Implementación de un sistema de seguridad con cerradura biométrica para el control de acceso a un domicilio

Rueda Sánchez, Stephanie Michelle

Departamento de Eléctrica y Electrónica

Carrear de Tecnología en Electrónica mención Instrumentación & Aviónica

Monografía, previo a la obtención del título de Tecnólogo en Electrónica mención Instrumentación y Aviónica

Ing. Calvopiña Osorio, Jenny Paola

Latacunga, 20 de mayo del 2021

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA MENCIÓN

INSTRUMENTACIÓN Y AVIÓNICA

CERTIFICACIÓN

Certifico que la monografía, "**IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CON CERRADURA BIOMÉTRICA PARA EL CONTROL DE ACCESO A UN DOMICILIO"** fue realizado por la señorita ***Rueda Sánchez, Stephanie Michelle*** la cual ha sido revisada y analizada en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Latacunga, 20 de mayo del 2021

Firmado electrónicamente por:
JENNY PAOLA CALVOPINA OSORIO

……
Ing. Calvopiña Osorio, Jenny Paola
C.C.: 0503390239

URKUND

Urkund Analysis Result

Analysed Document: PROYECTO TECNICO_MICHELLE RUEDA.pdf (D105620747)
Submitted: 5/19/2021 11:20:00 PM
Submitted By: smrueda2@espe.edu.ec
Significance: 2 %

Sources included in the report:

Tesis-Molina 1 y 2.docx (D62711229)
DOCUMENTO DE TESIS 22 AGOSTO.docx (D21465374)
SEBASTIAN ALEXANDER TRUJILLO FLORES.pdf (D97871381)
https://repository.ucatolica.edu.co/bitstream/10983/24032/1/Final%20Trabajo%20de%20grado.pdf
http://190.169.30.62/bitstream/123456789/14700/1/TEG%20-%20De%20Sousa%2C%20Mora.pdf
https://dspace.ups.edu.ec/bitstream/123456789/18536/1/UPS%20-%20ST004470.pdf

Instances where selected sources appear:

10

JENNY PAOLA CALVOPINA OSORIO

Ing. Calvopiña Osorio, Jenny Paola
C.C.: 0503390239

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA MENCIÓN

INSTRUMENTACIÓN Y AVIÓNICA

RESPONSABILIDAD DE AUTORÍA

Yo, ***Rueda Sánchez, Stephanie Michelle***, con cédula de ciudadanía **N° 1805168844**, declaro que el contenido, ideas y criterios de la monografía**: IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CON CERRADURA BIOMÉTRICA PARA EL CONTROL DE ACCESO A UN DOMICILIO,** es de mi autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos, y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 20 de mayo del 2021

……

Rueda Sánchez, Stephanie Michelle

C.C.: 1805168844

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE TECNOLOGÍA EN ELECTRÓNICA MENCIÓN INSTRUMENTACIÓN Y AVIÓNICA

AUTORIZACIÓN DE PUBLICACIÓN

Yo ***Rueda Sánchez, Stephanie Michelle***, con cédula de ciudadanía **N° 1805168844**, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar la monografía: **IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD CON CERRADURA BIOMÉTRICA PARA EL CONTROL DE ACCESO A UN DOMICILIO** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Latacunga, 20 de mayo del 2021

……

Rueda Sánchez, Stephanie Michelle

C.C.: 1805168844

Dedicatoria

A mi madre, por su apoyo, sus palabras de consuelo, por su infinita paciencia y su gran amor, que hicieron de mi la mujer responsable y valiente que soy.

A mi hermana, por animarme cada día a sonreír, apoyarme y saber que cada esfuerzo es por ella.

RUEDA SÁNCHEZ STEPHANIE MICHELLE

Agradecimiento

A mí, por creer que lo voy a lograr, por superarme todos los días, por demostrar que una mujer puede superar sus propias expectativas, por levantarme todos los días temprano y pedir a Dios que me de fuerzas para seguir adelante, por desvelarme muchos días, por dañar y volver arreglar los proyectos que me dieron experiencia y por los buenos momentos que compartí con gente muy valiosa.

A toda mi familia por empujarme a ser mejor cada día y luchar por un mejor futuro.

RUEDA SÁNCHEZ STEPHANIE MICHELLE

Tabla de contenidos

Índice de tablas

Índice de figuras

Resumen

Para el presente proyecto de titulación, se implementa un sistema de seguridad para un domicilio a través de una cerradura biométrica el cual permitirá el control de acceso de dicha vivienda para resguardar las pertenencias e integridad de la familia utilizando un sistema de identificación facial basado en la tecnología Raspberry Pi, un software libre de visión por computadora como es OPENCV y un entorno de programación compatible como es Python. Se realizó la programación basado en el procesamiento digital de imágenes mediante una cámara conectada a la tarjeta Raspberry registrando los aspectos físicos y rasgos faciales, este sistema permite el acceso únicamente a las personas que lo frecuentan y están registrados como usuarios en una tarjeta de memoria microSD que procesa el reconocimiento facial comparándola con los registros almacenados y otorgando el acceso a la vivienda, este proceso permitirá al activación de un relé o relevador que al ser energizado mediante la tarjeta Raspberry accionara la cerradura eléctrica permitiendo la apertura de la puerta del domicilio. Además del envió de imágenes por correo electrónico al propietario de la vivienda registrando las personas que van a ingresar mediante un sensor de movimiento colocado en la parte inferior de la puerta, el cual detectara la presencia de una persona a los 3 metros de distancia. Al final del documento se incluye los resultados de las pruebas de funcionamiento.

PALABRAS CLAVE:

- **RECONOCIMIENTO FACIAL.**
- **TECNOLOGÍA RASPBERRY.**
- **SEGURIDAD BIOMÉTRICA.**
- **CONTROL DE ACCESO.**

Abstract

For this degree project, a security system is implemented for a home through a biometric lock which will allow access control of the house to protect the belongings and integrity of the family using a facial identification system based on Raspberry Pi technology, a free computer vision software such as OPENCV and a compatible programming environment such as Python. Programming was performed based on digital image processing through a camera connected to the Raspberry card recording the physical aspects and facial features, this system allows access only to people who frequent it and are registered as users on a microSD memory card that processes facial recognition by comparing it with the stored records and granting access to the house, this process will allow the activation of a relay or relay that when energized by the Raspberry card will trigger the electric lock allowing the opening of the door of the house. In addition to sending images by email to the owner of the house registering the people who will enter through a motion sensor placed at the bottom of the door, which will detect the presence of a person at 3 meters away. At the end of the document the results of the operation tests are included.

KEY WORDS:

- **FACIAL RECOGNITION.**
- **RASPBERRY TECHNOLOGY.**
- **BIOMETRIC SECURITY.**
- **ACCESS CONTROL.**

CAPITULO I

1. Introducción

1.1 Tema

Implementación de un sistema de seguridad con cerradura biométrica para el control de acceso a un domicilio

1.2 Antecedentes

Hoy en día los avances tecnológicos han mejorado la vida de muchas personas, facilitando herramientas, dispositivos o máquinas automatizadas que prometen muchas mejoras y cambios positivos en cualquier aérea ya sea industrial, ambiental o humanitario a nivel global.

La seguridad en un hogar es necesaria y primordial para el bienestar de las personas que residen en él, tomando medidas para crear un ambiente seguro y libre de miedos, es prioridad absoluta garantizar la integridad física frente a cualquier amenaza del exterior con dispositivos al alcance de nuestros bolsillos (Bricoladores, S. 2018).

La seguridad en los hogares es un tema primordial y sensible de tratar ya que involucra todos los espacios del hogar íntimos y abiertos, frecuentemente al hablar de seguridad se entiende por mecanismos que prevengan robos, actos vandálicos y otros percances principalmente en el exterior del hogar. Un sistema de seguridad desde el más básico para el hogar puede llegar a costar alrededor de 200 a 500 $ dólares y los más sofisticados con aplicaciones móviles pueden llegar a costar miles de dólares (Martínez Pablo, 2019).

Para el desarrollo de sistemas automatizados de seguridad se puede tener en cuenta diversas técnicas y aplicaciones que faciliten al usuario su uso y funcionamiento ideal, como son la huella dactilar, el reconocimiento facial, la identificación por iris, entre otras técnicas novedosas que cada día se desarrollan mediante diferentes software y hardware. Además, existen alternativas más económicas en placas de desarrollo como son Arduino, Raspberry Pi, Beaglebone, Intel Galileo Gen, entre otras placas con las que se puede implementar sistemas de seguridad más accesibles y que se adapten a las necesidades de un hogar.

Como se ha podido evidenciar, existen varias razones por las cuales un hogar debe ser protegido y vigilado de manera segura ya sea este con un sistema completo de seguridad con dispositivos sofisticados y asesoría inteligente o un sistema no complejo pero eficiente que permita salir de casa de manera segura.

1.3 Planteamiento del problema

En los últimos meses la economía mundial ha cambiado drásticamente debido a la pandemia del Covid-19 que está atravesando y ha generado una disminución de ingresos en todos los hogares, aumentando el número de vandalismos e intromisión a la propiedad privada, dejando vulnerables a familias y sus pertenencias.

En la prensa a diario, se encuentran publicaciones de saqueos y vandalismo que han asustado a la población generando disturbios y miedo en muchas partes del país, dejando en evidencia que existe un gran impacto de vulnerabilidad en los hogares debido a la pandemia, demandando mayor gasto en sistemas de seguridad que protejan el hogar y las personas que lo frecuentan.

Por lo expuesto es necesario generar alternativas más económicas y accesibles en cuestión de seguridad para el hogar, que permita salir sin preocupaciones y actuar de manera rápida cuando este lo requiera, otorgando así opciones de manera eficiente y sustentable.

1.4 Justificación

El presente proyecto de grado plantea el uso de la tecnología como una solución útil y eficaz, mediante una cerradura biométrica que registrará los rasgos faciales solamente de los usuarios que frecuentan el domicilio para la apertura del mismo y con el envío de imágenes al correo electrónico de la persona que ingresa. Este sistema de seguridad que se implementará, ayudará a:

- Obtener la información de quienes ingresaron y salieron del domicilio.
- Registrar un sin número de rostros faciales para la apertura del domicilio.
- Activar y desactivar la cerradura biométrica solamente por el propietario mediante el reconocimiento facial.

Los residentes directos del hogar se beneficiarán del sistema de seguridad biométrica manteniendo la seguridad del hogar, sus pertenencias y a las personas que lo frecuentan, conservando la tranquilidad y confianza al salir del hogar sin preocupaciones.

El propósito de la investigación y la implementación del sistema de seguridad biométrico es brindar una alternativa de bajo costo y eficaz en la detección facial, ejecutando programaciones y algoritmos que faciliten el uso del sistema y elementos necesarios de fácil adquisición como es la tarjeta Raspberry Pi, cámara, fuentes de alimentación, relé de un canal, cerradura eléctrica, sensor de movimiento y conexiones que aporten a la construcción del proyecto.

1.5 Objetivos

1.5.1 *Objetivo General*

Implementar un sistema de seguridad con cerradura biométrica para el control de acceso a un domicilio.

1.5.2 *Objetivos específicos*

- Analizar la importancia de la seguridad electrónica en los hogares con alternativas accesibles y eficientes como es la biométrica.
- Definir las características y requerimientos del domicilio para el diseño del sistema de reconocimiento facial mediante tecnología Raspberry.
- Implementar y comprobar el funcionamiento del sistema de seguridad biométrico.

1.6 Alcance

La solución propuesta se implementará mediante tarjetas electrónicas como Raspberry Pi, Relé, alarma, sensor de movimiento y programaciones que permitirán la activación de la cerradura mediante el reconocimiento facial.

Finalmente se desarrollará la instalación del sistema de seguridad en un domicilio, con la demostración y verificación de la cerradura biométrica mejorando la calidad y estilo de vida de los propietarios de la vivienda y a su vez aumentar el nivel de seguridad de la puerta principal de su hogar. Este presente proyecto también servirá de fuente de información y consulta para todas aquellas personas relacionadas o interesadas en el tema, ya que su uso aumenta sustancialmente, debido a que los rasgos físicos son imposibles de falsificar.

CAPITULO II

2. Marco teórico

2.1 Automatización y seguridad

Cada año la digitalización global es una ventaja que mejora el bienestar en hogares o domicilios generando gran comodidad y bienestar a través del control inteligente de dispositivos IoT en nuestros hogares.

Una vivienda premium abarca 3 aspectos importantes: confortable, sostenible y segura; siendo un reto conseguir que las nuevas tecnologías sean compatibles y equivalentes a los protocolos de seguridad según Ángel Olleros educador de seguridad. (Olleros,2020).

Para la automatización su objetivo es interconectar todos los dispositivos y elementos posibles facilitando no solo la seguridad del hogar también ofrecer conforts del mismo en un solo dispositivo cómodo y fácil de utilizar. Sin embargo, todos estos sistemas se basan en controladores y aplicaciones que dependen de servidores de internet por lo cual la seguridad de un hogar también dependerá de los proveedores del servicio automatizado, elevando así sus costos.

2.1.1 Domótica e Inmótica

La domótica hace referencia a un conjunto de sistemas óptimos para automatizar un hogar. Todos estos elementos enlazados electrónicamente mediante software dan la posibilidad de controlar a distancia o al interior de la vivienda su entorno y seguridad. (Romero, 2010).

La domótica trae una serie de beneficios que actúan en varias áreas como se muestra en la figura 1 y se especifica a continuación:

- **Confort.** La mayoría de tareas en el hogar pueden ser automatizadas, principalmente las áreas denominadas CVC (climatización, ventilación y calefacción). Todos los sistemas que contribuyen al bienestar, comodidad y reducción del trabajo doméstico.
- **Seguridad.** Es una de las opciones más demandadas y desarrolladas a nivel global, integrando múltiples acciones en una sola aplicación. Puede llegar a detectar cualquier tipo de fuga, fuego o intrusos activando las respectivas alarmas y notificando a los servidores.
- **Ahorro energético.** Al ser todo de manera automática pueden ser programables muchas funciones para desconectar o conectar los diferentes aparatos del hogar con la finalidad de reducir costos.
- **Comunicación.** Todos los sistemas al estar interconectados pueden ser accesibles a su configuración e información.

Figura 1

Áreas de Domótica

Nota: La figura muestra las diferentes áreas que puede ser aplicado la Domótica. (Instalaciones Domóticas, 2020).

Uno de los temas a tratar con más relevancia en la domótica es la seguridad del hogar, esta problemática creciente en los últimos tiempos puede ejercer varias soluciones como cámaras de vigilancia, sensores de presencia, alarmas, accesos biométricos, entre otros que la convierten en un hogar seguro.

Por otro lado, la inmótica es un conjunto de tecnologías automatizadas aplicado a edificios de dimensiones grandes como hoteles, escuelas, centros comerciales, hospitales y otros, aportando un ahorro energético, seguridad y confort, gestionando servicios para reducir costes de energía y operación, creando así edificios inteligentes que aporten mayor crecimiento tecnológico. (Romero, 2010).

La inmótica centra la automatización integral de edificios empleando una tecnología más avanzada logrando proporcionando información del funcionamiento, el estado del servicio, los mantenimientos necesarios, entre otras funciones que interconectan por medio de redes interiores y exteriores de manera inteligente, optimizan los sistemas de control y automatización. Su utilización conduce varias mejoras como:

- Mejora la eficiencia energética, reduciendo su consumo y optimizando su funcionamiento.
- Mejora notablemente la seguridad y el confort, debido a la tecnología accesible, eficiente y fácil de utilizar.
- Facilita el mantenimiento del edificio con simples revisiones.

Algunas de las diferencias entre Domótica e Inmótica se puede observar en la tabla 1.

Tabla 1

Diferencia entre Domótica e Inmótica

DOMÓTICA	**INMÓTICA**
Aplicado a viviendas o propiedades en escala pequeña	Aplicado a edificios no destinados a vivienda, a escalas grandes como: hoteles, aeropuertos, universidades, entre otros.
Mejoran la eficiencia en el hogar aplicándolo a funciones específicas en la vivienda.	Mejora considerablemente los sistemas de control y vigilancia, con mayor capacidad de funciones complejas.
Sistemas más sencillos y fáciles de gestionar.	Sistemas más complejos que requieren de personas calificadas para su instalación y mantenimiento.
Sus precios son más variados debido a que son sistemas básicos.	Varía mucho sus valores dependiendo el tamaño del edificio o lugar a ser instalados.
La mayoría de sistemas domóticos utilizan las redes inalámbricas para su instalación. Facilitando su arquitectura.	Es más usual encontrar sistemas centralizados y distribuidos con cableado y de manera secundaria de forma inalámbrica.

Nota: la tabla muestra las diferencias entre la Domótica e Inmótica en el ámbito general. (Domótica e inmótica: viviendas y edificios inteligentes, 2011).

2.1.2 Biometría

Para la Real Academia de la Lengua Española biometría es el estudio mensurativo o estadístico de los fenómenos o procesos biológicos. (Asale, R., 2020). Sin embargo, para los fines que concierne la biometría es un conjunto de métodos automatizados para el análisis de determinadas características humanas las cuales serán identificadas o autenticadas.

El uso de las tecnologías biométricas ha producido un enorme crecimiento en la última década, este tipo de reconocimiento físico resulta único, inimitable e intransferible destacando sus aplicaciones en el ámbito de la seguridad.
Todo rasgo biométrico se agrupa en los siguientes tipos:

- **Fisiológicos o morfológicos:** conlleva aquellos rasgos inalterables como: la huella dactilar, voz, rostros, iris y retina del ojo, palma de la mano mediante venas y sus ramificaciones.
- **Conductuales:** hacen referencia a las características de la conducta de la persona como: dinámica de firma, tipo de escritura, modulaciones de voz, pulsaciones de teclado, etc.

Los sistemas biométricos analizan determinadas características de una o más personas, mediante un lector o sensor que digitaliza el patrón para ser autenticado a través del software el cual analiza y encripta dicha información para comparar los datos ingresados y autorizar al individuo.

Con el pasar del tiempo se ha mejorado mucho la calidad de lectura de los sensores disminuyendo las tasas de errores y aumentado su optimización, mejorando no solo la utilización de softwares libres también un sin número de aplicaciones que pueden ser acopladas a nuestro entorno como se puede evidenciar en la Tabla 2.

Tabla 2

Tipos de Biometría

TIPO DE TECNOLOGIA	FUNCIONAMIENTO	USOS
HUELLA DACTILAR	Está basado en un escáner o sensor óptico, utilizando técnicas de análisis de patrón, según los registros almacenados.	Desbloqueo de celulares, formas de pago, firma, registro laboral.
FACIAL	Esta técnica reconoce a una persona a partir de una imagen o fotografía, todo mediante programaciones que analizan los rostros humanos.	Control de acceso, investigación de delitos.
IRIS	Este método utiliza una cámara infrarroja que verifica las características del iris para identificar a la persona.	Gestión de fronteras y defensa, dispositivos móviles con cámaras infrarrojas.
GEOMETRÍA DE LA MANO	Utiliza la forma de la mano para identificar a la persona mediante cinco guías y capturas en 3D son verificadas las curvas, dedos, grosor y longitud.	Identificación criminal, control de acceso de personal.
RETINA	Utiliza un patrón de vasos sanguíneos, este al ser único la convierte en una técnica muy segura y eficaz.	Servicios médicos, centros penitenciarios.
LÍNEAS DE LA PALMA DE LA MANO	Mediante los surcos y pliegues de la mano, el sensor busca las coincidencias para identificar al individuo.	Acceso a bancos.

TIPO DE TECNOLOGÍA	FUNCINAMIENTO	USOS
GEOMETRÍA DE LAS VENAS	Se basa en la estructura de las venas de la mano o el dedo, estas al ser definidas antes del nacimiento las posibilidades de similitudes son nulas. Mediante un sensor infrarrojo se obtiene la imagen del patrón de las venas generando una plantilla biométrica.	Seguridad electrónica.
FORMA DE OREJAS	A partir de las formas de las orejas, es analizado con una imagen infrarroja identificando a la persona.	Control de presencia, autenticación.
PIEL	Mediante una imagen de la superficie de la piel, es clasificada mediante algoritmos de análisis su textura, características, generando una serie de plantillas para su identificación.	Es una mejora del reconocimiento dactilar y facial.

Nota: La tabla muestra las tecnologías biométricas que existen en la actualidad. (Estudios sobre las tecnologías biométricas aplicadas a la seguridad, 2011).

Los aspectos fisiológicos son considerados los más seguros y difíciles de falsificar, por lo expuesto se puede considerar que los sistemas de seguridad que utilizan sistemas biométricos convertirán a una vivienda mucho más segura y de manera eficiente.

2.2 Reconocimiento facial

El reconocimiento facial es el segundo sistema más empleado en el mundo, siendo abarcado en diferentes áreas de la investigación, esto puede ser utilizados a distancia, sin el contacto del usuario, mediante una cámara, un software y una serie de algoritmos que reconoce los patrones de las facciones del rostro de la persona transformando a una imagen bidimensional o tridimensional, creando una matriz de similitudes y comparándolas con la base de datos de cientos de fotos. El software emplea las siguientes fases:

- **Detección:** captura el rostro del usuario.
- **Extracción de características faciales:** una vez obtenida la información biométrica de las facciones del usuario, denominado patrón biométrico facial.
- **Comparación:** mediante la base de datos ya antes registrada, se compara la información obteniendo un porcentaje de similitud.
- **Toma de decisión:** al obtener el porcentaje de similitud con el umbral de coincidencia muy elevado se otorgará el permiso de la persona caso contrario negará el acceso.

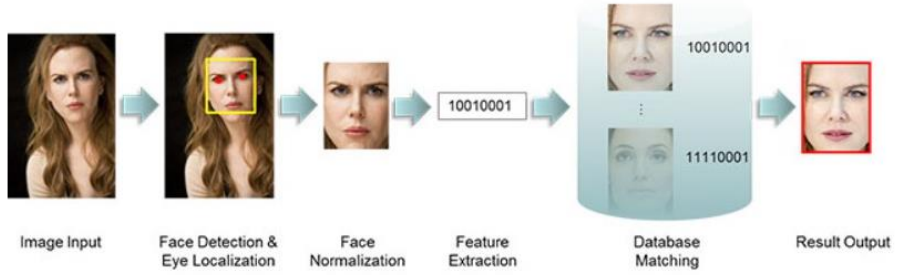
2.3 Fases del reconocimiento facial

La visión artificial es una de las áreas más investigadas y desarrolladas en el campo de la tecnología, en particular el reconocimiento facial que forma parte de las soluciones más complejas y requeridas en el mundo ha desarrollado métodos y técnicas cada vez más seguras para que el reconocimiento de personas no pueda ser suplantado por imágenes o fotocopias de usuarios vulnerando la seguridad de los sistemas.

El desarrollo de esta tecnología avanzado con el pasar de los años a utilizar softwares más complejos para la autenticación de personas, es así que se divide en varias fases que permiten una autenticación eficaz y segura como se muestra en la figura 2. (Gavilán, 2020).

Figura 2

Fases del reconocimiento facial



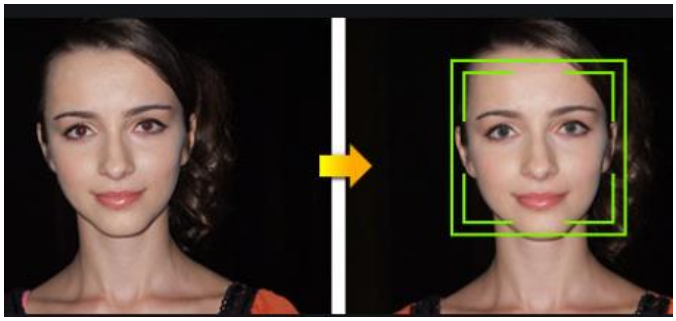
Nota: La imagen muestra las fases que transcurre una imagen para ser detectada. (Las cuatro fases del reconocimiento facial, 2020).

2.3.1 Detección de rasgos faciales y normalización.

La primera fase de detección consiste en reconocer la imagen del usuario o usuarios que estén presentes, esto mediante la cámara que este implementada. Al capturar el rostro de la persona el programa obtiene la información biométrica de todos los rasgos faciales denominados patrón biométrico facial. Estas áreas específicas son captadas por el dispositivo, descartando toda área que no corresponda a un patrón facial, ignorando el fondo de la imagen y formando una silueta en el rostro identificado. La extracción biométrica es analizada por el dispositivo, alineando todos los rasgos encontrados, comúnmente llamado normalización las imágenes son ajustadas según sus elementos ya sean por geometría, tamaño o fotometría se realiza un escalado y recorte rectangular de la imagen como se evidencia en la figura 3, para conseguir una coincidencia entre miles de imágenes dentro de la base de datos. (Gavilán,2020).

Figura 3

Detección y Normalización



Nota: La figura muestra el recuadro de normalización al detectar un rostro. (Robologs, 2020).

2.3.2 Extracción de imágenes.

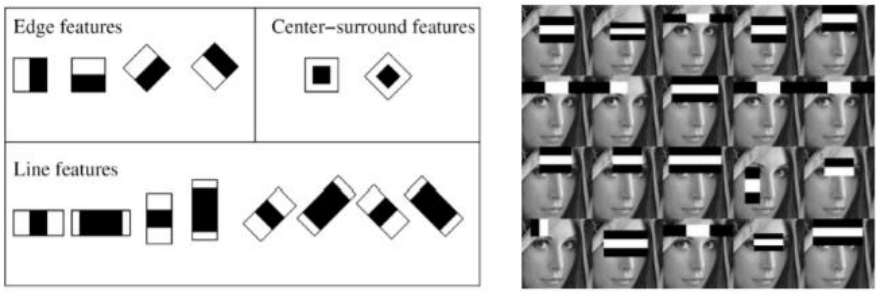
Una vez obtenida la información biométrica inicia la fase de búsqueda de similitudes, estableciendo un patrón biométrico facial que es comparado en una plantilla de imágenes de la base de datos. La extracción de características de la imagen puede ser obtenida mediante varios métodos de detección facial que utilizan distintos algoritmos para detectar objetos en tiempo real, el más popular y eficiente es el método de Viola-Jones, el cual será utilizado en el presente proyecto.

2.3.3 Algoritmo de Viola-Jones

Este algoritmo creado en 2001 por Paul Viola y Michael Jones para la detección de objetos concretos basa en un algoritmo clasificador llamado Haar-like features, que emplea una serie de rectángulos clasificadores sobre una región de interés como se muestra en la figura 4, cuando se quiere detectar un objeto se buscan diferencias en regiones rectangulares en una ventana de detección, sumando los pixeles de cada región que pueden ser calculados como positivos y negativos. Si todos los clasificadores dan como resultado positivo se considera una coincidencia al detectar un rostro. (Real Python, 2020)

Figura 4

Extracción de imágenes – Método Viola-Jones



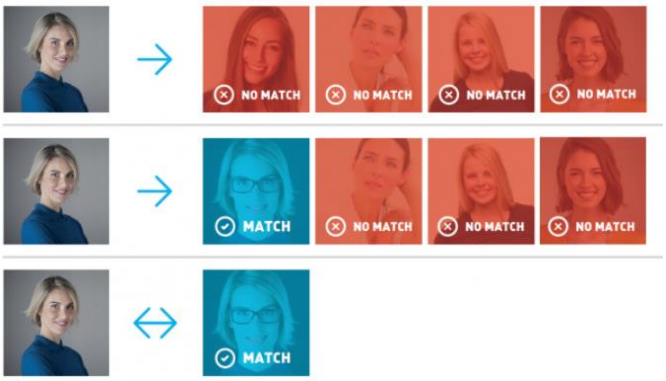
Nota: La figura muestra los tipos de caracteres del método de Viola-Jones. (Reconocimiento facial mediante el Análisis de Componentes Principales, 2017).

2.3.4 Reconocimiento.

Para la última fase se compara toda la información recopilada para obtener un porcentaje de similitud del rostro detectado e identificarlo. En esta etapa se verifica todos los patrones obtenidos con una plantilla anteriormente establecida en el sistema, clasificando las características del rostro y encontrando las similitudes para identificarlo, una vez obtenido un porcentaje mayor de similitud toma la decisión el sistema e identifica a la persona, como se evidencia en la figura 5. (Gavilán, 2020)

Figura 5

Reconocimiento de rostros



Nota: La figura muestra la verificación de un rostro después de compararlo en una base de datos. (Algoritmos de reconocimiento facial, 2017).

2.4 Raspberry Pi.

Raspberry Pi Foundation (Fundación Raspberry Pi), es una organización benéfica de Reino Unido que trabaja desde el 2009, en la creación de placas de tamaño reducido, impulsando a miles de jóvenes a potenciar la enseñanza de la informática y el mundo digital. A lo largo de los años la Fundación Raspberry ha desarrollado una gran variedad de tarjetas y módulos de enseñanza con un sistema operativo de código abierto mediante un lenguaje de programación Dev C++.

Las placas Raspberry poseen un ordenador completo con tamaños reducidos para llevarlos a cualquier lado, actualmente son los productos más vendidos a nivel mundial. Son un sin número de tareas que puede realizarse como reproducción de video, desarrollo de videojuegos, modificación de archivos, entre otros. Al igual que su placa tiene una gran capacidad de conectar componentes extras para funcionar como un mini computador.

2.4.1 Raspberry Pi 3 Modelo B+

La Raspberry Pi 3 Modelo B+, es un pequeño ordenador con múltiples funciones, que, a mejorado su diseño y sus funciones en consideración a versiones anteriores, este mini computador de bajo costo fue desarrollado con el objetivo de estimular la enseñanza de la programación. Esta placa posee muchas características especiales que la hacen una herramienta muy útil al momento de elaborar proyectos o programar. Esta placa disponible desde el 2014 utiliza el mismo procesador a sus placas anteriores, pero con algunas mejoras como la mayor capacidad de conectividad con redes inalámbricas, más puertos USB, como se puede observar en la figura 6 y se evidencia en su hoja técnica del anexo C.

En la tabla 3 se puede observar algunas de sus características:

Tabla 3

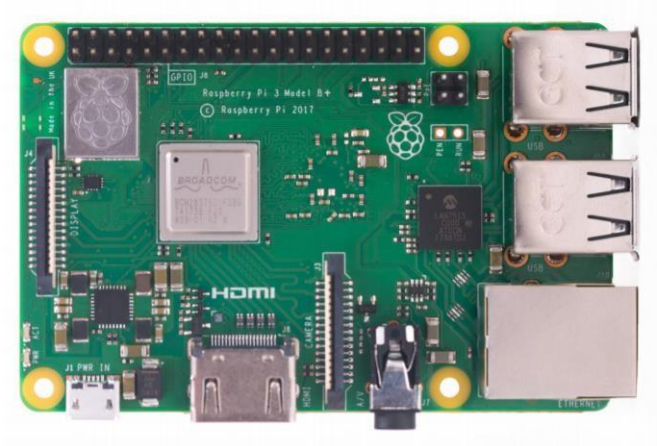
Características Raspberry Pi 3 Modelo B+

ESPECIFICACIONES	CARACTERÍSTICAS
Procesador	Broadcom BCM2837B0 DE 64 bits a 1,4 GHz
Red	LAN inalámbrica, bluetooth 4.2
Puertos	4 puertos USB 1 puerto HDMI 1 puerto de cámara 1 puerto para pantalla
Pines	40 pines GPIO
Alimentación	5V / 2,5 A CC
Memoria	Micro SD

Nota: La tabla muestra las características específicas de tarjeta. (Datasheet Raspberry Pi 3, 2020).

Figura 6

Tarjeta Raspberry Pi 3 Modelo B+



Nota: La imagen muestra la tarjeta física de la Raspberry Pi 3 B+. (Datasheet Raspberry Pi 3, 2020).

2.4.2 Ventajas.

Debido a sus especificaciones con grandes beneficios la Raspberry PI posee muchas ventajas en informática y programación:

- Hardware listo para usar sin necesidad de instalaciones extras.
- Componentes necesarios como un miniordenador.
- Posee una plataforma de programación.
- El coste de la placa es accesible.
- Capacidad amplia y potente.
- Su software es de código abierto.

2.4.3 Funcionamiento y Usos.

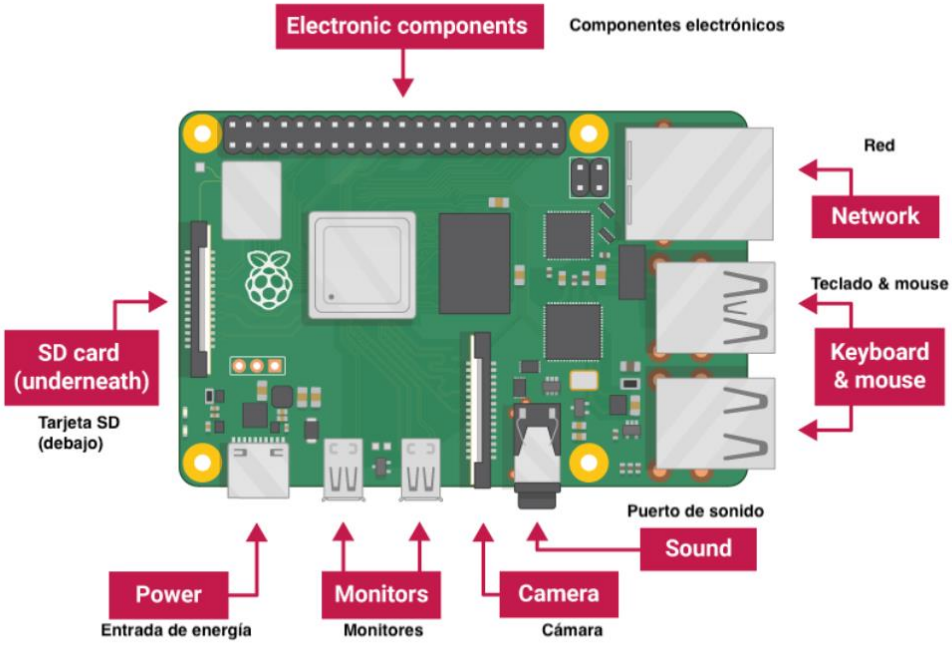
La tarjeta Raspberry Pi al ser un mini ordenado trabaja mediante un sistema operativo compatible llamado Raspbian, el cual permitirá un entorno muy amigable y nada complejo. Este sistema permite ingresar a todas las funciones y aplicaciones que la tarjeta dispone. Además, la Raspberry Pi posee funciones externas que facilitan su uso como se observa en la figura 7 y se especifica a continuación:

- **Puerto USB:** pueden ser utilizados para conectar teclado y mouse u otros componentes con unidad USB.
- **Ranura de tarjeta SD:** el sistema de almacenamiento se basa en una micro SD, donde ira instalada el sistema operativo y se podrá guardar todos los archivos realizados.
- **Puerto Ethernet:** se utiliza para conectar a una red con cable a la tarjeta, pero también puede ser conectada mediante una red LAM inalámbrica una vez ingresado al sistema e incorporar la red Wifi.
- **Salida de audio:** apto para auriculares y altavoces.

- **Puerto HDMI:** se conecta el monitor o pantalla para la interacción y control de la tarjeta.
- **Alimentación micro USB:** se conecta una fuente de alimentación compatible con los valores establecidos por el fabricante normalmente son de 5V a 2,5 A.
- **Puertos GPIO:** estos 40 pines permiten la conexión de componentes electrónicos externos para proyectos y poseen dos pines de salida de voltaje de 3.3V y 5V.

Figura 7

Partes de la Raspberry Pi



Nota: La figura muestra las partes de la tarjeta Raspberry Pi en general. (Página Oficial Raspberry Pi Fundation, 2021).

2.5 Cámara.

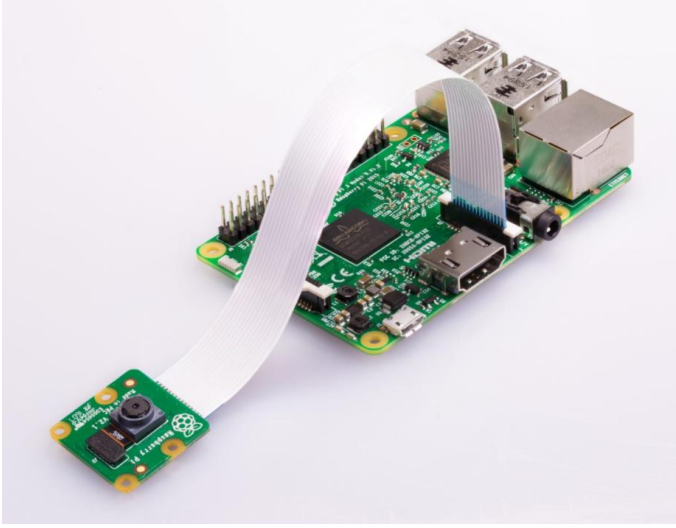
La cámara para la tarjeta Raspberry Pi es un modelo capaz de tomar fotografías en alta resolución y videos HD 1080p, posee un cable flexible para ser insertado en la tarjeta, existen dos versiones del módulo de la cámara:

- **Versión estándar:** está diseñada para fotografía con luz normal
- **Versión NoIR:** no contiene filtros infrarrojos, puede ser ocupada en la oscuridad con luces externas infrarrojas.

La cámara ofrece una reducción de ruido y borrones debido a las funciones de control de exposición, detención de luminosidad y balance de blancos. Además, es compatible con el sistema operativo Raspbian para ser controlado mediante programación y es de fácil colocación mediante una ranura que permite conectar la cámara con la tarjeta mediante un cable de datos como se muestra en la figura 8.

Figura 8

Cámara para Raspberry Pi



Nota: La figura muestra el módulo de la cámara Raspberry. (Página Oficial Raspberry Pi Fundation, 2021)

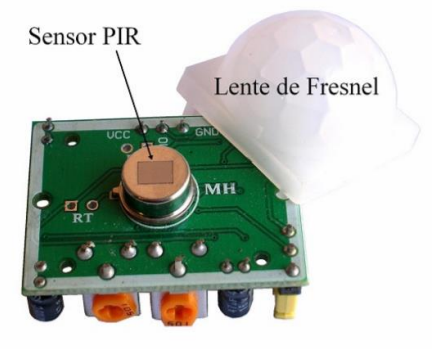
2.6 Sensor de movimiento

Un sensor de movimiento es un dispositivo electrónico que está compuesto por elementos receptores y emisores de señales que reaccionan a un movimiento físico en un área determinada. (Grupo Legrand, 2020)

Su principio de funcionamiento se basa en dos elementos: el sensor PIR o sensor infrarrojo pasivo el cual detecta la radiación electromagnética infrarroja de personas u objetos debido a su temperatura y el lente de Fresnel que permite el paso de la radiación infrarroja para ser encapsulada en la superficie del sensor permitiendo mayor sensibilidad del dispositivo. Dos elementos que conforman el sensor de movimiento como se muestra en la figura 9.

Figura 9

Elementos del Sensor de movimiento

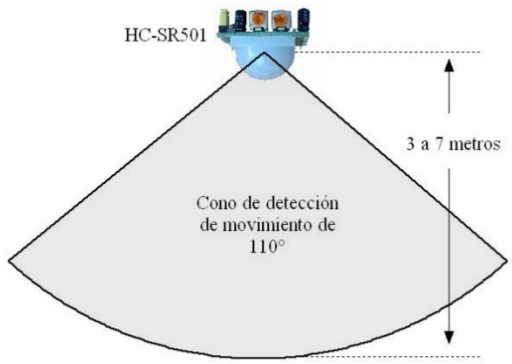


Nota: La figura muestra dos elementos principales que conforma el sensor PIR para la detección de movimiento. (Manual de usuario Sensor de movimiento PIR, 2017)

Los sensores cuentan con un sistema ON/OFF automático que optimiza el consumo y eficiencia energética. Además, posee dos potenciómetros para modificar los parámetros de tiempo de disparo de la señal y la distancia de detección, este posee un rango de 3 a 7 metros de distancia con un ángulo de 90° a 110° como se muestra en la figura 10.

Figura 10

Rango y ángulo de detección



Nota: La figura muestra el rango y ángulo en que trabaja el sensor PIR. (Manual de usuario sensor de movimiento PIR, 2017)

Algunas de sus especificaciones técnicas se mencionan en la tabla 4.

Tabla 4

Especificaciones Técnicas Sensor PIR

ESPECIFICACIONES	**VALORES**
Voltaje	5 a 12 VDC
Corriente	1 mA
Rango de distancia	3 a 7 metros ajustable
Ángulo de detección	110°
Salida de alarma (tiempo)	3 segundos a 5 minutos ajustable
Temperatura de operación	-15° a + 70° C
Dimensiones	3.2 x 2.4 x 1.8 cm

Nota: La tabla muestra las especificaciones técnicas del sensor de movimiento. (Manual de usuario sensor de movimiento PIR, 2017)

2.7 Buzzer o Zumbador

Un buzzer o zumbador es un transductor que convierte la energía eléctrica o una señal en sonido, su funcionamiento se basa en el efecto piezoeléctrico y puede alcanzar los 80dB(decibeles) de su nivel sonoro. Se utiliza comúnmente para la elaboración de alarmas, computadores, electrodomésticos, alarmas de automóviles, entre otros dispositivos. (UNIT, Electronics, 2021)

Algunas de sus características se videncia en la tabla 5.

Tabla 5

Características del Buzzer

Especificaciones	**Características**
Voltaje	5V DC
Corriente	30mA
Dimensiones	12mm x 9.5mm
Frecuencia de resonancia	23k Hz
Salida de sonido	85 dB
Temperatura de trabajo	-20°c a 70°C
Pines	VCC y GND

Nota: La tabla muestra las especificaciones técnicas del Buzzer o Zumbador. (Datasheet Buzzer Activo, 2021)

Existen dos tipos de Buzzer Activo y Pasivo, un Buzzer activo posee su propia frecuencia y le permite generar un sonido o pitido cuando se enciende. Un Buzzer pasivo no posee una frecuencia propia debe ser colocada a la frecuencia sonora deseada, es como un parlante con impedancia alta. Para el proyecto se utilizará un zumbador activo como se muestra en la figura 11, facilitando las conexiones.

Figura 11

Buzzer o Zumbador

Nota: La figura muestra la forma física del Buzzer o Zumbador que se utilizará en el proyecto. (UNIT Electronics, 2021)

2.8 Software OPENCV - PYTHON

OpenCV es una biblioteca de software de visión artificial y aprendizaje automático de código abierto, creado para aportar una infraestructura de visión por computadora fácil de programar. Posee una licencia BSD el cual puede ser utilizado por empresas y modificar su código, posee una amplia biblioteca de algoritmos optimizados de última generación y clásicos que pueden ser ocupados para la detección y reconocimiento de rostros, identificación de objetos, clasificación de personas, rastreo de movimiento, etc. Posee interfaces de C++, Python, Java y MATLAB, siendo compatible con Windows, Android, Linux y Mac OS. (OpenCV,2021)

Por otro lado, Python es un lenguaje de programación con un enfoque no definido, lanzado en el 2000 por Guido Van Rossum, programador holandés, este tipo de lenguaje posee una sintaxis muy legible y fácil de entender, está desarrollado con una licencia de Open source, es decir, de código abierto por lo que se puede utilizar libremente.

Algunas de sus características son:

- Utiliza una sintaxis de fácil lectura y escritura.
- Es ideal para el desarrollo de prototipos y otras tareas de programación.
- Posee una gran biblioteca de códigos.
- Se ejecuta en cualquier sistema: Windows, Mac OS, Linux, Unix, Android y iOS.
- El software es libre.
- Es interpretado y multiplataforma.
- Puede ejecutarse en distintos sistemas operativos y plataformas, sin necesidad de cambiar el código original.
- Incluye una serie de librerías con estructuras de datos de alto nivel.

2.9 Funcionamiento.

Python al ser multiplataforma y multiparadigma es muy versátil para la elaboración de diversos proyectos ya sean para la web o de inteligencia artificial. De la misma forma OpenCV es una herramienta muy útil al momento de realizar el reconocimiento facial con una amplia biblioteca o librerías de visión por computadora, permitiendo el análisis de la imagen mediante algoritmos para la identificación y el reconocimiento. Es por ello que las dos herramientas se complementaran para la elaboración del sistema de seguridad, OpenCV ofrece librerías Haar, que clasifican los rostros y obtiene una serie de suma de pixeles para la identificación de la persona u objeto, siendo programado desde la plataforma de Python.

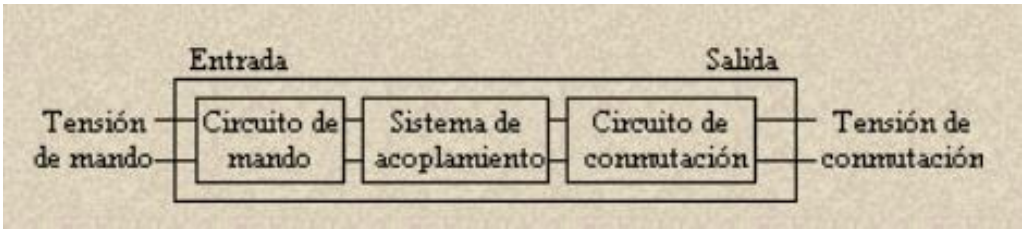
2.10 Relé

El relé puede ser definido como un interruptor eléctrico que permite el paso de la corriente mediante accionamiento eléctrico. Este permite abrir o cerrar contactos mediante electroimanes para activar un circuito de consumo considerable de electricidad con una potencia de 12 o 24 voltios. (SEAS, 2019).

El relé está compuesto de una bobina que produce un campo electromagnético para el contacto del relé que normalmente está abierto y al cerrarse permite el paso de la corriente, su estructura es cómoda y pequeña como se muestra en la figura 12. Para comprender su funcionamiento se puede interpretar mediante 3 bloques como se muestra en la figura 11, la etapa 1 está compuesto por el circuito de entrada o de control, la etapa 2 por un circuito de acoplamiento y la etapa 3 por el circuito de salida o carga.

Figura 12

Estructura del Relé



Nota: La figura muestra la estructura de un relé. (Peña & Montejo, 2018).

Algunas características generales son:

- Un aislamiento entre los terminales de entrada y salida.
- Soporta sobrecargas.
- Puede controlar circuitos de alto consumo con una débil señal eléctrica.
- Pueden prevenir daños en equipos detectando anormalidades eléctricas.

- Se pueden utilizar para la selección de circuitos cuando existe más de un circuito.
- Son ocupados para reducir el ruido eléctrico.

2.10.1 Tipos de relé

Existen diferentes tipos de relés:

- Electromecánicos, tienen variantes según el mecanismo de activación, ya sean de tipo armadura, polarizados, núcleo móvil, tripolares.
- De corriente alterna.
- Estado sólido, precisa una mayor velocidad en la conmutación.
- Térmicos, para la protección de sobrecargas.
- Temporizador o acción retardada, cumplen su activación de desconexión después del tiempo determinado.

Figura 13

Estructura física del Relé

Nota: La figura muestra la estructura física de un relé. (SEAS, 2019)

2.11 Cerradura solenoide

Esta cerradura está compuesta por solenoides que básicamente son electroimanes, este mecanismo de bloqueo de puerta está diseñado por una bobina de alambre de cobre con una armadura de metal en el medio, al ser energizada esa bobina tiene la capacidad de tirar de un extremo permitiendo el desbloqueo de la puerta y al retirar la energía el bloqueo de la misma, como se muestra en la figura 14 y sus dimensiones y especificaciones técnicas en el Anexo E.

Es aplicado de 9 a 12VDC, mediante una fuente de alimentación externa y que este sobre los 500mA, algunas de sus características son:

- Se activa de 1 a 10 segundos.
- Consume 650mA a 12V y 500mA a 9V.

Figura 14

Cerradura Solenoide

Nota: La figura muestra el físico de la cerradura solenoide de 12V. (Electronilab, 2019).

CAPITULO III

3. Desarrollo e implementación del proyecto

3.1 Implementación del proyecto.

El proyecto se basa en el desarrollo de un sistema en cascada para el reconocimiento facial de uno o más usuarios, que permitirá el acceso a la vivienda con la activación de una cerradura eléctrica. Para el desarrollo de este sistema se necesitan varias herramientas de software y hardware que ayudarán a lograr los objetivos planteados, la figura 15 muestra los dispositivos principales del sistema, así como las conexiones de los elementos electrónicos.

Las herramientas de hardware deben ajustarse a las condiciones que requiere el sistema y cumplan con las características necesarias, estas son:

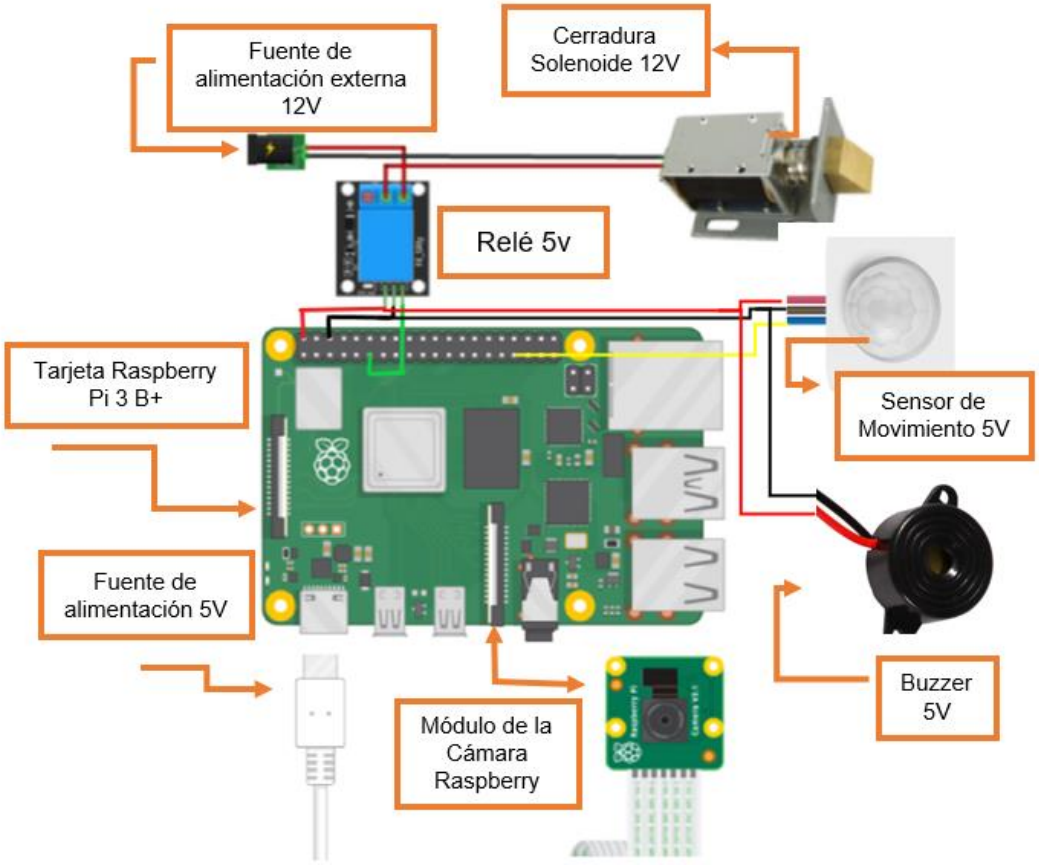
- Placa de desarrollo Raspberry Pi modelo 3 B+.
- Cámara Raspberry Pi versión 1.3 compatible con la placa.
- Relé de 5V para la activación de la cerradura.
- Cerradura solenoide de 12V.
- Zumbador o Buzzer de 5V.
- Sensor de movimiento PIR.

Las herramientas de software serán utilizadas para la creación del programa, estas herramientas debes ser compatibles con la placa Raspberry Pi, estas son:

- Sistema operativo Raspbian para Raspberry Pi.
- Lenguaje de programación Python 3.7.3
- Algoritmos de OpenCV versión 4.1.0
- Técnicas de reconocimiento facial Viola-Jones.
- Clasificador Haard Cascada.

Figura 15

Elementos del proyecto

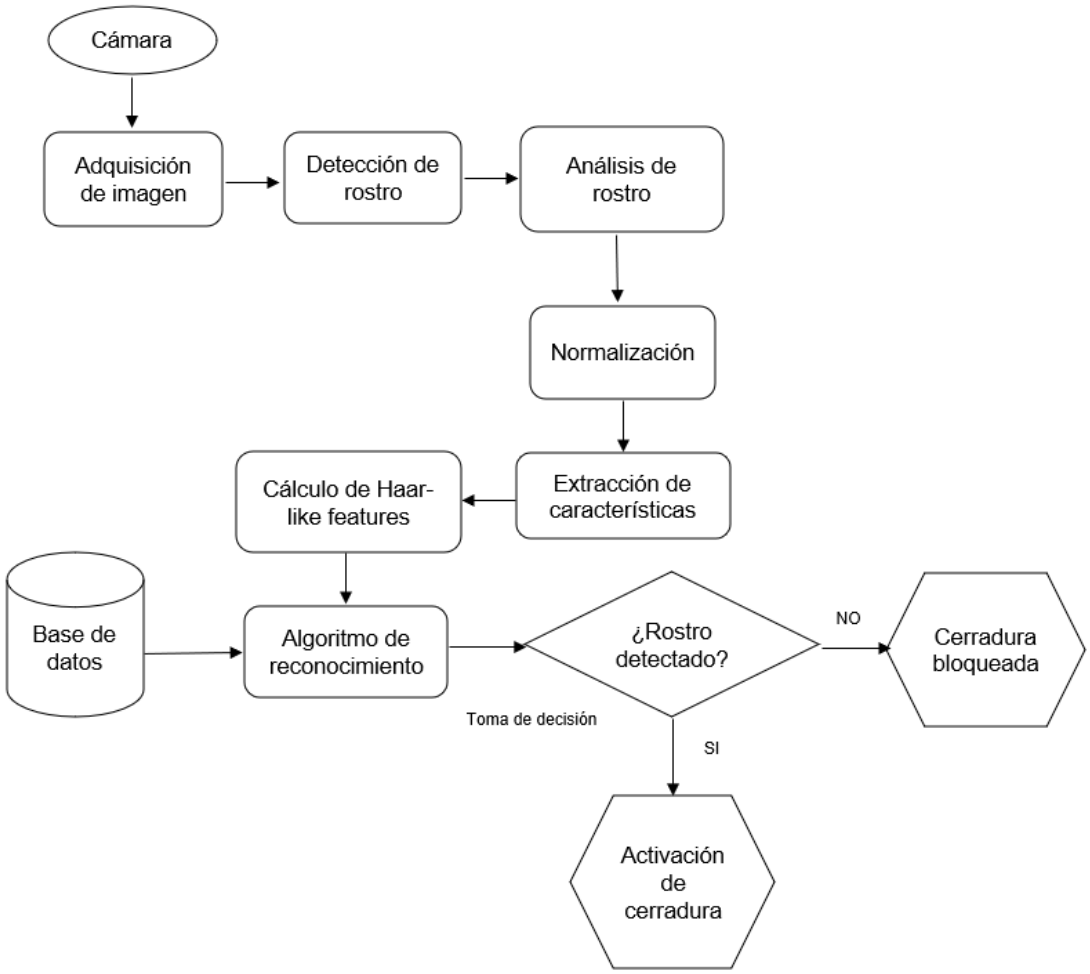


Nota: Los elementos ocupados son compatibles con la tarjeta de desarrollo Raspberry Pi y se alimentan de una fuente de 5V para la tarjeta Raspberry y 12V para la cerradura solenoide, el resto de elementos se alimentan desde los puertos GPIO de 5V.

El proyecto cumple con una serie de etapas para lograr el reconocimiento facial esto se puede explicar mediante un diagrama de flujo que la figura 16, muestra las diferentes etapas que se involucran en el sistema de detección y reconocimiento de rostros.

Figura 16

Diagrama de flujo Sistema de Reconocimiento Facial



Nota: El reconocimiento facial requiere de una serie de pasos indispensables para lograr su correcto funcionamiento.

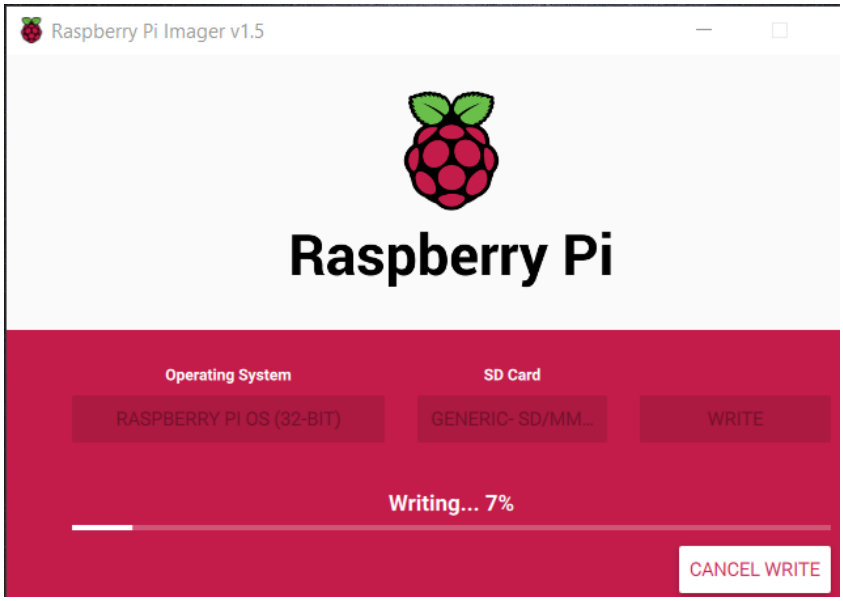
3.1.1 Instalación de Software

Descrito los requerimientos para el proyecto la placa Raspberry Pi3 B+ requiere de un sistema operativo que permita el funcionamiento de la misma, el sistema que se instaló es Raspberry Pi OS anteriormente llamado Raspbian que es el sistema operativo oficial compatible de la tarjeta, contiene los programas de educación ya preinstalados y de uso general como son Python, Java, entre otros.

Raspbian es la distribución de Linux y sistema operativo oficial de la Raspberry Pi, su uso es educativo o comercial gratuito. Para su instalación se requiere de una tarjeta micro SD mayor a 8GB para almacenar todos los programas a utilizar, en el caso del proyecto se utilizó una micro SD de 16GB donde se descargó el sistema operativo que ofrece la página oficial de Raspberry Pi, este puede ser instalado manualmente o por Raspberry Pi Imager que es un instalador de todas las distribuciones de sistemas operativos para Raspberry Pi como se muestra en la figura 17.

Figura 17

Instalación del Sistema Operativo Raspberry Pi OS



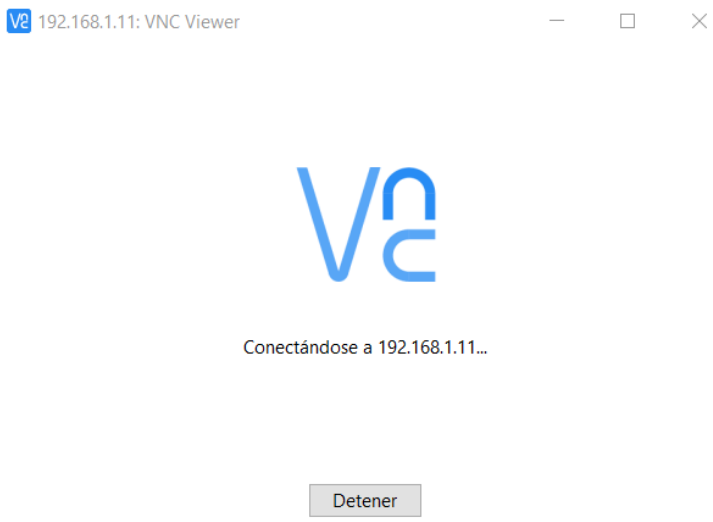
Nota: Instalación del sistema operativo Raspberry Pi OS en la tarjeta micro SD, mediante el programa Raspberry Pi Imager que se encarga de instalar los sistemas operativos para las placas Raspberry Pi.

Una vez instalado el sistema operativo en la tarjeta de memoria se procede a insertar en la ranura de la Raspberry la micro SD, se conecta un cable Ethernet al modem de Internet para facilitar la conexión de la placa y obtener la dirección IP de la misma y una alimentación de 5V a 2.5 A.

El arranque de la placa se lo realizó vía remota mediante el programa VNC Viewer como se muestra en la figura 18, el cual permite controlar la tarjeta Raspberry Pi de forma remota desde cualquier computador con la dirección IP proporcionada por el Modem de internet.

Figura 18

Conexión remota de Raspberry Pi

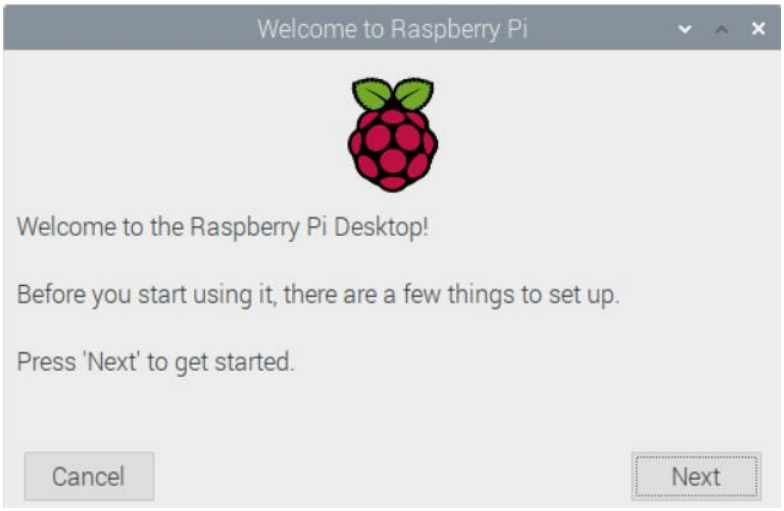


Nota: la conexión remota de la Raspberry Pi se realiza mediante el programa VNC Viewer con la dirección IP que proporciona la tarjeta.

Después de conectarse con el sistema remoto de la placa se procedió con las configuraciones automáticas como se muestra en la figura 19, el cual inician automáticamente en la tarjeta como: idioma, conexiones wifi, contraseñas, actualización de software, entre otros.

Figura 19

Configuración de inicio de la Raspberry Pi



Nota: Configuración inicial de la Raspberry Pi, una vez terminada toda la configuración se reinicia y está lista para usarse.

3.1.2 Herramientas de software Python - OpenCV

Dado los requerimientos del proyecto con respecto al software y las aplicaciones a usar el proyecto está enfocado en un software libre (Open Source), debido a los costos elevados para la adquisición de un software del mercado. Este también debe ser compatible con la placa de desarrollo que se va a utilizar, por esta razón el software de programación que se utilizó es Python, debido a que en la actualidad es una plataforma de programación muy popular y de fácil manejo. Además, al ser un lenguaje de programación gratuito, de código abierto y multiplataforma, está disponible para diversos sistemas y no permite vulneraciones en los trabajos realizados por el programador.

Además, para el reconocimiento facial se ha utilizado las herramientas de OpenCV, debido a que posee una gran biblioteca o librerías de visión artificial,

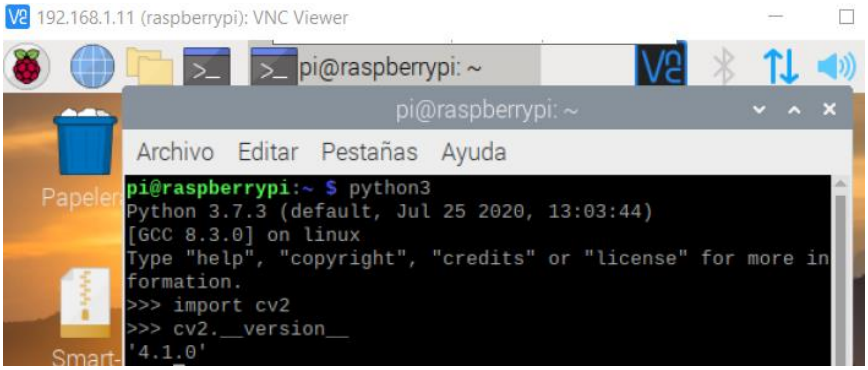
permitiendo el análisis de rostros e imágenes mediante algoritmos de identificación y reconocedor de objetos.

3.1.3 Código de programación.

Para la programación se utilizó dos programas con versiones compatibles con el reconocimiento facial y la Raspberry Pi que no proporcionen errores al realizar la detección y reconocimiento de rostros, estos son Python 3.7.3 y OpenCV 4.1.0, estas versiones han sido mejoradas en sus clasificadores y librerías que comparten al momento de identificar rostros. Mediante el símbolo del sistema de la Raspberry Pi fueron instalados los dos programas mediante comando de programación como se muestra en la figura 20, posteriormente se puede iniciar con la programación de reconocimiento facial.

Figura 20

Programas compatibles con el reconocimiento facial



Nota: Las versiones de Python y OpenCV son importantes para no encontrar errores al momento de programar la tarjeta.

Además, mediante la Raspberry se habilitó los pines que serán utilizados para alimentar y activar el circuito llamados GPIO y se habilitó la cámara que permitirá capturar los rostros para ser identificados como se demuestra en la figura 21.

Figura 21

Habilitación de pines GPIO

Nota: Se habilitó de los pines GPIO mediante la configuración de la Raspberry los cuales permitirán la activación de los puertos que serán programados.

3.1.4.1 Almacenamiento de datos y rostros.

Para el inicio del reconocimiento de rostros se debe recopilar una serie de imágenes capturadas por la cámara Raspberry Pi, las mismas que serán almacenadas en la base de datos de la placa, cada una con una carpeta que llevará su nombre, el código de Python tomará 30 fotos de cada persona que se desea identificar y este realizará el proceso de detección y reconocimiento mediante un clasificador ya pre entrenado de OpenCV.

El proyecto cuenta con 4 programaciones para la detección facial y la alerta de alarma cuando registra un movimiento el sensor PIR. Se inició con el primer código de recopilación de datos, donde se importó los paquetes de almacenamiento de rostros y datos, como la librería de la cámara y las librerías de los clasificadores, los cuales son evidenciados en la figura 22.

Figura 22

Declaración de librerías

```
1  import cv2
2  from picamera.array import PiRGBArray
3  from picamera import PiCamera
4  import numpy as np
5  import os
6  import sys
7
```

Nota: Se importó las librerías que perimirán la activación de la cámara, la clasificación de rostros mediante PiRGBArray y matrices NumPy.

Las siguientes líneas determinaron la resolución de la cámara en 640,480 y la velocidad de las fotografías en 30fps (fotogramas por segundo) como se evidencia en la figura 23. Así mismo se determinó un PiRGArray proporcionando una matriz tridimensional organizada a partir de las capturas tomadas, también se declaró el archivo cascada que permitió obtener las características de cada usuario. Automáticamente el programa crea una carpeta con el nombre del usuario donde se guardará las fotografías que la cámara capturará en el directorio que se asignó para el programa.

Figura 23

Cámara y archivo cascada

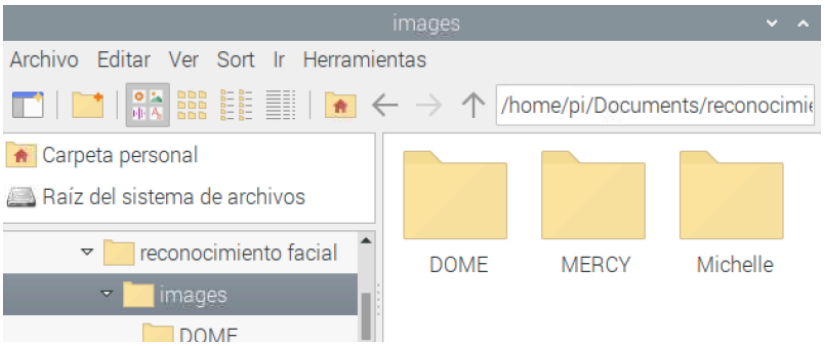
```
 9  camera.resolution = (640, 480)
10  camera.framerate = 30
11  rawCapture = PiRGBArray(camera, size=(640, 480))
12
13  faceCascade = cv2.CascadeClassifier("haarcascade_frontal
14
15  name = input("What's his/her Name? ")
16  dirName = "./images/" + name
17  print(dirName)
```

Nota: El archivo cascada contiene una base de datos pre – entrenados que mediante el algoritmo Viola-Jones, detecta los rasgos faciales de los usuarios permitiendo una mayor eficacia en la comparación de rasgos faciales.

Estas imágenes son trasformadas a escala de grises mediante la matriz NumPy que las clasifica y guarda los rasgos y datos de las personas. Cada imagen que es capturada se refleja en un cuadro de color verde cuando es detectado un rasgo facial ya identificado de la persona y recorta el rostro a coordenadas rectangulares para extraer la imagen y guardarla en la carpeta ya creada con el nombre del usuario como se muestra en la figura 24, para el proyecto se guardará las imágenes de 3 usuarios que frecuentan la vivienda.

Figura 24

Carpeta de usuarios



Nota: Cada carpeta creada guarda las imágenes de los usuarios con diferentes capturas para detectarlos posteriormente.

3.1.4.2 Entrenador del reconocimiento.

Una vez recopilado los rostros de los usuarios se procedió a entrenar el reconocedor de rostros para establecer una relación entre el usuario y las imágenes guardadas, en esta etapa los clasificadores recopilan toda la información para guardar en su base de datos el número de usuarios y sus características. Para lo cual OpenCV posee la librería LBPH (Histograma de patrones binarios locales), el cual permitirá la comparación de datos y describir las texturas de las imágenes en escala de grises, para realizar la comparación de rasgos faciales de manera óptima, esto se puede evidenciar en la figura 25.

Figura 25

Librería LBPH

```
7  faceCascade = cv2.CascadeClassifier("haarcascade_frontal
8  recognizer = cv2.face.LBPHFaceRecognizer_create()
9
10 baseDir = os.path.dirname(os.path.abspath(__file__))
11 imageDir = os.path.join(baseDir, "images")
```

Nota: Las líneas 7 y 8 cargaran los clasificadores para entrenar al reconocedor.

El programa se redirecciona a cada carpeta de los usuarios para crear una matriz NumPy y clasificar por rasgos a cada persona, esto se declaró en las siguientes líneas de la figura 26.

Figura 26

Matriz NumPy

```
20     for file in files:
21         print(file)
22         if file.endswith("png") or file.endswith("jpg"):
23             path = os.path.join(root, file)
24             label = os.path.basename(root)
25             print(label)
26
27             if not label in labelIds:
28                 labelIds[label] = currentId
29                 print(labelIds)
30                 currentId += 1
31
32             id_ = labelIds[label]
33             pilImage = Image.open(path).convert("L")
34             imageArray = np.array(pilImage, "uint8")
35             faces = faceCascade.detectMultiScale(imageArray, scaleFactor=1.1,
36
```

Nota: la librería NumPy realiza cálculos mediante las matrices creadas para la identificación de rostros.

Una vez culminado las matrices el programa crea un documento trainer.yml que está encargado de etiquetar con el nombre del usuario a la persona que está viendo con el fin de decidir si coincide o no la persona registrada en la base de datos esto es declarado en las líneas de la figura 27.

Figura 27

Detección final

```
41
42 with open("labels", "wb") as f:
43     pickle.dump(labelIds, f)
44     f.close()
45
46 recognizer.train(xTrain, np.array(yLabels))
47 recognizer.save("trainer.yml")
48 print(labelIds)
```

Nota: Las líneas 37 a 40 se asegurarán que la persona frente a la cámara sea la misma de los archivos guardados, las líneas 42-44 etiqueta con el nombre del usuario al momento de reconocer a la persona y las líneas 46-48 guarda todos los registros.

3.1.4.3 Reconocimiento de rostros.

Para la siguiente etapa el reconocedor de rostros deberá detectar al usuario para activar los pines GPIO y así encender el relé, si este coincide se activará la cerradura, para ello en las primeras líneas que se muestra en la figura 28, se declaró las librerías que se ocuparan para activar la cámara, el reconocedor ya pre - entrenado y los pines GPIO que activaran el circuito externo.

Figura 28

Librerías GPIO

reconocimiento.py | entrenador.py | detector.py

```
1 import cv2
2 from picamera.array import PiRGBArray
3 from picamera import PiCamera
4 import numpy as np
5 import pickle
6 import RPi.GPIO as GPIO
7 from time import sleep
8
```

Nota: Se importó todas las librerías requeridas para la activación del circuito.

Las siguientes líneas de la figura 29, fueron declaradas para crear un archivo pickle el cual contiene todos los usuarios registrados y el clasificador que detectara las caras. Además, se cargó el clasificador Haar cascade para la detección y datos ya entrenados.

Figura 29

Archivos registrados

```
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")
```

Nota: Las líneas escritas permitirán iniciar el reconocedor con los usuarios ya registrados.

Para que el programa empiece a detectar rostros ya registrados debe tener un porcentaje de similitud para la activación de la cerradura el cual se evidencia en la figura 30, se declaró que si este porcentaje es mayor al 70% los pines GPIO se activaran y la puerta se abrirá caso contrario permanecerá cerrado y no permitirá el ingreso al domicilio.

Figura 30

Porcentaje de similitud

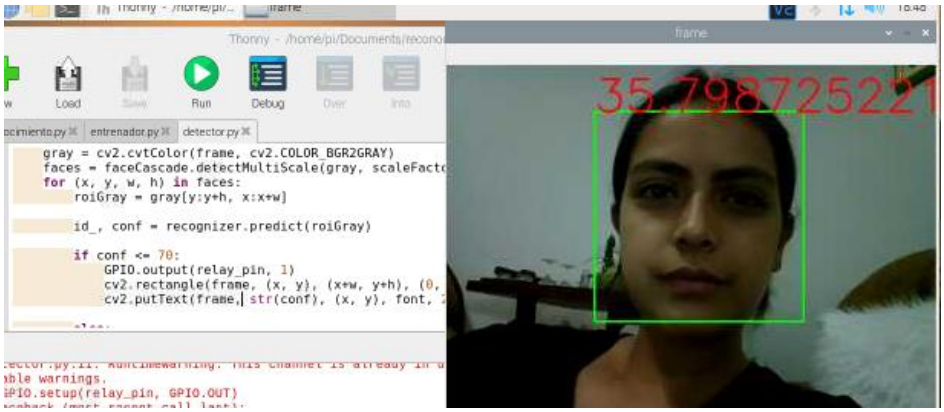
```
                print(name)

        if conf <= 70:
            GPIO.output(relay_pin, 1)
            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.

        else:
            GPIO.output(relay_pin, 0)
```

Nota: Las últimas líneas permitirán la activación de los pines GPIO para encender la cerradura.

Una vez terminado el código, el entrenador muestra en la pantalla el rostro de los usuarios que estén frente la cámara, marcando con un cuadro de color verde como se muestra en la figura 31, que significa que, a encontrado el rostro y los segundos tardados en detectar al usuario, una vez detectado el rostro se identificará al usuario y la cerradura se activará mediante los pines GPIO ya conectados a la cerradura y al relé, permitiendo el ingreso del usuario.

Figura 31

Detección de rostro

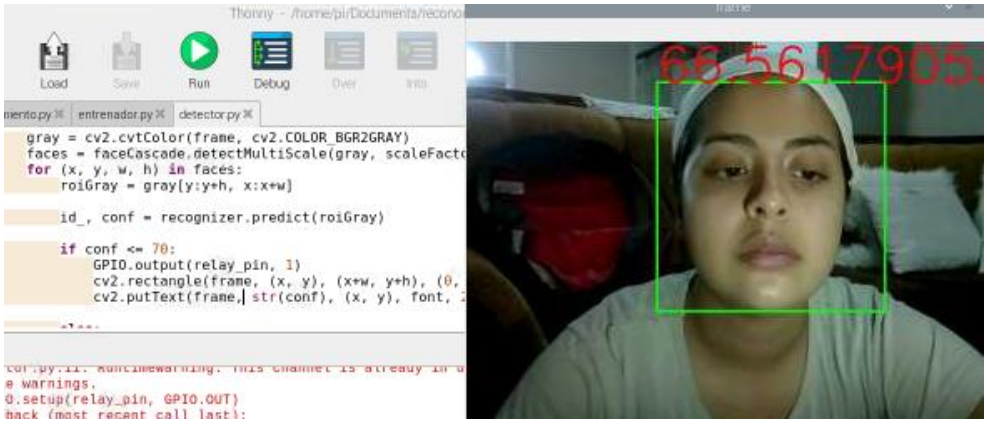


Nota: La figura muestra el rostro detectado del usuario 1 de la vivienda en un recuadro de color verde y el tiempo que se demoró en reconocerlo.

En la figura 32 se puede observar al usuario número 2 con más intensidad de luz detectando su rostro y el tiempo que se demoró, la nitidez de las fotografías, la calidad de la cámara tiene un valor muy importante para que el tiempo se acorte al momento de detectar un rostro, no obstante, existen más factores para menorar el tiempo de detección como el número de veces que el usuario interactúa con la cámara.

Figura 32

Detección usuario 2

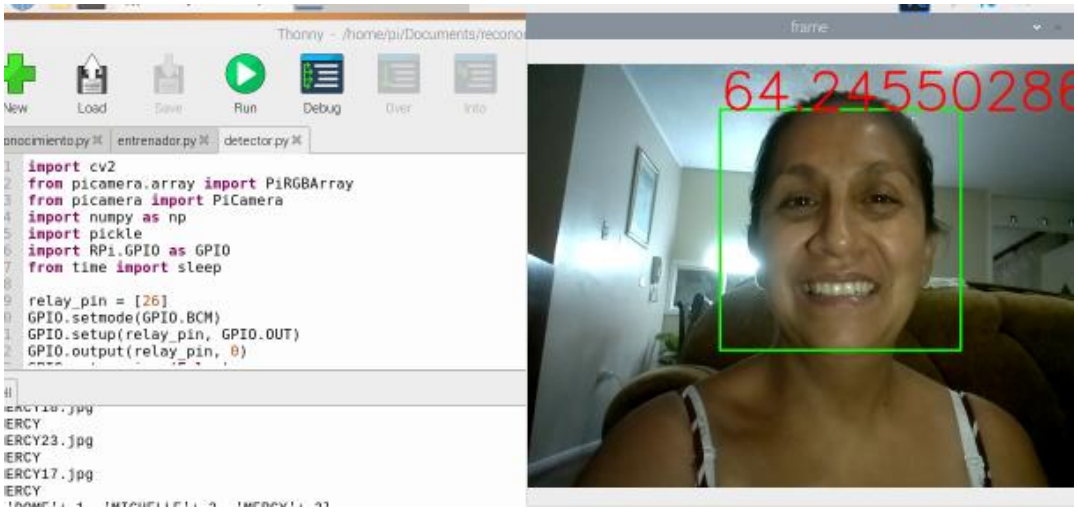


Nota: La figura muestra al usuario número 2 detectado por la cámara Raspberry y el tiempo que se demoró en ser detectado.

De la misma forma se realizó el reconocimiento facial del usuario numero 3 mostrado en la figura 33.

Figura 33

Detección usuario 3



Nota: La figura muestra la detección del usuario número 3 y como los anteriores registros lo enmarca en color verde con el tiempo que tardo en detectarlo.

Una vez culminada la programación de detección y reconocimiento facial se añadió la seguridad del sistema que permitirá estar informado de las personas que ingresan o se acercan a la puerta principal, mediante un sensor de movimiento PIR y el envío de imágenes por correo electrónico se puede desarrollar la seguridad del sistema de reconocimiento facial.

Para la detección de movimiento en la puerta del domicilio, es necesario añadir unas líneas de programación en el código de detección facial para que se ejecute el sensor PIR antes del reconocimiento facial como se muestra en la figura 34.

Figura 34

Líneas de programación del sensor PIR

```
13 toaddr = 'antonelasanchez1997@gmail.com'
14 me = 'tefamichu20@gmail.com'
15 Subject='Alerta de seguridad'
16
17 GPIO.setmode(GPIO.BCM)
18
19 P=PiCamera()
20 P.resolution= (1024,768)
21 P.start_preview()
22
23 GPIO.setup(23, GPIO.IN)
24 while True:
25     if GPIO.input(23):
26         print("Motion...")
27         #camera warm-up time
28         time.sleep(1)
29         P.capture('movement.jpg')
30         time.sleep(4)
31         subject='Alerta de Seguridad!!'
32         msg = MIMEMultipart()
33         msg['Subject'] = subject
```

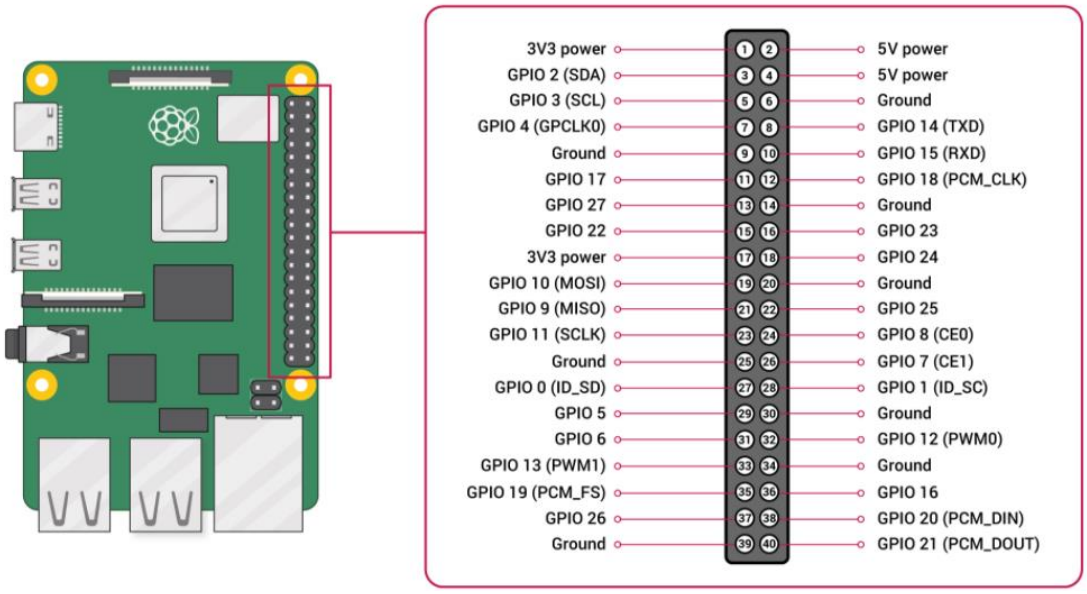
Nota: La figura muestra las líneas utilizadas para la activación del sensor y la cámara la cual tomara una fotografía para ser enviada por correo electrónico.

3.2 Montaje de elementos

Para el montaje del sistema de reconocimiento facial se establecerán los pines GPIO para la salida de la señal. La placa Raspberry Pi 3 B+ posee 40 pines de entrada/salida de propósito general y son evidenciados en la figura 35, la mayoría de los pines GPIO puede designarse en la programación como un pin entrada o salida y usarse para cualquier fin, estas características se evidencian en el Anexo C.

Figura 35

Distribución de pines GPIO

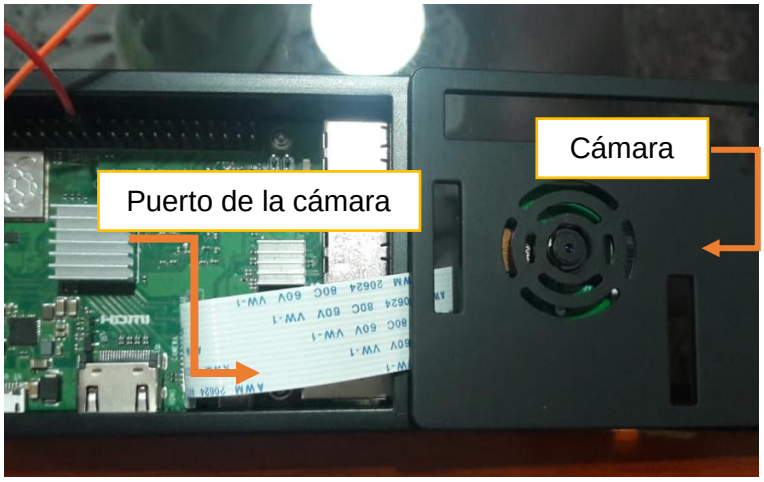


Nota: La figura muestra la distribución de los pines GPIO que la Raspberry Pi 3 B+ posee. (Página Oficial Raspberry Pi Fundation, 2021).

Un elemento primordial para el sistema biométrico es la cámara que detectara los rostros de los usuarios y la tarjeta Raspberry Pi posee un módulo para cámara muy fácil de conectar como se muestra en la figura 36 en el proyecto se utilizó una cámara Raspberry Pi versión 1.2 y sus especificaciones técnicas se evidencian en el Anexo A.

Figura 36

Conexión del módulo de la cámara

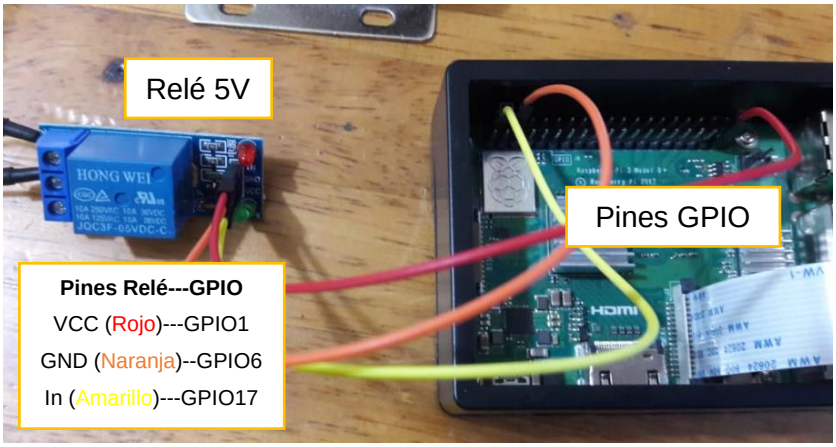


Nota: La figura muestra la conexión del módulo de la cámara en la tarjeta Raspberry Pi.

En la tarjeta se establecieron 3 pines de la placa GPIO para la conexión del relé, como se muestra en la figura 37, el pin GPIO 17 para la salida de la señal, el pin 4 que es VCC para una salida de 5V y el pin 6 que es GND, los tres pines fueron conectados al relé de 5V para activarlo cuando la cámara detecte un rostro conocido.

Figura 37

Conexión de relé con GPIO de Raspberry

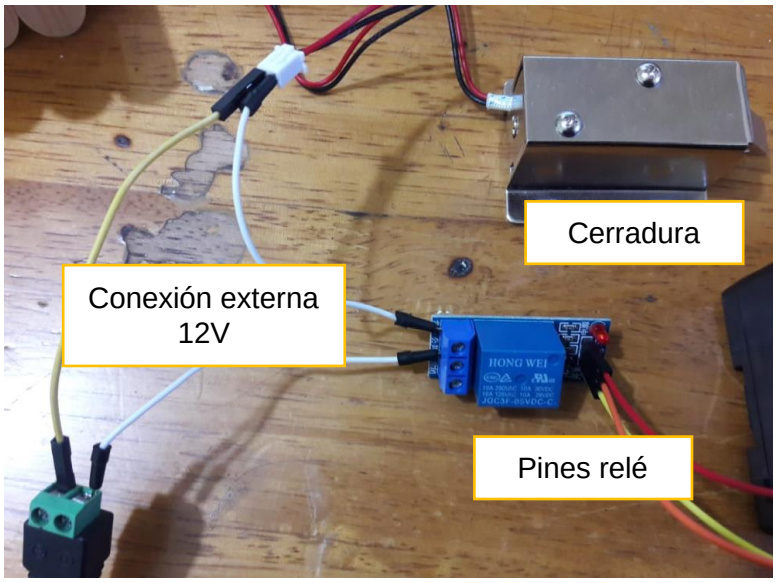


Nota: La imagen muestra la conexión de los pines GPIO de la tarjeta con el relé.

El relé será quien opere la activación o bloqueo de la cerradura solenoide, pero necesita de una fuente para alimentar la cerradura por ello se colocó una fuente externa de alimentación de 12V a 1A para energizar la cerradura, como se muestra en la figura 38. El pin común del relé se conectó con el positivo de la fuente de alimentación externa, el pin normalmente abierto se conectó con el positivo de la cerradura solenoide y el negativo de la fuente de alimentación externa con el negativo de la cerradura.

Figura 38

Conexiones de relé, cerradura y fuente de alimentación externa



Nota: La figura muestra la conexión realizada con el relé, la cerradura y la fuente de alimentación de 12V.

Para el sensor PIR y el Buzzer fueron designados 3 pines de la GPIO para el sensor de movimiento y 2 pines GPIO para él Buzzer, como se muestra en la figura 39, el pin GPIO 23 fue conectado al pin output del sensor de movimiento, el pin GPIO 22 al positivo del Buzzer.

Figura 39

Conexión de Buzzer y Sensor PIR

Nota: La figura muestra la conexión con los pines GPIO al Buzzer y al sensor PIR.

La conexión general de todos los componentes se evidencia en el anexo B, las mismas que fueron colocados en la puerta de ingreso al domicilio, tomando en cuenta la iluminación del lugar y la ubicación de la cámara.

La variación de iluminación es una de las características que más afecta al reconocimiento facial, debido a que es difícil identificar los patrones específicos de los usuarios cuando las tonalidades de piel cambian debido a la luz que se proyecta.

Es por ello que se debe tomar en cuenta algunos aspectos importantes para evitar errores al momento de la identificación, utilizar técnicas eficientes en el sistema como el nivel de gris en la imagen, gradiente para extraer bordes de la imagen en escala de grises y el reflejo facial que permite la estimación de campo.

Teniendo en cuenta estas técnicas se utilizó un algoritmo eficiente que permita visualizar las imágenes de los usuarios de mejor manera, además tener encuentra las variaciones físicas que puede tener los usuarios y que no llegue afectar al

identificador, en caso de haber cambios importantes se deberá actualizar el algoritmo del entrenador como la base de datos.

El lugar cuenta con mucha luz natural por el día lo que facilita una captura de la cámara más precisa y rápida, y por la noche es necesario el cambio de iluminación para un mejor enfoque, como se puede apreciar en la figura 40.

Figura 40

Luz artificial y luz natural en la puerta de ingreso

Nota: La figura muestra los dos tipos de iluminación que cuenta la puerta de ingreso al domicilio la imagen A muestra la luz artificial y la imagen B la luz natural.

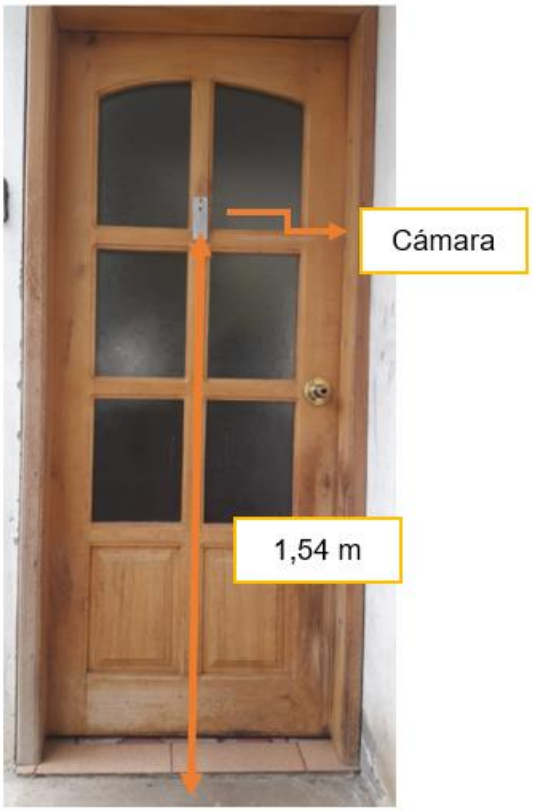
Otro de los principales inconvenientes de los sistemas de reconocimiento facial es la ubicación de la cámara, debido a que las distintas alturas que puede estar expuesta no siempre es el adecuado o no evite el contraste de luz al momento de detectar un rostro, perjudicando a la captura de la imagen, por ellos se establecieron

algunas condiciones ergonómicas que permitan una eficacia a la hora de identificar a los usuarios y bride un mayor confort cuando sea utilizado, estas condiciones son la altura de la cámara y la distancia para ser enfocado.

La altura es un aspecto fundamental para el reconocimiento facial, si es colocado de manera correcta permitirá una identificación más rápida, se debe tomar en cuenta la altura de las personas que frecuentan la vivienda, adaptándolo a los habitantes de cada hogar. Para el proyecto la cámara fue colocada a una distancia de 1,54 con respecto al suelo para facilitar a los usuarios, como se muestra en la figura 41.

Figura 41

Ubicación de la cámara

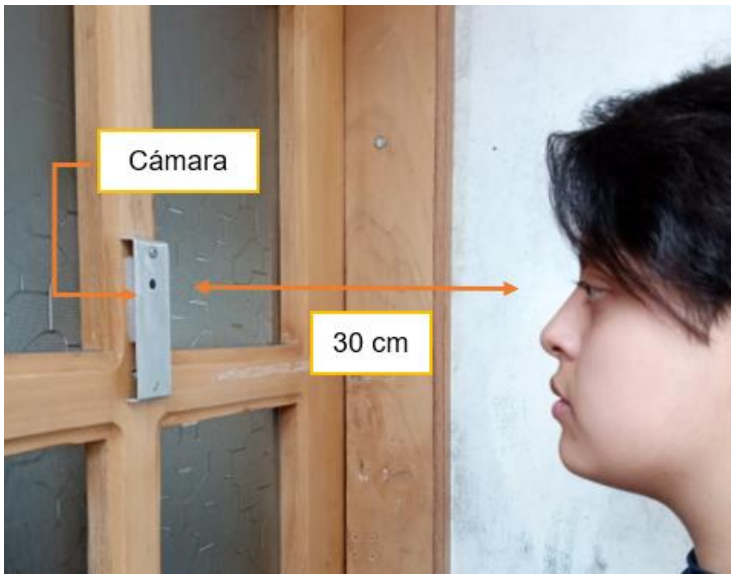


Nota: La figura muestra la ubicación de la cámara en la puerta de ingreso a la vivienda.

Debido a que se utilizó la cámara Raspberry y un algoritmo óptimo de clasificador para evitar errores de iluminación, no fue necesario realizar una inclinación de la cámara, solo ajustarla al tamaño de los usuarios y ajustarlo a una distancia razonable para una detección rápida, como se muestra en la figura 42.

Figura 42

Distancia entre la cámara y el usuario



Nota: La figura muestra la distancia a considerar para un buen enfoque de la cámara.

El sensor de movimiento PIR fue colocado en la parte inferior de la puerta secundaria de ingreso a la vivienda que detectará cualquier movimiento en un diámetro de 4 metros y un ángulo 110° grados para detectar a las personas que van a ingresar y aquellas ajenas a la vivienda que se acerquen a la misma, como se muestra en la figura 43.

Figura 43

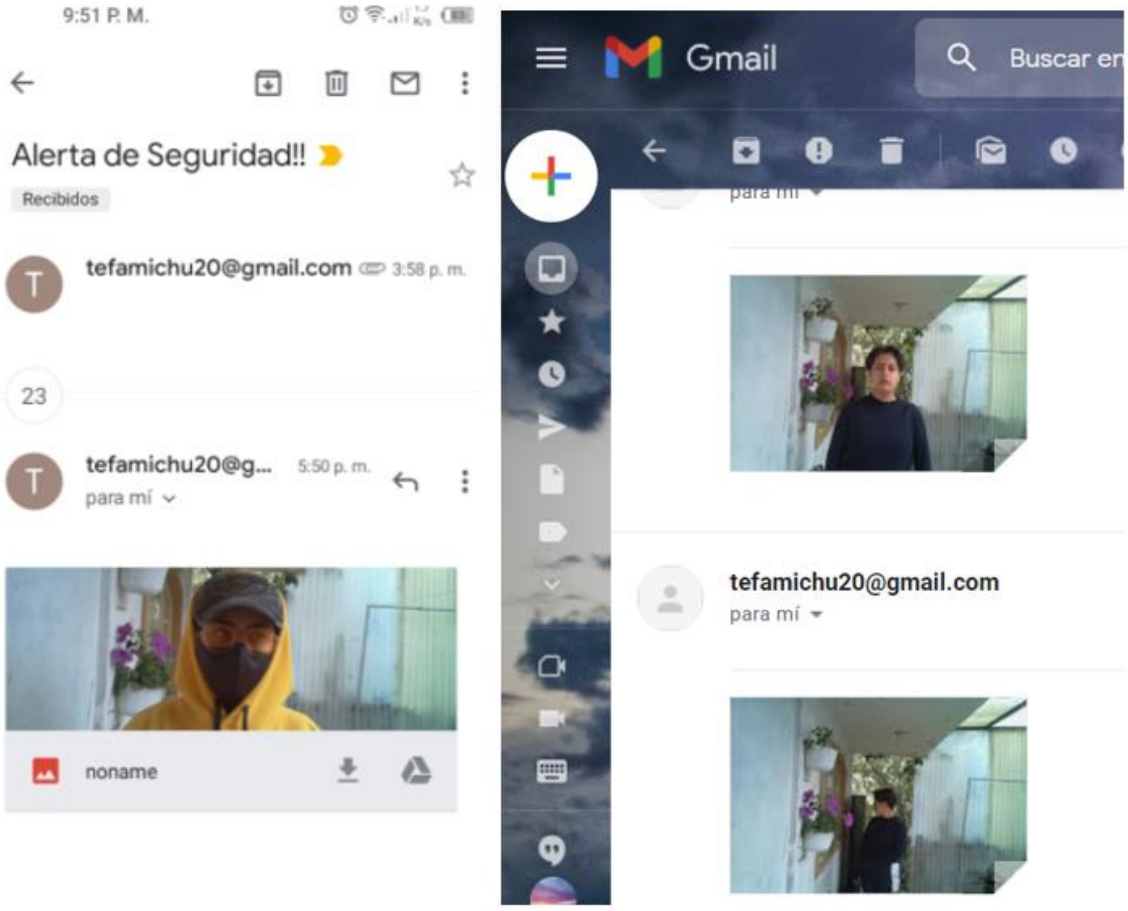
Ubicación del sensor de movimiento PIR

Nota: La figura muestra la ubicación del sensor PIR para la detección de movimiento hasta 4 metros del sensor.

El sensor de movimiento PIR al detectar a 4 metros de distancia la presencia de una persona, activara la cámara y tomara una fotografía de quien va a ingresar a la casa y la enviará por correo electrónico al propietario de la vivienda, como se muestra en la figura 44.

Figura 44

Envío de fotografía al correo electrónico



Nota: La figura muestra el envío de la fotografía al correo electrónico del propietario de la vivienda, capturada por la cámara.

De la misma forma se colocó un buzzer, en el interior de la vivienda como se muestra en la figura 45, el cual se activará al momento de encenderse la cerradura con 1 lógico identificando a una persona y se desactivará cuando la cerradura entregue un 0 lógico después de aproximadamente 5 segundos.

Figura 45

Instalación del buzzer

Nota: La figura muestra la instalación del buzzer en la caja del sistema en el interior de la vivienda.

3.3 Pruebas y resultados

Una vez culminado la implementación del sistema de reconocimiento facial se llevó a cabo las respectivas pruebas, se solicitó a 3 personas que frecuentan la vivienda sean capturados sus rostros para ejecutar el código que realizará el reconocimiento facial. Cada persona posee una carpeta con 30 fotos que el reconocedor ejecutara cuando se le solicite la identificación de la persona.

La idea de los resultados es comprobar que tan bien funciona la implementación del sistema, estas pruebas se extienden desde el inicio de la programación hasta la puesta en marcha del programa, ya que pasa por varias fases para la detección de rostros, por ellos se establecieron parámetros a considerar: la iluminación, el tiempo de respuesta y la distancia de la persona con la cámara para ser reconocida, entre otros.

3.3.4 Frecuencia de uso

La primera prueba se consideró la frecuencia de uso del reconocimiento facial y el tiempo de respuesta en entrenar el sistema, es decir si el usuario utiliza con mayor frecuencia el sistema biométrico para el almacenamiento de datos de sus rasgos faciales, el programa detectara más rápido quien es la persona que ingresa al domicilio ya que su algoritmo se basa en el entrenamiento de rasgos faciales, esto se puede evidenciar en la tabla número 6.

Tabla 6

Frecuencia de uso y tiempo de respuesta del entrenador

Frecuencia (Veces)	**Tiempo (seg)**
95 a 100	0 a 5
90 a 95	6 a 12
80 a 90	14 a 20
70 a 80	22 a 35
50 a 70	Mas de 40
0 a 50	Mas de 60

Nota: La tabla muestra una variación de porcentaje de las veces que el usuario paso por la cámara para ser identificado con mayor rapidez.

3.3.5 Iluminación de las imágenes

La segunda prueba que se realizaron fue de iluminación, para medir el tiempo de respuesta con luz natural en el día y luz artificial en la noche o en horas que este muy oscuro, esto se puede evidenciar en la tabla 7 y en la figura 46.

Tabla 7

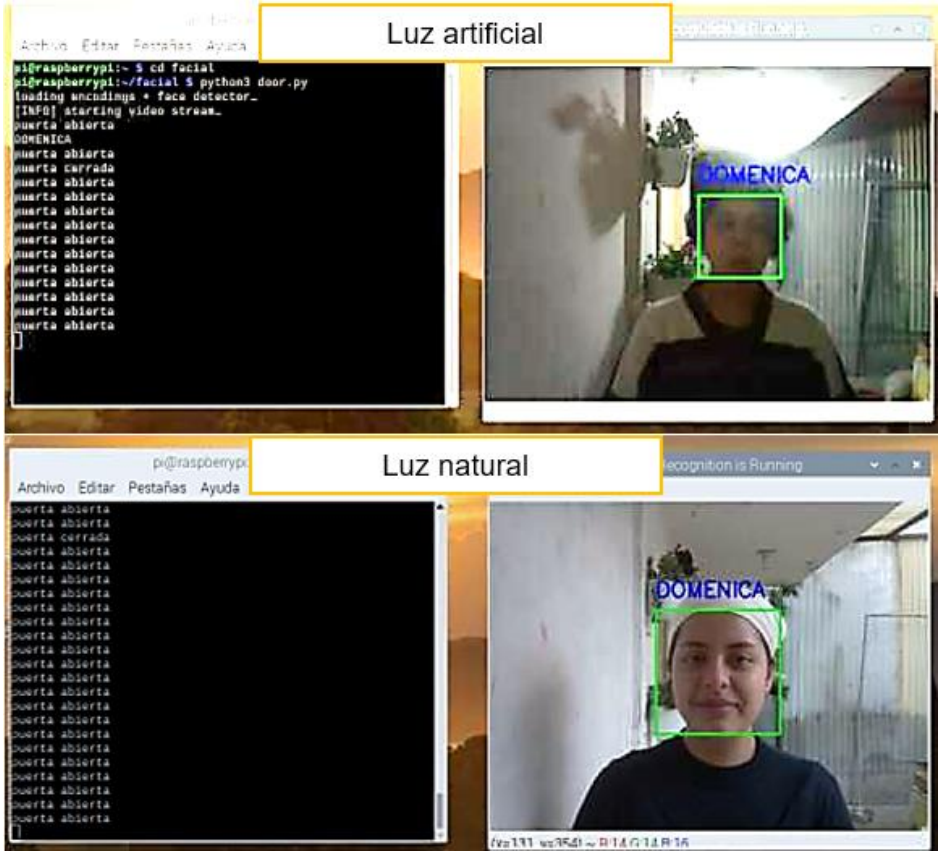
Pruebas de Iluminación

Usuarios	Iluminación	Porcentaje	Tiempo de respuesta (s)
DOME	Luz natural	90 %	30 s
	Luz artificial	50 %	66 s
MERCY	Luz natural	90 %	35 s
	Luz artificial	50 %	64 s
MICHELLE	Luz natural	90 %	20 s
	Luz artificial	50 %	35 s

Nota: En la tabla se evidencia los porcentajes y tiempos de respuesta que se obtuvieron con los usuarios.

Figura 46

Pruebas de iluminación



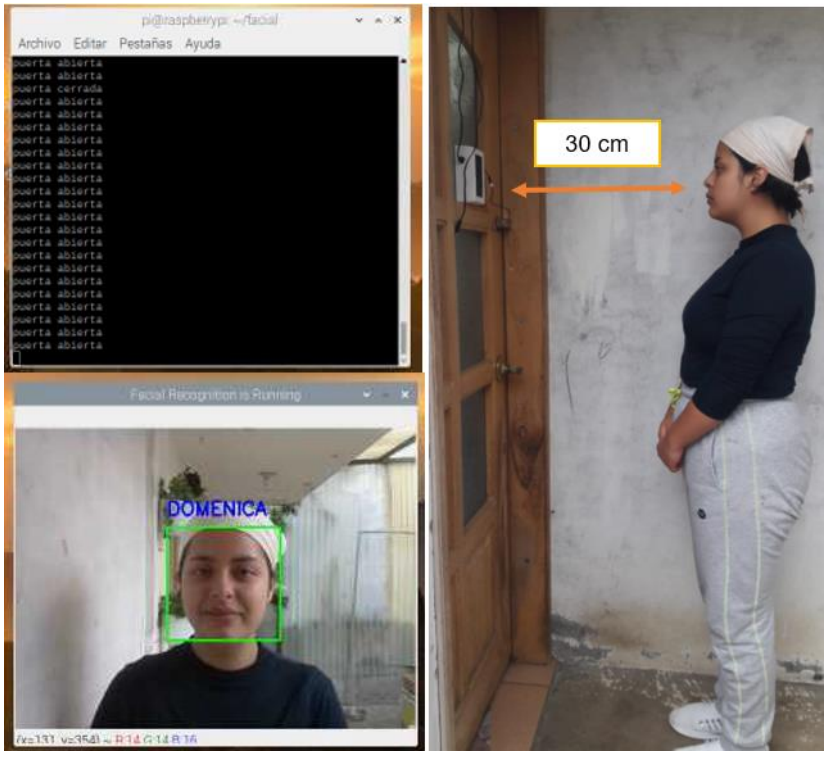
Nota: La figura muestra la identificación del usuario en distintos tiempos del día.

3.3.6 Distancia de detección

La tercera prueba que se realizó al sistema biométrico fue entre la distancia del usuario con la cámara, debido a que el sistema debe realizar la normalización de rostros necesita enmarcar al usuario a una distancia óptima para identificarlo, por esta razón el usuario debe colocarse frente a la cámara a la distancia de 30 cm para ser debidamente detectado por el sistema, como se muestra en la figura 47.

Figura 47

Distancia entre cámara y usuario



Nota: La figura muestra la identificación del usuario a una distancia optima de 30 cm.

Se determinaron distintas posiciones con respecto a la cámara para llegar a la distancia correcta, debido a que la cámara se encuentra en un pasillo de 4 metros para el ingreso al domicilio, se tomaron varias distancias como se evidencia en la tabla 8 y en la figura 48.

Tabla 8

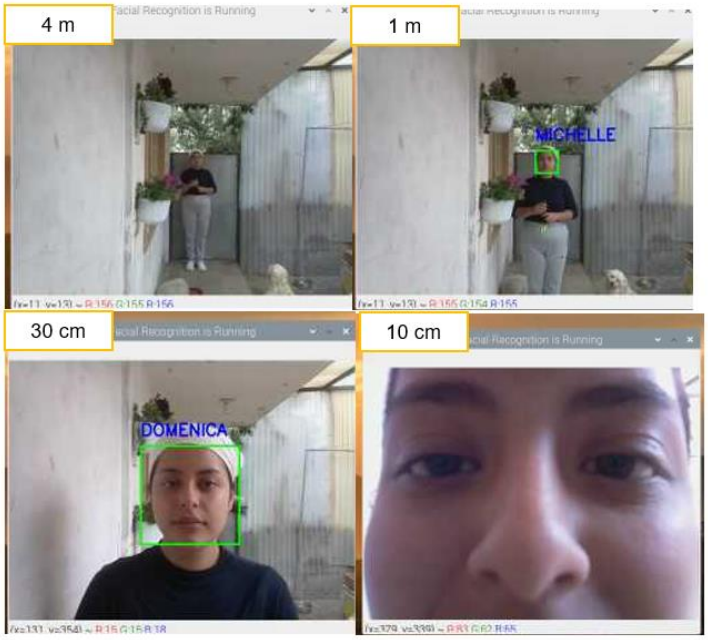
Referencias de distancias con la cámara

Distancia	Porcentaje de detección
10 cm	0 % sin enfoque
30 cm	100 % enfoque exitoso
80 cm	70 % no distingue el usuario
1 metro	30 % no distingue el usuario
3 metros	0 % no detecta el rostro
4 metros	0 % no detecta el rostro

Nota: En la tabla se puede evidenciar que a mayor distancia la cámara de la Raspberry no logra detectar de manera eficiente a los usuarios y se determinó que a una distancia de 30 cm tiene un enfoque eficaz y detecta correctamente al usuario.

Figura 48

Distancias de prueba

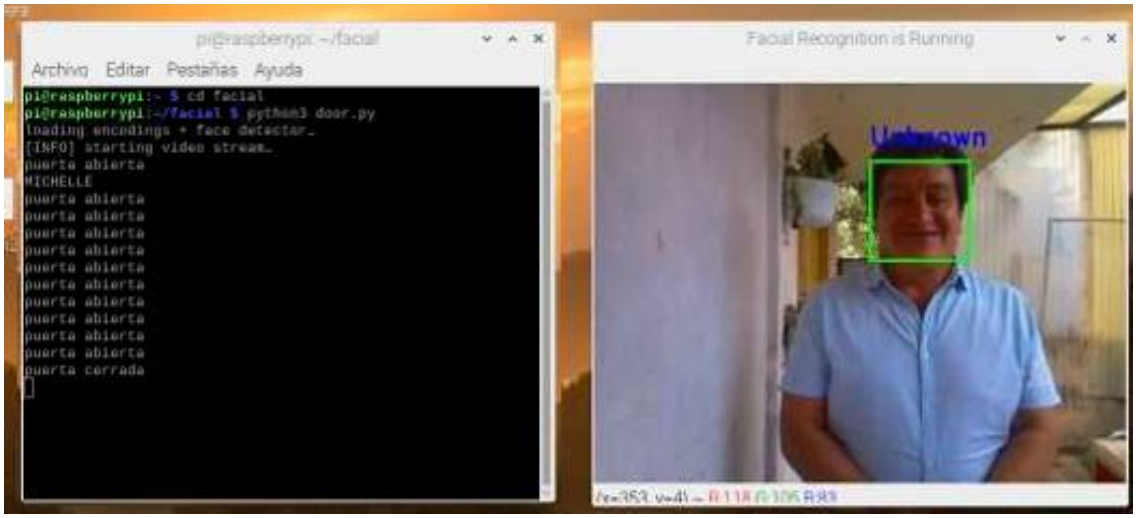


Nota: La figura muestra las distancias de prueba que se realizó para llegar a una distancia optima de 30 cm.

Una persona que ingresa al domicilio que no esté registrada en la base de datos del sistema, no podrá ingresar, debido a que no se activara el relé que acciona la cerradura y negara el paso del usuario extraño como se muestra en la figura 49.

Figura 49

Detección de usuario no identificado



Nota: La figura muestra a un usuario queriendo ingresar al domicilio, pero este no fue identificado y no se activa la cerradura.

3.3.7 Uso de accesorios

También fueron realizadas las pruebas con accesorios que se evidencia en la tabla 9, para comprobar el porcentaje de eficiencia del algoritmo de reconocimiento facial, con objetos muy comunes en los individuos que frecuentan la vivienda, esto es posible debido a la recolección de imágenes en la base de datos con los accesorios frecuentes que se evidencia en el Anexo D.

Tabla 9

Eficiencia de reconocimiento

Usuarios	Accesorios	Número de fotos	Porcentaje de reconocimiento
Michelle	Lentes	15/30	95%
	Bufanda	2/30	80%
	Gorra	15/30	75%
Domenica	Lentes	0/30	N/A
	Bufanda	5/30	85%
	Gorra	5/30	70%
Mercy	Lentes	5/30	90%
	Bufanda	5/30	85%
	Gorra	5/30	70%

Nota: La tabla muestra el porcentaje de eficiencia del reconocimiento facial con accesorios, este aumenta su eficacia según el número de fotografías que se almacene en la base de datos del sistema.

3.3.8 Sistema funcionando 24 horas – 7 días

Mediante un gráfico de resultados, como se muestra en la figura 50 se evidencia el uso del sistema de seguridad durante 7 días consecutivos las 24 horas del día. En este tiempo se observó que las 3 personas registradas en el sistema fueron identificadas 20 veces exitosamente, al llegar a los 5 días se registró tres intentos de ingreso de personas no identificadas y la activación de la alarma al no ser reconocidas por el sistema. También se observa que el sensor de movimiento se mantiene activo todo el tiempo que el sistema fue puesto a prueba enviando las imágenes de la persona que ingresa al domicilio.

Figura 50

Resultado de 7 Días – 24 Horas

Nota: La figura muestra los resultados obtenidos a lo largo de 7 días que fue puesto a prueba de manera consecutiva el sistema de seguridad con reconocimiento facial.

CAPITULO IV

4 Conclusiones y recomendaciones

4.1 Conclusiones

- Al realizar la recopilación de información de los sistemas de seguridad biométricos se evidencia que su uso aumenta la protección en hogares o lugares donde sean implementados, muchas de ellas eran viables para ser utilizadas en el proyecto, sin embargo, se tomó la decisión de usar técnicas de reconocimiento facial debido a sus múltiples beneficios, en especial evitar el contacto de superficies en donde pueden alojarse virus y bacterias, que hoy en día debe ser una prioridad para cualquier hogar.
- En la definición de los requerimientos de herramientas de hardware, software y algoritmos, se estableció el uso de tecnología Raspberry Pi para el funcionamiento del sistema biométrico, el cual trabaja mediante programación Python y clasificadores propios de OpenCV, simplificando la codificación y un correcto funcionamiento en diferentes instancias del día para la identificación de personas.
- El sistema de reconocimiento facial está basado en el uso de clasificadores pre – entrenados como Haar-like features, el mismo que fue utilizado en el proyecto para facilitar el entrenamiento del sistema con pocas imágenes y un algoritmo en cascada que clasificó las facciones de cada usuario.
- Analizando los requerimientos de los habitantes del domicilio, se determinó el uso de elementos compatibles con la Tarjeta Raspberry Pi para una mayor comodidad de instalación y detección de rostros, es así que su cámara se implementó a una altura de 1,54 metros, que es el tamaño promedio de los usuarios, brindando rapidez de detección con un tiempo menor a 10 segundos

aproximadamente y otorgando confort y seguridad al momento de implementarlo como un control de acceso.

4.2 Recomendaciones

- El uso de voltajes requeridos en el sistema es fundamental para no dañar ningún componente presente en la tarjeta, ya que cada elemento trabaja con valores diferentes y sobrepasar dichos valores puede afectar permanentemente al sistema.
- El uso de software adecuados para el reconocimiento facial como librerías de OpenCV y programación en Python que permita la edición de códigos necesarios para la identificación de personas y el almacenamiento de datos.
- La capacidad de almacenamiento en la tarjeta micro SD debe ser mayor a 8GB, debido a que el sistema operativo ocupa alrededor de 3GB, por lo tanto, una tarjeta de menor capacidad limita el buen funcionamiento y velocidad de la tarjeta Raspberry Pi.
- Investigar y estudiar el uso de tarjetas Raspberry Pi para minimizar errores de manipulación al momento de ejecutar cualquiera de sus sistemas o programaciones.

Bibliografía

Bricoladores, S. (2018). *Seguridad en el hogar: qué debemos proteger*. Recuperado el 8 de Diciembre del 2020, de simonelectric: https://bricoladores.simonelectric.com/seguridad-en-el-hogar-que-debemosproteger

Romero, C., Vázquez, F., & Castro, C. D. (2010). Domótica e inmótica: viviendas y edif. inteligentes. Recuperado el 8 de Diciembre del 2020, de GoogleBooks: https://books.google.com.ec/books?id=BphsGQAACAAJ&dq=Romero,+C.,+V%C3%A1zquez,+F.,+%26+Castro,+C.+D.+(2010).+Domotica+e+inmotica:+viviendas+y+edif.+inteligentes.&hl=es&sa=X&ved=2ahUKEwj3k7D53ZrvAhVCn-AKHeO2Cy0Q6AEwAXoECAMQAg

Álvarez, G. R. (2020). *La domótica, una alternativa contra el covid-19*. Recuperado el 8 de Diciembre del 2020, de El Comercio: https://www.elcomercio.com/tendencias/domotica-tecnologia-seguridad-viviendacovid19.html

Olleros, Á. (2020). *Sistemas de domótica y seguridad residencial*. Recuperado el 9 de diciembre del 2020, de Ángel Olleros: https://www.angelolleros.com/sistemas-domotica-seguridad-residencial/

Cérda, M., & Gas, M. (2020). *Instalaciones Domóticas* (1 ed.). recuperado el 12 de Diciembre del 2020, de Paraninfo: https://books.google.com.ec/books?id=HyLhDwAAQBAJ&printsec=frontcover&dq=domotica+pdf&hl=es419&sa=X&ved=2ahUKEwisx_7P7oDuAhXKt1kKHS99CQQ4ChDoATAIegQICRAC#v=onepage&q&f=true

Asale, R. (2020). *biometría | Diccionario de la lengua española*. Recuperado el 12 de diciembre del 2020, de Diccionario de la lengua española - Edición del Tricentenario:

https://dle.rae.es/biometr%C3%ADa

García L. (2011). *Estudio sobre las tecnologías biométricas aplicadas a la seguridad*. Recuperado el 12 de Diciembre del 2020, de congreso.gob.pe: http://www2.congreso.gob.pe/sicr/cendocbib/con4_uibd.nsf/65877225F2975B3F0257E6E006A2C3D/$FILE/EstudioSobreTecnolog%C3%ADasBiom%C3%A9tri casASeguridad.pdf

Umanick Technologies. (2017). *Sistemas biométricos: El reconocimiento facial* [Vídeo]. Recuperado el 12 de Diciembre del 2020, de YouTube: https://www.youtube.com/watch?v=gfc63k2PT8g

Kutxa, L. (2018). *¿Cómo funciona el reconocimiento facial?* Ba da beste modu bat. Recuperado el 13 de Diciembre del 2020, de Laboral Kutxa Blog: https://blog.laboralkutxa.com/como-funcionareconocimiento-facial/

Qué es Inmótica. (2010). Asociación Española de Domótica e Inmótica. Recuperado el 12 de Diciembre del 2020, de CEDOM: http://www.cedom.es/sobre-domotica/que-es-inmotica

Gavilán, I. G. R. (2020). Las cuatro fases del reconocimiento facial. Recuperado el 15 de Diciembre del 2020, de Ignacio G.R. Gavilán: https://ignaciogavilan.com/las-cuatro-fases-del-reconocimiento-facial/

G. (2020). Detección y reconocimiento facial con OpenCV, Python y FaceRecognition. robologs. Recuperado el 15 de Diciembre del 2020, de robologs: https://robologs.net/2020/05/05/deteccion-y-reconocimiento-facial-con-opencv-python-y-facerecognition/

A. (2017). Estimación de calidad de los algoritmos de reconocimiento facial. Recuperado el 15 de Diciembre del 2020, de FindFace Pro: https://findface.pro/es/blog/calidad-del-algoritmo-de-reconocimiento/

Datasheet Raspberry Pi Compute Module 3+. (2019). Recuperado el 3 de Enero del 2021, de Raspberry Pi Fundation: https://www.raspberrypi.org/documentation/hardware/computemodule/datasheets/rpi_DATA_CM3plus_1p0.pdf

Python 3 al descubierto - 2a ed. (2013). Recuperado el 3 de Enero del 2021, de Google Books: https://books.google.es/books?hl=es&lr=&id=f4BNDAAAQBAJ&oi=fnd&pg=PT3&dq=python+caracter%C3%ADsticas&ots=Ubhc-bC3qw&sig=NTHiBjuLzD2viEZQaQWW6VW7qNI#v=onepage&q=python%20caracter%C3%ADsticas&f=true

Chris, M. (2019). BeginnersGuide/Overview - Python Wiki. Recuperado el 4 de Enero del 2021, de Python.org. https://wiki.python.org/moin/BeginnersGuide/Overview

Leon, D. C., & Damara, I. (2011). Domótica e inmótica: viviendas y edificios inteligentes. Universidad Veracruzana. Recuperado el 4 de Enero del 2021, de docplayer: https://docplayer.es/10069547-Universidad-veracruzana-facultad-de-ingenieria-mecanica-electrica.html

Python, R. (2020). *Viola-Jones Object Detection Framework*. Recuperado el 5 de enero del 2021, de Python: https://realpython.com/lessons/viola-jones-object-detection-framework/

Gadgetoid. (2021). *Raspberry Pi GPIO Pinout*. Recuperado el 25 de Enero del 2021, de Raspberry Pi: https://pinout.xyz/

Solano, G. (2020). *Reconocimiento Facial | Python – OpenCV. Recuperado el 25 de Enero del 202, de omes-va.com*: https://omes-va.com/reconocimiento-facial-python-opencv/

Linux commands - Raspberry Pi Documentation. (2020). Recuperado el 26 de Enero del 2021, de Raspberry Pi: https://www.raspberrypi.org/documentation/linux/usage/commands.md

SEAS, Estudios Superiores Abiertos. (2019). *El Relé: para qué es, para qué sirve y qué tipos existen. Recuperado el 7 de Marzo del 2021, de* Blog de SEAS: https://www.seas.es/blog/automatizacion/el-rele-para-que-es-para-que-sirve-y-que-tipos-existen/

@dminw3b. (2020). *Sensores de Movimientos: Modelos y Funcionamiento*. Recuperado el 23 de Marzo del 2021, de Grupo Legrand: https://legrand.com.pe/sensores-de-movimiento-modelos-y-funcionamiento/

CDMX Electrónica. (2021). *Buzzer Zumbador 5V Activo - 30 mA*. Recuperado el 30 de Marzo del 2021, de UNIT Electronics: https://uelectronics.com/producto/buzzer-5v-activo/

Anexos