar la autenticación biométrica, donde el acceso se concede mediante reconocimiento de características biométricas en lugar de depender de contraseñas o tarjetas. Estos últimos, en última instancia, no garantizan una seguridad total debido a problemas como el robo de contraseñas, descubiertos u olvidos. El sistema de control de personal basado en huella digital representa uno de los sistemas de acceso biométrico más ampliamente utilizados. Sin embargo, existen numerosas alternativas igualmente interesantes que pueden operar en conjunto con software de administración.(Manuel, 2021)

Figura 3
Control de acceso basado en biometría.

Nota: El gráfico representa el acceso mediante biometría dactilar. Tomado de (Planet, s. f.)

Sistemas de reconocimiento facial

Utilizan tecnología de cámaras y algoritmos de procesamiento de imágenes para identificar y autenticar a las personas en función de sus características faciales únicas.

La identificación de rostros es un tema significativo en el campo de la visión por computadora, en el que los expertos han dedicado largos años de estudio. En la actualidad, los algoritmos para detectar rostros pueden funcionar eficazmente en hardware simple, como

nuestras computadoras personales. Es posible lograr esto mediante el uso de la librería de Python llamada OpenCV para desarrollar un detector de rostros, aprovechando la cámara web de un ordenador. La idea central detrás de estos algoritmos reside en el hecho de que todos los rostros humanos comparten ciertas características comunes. (Briones Gárate, 2020)

Figura 4

Control de acceso basado en reconocimiento facial.

Nota: El gráfico representa el acceso mediante sistema de reconocimiento facial. Tomado de (*CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL + CAMA[...]*, s. f.)

Sistemas de reconocimiento de voz

Estos sistemas analizan patrones y características únicas en la voz de un usuario para autenticar su identidad.

El control de acceso por reconocimiento de voz es un método avanzado de autenticación biométrica que se basa en las características vocales únicas de una persona para permitir el acceso a áreas restringidas. El proceso implica la captura y análisis de la voz del usuario para crear una plantilla única almacenada en una base de datos. Al intentar acceder, la voz del usuario se compara con la plantilla para otorgar o denegar el acceso. Aunque ofrece seguridad y comodidad, desafíos como el ruido ambiental y la calidad de los datos pueden afectar su precisión.

Figura 5

Control de acceso basado en reconocimiento de voz.

Nota: El gráfico representa el control de acceso mediante reconocimiento de voz. Tomado de (Cornieles, 2019)

2.1.3. Control de acceso mediante reconocimiento facial

El reconocimiento facial aplicado al control de acceso es una tecnología avanzada que permite identificar y autenticar a individuos mediante la captura y análisis de características únicas de sus rostros. Este proceso implica la utilización de algoritmos de visión por computadora y aprendizaje profundo, como redes neuronales convolucionales (CNN), para extraer y representar patrones faciales distintivos. Durante la programación, se adquieren imágenes faciales a través de cámaras de alta resolución, que luego son preprocesadas para mejorar la calidad y normalizar la iluminación. Las características faciales extraídas se comparan con una base de datos previamente registrada, y se utiliza una métrica de similitud, como la distancia euclidiana en un espacio de características, para determinar la coincidencia. Este enfoque proporciona un alto grado de precisión y seguridad en el control de acceso, permitiendo una gestión eficiente y sin contacto en entornos donde la seguridad es primordial, como instalaciones gubernamentales, corporativas o de alta seguridad. Sin embargo, es crucial implementar medidas adecuadas para garantizar la privacidad de los individuos y abordar posibles sesgos propios de los datos de entrenamiento.

El reconocimiento facial es un paso que va más allá de solo la detección, ya que no solo implica encontrar rostros, sino también identificar a quién pertenece cada rostro. Aquí hay algunos métodos y algoritmos utilizados para el reconocimiento facial:

- Eigenfaces: Este enfoque utiliza el análisis de componentes principales (PCA) para reducir la dimensionalidad de las imágenes de rostros y luego encuentra vectores propios

(eigenfaces) que representan características distintivas. La similitud entre caras propias se utiliza para el reconocimiento.

- Fisherfaces (LDA): Similar a Eigenfaces, Fisherfaces utiliza análisis lineal de discriminación (LDA) para maximizar la separación entre clases y mejorar la precisión del reconocimiento.

- Redes Neuronales Convolucionales (CNN): Al igual que en la detección facial, las CNN también se han aplicado al reconocimiento facial. Estas redes pueden aprender automáticamente características discriminativas de los rostros y clasificarlos en diferentes categorías.

- Patrones binarios locales (LBP): LBP es un método que se enfoca en los patrones locales de textura en una imagen. Es ampliamente utilizado para describir características locales de un rostro y se puede usar en combinación con algoritmos de clasificación para el reconocimiento

- FaceNet y DeepFace: Estas son arquitecturas de redes neuronales profundas especialmente diseñadas para el reconocimiento facial. Utilizan modelos de redes neuronales extremadamente profundas para mapear rostros a espacios de características donde la distancia euclidiana se puede utilizar para medir la similitud.

Es importante destacar que el reconocimiento facial plantea desafíos éticos y de privacidad, ya que puede tener implicaciones en la seguridad y la privacidad de las personas. La tecnología se ha utilizado en diversas aplicaciones, desde el desbloqueo de dispositivos hasta la vigilancia y la seguridad, lo que ha generado debates sobre su uso adecuado y sus posibles abusos.

2.1.4. Inteligencia artificial

La inteligencia artificial consiste en una amalgama de algoritmos concebidos para crear una diversidad de sistemas, máquinas y robots con la capacidad de imitar características humanas. Actualmente, destaca como uno de los campos con mayor expansión y promesa económica para los expertos en el ámbito, presentando oportunidades laborales de gran relevancia. (León Rodriguez & Viña Brito, 2017)

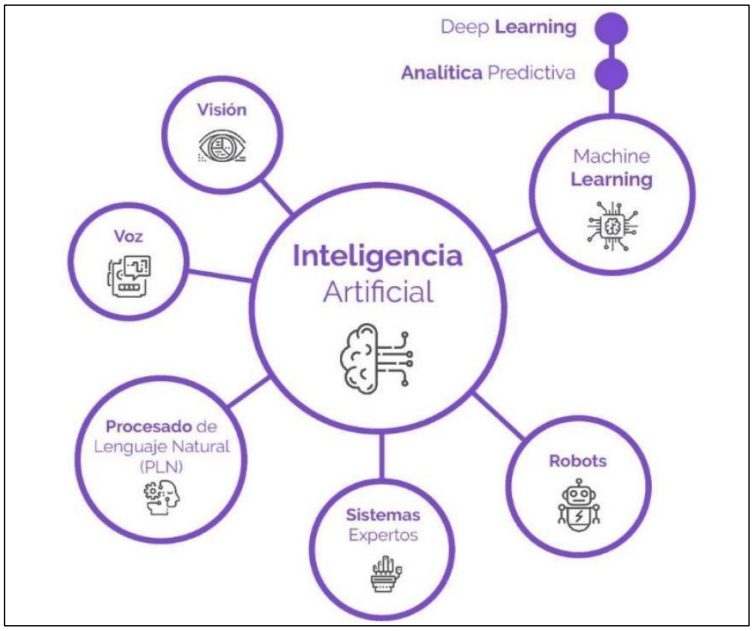
La inteligencia artificial (IA) se refiere a la simulación de procesos de inteligencia humana mediante la programación de sistemas informáticos. La síntesis en el contexto de la inteligencia artificial implica la creación de resultados o datos nuevos a partir de información existente, utilizando algoritmos y modelos matemáticos para generar contenido original.

La inteligencia artificial (IA) es la base en la cual se crean procesos que pueda recrear la inteligencia humana mediante el desarrollo de algoritmos creado en computación, para desarrollar un sistema con inteligencia artificial se debe considerar tres componentes fundamentales:

- Sistemas Computacionales
- Datos y gestión de los mismo
- Algoritmos de IA avanzados (Código)

En la figura 6 se muestra un esquema de los usos de la inteligencia artificial, el cual puede ser usado en voz, video, para realizar el procesamiento de lenguaje natural también se implementa ampliamente en la automatización de robots y para el reconocimiento facial. (Santander, 2023)

Figura 6
Usos de la inteligencia artificial.



Nota: El gráfico muestra los diferentes usos para la Inteligencia Artificial. Tomado de (Santander, 2023)

Inteligencia artificial aplicada a cámaras de videovigilancia y control de acceso

La inteligencia artificial (IA) ha revolucionado la industria de la videovigilancia y el control de acceso al permitir un enfoque más eficiente y preciso para garantizar la seguridad en diversos entornos. La aplicación de la IA en cámaras de videovigilancia y control de acceso abarca desde la detección y seguimiento de objetos hasta el análisis de comportamientos anómalos.

En la videovigilancia, las cámaras equipadas con IA pueden detectar automáticamente eventos de interés, como intrusiones, objetos abandonados o movimientos sospechosos. Los algoritmos de detección de objetos basados en redes neuronales convolucionales (CNN) permiten identificar y rastrear personas, vehículos y otros objetos en tiempo real. Estos sistemas también pueden distinguir entre diferentes tipos de objetos y realizar un seguimiento preciso incluso en condiciones de iluminación y clima variables.

Procesamiento de imágenes

El procesamiento de imágenes se refiere a la manipulación y análisis que se realiza a diferentes imágenes para obtener información significativa de las mismas, realizar acciones en ellas, como mejorar su resolución, cambiar la escala entre otras. Este proceso se realiza con diferentes técnicas y algoritmos informáticos los cuales se encargan de realizar diferentes acciones según las necesidades del usuario (*Procesamiento de imágenes*, 2023). Algunos pasos del procesamiento de las imágenes son:

- Adquisición de las imágenes: Primero se debe obtener las imágenes que se van a procesar en el sistema, para eso se realiza la captura u obtención mediante cámaras de video y otros dispositivos que capturen y a su vez almacenan las imágenes. Este procedimiento puede darse a través de la captura de imágenes en tiempo real y la calidad y la cantidad de datos capturados en esta etapa pueden influir además en la efectividad del procesamiento posterior y la eficiencia del sistema.

- Procesamiento de imágenes y realce de imagen: En este punto se establecen ajustes básicos necesarios en la imagen, entre ellos: Brillo, contraste, profundidad, equilibrio, saturación entre otros, con la finalidad de mejorar la calidad de las fotografías para poseer una base de datos confiable.

- Detección de bordes: En el procesamiento de las imágenes es importante detectar bordes, ya que esto ayuda a identificar objetos o poder segmentar las características de la información presente en la imagen. En este proceso también influye la intensidad de los píxeles y también el límite entre diferentes objetos.

- Reconocimiento de patrones: La base de datos requiere reconocer distintos patrones capaces de detectar objetos para con ello identificar y dar seguimiento a los diferentes escenarios a los cuales puede estar sujeto. Este reconocimiento de patrones está basado en diferenciar formas, texturas, colores etc.

- Aprendizaje automático: Este proceso está arraigado a la inteligencia artificial, el mismo que se encarga de revisar la información de la base de datos en las que se incluyen varias imágenes y tiene el objetivo de dar lugar al reconocimiento de rostros, escenarios y características, con el propósito de aprender automáticamente y guardar a su vez información nueva que servirá para el reconocimiento posterior de personas.

El procesamiento de imágenes es uno de los temas principales y fundamentales en la informática e inteligencia artificial que lleva consigo una serie de procedimientos, técnicas y algoritmos capaces de identificar y analizar todo tipo de imágenes con el objetivo de obtener información útil, almacenar en bases de datos y realizar con ello varias funciones capaces de resolver problemas, ayudar en el procesamiento de datos en tiempo real y minimizar además tiempos de operación, como también, ayudar en temas de seguridad. Algunos de los tipos de enfoque para el procesamiento de imágenes son:

- Procesamiento de Imágenes con redes neuronales convolucionales (CNN)
- Segmentación semántica con redes neuronales.
- Generación de imágenes con redes generativas adversariales (GAN).
- Transferencia de estilo.
- Aumento de datos.
- Reconocimiento de objetos y clasificación.
- Detección de rostros y características faciales.
- Superresolución con redes neuronales.
- Procesamiento de imágenes médicas.
- Autenticación y manipulación de imágenes.

Para el presente proyecto, se tomará en consideración usar el tipo de procesamiento de Imágenes con Redes Neuronales Convolucionales (CNN).

2.1.5. Redes neuronales convolucionales (CNN)

Son un tipo de arquitectura de redes neuronales profundas las mismas que fueron diseñadas principalmente para el procesamiento y análisis de imágenes y, en algunos casos, también datos secuenciales, como audio y texto. Estas redes son particularmente eficientes en la extracción de características y patrones relevantes en datos de alta dimensionalidad por lo cual es altamente

utilizado para el procesamiento de imágenes. Las principales características y componentes de las redes neuronales convolucionales son:

Capa de convolución

La capa de convolución constituye el núcleo central de una CNN y es aquí donde ocurre la mayor parte de los cálculos ya que en esta capa se compone de elementos esenciales, como la entrada de datos, un filtro y un mapa de características, al considerar una imagen a color, esta se compone de una matriz tridimensional de píxeles lo cual implica tres dimensiones: altura, ancho y profundidad, relacionadas con los colores RGB en la imagen. Además, hay un elemento llamado filtro o también se le conoce como kernel, que se desplaza por la imagen buscando rasgos específicos según las necesidades del usuario. A esta operación se le llama convolución.

Entonces al comenzar por el filtro, similar a un fragmento de la imagen, se puede determinar que es un conjunto de datos dispuesto en una matriz bidimensional para que así pueda reflejar una cierta parte de la imagen. Aunque su tamaño puede variar según la variable de entrada, comúnmente se utiliza o se recrea una matriz de 3x3, posteriormente, el filtro se aplica sobre alguna zona de la imagen para poder realizar una operación que en este caso es el producto escalar entre los valores de entrada y el filtro, el resultado de estas operaciones se debe posicionar o establecer en una matriz de salida. El proceso se repite continuamente como sucesivos desplazamientos del filtro hasta que se logre cubrir toda la imagen. La culminación de estos productos escalares se denomina mapa de características.

Cabe indicar que esa capa de convolución puede ir seguida por diversas capas de convolución, por lo cual se habla de capas convolucionales jerárquicas, las mismas que se van añadiendo según se desea extraer las características de la variable de entrada.

Capa de agrupación

La capa de agrupación comúnmente también llamada submuestreo, tiene como principal objetivo poder disminuir la dimensión de la entrada, reduciendo así la cantidad de parámetros. A diferencia de la capa de convolución, aquí el filtro no posee pesos. En su lugar, el filtro aplica una función de agregación a los valores en el campo receptivo y llena la matriz de salida. Existen dos enfoques principales de agrupación:

Agrupación máxima: el filtro selecciona el valor más grande en el campo receptivo y lo envía a la matriz de salida. Este enfoque es más común que la agrupación media.

Agrupación media: el filtro calcula el promedio de los valores en el campo receptivo y lo envía a la matriz de salida.

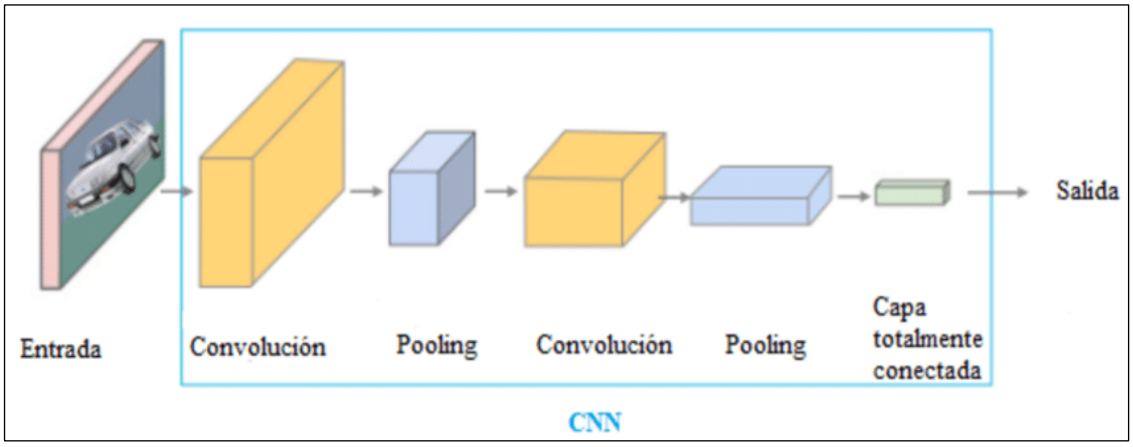
A pesar de que se pierde algo de información en esta capa, su uso trae consigo ventajas para la CNN, incluyendo la reducción de complejidad, mejor eficiencia y mitigación del riesgo de sobreajuste.

Capa totalmente conectada

Los valores de píxeles de la imagen de entrada no están directamente relacionados con la capa de salida o también se puede decir que no se encuentra relacionada en capas parcialmente conectadas. Sin embargo, en esta capa, cada nodo de la capa de salida deberá estar enlazado directamente con un nodo referente a la capa anterior. Esta capa tiene como principal labor la clasificación basándose en los rasgos, características o parámetros que fueron extraídos de las capas anteriores, mientras que las capas previamente expuestas emplean continuamente funciones ReLU, esta capa suele utilizar una función de activación llamadas softmax con el objetivo de poder para clasificar las entradas de manera adecuada según los requerimientos y generar una probabilidad entre 0 y 1. (*¿Qué son las redes neuronales convolucionales?*, IBM, 2023)

Las redes neuronales convolucionales han demostrado ser extremadamente efectivas en una amplia variedad de tareas de visión por computadora, como clasificación de imágenes, detección de objetos, segmentación semántica, generación de imágenes y más. Además, su versatilidad ha permitido su adaptación a otros tipos de datos, como series temporales y datos secuenciales. En la figura 3 se puede observar un diagrama representativo de este tipo de inteligencia artificial.

Figura 7
Esquema de una CNN.



Nota: La imagen muestra el esquema de una red neuronal convolucional. Tomado de (*¿Qué son las redes neuronales convolucionales?*, IBM, 2023)

Matrices en las capas convolucionales

Dentro del procesamiento de imágenes las capas convolucionales y las CNN emplean matrices conocidas como "filtros" o "kernels" para realizar la operación de convolución que permite a la red aprender y detectar patrones visuales en los datos de entrada. Cada filtro se desliza sobre la imagen, multiplicando sus valores con los valores correspondientes de la región de la imagen actual, estas matrices contienen coeficientes numéricos que son capaces de determinar cómo se realiza la convolución en la imagen de entrada, posteriormente los resultados se suman para obtener un solo valor en la salida, que representa la activación y validación del filtro.

Reconocimiento facial con IA

La inteligencia artificial es aplicada al reconocimiento facial la misma que es una tecnología que ha ganado popularidad en los últimos años debido a su uso en diferentes sistemas ya sea de industria, medicina, comercio entre otros. Este sistema se basa en el procesamiento de imágenes y patrones los cuales permiten identificar características únicas que presenta cada ser humano y según eso poder realizar algún control o acción (*¿Qué es el reconocimiento facial?*, AWS, 2023). Se compone de las siguientes etapas:

- Detección de rostros: La IA primero localiza y delimita las caras en una imagen o video utilizando algoritmos de detección facial.

- Extracción de características: La IA analiza características específicas del rostro, como la posición de los ojos, nariz, boca y otros elementos distintivos, para crear un conjunto de datos que represente al individuo.

- Creación de una huella facial: La información extraída se convierte en una "huella facial" única y encriptada, que se compara con las huellas faciales almacenadas en una base de datos.

- Comparación y Verificación: La IA compara la huella facial con las que tiene en su base de datos para verificar si hay una coincidencia. Si la similitud supera un umbral definido, se considera una coincidencia positiva.

2.1.6. Detección de armas mediante inteligencia artificial (IA)

Sistemas de videovigilancia es una aplicación importante para mejorar la seguridad en entornos públicos y privados. Esta tecnología utiliza algoritmos de procesamiento de imágenes y aprendizaje automático para identificar automáticamente la presencia de armas en imágenes o videos capturados por cámaras de seguridad. El proceso general de detección de armas mediante IA en videovigilancia implica los siguientes pasos:

- Captura de vídeo: Las cámaras de seguridad capturan imágenes o vídeos en tiempo real de un área específica.

- Preprocesamiento de Imágenes: Las imágenes o cuadros de video capturados se procesan para mejorar la calidad y el contraste, lo que facilita la detección de objetos.

- Extracción de características: En esta etapa, se extraen características relevantes de las imágenes, como bordes, formas y texturas, que se utilizarán como entradas para los algoritmos de detección.

- Modelo de Detección: Se entrenan modelos de aprendizaje automático, como redes neuronales convolucionales (CNN) u otros enfoques de detección de objetos, utilizando conjuntos de datos que contienen imágenes de armas y sin armas. Estos modelos aprenden a identificar patrones y características distintivas de las armas.

- Etiquetado y Anotación: Las imágenes de entrenamiento deben estar etiquetadas para indicar si contienen armas o no. Esto es crucial para enseñar al modelo a distinguir entre imágenes con armas y otras sin armas.

- Entrenamiento y Ajuste: Se alimentan las imágenes etiquetadas al modelo, que ajusta sus pesos y parámetros internos para aprender a realizar la detección de manera precisa.

- Detección en tiempo real: Una vez que el modelo está entrenado, se implementa en el sistema de videovigilancia para realizar la detección en tiempo real. El modelo analiza continuamente los cuadros de video y marca las áreas donde se detectan posibles armas.

- Notificación y acciones: Cuando se detecta una posible arma, el sistema puede activar notificaciones a los operadores de seguridad o tomar medidas automáticas, como alertar a las autoridades, activar alarmas o seguir el objeto sospechoso con cámaras móviles.

- Evaluación y mejora: La precisión del sistema de detección se evalúa continuamente y se pueden realizar ajustes en el modelo para mejorar su rendimiento. Esto puede implicar la

incorporación de más datos de entrenamiento, ajustes en los parámetros del modelo o incluso la implementación de modelos más avanzados.

Es importante tener en cuenta que, si bien la detección de armas mediante IA puede ser una herramienta valiosa para mejorar la seguridad, también puede plantear desafíos éticos y de privacidad. Es necesario equilibrar la necesidad de seguridad con la protección de la privacidad de las personas y considerar posibles sesgos en la detección automática.

2.1.7. Reconocimiento de placas

Para implementar el reconocimiento de placas, se inicia extrayendo el cuadro de la escena en el que se ha detectado un vehículo. Luego, mediante una serie de técnicas de procesamiento de imágenes, se aplican filtros que permiten resaltar la región donde se encuentra la placa de matrícula. Este proceso de segmentación es esencial para aislar la placa del resto de la imagen, preparándola para la etapa de reconocimiento de caracteres.

La incorporación de la detección de placas a través de inteligencia artificial para el control de acceso y vigilancia en un entorno residencial conlleva una serie de beneficios directos que promueven tanto la seguridad como la conveniencia en este contexto específico. Una de las ventajas más evidentes es la automatización del proceso de ingreso. Al implementar esta tecnología, el sistema puede reconocer automáticamente las placas de vehículos autorizados, lo que elimina la necesidad de que los residentes presenten tarjetas o identificaciones manuales al entrar o salir. Esto agiliza significativamente el acceso y reduce las posibles demoras, especialmente en momentos de alto tráfico.

La alta precisión de los algoritmos de detección y reconocimiento de placas garantiza que solo los vehículos autorizados sean admitidos en el domicilio. Esto minimiza los errores de identificación y reduce los riesgos de permitir el ingreso a vehículos no autorizados, aumentando la seguridad de la comunidad. La tecnología de detección de placas también ofrece un beneficio en términos de registro y seguimiento. El sistema puede mantener un historial detallado de los vehículos que han accedido al domicilio, lo que resulta útil tanto para la gestión interna como para posibles investigaciones en caso de incidentes. Esta función proporciona una capa adicional de seguridad y responsabilidad.

2.2. Descripción de la propuesta

Actualmente vivimos en un entorno cada vez más interconectado y vanguardista, la seguridad y el monitoreo en domicilios es uno de los factores más importantes que no pasa por desapercibido, siendo un tema que cada vez más usuarios optan por adquirir. El presente

proyecto tiene como objetivo principal desarrollar un sistema avanzado con el uso de inteligencia artificial para videovigilancia, utilizando herramientas y sistemas modernos capaces de procesar imágenes y detectar a su vez entornos inusuales con el fin de advertir a los usuarios que se encuentran ante un cierto peligro.

Al aplicar los fundamentos teóricos, se procederá a seleccionar los componentes adecuados para su correcto funcionamiento para posteriormente desarrollar un algoritmo eficiente. Este trabajo contribuirá al avance de la tecnología de vigilancia residencial y su aplicación en el contexto de la inteligencia artificial. Una vez desarrollado el sistema, con su previo análisis y evaluación, el sistema se implementará en un domicilio local, el cual busca brindar a los usuarios un equipo capaz de garantizar la seguridad y tranquilidad dentro y fuera del hogar.

a. Estructura general

En la figura 8 se muestra el diagrama de flujo que representa el sistema de videovigilancia y control de acceso con inteligencia artificial (IA) desde su inicio hasta su conclusión. En el inicio, se establece la inicialización del proceso de videovigilancia mediante la cámara ubicada en el domicilio. Estos flujos de vídeo se envían a un módulo de procesamiento donde la IA realiza tareas de detección y seguimiento de objetos y personas.

La IA analiza continuamente las imágenes para identificar patrones de comportamiento anormales o intrusos en las áreas vigiladas. Si se detecta alguna actividad sospechosa, el sistema enviará notificaciones a los propietarios, y procederá a un análisis más profundo de la situación. Además, el sistema de control de acceso integrado interactúa con la IA para verificar la identidad de las personas que intentan acceder a zonas restringidas. En el flujo de control de acceso, las personas autorizadas pueden emplear el reconocimiento facial para solicitar la entrada. La IA compara las características biométricas con los datos almacenados y, en caso de coincidencia, permite el acceso. En situaciones donde no se reconoce al individuo o se detecta un intento de acceso no autorizado, el sistema niega la entrada y puede generar alertas a los usuarios.

El sistema de videovigilancia y control de acceso con inteligencia artificial también incluye la detección de armas. En el diagrama de flujo, este proceso se integra como una parte crucial de la funcionalidad de seguridad.

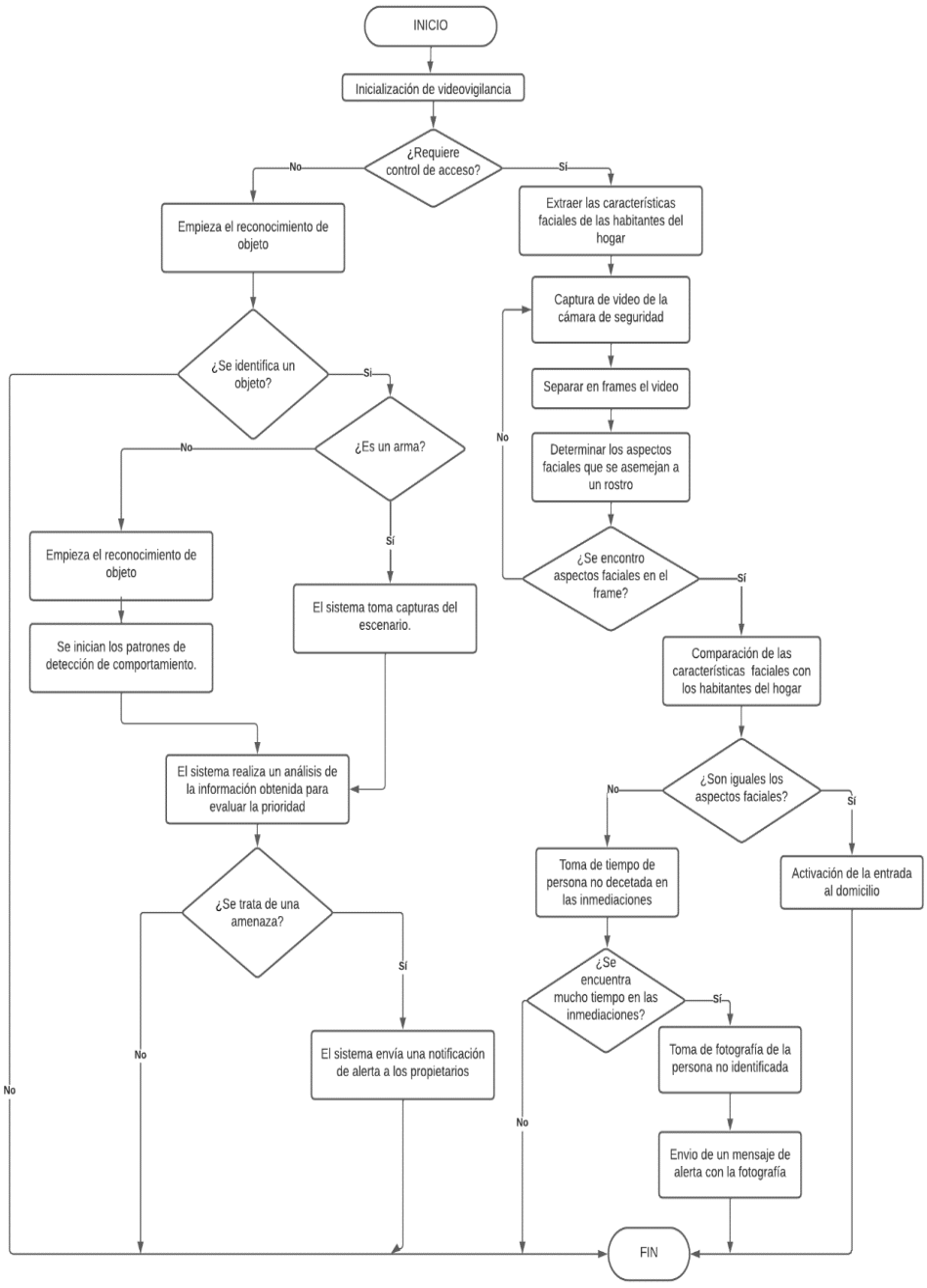
La detección de armas se realiza mediante algoritmos de IA especialmente diseñados para reconocer formas y características distintivas de armas de fuego u objetos similares en las imágenes capturadas por las cámaras de vigilancia. A medida que el flujo de video llega al

módulo de procesamiento de la IA, se ejecutan estos algoritmos para analizar las imágenes y buscar patrones que indiquen la presencia de armas.

A medida que el proceso avanza, la IA sigue monitoreando y analizando los flujos de vídeo y los datos de acceso en tiempo real. Los registros de actividad se almacenan para su posterior revisión y análisis. El diagrama de flujo culmina con la posibilidad de generar informes de incidentes y patrones de comportamiento a partir de los datos recopilados. Estos informes contribuyen a la toma de decisiones, la mejora de la seguridad y la optimización del sistema en el futuro.

Figura 8

Flujo funcional del sistema de videovigilancia y control de acceso.



b. Explicación del aporte

La propuesta plantea el desarrollo de un sistema de videovigilancia avanzado utilizando inteligencia artificial para garantizar la seguridad y el monitoreo de domicilios. Este sistema se enfocará en generar interactividad a través de diversas actividades con el propósito de mejorar la experiencia del usuario y brindarle un mayor control sobre su entorno. Esta interactividad es esencial, ya que permite a los usuarios estar más involucrados en la protección de su hogar, al

tiempo que reciben alertas y advertencias en caso de situaciones inusuales o de peligro. La interconectividad entre el sistema de videovigilancia y los usuarios crea una relación activa y participativa, lo que aumenta la eficacia del monitoreo y la respuesta ante cualquier amenaza.

En cuanto a los recursos utilizados para respaldar los aprendizajes, el proyecto se basa en componentes tecnológicos de última generación. Esto incluye cámaras de alta resolución con capacidades de detección de movimiento y reconocimiento facial, sensores de ambiente para la detección de cambios climáticos o intrusos, y sistemas de procesamiento de imágenes basados en inteligencia artificial. Estos recursos trabajan en conjunto para capturar, analizar y procesar datos en tiempo real, permitiendo la identificación de patrones y comportamientos anómalos en el entorno vigilado.

En términos de evaluación, se propone llevar a cabo actividades de pruebas exhaustivas para asegurar que el sistema funcione correctamente en diversas situaciones y escenarios. Estas pruebas involucrarán la simulación de eventos inusuales y peligrosos para evaluar la capacidad del sistema para detectarlos y alertar a los usuarios de manera precisa y oportuna. Además, se contempla la retroalimentación de los usuarios durante estas pruebas, lo que permitirá ajustes y mejoras basadas en la experiencia real de uso. Para la construcción del conocimiento, el proyecto desarrollará una serie de actividades que permitirán a los usuarios familiarizarse con el sistema y sus capacidades. Estas actividades incluyen la configuración inicial del sistema, la interacción con la interfaz de usuario para visualizar las imágenes y recibir alertas, así como el aprendizaje sobre el funcionamiento de los algoritmos de detección y reconocimiento utilizados. También se contempla la capacitación de los usuarios en la administración de la base de datos de personas conocidas y reconocidas, lo que les permitirá tener un control total sobre el acceso a su hogar.

La propuesta busca aprovechar la interactividad y la inteligencia artificial para desarrollar un sistema de videovigilancia avanzado y eficiente que garantice la seguridad en los hogares. Los componentes tecnológicos modernos, las actividades de evaluación y las actividades de construcción del conocimiento se combinan para brindar a los usuarios un enfoque integral en la protección de sus espacios, fomentando la participación activa y la tranquilidad en un entorno cada vez más conectado.

c. Estrategias y/o técnicas

En la construcción del sistema, se emplean estrategias metodológicas que se centran en la combinación de teoría y práctica para generar aprendizajes efectivos y significativos. La metodología utilizada se basa en un enfoque de aprendizaje experiencial, donde los usuarios

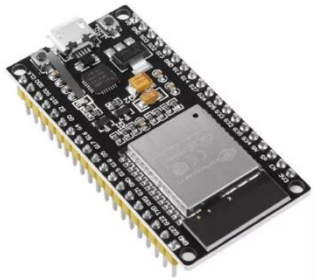
tienen la oportunidad de interactuar directamente con el sistema de videovigilancia y sus componentes. Esto se logra a través de prácticas que involucran la configuración, operación y análisis del sistema en un entorno controlado. Estas actividades permiten a los usuarios familiarizarse con la interfaz de usuario, comprender los conceptos clave de detección y reconocimiento de patrones, y experimentar cómo se aplican estos conceptos en situaciones reales de seguridad y monitoreo.

En cuanto a las herramientas tecnológicas empleadas, se opta por la utilización de cámaras de alta resolución con capacidades avanzadas de detección y reconocimiento. Estas cámaras son esenciales para capturar imágenes claras y detalladas que posteriormente serán procesadas por algoritmos de inteligencia artificial. Los algoritmos de procesamiento de imágenes y reconocimiento facial son herramientas clave en este sistema, ya que permiten identificar patrones y características específicas en las imágenes capturadas, como rostros desconocidos o comportamientos inusuales. Asimismo, se emplearán un componente central en la configuración será la Raspberry Pi 4 con 8 GB de memoria RAM. Esta placa de desarrollo ofrecerá el poder de procesamiento necesario para llevar a cabo las tareas de análisis de imágenes y ejecución de algoritmos de inteligencia artificial en tiempo real. La Raspberry Pi 4 también puede actuar como un controlador central para la gestión de cámaras y sensores, así como para la interacción con los usuarios a través de una interfaz de usuario intuitiva. Además de los componentes mencionados previamente, también se incluirán el ESP32 y un relé de alta potencia para una mayor funcionalidad y control del sistema. El ESP32 será utilizado como un módulo de comunicación y control adicional. Este microcontrolador de bajo consumo energético y alta capacidad de procesamiento permitirá establecer conexiones inalámbricas, como Wi-Fi o Bluetooth, para la comunicación con otros dispositivos o la gestión remota del sistema. Además, el ESP32 puede ser programado en entornos como Arduino, lo que facilita su integración y la creación de aplicaciones personalizadas. El relé de alta potencia se incorpora para el control de dispositivos de alta carga eléctrica, como puede ser el caso del control de acceso a puertas o portones. Un relé capaz de manejar 30 amperios ofrecerá la capacidad necesaria para controlar sistemas de acceso eléctricos de gran envergadura. La integración de este relé con la plataforma Arduino permitirá la automatización y el control remoto de dichos dispositivos a través del sistema de videovigilancia. Estos elementos se sumarán al ecosistema tecnológico del proyecto para ampliar sus capacidades y versatilidad.

La elección de herramientas tecnológicas de vanguardia se fundamenta en la necesidad de lograr una detección y alerta precisa y oportuna. La inteligencia artificial y el procesamiento de imágenes avanzado permiten al sistema identificar situaciones de peligro o anomalías con

mayor eficacia que los métodos tradicionales de videovigilancia. Estas herramientas no solo mejoran la capacidad de detección, sino que también reducen las falsas alarmas, brindando a los usuarios una experiencia de monitoreo más confiable y efectiva.

Tabla 1
Herramientas tecnológicas a emplear.

Cámara tipo DOMO PTZ 2 megapíxeles 1080P Starlight IR 25X HDCVI 	● Sensor de imagen: 1/2.8” STARVIS™ CMOS ● Píxeles efectivos: 1920(H) x 1080(V), 2 Megapixels ● Sistema de escaneo: progresivo ● Velocidad de obturación electrónica: 1/3s~1/300,000s ● Iluminación mínima: Color: Color: 0.005Lux@F1.6; 0Lux@F1.6 (IR on) ● Relación S / N: Más de 55 dB ● Distancia IR: Distancia hasta 150 m (492 pies) ● Control de encendido / apagado IR: Automático / manual ● LED IR: 6 ● Distancia focal: 4.8mm~120 mm ● Max Aperture: F1.6 ~ F4.4 ● Ángulo de visión H: 59.2° ~ 2.4° ● Control de enfoque: Auto/Manual ● Distancia de enfoque cercana: 100mm~ 1000mm ● Optical Zoom: 25x
Modulo ESP32 IOT y WiFi 	● Procesador Tensilica Xtensa 32bits LX6 hasta 240MHz. ● Wi-Fi: 802.11b/g/n/e/i (802.11n @ 2.4 Ghz hasta 150 Mbit/s). ● Bluetooth: v4.2 BR/EDR y bluetooth Low Energy (BLE). ● Rom:448 KiB. ● SRAM: 520 KiB.

	• RTC slow SRAM: 8 KiB. • RTC fast SRAM: 8 KiB. • eFuse: 1 Kbit. • Flash embebida: 0 MiB (ESP32-D0WDQ6, ESP32-D0WD, and ESP32-S0WD chips); 2 MiB (ESP32-D2WD chip); 4 MiB (ESP32-PICO-D4 SIP module). • Periféricos compatibles: ADC, DAC, I2C, UART, Interfaz CAN 2.0, SPI, I2S, RMII y PWM entre otros. • Seguridad tipo IEEE 802.11, WFA, WPA/WPA2 y WAPI. • Encriptación de memoria Flash. • Criptografía soportada por acelerador de hardware: AES, SHA-2, RSA, ECC, RNG. • Voltaje de trabajo 3.3VDC. • Energía y datos vía conector micro USB 5VDC.
Relé 24V 30A 1 canal 	• Módulo de Relé 24v 1 Canal Activación Alto O Bajo Arduino • Placa de interfaz de relé de canal de 24V equipada con relé de alta corriente, AC250V 10A; CC30V 10A. Indicador LED de estado incluido. • Ideal para aplicaciones industriales donde la mayoría de las señales son de 24Vdc. • Activación alto o bajo.
Raspberry Pi 4 con 8 GB 	• Procesador: Broadcom BCM2711, Cortex-A72 de cuatro núcleos (ARM v8) SoC de 64 bits a 1,5 GHz • Memoria RAM: 8GB LPDDR4 • Conectividad: LAN inalámbrica IEEE 802.11b / g / n / ac de 2.4 GHz y 5.0 GHz, Bluetooth 5.0, BLE • Gigabit Ethernet • 2 × USB 3.0

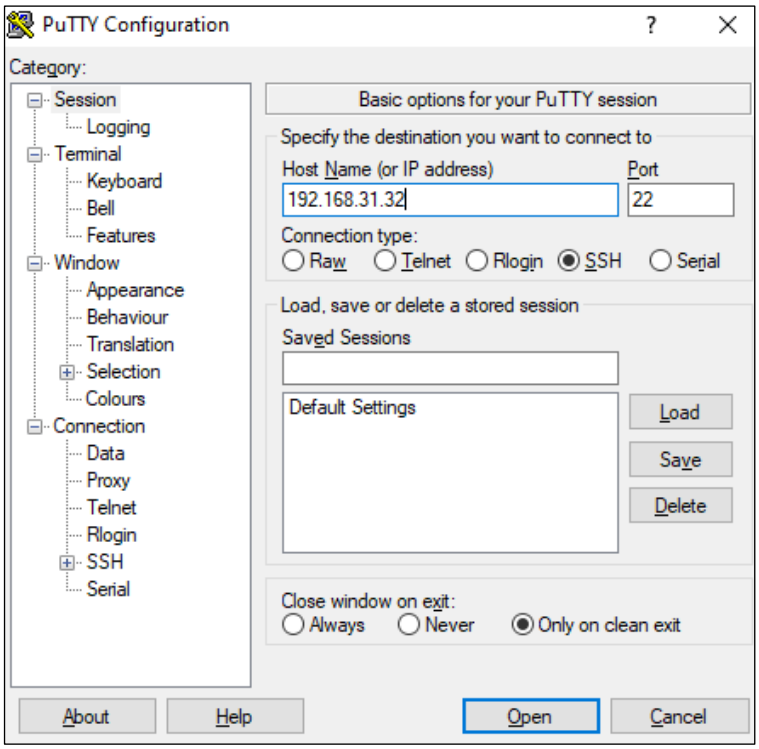
	● 2 × USB 2.0 ● GPIO: estándar de 40 pines ● Video y sonido: 2 puertos micro HDMI (hasta 4 Kp 60 admitidos) ● Puerto DSI para pantalla ● Puerto CSI para cámara ● Soporte de tarjeta SD: ranura para tarjeta micro SD para cargar el sistema operativo y almacenamiento de datos ● Potencia de entrada: 5V DC a través del conector USB-C (mínimo 3A) ● 5V DC a través de los GPIO (mínimo 3A) ● Power Over Ethernet (PoE) – habilitado (a través de un complemento PoE HAT por separado) ● Temperatura de funcionamiento 0–50ºC. ● Dimensiones: (88 x 58 x 18,5mm)

Configuración de la Raspberry

Se procede primero a configurar la Raspberry para instalar el sistema operativo y después instalar el servidor mqtt para poder activar el motor. En la figura 9, se observa el programa PuTTy el cual sirve para poder acceder a la Raspberry. En donde se configura la IP de las Raspberry y el puerto por el que se conecta SSH.

Figura 9

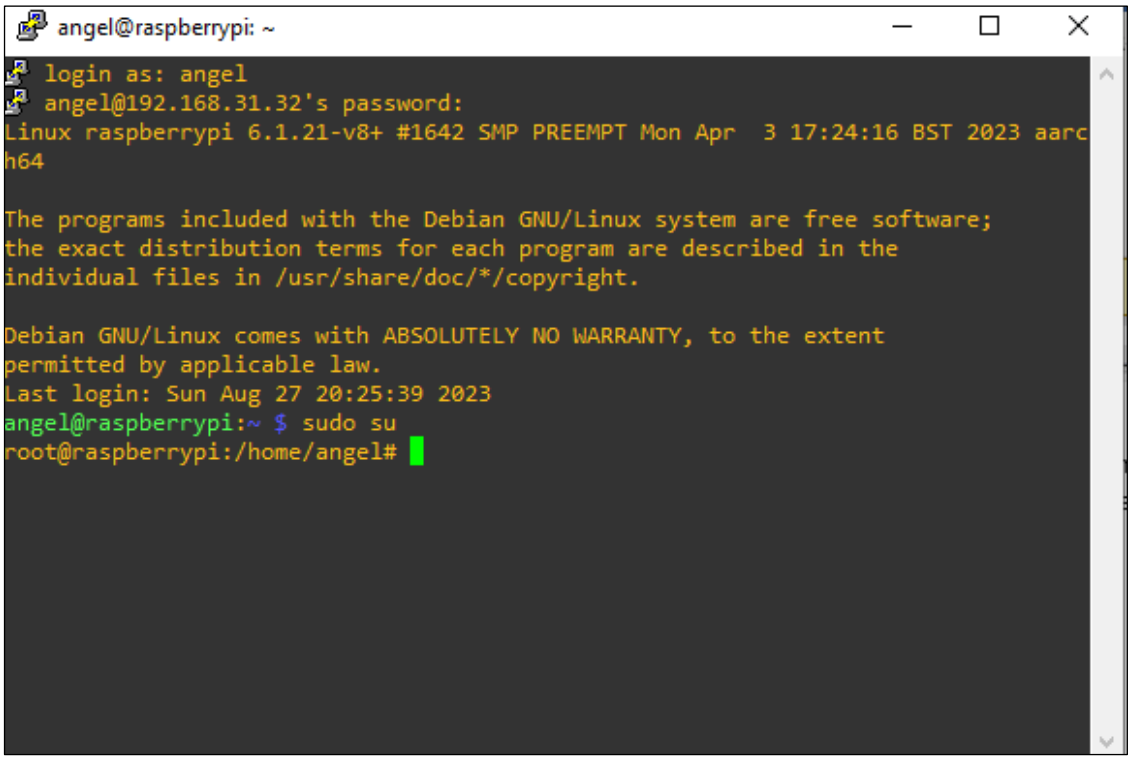
Configuración PuTTY.



En la ilustración 10 se observa el terminal para poder instalar todas las dependencias necesarias para el funcionamiento de la Raspberry.

Figura 10

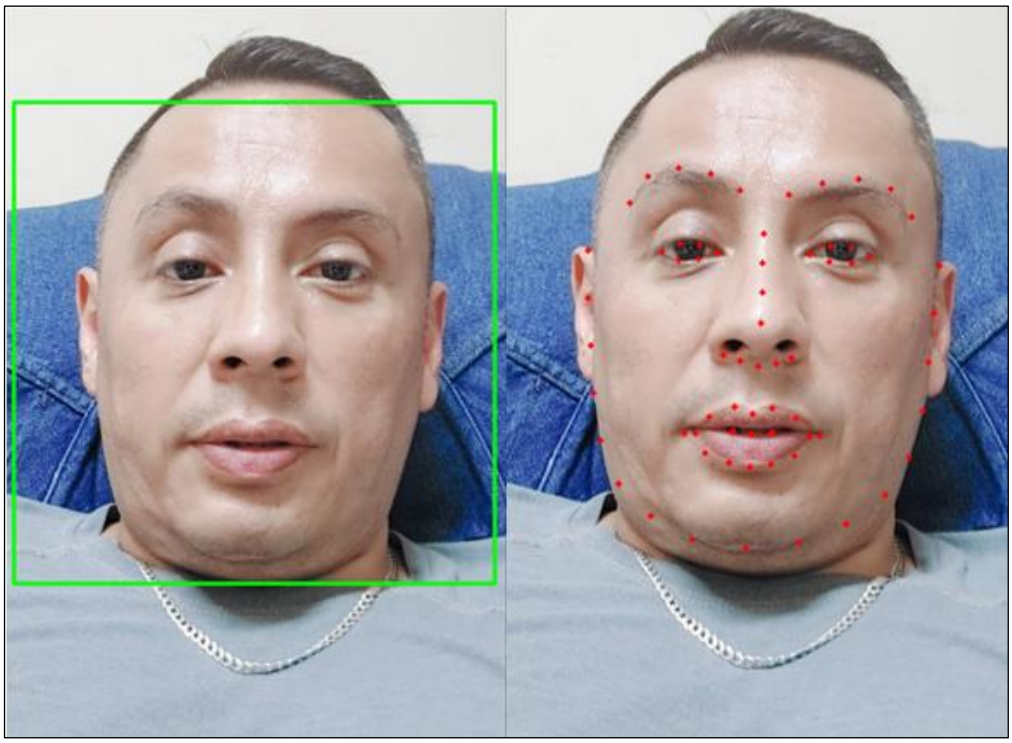
Terminal de Raspberry.



Reconocimiento facial

Para el reconocimiento facial se realiza la programación en Python en el cual por medio de redes neuronales convolucionales se procede a realizar la identificación de las características faciales. Primero es importante detectar el cuadro en donde se encuentra el rostro y segundo determinar los puntos fáciles, como se observa en la ilustración 11 en lado izquierdo se determina un cuadro alrededor del frame de video en donde se determine un rostro, mientras que en lado derecho se determinan los puntos faciales de acuerdo al rostro enmarcado en el video. Estas características faciales se convierten en un vector numérico en donde se encuentra la información de los puntos. Y por los cuales se va a realizar el análisis con los rostros en las cámaras de videovigilancia. Ya con los puntos característicos se procede a verificar con cada frame de video para determinar si la persona está autorizada a entrar o si se trata de un intruso en las inmediaciones

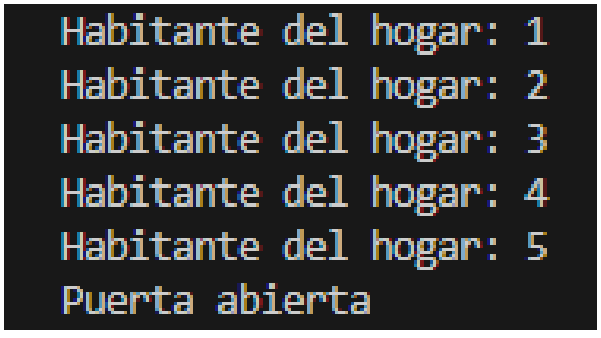
Figura *11*
Prueba de reconocimiento facial.



Control de acceso

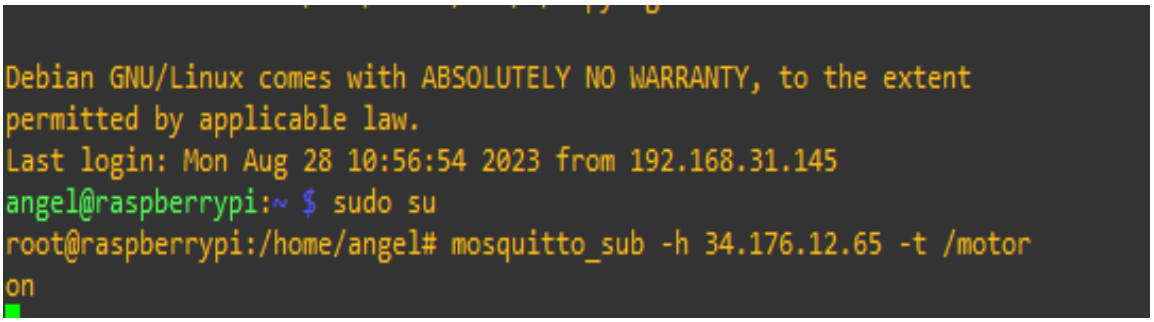
Para el control de acceso se determina si la persona en los frames de video consta en la base de datos de ocupantes del hogar y se debe tener una lectura constante de 5 segundos de la persona para poder activar la puerta, en la figura 4 se observa el conteo que realiza el sistema para poder activar la puerta, en el cual se envía mediante el protocolo MQTT un mensaje a la ESP32 para que active el relé que abrirá la puerta. En la Ilustración 12 se muestra el conteo de 5 segundos y se visualiza el mensaje de puerta abierta en donde se ilustra que se ha enviado el mensaje mediante mqtt.

Figura 12
Conteo para puerta abierta.



En la Ilustración 13, se configura para poder leer el tópico /motor y verificar que se haya enviado el mensaje por el tópico correctamente, como se observa al momento de realizar el conteo de 5 segundo de la persona se envía el mensaje “on” y se recibe en el tópico presente.

Figura 13
Configuración para el tópico.



Cabe indicar que la puerta se cierra automáticamente mediante un temporizador que se activa al momento de accionarse un fin de carrera.

Detección de objetos

Para la detección de objetos, específicamente un arma, se realiza un modelo de entrenamiento en el cual mediante una serie de imágenes y su archivo en xml se pueda identificar y detectar si en los frames de video se encuentra un arma, en la figura, se visualiza la carpeta con las imágenes y su respectivo archivo xml para poder entrenar al modelo que ayudará a reconocer si en un frame se encuentra un arma. Se realizó el entrenamiento con 2000 imágenes las mismas fueron sacadas de videos en los cuales se tomaba un frame cada cierto tiempo.

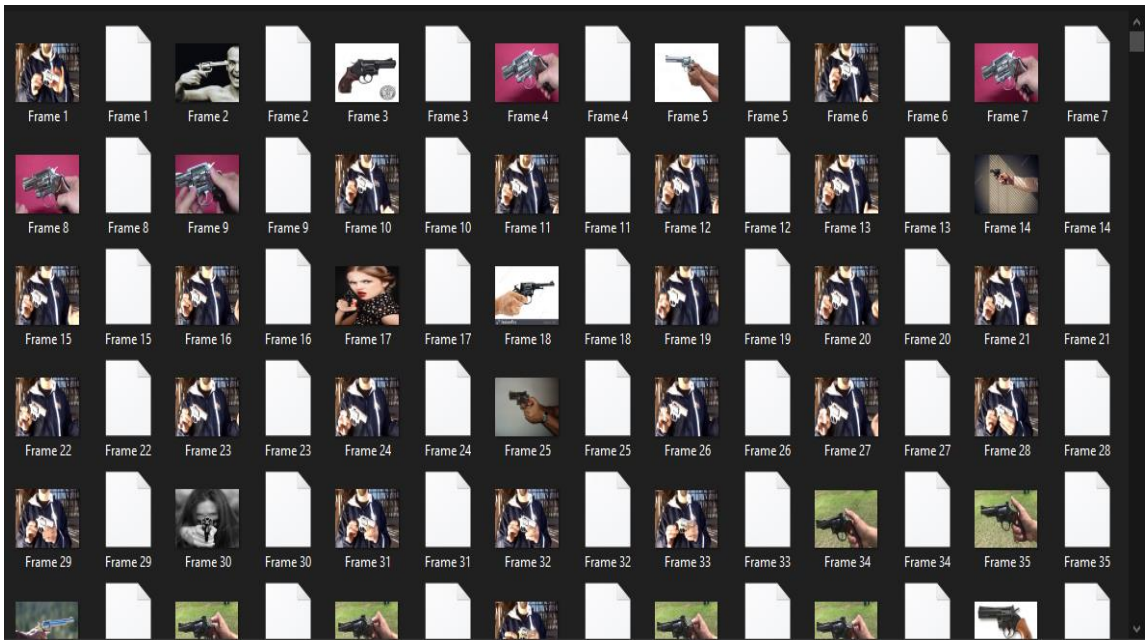
Durante el proceso de entrenamiento, se emplearon algoritmos avanzados de detección de objetos, como YOLO (You Only Look Once) para lograr un equilibrio entre precisión y velocidad en la detección. Después de completar el entrenamiento, el modelo se sometió a una rigurosa fase de validación y ajuste de hiperparámetros para garantizar que fuera capaz de identificar armas de manera confiable y precisa en una variedad de escenarios del mundo real.

YOLO, que significa "Sólo miras una vez", es un popular y poderoso algoritmo de detección de objetos en imágenes y vídeos. Fue propuesto por Joseph Redmon y Santosh Divvala en 2016 y ha sido fundamental en el campo de la visión por computadora debido a su capacidad para lograr una detección en tiempo real de objetos en imágenes y secuencias de video.

La característica distintiva de YOLO es su enfoque en la eficiencia y la velocidad de detección. A diferencia de otros métodos que dividían la detección en múltiples etapas (como la identificación de regiones de interés y luego la clasificación de esas regiones), YOLO aborda el problema de detección como una tarea de regresión. En lugar de predecir regiones y luego clasificar objetos, YOLO predice directamente cajas delimitadoras (bounding boxes) y las probabilidades de diferentes clases de objetos dentro de esas cajas.

Figura 14

Imágenes para el entrenamiento del modelo de inteligencia artificial.

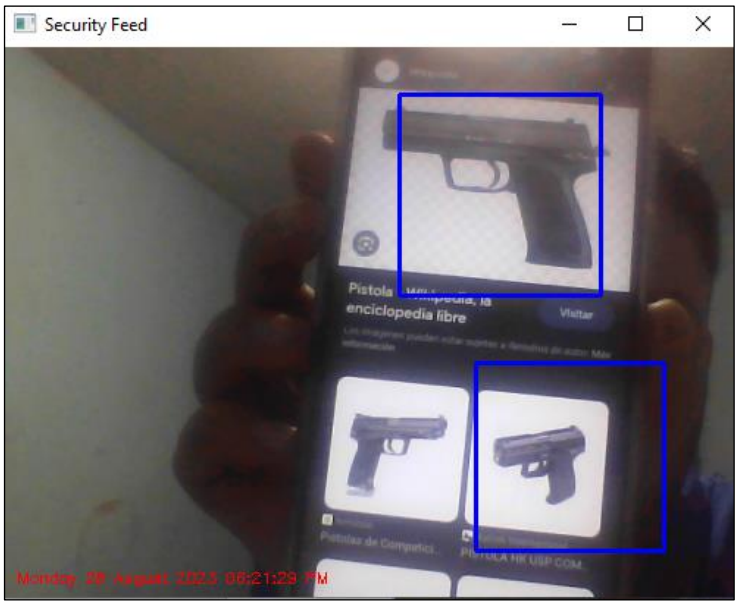


Cuando se aplica a la detección de armas, YOLO puede entrenarse para reconocer las características visuales distintivas de diferentes tipos de armas, como pistolas, cuchillos u otros objetos potencialmente peligrosos. La capacidad de YOLO para detectar objetos en diferentes posiciones, tamaños y orientaciones es crucial en la detección de armas, ya que las armas pueden aparecer en una variedad de contextos y poses. Además, la rapidez de YOLO permite escanear rápidamente los cuadros de un video en tiempo real y alertar sobre la presencia de armas, lo que puede ser esencial para la seguridad pública y la prevención de situaciones de riesgo.

Es importante destacar que, si bien YOLO puede ser efectivo en la detección de armas, ningún sistema de detección es infalible. Con el entrenamiento realizado se detectan armas en los frames de video y se encierra en un cuadro como se observa en la figura 15.

Figura 15

Detección de armas.



Detección de placas

Para la detección de placas primero es importante realizar el filtro en escala de grises, en la ilustración 16 en el lado izquierdo se visualiza la fotografía del vehículo con su respectiva placa posterior a eso se realiza un filtrado en escala de grises para acentuar los contrastes en la imagen, facilitando la identificación de la placa.

Figura 16

Reconocimiento de placa vehicular.

Una vez realizado en escala de grises se procede a convertir a una imagen binaria para extraer sus contornos y así determinar el sector en donde se encuentra la placa.

Figura 17

Conversión de imagen a binario para fácil detección de la placa vehicular.

De igual forma realizamos el negativo de la imagen binarizada y dibujamos sus contornos en donde se puede observar los contornos de los números de la placa.

Figura *18*

Negativo de la imagen binarizada.

Al realizar un contorno más pronunciado se puede observar en la figura 19 que se genera ya los números pertenecientes a la placa, ahora es necesario la técnica de redes neuronales y así determinar el valor de la placa.

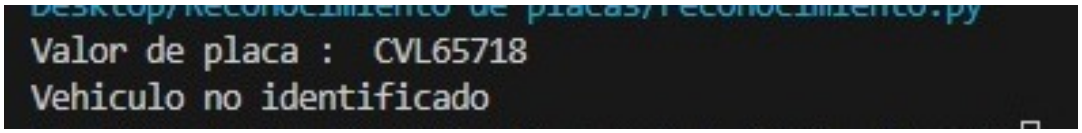
Figura 19

Identificación de los dígitos correspondientes a la placa vehicular.

Después de completar este proceso, se obtiene la impresión del valor de la placa detectada y se muestra en pantalla dicha identificación, como se indica en la ilustración 20. A continuación, esta información se compara con la lista de placas permitidas para el acceso al domicilio. Este procedimiento asegura que solo los vehículos autorizados sean admitidos.

Figura 20

Impresión en pantalla de los dígitos obtenidos de la detección de placas.



Reconocimiento de amenazas y envió de notificaciones

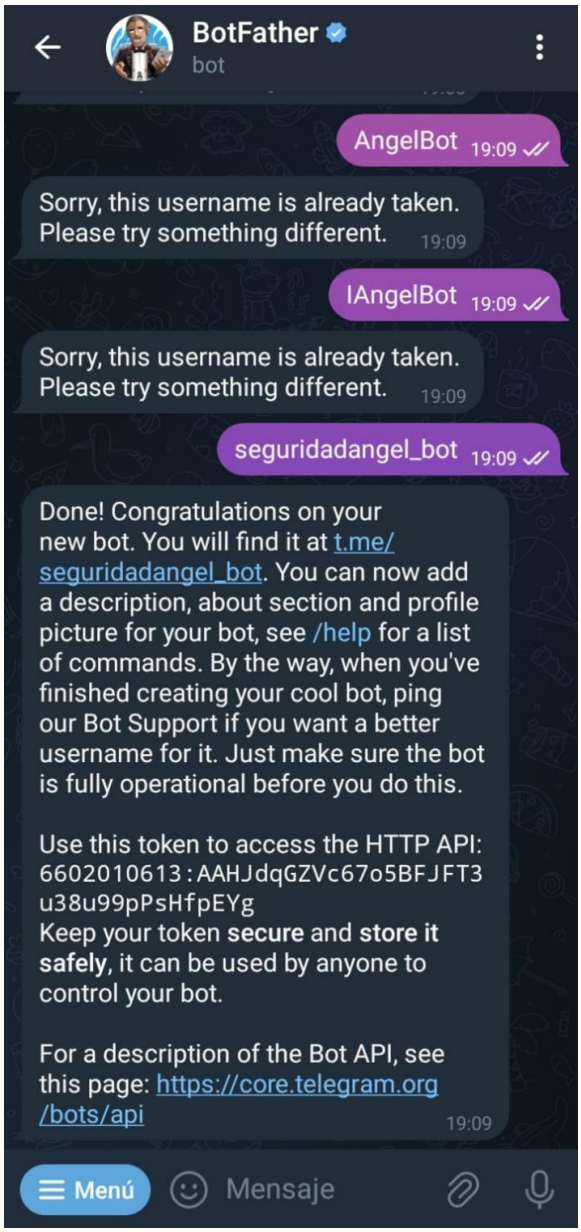
Después de que el sistema procese la información y detecte la presencia de un arma utilizando el modelo YOLO, la siguiente etapa es la activación de una alerta. En este caso, se ha optado por utilizar la plataforma de mensajería Telegram para transmitir la alerta de manera rápida y eficiente. Para lograr esto, seguirá un proceso que implica la creación de un bot personalizado a través de la función BotFather en Telegram.

La creación de este bot es para habilitar la comunicación automatizada entre el sistema esencial de detección y el grupo de alerta en Telegram. BotFather es una herramienta proporcionada por Telegram que permite a los usuarios crear y personalizar bots según sus necesidades. Al configurar el bot, se asignará un nombre único, en este caso, "seguridadangel_bot", como se muestra en la figura 16. Además de proporcionar el nombre, se establecerán otros parámetros y ajustes necesarios para que el bot funcione de manera adecuada.

Una vez que el bot esté configurado, se establecerá una integración entre el sistema de detección y el bot de Telegram. Cuando se detecta la presencia de un arma por parte del modelo YOLO, el sistema activará el bot, que enviará un mensaje de alerta al grupo especificado. En este grupo, los usuarios autorizados y responsables de la seguridad podrán recibir de inmediato la alerta y tomar las medidas necesarias para abordar la situación.

Figura 21

Plataforma Telegram para el envío de notificaciones de alerta.



Después de la creación del bot, se incorpora un grupo de seguridad de la residencia. Este bot será responsable de enviar mensajes que contengan información y fotografías del entorno en caso de detectar una posible amenaza. Su función principal es activarse cuando una persona se encuentra cerca de la propiedad, registrando y almacenando la información correspondiente. Si

esta situación se repite en varias ocasiones, el bot procederá a enviar automáticamente una fotografía al grupo de Telegram designado.

Programación ESP32

Para lograr una integración fluida entre el sistema de videovigilancia con IA y el control de acceso a través de la ESP32, se aprovecha la versatilidad de la plataforma Arduino y su entorno de programación. El ESP32 actúa como el intermediario entre el sistema de detección de objetos y el mecanismo de control de acceso de la puerta. La programación de la ESP32 se lleva a cabo utilizando el entorno de desarrollo Arduino, que proporciona una interfaz amigable y una amplia variedad de bibliotecas y recursos para facilitar el proceso de programación. Se establece una comunicación bidireccional con el sistema de videovigilancia a través de protocolos de comunicación como MQTT.

En primer lugar, el ESP32 se suscribe al tema MQTT (/motor) en el que el sistema de videovigilancia envía comandos. Cuando se recibe un mensaje a través de este tópico, el ESP32 interpreta la señal y activa el relé conectado al motor de la puerta mediante un pulso eléctrico. Este pulso permite que el motor se active y, por lo tanto, se abra o cierre la puerta de acceso. El uso de MQTT para la comunicación entre la ESP32 y el sistema de videovigilancia ofrece ventajas significativas en términos de eficiencia y escalabilidad. Además, la posibilidad de recibir comandos de manera remota a través de MQTT brinda una gran flexibilidad y comodidad para los usuarios autorizados.

Es esencial asegurarse de que la programación de la ESP32 sea segura y confiable. Se pueden implementar medidas de seguridad, como la autenticación y encriptación de las comunicaciones MQTT, para proteger la integridad de los comandos y la privacidad de los usuarios. En última instancia, la programación del ESP32 en este contexto agrega una capa de automatización y control inteligente al sistema de acceso, lo que permite que los miembros del hogar o usuarios autorizados puedan activar la puerta de manera conveniente y segura en respuesta a las alertas. de detección de objetos generados por el sistema de videovigilancia.

2.3. Validación de la propuesta

Para la elección de especialistas se ha considerado un perfil acorde a los siguientes criterios: formación académica relacionada con el tema investigativo, experiencia académica y/o laboral orientada a la gestión administrativa y motivación para participar. La siguiente tabla presenta información detallada de los actores seleccionados para la validación del modelo.

Tabla 2

Descripción de perfil de validadores.

Nombres y Apellidos	Años de experiencia	Titulación Académica	Cargo
Ing. Luis Alberto Puma Caiza	12	Magister en automatización y sistemas de control	Jefe de estaciones de captación de gas Ep Petroecuador
Ing. José Ignacio López	12	Magíster en electrónica y automatización	Supervisor de mantenimiento mecánico Ep Petroecuador
Ing. Gabriel Paredes Manobanda		Magister en automatización y sistemas de control	

Los objetivos perseguidos mediante la validación son los siguientes:

- Validar la metodología de trabajo aplicada en el desarrollo de la investigación.
- Aprobar los resultados, conclusiones y recomendaciones obtenidas.
- Redefinir (si es necesario) el enfoque de los elementos desarrollados en la propuesta, considerando la experiencia de los especialistas.
- Constatar las posibilidades potenciales de aplicación del modelo de gestión propuesto.

Tabla 3

Criterios de valuación

Criterios	Descripción
Impacto	Representa el alcance que tendrá el modelo de gestión y su representatividad en la generación de valor público.
Aplicabilidad	La capacidad de implementación del modelo considerando que los contenidos de la propuesta sean aplicables
Conceptualización	Los componentes de la propuesta tienen como base conceptos y teorías propias de la gestión por resultados de manera sistémica y articulada.
Actualidad	Los contenidos de la propuesta consideran los procedimientos actuales y los cambios científicos y tecnológicos que se producen en la nueva gestión pública.
Calidad Técnica	Miden los atributos cualitativos del contenido de la propuesta.
Factibilidad	Nivel de utilización del modelo propuesto por parte de la Entidad.
Pertinencia	Los contenidos de la propuesta son conducentes, concernientes y convenientes para solucionar el problema planteado.

Escala de evaluación. Elaborada por: *Ing. Wilmer Fabián Albarracín Guarochico MBA*

Tabla 4

Evaluación según importancia y representatividad

CRITERIOS	EVALUACIÓN SEGÚN IMPORTANCIA Y REPRESENTATIVIDAD				
	En Total Desacuerdo	En Desacuerdo	Ni de Acuerdo Ni en Desacuerdo	De Acuerdo	Totalmente Acuerdo
Impacto					X
Aplicabilidad					X
Conceptualización					X
Actualidad					X
Calidad Técnica					X
Factibilidad					X
Pertinencia				X	

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 5
Matriz de articulación.

Ejes o partes principales del proyecto		Breve descripción de los resultados de cada parte	Sustento teórico que se aplicó en la construcción del proyecto	Metodologías, herramientas técnicas y tecnológicas que se emplearon
1	Definición y análisis de diversos dispositivos electrónicos basados en su forma de funcionamiento en relación a las variables involucradas.	1.1. Para la selección óptima de los componentes electrónicos y plataformas del sistema de videovigilancia y control de acceso con inteligencia artificial, fue esencial llevar a cabo una investigación exhaustiva de los requisitos específicos de la vivienda. Además, se evaluó minuciosamente la disposición espacial en el entorno del sistema, asegurando una perfecta integración en el contexto de la implementación en el área de videovigilancia y control de acceso. 1.2. Se realizó una minuciosa revisión de los datos técnicos suministrados por los fabricantes de dispositivos. Este análisis detallado tuvo como objetivo identificar los modelos que mejor se adaptan al proyecto en cuestión dentro del	● Inteligencia Artificial y Aprendizaje Automático. ● Visión por Computadora. ● Redes Neuronales Convolucionales (CNN) ● Procesamiento de Señales. ● Comunicación y conectividad. ● Arquitectura de software y programación. ● Experiencia del usuario.	En el desarrollo del sistema de videovigilancia y control de acceso con inteligencia artificial, se emplearon metodologías y herramientas especializadas para diferentes aspectos. Para el dominio de Inteligencia Artificial y Aprendizaje Automático, se utilizaron bibliotecas ampliamente reconocidas que permitieron entrenar y ajustar modelos. En el campo de la Visión por Computadora, se aplican técnicas de procesamiento de imágenes en tiempo real y detección de objetos. Las Redes Neuronales Convolucionales (CNN) desempeñaron un papel central en la identificación de patrones. Para el Procesamiento de Señales, se implementaron enfoques que permitieron analizar datos provenientes de sensores. La Comunicación y Conectividad se lograron mediante protocolos que aseguren la transferencia efectiva de datos entre los componentes. En cuanto a la Arquitectura de Software y Programación, se adoptaron enfoques que faciliten la implementación y el monitoreo eficiente del

		sistema de videovigilancia y control de acceso con inteligencia artificial. Se considerarán aspectos como las especificaciones de rendimiento, el funcionamiento en diferentes situaciones y la armonía con otros elementos del sistema, garantizando así una selección precisa y compatible de los componentes.		sistema. Finalmente, se aplicarán conceptos de Experiencia del Usuario para diseñar interfaces amigables y efectivas. Cada elección se basó en la adecuación para abordar las demandas únicas de cada parte del proyecto.
2	El diseño adecuado y la interacción eficiente entre los diferentes componentes aseguran un sistema de videovigilancia y control de acceso con inteligencia artificial efectivo y confiable.	2.1. Los softwares de diseño de circuitos permiten diseñar esquemas y diseños de circuitos electrónicos de manera eficiente y precisa. 2.2. Las bibliotecas de IA proporcionan funcionalidades específicas para la detección de objetos, análisis de imágenes y redes neuronales convolucionales, esenciales para la implementación de la inteligencia artificial. 2.3. Lenguajes de programación como Python, C + +. Estos lenguajes son ampliamente utilizados para el desarrollo de algoritmos de control y lógica, permitiendo una implementación eficiente y flexible de la gestión del sistema.	● Diseño de Circuitos Electrónicos. ● Diseño de Control. ● Diseño de Aplicación. ● Programación. ● Cálculos y Simulaciones. ● Integración de Componentes.	Para el diseño de circuitos y componentes electrónicos se emplearon programas de diseño especializados que permitieron planificar las conexiones y disposición adecuadas. El diseño de control se basó en el uso de lenguajes de programación para implementar algoritmos y lógica de operación. Para crear la interfaz de usuario y las aplicaciones, se recurrió a frameworks que facilitaron la creación de interfaces amigables. La implementación de la inteligencia artificial y el procesamiento de datos se realizaron utilizando herramientas que permitieron desarrollar modelos y analizar información. Se emplearon herramientas para la simulación y validación de los cálculos teóricos. La integración de los componentes se logró a través de enfoques que permitieron conectar y ensamblar los elementos de manera efectiva. Cada elección se basa en la adecuación a las necesidades específicas de cada etapa del proyecto.

3	Implementación del sistema de videovigilancia y control de acceso con IA en una vivienda del barrio San Cristóbal perteneciente a Shushufindi.	3.1. Se fundamentó en conocimientos de captura de imágenes digitales y transmisión de video a través de redes IP para garantizar la calidad y eficiencia en la captura y transferencia de imágenes. 3.2. Se sustentará en la administración de datos y bases de datos, incluyendo teorías de diseño y estructuras de datos para gestionar eficaz y seguramente los registros del sistema. 3.3. Se apoyó en la teoría de control de motores y actuadores, aplicando principios de señales de control y retroalimentación para permitir la operación remota precisa de los motores en las puertas. 3.4. Se basa en la teoría de instalaciones eléctricas y redes de comunicación, abordando conceptos de cableado, interferencia y protocolos de comunicación para asegurar la transferencia confiable de datos entre los componentes del sistema.	● Cámaras de Vigilancia IP. ● Plataforma de Gestión de Datos. ● Control de Motores para Puertas. ● Instalaciones Eléctricas para Comunicaciones. ● Protocolos de comunicación.	En el desarrollo del proyecto, se emplearon fundamentos teóricos específicos para respaldar las cámaras de vigilancia IP mediante conocimientos de captura y transmisión de imágenes digitales, la plataforma de gestión de datos se basó en principios de administración de bases de datos y estructuras de datos eficientes, el control de motores para puertas se apoyó en teorías de control de actuadores y retroalimentación, y las instalaciones eléctricas para comunicaciones se sustentaron en la teoría de redes y protocolos de comunicación para asegurar la transferencia confiable de datos entre los componentes del sistema. Cada enfoque teórico respaldó la comprensión y aplicación efectiva de los elementos en el proyecto de videovigilancia y control de acceso con inteligencia artificial.

2.5. Análisis de resultados. Presentación y discusión.

Reconocimiento facial y control de acceso

Cuando se produce la aproximación hacia la residencia, uno de los ocupantes se encarga de llevar a cabo el proceso de reconocimiento facial, tal y como se ilustra en la Ilustración 22. A través de este proceso, se logra identificar de manera precisa a la persona en cuestión y se muestra su nombre acompañado de un porcentaje que refleja el grado de similitud. Para garantizar la confiabilidad del reconocimiento y prevenir posibles resultados erróneos, se ha incorporado una pausa de 5 segundos destinada al procesamiento de la información, como se detalla en la ilustración 23. Una vez transcurrido este corto lapso, se emite la señal que desencadena la activación de la puerta, asegurando así un sistema eficaz y seguro de acceso.

Figura 22

Reconocimiento facial de uno de los habitantes del domicilio.

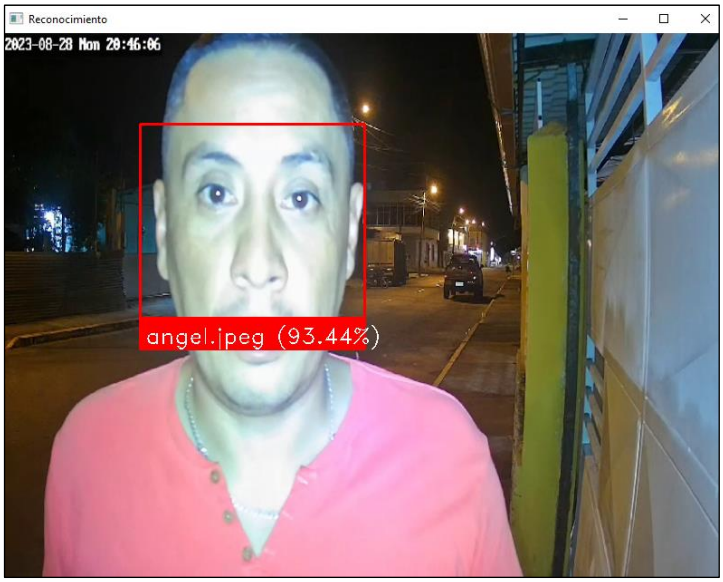
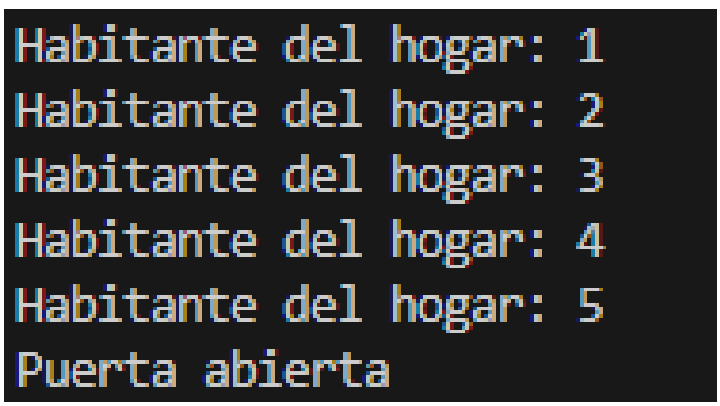


Figura 23

Pausa de 5 segundos para evitar falsos positivos en reconocimiento facial.

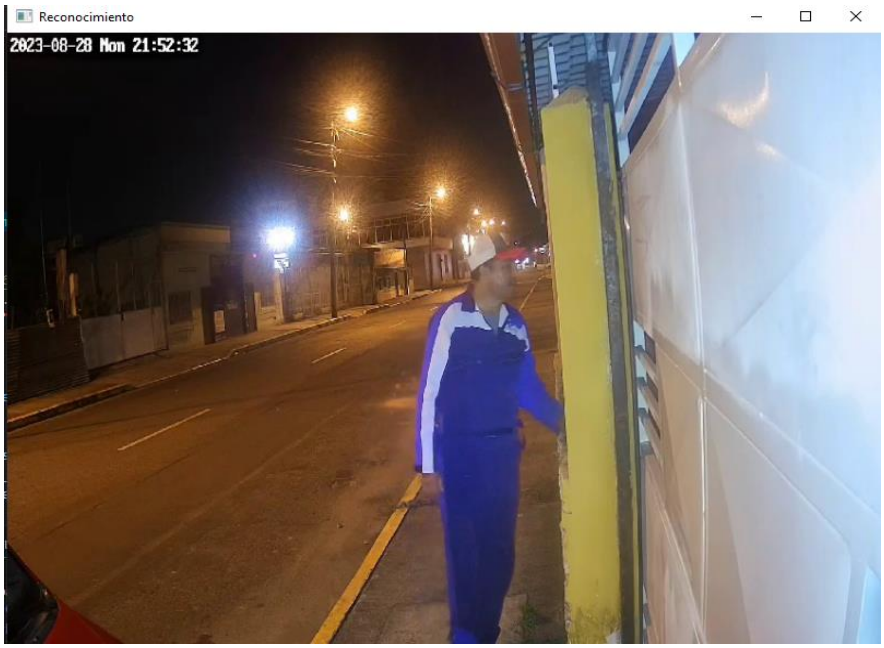


Detección de actitud sospechosa y personas desconocidas

Cuando en las inmediaciones se detecta a una persona con una actitud sospechosa, como se muestra en la ilustración 24, el sistema se activa y comienza su protocolo de reconocimiento facial. Una vez que se observa un comportamiento inusual, la cámara intensifica su vigilancia, capturando la actividad del individuo y sometiéndola a un análisis exhaustivo. Este análisis, que involucra la comparación con patrones preestablecidos, lleva aproximadamente 15 segundos, ya que el sistema busca en su base de datos para determinar si el rostro es conocido o no.

Figura 24

Simulación de una persona sospechosa ante la cámara de videovigilancia



Si la situación evalúa al individuo como una persona desconocida, como se muestra en la figura 25, el sistema se activa automáticamente y desencadena medidas de seguridad adicionales. Además, en un esfuerzo por mantener al propietario informado en tiempo real, el sistema envía una notificación a través de la plataforma de mensajería Telegram, enviando la alerta adjunta de la fotografía del sospechoso, tal cual se muestra en la figura 26.

Esta característica de notificación instantánea permite al propietario tomar decisiones oportunas y apropiadas en función de la situación observada. En resumen, al combinar el reconocimiento facial, la detección de comportamientos anómalos, la búsqueda en la base de datos y las notificaciones en tiempo real, se establece un sistema de seguridad completo y eficiente.

Figura 25

Detección de persona desconocida

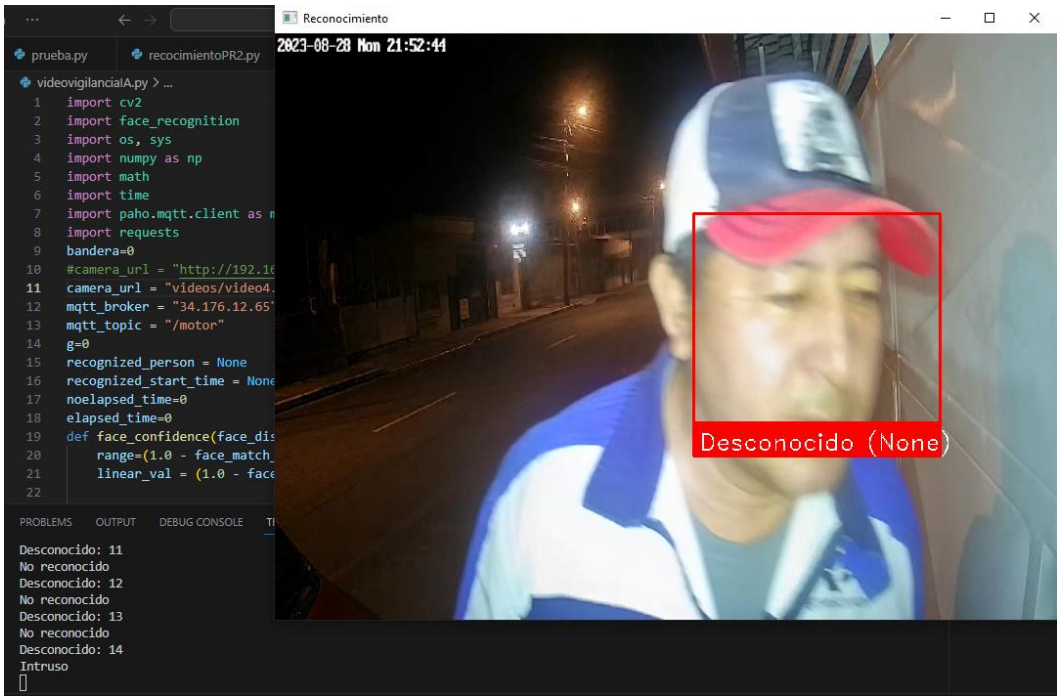


Figura 26

Notificación de alerta en la plataforma de Telegram.

Si la persona sospechosa sigue en las inmediaciones sigue tomando fotografías y enviándolas al grupo de Telegram.

Figura 27

Notificaciones enviadas por el sistema a Telegram.

Detección de comportamiento inusual de vehículos y registro de placas

El proceso de reconocimiento de matrículas se lleva a cabo a través del análisis de los cuadros de vídeo. En caso de que se identifique un vehículo en la imagen, se inicia la evaluación de la placa asociada. Si la matrícula coincide con alguno de los registros almacenados en la base de datos, se concede el acceso, tal como se muestra en las siguientes ilustraciones. Estas etapas incluyen la identificación de la matrícula y la determinación del propietario del vehículo. Sin embargo, en el escenario en el que el vehículo no esté registrado en la base de datos, se categoriza como un "vehículo no identificado" y se toman las medidas apropiadas según la configuración de seguridad establecida.

La relevancia de este sistema de reconocimiento de matrículas radica en su capacidad para fortalecer la seguridad y el control de acceso de manera eficiente. Al permitir la identificación automática de vehículos autorizados, se reduce el riesgo de intrusos no deseados y se agiliza el proceso de entrada. Además, al registrar y asociar matrículas con propietarios, se facilita la gestión de visitantes y la generación de registros. Este enfoque inteligente no solo optimiza la

seguridad, sino que también mejora la experiencia global de control de acceso, convirtiéndose en una herramienta esencial para mantener un entorno seguro y bien administrado.

Figura 28

Detección de los dígitos de la placa de un vehículo.

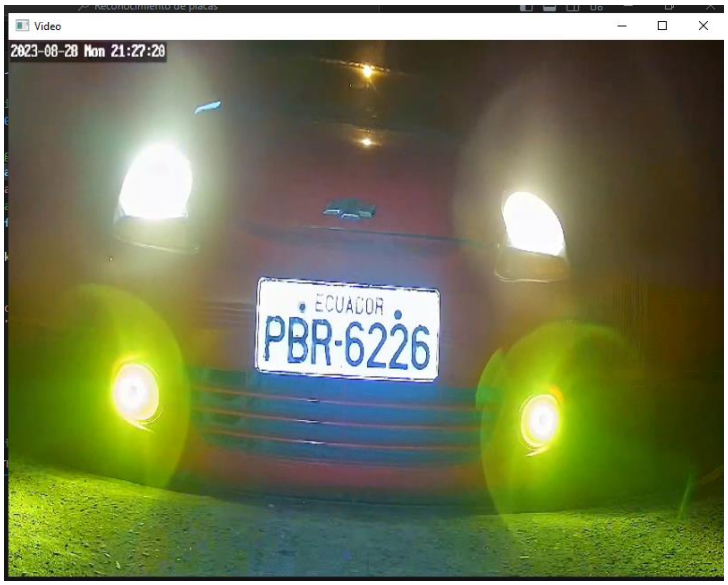


Figura 29

Análisis en el sistema para reconocimiento de placas.

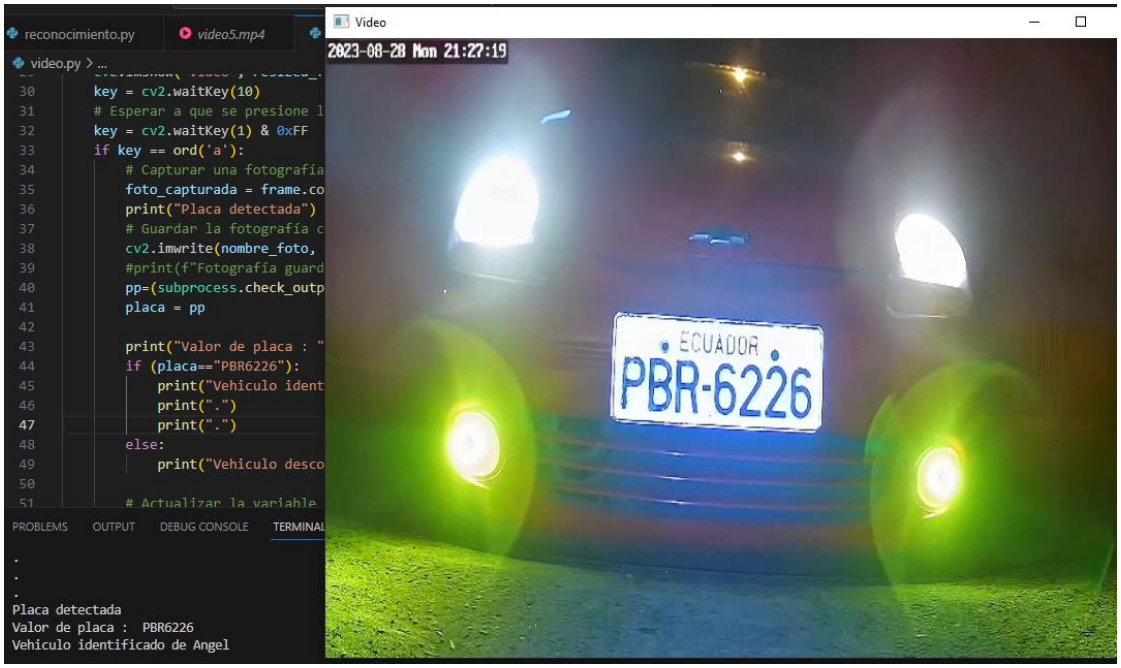
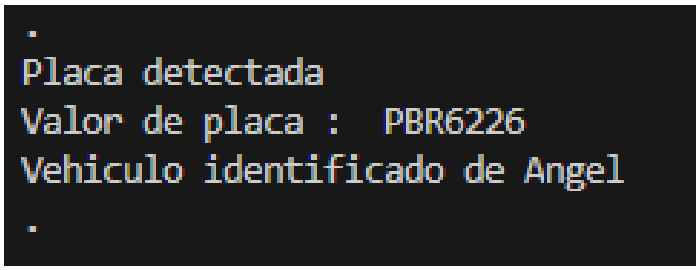


Figura 30

Control de acceso de vehículo al estar registrado en base de datos.



Confiabilidad del sistema

Las pruebas de funcionamiento expuestos anteriormente se realizaron en 12 personas ajenas a la propiedad y 4 personas habitantes de la casa. En la tabla 6 se muestran los resultados arrojados cuando se detectaron a las 12 personas que no estaban en la base de datos de la casa.

Tabla 6

Datos de personas desconocidas en el sistema.

Individuo	Detección como desconocido	Detección como habitante del Hogar	Confianza
Persona 1	SI	NO	Desconocida
Persona 2	SI	NO	Desconocida
Persona 3	SI	NO	Desconocida
Persona 4	SI	NO	Desconocida
Persona 5	SI	NO	Desconocida
Persona 6	SI	NO	Desconocida
Persona 7	SI	NO	Desconocida
Persona 8	SI	NO	Desconocida
Persona 9	SI	NO	Desconocida
Persona 10	SI	NO	Desconocida
Persona 11	SI	NO	Desconocida
Persona 12	SI	NO	Desconocida

Como se determina en la tabla anterior, se tiene una muestra de 12 personas en la cuales en la totalidad de las 12 personas fueron catalogados como desconocido con una confianza desconocida o nula, por lo cual al momento de realizar el nivel de confiabilidad del sistema para personas desconocidas, se tiene un 100% de confiabilidad para detectar personas desconocidas o ajenas al domicilio.

En la tabla 7 se muestra los resultado para los 4 habitantes del hogar, en el cual se muestra el porcentaje de confianza en las 5 interacciones que realiza el sistema para evitar falsos

positivos, y se determina si al final el sistema lo reconoce como habitante del hogar o como persona desconocida.

Tabla 5

Personas habitantes del hogar.

Individuo	Confianza en 5 Interacciones	Detección como habitante del Hogar	Detección como Desconocido
Persona 1	I1: 80.72 %	SI	NO
	I2: 86.65 %		
	I3: 89.24 %		
	I4: 89.37 %		
	I5: 92.56 %		
Persona 2	I1: 79.12 %	SI	NO
	I2: 88.45 %		
	I3: 90.14 %		
	I4: 90.27 %		
	I5: 92.86 %		
Persona 3	I1: 80.52 %	SI	NO
	I2: 85.76 %		
	I3: 83.85 %		
	I4: 89.22 %		
	I5: 90.36 %		
Persona 4	I1: 90.63 %	SI	NO
	I2: 89.16 %		
	I3: 91.42 %		
	I4: 87.65 %		
	I5: 92.06 %		

Según la tabla se tiene un promedio de confianza de las 5 interacciones de la persona 1 de 87.71 %, mientras que para la persona 2 se tiene un promedio de confianza de 88.16 %, para la persona 3 es de 85.94 % y por último para la persona 4 es de 90.28%, mediante el promedio de cada uno se puede calcular el promedio general del sistema en relación al nivel de confianza en el cual se determina en que el sistema tiene un promedio de nivel de confianza de 88% para el reconocimiento de rostros de los habitantes del hogar.

Al realizar las 5 interacciones para cada persona y así detectar que se trate de resultados estables se evita detectar falsos positivos y que se pueda abrir la puerta cuando no debe ser el caso, en la tabla se muestra que en las 4 personas después de las 5 interacciones se determinó como habitante del hogar, teniendo un 100% en la confiabilidad del sistema al momento de detectar las personas que viven en la casa.

Como último punto cabe indicar que las muestras tomadas para los habitantes del hogar, no se relacionan o se tienen rasgos familiares muy marcados entre sí o similitudes.

CONCLUSIONES

En la exploración y contextualización de los fundamentos teóricos sobre inteligencia artificial, se ha logrado establecer una base de conocimientos para comprender los principales conceptos que se enfocan a sistemas de videovigilancia inteligentes. Al momento de realizar la contextualización sobre inteligencia artificial se pudo conocer con más profundidad los sistemas que se enfocan al procesamiento de imágenes, siendo el principal método para el proyecto el de redes neuronales convolucionales, por lo cual fue el que se adoptó al sistema de videovigilancia con inteligencia artificial. La adquisición de la base teórica referente a este método de IA, brindó un mejor enfoque para la realización del presente proyecto ya que se obtuvo parámetros importantes referentes al funcionamiento de las CNN y así trabajar de la mejor forma para la videovigilancia.

Se determinaron los elementos electrónicos necesarios para desarrollar el sistema de videovigilancia, mediante un análisis de los requisitos del proyecto se han identificado y seleccionado los componentes adecuados para garantizar la captura y procesamiento de imágenes. Se seleccionó una Raspberry Pi como mejor opción para que sea el servidor local, aquí se encuentra el algoritmo de inteligencia artificial y en el cual se establece la base de datos tanto para el reconocimiento facial como para la detección de objetos. Mediante sus 8 GB de RAM, cumple con los requerimientos necesarios del sistema para que realice el procesamiento de los frames de video y realice el análisis de videovigilancia IA. Para la captura de video, se optó por cámaras IP, ya que estas proporcionan mayor facilidad al momento de capturar el video. A través de la dirección IP, se pudieron procesar mediante Python los frames y así llevar a cabo el proyecto. Al momento de activar el control de acceso, se determinó que el microcontrolador ESP32 era la mejor alternativa, ya que se puede conectar a una red WiFi y enviar o recibir información mediante la misma.

Se desarrolló el algoritmo de inteligencia artificial utilizando el lenguaje de programación Python a través de la aplicación de técnicas avanzadas de aprendizaje automático y procesamiento de imágenes, aquí se utilizó las redes neuronales convolucionales para extraer las características del rostro de los habitantes del hogar y también para detectar los rostros y los rasgos faciales en los frames del video, para la detección de objetos en el cual se planteó detectar si hay un arma en el sistema de videovigilancia se utilizó 2000 imágenes con sus respectivos archivos en XML, se realizó el entrenamiento mediante CNN y Yolo para que el sistema sea capaz de detectar y analizar situaciones de riesgo en el entorno del sistema de videovigilancia. Si el sistema detecta algo inusual ya sea un arma o una persona desconocida en

las inmediaciones el algoritmo remitirá una notificación al grupo de Telegram de los habitantes del hogar con la fotografía de las inmediaciones.

Se realizó la fase de validación del sistema de videovigilancia implementado en el domicilio mediante pruebas de funcionamiento, en donde se pueda determinar el correcto funcionamiento del control de acceso mediante el protocolo MQTT y el envío de notificaciones si se detecta algo sospechoso en las inmediaciones. La aplicación del sistema de videovigilancia y control de acceso mediante inteligencia artificial en un entorno real, brinda la oportunidad de recopilar datos reales y evaluar su desempeño en condiciones prácticas. Por lo tanto, la validación del correcto funcionamiento del sistema implementado en el domicilio del barrio San Cristóbal del cantón Shushufindi es esencial para asegurar su eficacia y confiabilidad en la detección de situaciones de emergencia y también el control de acceso.

RECOMENDACIONES

Continuar actualizándose sobre las últimas tendencias en inteligencia artificial y procesamiento de imágenes para estar al tanto de nuevas técnicas y enfoques que puedan mejorar aún más la precisión y eficacia del sistema de videovigilancia.

Se puede considerar la posibilidad de explorar cómo las técnicas de transferencia de aprendizaje podrían ser aplicadas para mejorar la eficiencia del entrenamiento y la precisión del modelo de reconocimiento facial y detección de objetos con el objetivo de plantear nuevos sistemas capaces de identificar cualquier tipo de situación e inclusive la detección parcial de rostros.

Realizar pruebas exhaustivas para encontrar el equilibrio entre la precisión del modelo y su eficiencia en la Raspberry Pi, asegurando que el sistema de videovigilancia mantenga un rendimiento óptimo en este entorno con recursos limitados. Además, Investigar y comparar otras alternativas de microcontroladores y placas de desarrollo que podrían ofrecer un mejor rendimiento y características para aplicaciones de videovigilancia inteligente.

Considerar la posibilidad de implementar técnicas de detección de anomalías en conjunto con las redes neuronales convolucionales para identificar comportamientos inusuales en el entorno de videovigilancia.

Considerar la recopilación continua de datos de validación en entornos reales para mejorar y ajustar periódicamente el sistema a medida que se enfrenta a situaciones nuevas y cambiantes.

Para socializar y dar a conocer a la comunidad sobre este tipo de tecnologías de cámaras de videovigilancia y control de acceso, se recomienda llevar a cabo una estrategia de comunicación que combine presentaciones claras en reuniones comunitarias, información en redes sociales y carteles informativos para resaltar los beneficios en el tema de seguridad que presenta este tipo de sistemas inteligentes.

BIBLIOGRAFÍA

Amores, A. (2017). *Reconocimiento de imágenes en frames de vídeo utilizando redes neuronales*. https://repositorio.espe.edu.ec/handle/21000/13458

Briones Gárate, E. A. (2020). *Sistema web de reconocimiento facial para control de acceso biométrico, utilizando inteligencia artificial* [MasterThesis, ESPOL. FIEC]. http://www.dspace.espol.edu.ec/handle/123456789/50333

Britti, G. (2021). *Servicios de video vigilancia hogareño con soporte de inteligencia artificial*. http://repositorio.udesa.edu.ar/jspui/handle/10908/18682

Caba Costales, C. S., & Jara Chávez, C. V. (2018). *Reconocimiento y creación del modelo facial 3D mediante sistema de vídeo aplicado a la seguridad usando inteligencia artificial.* [BachelorThesis, Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/9198

Cataño-Añazco, K. E., Sevincha-Chacabana, M. A., Vargas-Salas, O., & Barragán-Huamán, H. Y. (2023). La inteligencia artificial y la video-vigilancia en la predicción y detección de delitos en espacio-tiempo: Una revisión sistemática. *Revista Criminalidad*, *65*(1), Article 1. https://doi.org/10.47741/17943108.398

Changotasig Yánez, J. F. (2023). *PROCESAMIENTO DIGITAL DE IMÁGENES MEDIANTE INTELIGENCIA ARTIFICIAL PARA LA DETECCIÓN DE ACCIDENTES DE TRÁNSITO EN QUITO* [MasterThesis, Quito, Ecuador: Editorial UISRAEL]. http://repositorio.uisrael.edu.ec/handle/47000/3508

CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL + CAMA[...]. (s. f.). Open Support. Recuperado 28 de agosto de 2023, de http://www.opensupport.com.bo/shop/product/biocam300-control-de-acceso-por-reconocimiento-facial-cama-13095?category=83&page=5

Cornieles, P. (2019, marzo 20). ¿Por qué los controles de acceso de biometría de voz son los más eficaces?. *IA Latam*. ttps://ia-latam.com/2019/03/20/por-que-los-controles-de-acceso-de-biometria-de-voz-son-los-mas-eficaces/

Esteban Nieto, N. (2018). *Tipos de Investigación*.

Guerrero Moreno, D. M. (2017). *Diseño e implementación de un sistema de video vigilancia utilizando cámaras IP y tecnología OPEN SOURCE que permite el acceso remoto por web al sistema y el envío de notificaciones vía correo electrónico para el laboratorio de computación de la unidad educativa "ZEUS"* [BachelorThesis, Quito: Universidad Israel, 2017]. http://repositorio.uisrael.edu.ec/handle/47000/1300

Gutiérrez Santamarta, D. (2021, julio). *Videovigilancia IA* [Info:eu-repo/semantics/bachelorThesis]. E.T.S.I de Sistemas Informáticos (UPM). https://oa.upm.es/68128/

León Rodríguez, G. de la C., & Viña Brito, S. M. (2017). *La inteligencia artificial en la educación superior. Oportunidades y amenazas*. https://doi.org/10.33890/innova.v2.n8.1.2017.399

Manuel. (2021, julio 29). Control de Acceso Biométrico | Tipos y beneficios de implantarlo. *Blog de Recursos Humanos de Bizneo HR: práctico y actual*. https://www.bizneo.com/blog/control-de-acceso-biometrico/

Mella, C. (2023, julio 10). *La inseguridad en Ecuador escala a niveles históricos y se impone como prioridad del próximo Gobierno*. El País. https://elpais.com/internacional/2023-07-10/la-inseguridad-en-ecuador-escala-a-niveles-historicos-y-se-impone-como-prioridad-del-proximo-gobierno.html

Planet, N. (s. f.). *Accesos biométricos: Qué son, cómo funcionan y cuál necesitas*. Recuperado 28 de agosto de 2023, de https://blog.nuoplanet.com/accesos-biometricos-que-son-como-funcionan-y-cual-necesitas

Procesamiento de imágenes. (2023, agosto 11). https://www.vistronica.com/blog/post/procesamiento-de-imagenes.html

¿Qué es el reconocimiento facial? - Explicación del software de reconocimiento facial y análisis facial - AWS. (2023, agosto 18). Amazon Web Services, Inc. https://aws.amazon.com/es/what-is/facial-recognition/

¿Qué son las redes neuronales convolucionales? | IBM. (2023, agosto 18). https://www.ibm.com/es-es/topics/convolutional-neural-networks

RFID para la gestión del control de acceso que le gustaría saber: Xinyetong. (s. f.). *Https://Www.Asiarfid.Com/Es*. Recuperado 28 de agosto de 2023, de https://www.asiarfid.com/es/rfid-for-access-control.html

Santander, C. (2023, agosto 11). *Machine Learning vs. Deep Learning—CDA Informática*. https://www.cdainfo.com/es/noticias/148-machine-learning-vs-deep-learning

Tipos de cámaras de vigilancia para casa: Analógica o digital. (2021, noviembre 26). Blog HomeGO. https://homego.es/blog/tipos-de-camara-de-vigilancia-para-casa-analogica-o-digital/

Villegas, J. (s. f.). *¿Qué es un Sistema de Control de Acceso?* Recuperado 28 de agosto de 2023, de https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

ANEXOS

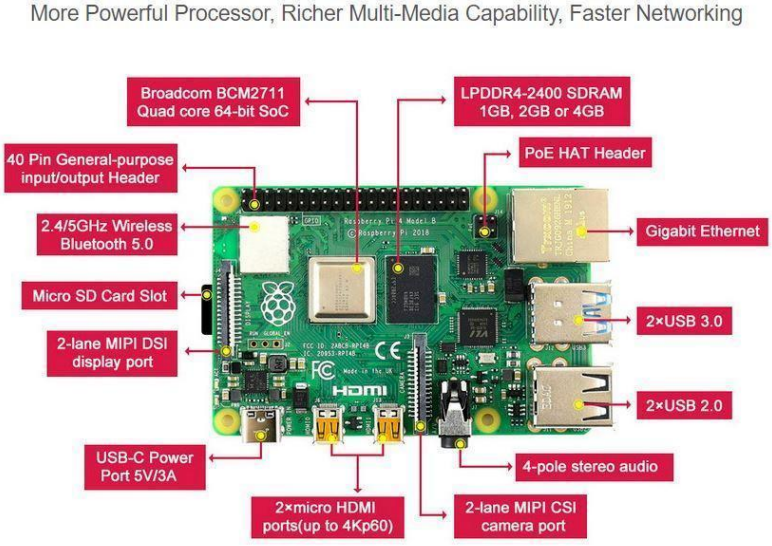
ANEXO 1

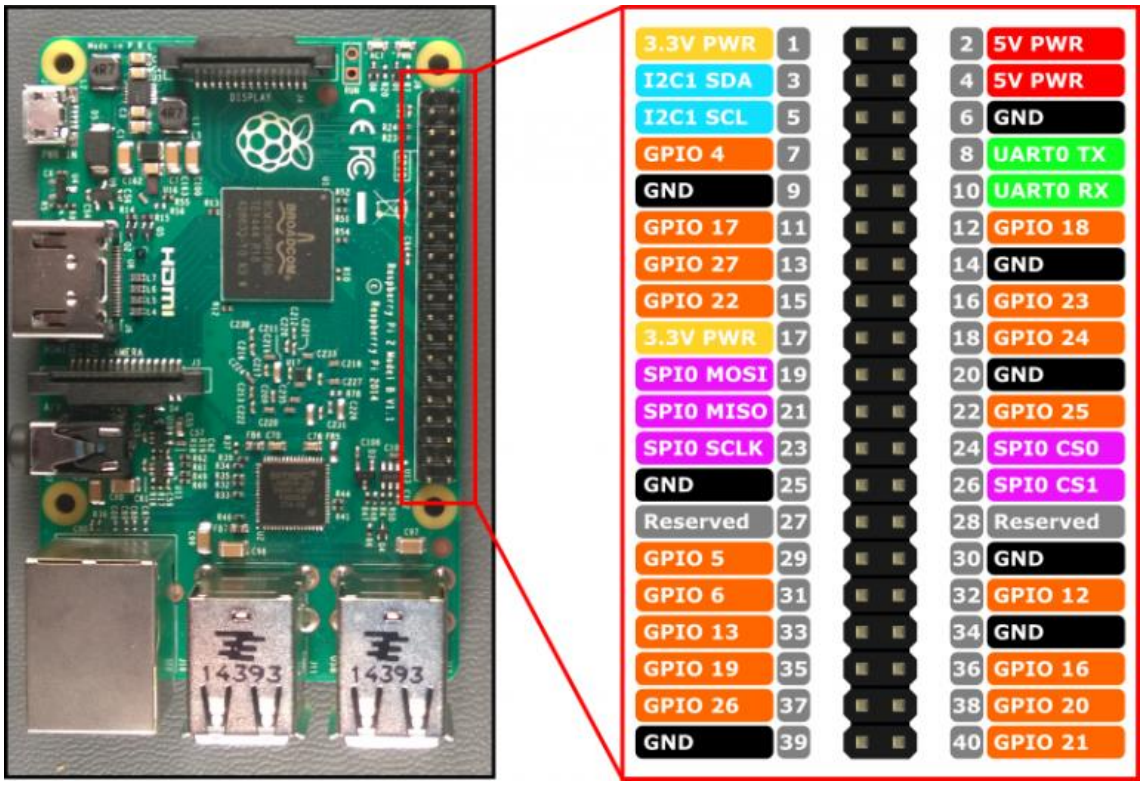
Datos técnicos de la cámara de videovigilancia

Características técnicas	
Modelo	Cámara WiFi inalámbrica Tuya Smart 5.0MP
Dieta	CC5V 1.5A
píxeles	Cámara de 5,0 megapíxeles
Lente	3,6 mm
Velocidad de fotogramas por segundo	15 fps
corte IR	Incluido
Vision nocturna	8 - 10 metros
Audio bidireccional	Soportado
Entrada de audio	Micrófono incorporado
Salida de audio	altavoz integrado
Proceso de vídeo	H.265; soporte de doble flujo
píxel	2560 × 1920
Wifi	IEEE 802.11 b/n/g 2,4 GHz
Motor PTZ	Control de motores integrado
Ángulo de rotación	Horizontales: 355° Verticales: 90°
memoria local	Admite tarjetas de memoria de hasta 128G TF (tarjeta SD no incluida)
Temperatura de funcionamiento	-10°C ~ +50°C
Ambiente	Cámara para uso en interiores
Humedad de funcionamiento	Menos del 95% de humedad relativa
Control de voz compatible	Amazon Alexa - Página principal de Google
Dimensiones	9X8,5X15cm

ANEXO 2

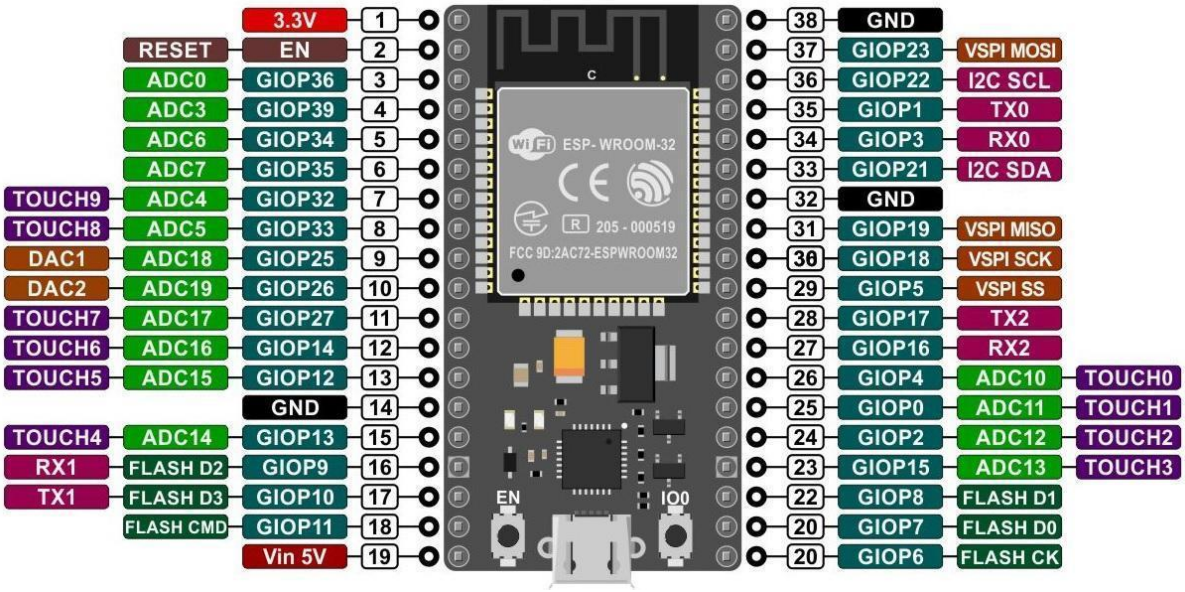
Diagrama electrónico de la Raspberry Pi 4





ANEXO 3

Diagrama electrónico de la tarjeta ESP32



ANEXO 4

Programación videovigilancia IA Y Control de acceso

```
import cv2
import face_recognition
import os, sys
import numpy as np
import math
import time
import paho.mqtt.client as mqtt
import requests
bandera=0
camera_url = "http://192.168.31.138:8080/video"
mqtt_broker = "34.176.12.65"
mqtt_topic = "/motor"
g=0
recognized_person = None
recognized_start_time = None
noelapsed_time=0
elapsed_time=0
def face_confidence(face_distance, face_match_threshold=0.6):
    range=(1.0 - face_match_threshold)
    linear_val = (1.0 - face_distance)/(range * 2.0)

    if face_distance > face_match_threshold:
        return str(round(linear_val*100,2))+"%"
    else:
        value=(linear_val + ((1.0 - linear_val)* math.pow((linear_val - 0.5) * 2, 0.2)))*100
        return str(round(value,2))+"%"
```

```
class FaceRecognition:
    face_locations=[]
    face_encodings=[]
    face_names=[]
    known_face_encodings=[]
    known_face_names=[]
    process_current_frame=True
    unknown_start_time = None

    def __init__(self):
        self.encode_faces()

    def encode_faces(self):
        for image in os.listdir('faces'):
            face_image=face_recognition.load_image_file(f'faces/{image}')
            face_encoding=face_recognition.face_encodings(face_image)[0]

            self.known_face_encodings.append(face_encoding)
            self.known_face_names.append(image)

    def run_recognition(self):
        global g, recognized_person, recognized_start_time, noelapsed_time, elapsed_time
        video_capture = cv2.VideoCapture(camera_url)
        #video_capture = cv2.VideoCapture(0)
        client = mqtt.Client()
        client.connect(mqtt_broker, 1883, 60)
```

videovigilancialA.py > ...

```
                self.face_names=[]
                for face_encoding in self.face_encodings:
                    matches= face_recognition.compare_faces(self.known_face_encodings, face_encoding)
                    faces_distances= face_recognition.face_distance(self.known_face_encodings, face_encoding)
                    best_match_index= np.argmin(faces_distances)
                    if matches[best_match_index]:
                        name = self.known_face_names[best_match_index]
                        confidence = face_confidence(faces_distances[best_match_index])
                        elapsed_time = elapsed_time+1
                        print(f"Habitante del hogar: {elapsed_time}"+"")
                        time.sleep(1)
                        if elapsed_time >= 5:
                            client.publish(mqtt_topic, "on")
                            print("Puerta abierta")
                            elapsed_time=0
                    else:
                        print("No reconocido")
                        name="Desconocido"
                        confidence="None"
                        print(f"Desconocido: {noelapsed_time}")
                        noelapsed_time = noelapsed_time+1
                        if noelapsed_time >= 15:
                                print("Intruso")
                                intruder_image_path = "intrusos/intruso_" + str(int(time.time())) + ".jpg"
                                cv2.imwrite(intruder_image_path, frame)
                                r=requests.post('https://api.telegram.org/bot6602010613:AAHJdqGZVc67o5BFJFT3u38u99pPsHfpEYg
                                files={'photo': (intruder_image_path, open(intruder_image_path, 'rb'))}
```

ideovigilancialA.py > ...

```
                            noelapsed_time=0
                        self.face_names.append(f'{name} ({confidence})')

            self.process_current_frame = not self.process_current_frame

            for (top,right, bottom, left), name in zip(self.face_locations, self.face_names):
                top *= 4
                right *= 4
                bottom *= 4
                left *= 4

                cv2.rectangle(frame, (left, top), (right, bottom), (0,0,255), 2)
                cv2.rectangle(frame, (left, bottom - 35), (right, bottom), (0,0,255), -1)
                cv2.putText(frame, name, (left + 6, bottom - 6), cv2.FONT_HERSHEY_DUPLEX, 0.8, (255,255,255), 1)

            cv2.imshow('Reconocimiento', frame)

            if cv2.waitKey(1) == ord ('q'):
                break

        video_capture.release()
        cv2.destroyAllWindows()
        client.loop_stop()
        client.disconnect()
```