INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO

TECNOLOGÍA SUPERIOR EN ELECTRÓNICA

"IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023."

INFORME DEL PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN LA TECNOLÓGÍA SUPERIOR EN ELECTRÓNICA.

AUTOR:

Castillo Torres Duván Anival

DIRECTORA:

Ing. Mingo Morocho Leydi Maribel, Mgs.

Loja, 07 de noviembre del 2023

a. Certificación

Ing.

Leydi Maribel Mingo Morocho, Mgs.

DIRECTORA DE INVESTIGACIÓN

CERTIFICA:

Que ha supervisado el presente proyecto de investigación titulado "IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023." el mismo que cumple con lo establecido por el Instituto Superior Tecnológico Sudamericano; por consiguiente, autorizo su presentación ante el tribunal respectivo.

Loja, 07 de noviembre de 2023

…….

Firma

Ing. Leydi Maribel Mingo Morocho, Mgs.

b. Declaración juramentada

Loja, 07 de noviembre de 2023

Nombres: Duván Anival

Apellidos: Castillo Torres

Cédula de Identidad: 1104574445

Carrera: Electrónica

Semestre de ejecución del proceso de titulación: Abril – Agosto 2023

Tema de proyecto de investigación de fin de carrera con fines de titulación:

"IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023."

En calidad de estudiante del Instituto Superior Tecnológico Sudamericano de la ciudad de Loja;

Declaro bajo juramento que:

1. Soy autor del trabajo intelectual y de investigación del proyecto de fin de carrera.
2. El trabajo de investigación de fin de carrera no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas.
3. El trabajo de investigación de fin de carrera presentado no atenta contra derechos de terceros.

4. El trabajo de investigación de fin de carrera no ha sido publicado ni presentado anteriormente para obtener algún grado académico previo o título profesional.
5. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados, ni copiados. Las imágenes, tablas, gráficas, fotografías y demás son de mi autoría; y en el caso contrario aparecen con las correspondientes citas o fuentes.

Por lo expuesto; mediante la presente asumo frente al INSTITUTO cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del trabajo de investigación de fin de carrera.

En consecuencia, me hago responsable frente al INSTITUTO y frente a terceros, de cualquier daño que pudiera ocasionar al INSTITUTO o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causa en el trabajo de investigación de fin de carrera presentado, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello.

Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para EL INSTITUTO en favor de terceros por motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación de fin de carrera.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente dispuesta por la

LOES y sus respectivos reglamentos y del Instituto Superior Tecnológico Sudamericano de la ciudad de Loja.

Firma ……

Nro. Cédula 11045744

c. Dedicatoria

Este proyecto está dedicado con un profundo sentimiento de gratitud a todas las personas que han sido una fuente inagotable de motivación a lo largo de mi trayecto académico. En particular, deseo expresar mi sincero reconocimiento a mi querida señora Michu y a mi hijita Renata, quienes siempre han sido mi inquebrantable fuente de inspiración, impulsándome a seguir adelante en esta travesía. Asimismo, quiero manifestar mi más profundo agradecimiento a mi directora de tesis, cuya guía experta y apoyo incansable fueron fundamentales para la realización de este proyecto. No puedo dejar de mencionar a mis abuelitos y amigos, quienes han permanecido a mi lado brindándome su amor, cariño y confianza en todo momento. Esta dedicación es un tributo a todos ellos, con la esperanza ferviente de que este proyecto contribuya al avance de la tecnología en nuestra sociedad.

Castillo Torres Duván Anival

d. Agradecimiento

Es con un profundo sentido de agradecimiento que dirijo estas palabras al Instituto Superior Tecnológico Sudamericano, una institución que me brindó la invaluable oportunidad de forjar mi camino como profesional en el fascinante campo de la electrónica. En este viaje de aprendizaje, no puedo pasar por alto el papel fundamental desempeñado por los dedicados docentes que me acompañaron en cada paso de mi formación. Su esfuerzo incansable y su pasión por la enseñanza han dejado una huella indeleble en mi camino académico.

Finalmente, quiero expresar mi más sincero agradecimiento a mi familia y amigos, quienes han sido un sólido pilar de apoyo a lo largo de esta travesía. Sus palabras alentadoras y su respaldo inquebrantable han sido la fuerza impulsora detrás de mis logros. Sin su comprensión y apoyo, nada de esto hubiera sido posible. Mi corazón se llena de gratitud y reconocimiento hacia todos ustedes.

Castillo Torres Duván Anival

e. Acta de cesión de derechos

ACTA DE CESIÓN DE DERECHOS DE PROYECTO DE INVESTIGACIÓN DE FIN DE CARRERA

Conste por el presente documento la Cesión de los Derechos de proyecto de investigación de fin de carrera, de conformidad con las siguientes cláusulas:

PRIMERA. - Por sus propios derechos; la Ing. Leydi Maribel Mingo Morocho, en calidad de Directora del proyecto de investigación de fin de carrera; y, Duván Anival Castillo Torres, en calidad de autor del proyecto de investigación de fin de carrera; mayores de edad emiten la presente acta de cesión de derechos

SEGUNDA. – Duván Anival Castillo Torrres, realizó la Investigación titulada titulado "IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023." para optar por el título de Tecnólogo en Electrónica, en el Instituto Superior Tecnológico Sudamericano de Loja, bajo la dirección de la Ing. Leydi Maribel Mingo Morocho.

TERCERA.- Es política del Instituto que los proyectos de investigación de fin de carrera se apliquen y materialicen en beneficio de la comunidad.

CUARTA. - Los comparecientes Ing. Leydi Maribel Mingo Morocho, en calidad de Director del proyecto de investigación de fin de carrera y Duván Anival Castillo Torres como autor, por medio del presente instrumento, tienen a bien ceder en forma gratuita sus

derechos de proyecto de investigación de fin de carrera titulado titulado "IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023." a favor del Instituto Superior Tecnológico Sudamericano de Loja; y, conceden autorización para que el Instituto pueda utilizar esta investigación en su beneficio y/o de la comunidad, sin reserva alguna.

QUINTA.- Aceptación.- Las partes declaran que aceptan expresamente todo lo estipulado en la presente cesión de derechos.

Para constancia suscriben la presente cesión de derechos, en la ciudad de Loja, en el mes de octubre del año 2023.

F. _____ F. _____

Ing. Leydi Maribel Mingo Morocho, Mgs
C.I. 1105653792

Duván Anival Castillo Torres
C.I. 1104574445

1. Índice de contenidos

a. Certificación II

b. Declaración juramentada III

c. Dedicatoria VI

d. Agradecimiento VII

e. Acta de cesión de derechos VIII

1. Índice de contenidos 10

1.1 Índice de Figuras 15

1.2 Índice de Tablas 17

2. Resumen 18

3. ABSTRACT 19

4. Problema 20

5. Tema 22

6. Línea y sublínea de investigación 23

6.1 Línea de Investigación: 23

6.2 Sub línea de Investigación: 23

7. Justificación 24

8. Objetivos 26

8.1 Objetivo General 26

8.2 Objetivos Específicos 26

Marco teórico 27

9.1 Marco Referencial 27

9.2 Marco Conceptual 28

9.2.1 Sistema de seguridad 28

9.2.2 Seguridad electrónica 29

9.2.3 Sistema de control de acceso electrónico. 29

9.2.4 Métodos de autenticación 29

9.2.5 Cards RFID 30

9.2.6 Acreditación basada en el móvil 30

9.2.7 El código QR 30

9.2.8 El número de PIN 30

9.2.9 Biometría 30

9.2.10 Inteligencia Artificial 31

9.2.11 Visión por computadora 33

9.2.12 Detección de objetos 33

9.2.13 Análisis de vídeo 33

9.2.14 Aplicaciones de la visión por computadora 34

9.3 Librería OpenCV 35

9.4 Trabajos Relacionados 36

10. Diseño Metodológico 38

10.1 Métodos de investigación 38

10.1.1 Método Hermenéutico 38

10.1.2 Método Fenomenológico 38

10.1.3 Método Práctico Proyectual 39

10.2 Técnicas de investigación 39

10.2.1 Técnica de Observación 39

10.2.2 Técnica de investigación documental 40

10.2.3 Técnica de prueba y error 40

11. Propuesta practica de acción 42

11.1 Hardware 42

11.2 Raspberry Pi modelo 4B 42

11.3 Puertos Gpio de la tarjeta Raspberry pi 43

11.4 Módulo de cámara Raspberry Pi 44

11.5 Modulo Relé 45

11.6 Cerradura electrónica DC 12V. 46

11.7 Sensor de interruptor de contacto magnético 47

11.8 Software 48

11.9 Rasberry pi imager 49

11.10 Sistema Operativo Raspbian 50

11.11 Advanced IP Scanner 51

11.12 MobaXterm 52

11.13 Realvnc viewer 53

11.14 Herramientas de software 54

11.15 Python 55

11.16 Telegram 56

12. Desarrollo de la propuesta de acción 57

12.1 Diseño y construcción del prototipo 57

12.1.1 Conexión de la cámara y relé a la tarjeta Raspberry Pi 57

12.1.2 Conexión y funcionamiento de la cámara 58

12.1.3 Configuración de la tarjeta Raspberry Pi 4. 59

12.1.4 Instalación a través de consola de las diferentes bibliotecas 60

12.1.5 Configuración del Boot en Telegram 61

12.2 Funcionamiento general del Prototipo 61

12.2.1 Diagrama de flujo 62

12.2.2 Captura de imágenes 64

12.2.3 Entrenamiento 66

12.2.3.1 Algoritmo LBP. 67

12.2.4 Reconocimiento 68

12.3 Proceso de instalación física del Prototipo 70

12.4 Prueba de funcionamiento y resultados 71

12.4.1 Pruebas 71

12.4.2 Resultados 72

13. Conclusiones 77

14. Recomendaciones 79

15. Bibliografía 80

16. Anexos 84

16.1 Anexo I: Certificado de aprobación 84

16.2 Anexo II: Autorización para la ejecución 85

16.3 Anexo III: Certificado de implementación 86

16.4 Anexo IV: Presupuesto 87

16.5 Anexo V: Cronograma 90

16.6 Anexo VI: Programación 91

16.6.1 Programación detección de rostro 91

16.6.2 Programación para el entrenador 94

16.6.3 Programa activador 97

16.7 Anexo VII: Conexión de sensor. 102

16.8 Anexo VIII: Certificado del Abstract 104

1.1 Índice de Figuras

Figura 1 Ubicación del Prototipo 28

Figura 2 Tarjeta Raspberry Pi 4 43

Figura 3 Puertos Gpio de la tarjeta Raspberry pi. 44

Figura 4 Módulo de cámara Raspberry Pi..... 45

Figura 5 Modulo Relé 46

Figura 6 Solenoide tipo chapa 12V. 47

Figura 7 Sensor de interruptor de contacto magnético..... 48

Figura 8 Rasberry pi imager..... 49

Figura 9 Activación Protocolo SSH 50

Figura 10 Sistema Operativo Instalado 51

Figura 11 Advanced IP Scanner..... 52

Figura 12 MobaXterm..... 53

Figura 13 Realvnc viewer 54

Figura 14 Thonny Python..... 55

Figura 15 Entorno de Telegram 56

Figura 16 Diagrama electrónico..... 57

Figura 17 Conexión Raspberry con módulo de cámara 58

Figura 18 Cámara funcionando..... 59

Figura 19 Comandos para la configuración inicial. 60

Figura 20 Comandos utilizados..... 60

Figura 21 Configuración del Boot en Telegram 61

Figura 22 Arquitectura general del proyecto. 62

Figura 23 Diagrama de flujo 63

Figura 24 Diagrama de flujo captura de video 64

Figura 25 Detección de un rostro 65

Figura 26 Base de datos 66

Figura 27 Clasificación 67

Figura 28 Diagrama de flujo del entrenamiento. 68

Figura 29 Diagrama Reconocimiento Facial y envió de notificaciones a Telegram…..69

Figura 30 Prototipo Instalado 70

Figura 31 Cerradura Instalada 70

Figura 32 Usuario 1 73

Figura 33 Notificación a Telegram 73

Figura 34 Usuario 2 74

Figura 35 Notificación a Telegram segundo usuario. 74

Figura 36 Usuario 3 75

Figura 37 Notificación a Telegram tercer usuario. 75

Figura 38 Usuario no registrado 76

Figura 39 conexión de la cámara y sensor magnético 102

Figura 40 Pruebas de sensor magnetico 102

Figura 41 Programación para la prueba del sensor 103

1.2 Índice de Tablas

Tabla 1 Pruebas de intentos Realizados. 71

Tabla 2 Componentes para el prototipo. 87

Tabla 3 Recursos del proyecto 88

Tabla 4 Presupuesto del proyecto 89

Tabla 5 Cronograma de actividades 90

2. Resumen

En la actualidad, la problemática de la inseguridad en las viviendas ha llevado a la búsqueda de soluciones más accesibles y efectivas. Los recursos tradicionales de seguridad suelen ser costosos e ineficientes. El objetivo principal del proyecto es implementar un sistema innovador que aborde esta problemática. Se trata de un sistema de reconocimiento facial con notificaciones móviles utilizando Raspberry Pi para el control de acceso residencial. El diseño del sistema de autentificación se llevó a cabo directamente en la Raspberry Pi 4, con la ayuda de Python y las bibliotecas de OpenCV, cuya eficacia se evaluó en una base de datos de 5 personas. Este sistema se diseñó con dos parámetros que funcionan conjuntamente: la creación de una base de datos que permite agregar de manera sencilla a los individuos y el reconocimiento facial que permite identificar a la persona. El objetivo de este sistema es proporcionar una solución más asequible y eficiente para mejorar la seguridad en los hogares. Se emplearon varios métodos de investigación, incluyendo el método hermenéutico para interpretar los datos observados y plantear una solución viable que involucra tecnología tangible e intangible, como teléfonos celulares y software; el método fenomenológico para comprender cómo las personas toman medidas de precaución para proteger sus hogares y cómo la falta de sistemas de seguridad asequibles afecta sus decisiones; y el método práctico proyectual, que se centró en la implementación real del sistema de seguridad en una vivienda. Se llevaron a cabo pruebas de campo para verificar su funcionamiento, logrando una tasa de identificación de rostros del 80%. Además, se realizaron experimentos en cada una de las etapas del sistema para evaluarlo con sus puntos favorables y desfavorables.

Palabras Claves: Reconocimiento, facial, Raspberry, OpenCv.

3. ABSTRACT

Currently, the problem of housing insecurity has led to the search for more accessible and effective solutions. Traditional security resources are often expensive and inefficient. The main objective of the project is to implement an innovative system that addresses this problem.

The main objective of the project is to implement an innovative system that addresses this problem. This is a facial recognition system with mobile notifications using Raspberry Pi for residential access control. The design of the authentication system was carried out directly on the Raspberry Pi 4, with the help of Python and OpenCV libraries, the effectiveness of which was evaluated on a database of 5 people. This system was designed with two parameters that work together: the creation of a database that allows individuals to be easily added and facial recognition that allows the person to be identified. The goal of this system is to provide a more affordable and efficient solution to improve home security. Various research methods were used, including the hermeneutic method to interpret the observed data and propose a viable solution that involves tangible and intangible technology, such as cell phones and software; the phenomenological method to understand how people take precautionary measures to protect their homes and how the lack of affordable security systems affects their decisions; and the practical project method, which focused on the actual implementation of the security system in a home.

Field tests were carried out to verify its operation, achieving a face identification rate of 80%. In addition, experiments were carried out in each of the stages of the system to evaluate it with its favorable and unfavorable points.

Keywords: Recognition, facial, Raspberry, OpenCv.

TRADUCIDO POR. Lic. Juan Pablo Quezada Rosales

DOCENTE ISTS- CIS

C.I.1104039621

4. Problema

Hoy en día gracias a la integración de internet y las tecnologías emergentes como es la inteligencia artificial tenemos la posibilidad de obtener, procesar y examinar imágenes, formas, colores etc. Con la finalidad de ser tratadas con un ordenador por medio de técnicas que se apliquen para la categorización de las imágenes o la toma de decisiones (Marketing, 2022).

Sin embargo, muchas personas que quieren cubrir las necesidades de control de estos sistemas de seguridad y bienestar optan por adquirir estos sistemas, que suelen ser ineficientes e inseguros. Además, las empresas que venden este tipo de sistema de seguridad ofrecen sus servicios a un precio bastante alto, y a menudo cobrar una mensualidad. Por ejemplo, según el diario La Hora, "Los sistemas de seguridad pueden llegar a tener un costo de 620 dólares, 320 $ en implementación de cámaras y 300$ de la alarma. Agregando un valor mensual de 20 dólares por el monitoreo que brinda el personal de las empresas" Esto conlleva que las personas busquen sistemas que no solo faciliten a los usuarios el manejo del sistema, sino que también ofrezcan más seguridad a los usuarios sin estar sujetos a los altos costos económicos de instalación y artefactos (LA HORA, 2022).

En Ecuador sabemos que la delincuencia es un tema muy importante para tratar ya que día a día la inseguridad sigue teniendo victimas esto se ve reflejado en videos difundidos en redes sociales con imágenes de robos y gente ingresando a hogares ajenos. En 2022 se registró una tasa de 15.48 de muertes por cada 100 mil habitantes debido a esto la Policía Nacional opta por incrementar las cámaras de video vigilancia y alarmas

comunitarias en puntos específicos esto dio una reducción del 31% en la delincuencia (Cmella & Cmella, 2022).

En la ciudad de Loja según las estadísticas, en lo que va del 2023, de enero al 15 de abril, se registran 71 robos a domicilios frente a 89 que se presentaron en el 2022 (La Hora, 2023). Es por esta razón que se requiere reforzar los diferentes sistemas como lo es la video vigilancia Pedro Sánchez, analista del Sistema de Videovigilancia, comentó que en diez sitios se instalaron cámaras con megafonía, que es parte del proyecto piloto para disuadir en temas de seguridad. Al saber que existen cámaras comunales en los diferentes barrios de la ciudad, pero los ciudadanos no tienen acceso directo a la información ya que se tiene que pagar elevados precios para el uso de la plataforma y mantenimiento para su buena funcionalidad (Sarango, 2023).

Es por lo que en el presente proyecto se pretende dar solución a este gran problema como lo es la inseguridad en las viviendas mediante la implementación de un sistema de reconocimiento facial con notificaciones móviles a través de Telegram y así disminuir la inseguridad en nuestros hogares.

5. Tema

"IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023."

6. Línea y sublínea de investigación

6.1 Línea de Investigación:

Desarrollo tecnológico, internet de las cosas, big data e innovación en procesos de automatización y sistematización organizacional.

6.2 Sub línea de Investigación:

Desafíos de la Industria 4.0.

7. Justificación

El presente proyecto se va a trabajar mediante la línea de investigación uno: desarrollo tecnológico, internet de las cosas, big data e innovación en procesos de automatización y sistematización organizacional, porque planea incorporar un sistema de reconocimiento facial utilizando la Raspberry pi que estará conectado a internet y podrá enviar mensajes de alerta a dispositivos móviles. Además, se ajusta a la sub línea desafíos de la Industria 4.0 debido a que el usuario va a ser capaz de tener un registro de las notificaciones y va a poder gestionarlas, estas son características que la Industria 4.0 utiliza para optimizar procesos y tiempos de ejecución.

En la elaboración del siguiente proyecto de investigación se procederá a desarrollar un dispositivo de reconocimiento facial que de acceso a los integrantes una vivienda, en el cual se ven reflejados los conocimientos técnicos y teóricos adquiridos a través de la práctica, ya que, en la carrera la parte práctica y la teórica se han complementado durante toda mi formación, programación, elaboración de circuitos y robótica. Adicionalmente, el proyecto de investigación es la demostración de habilidades y conocimientos adquiridos para la obtención del título de tercer nivel en la Tecnología Superior en Electrónica del Instituto Superior Tecnológico Sudamericano.

Por otra parte, este proyecto de tesis demuestra el uso de diferentes tecnologías emergentes en los últimos años como lo es la inteligencia artificial (AI). Esta tecnología se la puede usar para crear proyectos innovadores, en esta ocasión se la combinara con dispositivos de control electrónico con la finalidad de resolver un problema social que es

la seguridad de viviendas, hoy en día es muy recomendado este tipo de seguridad con inteligencia artificial (AI) ya que los usuarios los prefieren por su eficiencia y seguridad.

Al estar en un entorno donde cada vez la inseguridad en la ciudad crece y como medida de prevención, se propone implementar un sistema de acceso a los integrantes de una vivienda, donde se utilizará técnicas de inteligencia artificial que esta mediante una base de datos que se encontrará alojada en el sistema dará acceso a los integrantes del hogar usando control electrónico. Para llevar a cabo el sistema se procederá a conseguir los diferentes módulos en tiendas electrónicas nacionales ya que su obtención es más rápida y los precios económicos.

8. Objetivos

8.1 Objetivo General

- Implementar un sistema de reconocimiento facial con notificaciones móviles utilizando Rasberry Pi para control de acceso residencial en la ciudad de Loja durante el periodo abril-septiembre 2023.

8.2 Objetivos Específicos

- Realizar una investigación teórica mediante bases científicas para entender la interacción de la Raspberry Pi y las diferentes herramientas de inteligencia artificial (AI).
- Programar la Rasberry Pi para que de acceso a los integrantes de una vivienda haciendo uso de las técnicas de inteligencia artificial (AI).
- Configurar la API de mensajería de seguridad automático mediante software libre para recibir notificaciones en un dispositivo móvil.
- Implementar el prototipo en su ubicación correspondiente para realizar pruebas de funcionamiento y comprobar la eficacia del sistema, asegurando la conectividad, comunicación y continuidad del servicio.

Marco teórico

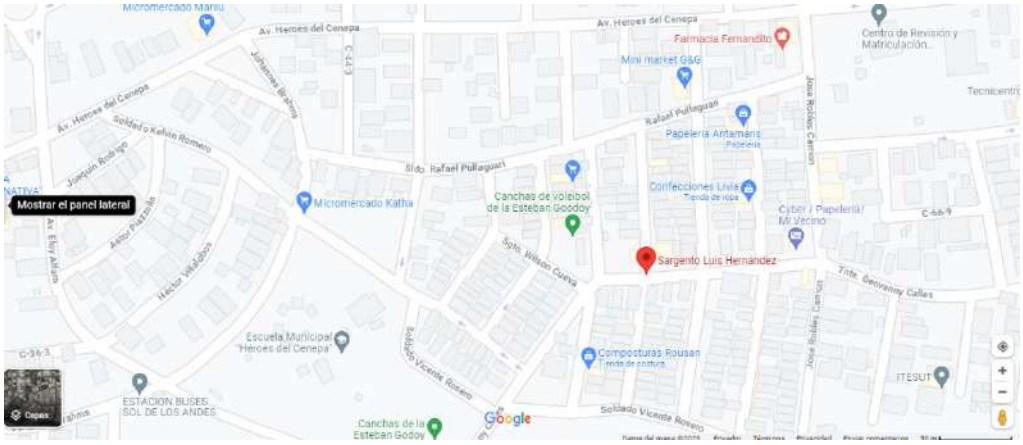
9.1 Marco Referencial

El proyecto de investigación propone realizar un prototipo el cual va a estar instalado en un departamento ubicado en el barrio esteban Godoy primera etapa calles Luis Hernández y Rafael Paraguarí, en la parroquia el sagrario del cantón Loja. En la Figura 1 se muestra la ubicación en el mapa de la ciudad. El acceso a internet en Ecuador es de 80,1% (14,25 millones de usuarios), de los cuales 14 millones accede a redes sociales principalmente desde dispositivos móviles. Pese a ellos, se estima que existen 2,2 millones de personas de 15 a 49 años dentro del analfabetismo digital, definido como aquellos que no tienen celular activado, no ha utilizado computadora no internet en los últimos 12 meses (Pablo, 2021), teniendo esta información el proyecto podría replicarse en un porcentaje considerable de la ciudad por el acceso al internet.

El reconocimiento facial se puede aplicar en el control de accesos a edificios públicos y privados, cajeros automáticos, laboratorios de investigación, como clave secreta de acceso para el uso de ordenadores personales o terminales móviles de última generación, así como para servir de tarjeta de visita de una persona. Teniendo en cuenta estas aplicaciones el proyecto tendría una gran aceptación ya que en ciudad de Loja existen un sin número de cajeros y edificios donde se podría instalar este dispositivo.

Figura 1

Ubicación del Prototipo



Nota. Captura tomada de Google Maps, la marca roja corresponde a la ubicación geográfica donde se instalará el prototipo.

El desarrollo del proyecto se implementó con software y hardware de libre distribución como una Raspberry PI. Llegando a instalar en la Raspberry PI un sistema operativo en base Linux e instalar compiladores para poder programar y controlar los puertos de entrada y salida que dispone la tarjeta, si el sensor de movimiento detecta presencia se activará la cámara y se enviará una notificación a un dispositivo móvil en este caso la aplicación Telegram la cual no tienen costo por mantenimiento o uso de plataforma.

9.2 Marco Conceptual

9.2.1 Sistema de seguridad

El sistema de seguridad es un conjunto de elementos interconectados, cuyo objetivo principal es crear un nivel de protección contra todos los aspectos de riesgo que pueden afectar negativamente a la integridad de la población (personas, familias,

empresas...), peligros, errores o crimen y para crear una sensación de paz para cualquiera de ellos presencia (Secatel, 2019).

9.2.2 Seguridad electrónica

La instalación de una variedad de bienes o servicios en dispositivos electrónicos es la base de la seguridad electrónica. Estos artefactos permiten que los planes de seguridad convencionales se complementen con avisos y controles más estrictos. La protección de las personas, las propiedades y el entorno requiere sistemas de seguridad electrónicos. Estos sistemas basados en tecnología electrónica avanzada ofrecen mayor seguridad y tranquilidad en una amplia gama de aplicaciones. A medida que avanza la tecnología, la capacidad de los sistemas de seguridad electrónicos para detectar y prevenir amenazas seguirá mejorando. Al aprovechar los avances en la inteligencia artificial, el reconocimiento de patrones y la conectividad, estos sistemas se convertirán en una herramienta aún más crucial para garantizar la seguridad en la era digital. (Secatel, 2019).

9.2.3 Sistema de control de acceso electrónico.

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica mediante la validación de la identificación utilizando varios tipos de lectura (clave por teclado, tags de proximidad o biometría), y a su vez controlando el recurso (puerta, torniquete o talanquera) mediante un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor (Villegas, 2009).

9.2.4 Métodos de autenticación

En el mercado tenemos varios sistemas de autenticación algunos más simples que otros pero que cumplen la función de dar acceso a un lugar delimitado entre estos tenemos:

9.2.5 Cards RFID

En primer lugar, el control se puede realizar utilizando tarjetas RFID, que transmiten una señal cuando se acercan a un lector. Y este transmite una secuencia numérica que una controladora verifica.

9.2.6 Acreditación basada en el móvil

Muy parecidas a las tarjetas RFID que utiliza las señales NFC o BLE del propio móvil en lugar de las tarjetas RFID. Para que se pueda encriptar el número de identificación de usuario en el móvil y usarlo sobre el lector, una plataforma debe autenticar previamente este tipo de acreditación mediante una aplicación o correo electrónico.

9.2.7 El código QR

Otro método de autenticación es el código QR. En esencia, se trata de códigos de barras que permiten almacenar y personalizar datos, lo que lo ha hecho muy popular en los últimos diez años. Sin embargo, su incorporación y aplicación en el campo dependen de lectores expertos.

9.2.8 El número de PIN

El usuario puede usar un PIN o número de identificación personal, que es una secuencia numérica que le permite marcar una serie de dígitos en un teclado o lector.

9.2.9 Biometría

Finalmente, la autenticación por biometría, que comenzó con la captura de huellas como método de autenticación individual. Esta estrategia se basa en la captura de puntos

únicos que forman la huella del usuario, y el patrón que conforma la huella es lo que se procesa sobre la plataforma que permite el acceso. Otros como la lectura de venas, iris, palma y reconocimiento facial se han desarrollado a raíz de este método.

9.2.10 Inteligencia Artificial

La inteligencia artificial (IA) se refiere a "la capacidad de las máquinas para imitar o simular la inteligencia humana en la realización de tareas específicas" (Russell & Norvig, 2016, p. 2). Es un campo multidisciplinario que combina la informática, la estadística, las matemáticas y otras disciplinas para desarrollar sistemas y programas que puedan realizar tareas que normalmente requerirían la intervención humana y el uso del razonamiento.

La IA se basa en la idea de que las máquinas pueden ser programadas para "procesar información, aprender de ella y tomar decisiones basadas en esos datos" (Russell & Norvig, 2016, p. 2). En lugar de seguir instrucciones explícitas para cada tarea, los sistemas de IA son capaces de analizar grandes cantidades de datos, reconocer patrones, extraer información relevante y ajustar su comportamiento en función de las experiencias anteriores.

Existen diferentes enfoques dentro de la IA, que incluyen el aprendizaje automático (Machine Learning), que es un enfoque que permite a las máquinas "aprender de los datos y mejorar su rendimiento a medida que se les proporciona más información" (Mitchell, 1997, p. 2). El aprendizaje automático se basa en algoritmos que permiten a los sistemas reconocer patrones y tomar decisiones basadas en esos patrones.

Otro enfoque dentro de la IA son las redes neuronales artificiales (Artificial Neural Networks), que son "estructuras de procesamiento de información inspiradas en la forma en que funciona el cerebro humano" (Russell & Norvig, 2016, p. 19). Estas redes consisten en una red interconectada de nodos o "neuronas" artificiales que procesan y transmiten información. Las redes neuronales se utilizan en el aprendizaje automático para reconocer patrones complejos y realizar tareas como reconocimiento de imágenes, procesamiento del lenguaje natural, entre otros.

El procesamiento del lenguaje natural (Natural Language Processing) es otro enfoque de la IA que se enfoca en la interacción entre las máquinas y el lenguaje humano (Jurafsky & Martin, 2019). Los sistemas de procesamiento del lenguaje natural permiten a las máquinas comprender, interpretar y generar lenguaje humano de manera efectiva. Se utilizan en aplicaciones como asistentes virtuales, traducción automática, análisis de sentimientos, entre otros.

Además, la visión por computadora (Computer Vision) es el campo de la IA que se ocupa de capacitar a las máquinas para interpretar y comprender el contenido visual, como imágenes y videos (Forsyth & Ponce, 2012). Los sistemas de visión por computadora pueden reconocer objetos, realizar seguimiento de movimientos, detectar características y realizar tareas relacionadas con la percepción visual.

La inteligencia artificial tiene una amplia gama de aplicaciones en diversos campos, como la medicina, la industria manufacturera, la automoción, la atención al cliente, la seguridad, entre otros (Russell & Norvig, 2016).

9.2.11 Visión por computadora

La visión por computadora es un campo de la inteligencia artificial que se relaciona con el análisis de imágenes y videos e incluye un conjunto de técnicas que permiten a las computadoras ver y extraer información de lo que se ha visto. Los sistemas están compuestos por una cámara de video o fotográfica y un software especializado que puede identificar y clasificar objetos. Son capaces de analizar caras y emociones, así como imágenes (fotos, imágenes, videos, códigos de barras). Se utilizan tecnologías de aprendizaje automático y se recopilan grandes cantidades de datos para enseñaran una computadora a ver, lo que permite resaltar características y combinaciones de estas para identificar aún más objetos similares (Marketing, 2022).

9.2.12 Detección de objetos

La computadora analiza videos de cámaras utilizando algoritmos para detectar algún objeto extraño. Si esto sucede, el software enviará una señal a la persona o incluso al software encargado de controlar esa zona para que analice por qué ese objeto se encuentra allí. Además, se puede usar para buscar personas, animales u objetos que se han perdido en alguna parte del planeta. En resumen, la tecnología de visión por computadora siempre está atenta al lugar y a las imágenes que se muestran para garantizar un resultado óptimo en el trabajo (RecFaces, 2021).

9.2.13 Análisis de vídeo

El software de visión computarizada tiene grandes posibilidades de análisis de video con el objetivo de crear un esquema completo de lo que está pasando en él, lo que ayuda a analizar una gran cantidad de material de video para poder detectar elementos

importantes, ya sea algún objeto o persona que no debe estar ahí, como también algún fenómeno natural o artificial que ocurra frente a una cámara de vigilancia con el software de visión computarizada (RecFaces, 2021).

9.2.14 Aplicaciones de la visión por computadora

- Reconocimiento óptico de caracteres (OCR): Que consiste en la identificación automáticamente a partir de una imagen de símbolos o caracteres que pertenecen a un determinado alfabeto, para luego almacenarlos en forma de datos.
- Inspección robotizada: La inspección rápida de las piezas para garantizar la calidad de los componentes de fabricación utilizando una visión estéreo con iluminación especializada.
- Venta al por menor: Como ser los clásicos lectores de barras que encontramos en los supermercados para reconocer los precios de los productos en la línea de cajas.
- Construcción de modelos 3D: La construcción automatizada de modelos 3D a partir de fotografías.
- Imágenes médicas: Como ser la tecnología utilizada para tomar radiografías y las técnicas para detectar tumores malignos y anomalías en las mismas.
- Seguridad automotriz: Ayudando a detectar obstáculos mediante un sistema de conducción asistida utilizando diferentes cámaras.
- Captura de movimiento: Utilizando marcadores retro-reflexivos vistos desde múltiples cámaras u otras técnicas para la captura de movimientos de los actores para utilizar en animación por computadora.
- Vigilancia: Monitoreo de intrusos, análisis del tráfico vial, y monitoreo de piscinas para víctimas de ahogamiento.

- Reconocimiento de huellas dactilares y biometría: Para la identificación automática de accesos y también utilizada para aplicaciones forenses.
- Detección de caras: Utilizado para mejorar el foco de las cámaras y para hacer una búsqueda más relevante de personas en imágenes.

9.3 Librería OpenCV

"OpenCV fue oficialmente lanzado en 1999 como parte de un proyecto de investigación de Intel destinado a mejorar las aplicaciones intensivas en CPU. Este proyecto formaba parte de una serie de iniciativas que también incluían el trazado de rayos en tiempo real y las visualizaciones en 3D. El equipo de Intel fue uno de los principales contribuyentes a este proyecto, desarrollando una biblioteca de rendimiento.

En sus primeros días, los objetivos de OpenCV se describían de la siguiente manera:

1. Avanzar en la investigación al proporcionar una visión libre y código optimizado para las bases de infraestructura de visión.
2. Difundir el conocimiento de la visión al ofrecer una infraestructura común que los desarrolladores pudieran utilizar, lo que facilitaba la lectura y transferencia de código.
3. Promover aplicaciones comerciales basadas en visión al ofrecer un código portátil y optimizado de forma gratuita, sin necesidad de que fuese abierto o gratuito.

Es importante destacar que esta biblioteca es multiplataforma y es compatible con Mac OSX, Windows y Linux." (Soler, n.d.).

Las siglas "OpenCV" provienen de "Open Source Computer Vision Library", que en español se traduce como "Biblioteca Abierta de Visión por Computadora". OpenCV es una librería de procesamiento de imágenes diseñada principalmente para aplicaciones de visión por computadora en tiempo real. Algunas de sus principales funcionalidades incluyen:

- Captura en tiempo real: OpenCV permite la adquisición y procesamiento de imágenes o video en tiempo real desde cámaras u otras fuentes.
- Importación de archivos de video: Permite la importación y manipulación de archivos de video almacenados en diversos formatos.
- Tratamiento básico de imágenes: OpenCV proporciona funciones para ajustar el brillo, contraste, umbralización y otras operaciones básicas de procesamiento de imágenes.
- Detección de objetos: La librería incluye algoritmos y técnicas para la detección de objetos, como caras o cuerpos, en imágenes o secuencias de video.

Estas son solo algunas de las funcionalidades destacadas de OpenCV, pero la librería ofrece muchas más herramientas y algoritmos para el procesamiento y análisis de imágenes (Soler, n.d.).

9.4 Trabajos Relacionados

Un estudiante en la universidad tecnológica de Israel desarrollo un sistema de acceso multimodal seguro, mediante dos patrones biométricos en este caso el facial y la voz, para ello es necesario explorar los proyectos precedentes relacionados con este tema,

analizando sus fortalezas y debilidades, tomando en cuenta aquellos métodos y técnicas que puedan ser enfocados hacia un sistema libre, de esa forma plasmarlo en un ambiente de programación basado en Python. En el cual unió dos técnicas diferentes en una para el reconocimiento facial y la otra para reconocer voz (Escobar, 2022).

En la universidad salesiana dos estudiantes previos a obtener su título de ingeniería desarrollaron un sistema de reconocimiento facial usando un dispositivo llamado LattePanda el cual es una tarjeta de alto nivel, esto demuestra que tenemos varias alternativas a la hora de hacer un proyecto con esta temática ya que por mi parte he decidido usar una Rasberry PI (Nacipucha & Frías, 2020).

Un estudiante de la Universidad Distrital Francisco José de Caldas elaboro un control de cerradura eléctrica mediante el reconocimiento facial, donde se utilizó una cámara web que toma la información del entorno, después, esa información va a ser tratada por el programa Matlab en un ordenador. El software verificó si hay un rostro humano en las imágenes logradas por la cámara web; en la situación de hallar un rostro humano y que este corresponda a alguno de los usuarios de la base de datos, el ordenador tomó la elección de activar una cerradura electrónica mediante la comunicación con un microcontrolador. Igualmente, todo el proceso se pudo visualizar a partir de una interfaz gráfica que posibilitó visualizar todos los eventos del sistema descrito (Latorre, 2016).

10. Diseño Metodológico

10.1 Métodos de investigación

10.1.1 Método Hermenéutico

El método hermenéutico está basado en la interpretación de datos producto de la observación de eventos, aplicados en varias áreas de la filosofía, el lenguaje e interpretación gramatical, lo que recuerda al método científico que parte de la observación, experimentación para determinar conclusiones (Muñoz y Muñoz, 2021).

Este método se aplicó empíricamente para determinar el problema que se intenta solucionar, es decir, se planteó una alternativa viable para notificar al usuario, con el uso de nuevas herramientas tangibles como el celular e intangibles como el software que se ejecuta tanto en la Rasberry Pi como en el celular.

10.1.2 Método Fenomenológico

El método fenomenológico es aquel que permite explorar diferentes situaciones de la vida y del mundo, entendiendo que se lo realiza desde un punto de vista subjetivo, es decir, a partir de los sentidos y de lo que se hace con lo que se percibe en nuestra conciencia (Ayala, 2021).

El proyecto se fundamentó en el uso de la tarjeta Raspberry Pi, la cual fue seleccionada debido a sus destacadas características. Esta elección se basó en su historial probado en diversos proyectos de investigación enfocados en la seguridad de acceso inteligente, aprovechando su capacidad para controlar actuadores y su potencia de procesamiento. Además, la Raspberry Pi se destacó por ser una opción económicamente viable gracias a su bajo costo y su amplia disponibilidad.

10.1.3 Método Práctico Proyectual

De acuerdo con la siguiente definición del método “según el experto Oil Aicher servirá para definir los límites en los que deberá moverse el diseñador” (Cordero-clavijo y Quevedo-jumbo, 2020), a través de este método se identifican las actividades a desarrollarse considerando prioridades.

El método práctico proyectual consistió en la implementación de un sistema de seguridad para viviendas que, mediante nuestro rostro, abría una puerta, el cual se implementó en una casa para realizar y analizar las pruebas de campo respectivas donde se verificó el funcionamiento del sistema de seguridad implementado, confirmando que cumplió los objetivos planteados y el proceso adecuado del mismo.

10.2 Técnicas de investigación

10.2.1 Técnica de Observación

La técnica observación directa en el campo de investigación se la propone, ya que esta está relacionada con el método hermenéutico antes visto esto permitirá obtener las primeras respectivas a la problemática a resolver (Muñoz y Muñoz, 2021), recoger datos relevantes y sobre todo verificar los posibles escenarios para la implementación del sistema.

Esta estrategia se utilizó para recopilar y seleccionar información precisa de varios artículos y páginas web para la construcción del sistema de seguridad, así como para seleccionar de manera precisa los diferentes materiales, componentes electrónicos para tener en cuenta durante el desarrollo del proyecto.

10.2.2 Técnica de investigación documental

La investigación documental de la misma forma que se la define constituye una secuencia de procedimiento y técnicas que los trabajadores en información descubrieron y perfeccionaron durante la historia con el propósito de ofrecer información a la sociedad, esa información se la encuentra en las bibliotecas (Tancara,1993).

Con la llegada de Internet como fuente de información, los investigadores tienen acceso a una amplia variedad de recursos de libre acceso. Además, en el ámbito de compartir software, existe la disponibilidad de bibliotecas de código abierto que pueden ser utilizadas directamente o adaptadas para aplicaciones específicas. Este proyecto se cimentó en base a los siguientes principios: desde una perspectiva física o de hardware, se llevó a cabo un estudio exhaustivo de los fenómenos físicos relacionados con el diseño y la conexión de sensores y actuadores. Se consultaron manuales técnicos para obtener las especificaciones de voltaje y corriente requeridas para su funcionamiento óptimo. En el ámbito del software, se incorporó parte del código de bibliotecas existentes que se ejecutan en el proyecto, y, además, se desarrollaron algoritmos personalizados para lograr el funcionamiento necesario y generar las notificaciones requeridas.

10.2.3 Técnica de prueba y error

La prueba y error es una técnica para obtener conocimiento, reparación o solución de problemas que prueba una probabilidad y luego determina si funciona. En caso de que el resultado no sea el esperado, se intenta otra opción y se continúa intentando hasta que se obtiene un resultado positivo (Enciclopedia Online,2018).

La técnica de prueba y error se utilizó para realizar las diversas conexiones y programación electrónicas. La programación requiere concentración, amplios conocimientos y habilidades excepcionales en la manipulación de componentes electrónicos para crear un sistema adecuado para la prueba. La interacción entre el sistema y un miembro de la familia en sus pruebas de campo comprueba esto.

11. Propuesta practica de acción

En esta sección se desglosará el hardware utilizado, describiendo los componentes y su función en el proyecto, así como las aplicaciones utilizadas para la programación. También se incluirá el software utilizado para generar notificaciones, indicando el proceso para realizar pruebas de funcionamiento y detallando los resultados.

11.1 Hardware

Son los componentes físicos y tangibles de una computadora o sistema informático que se utilizan para procesar, almacenar y manipular datos. A continuación, se enumera el conjunto de componentes utilizados en el proyecto, junto con una breve descripción de cómo se utilizaron en el trabajo que se completó.

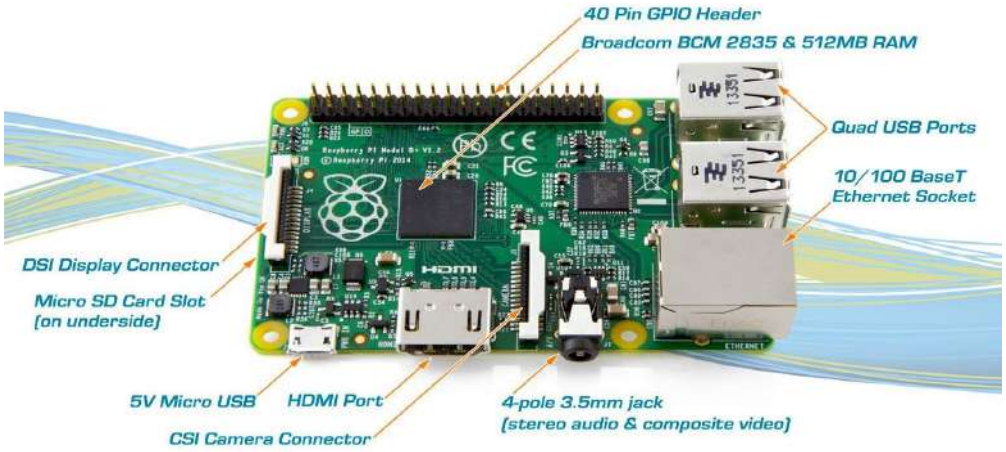
11.2 Raspberry Pi modelo 4B

La Raspberry Pi 4 Modelo B es una solución de bajo costo que puede utilizarse en una variedad de proyectos de electrónica, programación e informática. Es equipado con un procesador ARM Cortex-A72 de 64 bits de cuatro núcleos a 1.5 GHz, que puede aumentar hasta 2.0 GHz, y tiene una variedad de opciones de memoria RAM, incluidas 2 GB, 4 GB y 8 GB (Rus, 2019).

Para el desarrollo del prototipo, la Raspberry Pi se emplea como un controlador del sistema, donde almacena y procesa la información que se obtiene de la cámara. Los datos se visualizan a la pantalla, donde se puede ver en tiempo real lo que la cámara está captando. La arquitectura física de la Raspberry Pi 4 modelo b se muestra en la Figura 2, donde se detallan sus componentes.

Figura 2

Tarjeta Raspberry Pi 4



Nota. Aquí se demuestra la arquitectura de una Raspberry Pi. Tomado de (https://lifebitblog.wordpress.com/2014/11/06/nuevo-modelode-raspberry-pi-la-model-b/)

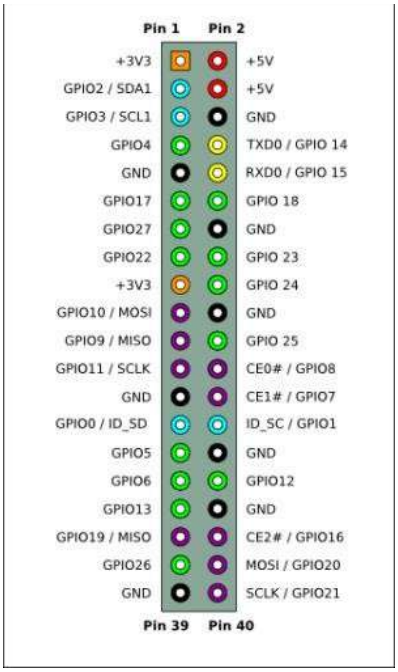
11.3 Puertos Gpio de la tarjeta Raspberry pi

Son un conjunto de conexiones que se pueden usar como entradas o salidas para varias aplicaciones. Estos pines están incluidos en todos los modelos de tarjetas, lo que permite completar una variedad de proyectos. Todos los pines son de tipo “unbuffered”, es decir, no disponen de buffers de protección, así que se deberá tener cuidado con las magnitudes (voltajes, intensidad…) cuando se conecten componentes a ellos para no dañar la placa.

Pines de alimentación: hay pines que proporcionan alimentación an estas caídas de tensión a 5V, 3.3V (limitados a 50mA) y tierra (GND o Ground). Pueden funcionar como fuente de alimentación, pero también se pueden usar otras fuentes (pilas, fuentes de alimentación externasetc.). DNC (Do Not Connect): estos pines no tienen ninguna función, pero pueden utilizarse para otros propósitos. Los primeros modelos de Raspberry Pi los incluyen. Las placas actuales los marcan como GND.

Figura 3

Puertos Gpio de la tarjeta Raspberry pi.



Nota. Se describen los puertos de la Raspberry Pi. Tomado de https://www.electronicayciencia.com/2016/11/conexion-gpiode-raspberry-pi-3.html

11.4 Módulo de cámara Raspberry Pi

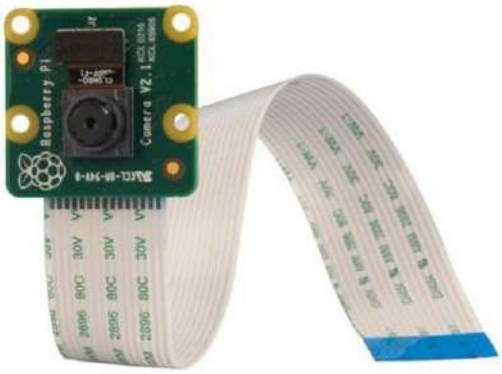
El conector CSI de la Raspberry Pi se conecta directamente a la placa de cámara de la Raspberry Pi. El módulo de enfoque fijo de la placa de cámara Raspberry Pi contiene un sensor Omnivision 5647 de 5MP (2592-1944 píxeles). El módulo se conecta a Raspberry Pi a través de un cable plano de 15 pines a la interfaz serial de cámara MIPI (CSI) de 15 pines, que fue diseñada para funcionar con cámaras (Pastor,2020).

Lo que se logro es que la cámara se pueda configurar para capturar imágenes de aquellos que intentan ingresar al área protegida. Para garantizar que los retratos

sean claros y adecuadas para el reconocimiento facial, puede establecer una ubicación específica y un ángulo apropiados.

Figura 4

Módulo de cámara Raspberry Pi



Nota. Se la utilizo para obtener las imágenes que se usaran para el reconocimiento facial. Tomado de https://ecuarobot.com/2020/02/19/comenzando-con-elmodulo-de-camara-raspberry-pi/ .

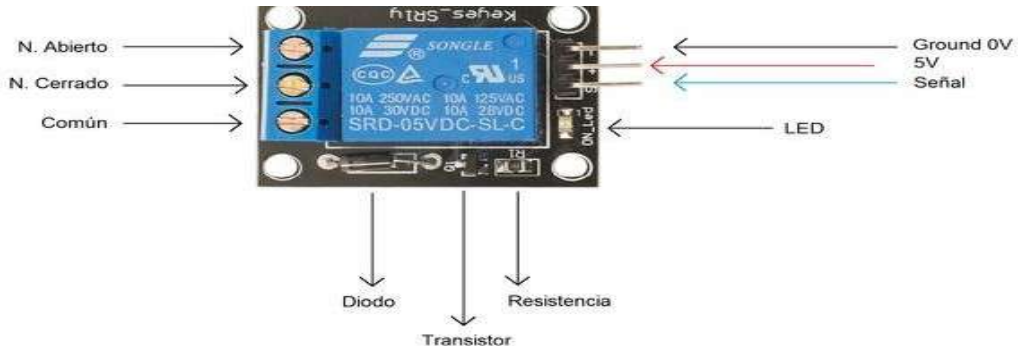
11.5 Modulo Relé

El relé funciona como un interruptor eléctrico cuando está cerrado y cuando está abierto, pero funciona eléctricamente en lugar de manualmente. El relé consiste en una bobina que está conectada a una corriente. Cuando se activa la bobina, se crea un campo electromagnético que cierra el contacto normalmente abierto del relé, lo que permite que la corriente circule por un circuito para realizar tareas como encender una lámpara o arrancar un motor (SEAS, 2019).

El módulo relé se usó para activar la cerradura eléctrica y mantener la puerta cerrada. Cuando alguien es identificado por el sistema de reconocimiento de rostros, el relé se desactiva y la puerta se abre. En Figura 5 se muestra la configuración del módulo.

Figura 5

Modulo Relé



Nota. Tomado de https://compras.patagoniatec.com/productos/modulo-rele-1canal-5v-ky-019/

11.6 Cerradura electrónica DC 12V.

Es básicamente una cerradura electrónica que se usa para cerrar puertas, gabinetes, seguros, etc. Porque el cerrojo está normalmente extendido, aplicarle corriente gracias a sus bobinas estas se activan y abre la puerta del proyecto a desarrollar (HeTPro, 2023).

Se ha incorporado una cerradura tipo solenoide al proyecto con el objetivo de proporcionar un acceso más seguro y sin contacto físico. Esta incorporación puede resultar especialmente beneficiosa en lugares donde se requiere un alto nivel de seguridad o se prioriza la higiene. Además, la integración de estos sistemas con tecnología biométrica puede agilizar el proceso de entrada y permitir un registro más confiable de los eventos de acceso. En la Figura 6 se muestra la composición de la cerradura electromagnética.

Figura 6

Solenoide tipo chapa 12V.

Nota. Tomado de https://www.330ohms.com/products/solenoide-tipo-chapa12v#:~:text=Es%20b%C3%A1sicamente%20una%20cerradura%20electr%C3%B3nica, la%20puerta%20de%20tu%20proyecto.

11.7 Sensor de interruptor de contacto magnético

Un sensor de interruptor de contacto magnético utiliza un campo magnético para detectar si una puerta, ventana u otro tipo de acceso está abierto o cerrado. Estos sensores se componen de dos partes principales: un imán y un interruptor de reed (Llorente, 2017).

El sensor mencionado se utilizó con una Raspberry Pi para enviar notificaciones a Telegram cuando se detecte un cambio en el estado del interruptor en este caso enviara una notificación cuando detecte estado abierto y otra cuando este en estado cerrado.

Figura 7

Sensor de interruptor de contacto magnético

Nota. Este sensor estará instalado en la puerta para que detecte la señal y envié una notificación a telegram. Tomada de https://blogmasterwalkershop.com.br/arduino/como-usar-com-arduino-sensor-magnetico-com-fio-para-alarme-mc-38

11.8 Software

Aquí se optó por utilizar el protocolo de comunicaciones seguras entre dos sistemas basado en una arquitectura de cliente/servidor. Secure Shell (SSH) que permite a los usuarios conectarse de forma remota a un host, y este protocolo realiza una encriptación de la conexión. Esto impide que un observador malicioso pueda monitorizar la comunicación y obtener contraseñas u otros datos, ya que la información está encriptada. Para la instalación se utilizó el programa Rasberry pi imager y se procedió habilitar el protocolo SSH.

11.9 Rasberry pi imager

El uso del Raspberry Pi Imager permite la instalación rápida y sencilla de Raspberry Pi OS y otros sistemas operativos en una tarjeta microSD lista para usar con la Raspberry Pi. En todo caso se simplifica significativamente el proceso de instalación de sistemas operativos en una Raspberry Pi, lo que ahorra tiempo, reduce la complejidad y hace que esta plataforma sea más accesible para una variedad de usuarios, lo que respalda su creciente popularidad en diversas aplicaciones y proyectos.

Aquí se seleccionó la imagen del sistema Operativo elegido y se procedió a instalar en la microSD sin olvidar de activar el protocolo SSH y se asignó un nombre y contraseña al dispositivo.

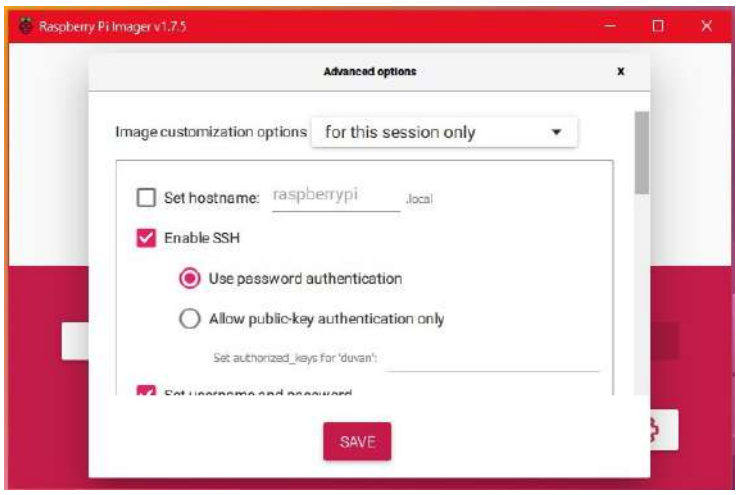
Figura 8

Rasberry pi imager

Nota. Imagen del programa ya instalado Castillo Torres, 2023.

Figura 9

Activación Protocolo SSH



Nota. Imagen de la activación del protocolo SSH Castillo Torres, 2023.

11.10 Sistema Operativo Raspbian

Raspbian, que se lanzó en Julio de 2012, es el sistema operativo que se ha optimizado para esta placa. Debido a que Raspbian está basado en Debian, el sistema de reconocimiento facial creado podría funcionar en cualquier distribución de Linux basada en el sistema operativo Mimo. La imagen del firmware, cuyos drivers son propietarios y accesibles a través de bibliotecas, se conoce como blob binario. Las llamadas a bibliotecas en tiempo de ejecución se comunican con los drivers del kernel de Linux por el software de aplicación (Merino, 2020).

Para el desarrollo del proyecto se procedió a instalar la versión completa ya que se tienen los recursos necesarios para instalarlo una vez en el sistema se configuro la fecha y hora, el idioma y la red inalámbrica para no tener que estar conectando la Rasberry al router a continuación se muestra una Figura 10 donde se aprecia el escritorio de Raspbian.

Figura 10

Sistema Operativo Instalado

Nota. Tomado de https://www.tomshardware.com/news/raspberry-pi-os-nolonger-raspbian

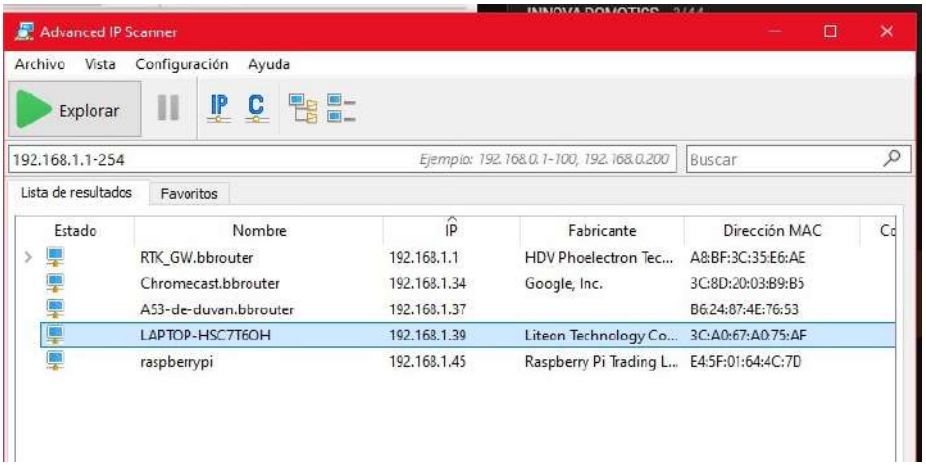
11.11 Advanced IP Scanner

Escáner de red gratuito y fiable para analizar LAN El software puede escanear todos los dispositivos de red, acceder a las carpetas compartidas y a los servidores FTP, controlar remotamente las computadoras (a través de RDP y Radmin) e incluso apagar las computadoras. Es simple de usar y funciona como una edición portátil. Cada administrador de red debería considerarlo como su primera opción.

La herramienta se utilizó para escanear la red donde se levantó el sistema y descubrir qué dispositivos están conectados, incluyendo computadoras, impresoras, routers, cámaras IP y otros dispositivos de red. En este caso se descubrió la Rasberry Pi y así obtener su IP.

Figura 11

Advanced IP Scanner



Nota. Imagen tomada del programa ya ejecutado, aquí me da la IP del Rasberry la cual es 192.168.1.45.

11.12 MobaXterm

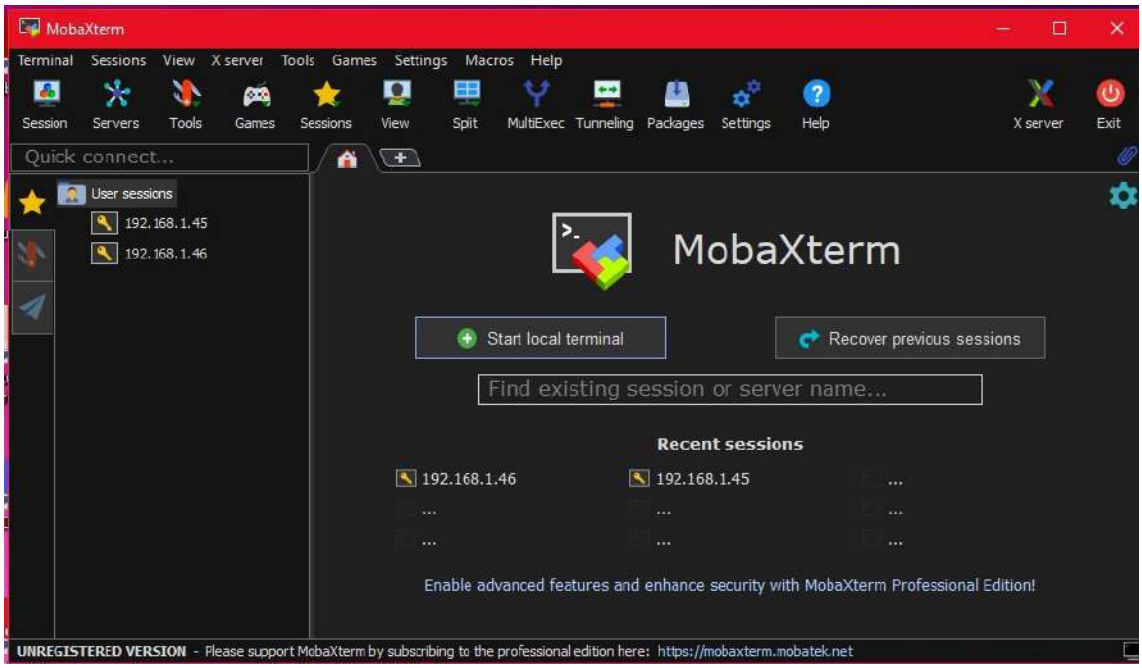
MobaXterm es una terminal para Windows mejorada que incorpora un servidor X11, múltiples herramientas de red para computación remota y todos los paquetes necesarios de Unix en un solo archivo ejecutable. MobaXterm ha sido creado para satisfacer las necesidades de los usuarios de computadoras, administradores de sistemas, desarrolladores de aplicaciones y webmasters, ofreciendo: una terminal multitab con comandos Unix embebidos (ls, cd, cat, sed, grep, awk, rsync, wget, etc.), un servidos X11 integrado para exportar fácilmente su visualización en Unix/Linux, un administrador de sesión con muchas herramientas de red (SSH, RDP, VNC) (*Software Shop*, 2023).

MobaXterm en Raspberry Pi brinda una forma conveniente de interactuar con la Raspberry Pi desde una computadora con Windows, permitiendo trabajar con la línea de comandos y ejecutar aplicaciones gráficas de forma remota. Esto es especialmente útil para administrar la Raspberry Pi desde una máquina con Windows sin tener que conectar una pantalla, teclado y ratón directamente a la Raspberry Pi hay

que tener en cuenta el usuario y contraseña al momento que habilitamos el protocolo SSH. En la figura 12 se muestra el entorno de MobaXterm.

Figura 12

MobaXterm



Nota. Imagen tomada del programa ya ejecutado, aquí se crean las sesiones con las IPs antes analizadas (192.168.1.45) la Ip (192.168.1.46) esto ayuda después a configurar la red inalámbrica.

11.13 Realvnc viewer

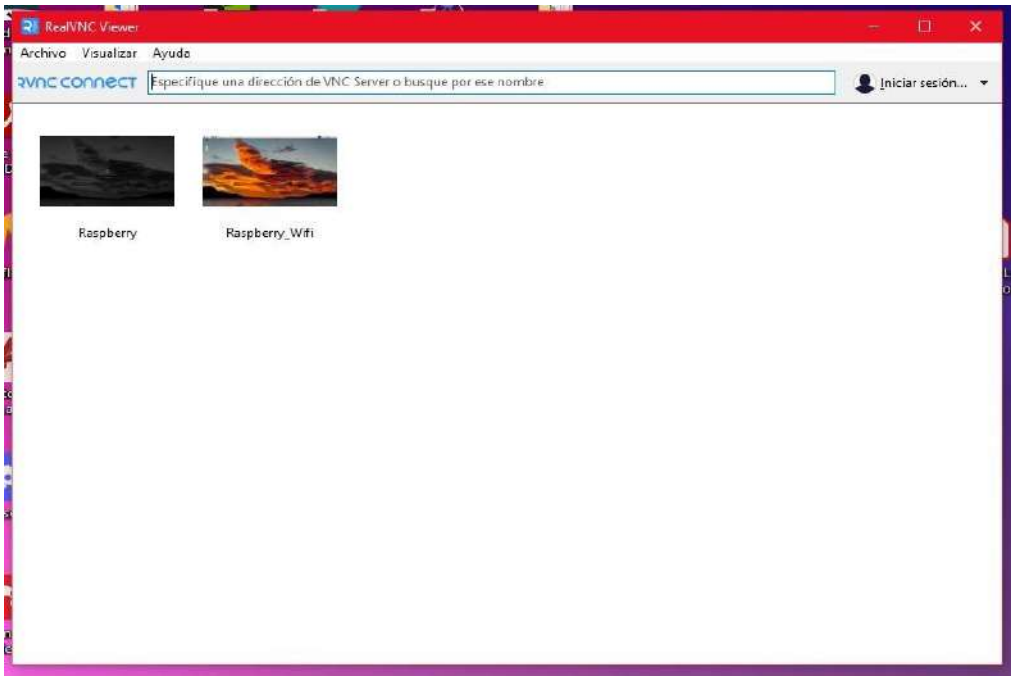
VNC por sus siglas en inglés Virtual Network Computing o en español, Computación Virtual en Red, es un software de código libre de tipo cliente servidor que permite ver la pantalla del ordenador servidor y controlarlo en uno o varios ordenadores clientes sin importar que sistema operativo pueda ejecutar el cliente o el servidor, podemos ver la pantalla y controlar el equipo del que ejecuta el servidor desde el cliente (*Navegación*, 2020).

En este programa podemos ejecutar aplicaciones, realizar tareas y configurar la Raspberry Pi como si estuvieras trabajando directamente en ella en este caso creamos

una sesión llamada Raspberry_wifi en donde se trabaja de forma inalámbrica en el entorno de Raspbian.

Figura 13

Realvnc viewer



Nota. Imagen tomada del programa ya ejecutado, aquí se crean las sesiones y se asigna un nombre.

11.14 Herramientas de software

La biblioteca OpenCV fue elegida para esta investigación porque tiene algoritmos de reconocimiento facial implementados, lo que brinda mayor flexibilidad al buscar una solución al problema de reconocimiento. Esto, junto con su extensa documentación y el hecho de ser multiplataforma, contribuyó a su elección. Igualmente, OpenCV se utiliza en una gran cantidad de desarrollos en todo el mundo, incluidos los que se ejecutan en una Raspberry Pi, lo que ofrece ventajas de investigación una vez que se elige la herramienta de hardware.

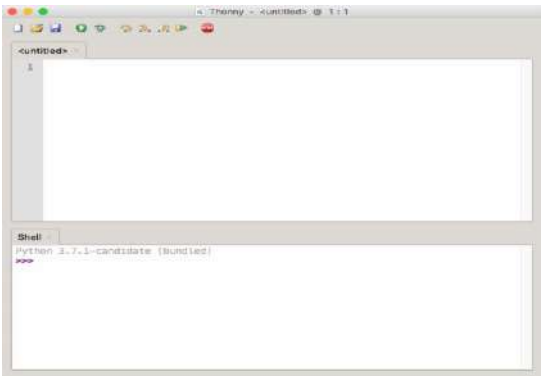
11.15 Python

Python es un lenguaje de programación de alto nivel, orientado a objetos con semántica dinámica que se utiliza principalmente para el desarrollo web y de aplicaciones informáticas en términos técnicos. Debido a que ofrece opciones de tipificación y encuadernación dinámicas, es muy atractivo en el campo del desarrollo de aplicaciones rápidas (Londoño, 2023).

En la tarjeta Raspberry Pi se ha instalado previamente un editor de códigos llamado Tonny Python, que es una IDE de programación más simple para principiantes que facilita la creación de nuevos proyectos. Sus características incluyen múltiples formas de recorrer el código, evaluación paso a paso de la expresión y un modo para explicar conceptos de referencias, como se muestra en la Figura 14.

Figura 14

Thonny Python



Nota. Tomado de https://realpython.com/python-thonny/

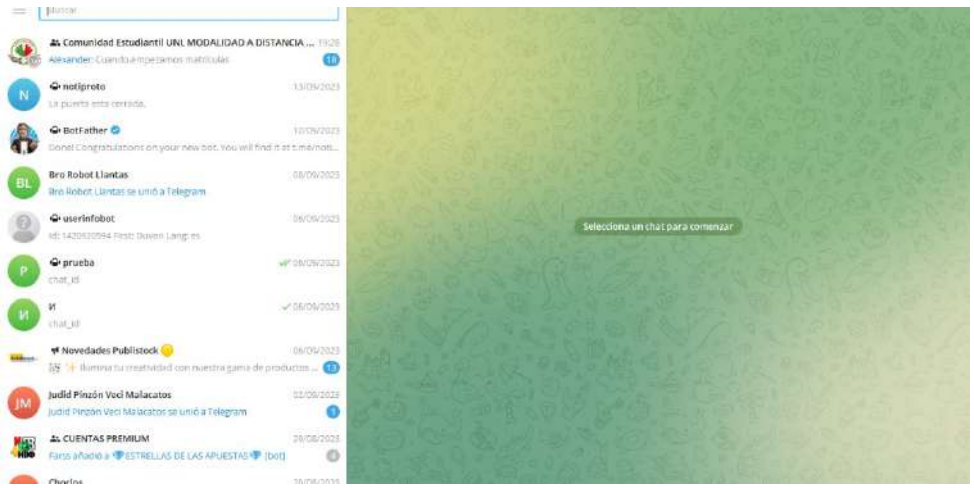
11.16 Telegram

Telegram es una aplicación de mensajería instantánea y plataforma de comunicación en línea. Fue desarrollada por los hermanos Pavel y Nikolai Durov y lanzada en 2013. Telegram se ha destacado por ofrecer una serie de características y ventajas que la distinguen de otras aplicaciones de mensajería (*Curso de Telegram*, 2013).

Telegram destaca por su capacidad de permitir la creación de bots personalizados y proporcionar una API abierta que promueve la innovación y la automatización. Esto se convirtió en una elección fundamental al desarrollar nuestro proyecto. En este proyecto específico, aprovechamos estas características de Telegram para lograr un objetivo concreto: cuando el sensor de interruptor de contacto magnético se activa, envía una señal a una Raspberry Pi, la cual, a su vez, envía una notificación a través de Telegram. Esta integración nos permite mantenernos informados y tomar medidas oportunas en función de las detecciones del sensor, lo que resulta en un sistema eficaz y de respuesta rápida.

Figura 15

Entorno de Telegram



Nota. Imagen de Telegram en escritorio (Autoría propia).

12. Desarrollo de la propuesta de acción

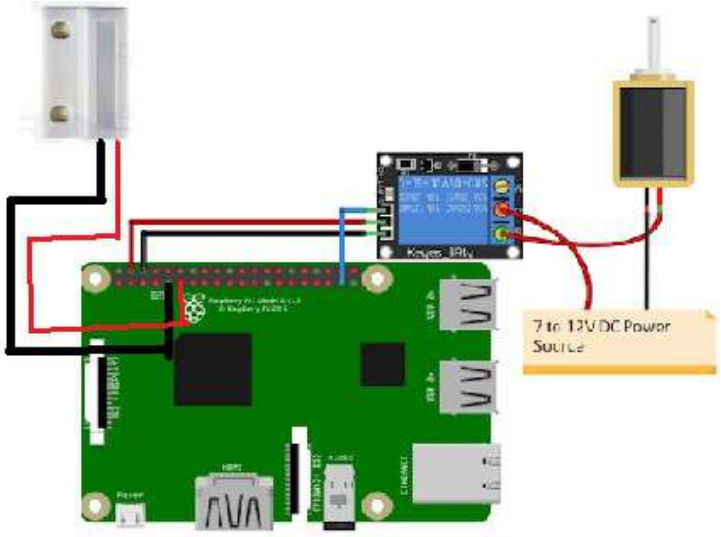
12.1 Diseño y construcción del prototipo

12.1.1 Conexión de la cámara y relé a la tarjeta Raspberry Pi

Para que la cerradura electrónica funcione correctamente, es esencial seguir las especificaciones proporcionadas. La cerradura opera a 12VDC, lo que requiere una fuente de alimentación externa conectada al terminal común del relé. Además, la cámara debe conectarse al puerto CSI de la tarjeta. A continuación, se establece la conexión del relé: la señal del relé se conecta al puerto GPIO 26 de la Raspberry Pi, mientras que el positivo se conecta a un puerto de 5 voltios y el negativo se enlaza a un puerto GND de la tarjeta. Por último, se conecta el sensor magnético al puerto 18 de la tarjeta y se asegura que el GND esté conectado adecuadamente. Estas configuraciones permitirán que la cerradura electrónica funcione de manera óptima en la Raspberry Pi, cumpliendo con las especificaciones requeridas, a continuación, en la figura 16 se detallan las conexiones.

Figura 16

Diagrama electrónico



Nota. Aquí se muestran las conexiones con los sensores y actuadores usados en el proyecto.

12.1.2 Conexión y funcionamiento de la cámara

Al momento de comprender el funcionamiento de la cámara, se desarrolló un pequeño programa con la finalidad de tener un punto de partida para el proyecto y aplicarlo a sus necesidades. El propósito de esta iniciativa es el procesamiento de la imagen capturada por el módulo con el fin de llevar a cabo la identificación facial utilizando una base de datos preexistente.

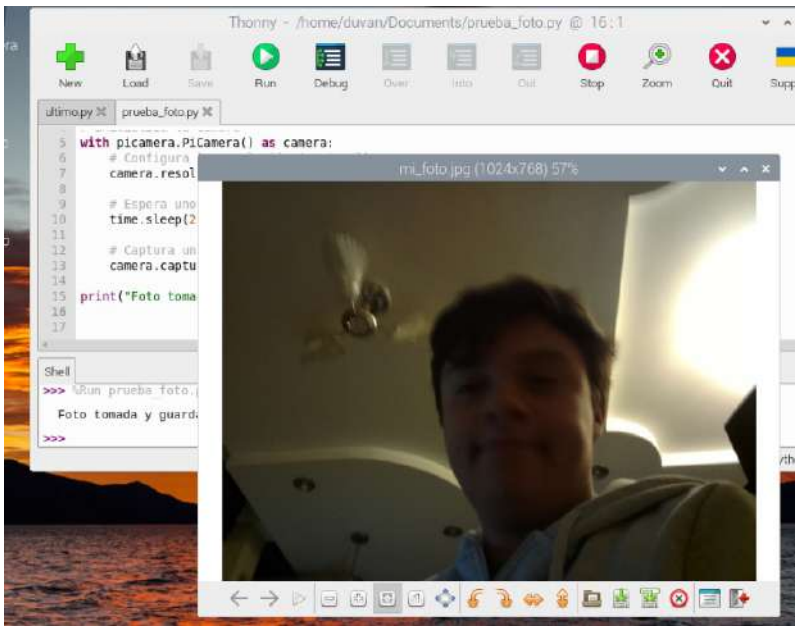
Figura 17

Conexión Raspberry con módulo de cámara

Nota. Fotografía de conexión de la tarjeta al módulo de cámara.

Figura 18

Cámara funcionando



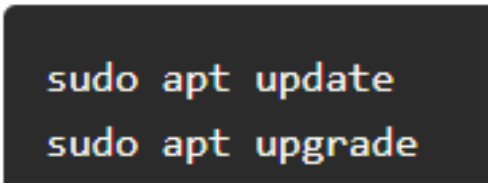
Nota. Interactuamos con la cámara.

12.1.3 Configuración de la tarjeta Raspberry Pi 4.

En la configuración de la tarjeta Raspberry Pi 4 para un proyecto de reconocimiento facial, se comienza instalando el sistema operativo Raspbian desde el sitio web oficial de Raspberry Pi, utilizando Rasberry Pi imager para escribir la imagen en una tarjeta SD de 32 GB. Al encender la Raspberry Pi, lleva a cabo la configuración inicial, que abarca la selección del idioma, la configuración de la red y la contraseña de inicio de sesión. Siempre es necesario mantener el sistema operativo actualizado ejecutando comandos en la terminal para obtener las últimas actualizaciones como se muestra en la figura 19.

Figura 19

Comandos para la configuración inicial.



Nota. Comandos iniciales

12.1.4 Instalación a través de consola de las diferentes bibliotecas

Para el desarrollo del proyecto de reconocimiento facial, se requirió la instalación de varias bibliotecas y herramientas a través de consola. Estas librerías se fueron instalando mediante el proyecto lo solicitaba por ejemplo OpenCV es una biblioteca fundamental de visión por computadora para el reconocimiento facial, también esta OpenCV Contrib que sirve para utilizar módulos adicionales de OpenCV, como el de reconocimiento facial, es necesario instalar las contribuciones de OpenCV ,también se usó NumPy que es una biblioteca esencial para el procesamiento de matrices y datos, también se utilizó Dlib que es una biblioteca que incluye herramientas útiles para el reconocimiento facial.

Figura 20

Comandos utilizados

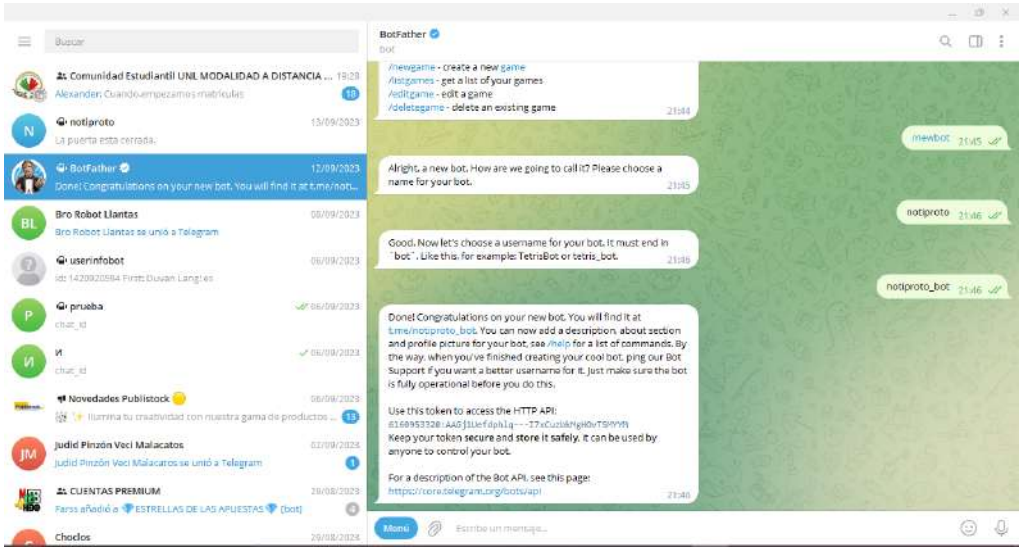
Nota. Instalación de las diferentes librerías

12.1.5 Configuración del Boot en Telegram

Para crear el Bot en Telegram primero necesitamos de la aplicación y buscar "BotFather" en la barra de búsqueda, al iniciar una conversación con el BotFather se usa el comando /newbot para crear un nuevo bot y se siguen las instrucciones para darle un ID y asignarle un nuevo nombre de usuario al bot. Por último, BotFather nos proporciona un token de acceso único para el bot. Los que luego usaremos en el código para recibir las notificaciones.

Figura 21

Configuración del Boot en Telegram



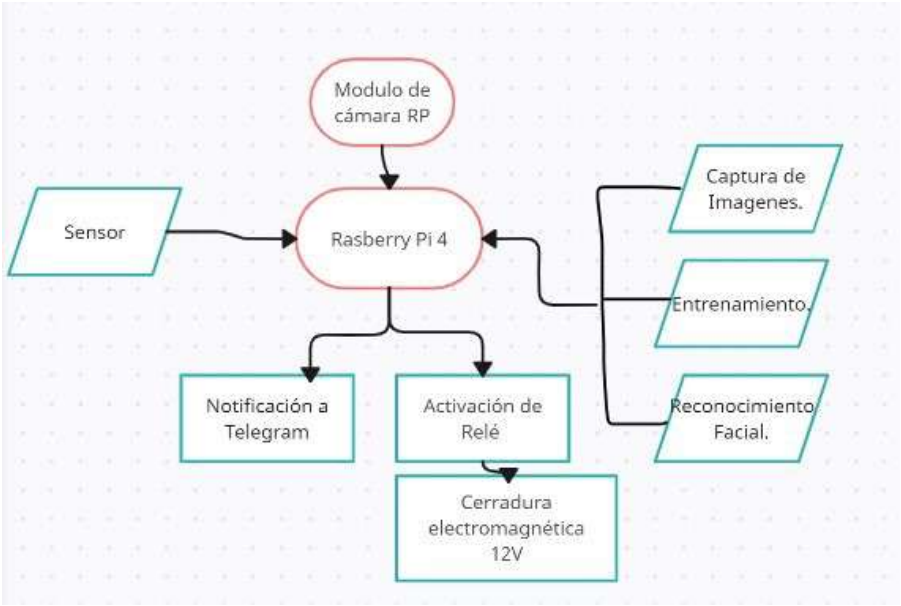
Nota. Aquí se muestra cómo se creó el Boot en donde obtenemos el token para las notificaciones.

12.2 Funcionamiento general del Prototipo

Este apartado es esencial para la replicabilidad y validación del prototipo, ya que proporciona una guía completa de los procedimientos, asegurando que otros puedan reproducir y verificar los resultados, lo que aumenta la credibilidad y confiabilidad del proyecto. En la Figura 22 se puede apreciar la arquitectura general.

Figura 22

Arquitectura general del proyecto.



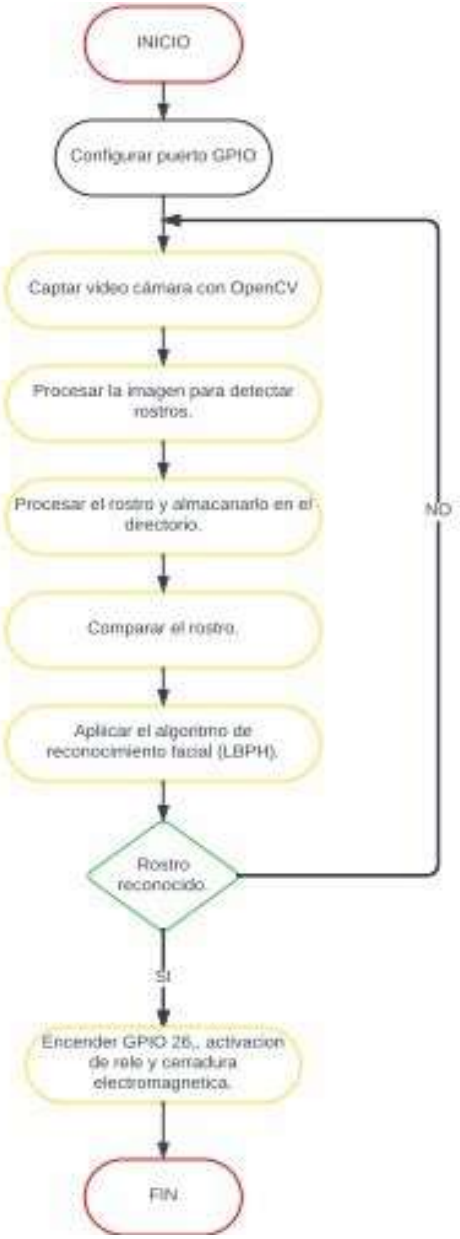
Nota. Aquí se muestra de forma general el funcionamiento del sistema.

12.2.1 Diagrama de flujo

El control comienza configurando los puertos GPIO de la Raspberry Pi para acceder a la cámara. Cuando el programa comienza, la librería Opencv lee las imágenes de la cámara y las procesa para detectar, recortar, cambiar el tamaño, ecualizar, etc. Primero, una imagen debe detectar un rostro. Un rostro válido es cuando la imagen identifica correctamente una cara de una persona y se almacena en un directorio creado para comparar los rostros transformados en histogramas con el algoritmo de reconocimiento facial LBPH. Si el relé detecta un rostro, el relé se activa enviando un pulso a la cerradura electromagnética para abrir. Si no detecta un rostro, el relé no se activa. En la figura 23 se muestra el funcionamiento general del prototipo.

Figura 23

Diagrama de flujo



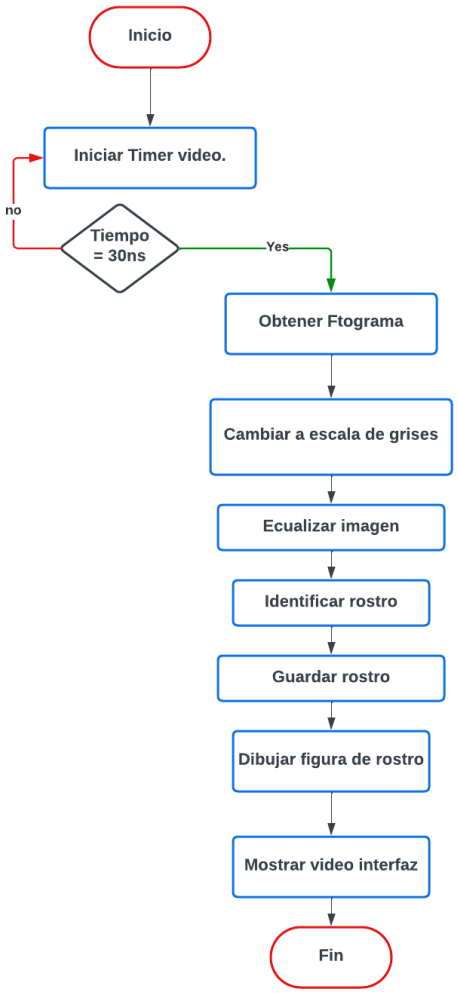
Nota. Se aprecia el funcionamiento del prototipo.

12.2.2 Captura de imágenes

Cuando se enciende el control de acceso, comienza a grabar el video. Cada 30 FPS (fotogramas por segundo) genera un fotograma, que debe ser cambiado a escala de grises porque los clasificadores que reconocen los rasgos funcionan exclusivamente a escala de grises. El diagrama de flujo de la captura de video se muestra en la figura 24, y se puede encontrar el código en el Anexo 6.

Figura 24

Diagrama de flujo captura de video

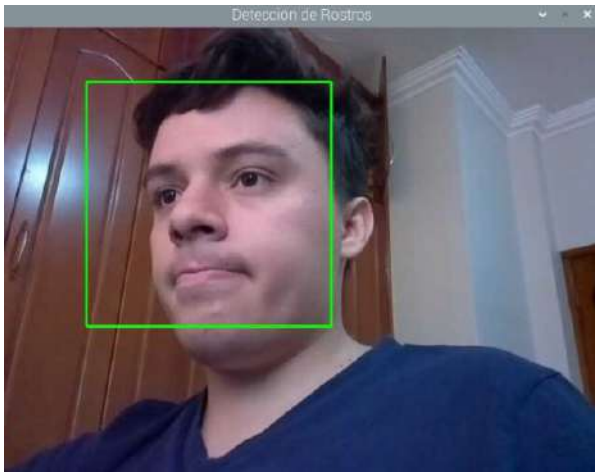


Nota. Se describe el funcionamiento del código para capturar el video.

La fase de identificación en los sistemas de reconocimiento facial reviste una importancia crucial, ya que un deficiente proceso de detección de rostros puede repercutir negativamente en las etapas posteriores. Para la detección de rostros, se empleó el clasificador "haarcascade frontalface default.xml", el cual facilita la localización de caras en posición frontal en una imagen, tal como se ilustra en la figura 25.

Figura 25

Detección de un rostro



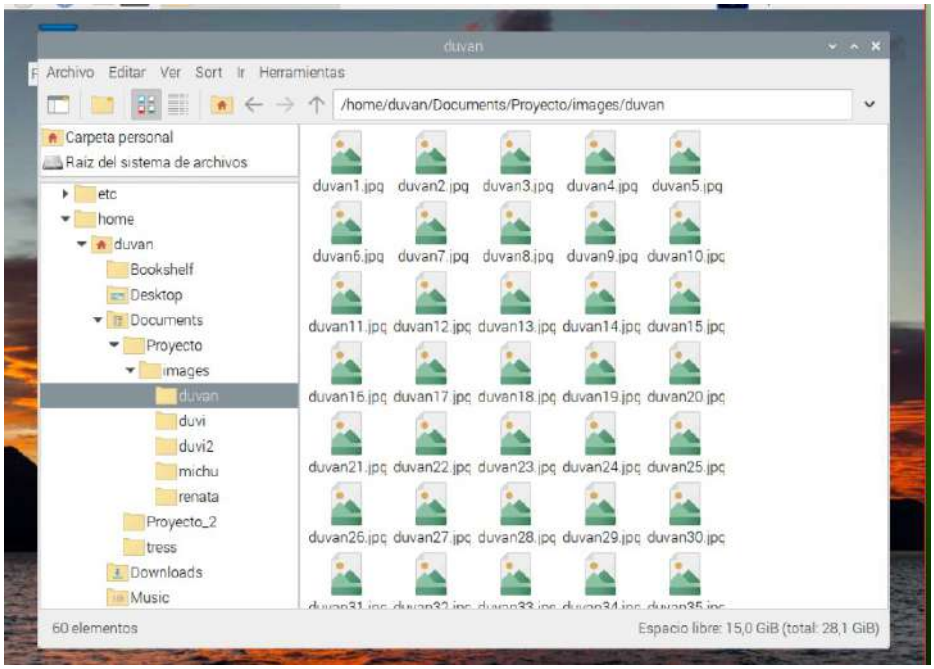
Nota. Se ve como el sistema detecta el rostro.

El algoritmo no se limita únicamente a identificar y verificar a las personas mediante la detección de rostros, sino que debe considerar otros factores que podrían complicar dicha detección. Estos factores incluyen el estado de ánimo de la persona, el tamaño del rostro, problemas de iluminación y la presencia de elementos como lentes, barba, gorros, y más.

La obtención del rostro se realiza mediante la identificación de la cara. Dado que solo se requiere el rostro en etapas posteriores, se almacenan todas las imágenes recortadas en una única carpeta y se convierten a escala de grises, como se muestra en la figura 26. Esto simplifica el proceso de reconocimiento posterior.

Figura 26

Base de datos



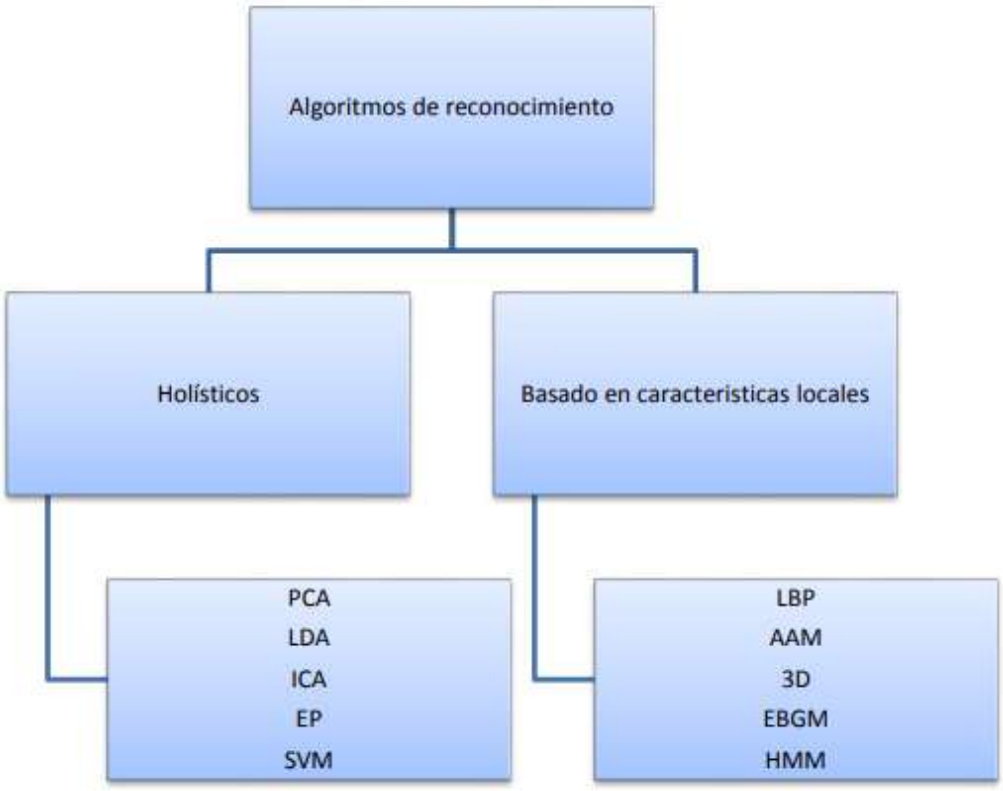
Nota. Se observa cómo se creó la base de datos.

12.2.3 Entrenamiento

En el proceso de entrenamiento, el objetivo principal es la extracción, que se emplea con el propósito de adquirir los atributos distintivos que resultan relevantes para realizar la comparación. Se han desarrollado diversos algoritmos y métodos que permiten la identificación de individuos, tal como se muestra en la figura 27.

Figura 27

Clasificación



Nota. Clasificación de métodos de reconocimiento facial.

12.2.3.1 Algoritmo LBP.

Este enfoque se fundamenta en la extracción de características faciales, como la nariz, los ojos y la boca, con el fin de clasificar sus propiedades geométricas. Mediante la identificación de diversos puntos clave, se generan vectores que incluyen información sobre las distancias entre estos puntos. Cuantos más puntos característicos se puedan identificar, mayor cantidad de distancias se podrán calcular, lo que conduce a un mejor rendimiento en el proceso de reconocimiento.

Esta función entrena todos los rostros almacenados de cada usuario. Después de guardar cada rostro válido en las carpetas de cada usuario, se selecciona la técnica de entrenamiento LBPH. Cuando se aplica el algoritmo de entrenamiento, todo queda almacenado en la memoria de la Raspberry Pi y listo para su uso. El diagrama de flujo

del entrenamiento se muestra en la figura 28, y el código que se utilizó para entrenar se encuentra en el Anexo 6.

Figura 28

Diagrama de flujo del entrenamiento.

Nota. Se muestra cómo es que funciona el código para entrenar el programa

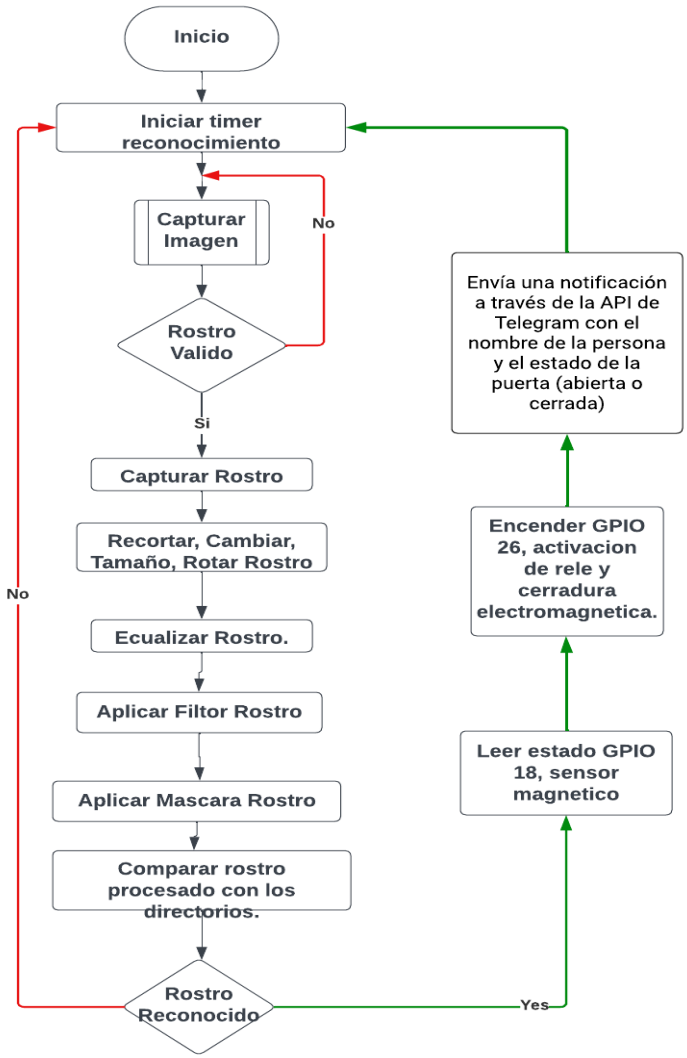
12.2.4 Reconocimiento

La biblioteca OpenCV incluye una clase diseñada para la utilización del algoritmo de detección de rostros LBPH (Patrones Locales Binarios). El proceso de reconocimiento facial comienza con un período de espera durante el cual se capturan imágenes y se verifica la presencia de un rostro válido. En casos en los que no se detecta un rostro, se procede a capturar más imágenes. En contraste, si se identifica un rostro, se avanza al siguiente paso que involucra el procedimiento de procesamiento de imágenes detallado en el primer diagrama de flujo.

Posteriormente, el algoritmo compara el rostro procesado. Si el rostro capturado no está registrado en la base de datos previamente creada, la puerta permanece cerrada. En cambio, si el sistema reconoce el rostro capturado, la puerta de la vivienda se desbloquea de manera automática. En la Figura 29 se presenta el diagrama de flujo correspondiente al proceso de reconocimiento. Además, en la sección de Anexo 6 se proporciona el código empleado para el funcionamiento del sistema de reconocimiento facial.

Figura 29

Diagrama Reconocimiento Facial y envió de notificaciones a Telegram.



Nota. Aquí se muestra el funcionamiento del reconocimiento facial.

12.3 Proceso de instalación física del Prototipo

Para la instalación del prototipo, se tomó la decisión de alojar la Raspberry Pi en una caja protectora debido a su sensibilidad. Además, se ubicó la cámara de la Raspberry en una posición óptima para capturar adecuadamente la cerradura electrónica. Esta última se colocó invertida para que pueda desempeñar su función correctamente en la puerta.

Figura 30

Prototipo Instalado

Nota. Se muestra la Raspberry en su caja para proteger de cualquier golpe.

Figura 31

Cerradura Instalada

Nota. Se puede apreciar la cerradura electrónica.

12.4 Prueba de funcionamiento y resultados

12.4.1 Pruebas

Para llevar a cabo las pruebas pertinentes del equipo, se inscribieron tres usuarios en el sistema de control de acceso, a saber, la madre, el padre y la hija, quienes serán los encargados de acceder a la vivienda. Se debe tener en cuenta que se utiliza la representación lógica de "SI" como uno lógico y "NO" como cero lógico. Además, se registraron las notificaciones enviadas a través de Telegram. La Tabla 1 muestra los intentos realizados y los aciertos obtenidos por cada usuario.

Tabla 1

Pruebas de intentos Realizados.

Usuarios	**Intentos**				**Notificaciones**
	1	2	3	4	
1	SI	SI	SI	SI	SI
2	SI	SI	SI	SI	SI
3	SI	SI	SI	SI	SI
Usuarios que no se encuentran en la base de datos					
4	NO	NO	NO	NO	NO
5	NO	NO	NO	NO	NO

Nota. Podemos ver que las notificaciones dependen en si del estado del reconocimiento facial.

Los resultados de los intentos de acceso a la vivienda arrojaron un satisfactorio porcentaje de éxito del 100%. Cada uno de los usuarios contaba con 60 imágenes almacenadas en la memoria de las Raspberry Pi. Además, se llevaron a cabo pruebas de ingreso con individuos que no estaban previamente registrados en la tarjeta.

En lo que respecta a las pruebas realizadas con personas desconocidas, el sistema de reconocimiento facial demostró su eficacia al no reconocer a estos

individuos, lo que resultó en la denegación de acceso. Por otro lado, con respecto a los usuarios 1, 2 y 3, el sistema los identificó sin ningún inconveniente y procedió a enviar notificaciones a Telegram, permitiéndoles el acceso al hogar de manera oportuna.

12.4.2 Resultados

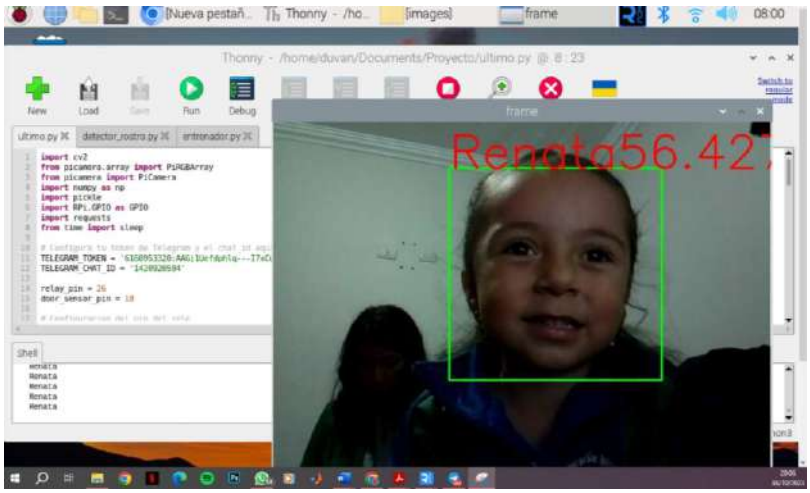
La tarjeta Raspberry funciona correctamente de acuerdo con los requisitos establecidos. En primer lugar, el sistema captura imágenes de los rostros presentes en su entorno. Posteriormente, el sistema aprende a reconocer los rostros capturados y procede a otorgar acceso si se cumple con ciertos criterios de reconocimiento facial.

Para lograr esto, el sistema procesa cada imagen capturada, detecta automáticamente las caras en cada una de ellas y se esfuerza por identificarlas utilizando un modelo de reconocimiento previamente entrenado. Cuando una cara es reconocida con un nivel de confianza igual o inferior a 70, el sistema activa la cerradura electrónica. Además, se resalta la cara reconocida mediante un cuadro en la imagen y se envía una notificación a través de Telegram. Esta notificación incluye el nombre de la persona reconocida y el estado actual de la puerta, indicando si está abierta o cerrada.

En la figura 32, se observa un exitoso proceso de reconocimiento facial llevado a cabo, revelando la identificación de Renata. Asimismo, en la figura 33, se puede verificar la emisión de notificaciones en Telegram que incluyen el nombre de Renata y el estado actual de la puerta.

Figura 32

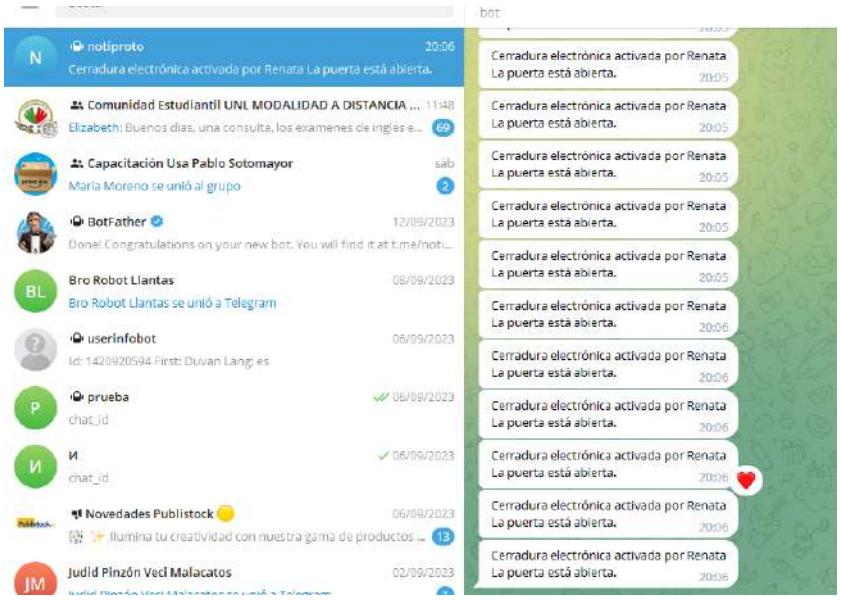
Usuario 1



Nota. Entorno del reconocimiento facial, primer usuario.

Figura 33

Notificación a Telegram

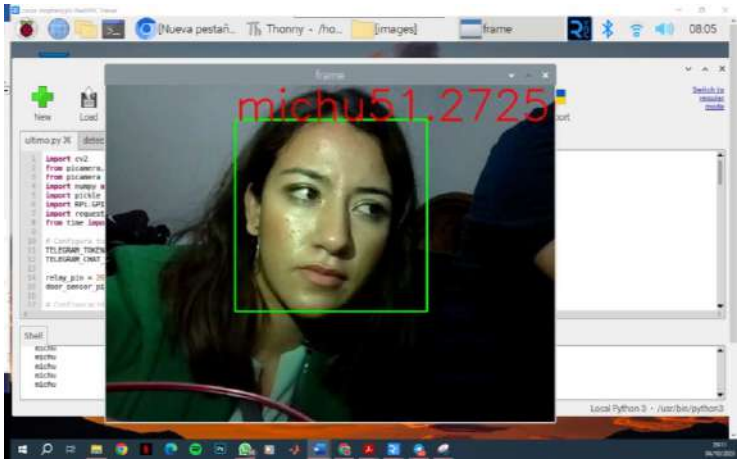


Nota. Entorno de notificaciones a Telegram, primer usuario.

En la figura 34, se aprecia un exitoso proceso de reconocimiento facial en el cual se revela la identificación del segundo usuario, conocido como "michu". Además, en la figura 35, se evidencia la emisión de notificaciones en Telegram que contienen el nombre de "michu" junto con el estado actual de la puerta.

Figura 34

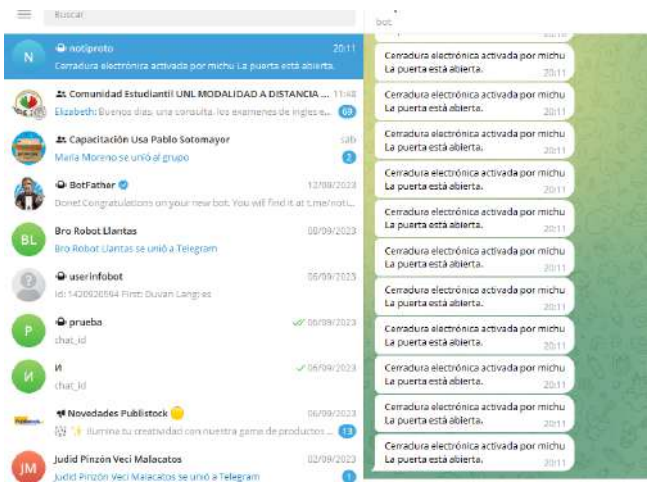
Usuario 2



Nota. Entorno del reconocimiento facial, segundo usuario.

Figura 35

Notificación a Telegram segundo usuario.



Nota. Entorno de notificaciones a Telegram, segundo usuario.

En la figura 36, se aprecia un exitoso proceso de reconocimiento facial en el cual se revela la identificación del tercer usuario, conocido como "duvan". Además, en la figura 37, se evidencia la emisión de notificaciones en Telegram que contienen el nombre de "duvan" junto con el estado actual de la puerta.

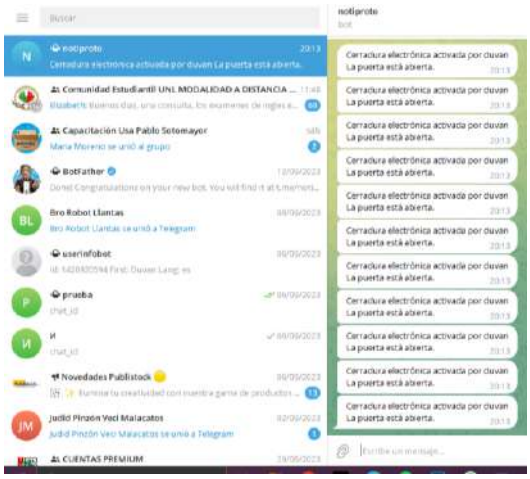
Figura 36

Usuario 3

Nota. Entorno del reconocimiento facial, tercer usuario.

Figura 37

Notificación a Telegram tercer usuario.

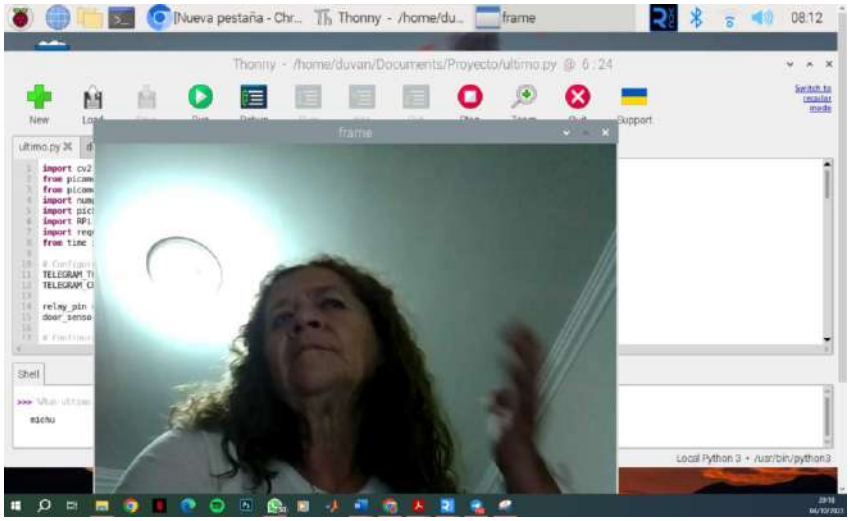


Nota. Entorno de notificaciones a Telegram, tercer usuario.

En la figura 38, se observa a un usuario no registrado, lo que resulta en que el sistema de reconocimiento facial no genere interacciones y, como consecuencia, no se envían notificaciones a Telegram.

Figura 38

Usuario no registrado



Nota. El sistema no reconoce a este usuario por lo tanto no hay interacción.

13. Conclusiones

- La investigación teórica que se llevó a cabo para comprender la interacción entre la Raspberry Pi y la inteligencia artificial, con un enfoque específico en el reconocimiento facial, proporciona los fundamentos necesarios para el desarrollo de soluciones prácticas y eficientes. Esta comprensión sólida allana el camino para la creación de aplicaciones que aprovechan al máximo el potencial de la Raspberry Pi en escenarios del mundo real. Esta sinergia entre la Raspberry Pi y la inteligencia artificial promete contribuir significativamente al avance de la tecnología y su aplicación en una amplia variedad de campos.
- El algoritmo LBPH (Local Binary Patterns Histograms) es una herramienta de procesamiento de imágenes ampliamente utilizada en aplicaciones de visión por computadora y puede formar parte de sistemas más amplios de inteligencia artificial. Su robustez en el reconocimiento facial frente a cambios en la iluminación, junto con su capacidad para identificar características clave como los ojos, la nariz y la boca, y la capacidad de ecualización de los niveles de gris, hacen que sea una opción valiosa. Esto se traduce en un reconocimiento de usuarios más rápido y con menos errores. En resumen, el LBPH es una herramienta versátil y efectiva para abordar desafíos específicos de reconocimiento facial en aplicaciones de visión por computadora.
- La configuración de una API de mensajería de seguridad automática con software libre permite la comunicación eficiente entre el sistema de seguridad y un dispositivo móvil. Esto facilita la recepción de notificaciones en tiempo real, lo que es fundamental para mantener informados a los usuarios sobre eventos de seguridad en su hogar.

- Tras llevar a cabo pruebas exhaustivas de funcionamiento, se logró un impresionante 100% de precisión en la identificación de rostros. Los usuarios 1, 2 y 3 cuentan con 60 imágenes respectivas almacenadas en la tarjeta, y las pruebas de acceso con otras personas no registradas en el sistema arrojaron resultados satisfactorios, ya que se les denegó el acceso. En cuanto a las notificaciones, estas son generadas según un umbral del 70% de similitud, y se envían alertas a través de Telegram. Estos resultados sólidos indican que el dispositivo está listo para su implementación en entornos residenciales, destacando su capacidad para garantizar la seguridad y el acceso controlado de manera efectiva.

14. Recomendaciones

- En la investigación de literatura relevante, se ha identificado la posibilidad de implementar los algoritmos Eigenface o Fisherface en conjunción con el algoritmo LBPH. Se recomienda llevar a cabo una comparación exhaustiva de estos algoritmos para evaluar su eficiencia y determinar cuál de ellos se adecua mejor a los objetivos del proyecto.
- Se recomienda expandir la capacidad de almacenamiento y crear un directorio que pueda acomodar a un mayor número de usuarios, se aconseja la utilización de una tarjeta microSD de 32 gigabytes de clase 10. Es importante recordar que esta tarjeta albergará tanto el sistema operativo como las imágenes de los rostros, garantizando así un espacio suficiente y un rendimiento óptimo.
- En relación con las pruebas de funcionamiento, se debe tener en cuenta el nivel de iluminación del entorno. Cuando el dispositivo se encuentre en condiciones de luz insuficiente, es probable que no sea capaz de detectar ningún rostro. Se subraya la importancia de considerar la necesidad de contar con iluminación adicional cuando se prevé que el prototipo estará en funcionamiento durante la noche. Además, se recomienda implementar notificaciones a través de Telegram para informar a los usuarios sobre el estado de acceso y otras alertas relevantes en tiempo real.

15. Bibliografía

Ayala, M. (2021, agosto 5). *Método fenomenológico: qué es, características, etapas, ejemplos*. https://www.lifeder.com/metodo-fenomenologico/

Cmella, & Cmella. (2022). Ecuador alcanza la tasa más alta de muertes violentas de la última década. *Primicias*. https://www.primicias.ec/noticias/en-exclusiva/ecuador-tasa-muertes-violentas-ultima-decada/

Cordero-clavijo, A. M., y Quevedo-jumbo, J. M. (2020). *Habilidades blandas, un factor de competitividad en el perfil del servidor público*. Polo del Conocimiento. 10.23857/pc.v5i51399

Enciclopedia Online. (2018). Prueba y error | Qué es, Definición y Concepto.https://enciclopediaonline.com/es/ensayo-y-error/

Escobar, E. (2022). SISTEMA DE CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL Y COMANDO DE VOZ EN PYTHON (Ing.). UNIVERSIDAD TECNOLÓGICA ISRAEL.

https://repository.udistrital.edu.co/handle/11349/4687

LA HORA. (2022, 10 junio). *Se incrementa la demanda de instalaciones de sistemas de seguridad*. La hora. Recuperado 16 de mayo de 2023, de https://www.lahora.com.ec/tungurahua/ambato-incrementa-demanda-instalaciones-sistemas-seguridad/

La Hora. (2023, 18 abril). *Robos generan temor en transeúntes y propietarios de viviendas*. Recuperado 16 de mayo de 2023, de https://www.lahora.com.ec/loja/robos-temor-viviendas/

Lezama. (2001). *Estructura y funcionalidad de un sistema de seguridad - PDF Descargar libre*. Suncare. https://docplayer.es/490911-Capitulo-1-estructura-y-funcionalidad-de-un-sistema-de-seguridad.html

Libro: Forsyth, D., & Ponce, J. (2012). Computer Vision: A Modern Approach (2nd ed.). Pearson.

Libro: Jurafsky, D., & Martin, J. H. (2019). Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition (3rd ed.). Pearson.

Libro: Mitchell, T. M. (1997). Machine Learning. McGraw-Hill.

Libro: Russell, S. J., & Norvig, P. (2016). Artificial Intelligence: A Modern Approach (3rd ed.). Pearson.

Marketing. (2022, January 31). *Visión por Computador ✔ Qué es, Aplicaciones y Objetivos*. EDS Robotics; EDS Robotics. https://www.edsrobotics.com/blog/vision-computador-que-es/

Marketing. (2022, January 31). *Visión por Computador ✔ Qué es, Aplicaciones y Objetivos*. EDS Robotics; EDS Robotics. https://www.edsrobotics.com/blog/vision-computador-que-es/

Moreno Latorre, J. P. (2016). Prototipopc. va el control de una cerradura electrónica por medio de reconocimiento facial.

Muñoz, M. M., y Muñoz, M. M. (2021). La actualidad del método hermenéutico de Friedrich Schleiermacher. *Escritos*, *29*(62), 56-72. https://doi.org/10.18566/ESCR.V29N62.A04

Nacipucha, C., & Frías, J. (2020). Diseño de un prototipo de control de acceso a través de reconocimiento facial mediante el uso de la tarjeta LattlePanda. UNIVERSIDAD POLITECNICA SALECIANA DEL ECUADOR.

Pablo, J. (2021, January 22). *ESTADO DIGITAL ECUADOR 2021 – ESTADÍSTICAS DIGITALES ACTUALIZADAS - Mentinno - Formacion Gerencial Blog*. Mentinno - Formacion Gerencial Blog. https://blog.formaciongerencial.com/estadodigitalecuador2021/#:~:text=Ecuador%20cuenta%20con%20un%2080,sociales%20principalmente%20desde%20dispositivos%20m%C3%B3viles.

RecFaces. (2021, May 24). *¿Qué es la visión por computadora? Principales funciones*. RecFaces; RecFaces. https://recfaces.com/es/articles/vision-computador-soluciones

Sarango, B. (2023). Implementan más cámaras de videovigilancia en el cantón Loja. *Blog*. https://primerreporte.com/2023/03/29/implementan-mas-camaras-de-videovigilancia-en-el-canton-loja/

Secatel. (2019, June 18). *¿Qué es la Seguridad Electrónica? - Secatel SCC*. Secatel SCC. https://secatel.com/que-es-la-seguridad-electronica/

Soler, A. (n.d.). *Informe de OpenCV y Tratamiento de Imágenes*. https://www.informatica-juridica.com/wp-content/uploads/2014/01/Informe_OpenCV_Tratamiento_Imagenes.pdf

Tancara, C. (1993). La investigación documental. Temas Sociales, 17, 91–106.

Villegas, J. (2009, February 23). *¿Qué es un Sistema de Control de Acceso?* Tecnoseguro.com; TECNOSeguro. https://www.tecnoseguro.com/faqs/control-de-acceso/que-es-un-control-de-acceso

Rus, C. (2019, June 24). *Raspberry Pi 4 es oficial: una completa actualización con procesador Cortex-A72, hasta 4 GB de RAM y...* Xataka.com; Xataka. https://www.xataka.com/ordenadores/raspberry-pi-4-caracteristicas-precio-ficha-tecnica

Pastor, J. (2020, April 30). *La Raspberry Pi High Quality Camera es un sensor de 12,3 MP para la RPi que permite usar objetivos...* Xataka.com; Xataka. https://www.xataka.com/fotografia-y-video/raspberry-pi-high-quality-camera-sensor-12-3-mp-para-rpi-que-permite-usar-objetivos-intercambiables

HeTPro. (2023). *Cerradura eléctrica con solenoide 12V DC*. Hetpro-Store.com. https://hetpro-store.com/cerradura-electrica-con-solenoide-12v-dc/

Llorente, A. (2017, June). *Sensores magnéticos con latch e interruptor*. Diarioelectronicohoy.com. https://www.diarioelectronicohoy.com/sensores-magneticos-con-latch/

Curso De Telegram. (2013). GCFGlobal.org. https://edu.gcfglobal.org/es/curso-de-telegram/que-es-telegram/1/#

Londoño, P. (2023, April 3). *Qué es Python, para qué sirve y cómo se usa (+ recursos para aprender)*. Hubspot.es. https://blog.hubspot.es/website/que-es-python

16. Anexos

16.1 Anexo I: Certificado de aprobación

INSTITUTO TECNOLÓGICO SUDAMERICANO

VICERRECTORADO ACADÉMICO

Loja, 17 de Julio del 2023
Of. N° 842 -VDIN-ISTS-2023

Sr.(ita). CASTILLO TORRES DUVAN ANIVAL
ESTUDIANTE DE LA CARRERA DE TECNOLOGÍA SUPERIOR EN ELECTRONICA

Ciudad

De mi consideración:

Por medio de la presente me dirijo a ustedes para comunicarles que una vez revisado el anteproyecto de investigación de fin de carrera de su autoría titulado **IMPLEMENTACIÓN DE UN SISTEMA DE RECONOCIMIENTO FACIAL CON NOTIFICACIONES MÓVILES PARA CONTROL DE ACCESO RESIDENCIAL UTILIZANDO RASPBERRY PI EN LA CIUDAD DE LOJA DURANTE EL PERIODO ABRIL-SEPTIEMBRE 2023**, el mismo cumple con los lineamientos establecidos por la institución; por lo que se autoriza su realización y puesta en marcha, para lo cual se nombra como director de su proyecto de fin de carrera (el/la) ING. LEYDI MARIBEL MINGO MOROCHO.

Particular que le hago conocer para los fines pertinentes.

Atentamente,

Ing. Germán Patricio Villamarín Coronel Mgs.
VICERRECTOR DE DESARROLLO E INNOVACION DEL ISTS

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO VICERRECTORADO

Matriz: Miguel Riofrío 156-25 entre Sucre y Bolívar. Telfs: 07-2587258 / 07-2587210 Pagina Web: www.tecnologicosudamericano.edu.ec

16.2 Anexo II: Autorización para la ejecución

Yo, Ing. Leydi Maribel Mingo Morocho, Mgs. con documento de identidad 1105653792, coordinadora de la carrera de Electrónica del Instituto Superior Tecnológico Sudamericano de la ciudad de Loja a petición verbal del interesado.

AUTORIZO

A Duvan Anival Castillo Torres con cédula de identidad Nro. 1104574445, estudiantes del sexto ciclo de la carrera de Electrónica del "Instituto Superior Tecnológico Sudamericano"; para que realicen su proyecto de investigación de fin de carrera titulado: "Implementación de un sistema de reconocimiento facial con notificaciones móviles para control de acceso residencial utilizando raspberry pi en la ciudad de Loja durante el periodo abril-septiembre 2023."para lo cual nos comprometemos en entregar a los estudiantes la información necesaria hasta que culmine dicho proceso.

Loja, 07 de noviembre del 2023

Ing. Leydi Maribel Mingo Morocho, Mgs.

C.I. 1105653792

16.3 Anexo III: Certificado de implementación

Loja, 07 de noviembre del 2023

Ing. Leydi Maribel Mingo Morocho

TUTOR DEL SEMINARIO DE PROYECTOS DE INVESTIGACIÓN DE FIN DE CARRERA- ELECTRÓNICA, a petición verbal por parte del interesado.

CERTIFICO

Que el ***Sr Duvan Anival Castillo Torres*** *con cédula* ***1104574445*** *ha venido trabajando en el Proyecto de fin de carrera titulado* "Implementación de un sistema de reconocimiento facial con notificaciones móviles para control de acceso residencial utilizando raspberry pi en la ciudad de Loja durante el periodo abril-septiembre 2023."; *el mismo que se encuentra a la presente fecha en un 100% culminado según los requerimientos funcionales planteados. Lo certifico en honor a la verdad para los fines pertinentes y a solicitud del interesado.*

Ing. Leydi Maribel Mingo Morocho, Mgs.

TUTOR DE PROYECTO DE INVESTIGACIÓN DE FIN DE CARRERA

Semestre abril – septiembre 2023

16.4 Anexo IV: Presupuesto

A continuación, se describe los costos del proyecto, en la tabla 1 se detalla los componentes electrónicos y materiales que se van a utilizar en el prototipo, en la tabla 2 se describe los recursos humanos, tecnológicos y logísticos, por último, en la tabla 3 se describe el presupuesto total del proyecto.

Tabla 2

Componentes para el prototipo.

Cantidad	Componentes	VALOR UNITARIO	VALOR TOTAL
1	Placa Computadora Raspberry Pi 4 B 4G.	$150.00	$150.00
1	Cámara Para RasberryPi	$10.00	$10.00
1	Modulo Relé	$2.00	$2.00
1	Fuente 12V	$4.00	$4.00
1	Cerradura eléctrica solenoide 12V DC	$10.00	$10.00
1	Otros	$50.00	$50.00
		TOTAL	$226.00

Tabla 3

Recursos del proyecto

Recursos Humanos				
Cantidad	**Nombre del recurso**	**Descripción**	**Valor unitario**	**Valor total**
1	Desarrollador del proyecto	Estudiante que documenta el proyecto	$0.00	$0.00
1	Directora del proyecto	Tutor que guía el desarrollo del proyecto	$0.00	$0.00
1	Propietario inmueble	Propietario del inmueble donde se implementará el prototipo	$0.00	$0.00
			TOTAL	**$0.00**
Recursos Tecnológicos				
Cantidad	**Nombre del recurso**	**Descripción**	**Valor unitario**	**Valor total**
6 (meses)	Internet	Búsqueda de información	$11	$66
			TOTAL	**$66**
Hardware				
Cantidad	**Nombre del recurso**	**Descripción**	**Valor unitario**	**Valor total**
1	Celular	Capturas y pruebas	$300.00	$50.00 (depreciado)
1	Computador	Búsqueda de información, codificación del código en el software Arduino	$900.00	$200.00 (depreciado)
			TOTAL	**$250.00**
Software				
Cantidad	**Nombre del recurso**	**Descripción**	**Valor unitario**	**Valor total**
1	Office	Word, Excel, PowerPoint	$0.00	$0.00
1	Rasbian	Sistema Operativo	$0.00	$0.00
			TOTAL	**$0.00**
Recursos Logísticos				
Cantidad	**Nombre del recurso**	**Descripción**	**Valor unitario**	**Valor total**
1	Resma de hojas	Impresión de documentos para el desarrollo del proyecto	$5.00	$5.00
			TOTAL	**$5.00**

Tabla 4

Presupuesto del proyecto

Presupuesto del proyecto	
Recursos Humanos	$0.00
Recursos Tecnológicos	$66.00
Hardware	$250.00
Software	$0.00
Recursos Logísticos	$5.00
Componentes para el prototipo	$226.00
TOTAL	**$547.00**

16.5 Anexo V: Cronograma

Tabla 5

Cronograma de Actividades

CRONOGRAMA DETALLADO DE ACTIVIDADES																															
ESTUDIANTE: DUVAN ANIVAL CASTILLO TORRES.																															
CARRERA: Tecnología Superior en Electrónica.		**SEMESTRE:** abril – septiembre 2023																													
ACTIVIDADES		Abril				Mayo				Junio				Julio				Agosto				Septiembre				Octubre					
Componente	**Proyecto de Investigación de Fin de Carrera**	Semana				Semana				Semana				Semana				Semana				Semana				Semana					
# Por Semanas		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
Petición de solicitudes para el proceso de titulación		x	x																												
Identificación del problema				x																											
Planteamiento del tema					x																										
Elaboración de justificación						x																									
Planteamiento objetivos general y específicos							x																								
Marco institucional y Marco teórico								x	x																						
Elaboración de la Metodología										x																					
Presentación del Anteproyecto de Investigación											x																				
Desarrollo de investigación y propuesta de acción												x	x	x	x	x	x	x	x	x	x	x	x	x	x	x					
Elaboración de conclusiones y recomendaciones																											x	x			
Entrega de borradores de proyectos de investigación de fin de carrera																															x

16.6 Anexo VI: Programación

16.6.1 Programación detección de rostro

```
import cv2

from picamera.array import PiRGBArray

from picamera import PiCamera

import numpy as np

import os

import sys



camera = PiCamera()

camera.resolution = (640, 480)

camera.framerate = 60

rawCapture = PiRGBArray(camera, size=(640, 480))



faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")



name = input("Ingrese el nombre de la persona ")

dirName = "./images/" + name

print(dirName)

if not os.path.exists(dirName):
```

```
            os.makedirs(dirName)
            print("Directorio creado")
        else:
            print("No se creo el directorio")
            sys.exit()

        count = 1
        for frame in camera.capture_continuous(rawCapture, format="bgr",
use_video_port=True):
            if count > 60:
                break
            frame = frame.array
            gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
            faces = faceCascade.detectMultiScale(gray, scaleFactor = 1.5,
minNeighbors = 5)
            for (x, y, w, h) in faces:
                roiGray = gray[y:y+h, x:x+w]
                fileName = dirName + "/" + name + str(count) + ".jpg"
                cv2.imwrite(fileName, roiGray)
                cv2.imshow("face", roiGray)
```

```
            cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
            count += 1


        cv2.imshow('frame', frame)
        key = cv2.waitKey(1)
        rawCapture.truncate(0)


        if key == 27:
            break

cv2.destroyAllWindows()
```

16.6.2 Programación para el entrenador

```
import os

import numpy as np

from PIL import Image

import cv2

import pickle



faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

recognizer = cv2.face.LBPHFaceRecognizer_create()



baseDir = os.path.dirname(os.path.abspath(_file_))

imageDir = os.path.join(baseDir, "images")



currentId = 1

labelIds = {}

yLabels = []

xTrain = []



for root, dirs, files in os.walk(imageDir):

        print(root, dirs, files)
```

```
                for file in files:
                    print(file)
                    if file.endswith("png") or file.endswith("jpg"):
                        path = os.path.join(root, file)
                        label = os.path.basename(root)
                        print(label)

                        if not label in labelIds:
                            labelIds[label] = currentId
                            print(labelIds)
                            currentId += 1

                        id_ = labelIds[label]
                        pilImage = Image.open(path).convert("L")
                        imageArray = np.array(pilImage, "uint8")
                        faces = faceCascade.detectMultiScale(imageArray,
scaleFactor=1.1, minNeighbors=5)

                        for (x, y, w, h) in faces:
                            roi = imageArray[y:y+h, x:x+w]
```

```
                    xTrain.append(roi)
                    yLabels.append(id_)

with open("labels", "wb") as f:
        pickle.dump(labelIds, f)
        f.close()

recognizer.train(xTrain, np.array(yLabels))
recognizer.save("trainer.yml")
print(labelIds)
```

16.6.3 Programa activador

```
import cv2

from picamera.array import PiRGBArray

from picamera import PiCamera

import numpy as np

import pickle

import RPi.GPIO as GPIO

import requests

from time import sleep



# Configura tu token de Telegram y el chat_id aquí

TELEGRAM_TOKEN = '6160953320:AAGj1Uefdphlq---
I7xCuzbkMgHOvTSMYYM'

TELEGRAM_CHAT_ID = '1420920594'



relay_pin = 26

door_sensor_pin = 18



# Configuración del pin del relé

GPIO.setmode(GPIO.BCM)
```

```
GPIO.setwarnings(False)  # Desactiva las advertencias de GPIO

GPIO.setup(relay_pin, GPIO.OUT)

GPIO.setup(door_sensor_pin, GPIO.IN)


# Inicializa el pin del relé en el estado desactivado (HIGH)

GPIO.output(relay_pin, 1)


with open('labels', 'rb') as f:

    dicti = pickle.load(f)

    f.close()


camera = PiCamera()

camera.resolution = (640, 480)

camera.framerate = 30

rawCapture = PiRGBArray(camera, size=(640, 480))


faceCascade = cv2.CascadeClassifier("haarcascade_frontalface_default.xml")

recognizer = cv2.face_LBPHFaceRecognizer.create()

recognizer.read("trainer.yml")
```

```
        font = cv2.FONT_HERSHEY_SIMPLEX


        while True:

            for frame in camera.capture_continuous(rawCapture, format="bgr",
use_video_port=True):

                frame = frame.array

                gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)

                faces = faceCascade.detectMultiScale(gray, scaleFactor=1.5,
minNeighbors=5)


                for (x, y, w, h) in faces:

                    roiGray = gray[y:y + h, x:x + w]

                    id_, conf = recognizer.predict(roiGray)


                    for name, value in dicti.items():

                        if value == id_:

                            print(name)


                    if conf <= 70:

                        GPIO.output(relay_pin, 0)
```

```
                cv2.rectangle(frame, (x, y), (x + w, y + h), (0, 255, 0), 2)
                cv2.putText(frame, name + str(conf), (x, y), font, 2, (0, 0, 255), 2,
cv2.LINE_AA)

                # Lee el estado del sensor magnético
                door_status = GPIO.input(door_sensor_pin)

                # Determina si la puerta está abierta o cerrada
                if door_status == GPIO.HIGH:
                    door_status_message = "La puerta está abierta."
                else:
                    door_status_message = "La puerta está cerrada."

                # Envía una notificación a Telegram con el estado de la puerta
                message = f'Cerradura electrónica activada por
{name}\n{door_status_message}'
                telegram_url =
f'https://api.telegram.org/bot{TELEGRAM_TOKEN}/sendMessage'
                payload = {
                    'chat_id': TELEGRAM_CHAT_ID,
```

```
            'text': message
        }
        requests.post(telegram_url, data=payload)

    else:
        GPIO.output(relay_pin, 1)

    cv2.imshow('frame', frame)
    key = cv2.waitKey(1)

    rawCapture.truncate(0)

    if key == 27:
        break

cv2.destroyAllWindows()
```

16.7 Anexo VII: Conexión de sensor.

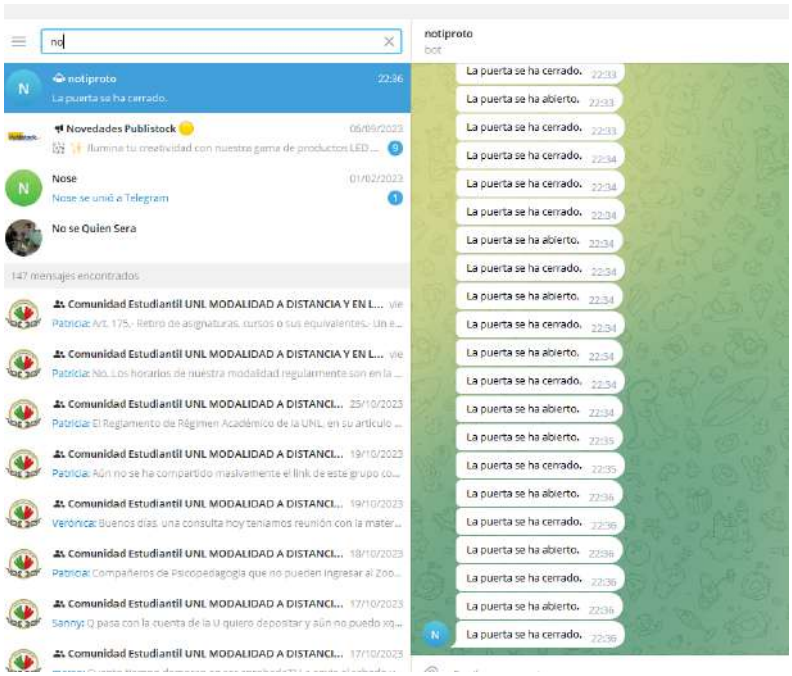
Figura 39

conexión de la cámara y sensor magnético

Nota. Se prueba la función de la cámara y el sensor magnético.

Figura 40

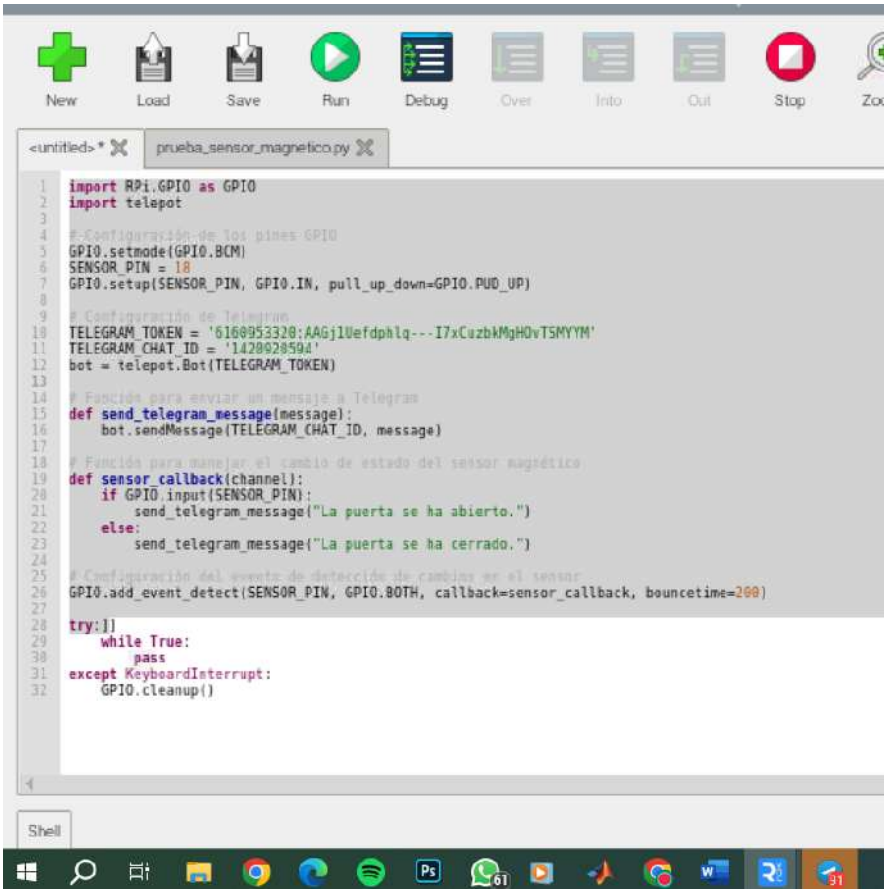
Pruebas de sensor magnetico



Nota. Se verifican las notificaciones en telegram.

Figura 41

Programación para la prueba del sensor



Nota. Programación usada para la prueba de envió de notificaciones a Telegram

16.8 Anexo VIII: Certificado del Abstract

INSTITUTO TECNOLÓGICO SUDAMERICANO *Hacemos gente de talento!*

ENGLISH AREA SUDAMERICANO INSTITUTE

CIS CENTRO DE IDIOMAS SUDAMERICANO

CERTF. Nº. 006-KC-ISTS-2023
Loja,30 de Octubre de 2023

La suscrita, Lic. Karla Juliana Castillo Abendaño, ***DOCENTE DEL ÁREA DE INGLÉS - CIS DEL INSTITUTO SUPERIOR TECNOLÓGICO "SUDAMERICANO"****, a petición de la parte interesada y en forma legal,*

C E R T I F I C A:

Que el apartado ***ABSTRACT*** *del Proyecto de Investigación de Fin de Carrera del señor DUVAN ANIVAL CASTILLO TORRES estudiante en proceso de titulación periodo Abril – Noviembre 2023 de la carrera de ELECTRÓNICA; está correctamente traducido, luego de haber ejecutado las correcciones emitidas por mi persona; por cuanto se autoriza la impresión y presentación dentro del empastado final previo a la disertación del proyecto.*

Particular que comunico en honor a la verdad para los fines académicos pertinentes.

English is a piece of cake.

Checked by:
Lic. Karla Juliana Castillo Abendaño
ENGLISH TEACHER

Lic. Karla Juliana Castillo Abendaño
DOCENTE DEL ÁREA DE INGLÉS ISTS - CIS