ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

"IMPLEMENTACIÓN DE UN MÓDULO DOMÓTICO DE SEGURIDAD RESIDENCIAL APLICANDO TÉCNICAS DE VISIÓN ARTIFICIAL PARA LA IDENTIFICACIÓN DE ROSTROS."

Trabajo de titulación

Tipo: Dispositivo Tecnológico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN

AUTORES:

HENRY VLADIMIR CAIZA LEMA

ALEXANDER SEBASTIÁN YANZA QUINGATUÑA

Riobamba – Ecuador

2021

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

"IMPLEMENTACIÓN DE UN MÓDULO DOMÓTICO DE SEGURIDAD RESIDENCIAL APLICANDO TÉCNICAS DE VISIÓN ARTIFICIAL PARA LA IDENTIFICACIÓN DE ROSTROS."

Trabajo de titulación

Tipo: Dispositivo Tecnológico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN

AUTORES: HENRY VLADIMIR CAIZA LEMA

ALEXANDER SEBASTIÁN YANZA QUINGATUÑA

DIRECTOR: Ing. JOSÉ LUIS TINAJERO LEÓN

Riobamba – Ecuador

2021

"Nosotros **HENRY VLADIMIR CAIZA LEMA** y **ALEXANDER SEBASTIÁN YANZA QUINGATUÑA,** declaramos que el presente trabajo de titulación es de nuestra autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autores asumimos la responsabilidad legal y académica de los contenidos de este trabajo de titulación; el patrimonio intelectual pertenece a la Escuela Superior Politécnica de Chimborazo.

Riobamba, 18 de septiembre del 2021

Henry Vladimir Caiza Lema	**Alexander Sebastián Yanza Quingatuña**
CI: 050423204-2	**CI:180489125-5**

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA ELECTRÓNICA Y AUTOMATIZACIÓN

El Tribunal de Trabajo de Titulación certifica que: El trabajo de titulación; Tipo: Dispositivo Tecnológico, **"IMPLEMENTACIÓN DE UN MÓDULO DOMÓTICO DE SEGURIDAD RESIDENCIAL APLICANDO TÉCNICAS DE VISIÓN ARTIFICIAL PARA LA IDENTIFICACIÓN DE ROSTROS."**, realizado por los señores **HENRY VLADIMIR CAIZA LEMA y ALEXANDER SEBASTIÁN YANZA QUINGATUÑA**, ha sido minuciosamente revisado por los Miembros del Tribunal de Trabajo de Titulación, el mismo que cumple con los requisitos científicos , técnicos, legales, en tal virtud el Tribunal Autoriza su presentación.

	FIRMA	FECHA
Ing. Verónica Elizabeth Mora Chunllo **PRESIDENTE DEL TRIBUNAL**	VERONICA ELIZABETH MORA CHUNLLO Digitally signed by VERONICA ELIZABETH MORA CHUNLLO Date: 2021.12.03 09:43:57 -05'00' ……..	21-12-02
Ing. José Luis Tinajero León **DIRECTOR DE TRABAJO DE TITULACIÓN**	Firmado electrónicamente por: **JOSE LUIS TINAJERO** ……..	21-12-02
Ing. Pablo Eduardo Lozada Yánez **MIEMBRO DE TRIBUNAL**	Firmado digitalmente por PABLO EDUARDO LOZADA YANEZ ……..	21-12-02

DEDICATORIA

El presente trabajo está dedicado a mi familia y en especial a mis padres Alberto Caiza y Blanca Lema por ser mi apoyo y ejemplo a seguir, por todo el sacrificio que han hecho para darme lo más valioso que es la educación, también a mi hermana Lisbeth Caiza que siempre me apoya en todas mis decisiones, son mi tesoro más valioso, gracias por estar siempre pendientes de cada etapa de mi vida, y me dan el valor para seguir adelante sin miedo a nuevos retos.

Henry

El presente trabajo está dedicado a mis padres Jaime y Mónica en especial a mi madre quien me ha apoyado a lo largo de este proceso, el camino para llegar aquí no ha sido fácil y su esfuerzo, sus palabras de apoyo me han ayudado a perseverar y superar las adversidades, Con orgullo este logro es de ustedes.

Alexander

AGRADECIMIENTO

Nacimos para cometer errores, no para fingir ser personas perfectas, en el camino se encuentra una infinidad de tropiezos, pero de ellas se aprende, agradezco a Dios y a mis maravillosos padres y hermana que son el pilar fundamental de mi vida, por guiarme durante toda la carrera y ser mi fortaleza en mis momentos tristes, gracias por el esfuerzo, sus consejos y regaños que junto a toda mi familia han logrado que cumpla con esta gran meta.

Henry

Lograr una meta por sí solo es imposible, es por ello que agradezco a todas las personas que me han ayudado a cumplir uno mi mis objetivos personales, agradezco a mis padres que hicieron todo lo posible por dejarme la mejor herencia que los padres pueden dejar a sus hijos que es la educación, agradezco a mi novia quien ha estado en los momentos más complicados dándome palabras de aliento y ayudándome a crecer como persona, a mis amigos Andrés, Katy, Henry, Alex, Brayan que a lo largo de la carrera formamos una gran amistad y que las anécdotas vividas juntos jamás se olvidarán.

Alexander

TABLA DE CONTENIDO

CAPÍTULO II

CAPÍTULO III

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

ÍNDICE DE ABREVIATURAS

AC: Corriente Alterna.

API: Interfaz De Programación De Aplicaciones.

ARM: Advanced RISC Machine / Máquina RISC Avanzada.

AVR: Automatic Voltage Regulator / Regulador Automático de Voltaje.

BCM: Body Controller Module / Computadora De Chasís.

BSD: Distribución De Software Berkeley.

CCTV: Closed Circuit Television / Circuito Cerrado De Televisión.

CSI: Camera Serial Interface / Interfaz Serie para Cámara.

DC: Corriente Continua.

DDNS: Dynamic Domain Name System / Sistema Dinámico De Nombres De Dominio.

DNS: Domain Name System / Sistema De Nombres De Dominio.

DSC: Dynamic Stability Control / Sistema De Control Dinámico De Estabilidad.

DSI: Display interfaz serial / Interfaz Serie paraOpantalla

FPGA: Field Programmable Gate Arrays / Matriz De Puertas Lógicas Programable En Campo.

FPS: Frames For Second / Cuadros Por Segundo.

FTP: File Transfer Protocol / Protocolo de transferencia de archivos.

GPIO: General Purpose Input-Output / Entrada-Salida De Uso General.

HTTPS: Hypertext Transfer Protocol Secure / Protocolo Seguro De Transferencia De Hipertexto.

ICMP: Internet Control Message Protocol / Protocolo De Mensajes De Control De Internet.

IDE: Entorno De Desarrollo Integrado.

IGMP: Protocolo De Administración De Grupos De Internet.

IP: Protocolo de Internet.

ISO: International Organization for Standardization / Organización Internacional para la Estandarización.

LAN: Local Area Network / Red De Area Local.

LBP: Patrones Binarios Locales.

LBPH: Histograma De Patrones Binarios Locales**.**

LPDDR: Low Power Double Data Rate / Velocidad De Datos Doble De Baja Potencia.

NTP: Network Time Protocol / Protocolo De Tiempo De Red.

NVR: Network Video Recorder / Grabador de Video de Red

PIC: Programmable Interrupt Controller / Controlador programable de interrupciones.

PoE: Power Over Ethernet / Alimentación A Través De Ethernet.

PPPoE: Point-To-Point Protocol Over Ethernet / Protocolo Punto A Punto Sobre Ethernet.

PWM: Pulse Width Modulation / Modulación por Ancho de Pulsos.

QoS: Quality Of Service / Calidad De Servicio.

RAM: Random Access Memory / Memoria de Acceso Aleatorio.

RISC: Reduced Instruction Set Computer / Computador Con Conjunto De Instrucciones Reducido.

RTCP: Real Time Transport Protocol / Protocolo De Transporte En Tiempo Real.

RTSP: Real Time Streaming Protocol / Protocolo De Transmisión En Tiempo Real.

SMTP: Simple Mail Transfer Protocol / Protocolo Simple De Transferencia De Correo.

SNMP: Simple Network Management Protocol / Protocolo Simple De Administración De Red.

SoC: System On A Chip / Sistema En Chip

TCP: Transmission Control Protocol / Protocolo De Control De Transmisión.

UDP: User Datagram Protocol / Protocolo De Datagramas De Usuario.

USB: Bus Universal en Serie

VA: Visión Artificial.

VHDL: Very High Speed Integrated Circuit Hardware Description Language / Lenguaje de Descripción de Hardware para Circuitos Integrados de Muy Alta Velocidad.

WAN: Wide Area Network / Red De Área Amplia.

RESUMEN

El presente trabajo de titulación se desarrolló con el objetivo de implementar un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la detección de rostros. El mismo que mediante el uso de una red de video vigilancia convencional, obtiene las imágenes a través del protocolo de comunicación RTSP de una cámara IP para el posterior procesamiento haciendo uso de un microordenador como la Raspberry Pi 4, dichas imágenes son analizadas con herramientas de visión artificial que permiten seleccionar características de los rostros a través de librerías de OpenCV y clasificadores HAAR, este algoritmo se ejecuta sobre el sistema operativo Raspberry Pi OS basado en Linux propio de la tarjeta de desarrollo, el cual también permite la activación de salidas en caso de vulnerar la red de video vigilancia ejecutándose un protocolo de seguridad como alarma y simulación de presencia. El módulo consta de una interfaz gráfica desarrollada en Node-red que permite la activación o desactivación del mismo, al igual que consta de un botón de pánico en caso de requerirlo, también se encuentra vinculada a la red social Telegram que gracias a sus políticas de privacidad recibe la notificación del estado del módulo y fotografía del rostro de la persona que no se encuentre registrada en la base de datos incluyendo comandos para encender o apagar el módulo directamente desde la mencionada aplicación. Se concluye que la cámara se debe ubicar a una altura de 240 cm y el alcance máximo de detección a 160 cm para obtener resultados satisfactorios. Se recomienda ingresar por lo menos unas 20 imágenes por cada tipo de ambiente a la base de datos, es decir, para climas soleado, nublado, nocturno, etc. esto mejorará la robustez del módulo.
Palabras clave: <VISIÓN ARTIFICIAL> <DOMÓTICA> <VIDEO VIGILANCIA> <OPEN CV (SOFTWARE)> <PROCESAMIENTO DE IMÁGENES>.

ABSTRACT

This graduate research aimed to implement a home automation module for residential security applying artificial vision techniques for face detection. With the use of a conventional video surveillance network obtains the images through the RTSP communication protocol from an IP camera for further processing using a microcomputer such as the Raspberry Pi 4, those images are analyzed with artificial vision tools allowing to select of facial features through OpenCV libraries and HAAR classifiers, this algorithm runs on Pi OS operating system based Linux own of developing board, which also allows the activation of outputs in case of violating the video surveillance network by executing a security protocol such as alarm and presence simulation. The module consists of a graphical interface developed in Node-red that allows its activation or deactivation and a panic button if required. It is also linked to the social network Telegram that, thanks to its policies of Privacy, receive the notification of the status of the module and a photograph of the face of the person who is not registered in the database, including commands to turn the module on or off directly from the application mentioned above. It is concluded that the camera should be located at the height of 240 cm and the maximum detection range at 160 cm to obtain satisfactory results. It is recommended to enter at least 20 images for each type of environment into the database, that is, for sunny, cloudy, night climates, etc; this will improve the robustness of the module.

Keywords: <ARTIFICIAL VISION> <HOME AUTOMATION> <VIDEO SURVEILLANCE> <OPEN CV (SOFTWARE)> <IMAGE PROCESSING>.

INTRODUCCIÓN

Actualmente los sistemas de seguridad que integran técnicas visón artificial permiten identificar a un individuo en base a sus características físicas, como el reconocimiento de rostros, detección de huellas digitales o reconocimiento de voz entre otros. Estos sistemas desempeñan un papel de suma importancia dentro del desarrollo de hogares inteligentes.

Los módulos de seguridad agregados a la automatización dentro del ambiente domiciliario forman parte primordial de la domótica, el mismo que está conformado por un sistema de cámaras de video vigilancia, cuya fuente de video permite realizar la comparación de determinados rasgos faciales de la imagen con la almacenada en una base de datos, convirtiendo así un sistema de video vigilancia convencional en un sistema de video vigilancia inteligente. La necesidad de incrementar la seguridad se deja sentir en todo el mundo, no solo por compañías privadas sino también por los gobiernos y las instituciones públicas. Debido a esto, últimamente los sistemas de video vigilancia inteligente se han convertido en una importante área de investigación gracias a su aplicación en el sector de la seguridad (Moctezuma, 2016, p. 1).

Por lo tanto, la implementación del módulo domótico de seguridad residencial que aplica técnicas de visión artificial para la detección de rostros, permite aprovechar la tecnología existente y optimizarla usando algoritmos y métodos de detección facial que permita reducir los tiempos del procesamiento de imágenes.

ANTECEDENTES

Los importantes avances tecnológicos y las necesidades a ser atendidas generan cada vez, más recursos para el desarrollo de nuevos dispositivos, así como el aumento de la innovación de tecnología destinada a infinitas tareas, al punto en el que, el ser humano puede desarrollar su vida diaria con mayor facilidad y optimizar su labor. El ahorro de tiempo, recursos y, lo más importante, proporcionar nuevos campos de investigación para el desarrollo de nuevos dispositivos (Guranga, 2018, p. 2).

En los últimos años, el desarrollo de equipos de seguridad para el hogar, ha aumentado debido a los problemas de seguridad existentes, esto permite la creación de diversas aplicaciones y diversos usos de los beneficios que brindan este tipo de tecnologías. Para el desarrollo de los equipos se basan en el uso de varios dispositivos de seguridad en la actualidad existentes. A través del monitoreo y operación centralizada en placas de desarrollo de bajo costo, estas placas de desarrollo son altamente accesibles para la gestión de la información, proporcionando a los usuarios un mayor grado de confianza y fácil acceso a todos los componentes configurados en el sistema de seguridad.

En el Ecuador la domótica, sobresale como nueva tecnología que se adapta a los cambios en las redes de telecomunicaciones, el cual permite explorar estas vías de comunicación para brindar nuevos servicios, es por ello que en varias universidades y escuelas politécnicas del país se han desarrollado trabajos de investigación con el objetivo de brindar soluciones a diferentes problemas de seguridad en los hogares a través de la implementación de este tipo de tecnologías.

En el año 2016 en la Universidad Técnica de Machala se realizó una tesis con el título "DISEÑO Y CONSTRUCCIÓN DE UN PROTOTIPO DE SISTEMA DE SEGURIDAD DE UNA CASA UTILIZANDO LA PLATAFORMA ARDUINO", en la cual se desarrolló un prototipo para detectar movimiento de personas, apertura de puertas como variables para el sistema de seguridad, para este prototipo se utilizó la tarjeta de desarrollo Arduino UNO, junto con un módulo de WIFI compatible para la tarjeta de desarrollo para la administración de datos a través de la red (Tapia, 2016, p. 8).

En el año 2018 en la Escuela Superior Politécnica de Chimborazo se desarrolló una tesis con el título de "DISEÑO DE UN SISTEMA PARA SEGURIDAD DE UNA VIVIENDA MEDIANTE PASARELA ACTIVADA POR VOZ Y VIDEO A DESARROLLARSE", este era controlado a través de un Arduino mega es cual controlaba los diferentes sensores instalados en la vivienda, además usa comandos de voz para su funcionamiento, de la misma forma utiliza cámaras de seguridad y un NVR (Network Video Recorder) para administrar las cámaras a través de la red .

En el mismo año en el artículo "IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD INDEPENDIENTE Y AUTOMATIZACIÓN DE UNA RESIDENCIA POR MEDIO DEL

INTERNET DE LAS COSAS", se muestra a parte del monitoreo de vigilancia controles como la iluminación, apertura y cierre de puertas y ventas, control de temperatura a través de una página Web la cual cuenta con control de ingreso para que personas no autorizadas entran a dicha página (Fuentes y Perez, 2018, p. 2).

En los mencionados trabajos se puede evidenciar la importancia de los sistemas de seguridad para el hogar, y como se busca aprovechar las tecnologías modernas para mejores los sistemas de seguridad, brindando más beneficios y buscando un desarrollo tecnológico en el país.

JUSTIFICACIÓN TEÓRICA

En los últimos años los índices de robos a domicilios han aumentado a nivel nacional, ya que la mayoría de domicilios no cuentan con un sistema de seguridad, debido al alto costo que estos representan, y aquellos que cuentan con un sistema de seguridad por lo general son cámaras de seguridad, alarmas o cercos eléctricos sin embargo resultan vulnerables cuando el domicilio está deshabitado y el sector en donde está ubicado no es muy poblado.

En asaltos a viviendas, los mayores inconvenientes están en Guayaquil, Quito y Machala. En donde se evidencia diferentes modalidades de robo, desde un domicilio deshabitado, hasta el uso de armas para intimidar a los habitantes en caso de que se encuentren en el interior del mismo. Al no contar con un sistema eficiente de seguridad que alerte la presencia de personas extrañas estos casos se llegan a notificar a la Policía muy tarde, en algunos casos se puede identificar a través de cámaras de seguridad en donde queda grabado el robo.

Es por ello que en las residencias actuales existe la necesidad de actualizar los sistemas internos de vigilancia, seguridad y optimizar diversas funciones para mejorar la eficiencia y comodidad de diferentes actividades que la persona puede realizar en el hogar, a través de la domótica, internet de las cosas y visión artificial.

El uso de estas tecnologías permite automatizar ciertas actividades para que puedan desarrollarse por sí mismas sin la participación directa de un ser humano. En el caso de una residencia, la automatización puede corresponder a la ejecución de tareas domésticas, como control de iluminación, calefacción y ventilación, apertura y cierre de puertas, ventanas y portones, incluidas funciones como los sistemas de vigilancia y seguridad.

La domótica es una nueva tecnología que se adapta a los cambios en las redes de telecomunicaciones, y lo que se está haciendo es explorar estas vías de comunicación para brindar nuevos servicios en ellas, no solo de voz. Pero en este campo, ya sea informático o electrónico, sigue siendo necesario el conocimiento y la formación de profesionales dedicados al desarrollo de este tipo de aplicaciones. En Ecuador, las empresas que brindan soluciones de domótica

utilizan sistemas de fabricación extranjera y aquí solo se realiza la comercialización, pero la idea no es convertirse en consumidor, sino en fabricante de equipos de domótica (Morejon 2016).

El trabajo propuesto en este documento se enfoca en la integración de un módulo domótico de seguridad con la integración de la visión artificial para el reconocimiento de rostros en viviendas y zonas residenciales que permitirán identificar si las personas detectadas por las cámaras tienen autorización de estar en el domicilio, caso contrario se activará un protocolo de seguridad.

JUSTIFICACIÓN APLICATIVA

La figura (1), muestra la propuesta del módulo a ser implementado, el cual estará compuesto por una red de cámaras y sensores los cuales se ubicaran en lugares estratégicos con el objetivo de tener un rango amplio de visión para poder garantizar la seguridad y el correcto monitoreo, los cuales proveerán de información de los exteriores de la vivienda, esta información será enviada a una tarjeta de desarrollo que se encargará de procesar las imágenes y posteriormente compararlas con imágenes registradas en una base de datos, el módulo permitirá al usuario configurarlo en dos modos, el primero consiste en notificar al dueño del inmueble la presencia de intrusos, esto se logra mediante un algoritmo de procesamiento de imágenes que compare los rostros obtenidos por la cámara de seguridad con los almacenados en una base de datos, y de manera inmediata se activará una alarma, a su vez se bloqueara el acceso. El segundo modo se activará cuando el domicilio se encuentra deshabitado, este realizará las acciones mencionadas en el primer modo, además de electrificar cerraduras de puertas y marcos de ventanas con el objetivo de garantizar la seguridad del domicilio y de igual manera se simulará la presencia de personas activando ciertos electrodomésticos y luces de la casa. La arquitectura que se utilizará para el desarrollo de este módulo será centralizada ya que todos los elementos que forman parte del mismo se conectarán directamente a la tarjeta de desarrollo, la cual procesa los datos y ejecutará las acciones descritas anteriormente.

Todo esto se lo podrá controlar y monitorear a través de un dispositivo móvil el cual proporcionará información en tiempo real.

OBJETIVOS

OBJETIVO GENERAL

Implementar un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros.

OBJETIVOS ESPECÍFICOS

- Estudiar las tecnologías existentes de dispositivos de seguridad basados en visión artificial.
- Establecer los requerimientos de diseño que debe cumplir el prototipo.
- Definir el diseño apropiado que permita cumplir con los requerimientos establecidos en la construcción del prototipo.
- Integrar los componentes de hardware y software adecuados que permita cumplir con los requerimientos establecidos para el prototipo.
- Examinar la confiabilidad del módulo implementado a través de pruebas realizadas en diferentes escenarios posibles para la detección de rostros.

CAPÍTULO I

1. MARCO TEÓRICO

En este capítulo se detalla los conceptos básicos de lo que es domótica y como se puede aplicar a un módulo de seguridad domótico, así como los principales elementos que conforman dicho módulo.

1.1. Domótica e Inmótica

Es un conjunto de servicios domiciliarios proporcionados por un sistema multifuncional, que pueden conectarse entre sí o a redes de comunicación interiores y exteriores. Su propósito es garantizar el ahorro, la comodidad y la seguridad del usuario, al tiempo que reduce el consumo de energía, la gestión eficaz de la tecnología del hogar y un alto nivel seguridad (Navarro, 2015, p. 25).

En la Figura 1-1 se puede observar los principales elementos que nos permite cumplir con estos requerimientos, como son cámaras de vigilancia y sensores para la seguridad, control de temperatura para el apartado de confort, comunicación a través de diferentes dispositivos como celulares y computadores.

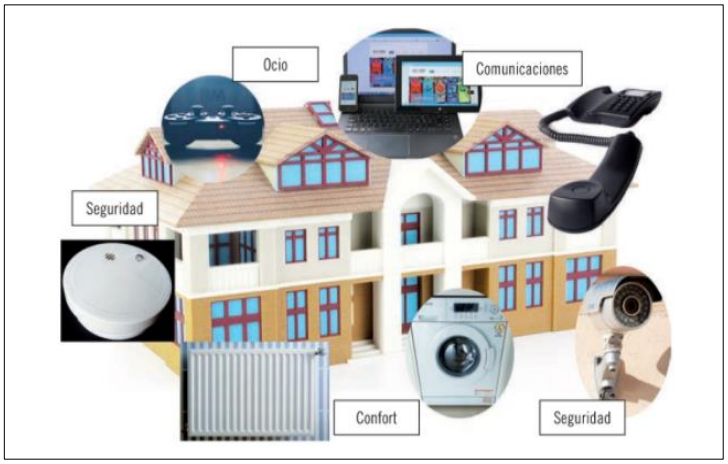


Figura 1-1: Principales elementos de un sistema domótico.

Fuente: Tobajas, 2014, p.5.

La domótica permite aplicar este concepto en varios elementos de una casa, mientras que la Inmótica se enfoca en aplicarlo a edificios, como locales comerciales, hoteles, hospitales y edificios en general (Tobajas, 2014, p. 7).

Al momento de implementar estos servicios es importante cumplir con los siguientes objetivos:

- **Confort. –** Dar comodidad al usuario al realizar actividades dentro de su domicilio.
- **Gestión energética. -** Permite regular, programar y optimizar la cantidad adecuada de energía a utilizar para desarrollar las actividades del hogar con el mínimo costo.
- **Comunicación. -** Permite la interacción entre los dispositivos de la instalación, además permite el acceso a la vivienda desde el exterior.
- **Seguridad. -** Consiste en una red encargada de salvaguardar tanto bienes como la seguridad de las personas que se encuentran en el inmueble.

1.1.1. Tipología

En cualquier proyecto de domótica, es necesario encontrar y determinar la forma de implementar los diferentes elementos de la instalación. Por tanto, se pueden distinguir diferentes tipos de arquitectura (Sánchez, 2017, p. 22):

- **Arquitectura centralizada**

Es aquella en la que los elementos de la instalación (sensores, actuadores) están conectados a una unidad central de control que se encarga de procesar toda la información que recibe. En la Figura 2-1 se observa gráficamente este tipo de arquitectura (Tobajas, 2014, p. 16).

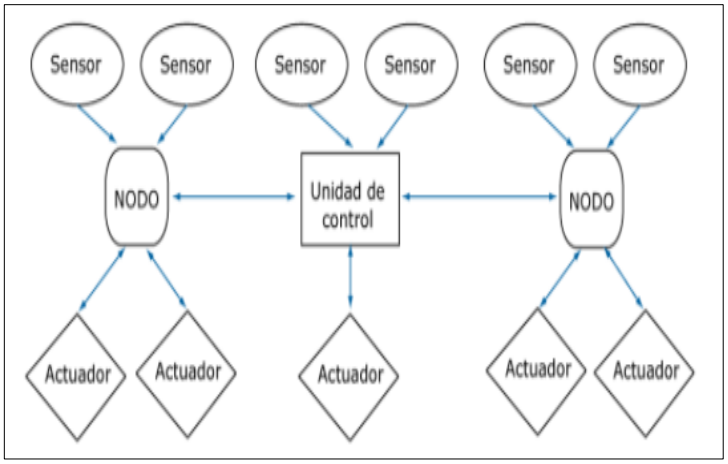


Figura 2-1: Diagrama de la arquitectura centralizada.

Fuente: Tobajas, 2014, p.16.

- **Arquitectura descentralizada**

Es aquella en la que existe más de una unidad de control, en la que cada control actúa de forma independiente tal como se observa en la Figura 3-1, en esta arquitectura se debe estandarizar la comunicación a través de protocolos y ya no se requiere de mucho cableado (Tobajas, 2014, p. 17).

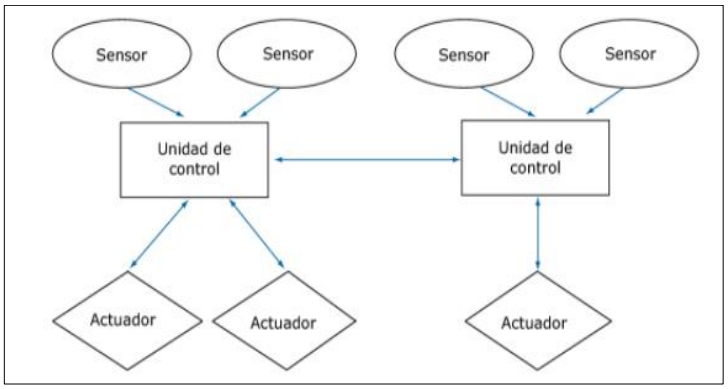


Figura 3-1: Diagrama de la arquitectura descentralizada.

Fuente: Tobajas, 2014, p.17.

- **Arquitectura distribuida**

Es aquella que se compone de las dos arquitecturas mencionadas anteriormente como se observa en la Figura 4-1. Las unidades de control se pueden comunicar mediante buses de comunicación, wifi, bluetooth o radio frecuencia para intercambiar información (Tobajas, 2014, pp. 17-18).

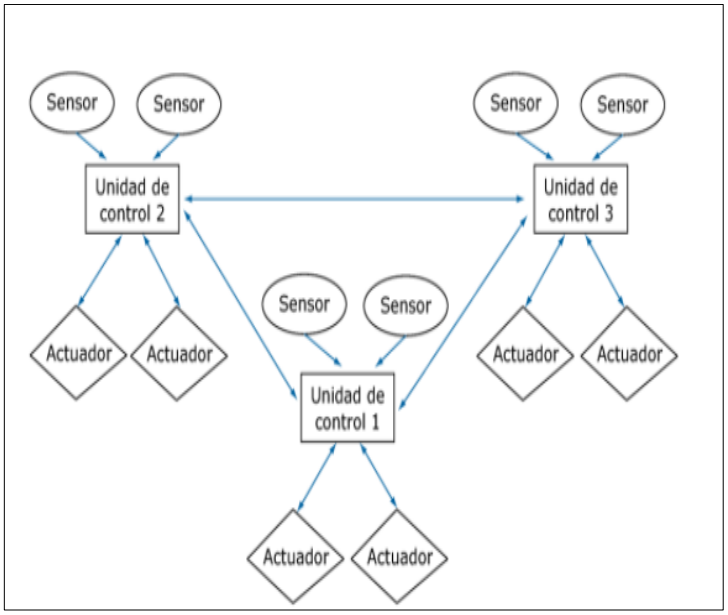


Figura 4-1: Diagrama de la arquitectura distribuida.

Fuente: Tobajas, 2014, p.18.

En la Tabla 1-1 se detalla las principales ventajas y desventajas de las arquitecturas mencionadas, debido a que se realizar un módulo que se encargara de la seguridad del hogar, es recomendable utilizar la arquitectura centralizada, ya que se utilizara una tarjeta de desarrollo que realizara la

función de la unidad de control y es la única encargada de procesar la información y realizar las tareas programadas.

Tabla 1-1. Ventajas y desventajas de las arquitecturas domóticas.

Arquitectura	Ventajas	Desventajas
Centralizada	-Fácil instalación. -Son más económicas. -Ideal para un sistema residencial.	-Su funcionamiento depende exclusivamente de la unidad de control, si esta deja de funcionar, el sistema también. -Tiene una capacidad limitada ya que son cableados.
Descentralizada	-Ofrecen mayor seguridad en su funcionamiento. -Es más sencillo ampliar este sistema.	-Ya que usa buses de comunicación, se requiere de un protocolo de comunicación y no todos los dispositivos son compatibles. -Al requerir más elementos para comunicarse suelen ser más costosos.
Distribuida	-Los elementos trabajan de forma autónoma.	-Es mucho más complejo y requiere mayor conocimiento. -Son más costosos.

Realizado por: Caiza H., Yanza A., 2021.

1.1.2. Elementos de un módulo domótico

Cuando hablamos de un módulo domótico, no nos referimos a un único elemento aislado que lo contiene todo, sino al contrario, se trata de un conjunto de elementos interconectados que se configuran de forma específica para realizar las tareas que desee el usuario (Bermúdez y Navas, 2015, p. 15). Para ello es necesario conocer los siguientes conceptos:

- **Señal de entrada. -** Son las señales que permiten al controlador tomar decisiones, estas son proporcionadas por sensores, pueden ser digitales o analógicas.
- **Señal de salida.** - Es la respuesta del sistema como consecuencia de la señal de entrada, al igual que la anterior puede ser digital o analógica.
- **Sensores.** - Transforma una magnitud física (luminosidad, temperatura) en una magnitud eléctrica.
- **Actuadores. –** Realiza una acción en respuesta a la información recibida por parte del controlador.
- **Controlador.** – Es la unidad central de una instalación domótica, se encarga de procesar las señales y tomar las acciones programadas. En otras palabras, es un ordenador con un software diseñado para la gestión de la instalación (Bermúdez y Navas, 2015, p. 33).

- **Sistema de respaldo de alimentación. –** Permite que el módulo funcione de forma independiente de la red doméstica, ya sea de forma continua o por un tiempo limitado.

1.1.3. Seguridad

Es el campo que más importante en instalaciones domóticas ya que se contempla la protección de las personas y los bienes de las mismas, en dicha área la utilización de equipos de control especialmente cámaras de video y sensores en su mayoría son aplicados no solo a la seguridad ante robos e intrusiones al hogar, sino también ante fugas de gas, detección de incendios, escapes de agua, entre los más comunes (Alban, 2018, p. 10).

- **Elementos de un módulo de alarma y seguridad**

El propósito es brindar información sobre cualquier tipo de problema que pueda ocurrir en el inmueble, brindar avisos o localizarlos dentro del alcance de las capacidades del sistema (Jiménez, 2015). La mayoría de los módulos de seguridad cuentan con los siguientes elementos.

- **Sensores o detectores. -** Detector de incendio, de agua, de gas, de presencia, cámaras de video vigilancia, pulsadores de alerta.
- **Actuadores. –** Sirenas acústicas y luminosas, sistema contra incendios, sistema de apertura de puertas, ventanas, válvulas de agua y gas.
- **Controlador. –** Microcontroladores y tarjetas de desarrollo (Arduino, raspberry, esp32, fpga, etc.).

A continuación, se realizará una breve descripción de los elementos más comunes en los módulos de seguridad para proteger un inmueble:

- Detector de presencia. – Estos elementos son muy utilizados en sistemas de seguridad ya que detectan movimiento o presencia de personas. Por ello se suelen colocar tanto en la parte exterior como interior de la vivienda. Esto permite tomar decisiones al controlador, como activar sistemas de iluminación o alarmas (Sánchez, 2017, p. 43).
- Detector de intrusión. – Estos sensores suelen utilizarse para proteger el acceso a edificios como puertas y ventanas.
- Alarmas. – Su objetivo es poner en alerta a través de señales luminosas o acústicas cuando ocurra un problema. Dentro de los más usados en instalaciones domóticas son las sirenas (Sánchez, 2017, p. 63).
- Electrificador. – Es un dispositivo electrónico que se utiliza para energizar por lo general cercos eléctricos. Este dispositivo genera pulsos de alta tensión y han sido diseñados para no hacer daño a los seres vivos.

1.2. Sistema de Video Vigilancia

Es un recurso clave para la lucha contra la delincuencia e inseguridad. Tratando de responder a estas necesidades, la comunidad científica se centra en detectar, seguir a las personas, así como identificar su comportamiento. La videovigilancia tradicional consiste en monitorear el comportamiento, actividades y otros cambios en el entorno, por medio de operadores visuales del sistema que intentan proporcionar seguridad a la zona vigilada. En términos generales, la video vigilancia de una zona amplia y crítica requiere de un sistema de múltiples cámaras que sirvan para monitorear a las personas de forma constante (Moctezuma, 2016, p. 258).

1.2.1. Sistema de Videovigilancia IP

Es una tecnología de video vigilancia para la supervisión de diversos ambientes y operaciones que se ejecutan en su estructura interna. Su denominación de circuito cerrado se debe a sus componentes que se encuentran enlazados entre sí, donde se envían imágenes desde cualquier punto hacia otro en tiempo real. Este sistema permite la supervisión visual mediante la grabación del evento ocurrido (Fernández, 2017, p. 15). En la Figura 5-1 se visualiza un sistema CCTV IP en conjunto con los elementos que lo conforman. Estos son:

- Cámaras de red o cámaras IP
- NVR, Network Video Recorder o Grabador de Red
- Etapa de gestión y control de las imágenes
- La transmisión de toda la información se hace a través de la red IP

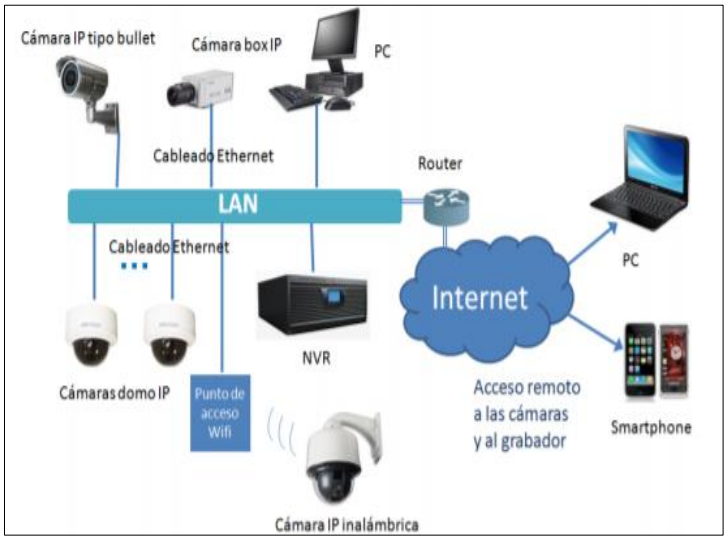


Figura 5-1: Sistema de videovigilancia IP.

Fuente: Martí 2013, p. 6.

Una de las grandes ventajas de estos sistemas es su acceso remoto, lo que significa que el usuario puede monitorear desde cualquier parte en cualquier momento, además que este puede ser escalable, es decir se pueden conectar un número limitado de cámaras ya sea de forma inalámbrica o a través de cables (Barreno, 2013, p. 37).

- **Sistema IP**

Se diferencia de otros por su resolución, formato digital (pixeles), y el detalle de no requerir una transformación. Es así que el sistema digital con cámaras IP como se observa en la Figura 6-1 indica, la conexión por medios físicos o vía inalámbrica a una red, junto con el NVR (Network Video Recorder o Grabador de Vídeo de Red) que permite grabar en tiempo real y administrar imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red. Este último es un poco caro, pero ofrece mayor calidad, menos ruido y mayor resolución. Puede ser un sistema basado en computadora o un sistema autónomo. Puede usar un cable UTP que es más barato que el RG59 o incluso wifi (Fernández, 2017, p. 15).

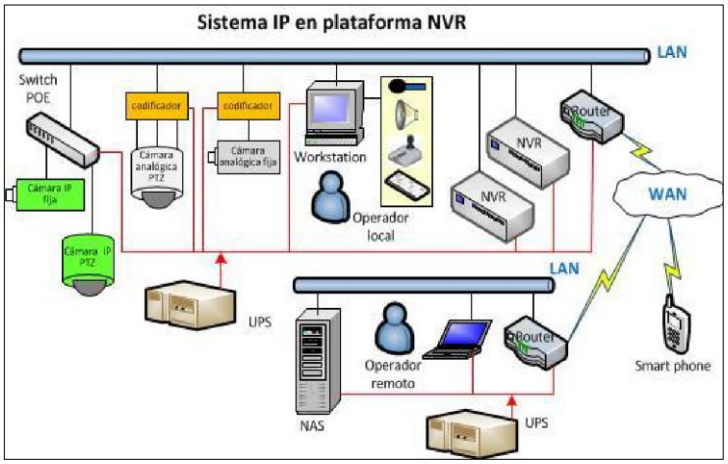


Figura 6-1: Sistema CCTV IP, (NVR).

Fuente: Fernández, 2017, p. 16.

- **Cámaras IP**

Este tipo de cámaras permiten visualizar en tiempo real, además pueden modificar sus movimientos lo que le permite ser un sistema más flexible y con más prestaciones que las cámaras analógicas (Barreno, 2013, p. 32).

Las cámaras IP facilitan la grabación de imágenes con secuencias o fotogramas, en formatos digitales para posteriormente hacer la verificación de los sucesos en las zonas vigiladas (Fernández 2017, pp. 16-17). En la Figura 7-1 se puede observar un ejemplo de una cámara IP de la marca Sony, es fácil de instalar y resistente a los cambios del tiempo, además la mayoría de cámaras permiten grabar imágenes en buena calidad bajo poca iluminación por lo que resulta ideal para una amplia

gama de actividades de vigilancia y seguridad en exteriores: desde centros urbanos, sistemas de transporte y centros comerciales a centros educativos y universidades (Barreno, 2013, p. 33).

Figura 7-1: Cámara IP Sony SNC-EB642R.

Fuente: SONY, 2020.

1.2.2. Video vigilancia inteligente

La principal diferencia entre el sistema tradicional y el sistema de video vigilancia inteligente radica en el análisis automático de la escena, este análisis puede comprender diferentes tareas importantes para la seguridad en general, algunas de estas tareas son: detección, seguimiento e identificación de persona, objetos, análisis del comportamiento de las personas, análisis de las trayectorias, entre otras. La identificación de personas es una de las principales tareas de un sistema de video vigilancia inteligente, para ello, normalmente se utilizan características biométricas que son aquellos rasgos fisiológicos que son únicos a los seres humanos como la cara, la huella dactilar, la voz, la retina, etc. Estas características pueden ser obtenidas mediante algoritmos de visión artificial (Moctezuma, 2016, p. 259).

1.3. Visión artificial

Es una disciplina que intenta imitar la capacidad de algunos seres vivos para observar y comprender escenas. El problema que trata suele consistir en extraer determinada información de la escena (habitualmente captando esta información en forma de imágenes) para poder tomar determinadas decisiones posteriormente. La visión artificial propone una serie de tecnologías diseñadas para realizar tales tareas (Vélez, 2003, p. 16).

1.3.1. Aplicaciones y métodos de visión artificial

Los patrones deben ser verificados mediante un control de precisión establecido para la selección de objetos, creando un sistema exacto para no tener errores ni variabilidades en la comparación y extracción de diversos objetos (Ludeña, 2019, p. 6).

1.3.2. LBPH

El método de patrones binarios locales fue diseñado para describir la textura. Para el uso de descripciones locales en ciertas áreas de la cara, puede proporcionar más información que otras, por lo que el descriptor de texturas tiende a promediar la información que describen, lo cual no es inconveniente cuando se describen caras porque es importante mantener la información sobre las relaciones espaciales. Para formar una descripción general del rostro, las imágenes faciales se dividen en diferentes regiones aplicando un histograma para obtener el operador LBPH, que describe la información independiente por área. Luego, conecta estas descripciones para construir una descripción general del rostro (Esparza et al. 2017, p. 148). El método de LBPH asigna etiquetas a cada píxel de la imagen, teniendo en cuenta la distribución de los píxeles aledaños, para lo cual ejecuta ciertos pasos descritos a continuación.

- Una máscara de tamaño determinado (8x8), recorre la imagen de manera iterativa seleccionando cada vez un píxel central y sus vecinos.
- Este píxel central se compara con cada uno de sus vecinos de forma ordenada. Se asigna un 1 cada vez que el píxel central sea menor que el pixel comparado y un 0 en el caso contrario, descrito matemáticamente en la ecuación 1 y como se observa gráficamente en la Figura 8-1 (Esparza et al. 2017, p. 148).
- El número binario que resulta, se convierte en un número decimal, que es contado en el histograma para formar la descripción. El histograma de todos los píxeles posteriormente es usado como la descripción de la textura de la imagen descrito en la ecuación 2 (Esparza et al., 2017).

$$LBP = \sum_{p=0}^{7} 1\, s(g_p - g_c) 2^p \qquad (1)$$

$$s(x) = \{1, \quad si\ x \geq 0\ \ 0,\ \ otro\ valor$$

Al analizar los diferentes parámetros en la extracción de la representación de la cara, notamos una relativa insensibilidad a la elección del operador LBP y el tamaño de la región. Este es un resultado interesante ya que los otros enfoques considerados son más sensibles a sus parámetros libres. Esto significa que solo se necesitan cálculos simples para la descripción del LBP, mientras que algunos otros métodos utilizan un entrenamiento exhaustivo para encontrar sus parámetros óptimos. Los resultados experimentales muestran claramente que el método basado en LBP supera a otros enfoques ya logró una tasa de reconocimiento del 97% en el caso de reconocer rostros bajo diferentes expresiones faciales, mientras que el mejor rendimiento entre los métodos probados no superó el 90%. (Ahonen et al., 2004, p. 480)

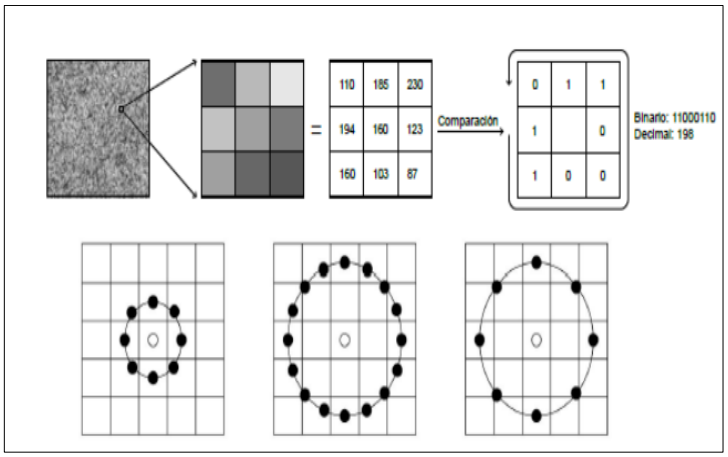


Figura 8-1: Obtención de los parámetros LBPH.

Realizado por: (Esparza et al. 2017, p. 148).

$$H_i = \sum_{xy}^{7} 1\, I[LBP(x,y) = i], \qquad i = 0, \dots, n-1 \qquad (2)$$

$$I(x) = \{1, \qquad si\ x\ es\ verdadero\ \ 0, \ \ otro\ valor$$

Aplicaciones:

- Identificación de objetos
- Ubicación de la posición de objetos
- Determinación de relaciones entre objetos
- Establecer coordenadas entre varios objetos
- Mediciones tridimensionales

Los resultados deben ser precisos y fiables, el sistema de localización de objetos debe comparar de manera rápida la forma de los objetos en líneas de producción.

1.3.3. Algoritmos de detección de rostros de rostros

El sistema de reconocimiento facial es una aplicación para identificar personas mediante fotografías o videos en base a sus características biométricas. El reconocimiento facial se divide en tres niveles: detección facial, extracción de características y reconocimiento facial como se observa en la Figura 9-1 (Senthilsingh C y Manikandan, 2014, p. 707).

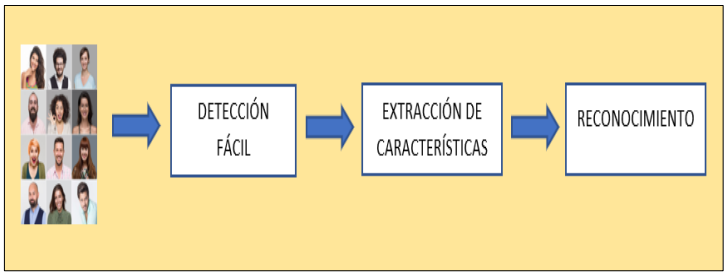


Figura 9-1: Etapas del reconocimiento de rostros.

Realizado por: Caiza H., Yanza A., 2020.

Principalmente existen dos tipos de reconocimiento: intrusivo y no intrusivo en el intrusivo el usuario está consciente sobre el reconocimiento, por ejemplo, el escaneo del iris del ojo mientras que el reconocimiento facial es no intrusivo ya que sin la necesidad de que la persona coopere puede ser identificada para ser autentificado (Senthilsingh C y Manikandan, 2014, p. 708). Existen varios algoritmos para la detección de rostros, pero el algoritmo propuesto por (Viola y Jones, 2001, p. 1) permite realizar este proceso de forma rápida.

- **Algoritmo Viola-Jones**

Es un método de aprendizaje autónomo para la detección visual de objetos, que puede procesar imágenes rápidamente y tiene un alto promedio de detección de objetos en tiempo real (Viola y Jones 2001, p. 2) por lo cual es muy utilizado en sistemas de detección de rostros. Esto es posible debido a tres aspectos claves.

1. Utiliza una nueva representación de la imagen denominada imagen integral.
2. Utiliza el algoritmo AdaBoost.
3. Utiliza clasificadores en cascada.

El concepto de imagen integral permite cálculos muy rápidos mediante la conversión previa de todos los píxeles de la imagen, con el objetivo de generar una matriz sobre la que se realizan los cálculos de las características Haar que son una característica rectangular simple utilizada como clasificador en cascada. (Viola y Jones, 2001, p. 3). En la Figura 10-1 se muestran estas características.

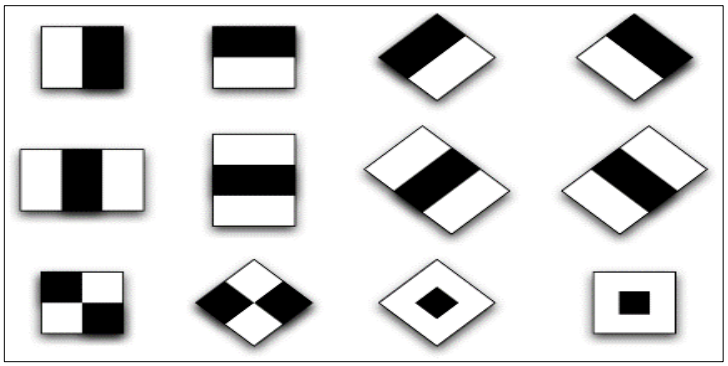


Figura 10-1: Características Haar.

Realizado por: Viola y Jones 2001, p. 2.

En el área especial de la imagen, las sumas de píxeles debajo de las áreas blancas se restan de las sumas de píxeles debajo de las áreas negras. Es decir, el peso del área blanca y negra se puede considerar como "1" y "-1", respectivamente (Gonzalez y Velásquez, 2019, p. 57). Este procedimiento se observa en la Figura 11-1 donde se observa como las características Haar se usan en la imagen.

Figura 11-1: Detección de rostros aplicando características Haar.

Realizado por: Viola y Jones, 2001, p. 4

Para la parte del clasificador cada uno es entrenado para detectar rostros con las características Haar conocido como AdaBoost que es un método de clasificación que combina varios clasificadores básicos para formar un clasificador único, más complejo y preciso. La idea se basa en que, siempre que haya una cantidad suficiente de muestras de entrenamiento disponibles, se pueden combinar varios clasificadores simples para formar uno de precisión mayor (Gonzalez y Velásquez 2019, p. 60).

Estos clasificadores se aplican en cascada en una región de interés para poder detectar un rostro, descartando rápidamente las regiones que no incluyen un rostro, una región se considera un rostro solamente si cada uno de los clasificadores aprueba que es un rostro (Jacobo, 2016, p. 29).
(Viola y Jones 2001, p. 4) Utilizan un enfoque de ventana deslizante en el que se deslizan ventanas de varias escalas a lo largo de toda la imagen. El factor de escala y el tamaño del paso de cambio son parámetros que debe decidir.

La extracción de características se utiliza para obtener información relacionada para realizar la comparación. En las últimas décadas se han desarrollado una gran cantidad de algoritmos en el campo del reconocimiento facial.

- **Identificación del rostro.**

Luego de realizar el proceso de detección de rostros viene la parte más complicada que es el de la identificación del mismo. El reconocimiento facial es el campo del reconocimiento de patrones, que se ha estudiado durante varios años. Para lograr este objetivo se realizan diferentes pasos:

- *Preprocesamiento de imágenes*. – En esta parte mediante el algoritmo de detección se puede extraer únicamente el rostro de la imagen captada por la cámara.
- *Extracción de características*. - La extracción de características es una de las etapas de las que depende el rendimiento de un sistema de reconocimiento facial. El objetivo principal de esta etapa es extraer la información más distintiva del rostro para eliminar información innecesaria (Valvert 2006, pp. 6-7). Dentro de las más comunes es la extracción de componentes básicos del rostro, así como relacionar la distancia que existe entre los ojos, nariz, boca, que son las características que más se diferencian en un rostro. En este trabajo se utilizará el algoritmo de Patrones Binarios Locales (LBP), ya que ampliamente utilizado en el reconocimiento de rostros (Gonzalez y Velásquez, 2019, p. 61).
- *Entrenamiento*. - Consiste básicamente en utilizar alguna forma de aprendizaje para que el sistema aprenda las caras que constituyen el conjunto de formación. El tipo de entrenamiento que se utilizará dependerá del método utilizado para la identificación.
- *Reconocimiento*. – En la última parte al módulo ingresaran imágenes que con diferentes rostros tantos los usados para el entrenamiento como otras diferentes, de tal modo que nos permite determinar la eficiencia del algoritmo utilizado.

Para evaluar la calidad de la predicción de un modelo entrenado previamente se puede usar la matriz de confusión la cual basa su análisis en la clasificación de los resultados reales o de predicción, donde las filas representan los valores de predicción y las columnas los reales de cada evento ya sean positivos o negativos descritos en el Capítulo III haciendo uso de la métrica de precisión y exactitud del algoritmo de visión artificial (Oñate 2020, p. 18). Los parámetros a considerar son:

- *True Negative [TN],*
- *True Positive [TP],*
- *False Positive [FP],*
- *False Negative [FN]*.

Estos parámetros permiten el cálculo de la precisión y exactitud en base a la ecuación (3) y (4) respectivamente.

$$precision = \frac{TP}{TP + FP} \qquad (3)$$

$$accuracy = \frac{(TP + TN)}{TP + TN + FP + FN} \quad (4)$$

1.4. Entorno de programación para el procesamiento de imágenes

Para realizar el procesamiento de imágenes que permita detectar el rostro se requiere de un entorno de programación que permita ejecutar el código apropiado para procesar la información. A continuación, se mencionan los más importantes.

1.4.1. Open CV

Es una biblioteca establecida por Intel en 1999, es multiplataforma por lo que se utiliza principalmente para sistemas de procesamiento de imágenes en tiempo real, incluidos los últimos algoritmos de visión por computadora (Thakur et al., 2020, p. 11799).

La librería Zopenca se puede integrar con diferentes lenguajes de programación, como C ++, Java, Python, por lo tanto, se puede utilizar para desarrollar aplicaciones para entornos web o de escritorio, además nos permite entrenar nuestros propios clasificadores para el reconocimiento de rostros. Es por ello que es muy usado en entornos de programación como Python, Matlab, LabVIEW, entre otros (Caballero, 2017, p. 32).

1.4.2. Matlab

MATLAB es un programa que contiene cientos de comandos matemáticos. Puede usarlo para dibujar gráficos de funciones, resolver ecuaciones, realizar pruebas estadísticas y más. Es un lenguaje de programación de alto nivel que puede comunicarse con otro tipo de lenguaje, como FORTRAN y C (Wilkinson 2003, p. 3). Además, cuenta con múltiples herramientas, entre ellas "Image Processing Toolbox" para el procesamiento de imágenes.

Esta herramienta contiene un conjunto completo de algoritmos estándar de referencia y aplicaciones de flujo de trabajo para el procesamiento, análisis y visualización de imágenes, y desarrollo de algoritmos. Puede realizar segmentación de imágenes, mejora de imágenes, reducción de ruido, transformación geométrica, registro de imágenes y procesamiento de imágenes en 3D, también es compatible con la librería OpenCV (Math works, 2020).

1.4.3. LabVIEW

Es un lenguaje y también un entorno de programación gráfica en el que se pueden crear aplicaciones de forma fácil y rápida, desarrollada por National Instruments y orientado para proyectos de instrumentación virtual. Posee dos ventanas principales que reciben el nombre de Panel Frontal y Diagrama de Bloques respectivamente (Lajara 2008, p. 4).

- Panel Frontal, es la parte que verá el usuario, suele tener fondo gris.
- Diagrama de Bloques, es donde se realizará la programación y suele tener fondo blanco.

En dichas ventanas se presenta el entorno de trabajo y los menús de herramientas, controles y funciones. Además, hay que considerar, estructuras, tipos de datos, manejo de ficheros, comunicación serie, adquisición de datos, protocolos de comunicación, acceso remoto VI server y comunicaciones avanzadas, sin ser menos importante la organización y el modelo de programación (Lajara, 2008, p. 4). Al igual que Matlab, este cuenta con varias herramientas para el procesamiento de imágenes.

El módulo Visión Development es usado para adoptar un enfoque abierto y adaptable para el desarrollo de software de visión artificial. Se puede elegir el hardware adecuado para su aplicación y configurar cámaras, adquirir imágenes y analizar resultados de inspección para desarrollar sistemas de visión artificial totalmente personalizados. Ayuda a utilizar la potencia de la programación gráfica para abordar una variedad de retos de desarrollo e implementación en aplicaciones de visión artificial (NATIONAL INSTRUMENTS CORP 2020).

Muchos algoritmos de procesamiento de imágenes son de naturaleza paralela, por lo que son adecuados para la implementación de tarjetas de desarrollo. Estos algoritmos que implican operar en píxeles, líneas y regiones de interés no requieren información de imagen avanzada, como patrones. Puede realizar estas funciones en áreas pequeñas y múltiples áreas de la imagen al mismo tiempo. Puede pasar datos de imagen a la tarjeta de desarrollo en paralelo y procesar los datos al mismo tiempo, porque no se requiere una unidad central de procesamiento para procesar los datos. El Módulo NI Vision Development contiene más de 50 funciones de procesamiento de imágenes (NATIONAL INSTRUMENTS CORP 2020).

1.4.4. Entornos que usen el lenguaje Python

Python es un lenguaje interpretado de alto nivel que se centra en la legibilidad y la facilidad de aprendizaje y uso. Python es un lenguaje multiplataforma, lo que significa que se puede usar en muchos sistemas diferentes. Puede ejecutarse en computadoras equipadas con Linux, BSD, Apple, Windows y muchos otros sistemas operativos, pero también hay versiones para otros dispositivos, como terminales de teléfonos inteligentes (Hinojosa 2015, p. 21).

Una de sus principales ventajas es que es un software libre, es decir no requiere de una licencia pagada para su uso ya sea privada o comercial, al ser un software libre se puede usar gratuitamente y desarrollar cualquier tipo de aplicación. Esto le permite brindar a toda la comunidad

oportunidades para beneficiarse y modificar los programas. Para hacer esto, se debe acceder al código fuente.

Python es un lenguaje completo con funciones completas, muy poderoso y viene con una serie de paquetes de software que brindan casi todas las funciones que puedes usar. Para lo que respecta a visión artificial es común utilizar la librería OpenCV ya que brinda muy buenos resultados.

- **Comparativa de los entornos de programación descritos.**

Los sistemas mencionados anteriormente ofrecen muchos beneficios para para esta investigación se utilizará OpenCV y Python como entorno para realizar el procesamiento de imágenes, ya que tanto Matlab como LabVIEW requieren de una licencia de alto costo lo cual limita a los demás usuarios. Mientras tanto OpenCV y Python son entornos libres cuya licencia es gratuita y tienen un alto rendimiento en el procesamiento indispensable para el procesamiento de imágenes.

1.5. Tarjetas de desarrollo para procesamiento de imágenes.

Desde el punto de vista de la ingeniería, es una herramienta destinada para el diseño y prototipado rápido de sistemas digitales o analógicos, dado que reduce el tiempo de verificación de las funciones del prototipo, la tarjeta de desarrollo es un elemento muy útil para aportar soluciones o mejoras en el prototipo (Cárdenas, Andrés y Gómez, 2013, p. 2).

1.5.1. Arduino

Arduino es un dispositivo de hardware libre que monta un microcontrolador en una placa de circuito impreso con los elementos necesarios para su funcionamiento y que dispone de un entorno de programación libre junto con un lenguaje de programación propio (Moreno, 2018, p. 26). Varios modelos de placa Arduino circulan por el mercado internacional, pero todos tienen en común la arquitectura tipo AVR de microcontroladores que incorporan, desarrollada y fabricada por Microchip.

1.5.2. Raspberry PI

Es un ordenador de placa reducida de bajo costo que cuenta con un procesador de arquitectura ARM (máquina RISC de Arcon) cuya principal característica es el bajo consumo energético, con el objetivo de estimular la enseñanza de ciencias de la computación (López 2017, p. 39).

Las características principales de este producto incluyen un procesador de dos núcleos de 64 bits de alto rendimiento, soporte de pantalla dual a resoluciones de hasta 4K a través de un par de

puertos HDMI micro tipo D, decodificación de video por hardware hasta 4Kp60, hasta 8GB de RAM, LAN inalámbrica de banda dual de 2,4 / 5,0 GHz, Bluetooth 5.0, Gigabit Ethernet, USB 3.0, y capacidad PoE que es una tecnología que combina señales de datos y energía en una sola conexión de cable Ethernet para realizar el funcionamiento de dispositivos con alimentación remota (RASPBERRY PI FOUNDATION 2020).

La LAN inalámbrica de banda dual y Bluetooth tienen certificación de cumplimiento modular, permitiendo que el tablero se diseñe en productos finales con una reducción significativa pruebas de cumplimiento, mejorando tanto el costo como el tiempo de comercialización.

1.5.3. FPGA

FPGA es un dispositivo que nos permite describir circuitos digitales en un lenguaje específico (los dos más comunes son VHDL y Verilog), una vez cargado en el chip, se puede crear físicamente en el chip. Su nombre es un acrónimo en inglés, que significa arreglos de compuertas lógicas programables o Field Programable Gate Array (Crespo 2017).

En su interior se encuentran compuertas lógicas, biestables y puertos de entrada y salida sin conectar, los cuales se conectarán según el circuito diseñado. Una de sus ventajas es que puede ejecutar múltiples tareas a la vez, por lo cual son mucho más rápidas que los microcontroladores debido a que estos ejecutan las tareas de forma secuencial.

Para el desarrollo del módulo se optó por utilizar una tarjeta de la familia Raspberry, ya que al ser un microcomputador nos permite instalar un sistema operativo lo cual no requiere de un ordenador para realizar el procesamiento, también su alta velocidad de procesamiento es fundamental para poder trabajar con datos en tiempo real a su vez es compatible con el lenguaje de programación Python que permite utilizar la librería OpenCV para la identificación de rostros.

CAPÍTULO II

2. MARCO METODOLÓGICO

Para la implementación de un módulo domótico de seguridad residencial aplicando técnicas de visión artificial es indispensable mencionar los tipos de hardware y software apropiados para para el correcto desarrollo del módulo detallando las características técnicas de los elementos a utilizar.

2.1. Requerimientos para el diseño del prototipo

De acuerdo al estudio realizado en el capítulo anterior se identificaron los requerimientos que debe cumplir el módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros, los cuales se enlistan a continuación.

- El módulo permite conectividad a internet.
- Obtención de imágenes con una resolución adecuada para su procesamiento.
- Permite obtener imágenes con una adecuada resolución en condiciones de baja luminosidad.
- Debe ser compacto, modular y escalable.
- Establecer el alcance máximo para el correcto funcionamiento del módulo.
- Capacidad de almacenar información.
- Que permita la conectividad de 1 cámara de videovigilancia IP.
- Emitir mensajes de alerta en tiempo real a aplicaciones de mensajería instantánea.

2.2. Concepción de la arquitectura general del prototipo.

La concepción general del módulo de seguridad domótica usando técnicas de visión artificial se observa en la Figura 1-2, donde se aprecia los diferentes elementos que lo conforman para la detección, monitoreo y alerta en tiempo real en un ambiente residencial.

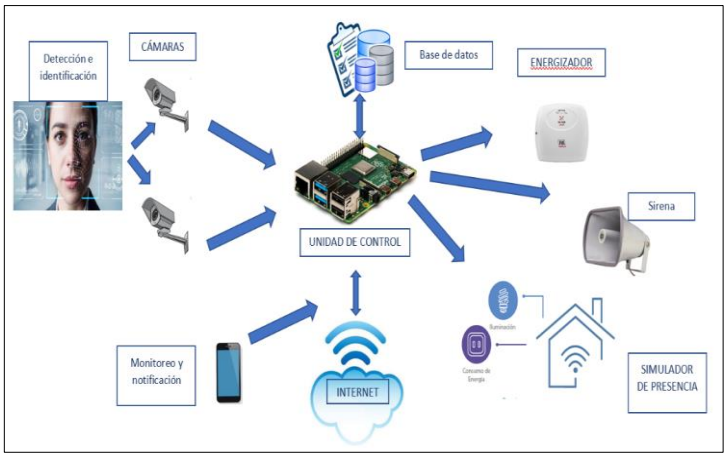


Figura 1-2: Concepción de la arquitectura general del prototipo.

Realizado por: Caiza H., y Yanza A., 2021.

El módulo estará compuesto por una cámara comercial de un sistema de video vigilancia convencional y sensores los cuales se ubicaran en lugares estratégicos con el objetivo de garantizar el correcto funcionamiento de la cámara para que tenga un rango amplio de visión sin obstrucción alguna, y garantizar una imagen clara, además proveerán de información de los exteriores de la vivienda, y a su vez se enviará esta información a la tarjeta de desarrollo raspberry Pi 4 que se encargará de procesar las imágenes y las compararlas con imágenes registradas en una base de datos ubicado en la nube, el módulo permitirá al usuario configurarlo en dos modos, el primero consiste en notificar al dueño del inmueble la presencia de intrusos cuyos rostros no se encuentren registrados, esto se logra mediante un algoritmo de procesamiento de imágenes que compare los rostros obtenidos por la cámara de seguridad con los almacenados, y de manera inmediata se activará una alarma, a su vez se bloqueara el acceso.

El segundo modo se activará cuando el domicilio se encuentra deshabitado, este realizará las acciones mencionadas en el primer modo, además de electrificar cerraduras de puertas y marcos de ventanas con el objetivo de garantizar la seguridad del domicilio y de igual manera se simulará la presencia de personas activando ciertos electrodomésticos y luces de la casa. La arquitectura que se utilizará para el desarrollo de este módulo será centralizada ya que cada elemento se conecta a la tarjeta de desarrollo permitiendo y al contar con conexión internet permite su monitoreo en tiempo real.

2.3. Diseño de los bloques del prototipo

Al tener definida la concepción de la arquitectura general del prototipo se detalla el diseño y construcción de cada bloque que se da a conocer en la Figura 2-2 que integra al módulo domótico de seguridad residencial aplicado técnicas de visión artificial para la identificación de rostros.
El diagrama de bloques que se observa en la figura, está compuesto por cinco bloques:

- **Imágenes:** se encarga de obtener una serie de imágenes en formato jpg mediante la cámara de seguridad IP hikvision que se encuentre ubicada estratégicamente en las inmediaciones de la vivienda para su posterior procesamiento en la tarjeta de desarrollo Raspberry Pi.
- **Alimentación:** provee de energía al módulo de seguridad y a los elementos externos como alarmas, luces y cargas especiales, mediante una fuente conmutada AC-DC de 12V a 10 Amp.
- **Detección, identificación y procesamiento:** está compuesto por una Raspberry Pi 4 modelo B que posee múltiples entradas, conexión a internet la cual permite detectar identificar y procesar la imagen mediante un algoritmo que se encuentra desarrollado en el sistema operativo Raspbian.

- **Monitoreo:** la información procesada es enviada al contacto registrado por el usuario mediante telegram en caso de que el rostro detectado no conste en la base de datos y podrá observar el comportamiento del sujeto mediante acceso en tiempo real a la cámara de seguridad.
- **Actuadores:** está compuesto por sirenas, electrificadores, sensores de movimiento que activan un protocolo de seguridad en caso de vulnerar el interior del domicilio.

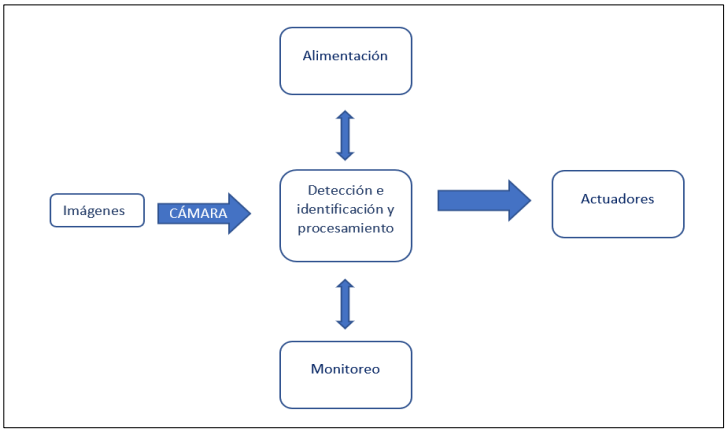


Figura 2-2: Diseño de los bloques del prototipo.

Realizado por: Caiza H., y Yanza A., 2021.

2.4. Requerimientos de hardware del sistema

2.4.1. Raspberry Pi 4 Modelo B

Salió al mercado en el 2019 y al igual que los modelos anteriores es un ordenador de placa simple y de bajo costo desarrollado en reino unido cuyo principal objetivo es la enseñanza de la computación en las escuelas Figura 3-2, tiene la misma funcionalidad que las computadoras convencionales por lo que puede ser usado en múltiples proyectos, además al ser de software libre ayuda en la enseñanza y mejorar las habilidades de la programación. Dispone de un sistema operativo basado en Linux denominado Raspberry Pi OS, la fuente de alimentación se conecta a través de un puerto microUSB tipo C y debe proporcionar 5V DC y una corriente nominal de 3A para su correcto funcionamiento (López 2017, p. 40). Cuenta con dos puertos microHDMI, tiene la capacidad de manejar una pantalla a 4k de 60Hz, o dos de 30Hz a 4k, además de características descritas en la Tabla 1-2 en relación a los modelos anteriores.

Losa pines GPIO es una de la característica más poderosa de las Raspberry Pi ya que cuenta con 40 pines distribuidos en la placa, y cualquiera de estos pines mediante software se puede designar como entrada o salida y usarse para múltiples propósitos.

Figura 3-2: Puertos principales de Raspberry Pi 4 model B.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 1-2: Modelos actuales de Raspberry Pi y sus características.

Especificaciones	Raspberry Pi 3 modelo B+	Raspberry Pi 3 modelo A+	Raspberry Pi 4 modelo B
SoC (Sistema en chip)	Broadcom BCM2837		Broadcom BCM2711
GPU (Unidad de Procesamiento gráfico)	Broadcom VideoCore IV, OpenGL ES 2.0, MPEG-2		Broadcom VideoCore VI, OpenGL ES 3.0
RAM	1GB LPDDR2 (Low-Power Double Data Rate) SDRAM	512MB LPDDR2 (Low-Power Double Data Rate).	1/2/4/8GB LPDDR4 (Low-Power Double Data Rate) SDRAM
Puerto USB 2.0.	4	1	2
Puerto USB 3.0.	2	0	2
Puertos GPIO	Disponible 40 pines		
Almacenamiento	microSD		
Video y Sonido	Dos puertos micro-HDMI que admiten pantallas de 4K a 60Hz a través de HDMI 2.0, puerto de pantalla MIPI DSI, puerto de cámara MIPI CSI, salida estéreo de 4 polos y puerto de vídeo compuesto.		
Alimentación	5V/3A	5V/2.5A	5V/3A
Peso	45g	23g	45g
Tamaño		85mm x 53mm	

Realizado por: (Caiza H., y Yanza A., 2021).

2.4.2. Módulo Relé 12v 4 Canales Nivel Alto Bajo.

Utilizado para el manejo de cargas de alta potencia, cuenta con cuatro canales como se observa en la Figura 4-2, que permite el encendido y apagado de luces, alarmas y electrificadores, el módulo se activa mediante una señal de 12V, soporta una carga máxima en NA de 250V/10Amp AC y 30V/10Amp DC, la luz indicadora verde representa la alimentación y la luz indicadora roja el estado del relé. Las características se observan en la Tabla 2-2.

Figura 4-2: Módulo relé 12v cuatro canales.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 2-2: Características técnicas del módulo relé de cuatro canales

Parámetros	Especificaciones
Canales de salida	Cuatro canales de salida
Corriente/Voltaje de conmutación	10A/250V-12A/125V 10A/30V-12A/28V
Voltaje de control	Min 5V – Max 12V
Led Indicador de PWR	Led color verde
Led Indicador de activación	Led color rojo
Tiempo de respuesta	10ms – 5 ms

Realizado por:(Caiza y Yanza, 2021).

2.4.3. Cámara IP HIKVISION DS-2CD1043G0-1 TIPO BALA

Usado para videovigilancia, en entornos tanto en el día como en la noche, con resolución de 4MP, posee control de ganancia automática el cual permite regular la intensidad de la señal para un nivel apropiado de visualización y grabación, es decir ajusta automáticamente la sensibilidad en cuanto a la iluminación para obtener una imagen balanceada. Permite también visualizar video y configuración de los parámetros de la cámara en línea mediante Software o Apps.

Se elige el dispositivo que se observa en la Figura 5-2, principalmente por la facilidad para ubicar en lugares externos alejados del módulo de seguridad lo que no se podría hacer con una cámara exclusiva para la Raspberry Pi 4.

Figura 5-2: Cámara IP HIKVISION DS-2CD1043G0-1 Tipo Bala.

Realizado por: Caiza H., y Yanza A., 2021.

En la actualidad es común observar este tipo de cámara en sistemas de video vigilancia domiciliarias por la relación costo beneficio que ofrece en el mercado, las características técnicas se describen en la Tabla 3-2.

Tabla 3-2: Características principales.

Parámetros	Especificaciones
Sensor de imagen	1/3" progressive scan CMOS
Resolución máxima	2560 × 1440 a 20fps
Longitud focal	2.8 mm, 4 mm, 6 mm
Apertura	F2.0
Infrarrojo	si
Rango de infrarrojo	30 m
Interruptor día / noche	Auto, programado
Reducción de ruido digital	3D DNR
Alimentación a través de Ethernet	si
Protocolos	TCP/IP, ICMP, HTTP, HTTPS, FTP, DHCP, DNS, DDNS, RTP, RTSP, RTCP, PPPoE, NTP, UPnP, SMTP, SNMP, IGMP, 802.1X, QoS, Ipv6 UDP, Bonjour
Interfaz de comunicación	1 RJ45 10M/100M self-adaptive Ethernet port
Condiciones de operación	-30°C a 50°C
Fuente de alimentación	12 VDC ± 25%, 5.5 mm coaxial power plug PoE (802.3af, class 3)
Consumo de energía y corriente	12 VDC, 0.4 A, Max: 5 W
Nivel de protección	IP67

Realizado por: Caiza H., Yanza A., 2021.

2.4.4. Hikvision DS-7104NI-Q1/M

NVR de cuatro canales como se observa en la Figura 6-2, con ancho de banda de grabación de entrada/salida de 40/60Mbps. Permite la visualización, almacenamiento y reproducción en vivo

de alta definición de hasta 6MP en IP el cual del cual se obtendrá la imagen para el procesamiento en el sistema de visión artificial. Las características técnicas se describen en la Tabla 4-2.

Figura 6-2: NVR HIKVISION.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 4-2: Características Técnicas.

Máximo número de canales	4
Puerto HDD	1
Capacidad máxima de disco duro	6T
Salda de monitorización	VGA+HDMI
Puertos POE	ninguno
Fuente de alimentación	12V
consumo	10W

Realizado por: Caiza H., Yanza A., 2021.

2.4.5. Fuente conmutada 12V-10Amp S120-12

Destinado para cargas que requieran una corriente continua del módulo domótico cuya entrada sea de 12V CD tanto para la alimentación o como señal de activación de los dispositivos como relés, cámaras de seguridad y sirena. La fuente cuenta con una estructura metálica con base de aluminio como se observa en la Figura 7-2 además posee protección contra sobrecargas y sobretensiones. Las características principales se describen en la Tabla 5-2.

Figura 7-2: Fuente 12v 10a metálico.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 5-2: Características principales.

Voltaje de salida	12v
Corriente Max.	10 Amp
Potencia nominal	120 W
Rizado y Ruido	120 mV P-P
Tiempo de activación	20 ms/VAC
Voltaje de entrada	110V/220V
eficiencia	Mayor al 80%

Realizado por: Caiza H., Yanza A., 2021.

2.4.6. Termomagnético EBS6BN.

Se aplica a sistemas de distribución de energía de baja tensión como en AC 50/60Hz, se utiliza como protección ante cortocircuito, sobrecarga y aislamiento Figura 8-2, además se aplica como estado de encendido y apagado dentro del tablero del módulo domótico de seguridad. Las características técnicas se describen en la Tabla 6-2.

Figura 8-2: Termomagnético EBASEE 6BN

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 6-2: Características técnicas.

Corriente nominal	1-63 Amp
Tensión nominal	240V
Disparo característico	BCD
Capacidad de ruptura	6000A
instalación	Carril din 35mm
Temperatura Max	-5/40°C
Nivel de protección	IP20

Realizado por: Caiza H., Yanza A., 2021.

2.4.7. Módulo Regulador Step Down Lm2596 3A

En un convertidor de reducción o buck típico como se observa en la Figura 9-2, la tensión de salida Vout depende de la tensión de entrada Vin y el ciclo de trabajo de conmutación D del

interruptor de potencia, el objetivo es producir una salida que sea continua pura (Hart, 2001). Permite tener un voltaje regulado a 5V a partir de una mayor 12V para el uso de microcontroladores, Arduino, PICs, Raspberry Pi, fuentes variables, drivers entre otros dependiendo de la aplicación. En la Tabla 7-2 se observan las características principales del módulo.

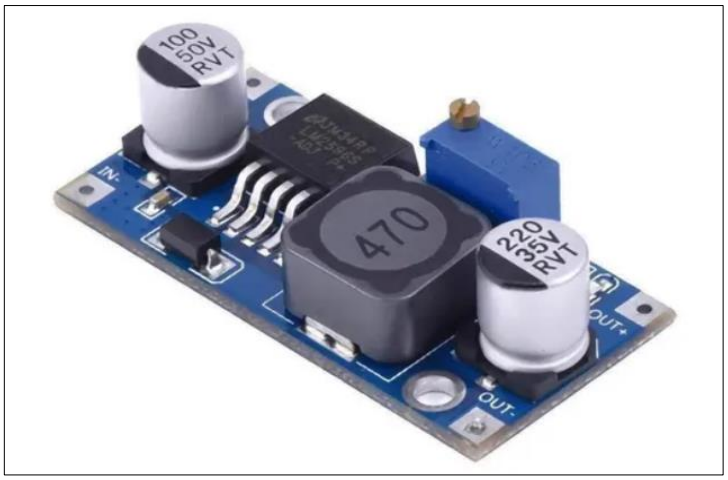


Figura 9-2: Módulo Regulador Step Down Lm2596 3Amp.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 7-2: Principales características.

Voltaje de entrada	4.5/40V
Voltaje de salida	1.5/35V (regulable)
Corriente de salida	3Amp máximo
Dimensiones	43x20x14 mm
Frecuencia de switching	150 KHz

Realizado por: Caiza H., Yanza A., 2021.

2.4.8. Electrificador JFL ECR-18

Permite cohibir la invasión de intrusos en el área protegida mediante electrificación de cercas ubicadas sobre o encima de muros, este dispositivo es parte del módulo domótico de seguridad con la finalidad de electrificar cerraduras y ventanas, este dispositivo que se observa en la Figura 10-2 no genera riesgos fatales a quien manipule el cableado ya que genera 0,5J que está dentro de los parámetros aceptados por la norma IEC 60335-2-76 que permite máximo Joules. En la Tabla 8-2 se describen las características técnicas más importantes para la instalación.

Figura 10-2: Electrificador ECR-18

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 8-2: Características técnicas.

Tensión de alimentación	127/220V AC-60Hz
Consumo	5W equivalente a 3,6 KWh/mes
Tensión de salida em abierto	18000V +/- 10%
Energía del pulso de salida	Menor a 0,5 Joules
Duración del pulso de salida	100 us
Corriente máxima de salida	400mA-500mA
Dimensiones	295x235x120mm
Batería de respaldo	Si, alimentado con 12VCC

Realizado por: Caiza H., Yanza A., 2021.

2.4.9. Sirena de 20W DSC

Diseñada para exteriores en todo tipo de ambiente, posee un tono sostenido de acuerdo a la instalación Figura 11-2. Las características técnicas se describen en la Tabla 9-2.

Figura 11-2: Sirena DSC 20W

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 9-2: Características técnicas.

Material de la estructura	ABS
Dimensiones	13.34 x 14.61 mm
Voltaje de alimentación	12VCD
Corriente máxima	700mA
Potencia	20W
Intensidad de volumen	110dB

Realizado por: Caiza H., Yanza A., 2021.

2.4.10. Esquema de conexión electrónica

En la Figura 12-2 se muestra el esquema electrónico del prototipo, en el cual se puede observar cómo están conectados los dispositivos que conforman el módulo de seguridad. A continuación, se detalla la función que cumple cada elemento.

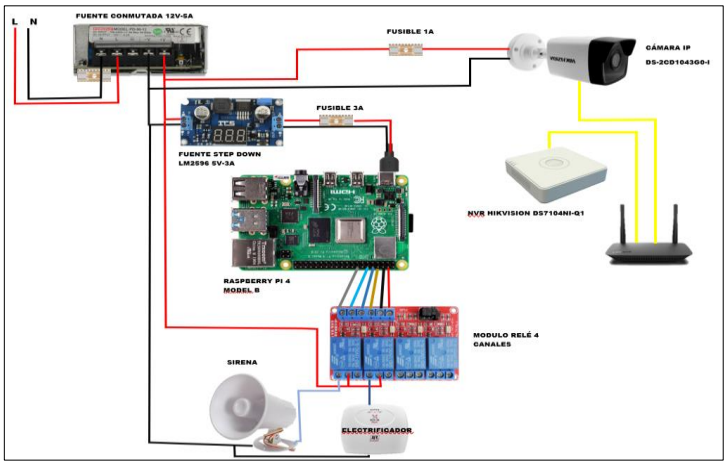


Figura 12-2: Esquema de conexión electrónico.

Realizado por: Caiza H., y Yanza A., 2021.

- La alimentación tanto para los equipos electrónicos como la cámara de seguridad vendrá dada por una fuente conmutada de 12V y 10A de salida, suficiente para alimentar todos los equipos que requieran corriente continua.
- Para la energizar la Raspberry se utiliza una fuente step down que permite reducir a la tensión a 5V y soporta 3A, a su vez se conecta un fusible de 3A para protegerla en caso de que se presente algún fallo.
- El módulo relé se energiza los terminales de "IN" y "GND" con los 5V y GND que provee la Raspberry. Las 4 entradas que activarán a los diferentes relés serán conectadas a las GPIO de la raspberry.
- Los relés activarán la sirena y el Electrificador, para ello se conecta los 12V de la fuente al terminal común de los relés, al terminal NA se conectará la carga y este se conectará a GND.

- La cámara se energiza con los 12V de la fuente, cuenta con una protección mediante un fusible de 1A. A su vez está conectada a la red directamente al router mediante un cable de red y mediante su dirección IP se conectará con el NVR.
- El NVR de igual manera estará conectado mediante un cable de red al router, y este permitirá grabar las imágenes obtenidas por la cámara.

2.5. Herramientas software del sistema

2.5.1. Open CV

Es una biblioteca de visión artificial de código abierto, la cual puede ser usada en lenguaje Python, que es el lenguaje con el que se puede programar la Raspberry, esta biblioteca es muy utilizada en aplicaciones que requieren procesamiento en tiempo real. Contiene varias funciones como inspección de productos, imágenes médicas, calibración de cámaras, etc. (Bradski y Kaehler 2008, p. 1).

2.5.2. Thonny IDE

Es un entorno de desarrollo que ya viene incluido en el sistema operativo de Raspbian, es muy sencillo de usar, para el desarrollo del módulo se desarrollaron 3 algoritmos diferentes. El primero permite crear la base de datos con los rostros de las personas para reconocer el rostro. El segundo permitirá realizar un entrenamiento y obtener un archivo que se utiliza en el último algoritmo que es la parte de identificación de rostros.

2.5.3. Crear la base de datos.

- Importar las librerías a utilizar, para el caso siguiente se importa la librería “cv2” e “imutils” que corresponde a OpenCv para realizar la parte de visión artificial.
- Importar la librería “os”, esta permite manipular la estructura de directorios, ayuda a leer y escribir archivos.
- Crear una ruta seleccionada (carpeta) con el nombre de la persona a identificar para crear la base de datos con la función **os.makedirs()**. En caso de que exista se sobrescribirá las imágenes.
- Una vez creada la carpeta se procede a obtener la información mediante la cámara con la función **cv2.VideoCapture()**, dentro de los paréntesis se debe indicar la cámara que se va utilizar, en el caso de la cámara IP se realizó la conexión mediante el protocolo rstp, para la cámara IP se utilizó la siguiente línea de código “**rtsp://admin:camara01@192.168.1.64:554/h264/ch1/main/av_stream**”.

- El siguiente paso es asignar al programa un clasificador para detectar el rostro mediante la función **cv2.CascadeClassifier**, OpenCv nos brinda muchas herramientas, una de ellas es que incluye los clasificadores Haar Cascade utilizados en el método de Viola Jones mediante "**cv2.data.haarcascades**".
- En un bucle de repetición **while** se realizará la detección del rostro el cual con la función **cv2.cvtColor()** asignamos el nombre la información que se obtiene de la cámara y luego se convierte a escala de grises mediante la función **cv2.COLOR_BGR2GRAY.**
- Con la función **faceClassif.detectMultiScale()** se utiliza la imagen en escala de grises, y se puede definir algunos parámetros, como el factor de escala que permite reducir el tamaño de la imagen, así como el número de vecinos, este valor se lo puede ir ajustando según los requerimientos del módulo.
- La cámara al identificar un rostro dibuja un rectángulo mediante la función **cv2.rectangle().**
- **cv2.resize()** define la imagen del rostro de un mismo tamaño para todas las imágenes, se recomienda que se hagan diferentes gestos y en diferentes condiciones de luz para que el sistema sea robusto.
- **cv2.imwrite()** almacena la imagen en la carpeta seleccionada al inicio, este proceso de lo debe realizar varias veces con el fin de obtener la mayor cantidad de muestras que permitan tener un algoritmo robusto.
- **cv2.destroyAllWindows()** función cierra todas las ventanas que se han utilizado para realizar el algoritmo.

En la Figura 13-2 se observa el diagrama de flujo del proceso para crear la base de datos.

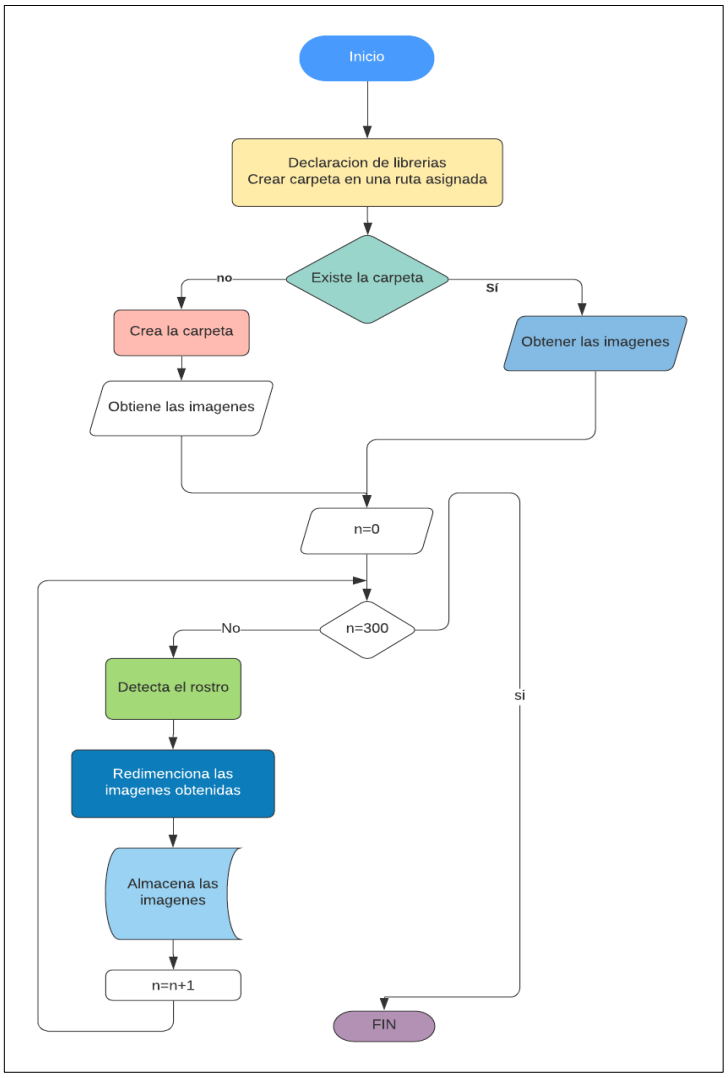


Figura 13-2: Diagrama de flujo de la base de datos.

Realizado por: Caiza H., y Yanza A., 2021.

2.5.4. Entrenamiento del algoritmo

Luego de la crear la base de datos se procede a crear un archivo que utilizará el método de Eigenface para entrenar este algoritmo con las imágenes creadas en el paso anterior.

- Se importan las librerías “cv2”, “os” y numpy.
- Se crea una variable la cual contendrá la ruta de la carpeta donde se almacenan las imágenes.
- **os.listdir().** La función permite identificar las carpetas que han sido creadas con el algoritmo anterior.
- Se crean dos variables en las que, una contendrá las etiquetas de cada persona, mientras que en la segunda se almacenará las imágenes de la base de datos.

- Se ejecuta un contador, esto en caso de que existan varias personas en la base de datos, incrementa el valor cuando termine de leer todas las imágenes de una persona y continúe con las demás.
- La función **cv2.face.EigenFaceRecognizercreate()** especifica el método a utilizar en el reconocimiento de rostros.
- La función **face_recognizer.train()** realiza el entrenamiento del algoritmo, en el argumento se especifica el array donde están almacenados los rostros y las etiquetas de las mismas.
- La función **face_recognizer.write()** crea un archivo que se añadirá en la en el programa de reconocimiento de rostros. Para ello se debe guardar con la extensión xml.

La Figura 14-2 muestra el diagrama de flujo del entrenamiento del algoritmo con las imágenes obtenidas en el paso anterior.

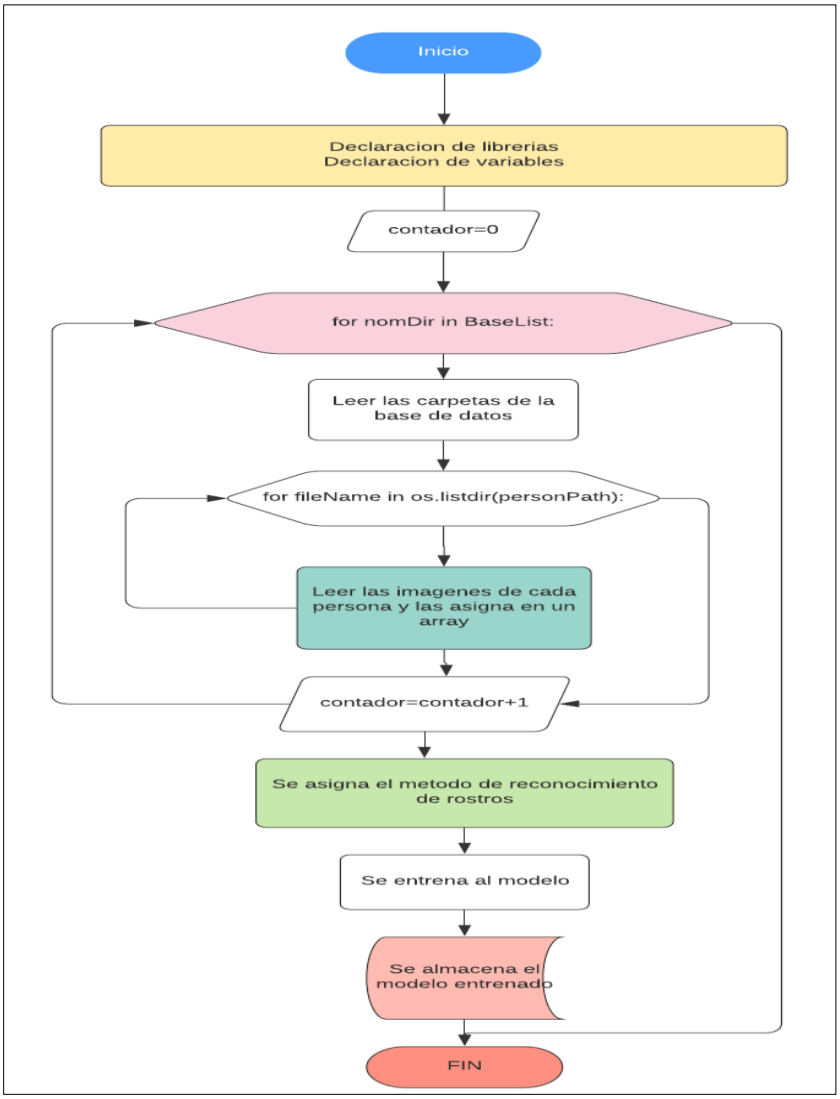


Figura 14-2: Diagrama de flujo para el entrenamiento del algoritmo de VA.

Realizado por: Caiza H., y Yanza A., 2021.

2.5.5. Reconocimiento facial

Luego de entrenar al algoritmo se utiliza el archivo creado que contiene al entrenador en un nuevo código para reducir tiempos de procesamiento, para ello se realiza los siguientes pasos cuyo diagrama de flujo se muestra en la Figura 15-2:

- Se importan las librerías **"cv2"** y **"os".**
- Se obtiene el nombre de las carpetas mediante la función **os.listdir(),** en el argumento se debe especificar la ruta donde se encuentra la carpeta con la base de datos.
- La función **cv2.face.EigenFaceRecognizercreate(),** especifica el método EigenFace para realizar el reconocimiento de rostros.
- La función **read()** añade al programa el archivo creado en el paso anterior con la extensión xml.
- La función **cv2.VideoCapture()** procede a tomar la información de la cámara de seguridad.
- La función **cv2.CascadeClassifier()** permite utilizar los clasificadores Haar Cascade para realizar la detección del rostro.
- En un bucle de repetición **while** se procede a realizar tanto la detección como el reconocimiento de rostros. Para la detección se utiliza la función **faceClassif.detectMultiScale()** y la función cv2.resize() en la que establecerán los parámetros como el en el primer paso.
- Se procede a realizar una comparación de la imagen obtenida con las que se encuentran almacenadas en la base de datos mediante la función **face_recognizer.predict().** En donde en el argumento se debe colocar la imagen obtenida por la cámara.
- Después de comparar las imágenes con la función **cv2.putText()** se colocará un texto sobre la imagen en la de ser una persona que se encuentra almacenada en la base de datos mostrará su nombre, caso contrario se mostrará "Persona desconocida" y se activará el sistema de seguridad.

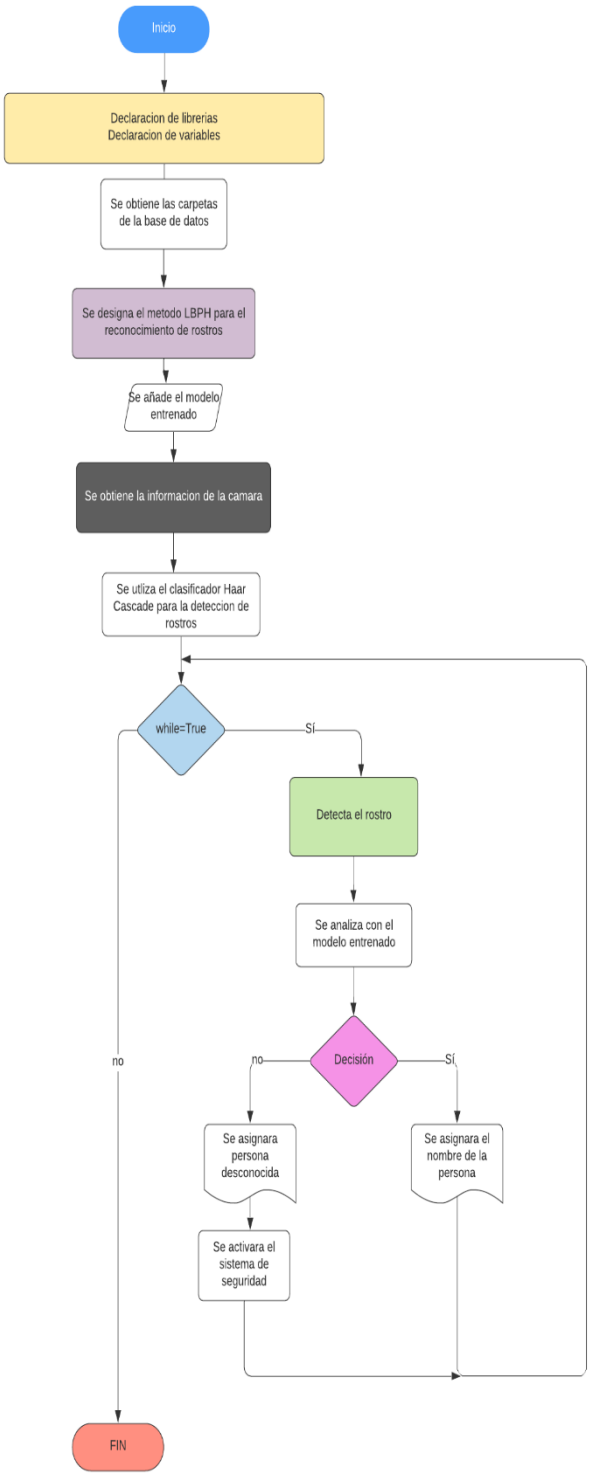


Figura 15-2: Diagrama de flujo para el reconocimiento facial.

Realizado por: Caiza H., y Yanza A., 2021.

2.5.6. Telegram

Es una aplicación que permite realizar conversaciones y llamadas en tiempo real, mantiene sus mensajes cifrados lo que evita ataques de hackers. Además, cuenta con una API abierta lo que permite crear nuestras propias aplicaciones una de ellas el API bot, que crea un usuario virtual que se encargará de realizar tareas asignadas, en este proyecto en bot enviará la notificación al usuario cuando ocurra algún evento en el sistema de seguridad (Telegram.org, 2020).

a) Instalación

Para instalar Telegram se debe realizar mediante el gestor de aplicación como Google Play o App Store.

b) Creación del usuario bot

Una vez instalado se debe buscar al usuario botfather como se muestra en la Figura 16-2 y dar clic en el usuario.

Figura 16-2: Usuario BotFather en la interfaz de Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

Posterior se abrirá un chat con la siguiente imagen Figura 17-2.

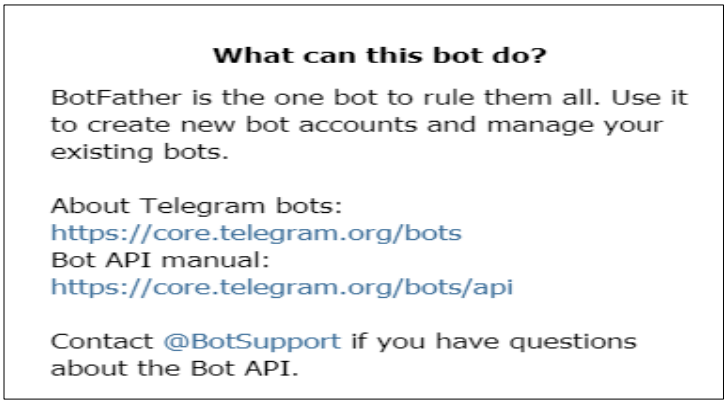


Figura 17-2: Configuración de BotFather en Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

Para inicializar se debe enviar en el chat el comando /start. Y BotFather brindará las opciones que continúe como se muestra en la siguiente Figura 18-2.

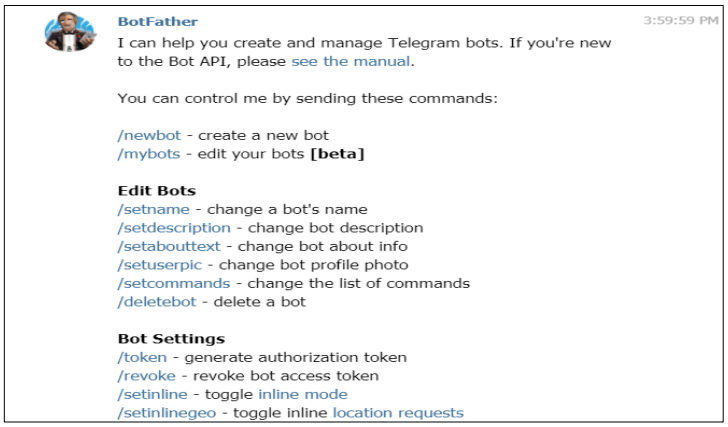


Figura 18-2: Panel para editar y crear Bots.

Realizado por: Caiza H., y Yanza A., 2021.

Para crear un bot se debe enviar el comando /newbot, posterior a esto se añade un nombre y un nombre de usuario. Si el nombre de usuario ya existe se debe crear otro, caso contrario no se creará el bot como se observa en la Figura 19-2 y mostrará el token de acceso al API. Este paso se puede observar en la Figura 20-2.

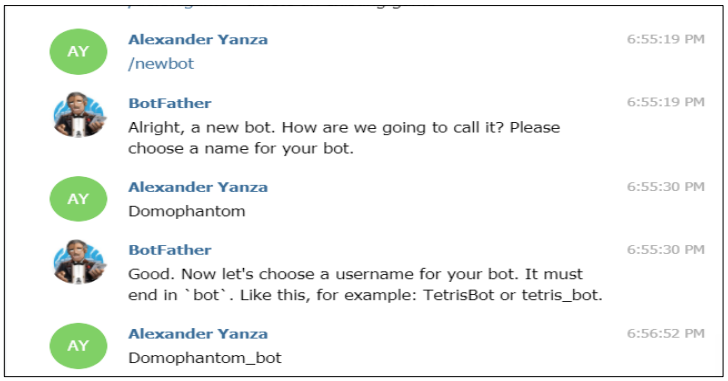


Figura 19-2: Creación del bot y nombre de usuario.

Realizado por: Caiza H., y Yanza A., 2021.

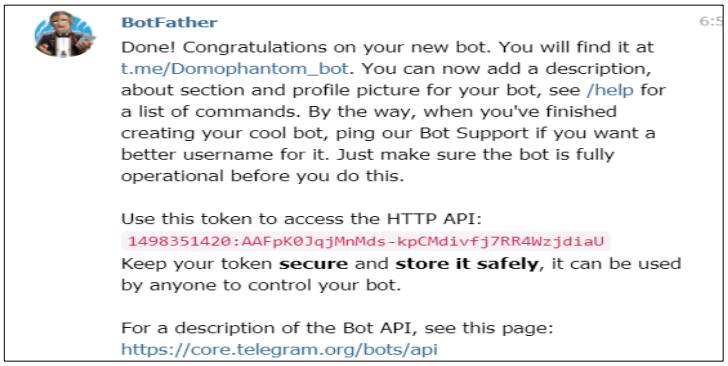


Figura 20-2: Validación del Bot y el token para su conexión con NodeRed.

Realizado por: Caiza H., y Yanza A., 2021.

Es importante anotar el token que nos brinda en este caso el token es *1498351420: AAFpK0JqjMnMds-kpCMdivfj7RR4WzjdiaU* lo cual es importante para conectar con NodeRed.

2.5.7. NodeRed

Es una herramienta que permite conectar dispositivos de hardware, como Raspberry Pi, con API y con algunos servicios de línea. Proporciona un editor de flujo que consiste en una red de procesos llamados nodos. Cada uno cumple una función y envía información a los nodos que se encuentren conectados como se muestra en la Figura 21-2 (Node Red 2020).

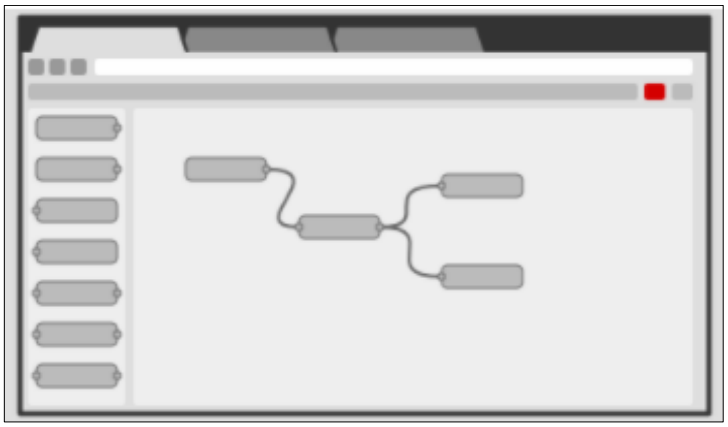


Figura 21-2: Interfaz de NodeRed.

Realizado por: Caiza H., y Yanza A., 2021.

Para realizar la instalación en la Raspberry Pi se debe ejecutar el siguiente comando sudo apt install build-essential git en el prompt de la Raspberry Pi, en caso de tener instalado se puede actualizar a la última versión mediante el comando apt-get install nodered (Node Red 2020).
Para inicializar NodeRed se debe ejecutar el comando node-red-start, para poder realizar un arranque automática de NodeRed para que siempre se ejecute la programación aun cuando se reinicie la Raspberry Pi se debe ejecutar el comando sudo systemctl enable nodered.service (Node Red 2020).

Una vez que se esté ejecutando NodeRed se puede conectar al editor a través de cualquier navegador a través de la dirección http: // localhost: 1880, si se ejecuta desde el propio navegador de la Raspberry Pi o si se desea acceder desde cualquier ordenador que se encuentre conectado a la red debemos ejecutar http://IP:1880, en donde la dirección IP debe ser la asignada a la Raspberry Pi. Para enviar alertas a Telegram debemos seguir los siguientes pasos.
Instalar la paleta de nodos para interactuar con Telegram, para ellos nos dirigimos a la opción Manage palette como se muestra en la Figura 22-2.

Figura 22-2: Opción para instalar nodos adicionales.

Realizado por: Caiza H., y Yanza A., 2021.

Aparece una ventana como la que se observa en la Figura 23-2, se debe dar clic en el botón de Install y colocar la palabra Telegram. Se debe instalar la opción que diga node-red-contrib-telgrambot.

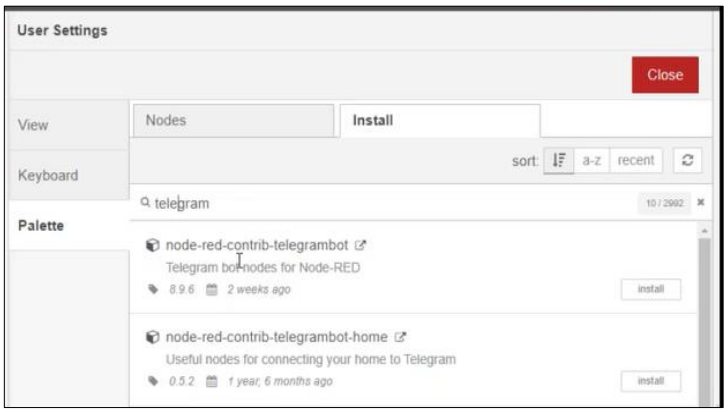


Figura 23-2: Instalación de nodos para Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

Una vez instalado se podrá observar en la parte derecha la paleta con los nodos de Telegram como se observa en la Figura 24-2.

Figura 24-2: Nodos para interactuar con la Raspberry

Realizado por: Caiza H., y Yanza A., 2021.

Para añadir el bot creado en Telegram se configura tanto el nodo reciver y sender, para ello se debe arrastrar los nodos a la zona cuadriculada y dar doble clic en los nodos, si es la primera vez que se ejecuta se mostrará una ventana como se muestra en la Figura 25-2,

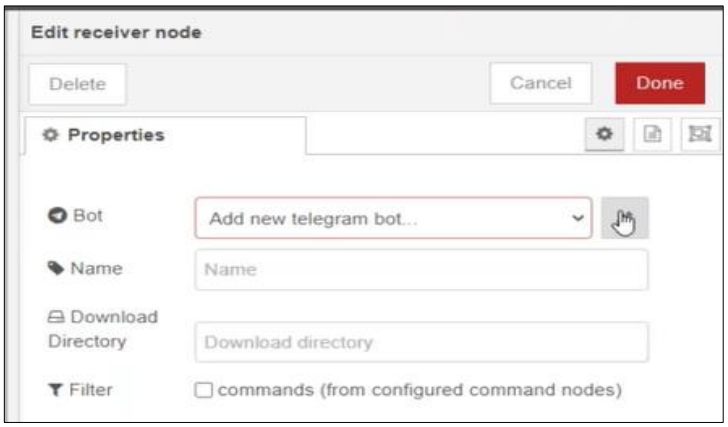


Figura 25-2: Ventana para añadir un nuevo Bot en NodeRed.

Realizado por: Caiza H., y Yanza A., 2021.

Para añadir un nuevo bot, dar clic en el lápiz que aparece en la opción de bot, una vez hecho eso aparecerá una ventana como se muestra en la Figura 26-2, en ella se debe escribir el nombre de usuario como el token del bot creado en Telegram.

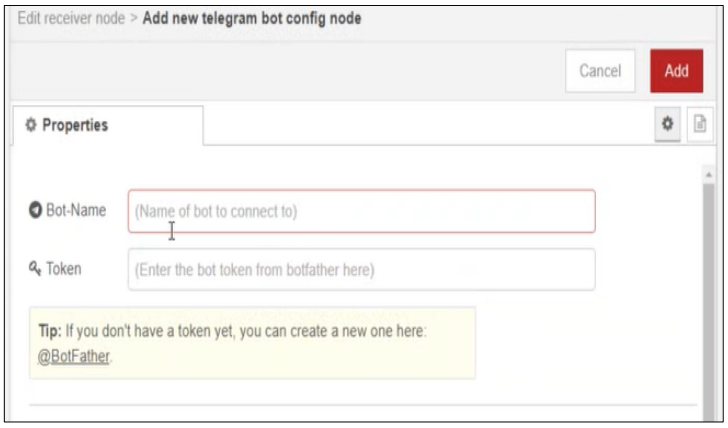


Figura 26-2: Ventana para colocar los datos del Bot creado en Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

La programación realizada en NodeRed se muestra en el siguiente diagrama de flujo que se observa en la Figura 27-2 y se describe a continuación.

- NodeRed permite configurar los puertos de la Raspberry Pi y además interactuar con Telegram.

- Desde Telegram se activa la GPIO17 para activar el sistema de seguridad.
- Cuando el sistema esté activado entrará en funcionamiento el programa de reconocimiento de rostros, el cual activará diferentes salidas cuando identifique una persona desconocida, de ser así reconocerá que la GPIO14 se activó y enviará la notificación de alerta al usuario.

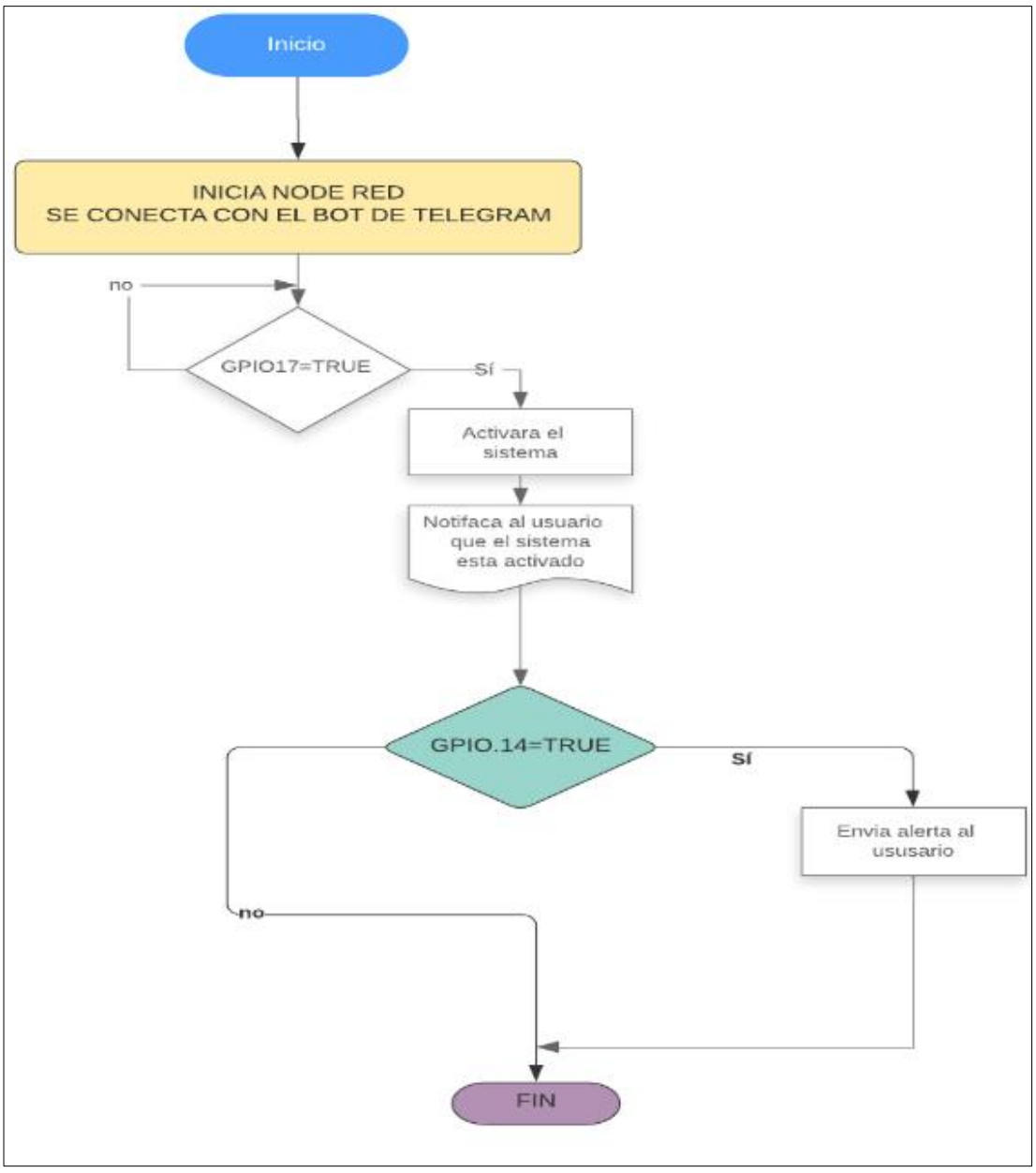


Figura 27-2: Diagrama de flujo de programación de salidas de Raspberry en NodeRed.

Realizado por: Caiza H., y Yanza A., 2021.

CAPÍTULO III

3. VALIDACIÓN DEL PROTOTIPO

Una vez finalizado el módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros, se presenta los valores obtenidos en las diferentes pruebas realizadas al prototipo en funcionamiento dentro de un ambiente real, con el objetivo de validar el módulo, las mismas que consisten en evaluar el algoritmo de reconocimiento de rostros para evaluar la precisión y exactitud, el porcentaje de error con respecto a la distancia, tiempo de ejecución y respuesta del módulo ante diferentes condiciones de luz.

3.1. Ubicación del dispositivo en la vivienda

En la implementación del módulo de seguridad en la vivienda se consideró algunos lineamientos básicos para la instalación, bajo las cuales se realizará la calibración de los parámetros del algoritmo de detección de rostros. Las principales consideraciones a seguir son las que se detallan a continuación.

1. La máxima distancia que la cámara de seguridad realiza el reconocimiento facial es de 160cm a una altura de 240 cm fijo desde el punto de instalación de la misma. Distancias mayores reduce la eficiencia en la detección, además la distancia mínima considerando que la cámara es tipo bala es a partir de los 40 cm del punto de instalación.
2. Para el uso del sistema el usuario debe enfocar el rostro a la cámara al menos una vez para que se realice el procesamiento de la imagen de acuerdo a la almacenada en la base de datos. En caso de no estar registrado la persona será identificada como desconocido procediendo a la activación del protocolo de seguridad como alarmas y notificación mediante Telegram al dueño del inmueble.

Las mencionadas consideraciones son de vital importancia para el correcto funcionamiento del módulo de seguridad. En la Figura 1-3 se observa la implementación del módulo de seguridad dentro del inmueble al igual que la instalación de la cámara de video vigilancia en el exterior de la misma.

Figura 1-3: Implementación de módulo de seguridad en la vivienda.

Realizado por: Caiza H., y Yanza A., 2021.

3.2. Configuración de la cámara HIKVISION

Para realizar las pruebas se debe tener en cuenta que el procesamiento de la Raspberry Pi 4 es limitado, es por ello que se configuro la cámara a una resolución de 1280*720P a 8 fps (frames por segundo) como se puede observar en la Figura 2-3, con esta configuración se obtuvo un procesamiento eficiente, en el cual el retardo del video original al video procesado para el reconocimiento facial fue de 2 segundos, con resolución más alta y velocidad de frames superior se obtiene tiempos de respuestas muy lento que no lo hacen un sistema óptimo.

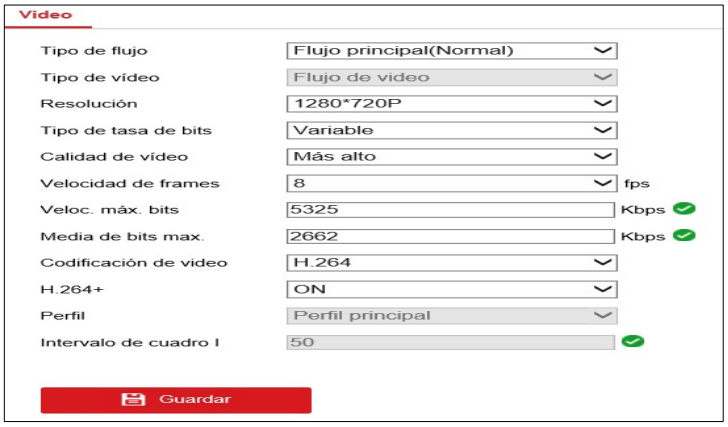


Figura 2-3: Configuración de la cámara IP HIKVISION**.**

Realizado por: Caiza H., y Yanza A., 2021.

3.3. Metodología para las pruebas.

Las pruebas se realizaron considerando el número de integrantes dentro de una familia promedio en una zona urbana en la ciudad de Ambato, tomando diez muestras en la mañana, tarde y noche en horas con mayor movimiento dentro del inmueble. Es importante antes de realizar las pruebas el número de individuos registrados en la base de datos.

3.4. Prueba de precisión y exactitud con un solo sujeto conocido.

Mediante el uso de la matriz de confusión la cual es una herramienta que permite visualizar el desempeño de un algoritmo, se toma en cuenta la métrica de precisión el cual permite medir la calidad en cuanto a la detección de rostros y además se obtiene el porcentaje de exactitud para evaluar la cantidad de aciertos del mismo.

En las Tablas 1-3 a la 4-3 se verifica la precisión y la exactitud que tiene el algoritmo para la detección de rostros con respecto a un sujeto conocido, con varias características tomando diez muestras en diferentes horas del día, destacando así un 100% de precisión y 99,1667% de exactitud.

Tabla 1-3: Porcentaje de Precisión y Exactitud con un Sujeto Conocido.

Sujeto Conocido sin artículos.							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	10	0	0	0	100,00	100,00
Noche	10	10	0	0	0	100,00	100,00
TOTAL	30	30	0	0	0	100,00	100,00

Realizado por: Caiza H., Yanza A., 2021.

En la Figura 3-3 se observa cómo el algoritmo es capaz de reconocer a sujeto almacenado en la base de datos, además se evidencia que no es necesario que mire directamente a la cámara, con pequeñas inclinaciones el algoritmo es capaz de reconocer el rostro.

Figura 3-3: Reconocimiento de sujeto sin artículos en la cabeza.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 2-3: Porcentaje de Precisión y Exactitud con un Sujeto Conocido con Gorra.

Sujeto Conocido gorra

Partes del día	N° de muestra	Detección Positiva TP	Detección Negativa TN	Falso Positivo FP	Falso Negativo FN	Precisión %	Exactitud %
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	10	0	0	0	100,00	100,00
Noche	10	10	0	0	0	100,00	100,00
TOTAL	30	30	0	0	0	100,00	100,00

Realizado por: Caiza H., Yanza A., 2021.

En la Figura 4-3 se observa el resultado de esta prueba, donde se observa que para este caso si es necesario que el sujeto mire directamente a la cámara, debido a que la gorra puede llegar a cubrir parte del rostro y no podrá reconocerlo.

Figura 4-3: Reconocimiento del sujeto utilizando una gorra.

Realizado por: Caiza H., y Yanza A., 2021.

En la figura anterior también se puede evidenciar que el uso de lentes no afecta al momento del reconocimiento, de igual forma se realizó pruebas en diferentes periodos del día cuyos resultados se muestran en la Tabla 3-3.

Tabla 3-3: Porcentaje de Precisión y Exactitud con un Sujeto Conocido con Lentes.

Sujeto Conocido con lentes							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	10	0	0	0	100,00	100,00
Noche	10	10	0	0	0	100,00	100,00
TOTAL	30	30	0	0	0	100,00	100,00

Realizado por: Caiza H., Yanza A., 2021.

En la Figura 5-3 se puede observar que cuando la persona no está almacenada en la base de datos el resultado es desconocido por ende en este caso el sistema de seguridad procederá a activarse y enviar alertas a través de Telegram.

Figura 5-3: Persona no registrada en la base de datos.

Realizado por: Caiza H., y Yanza A., 2021.

De la misma forma que las pruebas anteriores se toman 10 muestras en diferentes periodos del día para obtener resultados que permitan robustecer el sistema, en este caso en la Tabla 4-3 muestra el resultado de estas pruebas donde se evidencio que en la noche mostró un falso positivo.

Tabla 4-3: Porcentaje de Precisión y Exactitud con un Sujeto Desconocido.

Sujeto desconocido.							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	10	0	0	0	100,00	100,00
Noche	10	9	0	0	1	100,00	90,00
TOTAL	30	29	0	1	0	100,00	96,67

Realizado por: Caiza H., Yanza A., 2021.

En el Gráfico 1-3 se puede observar el resultado de la prueba de reconocimiento de un solo individuo, en el cual su comportamiento fue aceptable dando una exactitud del 99,19%, y la precisión del algoritmo de detectar un rostro dentro del área determinada del 100%.

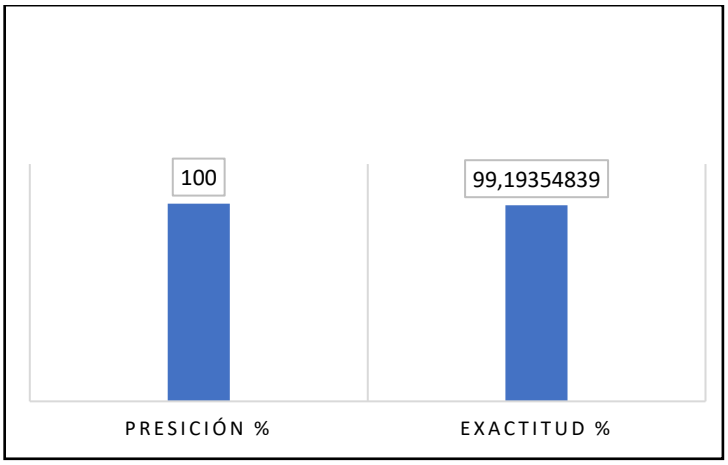


Gráfico 1-3: Porcentaje de Precisión y exactitud en la detección de un solo individuo.

Realizado por: Caiza H., y Yanza A., 2021.

3.5. Prueba de precisión y exactitud con varios sujetos.

En la Figura 6-3 se puede observar los resultados de la identificación de dos sujetos que se encuentran almacenados en la base de datos, de la misma forma que en la prueba anterior se realizó las pruebas en diferentes periodos del día, dichos resultados son mostrados en la Tabla 5-3.

Figura 6-3: Reconocimiento de dos personas

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 5-3: Porcentaje de Precisión y Exactitud con dos sujetos conocidos.

Dos sujetos conocidos.							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00

Tarde	10	9	0	0	1	100,00	90,00
Noche	10	7	1	2	0	77,78	80,00
TOTAL	30	26	1	2	1	92,86	90,00

Realizado por: Caiza H., Yanza A., 2021.

En la siguiente prueba se realizó la identificación de dos personas, de las cuales una estaba registrada en la base de datos mientras que la otra persona era desconocida, el resultado de esta prueba se puede observar en la Figura 7-3, y los datos de esta prueba se puede observar en la Tabla 6-3 en donde se pudo mostrar que en la noche existen más fallas.

Figura 7-3: Detección e identificación de dos personas.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 6-3: Porcentaje de Precisión y Exactitud con un conocido y otro desconocido.

Dos sujetos (1 conocido).							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	8	0	0	2	100,00	80,00
Noche	10	7	2	1	0	87,50	90,00
TOTAL	30	25	2	1	2	96,15	90,00

Realizado por: Caiza H., Yanza A., 2021.

Para realizar esta prueba se eliminó a dos sujetos de la base de datos para observar el comportamiento del algoritmo cuando detecta a dos personas, en la Figura 8-3 se muestra el resultado de esta prueba y en la Tabla 7-3 donde se observa que se obtuvo 1 falso positivo tanto en el periodo de la tarde y en la noche.

Figura 8-3: Reconocimiento de dos personas desconocidas.

Realizado por: Caiza H., y Yanza A., 2021.

Tabla 7-3: Porcentaje de Precisión y Exactitud con dos sujetos desconocidos.

Dos sujetos (desconocidos).							
Partes del día	**N° de muestra**	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Precisión %**	**Exactitud %**
Mañana	10	10	0	0	0	100,00	100,00
Tarde	10	9	0	1	0	90,00	90,00
Noche	10	9	0	1	0	90,00	90,00
TOTAL	30	28	0	2	0	96,55	96,55

Realizado por: Caiza H., Yanza A., 2021.

Al finalizar esta prueba se determina que el algoritmo es 95,18% en lo que respecta a la precisión, mientras que es 92,18% en lo que se refiere a exactitud como se muestra en el Gráfico 2-3, se pudo evidenciar que en el periodo de la noche es donde presenta algunos fallos, pero muestran resultados aceptables.

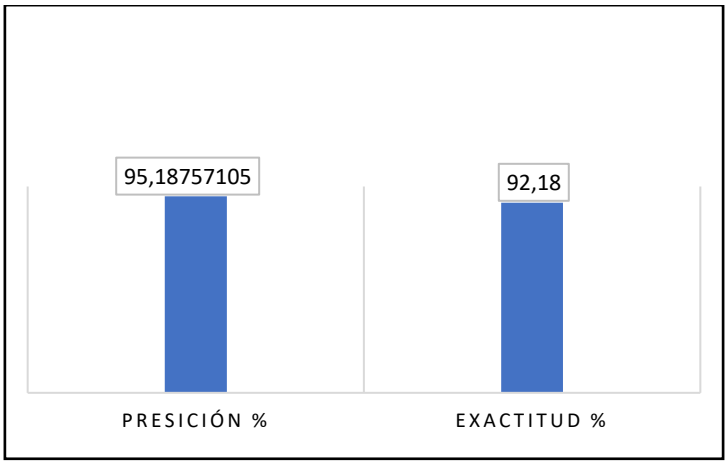


Gráfico 2-3: Porcentaje de Precisión y exactitud en la detección de dos individuos.

Realizado por: Caiza H., y Yanza A., 2021.

A continuación, se muestra la Tabla 8-3 de pruebas en la cual se detalla la cantidad de aciertos positivos en cada uno de los casos descritos con anterioridad, estos datos posteriormente serán usados para la obtención del porcentaje de efectividad en la identificación de rostros.

Tabla 8-3: Clasificación de los aciertos.

	Mañana				**Tarde**				**Noche**				
	TP	TN	FP	FN	TP	TN	FP	FN	TP	TN	FP	FN	
Sujeto conocido	10	x	x	x	10	x	x	x	10	x	x	x	30
Sujeto conocido/art	20	x	x	x	20	x	x	x	20	x	x	x	60
Sujeto desconocido	10	x	x	x	10	x	x	x	9	x	x	1	30
Dos sujetos conocidos	10	x	x	x	9	x	x	1	7	1	2	x	30
Conocido/Desconocido	10	x	x	x	8	x	x	2	7	2	1	x	30
Dos sujetos desconocidos	10	x	x	x	9	x	1	0	9	x	1	x	30
TOTAL	70	0	0	0	66	0	1	3	62	3	4	1	**210**

Realizado por: Caiza H., Yanza A., 2021.

Dentro de las pruebas realizadas en la Tabla 8-4 se detalla el total de detecciones positivas y negativas al igual que el total de falsos positivos y falsos negativos arrojados por el algoritmo de visión artificial.

Tabla 9-3: Aciertos totales según la matriz de confusión.

	TOTAL
TP	198
TN	3
FP	5
FN	4

Realizado por: Caiza H., Yanza A., 2021.

Con los datos obtenidos en la Tabla 9-3 se puede obtener el porcentaje de efectividad, para lo cual se realiza el cálculo:

$$\%\, efectividad = \frac{Aciertos\ Positivos}{N°\ de\ muestras} * 100\% \qquad (5)$$

$$\%\, efectividad = \frac{198}{210} * 100\%$$

$$\%\, efectividad = 94.29\%$$

El resultado obtenido muestra el porcentaje de efectividad del algoritmo en la identificación de rostros acorde al total de muestras realizadas.

3.6. Validación de la Hipótesis

La implementación de un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros permite mejorar la seguridad de una vivienda.

Para realizar la validación de la hipótesis se plantea la siguiente hipótesis nula (H0) e hipótesis alternativa (H1) respectivamente, siguiendo los siguientes pasos.

Paso 1 Plantear las hipótesis

- H0: El porcentaje de eficiencia de un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros no es mayor a un 97% $p \leq 97\%$.
- H1: El porcentaje de eficiencia de un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros es mayor a un 97% $p > 97\%$.

Paso 2 Seleccionar el nivel de significancia (alfa).

Se trabaja con un nivel de significancia del 5 %

Paso 3 Calcular el valor del estadístico de prueba.

Se va a utilizar como estadístico de prueba la distribución normal Z cuya ecuación es la siguiente para una proporción.

$$Z = \frac{\bar{\dot{p}} - p}{\sqrt{\frac{p.q}{n}}} \qquad (6)$$

Dónde:

$\bar{\dot{p}}$= Porcentaje de eficiencia del sistema.

p = Porcentaje de eficiencia esperado.

q = Porcentaje de fallas esperadas.

n = Número de muestras.

El porcentaje de eficiencia esperado es del 97% de acuerdo al trabajo de investigación de reconocimiento facial con patrones binarios locales descritos en el capítulo 1.

$$Z = \frac{0.9428 - 0.97}{\sqrt{\frac{0.97(0.03)}{210}}}$$

$$Z = -2.54$$

Paso 4. Establecer la regla de decisión**.**

Como se trabaja con un nivel de significancia del 5% y es una prueba de hipótesis de una sola cola se define un valor Zc = 1.96. Como se observa en el Gráfico 3-3.

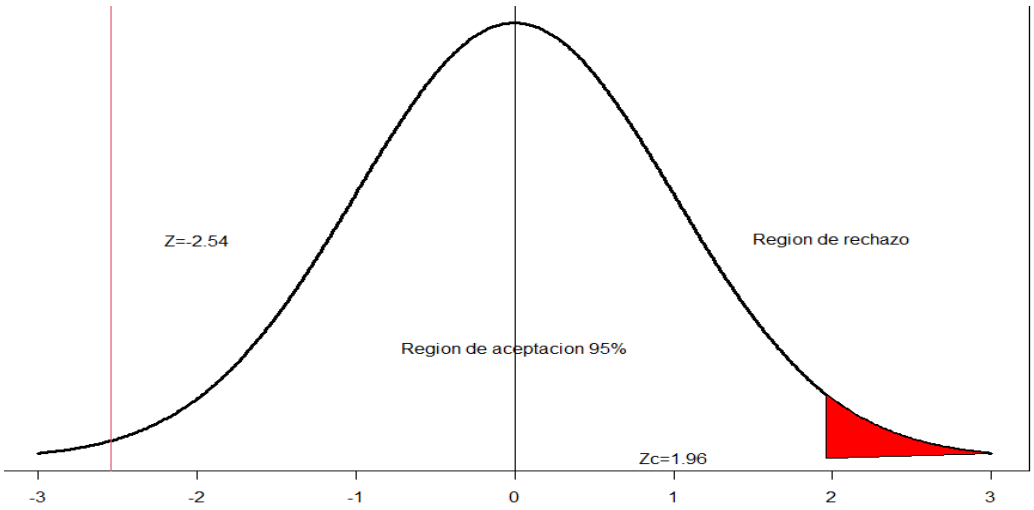


Gráfico 3-3: Distribución Normal.

Realizado por: Caiza H., y Yanza A., 2021.

La regla de decisión es se acepta H0 si Z < Zc, caso contrario se rechaza H0.

Paso. 5 toma de decisión

Como -2.54 < 1,65 se acepta H0, por lo tanto, el porcentaje de eficiencia de un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros no es mayor a un 97%, manejando un error del 3%.

3.7. Prueba de detección en diferentes niveles de iluminación

Se toman 10 pruebas en diferentes niveles de luminosidad, para ello se toma como referencia datos obtenidos de la aplicación para teléfono celular "Lux Meter" debido a que no se contaba con luxómetro físico y cuyo valor es elevado, la aplicación está disponible tanto para sistemas operativos Android e IOS, se tomó esta aplicación para tener valores de referencia ya que cuenta con una alta calificación dentro de la tienda 4,2/5 y valorada por 9583 personas. En la Figura 9-3 se puede observar la interfaz gráfica de esta aplicación, donde nos muestra una gráfica de tiempo, valores máximos, mínimos y promedio de los valores tomados.

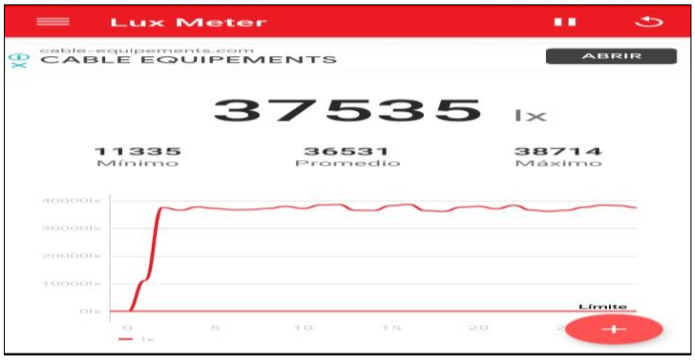


Figura 9-3: Aplicación Lux Meter.

Realizado por: Caiza H., y Yanza A., 2021.

Para la primera prueba los datos se tomaron en un día soleado, se tomaron 10 muestras con diferentes sujetos, tanto conocido como desconocido, al igual que con dos sujetos a la vez, arrojando los datos que se muestran en la Tabla 8-3, además se puede observar el tiempo que toma en identificar el rostro medido en segundos.

Tabla 10-3: Resultados de la prueba de detección de varios sujetos.

Luminosidad día soleado (11415-68162)					
N° de muestra	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Tiempo**
1	x				0,009324
2	x				0,009715
3	x				0,009882
4	x				0,010091
5	x				0,009716
6		x			0,009632
7	x				0,011648

8	x				0,014248
9	x				0,009895
10	x				0.01129

Realizado por: Caiza H., Yanza A., 2021.

La segunda prueba se tomó en un ambiente donde existía poca luz solar, de la misma forma que se realizó la prueba anterior, con diferentes sujetos, con algunos artículos como gorra y lentes, los resultados se muestran en la Tabla 9-3.

Tabla 11-3: Resultados de la prueba de detección en un ambiente de luz.

Luminosidad (11335-38714 lux)					
N° de muestra	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Tiempo**
1	x				0,0155
2	x				0,0141
3	x				0,0142
4	x				0,009
5			x		0,0134
6	x				0,0097
7	x				0,0096
8		x			0,0098
9		x			0,0095
10	x				0,1081

Realizado por: Caiza H., Yanza A., 2021.

La tercera prueba fue en un día nublado de la misma forma que los anteriores en la Tabla 10-3 se muestra los resultados de los datos obtenidos donde se observa que en este ambiente el sistema tuvo 3 fallos debido a la falta de iluminación.

Tabla 12-3: Tabla de prueba de luminosidad en día nublado.

Luminosidad día nublado (4985-5336 lux)					
N° de muestra	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Tiempo**
1		x			0,0154922
2	x				0,014069
3	x				0,014221
4	x				0,009017
5	x				0,0133683
6	x				0,0097012
7	x				0,009623
8		x			0,0098237
9		x			0,0094628
10	x				0,108098

Realizado por: Caiza H., Yanza A., 2021.

Para la prueba en la noche la cámara activa su modo de grabación nocturna, la cual le permite obtener imágenes en una buena calidad pese a que exista poco o nula iluminación natural, los datos se pueden observar en la Tabla 11-3, en donde pese a tener bajo nivel de iluminación el sistema muestra pocos fallos.

Tabla 13-3: Tabla de prueba de luminosidad en la noche.

Luminosidad noche (0 lux)					
N° de muestra	**Detección Positiva TP**	**Detección Negativa TN**	**Falso Positivo FP**	**Falso Negativo FN**	**Tiempo**
1	x				0,009775
2	x				0,008821
3	x				0,008895
4	x				0,009698
5	x				0,008835
6	x				0,011204
7	x				0,013614
8	x				0,00903
9				x	0,007946
10		x			0,009083

Realizado por: Caiza H., Yanza A., 2021.

3.8. Pruebas de control del módulo de forma remota.

El sistema puede ser activado remotamente desde una página web como a través de Telegram, las dos alternativas permiten tener un control sin necesidad de estar en el domicilio lo que permite activarlo desde cualquier parte del mundo siempre y cuando se tenga acceso a internet. En la Figura 10-3 se muestra la interfaz de la aplicación la cual permite activar o desactivar el módulo.

Figura 10-3: Interfaz del sistema de seguridad.

Realizado por: Caiza H., y Yanza A., 2021.

En la Figura 11-3 se muestran como activar el módulo a través de comandos en Telegram

Figura 11-3: Activación del módulo a través de Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

De igual manera en caso de identificar a una persona desconocida el módulo será capaz de enviar una foto a Telegram una foto de la persona desconocida como se muestra en la Figura 12-3 donde se observa como llegará el mensaje al usuario.

Figura 12-3: Mensaje de alerta para el usuario a través de Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

En caso de que el sistema no se encuentre desactivado estará funcionando el sistema de la cerca eléctrica, como la sirena y los sensores magnéticos y de movimiento, además la cámara grabará un video cada que registre movimiento, el cual se puede almacenar en la nube para mayor seguridad. Como se muestra en la Figura 13-3, en donde se puede observar cómo va almacenando la información en la nube lo cual brinda mayor seguridad al usuario.

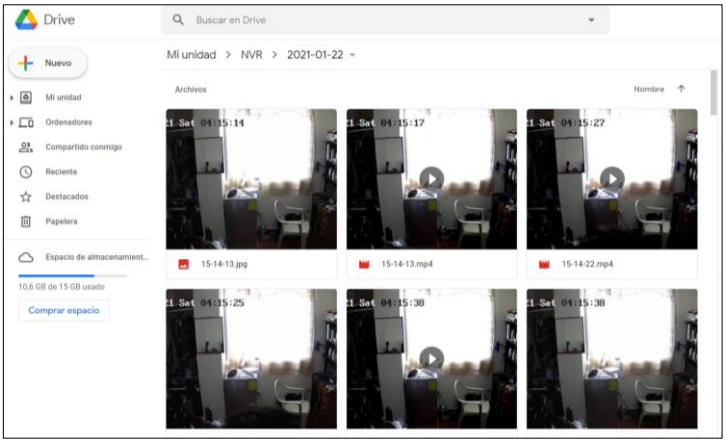


Figura 13-3: Almacenamiento de información dentro de la nube.

Realizado por: Caiza H., y Yanza A., 2021.

CAPÍTULO IV

4. EVALUACIÓN ECONÓMICA

En la siguiente tabla se detalla el costo final del prototipo desarrollado en esta investigación. Se debe tener en cuenta que cámaras que incluyan un sistema de visión artificial son más costosas que la mayoría de cámaras que se utilizan en los sistemas de seguridad para zonas residenciales.

Tabla 1-4: Costo de Hardware.

Cantidad	Detalle	V. Unitario	V. Total
1	Kit Raspberry Pi 4 model B (tarjeta Raspberry Pi4, carcasa, disipador y cargador)	140	140
1	Cámara IP HIKVISION ds-2cd1043g0-i	87.57	87.57
1	Fuente conmutada de 12V DC	14	14
1	Kit cerca eléctrico (Electrificador JFL, sirena, batería de respaldo, 4 letreros)	110	110
1	Módulo relé de 4 canales	7	7
1	Tablero eléctrico	50	50
1	Módulo Reductor De Voltaje (Buck) Lm2596 3a	4.50	4.50
1	Sensor PIR detector de movimiento	3.50	3.50
	Varios		40
	Total		**$456.57**

Realizado por: Caiza H., Yanza A., 2021.

El presente trabajo presenta algunas ventajas frente a diferentes soluciones comerciales que existen en el mercado en la Tabla 2-4 se puede observar una alternativa comercial, con equipos disponibles dentro del ámbito local

Tabla 2-4: Costo de una alternativa comercial

Cantidad	Detalle	V. Unitario	V. Total
1	Cámara Ip Acusense Tubo 2	165	165
1	NVR DS-7104NI-Q1/4P	99	99
1	Fuente centralizada para camaras 12v -10A	42	42
1	Kit cerca eléctrico (Electrificador JFL, sirena, batería de respaldo, 4 letreros)	110	110
1	Modulo Ethernet para electrificadores JFL	35	35
1	Kit de Alarma Inalambrica Ds-pwa32-kgt	184	184
1	Disco Duro de 1TB	38	38
	Total		**$673**

Realizado por: Caiza H., Yanza A., 2021.

Como se podrá observar el costo total de una alternativa comercial es similar al módulo propuesto ya que la primera tiene un costo de 489$, mientras que el modulo tiene un presupuesto de $456.57, sin embargo, existen algunos beneficios que destacan del sistema comercial los cuales se mencionan a continuación:

- El modulo permite reconocer el rostro de la persona que es captada por la imagen, mientras que la alternativa comercial solo puede detectar si es una persona o un vehículo para enviar alguna señal de alerta.
- El modulo permite trabajar con cualquier cámara IP independientemente de la tecnología del fabricante, mientras que en el ámbito comercial se deberá optar por cámaras que incorporen algún algoritmo de visión artificial como en el caso de las cámaras Hikvision que incorporan la tecnología Acusense que permite detectar si es una persona o un vehículo, siendo estas más costosas.
- El módulo permite una interconexión entre los equipos de seguridad independientemente del fabricante de los mismos, ya que al usar una Raspberry Pi 4 model B, podemos enviar señales de control a través de sus GPIO, incluido el monitoreo mediante internet, mientras que en el otro caso esto se ve limitado por las características que incluya el fabricante y la adquisición de otros dispositivos lo cual aumenta el precio final.

CONCLUSIONES

- Se implementó un módulo domótico de seguridad residencial aplicando técnicas de visión artificial para la identificación de rostros mediante el uso de cámaras IP de video-vigilancia comerciales, con ayuda de un algoritmo de reconocimiento de rostros, logrando obtener resultados aceptables.

- En la actualidad los dispositivos de seguridad que utilizan visión artificial requieren de algoritmos que permitan implementar técnicas de procesamiento de imagen, siendo una de la más aplicada el reconocimiento fácil que a través de ciertos rasgos característicos permite identificar al sujeto y tomar las acciones respectivas.

- El software y hardware utilizados en el módulo son de costo accesible, siendo el más importante la Raspberry Pi 4 considerada como un microordenador, el cual permite integrar conectividad a internet, su lenguaje de programación admite algoritmos de visión artificial de código abierto, además la información se obtiene mediante una cámara comercial que permite aprovechar las características que esta ofrece y controlar dispositivos de seguridad como alarmas, electrificador y sensores.

- El prototipo tiene un alcance máximo de 1.60m medidos desde la cámara hasta el sujeto, la cámara está colocada a una altura de 2.40m, el módulo que realiza el procesamiento debe permitir almacenar y transmitir información en tiempo real.

- Mediante el protocolo RTSP se transmite la imagen de video en tiempo real que se obtiene de la cámara IP al microordenador Raspberry Pi 4, el cual mediante la librería OpenCV y clasificadores HAAR ejecuta el algoritmo implementado y activar o desactivar los dispositivos de seguridad en caso de vulnerar la red de video-vigilancia.

- De las pruebas de reconocimiento de rostros se determinó que el sistema es efectivo en un 100% al momento de identificar a un sujeto almacenado en la base de datos, en un ambiente tanto soleado como nublado, sin embargo, el prototipo presenta errores en horas en las que la luminosidad es baja debido al cambio de día a noche o viceversa, sin embargo, en modo nocturno el sistema presenta resultados aceptables. Además, el tiempo de procesamiento incrementa conforme la imagen analizada presenta varios sujetos o su resolución es muy alta, la activación de los equipos de seguridad como el cerco eléctrico o alarma es de 0.3 segundos una vez que son activadas por el algoritmo.

RECOMENDACIONES

- Cada usuario debe ingresar por lo menos unas 20 imágenes por cada tipo de ambiente, es decir para soleado, nublado, nocturno, etc. Esto mejorará la robustez del módulo, mientras más imágenes logre almacenar mejor será el reconocimiento del módulo, pero a su vez se requerirá de mayor calculo computacional.

- Para poder controlar y monitorear desde una red externa se debe adquirir una versión pagada de las plataformas que brindan este servicio como REMOTE.IT.

- Integrar más cámaras al módulo que permita monitorear otro tipo de localidades del domicilio, como patios posteriores.

- Al momento de seleccionar la cámara IP se debe tener en cuenta que maneje el protocolo rstp, ya que este protocolo permite transmitir las imágenes a nuestro módulo de seguridad.
- Debido a que el módulo realiza varias tareas, y que debe estar disponible a cualquier hora, se recomienda usar un sistema de refrigeración para la Raspberry Pi 4 ya que a temperaturas elevadas bajará su rendimiento o a su vez se apagará para protegerse.

- Debido a que la Raspberry Pi 4 al ser un mini ordenador no cuenta con una GPU potente, es recomendable utilizar una tarjeta gráfica externa, esto ayudará a optimizar los algoritmos de visión artificial, sobre todo aquellos que se ejecutan en tiempo real y requieren muchos recursos como lo es el reconocimiento de rostros en tiempo real.

GLOSARIO

Algoritmo: Conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas.

Algoritmo AdaBoost: Consiste en crear varios predictores sencillos en secuencia, de tal manera que el segundo ajuste bien lo que el primero no ajustó, que el tercero ajuste un poco mejor lo que el segundo no pudo ajustar y así sucesivamente.

Apps: Es una aplicación de software que se puede utilizar en dispositivos móviles, tablets y ordenadores después de instalarla. Su finalidad es ayudar al usuario a realizar algo, ya sea de forma profesional como para su ocio o como entretenimiento.

Array: Son variables del mismo tipo de dato que tienen el mismo nombre y que se distinguen y referencian por un índice.

Características Biométricas: Es una característica biológica o de la conducta de un individuo que puede ser medida y distinguida.

Bot: Acortamiento por aféresis de la palabra, ya también española, robot se usa en referencia a un programa informático que efectúa automáticamente determinadas tareas.

Características Haar: Son funciones rectangulares simples de 2 dimensiones en las que se varía el tamaño y la posición de recuadros blancos y negros.

Corriente nominal: Consumo de corriente previsto para el motor trabajando a plena carga.

DHCP: es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada.

Dirección IP: dirección del Protocolo de Internet. Este protocolo es un conjunto de reglas para la comunicación a través de Internet, ya sea el envío de correo electrónico, la transmisión de vídeo o la conexión a un sitio web.

Histograma: es una representación gráfica de una variable en forma de barras, donde la superficie de cada barra es proporcional a la frecuencia de los valores representados.

HOST: Es cualquier computadora o máquina conectada a una red mediante un número de IP definido y un dominio, que ofrece recursos, información y servicios a sus usuarios.

IGMP: Es un protocolo que permite a un host anunciar su pertenencia multidifusión a grupos a switches y enrutadores vecinos. IGMP es un protocolo estándar que el conjunto de protocolos TCP/IP utiliza para lograr una multidifusión dinámica.

Módulo: Estructura o bloque de piezas que, en una construcción, se ubican en cantidad a fin de hacerla más sencilla, regular y económica. Todo módulo, por lo tanto, forma parte de un sistema y suele estar conectado de alguna manera con el resto de los componentes.

Multidifusión: es un tipo de transmisión de red que permite la comunicación desde una fuente a un grupo seleccionado de destinos.

Pixel: Unidad básica de una imagen digitalizada en pantalla a base de puntos de color o en escala de grises.

Potencia nominal: es la potencia máxima que, según determine y garantice el fabricante, puede suministrar un equipo en funcionamiento continuo, ajustándose a los rendimientos declarados por el fabricante.

QoS: La calidad de servicio se refiere a cualquier tecnología que gestiona el tráfico de datos para reducir la pérdida de paquetes, la latencia y el jitter, o fluctuación, en una red.

RTSP: es un protocolo no orientado a conexión, en lugar de esto el servidor mantiene una sesión asociada a un identificador, en la mayoría de los casos RTSP usa TCP para datos de control del reproductor y UDP para los datos de audio y vídeo, aunque también puede usar TCP en caso de que sea necesario.

Tensión nominal: La tensión nominal es la diferencia de potencial específica para la que se diseña un equipo o una instalación eléctrica.

UPnP: Es un conjunto de protocolos de comunicación que permite a periféricos en red, como computadoras personales, impresoras, pasarelas de Internet, puntos de acceso Wi-Fi y dispositivos móviles, descubrir de manera transparente la presencia de otros dispositivos en la red y establecer servicios de red de comunicación, compartición de datos y entretenimiento.

BIBLIOGRAFÍA

AHONEN, Timo; HADID, Abdenour; & PIETIKÄINEN, Matti. "Face recognition with local binary patterns". Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)», 2004. vol. 3021, pp. 469-481. ISSN 16113349. DOI 10.1007/978-3-540-24670-1_36.

ALBAN, Geesela del Rosario. Sistema domótico de apoyo para personas con discapacidad motriz mediante tecnología móvil y reconocimiento de voz. [en línea] (Trabajo de titulación). (Pregrado). Universidad Técnica de Ambato.2018, Ecuador, [Consulta: 4 diciembre 2020]. Disponiblehttps://repositorio.uta.edu.ec/jspui/bitstream/123456789/28012/1/Tesis_t1401ec.pdf.

BARRENO, Marcelo. Diseño de Prototipo Doméstico de Video Vigilancia con Cámaras IP por internet [en línea]. Universidad San Francisco De Quito. 2013. [Consulta: 4 diciembre 2020]. Disponible en: https://repositorio.usfq.edu.ec/handle/23000/2484.

BERMÚDEZ, José; & **NAVAS, Miguel**. *Montaje en instalaciones domóticas en edificios.* [en línea]. Malaga, IC Editorial. 2015. [Consulta: 25 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/43830.

BRADSKI, Gary; & **KAEHLER, Adrian**. "Learning OpenCV---Computer Vision with the OpenCV Library". IEEE Robotics & Automation Magazine,2008, O'Reilly. vol. 16, no. 3, pp. 100-100. ISSN 1070-9932. DOI 10.1109/mra.2009.933612.

CABALLERO, Edinson. Aplicación Práctica De La Visión Artificial Para El Reconocimiento De Rostros En Una Imagen, Utilizando Redes Neuronales Y Algoritmos De Reconocimiento De Objetos De La Biblioteca Opencv. [en línea]. BOGOTA D.C.: 2017. [Consulta: 26 noviembre 2020]. Disponible en: http://repository.udistrital.edu.co/bitstream/11349/6104/1/CaballeroBarrigaEdisonRene2017.pdf

CÁRDENAS, Geusseppe González; **ANDRÉS, Felipe**; & **GÓMEZ, Silva**. "Diseño e implementación de una Tarjeta de Desarrollo con profundización en desarrollo de aplicación de Touch Sensing". Innovation in Engineering, Technology and Education for Competitiveness and Prosperity, 2013. Disponible en: http://laccei.org/LACCEI2013-Cancun/RefereedPapers/RP157.pdf

CRESPO, Xavi; , *Qué es una FPGA y por qué jugarán un papel clave en el futuro | by Xabi*

Crespo | Planeta Chatbot : todo sobre los Chat bots, Voice apps e Inteligencia Artificial. [blog]. 2017. [Consulta: 26 noviembre 2020]. Disponible en: https://planetachatbot.com/qué-es-una-fpga-y-por-qué-jugarán-un-papel-clave-en-el-futuro-e76667dbce3e.

ESPARZA, Carlos; **TARAZONA, Christian**; **SANABRIA, Esdras**; & **VELAZCO, Daniel**; , "Reconocimiento facial basado en eigenfaces, lbhp y fisherfaces en la beagleboard-xM". *Revista Colombiana De Tecnologias De Avanzada (Rcta)*, 2017. vol. 2, no. 26. ISSN 1692-7257. DOI 10.24054/16927257.v26.n26.2015.2387.

FERNÁNDEZ, Pablo; , Sistema de seguridad y video vigilancia IP para una edificación inteligente con administración y monitoreo remoto.[en linea]. Universidad Israel. Quito. 2017. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/1458.

FUENTES, Oscar; & **PEREZ, Jose**. "Implementación de un sistema de seguridad independiente y automatización de una residencia por medio del internet de las cosas".IEEE Central America and Panama Student Conference, 2018, vol. 2018-Janua, pp. 1-5. DOI 10.1109/CONESCAPAN.2017.8277600.

GONZALEZ, Hirvin; & **VELÁSQUEZ, Sergio**. "Reconocimiento Facial utilizando Viola-Jones y Patrones Binarios". [en línea], 2019. vol. 23, pp. 1. Disponible en: file:///C:/Users/SBryan/Downloads/126-Artículo-287-2-10-20190912.pdf.

GURANGA, Juan.Diseño De Un Sistema Para Seguridad De Una Vivienda Mediante Pasarela Activada Por Voz Y Video A Desarrollarse En La Empresa “Rio Solar Smart Energy” De La Ciudad De Riobamba. Escuela Superior Politécnica De Chimborazo. 2018.

HINOJOSA, Ángel. *Python paso a paso* [en línea]. S.l.: RA-MA-Editorial. 2015. [Consulta: 26 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/107213.

JACOBO, Nestor. Optimizacion de Almacenamiento de Video Utilizando Reconocimiento Facial. Universidad de las Américas Puebla. 2016. Disponible en: http://catarina.udlap.mx/u_dl_a/tales/documentos/mcc/jacobo_a_np/

LAJARA, José. *LabVIEW: entorno gráfico de programación.* [en línea]. Marcombo. S.l.: s.n. 2008. [Consulta: 26 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/35715?page=15.

LÓPEZ, Eugenio. *Raspberry Pi: fundamentos y aplicaciones* [en línea]. S.l.: RA-MA Editorial. 2017. [Consulta: 25 noviembre 2020]. Disponible en: https://elibro.net/es/lc/espoch/titulos/106504?fs_q=Raspberry__Pi:__fundamentos__y__aplicaciones.&prev=fs.

LUDEÑA, Juan. Implementación De Un Sistema De Seguridad Para Supervisión De Niños Entre 2 A 4 Años Usando Visión Artificial. Escuela Superior Politecnica de Chimborazo.Riobamba. 2019. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/13593.

MARTÍ, Silvia. Diseño de un sistema de televigilancia sobre IP para el edificio CRAI de la Escuela Politécnica Superior de Gandia. (Trabajo final de grado). UNIVERSIDAD POLITECNICA DE VALENCIA. España. 2013. Disponible en: https://riunet.upv.es/bitstream/handle/10251/34082/memoria.pdf

MATH WORKS. *Image Processing Toolbox - MATLAB*. [en línea]. 2020. [Consulta: 26 noviembre 2020]. Disponible en: https://es.mathworks.com/products/image.html.

MOCTEZUMA, Alejandra. "Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video-vigilancia". Ingeniería, Investigación y Tecnología, 2016. vol. 17, no. 2, pp. 257-271. ISSN 14057743. DOI 10.1016/j.riit.2016.06.010.

MOREJON, Lenin.*La domótica en Ecuador está en sus primeros pasos y la universidad debe dinamizar su uso*. [en línea]. Guayaquil: 2016. [Consulta: 18 octubre 2020]. Disponible en: https://dialoguemos.ec/2016/08/la-domotica-en-ecuador-esta-en-sus-primeros-pasos-y-la-universidad-debe-dinamizar-su-uso/.

MORENO, Alfredo; , *Arduino: curso práctico* [en línea]. S.l.: RA-MA Editorial. 2018. [Consulta: 25 noviembre 2020]. Disponible en: https://elibro.net/es/lc/espoch/titulos/106517?fs_q=arduino&prev=fs.

NATIONAL INSTRUMENTS CORP. *10 Considerations When Choosing Vision Software - NI*. [en línea]. 2020. [Consulta: 26 noviembre 2020]. Disponible en: https://www.ni.com/es-cr/innovations/white-papers/06/10-considerations-when-choosing-vision-software.html.

NAVARRO, Francisco. *Domótica: gestión de la energía y gestión técnica de edificios* [en línea]. S.l.: RA-MA Editorial. 2015. [Consulta: 24 noviembre 2020]. Disponible en: https://elibro.net/es/lc/espoch/titulos/106476.

NODE RED. *Node-RED*. [en línea]. 2021. [Consulta: 12 enero 2021]. Disponible en: https://nodered.org/.

NODE RED. *Running on Raspberry Pi : Node-RED*. [en línea]. 2020b. [Consulta: 12 enero 2021]. Disponible en: https://nodered.org/docs/getting-started/raspberrypi.

OÑATE, Patricio. DISEÑO Y CONSTRUCCIÓN DE NODOS INTELIGENTES PARA DETECCIÓN DE ARMAS DENTRO DE UNA RED DE VIDEOVIGILANCIA UTILIZANDO VISIÓN ARTIFICIAL [en línea]. Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO. 2020. [Consulta: 13 septiembre 2021]. Disponible en: http://dspace.espoch.edu.ec/bitstream/123456789/13783/1/108T0323.pdf.

PUENTES, Diego. *Los reportes de robos y asaltos a personas y a casas aumentan en Quito | El Comercio*». [en línea]. Quito, 2020. 1 julio 2020. [Consulta: 18 octubre 2020]. Disponible en: https://www.elcomercio.com/actualidad/quito-robos-asaltos-casas-denuncias.html.

RASPBERRY PI FOUNDATION. *Raspberry Pi 4 Tech Specs*. [en línea]. 2020. [Consulta: 25 noviembre 2020]. Disponible en: https://www.raspberrypi.org/products/raspberry-pi-4-model-b/specifications/?resellerType=home.

SÁNCHEZ, Miguel Ángel. Planificación de la gestión y organización de los procesos de montaje de sistemas domóticos e inmóticos [en línea]. Madrid: RA-MA Editorial. 2017. [Consulta: 24 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/106575.

SENTHILSINGH C; & **MANIKANDAN, M.** "DESIGN AND IMPLEMENTATION OF FACE DETECTION USING ADABOOST ALGORITHM". Journal of Theoretical and Applied Information Technology [en línea], 2014. vol. 31, no. 3. [Consulta: 17 noviembre 2020]. ISSN 1817-3195. Disponible en: www.jatit.org.

SONY. *Cámara en red IP Full HD de tipo cilindro SNC-EB642R para exteriores - Sony Pro*. [en línea]. 2020. [Consulta: 3 diciembre 2020]. Disponible en: https://pro.sony/es_ES/products/fixed-cameras/snc-eb642r.

TAPIA, Wilson. Diseño y construcción de un prototipo de sistema de seguridad de una casa utilizando la plataforma Arduino [en línea]. S.l.: Universidad de Machala. 2016. Disponible en: http://repositorio.utmachala.edu.ec/handle/48000/7655.

TELEGRAM.ORG. *Preguntas frecuentes*. [en línea]. 2020. [Consulta: 12 enero 2021]. Disponible en: https://telegram.org/faq#p-que-es-telegram-que-puedo-hacer-aqui.

THAKUR, Amit; & **PRAKASH, Abhishek**; **MISHRA, et al. "**Facial recognition with open Cv». Advances in Intelligent Systems and Computing". Springer, 2020. pp. 213-218. ISBN 9783030372170. DOI 10.1007/978-3-030-37218-7_24. [Consulta: 24 noviembre 2020]. Disponible en: https://doi.org/10.1007/978-3-030-37218-7_24

TOBAJAS, Carlos. *INSTALACIONES DOMOTICAS* [en línea]. S.l.: Ediciones Ceysa. 2014. [Consulta: 24 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/43054.

VALVERT, Jorge. MÉTODOS Y TÉCNICAS DE RECONOCIMIENTO DE ROSTROS EN IMÁGENES DIGITALES BIDIMENSIONALES [en línea]. GUATEMALA: UNIVERSIDAD DE SAN CARLOS DE GUATEMALA. 2006. [Consulta: 4 diciembre 2020]. Disponible en: http://biblioteca.usac.edu.gt/tesis/08/08_0310_CS.pdf.

VÉLEZ, José. *Visión por computador* [en línea]. DYKINSON, S.L. Meléndez Valdés, 61 - 28015 Madrid, 2003 [Consulta: 25 noviembre 2020]. Disponible en: https://elibro.net/es/ereader/espoch/104894?fs_q=vision__por__computador&prev=fs.

VIOLA, Paul; & **JONES, Michael**. "Rapid object detection using a boosted cascade of simple features». Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition". S.l.: s.n., 2001. DOI 10.1109/cvpr.2001.990517. [Consulta: 4 diciembre 2020]. Disponible en: https://ieeexplore.ieee.org/document/990517

WILKINSON, Antony J. "A GUIDE TO MATLAB FOR BEGINNERS AND EXPERIENCED USERS". *International Journal of Numerical Modelling: Electronic Networks, Devices and Fields*», 2003. vol. 16, no. 2, pp. 197-197. ISSN 1099-1204. DOI 10.1002/jnm.479. [Consulta: 4 diciembre 2020]. Disponible en: https://onlinelibrary.wiley.com/doi/epdf/10.1002/jnm.479?src=getftr

ANEXOS

ANEXO A: MANUAL DE USUARIO

El módulo tiene como función principal implementar algoritmos de visión artificial para detectar rostros en cámaras de seguridad comerciales, permitiendo activar alertas o monitorear el estado el módulo de forma remota mediante una conexión a Internet. Se caracteriza porque permite acoplar cámaras de seguridad IP ya instaladas en el domicilio lo cual reduce el costo al no requerir modelos diferentes de cámaras, así como mediante la electrónica se puede monitorear una variedad de sensores, dentro de los principales sensores de movimiento o sensores magnéticos.

Las interfaces para controlar el módulo no tienen ninguna complejidad, se lo puede controlar mediante una aplicación Web o mediante una aplicación de mensajería que es Telegram, la cual se encuentra disponible para los sistemas operativos Android y IOS, así como también es compatible con un computador.

El propósito de este manual es mostrar la configuración que requiere tanto el módulo, como los métodos de control remoto que dispone.

- **Conexión del dispositivo mediante forma remota**

Para poder configurar el dispositivo, es necesario acceder para poder registrar los usuarios en la base de datos o a su vez para ejecutar el algoritmo de visión artificial, para ello podemos conectar la Raspberry Pi 4 a un monitor con entrada HDMI o a su vez podemos acceder mediante una forma remota en un computador a través de la aplicación VNC-Viewer, esta aplicación no permitirá acceder de forma remota al escritorio de la Raspberry Pi 4.

Para ello debemos conectar la Raspberry Pi 4 al router mediante un cable de red, ya que de esta forma estará conectada a la red y podremos obtener la dirección IP, para ello conectar el cable de red en el puerto Ethernet disponible en la Raspberry Pi 4, como se muestra en la Imagen 1.

Imagen 1: Conexión mediante cable Ethernet.

Realizado por: Caiza H., y Yanza A., 2021.

Luego de conectar de debe conectar a la Raspberry Pi 4 a la red eléctrica por medio de la fuente de 5V que viene incluido, a través de su puerto tipo C. Una vez conectado podemos obtener la dirección IP de la raspberry con la aplicación Advanced IP Scanner o cualquier otra aplicación que nos permita conocer que dispositivos están conectados a nuestra red y cuál es su dirección IP. La interfaz es muy sencilla y se puede visualizar en la Imagen 2, en la cual se puede apreciar como identifica a la Raspberry y cuál es la dirección IP que ocupa.

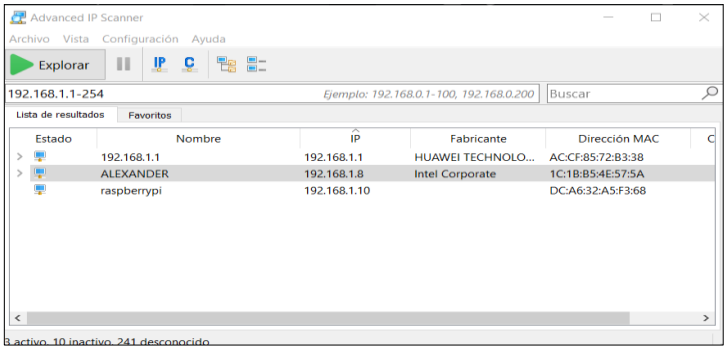


Imagen 2: Obtener dirección IP de la Raspberry Pi 4.

Realizado por: Caiza H., y Yanza A., 2021.

Luego de obtener la dirección IP abrimos la aplicación VNC-Viewer, en la cual en la barra de búsqueda digitamos la dirección IP de la Raspberry como se observa en la Imagen 3.

Imagen 3: Conectar la Raspberry mediante VNC-Viewer.

Realizado por: Caiza H., y Yanza A., 2021.

Al pulsar la tecla Enter empezara a conectarse, en caso de haber ingresado la dirección correcta aparecerá una ventana como se muestra en la Figura1-4, que pedirá al usuario que ingrese nombre de usuario y contraseña. Por defecto el usuario es “pi” y la contraseña es “raspberry”

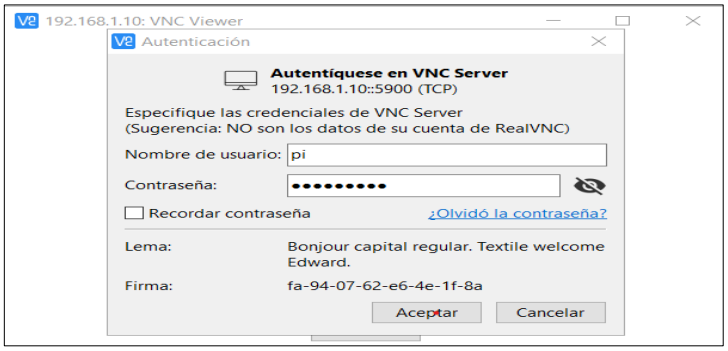


Imagen 4: Ingreso de usuario y contraseña en VNC-Viewer.

Realizado por: Caiza H., y Yanza A., 2021.

Al ingresar con los datos mencionados anteriormente nos aparecerá el escritorio de nuestra Raspberry Pi 4 como se observa en la Imagen 5 y se podrá controlar desde un computador o portátil sin necesidad de conectar periféricos como teclado, ratón o pantalla a la raspberry. De esta forma podremos ejecutar los respectivos códigos desde nuestro computador.

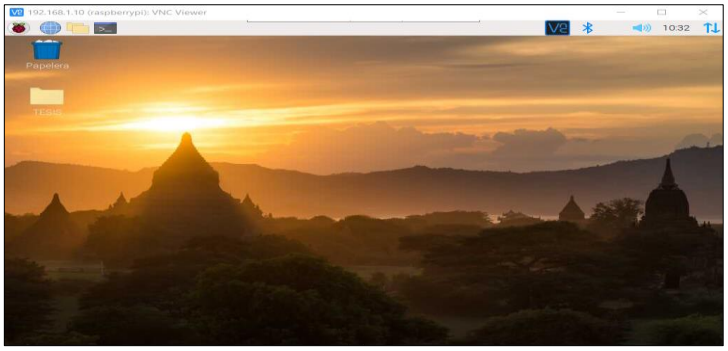


Imagen 5: Control de la Raspberry Pi 4 de forma remota.

Realizado por: Caiza H., y Yanza A., 2021.

- **Ingreso de usuarios a la base de datos**

Para poder ingresar a la base de datos el usuario deberá ejecutar el programa en el terminal de la raspberry mediante el siguiente código **python3 /home/pi/Desktop/TESIS/guide.py** como se muestra en la Imagen 6, el cual ejecutará el programa para ingresar a los usuarios a la base de datos.

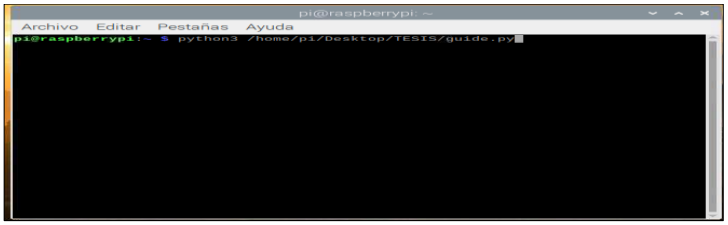


Imagen 6: Ejecutar código de la interfaz gráfica.

Realizado por: Caiza H., y Yanza A., 2021.

Luego de ejecutar el comando aparece la interfaz gráfica que se muestra en la Figura 1-7, en la cual deberemos ingresar el nombre de la persona en la casilla negra, esto permitirá crear o actualizar la información de los usuarios registrados en la base de datos.

Imagen 7: Interfaz gráfica para ingresar usuarios a la base de datos.

Realizado por: Caiza H., y Yanza A., 2021.

Posteriormente se debe dar clic en el botón **OBTENER IMAGEN** el cual, el cual permite obtener las imágenes del rostro de la persona a ser almacenada, para ello es necesario mirar a la cámara mientras se toma las muestras, en la Imagen 8 se observa la carpeta creada con las imágenes que se usaran para entrenar el algoritmo.

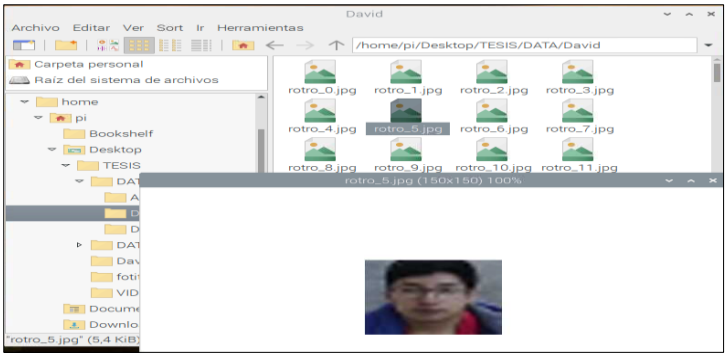


Imagen 8: Imágenes almacenadas en la base de datos.

Realizado por: Caiza H., y Yanza A., 2021.

Luego de tomar las imágenes se procede a dar clic en el botón de **ENTRENAR ALGORITMO,** el cual generara un archivo en formato **xml** que es un el formato que debe tener el entrenador para el algoritmo de reconocimiento de rostro. En la Imagen 9 se observa el archivo creado, el cual permite identificar si el sujeto detectado pertenece o no a la base de datos.

Imagen 9: Algoritmo generado por la interfaz gráfica.

Realizado por: Caiza H., y Yanza A., 2021.

1. Control remoto del sistema.

Para poder controlar el módulo de forma remota existen dos opciones, una mediante una aplicación web desarrollada en NodeRed y otra a través de la aplicación Telegram, para poder acceder desde una red local debemos digitar en cualquier navegador lo siguiente: "***DIRECCION_IP:1880/ui***", la cual llevara directamente a la página como se muestra en la Imagen 10, la cual muestra la imagen principal de la página web.

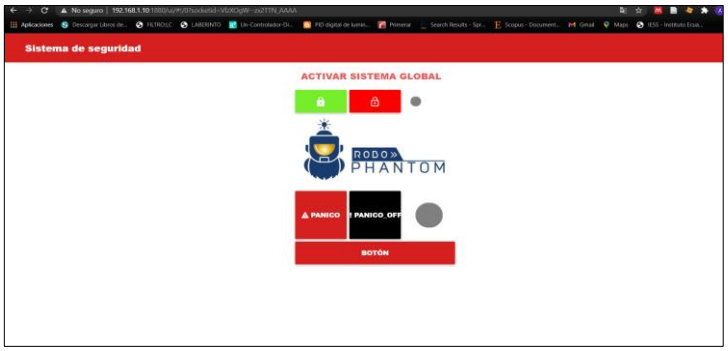


Imagen 10: Pagina web del módulo de seguridad.

Realizado por: Caiza H., y Yanza A., 2021.

Desde aquí se podrá visualizar el estado del módulo, se podrá conocer el estado de los sensores de movimiento y se podrá activar o desactivar tanto el módulo como la sirena en caso de que exista una emergencia, el cual activará la alarma. La ventaja de utilizar una página web es que se puede contratar un servicio VPN que permita manejar la página Web desde cualquier parte, lo cual requiere de un valor adicional que permita realizar esta acción.

Otra forma de controlar el sistema es mediante Telegram, en este caso las instrucciones se realizan mediante comandos para lo cual se debe anteponer **"/"** antes de cada palabra, en la Imagen 11 se observa los comandos principales del sistema.

Imagen 11: Comandos para controlar el módulo a través de Telegram.

Realizado por: Caiza H., y Yanza A., 2021.

Los comandos no necesitan ser escritos completamente en el caso de utilizar en un dispositivo móvil bastara con dar clic sobre el comando para que se ejecute, tanto el comando de encender como de apagar pedirán un mensaje de confirmación al usuario como se muestra en la Imagen 12 para asegurar que realmente quiere realizar esa acción.

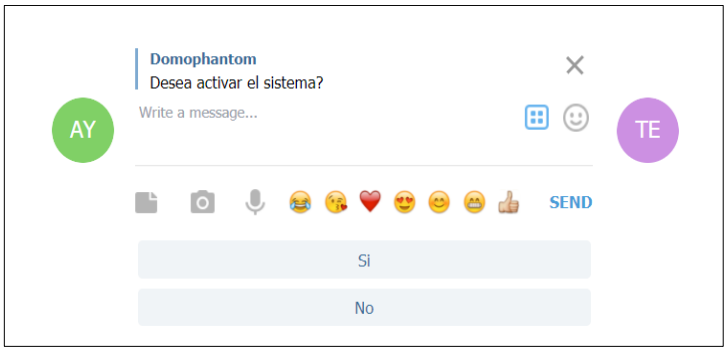


Imagen 12: Pregunta de confirmación para activar el módulo.

Realizado por: Caiza H., y Yanza A., 2021.

Posteriormente el módulo enviara un mensaje confirmando la acción que se decidió utilizar como se observa en la Imagen 13.

Imagen 13: Mensaje de confirmación.

Realizado por: Caiza H., y Yanza A., 2021.

En el módulo estará conectado a sus GPIO las entradas y salidas que permitan interactuar con los dispositivos de seguridad, tanto sensores como actuadores, estos han sido configurados previamente. Para obtener la información de la cámara se procede a utilizar algún protocolo como es **rtsp,** el cual permite enviar la información de la cámara directamente al algoritmo sin necesidad de otro dispositivo.Para el almacenamiento de información se utiliza el programa MotionEye que es un programa que permite monitorear cámaras de seguridad sin necesidad de un NVR, ya que cumple funciones similares. En la Imagen 14 se observa la interfaz de este programa.

Imagen 14: Interfaz del programa MotionEye.

Realizado por: Caiza H., y Yanza A., 2021.

Para ingresar una cámara debemos acceder mediante la dirección IP de la cámara a través del puerto 8765 como se muestra en la Imagen 15.

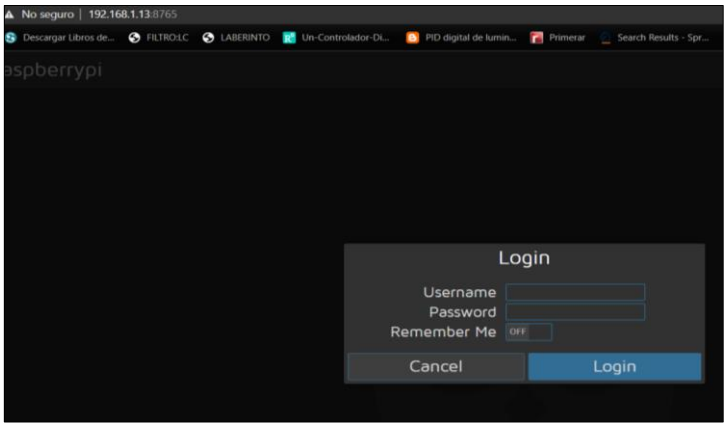


Imagen 15: Interfaz del programa MotionEye.

Realizado por: Caiza H., y Yanza A., 2021.

Por defecto el **username** es **admin**, y no tiene ninguna contraseña, una vez ingresado nos mostrara una ventana similar a la de la Imagen 16.

Imagen 16: Interfaz del programa MotionEye.

Realizado por: Caiza H., y Yanza A., 2021.

En la parte superior izquierda en el icono de las tres líneas permite añadir cámaras o visualizar las cámaras que cuenta el sistema como se muestra en la Imagen 17.

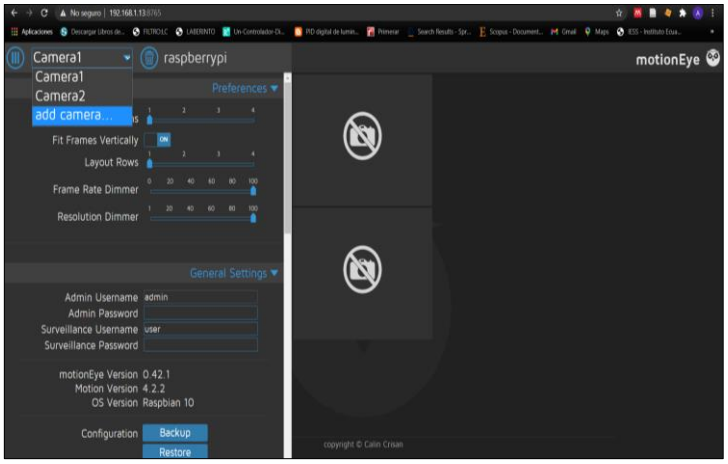


Imagen 17: Menú para añadir o ver la configuración de las cámaras.

Realizado por: Caiza H., y Yanza A., 2021.

Para añadir una cámara se debe ir a a opción **add camera**, la cual mostrara una ventana como el que se muestra en la Imagen 18, en la que se debe seleccionar el tipo de cámara que se utiliza.

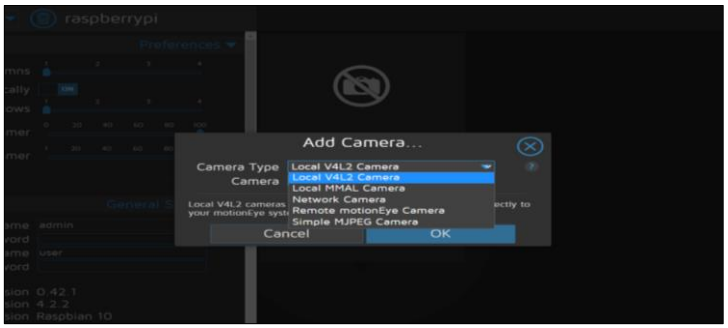


Imagen 18: Menú para añadir cámaras.

Realizado por: Caiza H., y Yanza A., 2021.

Para este caso particular la cámara que utiliza el módulo es una cámara IP, por lo que se deberá añadir la dirección **rstp** de la cámara, así como su nombre de usuario y contraseña, esta información viene en el manual de usuario de cada cámara como se muestra en la Imagen 19.

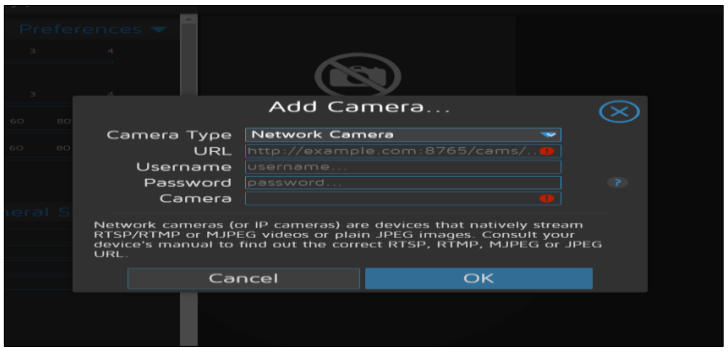


Imagen 19: Ingreso de datos de una cámara IP.

Realizado por: Caiza H., y Yanza A., 2021.

Una vez completado los pasos se podrá obtener inmediatamente acceso a la información de la cámara de seguridad. Para el almacenamiento de información debemos selección la dirección de destino en la opción **File Storage**, por defecto se guarda en la carpeta de instalación de MotionEye como se observa en la Imagen 20.

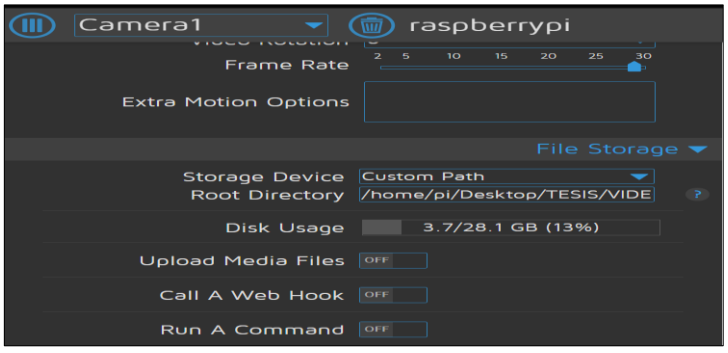


Imagen 20: Configuración de almacenamiento de la cámara.

Realizado por: Caiza H., y Yanza A., 2021.

En el mismo menú encontramos la opción **Upload Media Files**, para activar se debe dar clic en la parte de **off** y se activará el sistema, al hacer esto se activará una serie de opciones donde debemos seleccionar las opciones que nos dispone para almacenar la información en una nube, para este caso se elige la opción de **Google Drive** como se observa en la Imagen 21.

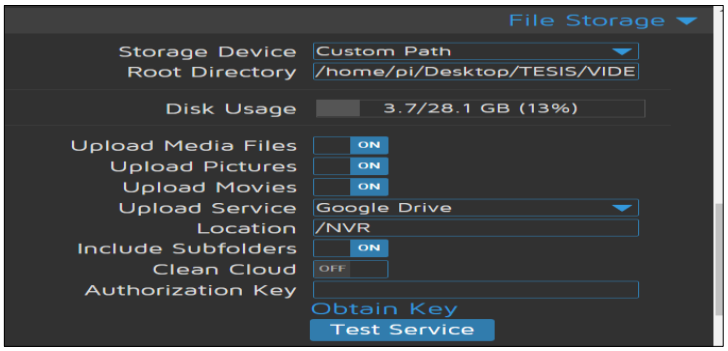


Imagen 21: Configuración de almacenamiento en la nube.

Realizado por: Caiza H., y Yanza A., 2021.

De esta forma podremos almacenar tanto imágenes como video en la nube, garantizando que la información quede respaldada. Para evitar que exista un consumo excesivo es recomendable almacenar la información en determinado momento, para ello se debe configurar en el menú de **Movies** como se muestra en la Imagen 22 donde en la opción de **Recording Mode** se debe seleccionar la opción **Motion Triggered**, la cual permite que se almacene solo cuando la cámara detecte movimiento, de la misma forma en la opción **Maximum Movie Length** se puede establer el tiempo de duración del video.

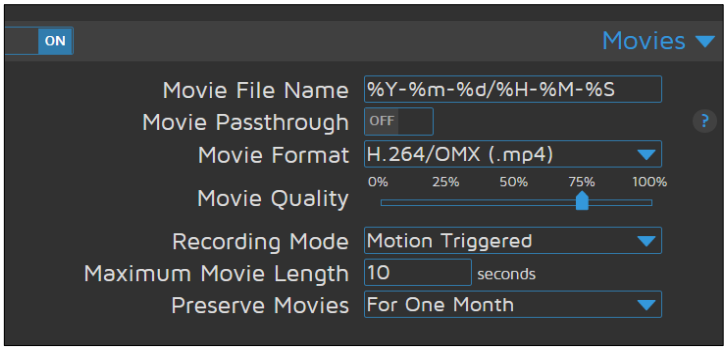


Imagen 22: Configuración de video mediante el detector de movimiento.

Realizado por: Caiza H., y Yanza A., 2021.

De esta forma se garantiza que no va estar almacenando constantemente la información, reduciendo la cantidad de espacio para el almacenamiento de la misma forma permite almacenar la información solo por cierto periodo de tiempo, que va desde un día hasta mantener almacenado la información para siempre, pero es recomendable seleccionar un periodo de tiempo ya que de esta forma no se necesitara expandir la unidad de almacenamiento.

ANEXO B: CÓDIGO FUENTE

Código para crear la base de datos y el entrenamiento

```
from tkinter import *
from tkinter import filedialog
from PIL import Image
from PIL import ImageTk
import cv2
import imutils
import os
import numpy as np
import tkinter as tk
import tkinter.font as tkFont
```

```
faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_default.xm
```

```
def entrenamiento():
    carpeta = '/home/pi/Desktop/TESIS/DATA'
    lista_personas = os.listdir(carpeta)
    print('Lista de personas: ', lista_personas)

    labels = []
    facesData = []
    label = 0

    for nameDir in lista_personas:
     carpeta = carpeta + '/' + nameDir
     print('Leyendo las imágenes')

     for fileName in os.listdir(pcarpeta):
        print('Rostros: ', nameDir + '/' + fileName)
        labels.append(label)
        facesData.append(cv2.imread(carpeta+'/'+fileName,0))
     label = label + 1

    face_recognizer = cv2.face.LBPHFaceRecognizer_create()

    print("Entrenando...")
    face_recognizer.train(facesData, np.array(labels))
    face_recognizer.write('modeLBPHFace.xml')
```

-Función para detectar el rostro

```
def deteccion():
 global cap
 personName=entry.get()
 dataPath= '/home/pi/Desktop/TESIS/DATOS'
 personPath = dataPath + '/' + personName
 if not os.path.exists(personPath):
     print('Carpeta creada: ',personPath)
     os.makedirs(personPath)
 count = 0
 while True:
    ret, frame = cap.read()
    if ret == False: break
    frame =  imutils.resize(frame, width=640)
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    auxFrame = frame.copy()
    faces = faceClassif.detectMultiScale(gray,1.2,5)
    for (x,y,w,h) in faces:
        cv2.rectangle(frame, (x,y),(x+w,y+h),(0,255,0),2)
        rostro = auxFrame[y:y+h,x:x+w]
        rostro = cv2.resize(rostro,(150,150),interpolation=cv2.INTER_CUBIC)
        cv2.imwrite(personPath + '/rotro_{}.jpg'.format(count),rostro)
        count = count + 1

            cv2.imshow('frame',frame)
            k =  cv2.waitKey(1)
            if k == 27 or count >= 10:
                cap.release()
                cv2.destroyAllWindows()
                break
```

-Función Iniciar

```
def Iniciar():
    global cap
    cap=cv2.VideoCapture(0,cv2.CAP_DSHOW)
    deteccion()
```

-Crear interfaz gráfica.

```
root= Tk()
root.geometry('500x300')
root.title("Ingreso de la base de datos")
root.configure(bg='#E9DD26')

entry = Entry(root)
entry.grid(row=0, column=1, padx=5, pady=5)

entry.config(justify="right", state="normal",bg="#000000",fg="#FFFFFF")
personName=entry.get()

etiqueta =Label(text="INGRESE EL NOMBRE DE USUARIO", bg="#E9DD26")
etiqueta.grid(row=0, column=0, padx=5, pady=5)

imagen=ImageTk.PhotoImage(file="loguito_opt.png")
btnObtImg = Button(root, text="OBTENER IMAGEN",activebackground="#9B0F0F", command= Iniciar,
btnObtImg.place(x=60, y=200)

btnEntrenar = Button(root, text="ENTRENAR ALGORITMO",activebackground="#E74026", command= ent
btnEntrenar.place(x=300, y=200)

lbllogo = Label(root, image=imagen,width=150, height=68)
lbllogo.place(x=150, y=80)
root.mainloop()
```

- **Reconocimiento facial**

-Importación de librerías y declaración de variables

```
import cv2
import os
import RPi.GPIO as GPIO
from time import time
GPIO.setwarnings(False)
GPIO.setmode(GPIO.BOARD)
GPIO.setup(15, GPIO.IN)
GPIO.setup(37, GPIO.OUT)
GPIO.setup(38, GPIO.OUT)


dataPath = '/home/pi/Desktop/TESIS/DATOS'
imagePaths = os.listdir(dataPath)
```

-Lectura de sensor de movimiento

```
if GPIO.input(15)==0:
   GPIO.output(37, 0)
elif GPIO.input(15)==1:
   print ("Persona detectada")
   GPIO.output(37, 1)
```

-Obtención de la imagen y detector de rostros

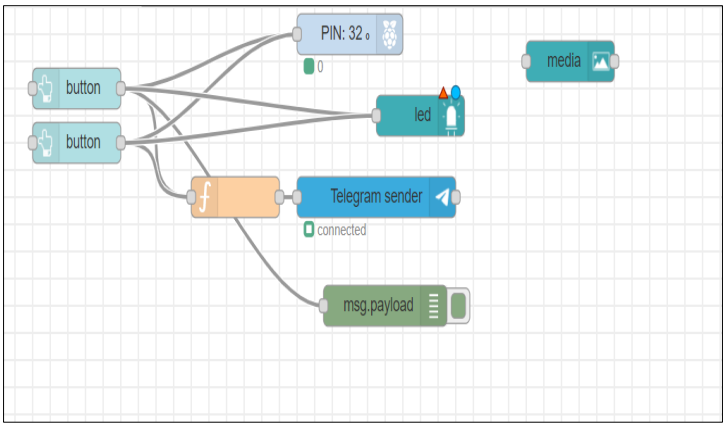
```
face_recognizer = cv2.face.LBPHFaceRecognizer_create()
face_recognizer.read('/home/pi/Desktop/TESIS/modeLBPHFace1.xml')
def rescaleFrame(frame, scale=0.30):
 width=int(frame.shape[1]*scale)
 height=int(frame.shape[0]*scale)
 dimensions=(width,height)
 return cv2.resize(frame,dimensions, interpolation=cv2.INTER_AREA)
cap = cv2.VideoCapture('rtsp://admin:camarita01@192.168.1.10:554/Streaming/Channels/101/'
faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_defaul
count = 0
count1 = 0
while True:
 ret,frame = cap.read()
 frame_resized =rescaleFrame(frame)
 if ret == False: break
 gray = cv2.cvtColor(frame_resized, cv2.COLOR_BGR2GRAY)
 auxFrame = gray.copy()

 faces = faceClassif.detectMultiScale(gray,
scaleFactor=1.1,
minNeighbors=5,
maxSize=(400,400))

for (x,y,w,h) in faces:
   rostro = auxFrame[y:y+h,x:x+w]
   rostro = cv2.resize(rostro,(150,150),interpolation= cv2.INTER_CUBIC)
   result = face_recognizer.predict(rostro)

   cv2.putText(frame_resized,'{}'.format(result),(x,y-5),1,1.3,(255,255,0),1,cv2.LINE_AA)
```

-Reconocimiento facial

```
    if result[1] < 80:
        cv2.putText(frame_resized,'{}'.format(imagePaths[result[0]]),(x,y-25),1,1.1,(0,255
        cv2.rectangle(frame_resized, (x,y),(x+w,y+h),(0,255,255),2)

        tiempo_final = time()
        tiempo_ejecucion = tiempo_final - tiempo_inicial
        print("El tiempo reconocimiento es: ",tiempo_ejecucion)
        print("Sistema desactivado")
        GPIO.output(38, 0)
        count = count + 1
    else:
        cv2.putText(frame_resized,'Desconocido',(x-10,y-20),1,0.8,(0,0,255),1,cv2.LINE_AA)
        cv2.rectangle(frame_resized, (x,y),(x+w,y+h),(0,0,255),2)
        cv2.imwrite('Desconocido1.png',frame_resized)
        GPIO.output(38, 1)
        count1 = count1 + 1
```

- **Configuración de NodeRed**

-Creación de la interfaz gráfica.



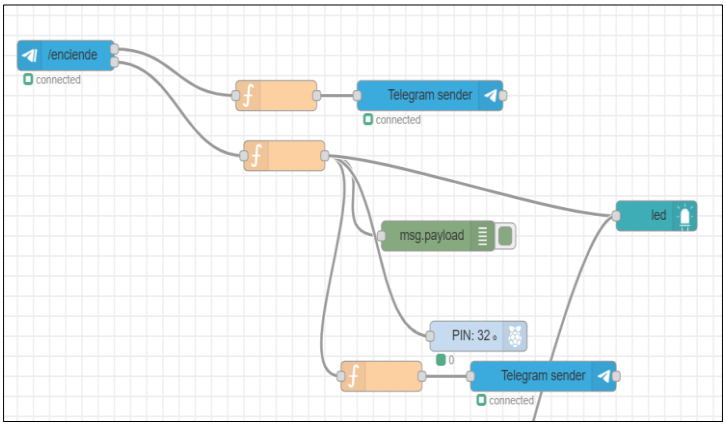
Realizado por: Caiza H., y Yanza A., 2021.

-Función para enviar mensaje a través de Telegram.

```
if (msg.payload == true)
{ msg.payload = {chatId:-288133984,type:"message",content:"Sistema activado"}
return msg}
else
  { msg.payload = {chatId:-288133984,type:"message",content:"Sistema desactivado"}
return msg}
```

Realizado por: Caiza H., y Yanza A., 2021.

-Programación para crear los comandos



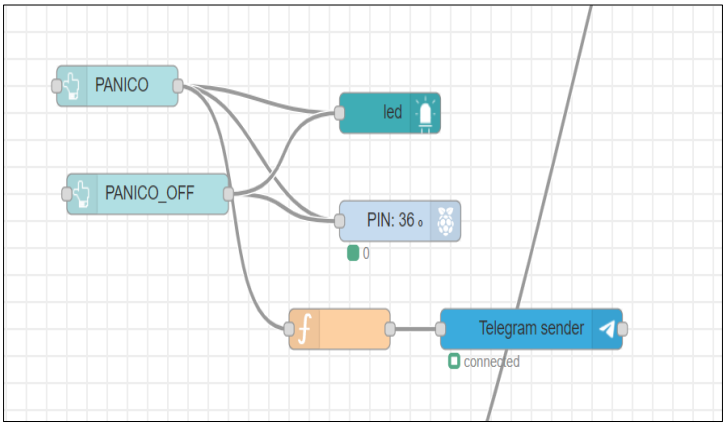
Realizado por: Caiza H., y Yanza A., 2021.

-Código para crear mensaje de pregunta al usuario

```
context.global.keyboard = { pending : true };

var opts = {
  reply_to_message_id: msg.payload.messageId,
  reply_markup: JSON.stringify({
    keyboard: [
      ['Si'],
      ['No']],
      'resize_keyboard' : true,
      'one_time_keyboard' : true
  })
};

msg.payload.content = 'Desea activar el sistema?';
msg.payload.options = opts;

return [ msg ];
```

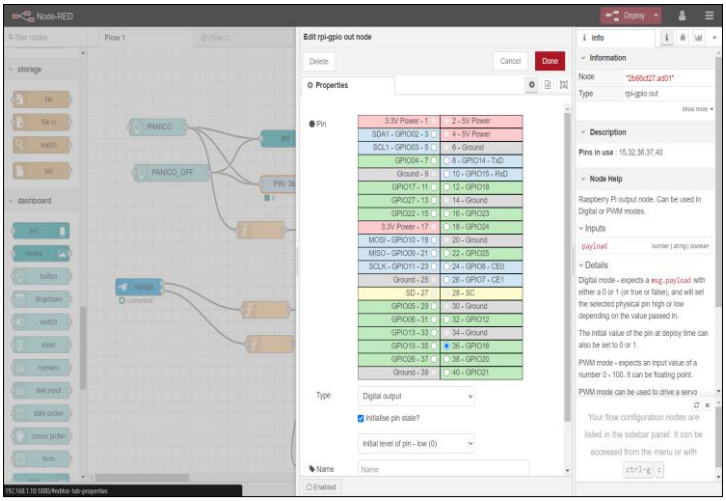
Realizado por: Caiza H., y Yanza A., 2021.

-Creación de botón de pánico.



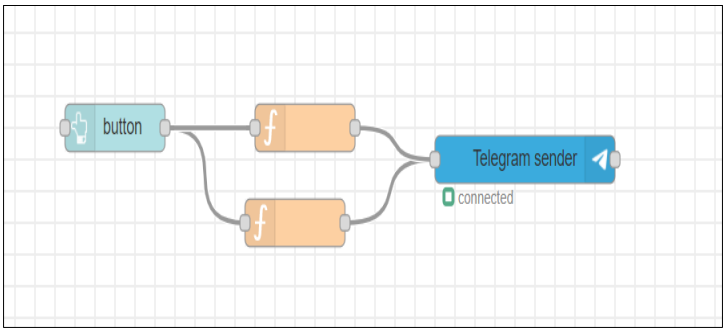
Realizado por: Caiza H., y Yanza A., 2021.

-Configuración de una GPIO como salida en la Raspberry Pi 4



Realizado por: Caiza H., y Yanza A., 2021.

-Configuración para enviar la imagen de alerta por medio de Telegram.



Realizado por: Caiza H., y Yanza A., 2021.

-Programación para enviar la fotografía desde la Raspberry Pi 4.

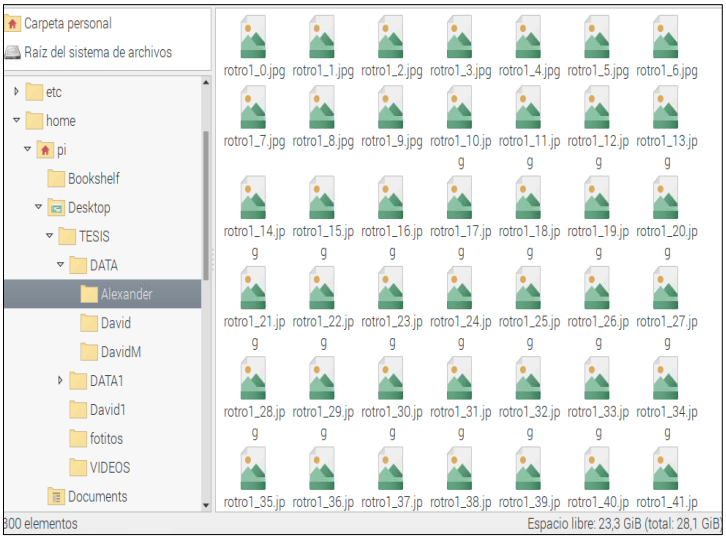
```
if (msg.payload == true)
{ msg.payload = {chatId:-288133984,type:"photo",content:"/home/pi/Desktop/TESIS/fot
return msg}
```

Realizado por: Caiza H., y Yanza A., 2021.

ANEXO C: TOMA DE MUESTRAS

- **Base de datos en la Raspberry Pi 4**

Se almacenan todas las muestras obtenidas mediante la interfaz gráfica.



Realizado por: Caiza H., y Yanza A., 2021.

El algoritmo obtiene únicamente el rostro del individuo el cual se procesará en el algoritmo de reconocimiento facial para su identificación.

Realizado por: Caiza H., y
Yanza A., 2021.

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS DEL APRENDIZAJE

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 03 / 12 / 2021

INFORMACIÓN DEL AUTOR/A (S)
Nombres – Apellidos: ALEXANDER SEBASTIÁN YANZA QUINGATUÑA HENRY VLADIMIR CAIZA LEMA
INFORMACIÓN INSTITUCIONAL
Facultad: INFORMÁTICA Y ELECTRÓNICA
Carrera: ELECTRÓNICA Y AUTOMATIZACIÓN
Título a optar: INGENIERO EN ELECTRÓNICA Y AUTOMATIZACIÓN
f. Analista de Biblioteca responsable: Lcdo. Holger Ramos, MSc.

Firmado electrónicamente por:
HOLGER GERMAN RAMOS UVIDIA

1874-DBRA-UPT-2021