ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES

DISEÑO DE UN PROTOTIPO DE SISTEMA INMÓTICO BASADO EN RECONOCIMIENTO FACIAL USANDO VISIÓN ARTIFICIAL, PARA CONTROLAR EL ACCESO EN ÁREAS RESTRINGIDAS

Trabajo de titulación

Tipo: Proyecto Técnico

Presentado para optar al grado académico de:

INGENIERO EN ELECTRÓNICA, CONTROL Y REDES INDUSTRIALES

AUTOR: CRISTIAN ANDRÉS PAÑI PIZARRO

DIRECTOR: ING. PABLO EDUARDO LOZADA YÁNEZ

Riobamba-Ecuador

2020

Yo, Cristian Andrés Pañi Pizarro, declaro que el presente trabajo de titulación es de mi autoría y los resultados del mismo son auténticos. Los textos en el documento que provienen de otras fuentes están debidamente citados y referenciados.

Como autor asumo la responsabilidad legal y académica de los contenidos de este trabajo de titulación. El patrimonio intelectual pertenece a la Escuela Superior Politécnica del Chimborazo.

Riobamba, 20 de junio del 2020

Cristian Andrés Pañi Pizarro
140125567-2

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

CARRERA DE INGENIERIA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES

El Tribunal de trabajo de titulación certifica que: El trabajo titulación tipo: Proyecto Técnico, **"DISEÑO DE UN PROTOTIPO DE SISTEMA INMÓTICO BASADO EN RECONOCIMIENTO FACIAL USANDO VISION ARTIFICIAL, PARA CONTROLAR EL ACCESO EN ÁREAS RESTRINGIDAS",** de responsabilidad del señor **CRISTIAN ANDRÉS PAÑI PIZARRO**, 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. Jorge Luis Hernández Ambato **PRESIDENTE DEL TRIBUNAL**		2020-10-19
Ing. Pablo Eduardo Lozada Yánez **DIRECTOR DEL TRABAJO DE TITULACION**		2020-10-19
Dr. Geovanny Estuardo Vallejo Vallejo **MIEMBRO DE TRIBUNAL**		2020-10-19

iii

DEDICATORIA

El presente trabajo lo dedico a mis padres pues gracias a su cariño y apoyo me han ayudado a fórjame en la persona hoy en día soy, me ensañaron las reglas de la vida y darle importancia a los pequeños detalles que se van presentando en el día a día, a mis hermanos los cuales mediante sus consejos y su apoyo me han ayudado a sobrellevar los obstáculos los cuales se pueden presentar en el camino hacia una meta.

Cristian

AGRADECIMIENTO

Primeramente, a Dios por todas las bendiciones brindadas en el transcurso de la vida, a mis padres por todo su amor, cariño, preocupación y apoyo sin esperar nada a cambio por estar junto a mí en los momentos difíciles, a mis hermanos por ser un pilar muy importante y ser la principal fuente de inspiración para llegar a cumplir las metas. A mis amigos y amigas quienes nunca me abandonaron sin importar lo difícil de la situación. Mil gracias a todos.

Cristian

TABLA DE CONTENIDO

INDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

INDICE DE ANEXOS

INDICE DE ABR EVIATURAS

APP: Aplicación

AAM: Modelo de Apariencia Activa

CAGR: Taza anual de crecimiento compuesto

DC: Corriente Continua (Directa)

EBGM: Grafica de Pareo Elástico

ENCMP: Estrategia Nacional para el Cambio de la Matriz Productiva

GLP: Licencia Publica General

GPIO: Pines de entrada y salida de propósito general

GUI: Interfaz Gráfica de Usuario

HMM: Modelo Oculto de Márkov

ICA: Análisis de Componentes Independientes

IDE: Interfaz de Desarrollo Integrado

LBP: Patrones Binarios Locales

LBPH: Los Histogramas de Patrones Binarios Locales

LDA: Análisis Lineal Discriminante

NPN: Se refiere que el transistor está formado por dos capas de material N y una capa de material P.

NSTC: Consejo Nacional de Ciencia y Tecnología

OpenCV: Visión Artificial Abierta

PCA: Análisis de Componentes Principales

PIR: Sensor Infrarrojo Pasivo

RFID: Identificación por radiofrecuencia

RGB: Red Green Blue

SQL: Lenguaje de Consulta Estructurado

SVM: Maquias de Vectores de Soporte

UNASUR: Unión de Naciones Suramericanas

URL: Localizador Uniforme de Recursos

V: Voltios

WPAN: Redes de Área Personal.

WLAN: Redes de Área Local

RESUMEN

El objetivo del presente trabajo de titulación fue el diseño de un prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas, se propuso el alcance de los siguientes objetivos: como principal fue el diseño del prototipo que cumpla todos los requisitos, además de investigar algoritmos de visión artificial mediante los cuales sea posible realizar el reconocimiento facial de una persona, para ello se hizo uso de clasificadores en cascada para la detección del rostro con la ayuda del algoritmo conocido como los histogramas de patrones binarios locales (LBPH), luego de las pruebas realizadas se llegó a la conclusión de que el algoritmo previamente diseñado cumple con los requisitos planteados, una vez definido el algoritmo de visión artificial, se procedió a definir el método de comunicación del algoritmo de visión artificial con los diferentes sensores y actuadores, esta comunicación se la realizó mediante cable par trenzado debido a las diferentes ventajas que posee, además de esto, el sistema se constituyó por una aplicación móvil la cual recibirá una notificación, la comunicación entre la placa controladora y la aplicación (app) se la realizó mediante internet. Del proceso de diseño e implementación se obtuvo como principal conclusión el uso de una tarjeta controladora raspberry pi la cual se acopló a las necesidades propias del sistema. Sin embargo, con el uso de la misma se hizo necesario el tratamiento de las señales de entrada y salida desde y hacia la placa controladora. Se recomienda tomar las debidas protecciones al usar voltajes superiores a los 3.3 VDC el cual es el voltaje de operación de la placa controladora, esto debido a que la raspberry no cuenta con protección desde los pines hacia la tarjeta por lo cual una incorrecta manipulación puede causar el daño completo de la raspberry.

Palabras Claves: <INTELIGENCIA ARTIFICIAL>, <VISIÓN ARTIFICIAL>, <SISTEMA INMÓTICO>, <RECONOCIMIENTO FACIAL>, <CONTROL DE ACCESO>, <SENSORES>, <ACTUADORES>.

ABSTRACT

The objective of the present degree work was the design of a prototype of an inmotic system based on facial recognition using artificial vision, to control access in restricted areas, the achievement of the following objectives was proposed: as the main one was the design of the prototype that meets all the requirements, in addition to investigating artificial vision algorithms through which it is possible to perform facial recognition of a person, for this, cascade classifiers were used for face detection with the help of the algorithm known as binary pattern premises histograms (LBPH), after the tests carried out it was concluded that the previously designed algorithm meets the requirements set out, once the artificial vision algorithm was defined, the communication method of the artificial vision algorithm was defined with the different sensors and actuators, this communication was carried out via cable p ar braided due to the different advantages it has, in addition to this, the system was constituted by a mobile application which will receive a notification, the communication between the controller board and the application (app) was carried out through the internet. The main conclusion of the design and implementation process was the use of a raspberry pi controller card which was coupled to the system's own needs. However, its use made it necessary to treat the input and output signals from and to the controller board. It is recommended to take the proper protections when using voltages higher than 3.3 VDC, which is the operating voltage of the controller board, this because the raspberry does not have protection from the pins to the board, therefore incorrect manipulation can cause complete damage to the raspberry.

Keywords: <ARTIFICIAL INTELLIGENCE>, <ARTIFICIAL VISION>, <IMMOTIC SYSTEM>, <FACIAL RECOGNITION>, <ACCESS CONTROL>, <SENSORS>, <ACTUATORS>.

INTRODUCCION

El constante avance de la tecnología ha permito el surgimiento de nuevos campos en el área de la innovación, en los últimos años se ha venido trabajando y desarrollando proyectos basados en la utilización de cámaras las cuales pretenden emular la visión humana con el fin de controlar procesos de una manera más óptima y eficiente, a este campo de la tecnología se lo conoce como visión artificial.

El principal campo de acción de esta tecnología es la industria, siendo utilizado principalmente en control de calidad de productos al inicio o final de la línea de producción. Así como en los últimos años se la ha venido usando en el área de la agroindustria para monitorización de cultivos, determinar si estos se encuentran contaminados o con algún tipo de plaga, este proceso se los realiza con el fin de obtener productos de mejor calidad.

La domótica e inmótica son otros de los campos de la tecnología las cuales está tomando fuerza en la actualidad. Esto debido a la conciencia ecológica desarrollada en la sociedad, pues el principal objetivo de estas dos tecnologías es el ahorro de los recursos utilizados en una vivienda, un edificio o un lugar de negocio o comercio, como son el agua, energía eléctrica, etc. Además, está orientado a la automatización de los diversos procesos presentes dentro de una edificación como apertura de puestas y persianas, control de temperatura interna, etc.

Quizá uno de los procesos a controlar más importantes dentro de la domótica e inmótica es el control de acceso a un área determinada, pues de esto depende la seguridad tanto de los personas, bienes materiales, monetarios e información.

Es por este motivo se desarrolla el presente trabajo de titulación, el cual lleva por tema “diseño de un prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas”. Este sistema se diferenciará de los dispositivos y sistemas analizados anteriormente pues además de realizar la detección facial para dar permiso a usuarios autorizados a ingresar a una determinada área, será capaz de almacenar la fecha y hora de ingreso de cada persona a determinada área en una base de datos y contará con un subsistema el cual al detectar un posible intento de ingreso a la fuerza a un área será capaz de almacenar el rostro de esa persona y enviar esta captura a la persona encargada de la seguridad o al dueño del edificio o empresa.

CAPITULO I

1 DIAGNOSTICO DEL PROBLEMA

1.1 Antecedentes

El mercado global de automatización de la vivienda y edificios fue valorado en $ 39,607 millones en 2016, y se proyecta que alcance $ 81,645 millones para 2023, creciendo a una tasa anual de crecimiento (CAGR) de 11,2% de 2017 a 2023. La domótica es la utilización de terminales inteligentes, es un sistema de automatización para controlar el hogar electrodomésticos y equipos. Se espera que el aumento del conocimiento sobre el uso eficiente de la energía, el aumento de los precios de la electricidad y los avances tecnológicos impulsen el crecimiento del mercado de la automatización del hogar. Por otra parte, el aumento de las preocupaciones de seguridad y protección impulsó la adopción del sistema de domótica, lo que impulsó el crecimiento del mercado. (Preksha V. 2017)

Otro proyecto digno de ser mencionado en el campo de la inmótica en nuestro país es el edificio donde funcionaba la sede de la unión de naciones suramericanas (UNASUR), este edificio fue concebido para reducir al máximo el consumo de recursos, para el ahorro de agua se diseñó un método para reutilizar el agua lluvia, se instalaron luces led en todos los ambientes para ahorrar el consumo energético, el cual también es disminuido con la instalación de celdas fotovoltaicas capaces de generar energía para el 24% de la edificación en general. Gracias a la incorporación de estas y otras tecnologías, así como su diseño esta edificación ha sido merecedora del premio IAI Best Desing Award.

Con el avance de la tecnología los aspectos de la seguridad también han ido actualizándose es así que uno de sus principales campos como lo es el control de acceso a emigrado desde los sistemas mecánicos o aquellos que necesitaban de una persona para activarlos, a procesos totalmente automatizados con diferentes tipos de tecnologías y dispositivos. Es importante realizar un estudio adecuado, segmentando las zonas, los grupos de acceso, los horarios permitidos, el nivel de acceso de cada usuario, medir la cantidad de personas o carros que transitan por cada zona y establecer claramente los objetivos de cada control de acceso. (MDA, 2014).

1.2 Delimitación del tema

1.2.1 *Realidad del tema a nivel mundial*

Los sistemas y dispositivos los cuales podemos encontrar en el mercado a nivel mundial de este campo de la tecnología son muy variados, partiendo del sistema creado por la empresa española FERMAX, el cual diseño un video portero capaz de ser controlado desde un smartphone, dicho sistema consta de un dispositivo instalado en la entrada del edificio, el cual tiene incorporado una cámara mediante la cual el usuario es capaz de visualizar a la persona intentando ingresar y para permitir su entrada presionando un botón desde su celular. El proyecto Amanora Gateway Tower en India es considerado uno de los edificios más lujos del mundo escogió a este sistema de video portero como su sistema de seguridad.

El sistema diseñado por la empresa Kimaldi está basado en un módulo de visión artificial para control de presencia de los empleados de una empresa y un módulo de control de accesos mediante huella digital y tarjeta con tecnología de identificación por radiofrecuencia (RFID), además cuenta con un módulo de reconocimiento facial conocido como HanvonFaceID el cual está orientado al uso de control de acceso y de presencia.

Dispositivos como control de presencia Facial Cool-A fueron diseñados para brindar la opción de ser usados para control de accesos mediante reconocimiento facial, lector de huella o contraseña. FacePass es otro de los dispositivos diseñados para el control de acceso y presencia de empleados en una empresa. UFACE4 es un dispositivo diseñado para el control de acceso cuenta con reconocimiento facial y cuenta con un relé orientado a permitir la apertura de una puerta o la activación de una sirena. Sin embargo, el inconveniente de estos dispositivos es sus costos elevados.

1.2.2 *Realidad del tema a nivel regional*

A nivel del continente americano se han venido dando varios avances en el campo del control de acceso, es así en el estado de Querétaro dos estudiantes crearon un sistema basado en algoritmos desarrollados en el software Matlab y con un controlador arduino para permitir leer el rostro de una persona y activar un relé usado para abrir una puerta.

En Brasil la unión de dos grandes empresas RealNetworks y Seventh hicieron posible la introducción a ese país de un algoritmo desarrollado por la universidad de Massachusetts, el cual

es capaz de diferenciar y reconocer miles de rostros y estimar sentimientos. Se prevé utilizar este algoritmo para distintos fines entre ellos el control de acceso.

En la Universidad Politécnica de Cartagena se desarrolló un sistema de control de acceso vehicular mediante reconocimiento de placas se prevé utilizar este código en el control de acceso de personas.

1.2.3 *Realidad del tema a nivel local*

En nuestro país los sistemas desarrollados en esta línea de investigación se dieron en la Universidad Técnica Particular de Loja donde se desarrolló un algoritmo para control de acceso basado en facial local Binary Patterns, este algoritmo servía para enviar una señal la cual se utilizaría para abrir una puerta basándose en el reconocimiento facial.

En la Universidad Politécnica Nacional se desarrolló un sistema de control de acceso basado en el perfil lateral de una persona, el proyecto se centró en comparar dos métodos de reconocimiento facial el primero se basaba en autentificación mediante procesamiento de imágenes y el segundo mediante redes neuronales.

Además, en nuestra institución en el año 2018 se elaboró una tesis con el tema reconocimiento y creación del modelo facial 3D mediante sistema de video aplicado a la seguridad usando inteligencia artificial. En este proyecto se creó un modelo 3D del rostro del usuario utilizando software Matlab.

Como se pudo evidenciar en la investigación realizada en este documento, el campo de la tecnología orientada al control de acceso se encuentra en constante avances por este motivo se ha decidido plantear como tema de trabajo de titulación el diseño de un prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas. Este sistema se diferencia de los dispositivos y sistemas analizados anteriormente pues además de realizar la detección facial para dar permiso a un determinado usuario para ingresar al área controlada, será capaz de almacenar la fecha y hora de ingreso en una base de datos además que cuenta con un subsistema el cual al detectar un posible intento de ingreso por la fuerza, será capaz de almacenar el rostro de la persona que se encuentra frente a la cámara y enviar una captura tomada en tiempo real mediante una aplicación móvil al encargado de seguridad de dicha empresa, fabrica o negocio.

1.3 Objetivos

1.3.1 *Objetivo General*

- Diseño de un prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas.

1.3.2 *Objetivos Específicos*

- Investigar algoritmos de visión artificial para conseguir el reconocimiento facial de una persona mediante cámaras.
- Diseñar un sistema inmótico el cual realizara sus diferentes acciones basadas en el algoritmo de visión artificial ya realizado.
- Determinar el mejor método para realizar la comunicación entre el controlador y los diferentes actuadores que ayudaran a realizar a apertura de las diferentes áreas en el sistema inmótico.
- Comprobar el funcionamiento del prototipo implementado en su totalidad y realizar las pruebas necesarias de manera que actué de acuerdo a los requerimientos.

1.4 Justificación aplicativa

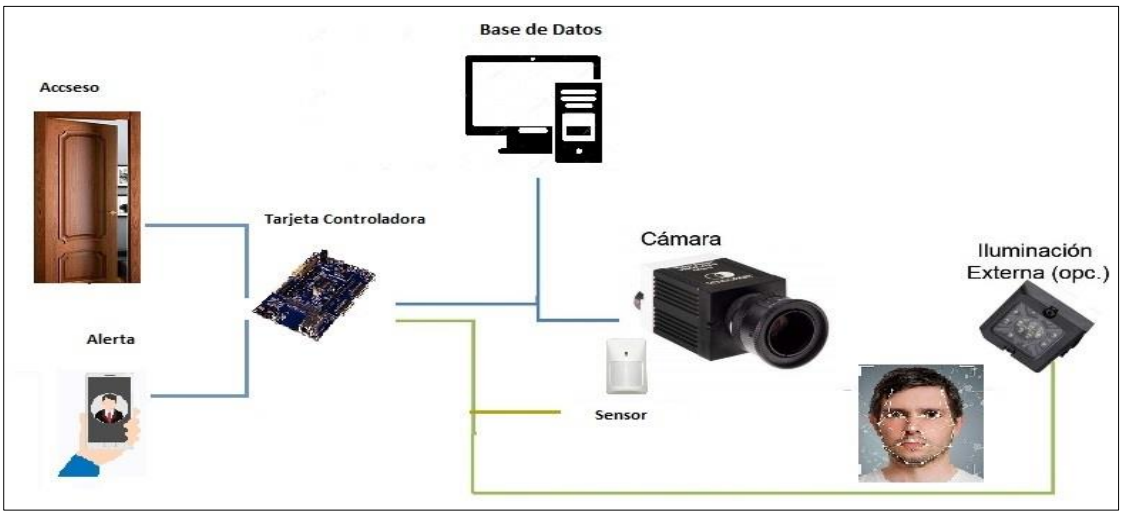


Figura 1: Funcionamiento del sistema.
Realizado por: Pañi, Cristian, 2020

La presente propuesta está orientada al diseño de un prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas.

El procedimiento de acción del sistema propuesto es el siguiente:

- El sistema está compuesto por un sensor de presencia o un sensor de movimiento el cual es el encargado de encender la cámara una vez haya realizado la detección de movimiento.
- La combinación de cámara y algoritmo de reconocimiento facial, es el encargado de detectar si existe un rostro en la escena, si la lectura es positiva se tomará una captura del rostro.
- El rostro es comparado con una base de datos del personal autorizado para ingresar al área en cuestión. Si este coincide con el perfil de alguna de las personas ingresadas en la base de datos se le permite el ingreso.
- Además, el sistema almacena la fecha hora, nombre, cedula y cargo de la persona a la cual se le permite el ingreso.
- Si alguien intenta ingresar por la fuerza a un área controlada, el sistema es capaz de almacenar una captura del rostro de dicha persona y enviar la misma además de una alerta al encargado de seguridad de dicha empresa, fábrica o negocio.

Como se mencionó anteriormente la ventaja del sistema propuesto ante los existentes es el almacenamiento de los datos de la persona autorizada para el ingreso y el aviso ante un intento de ingreso por la fuerza en una determinada área.

Este proyecto está alineado con la política del buen vivir puesta en marcha por el gobierno nacional, en el cual dice lo siguiente:

- La infraestructura productiva, la tecnología y el conocimiento son elementos fundamentales para fortalecer los circuitos comerciales solidarios, los encadenamientos productivos y las economías de escala capaces de dinamizar la competitividad sistémica del territorio nacional. (Plan Nacional de desarrollo 2017-2021)

- Otro de los aspectos fundamentales para el desarrollo económico del país fue la aprobación de la Estrategia Nacional para el Cambio de la Matriz Productiva (ENCMP), que buscó el fortalecimiento del sistema productivo basado en eficiencia e innovación. Para esto, se intensificaron esfuerzos encaminado a: 1) Generación de entornos y competitividad sistémica (clima de negocios, impulso de la compra pública, etc.); 2) Desarrollo y fortalecimiento de cadenas productivas (cacao, maricultura, metalmecánica, farmacéutica, turismo, software, etc.); y 3) Potenciamiento de industrias básicas (petroquímica, siderurgia, cobre, aluminio, astilleros y pulpa).

    - Los resultados son todavía parciales y requieren de políticas que apuntalen lo avanzado para conseguir efectos más plausibles de desarrollo de nuevas industrias y la incorporación de tecnología en los procesos de producción. (Plan Nacional de desarrollo 2017-2021)

Además, una de las metas propuestas de este plan es, incrementar la utilidad de las maquinarias, equipos y tecnologías productivas considerando criterios de obsolescencia programática a 2021. (Plan Nacional de desarrollo 2017-2021)

CAPITULO II

2 FUNDAMENTOS TEORICO

2.1 Domótica e Inmótica

2.1.1 *Conceptos*

Domótica termino orientado exclusivamente al ambiente del hogar y la vivienda, realiza el control de los procesos y tecnologías utilizados por las personas que habitan un espacio físico, conocido como casa o vivienda, además de brindar seguridad y confort, así como mantener una óptima comunicación entre el usuario y el sistema.

El termino inmótica hace referencia a la coordinación y gestión de los recursos e instalaciones con que se encuentran equipadas las edificaciones, así como su capacidad de comunicación, regulación y control. Está orientada a generar un mejor ambiente laboral para las personas que realizan sus actividades diarias dentro de las mismas. (B. Luque, R Navas,2015, pág. 152)

2.1.2 *Características de un sistema inmótico*

2.1.2.1 *Comunicación confiable*

La comunicación entre dispositivos los cuales forman parte del sistema inmótico debe darse de una manera precisa y eficiente, de este atributo depende que los paquetes de datos producidos en los diferentes sensores lleguen completos, de esta manera la unidad de control pueda tomar la mejor decisión de acuerdo a los mismos. (CEDOM, 2016)

2.1.2.2 *Comunicación segura*

La información manejada en un sistema inmótico, debe contar con la seguridad necesaria para evitar ser leída o utilizada por terceros, esto puede producir acciones dentro del sistema las cuales vulneraran la seguridad y privacidad de los usuarios.

2.1.2.3 *Fácil implementación y utilización*

El objetivo de una instalación inmótica es mejorar y hacer más fácil la calidad de vida de los usuarios, esto conlleva a que el control de los diferentes procesos debe ser muy sencillo, pues en varios casos los que utilizan el sistema son personas con poco o nulo conocimiento sobre cómo se realizan la programación o puesta en marcha de dicho proceso. (CEDOM, 2016)

2.1.2.4 *Bajo costo y protección de inversión*

Los dispositivos utilizados deben ser de bajo costo para evitar el costo elevado en el sistema en general y pueda llegar a todas las personas, además el ciclo de vida de los dispositivos y los componentes de la red deben ser acorde con los dispositivos del hogar con el fin de poder utilizar los mismo y no generar otra inversión al usuario.

2.1.3 ***Tipos de Topologías***

Se refiere a la forma de conexión entre los distintos dispositivos los cuales conforman una red, el tipo de topología a utilizar se decide en la etapa de diseño, para esto se debe tomar en cuenta la parte física y lógica de los componentes a utilizar. La topología determina únicamente forma de conexión, aspectos como distancia entre dispositivos, la taza de transmisión, el tipo de señales entre otros, no se estudian en esta instancia, pero pueden verse afectados por la topología utilizada.

2.1.3.1 *Topología en Bus*

Consiste en un cable largo el cual se extiende a lo largo de toda la red y en el cual se conectan los diferentes dispositivos, este tipo de topología es multipunto.

Su principal ventaja es la sencillez de instalación. Es importante encontrar el camino más eficiente para tender el cable troncal, para luego conectar los nodos mediante líneas de conexión de longitud variable. De esta manera se puede conseguir ahorro en la cantidad de cable a ser utilizado. (M. Miguel,2013, pág. 12)

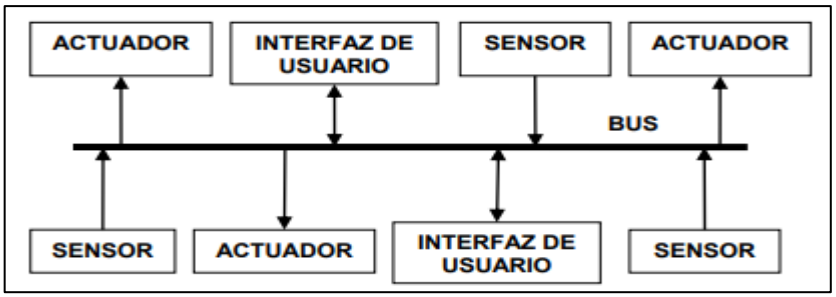


Figura 1-2: Topología Bus

Realizado por: Cupueran, M.; Ortiz, J. 2015

2.1.3.2 *Topología Estrella*

Se basa en un sistema de control centralizado, en donde los dispositivos están conectados a un elemento principal o controlador. Los dispositivos no están conectados entre sí directamente por lo tanto no existe tráfico directo de datos entre los dispositivos, estos son enviados al controlador y este es el encargado de distribuirlos. (J. Rivera, 2016, pag.23)

Este tipo de topología brinda ventajas en la facilidad de instalación de nuevos dispositivos en la red y al producirse una falla en uno de los dispositivos ese no afecta a los demás.

La desventaja presentada se encuentra cuando el controlador falla colapsa todo el sistema pues este es el encargado de toda la comunicación de la red, además al procesar toda la información de la red este dispositivo debe tener una gran capacidad de procesamiento.

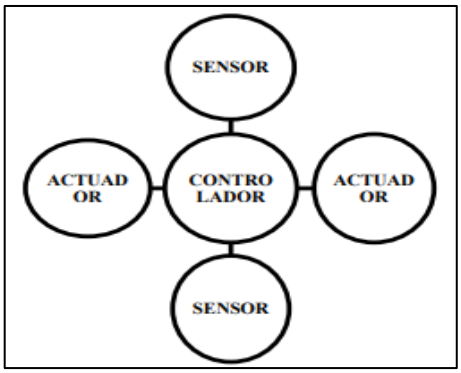


Figura 2-2: Topología Estrella

Realizado por: Cupueran, M.; Ortiz, J. 2015

2.1.3.3 *Topología Anillo*

En esta topología los datos pasan atreves de todos los dispositivos hasta encontrar su destino en una solo dirección. Cada dispositivo tiene un repetidor incorporado.

Esta topología es fácil de instalar y configurar cada dispositivo esta enlazado solamente con sus vecinos. Para remover o instalar un dispositivo solo hace falta quitar dos conexiones. La principal desventaja es si un dispositivo falla la comunicación en toda la red colapsa y si se quiere instalar un nuevo dispositivo es necesario para toda la red. (Cupueran, M.; Ortiz, J. 2015, pág. 18)

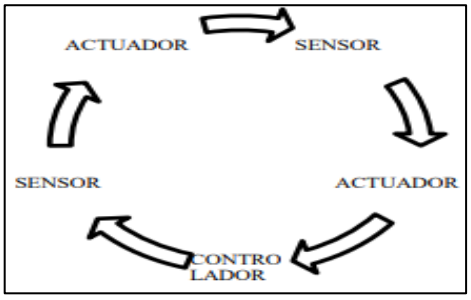


Figura 3-2: Topología Anillo

Realizado por: Cupueran, M.; Ortiz, J. 2015

2.1.3.4 *Topología Malla*

En esta topología cada dispositivo de la red tiene una conexión con los demás dispositivos, sin embargo, él envió de datos solo se produce entre dos dispositivos.

Las principales ventajas se dan cuando los datos solo son enviados desde un dispositivo emisor hacia un receptor eliminando el problema de tiempo de espera en la recepción y entrega de datos, además En esta topología no existe el riesgo de cuando uno de los dispositivos falle afecte la comunicación entre los demás.

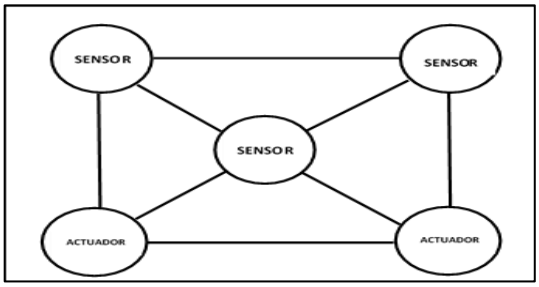


Figura 4-2: Topología Malla

Realizado por: Pañi, C. 2019

2.1.4 *Arquitectura*

La arquitectura de un sistema desde un punto de vista técnico es uno de las características, aquí se definirá la forma de conexión de todos los elementos y dispositivos en una edificación.

2.1.4.1 *Arquitectura Centralizada*

En este tipo de arquitectura un solo controlador gestiona toda la información de la red, es decir se encarga de recibir los datos de los diferentes sensores, la procesa y dependiendo de esto acciona un actuador el cual se encarga de realizar un proceso. El control de los sensores y actuadores se lo realiza en forma simultánea y el costo de dichos dispositivos es relativamente bajos al ser de tipo universal (gran oferta y económicos).

Su fácil instalación y uso, así como si un sensor o actuador falla no afecta al resto del sistema son las principales ventajas presentadas, mientras entre las desventajas tenemos su cantidad de cableado es significativo, el controlador debe tener una gran capacidad de procesamiento para poder procesar la información de todos los dispositivos conectados y además un fallo en el mismo produce un colapso total de sistema. (Alabuela, M.; Mañay, C. 2018, pág. 7)

Además, su capacidad de empleabilidad es reducida y es necesario una interfaz para comunicación con el usuario.

Figura 5-2: Arquitectura centralizada

Fuente: Alabuela, M.; Mañay, C. 2018

2.1.4.2 *Arquitectura Descentralizada*

Esta arquitectura consta de varios controladores los cuales son los encargados de procesar la información de un conjunto de sensores y actuadores conectados en él. La comunicación entre los diferentes controladores los cuales componen una red se la realiza mediante un bus de datos. Esto elimina la necesidad de tener un solo controlador encargado de procesar la información de toda la red.

La principal ventaja presentada se da cuando un controlador produce un error esto no afecta a todo el sistema, además, la cantidad de cableado se reduce respecto a la arquitectura anterior y su empleabilidad es fácil. (Alabuela, M.; Mañay, C. 2018, pág. 8)

Las desventajas constan de un elevado costo, requiere una computadora para la programación de los controladores y poder determinar cuándo se da una falla cual es el dispositivo que la produce además es necesario un alto nivel de conocimiento de programación.

Figura 6-2: Arquitectura centralizada

Fuente: Alabuela, M.; Mañay, C. 2018

2.1.4.3 *Arquitectura Distribuida*

En este tipo de arquitectura cada sensor y actuador es capaz de procesar la información que recibe, es decir cada uno de estos dispositivos actúa como un controlador. Un bus de datos recorre toda la red conectando los distintos dispositivos. Para la programación es necesario una computadora, una pantalla táctil o una consola. (Alabuela, M.; Mañay, C. 2018, pág. 8)

La principal ventaja es la misma analizada en la arquitectura descentralizada pues cuando ocurre un fallo en un dispositivo esto no afecta a toda la red, sus dispositivos poseen la característica de universalidad, su desventaja radica en el nivel de dificultad para su programación.

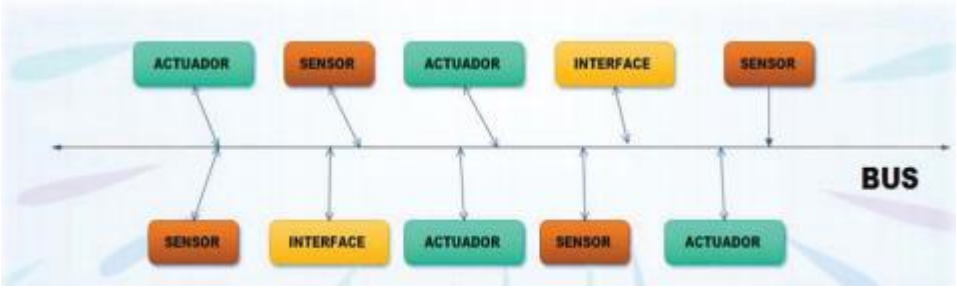


Figura 7-2: Arquitectura distribuida

Fuente: Alabuela, M.; Mañay, C. 2018

2.1.5 *Medios de transmisión*

El medio elegido condiciona tanto la distancia máxima, así como la velocidad de transferencia y el método de acceso al medio, entre otros parámetros. Según como sea la transmisión distinguimos entre medios guiados, si se sigue un camino físico como en un cable de cobre o en una fibra óptica, o inalámbricos, cuando la señal no sigue un camino, sino que se propaga por el aire. (C. Francisco,2002, pág. 29)

Para la seleccionar el medio de transmisión dentro de un sistema es necesario tener en cuenta factores como el ambiente en el cual se va a instalar, los dispositivos instalados en la edificación, así como la estructura del mismo.

2.1.5.1 *Medios Alámbricos*

Son también conocidos como medios guiados, son aquellos que utilizan cable o fibra para la comunicación, dentro de esta clasificación encontramos los siguientes:

Par trenzado: está conformado por dos hilos conductores trenzados entre sí y aislados para evitar interferencias externas o de otros cables ubicados alrededor. Es capaz de transmitir voz y datos mediante el mismo medio. Es el método de transmisión de información más antiguo y el más utilizado en la actualidad por su bajo costo y fácil instalación. Usualmente en un cable par trenzado podemos encontrar varias parejas de hilos conductores trenzados y de diferentes colores para su mejor distinción. (C. Francisco,2002, pág. 29)

Cable Coaxial: Formado por un hilo de cobre en el centro recubierto con un material aislante sobre el cual se colocó una malla la cual sirve para la conexión a tierra y sobre esta otra capa de material aislante. La principal ventaja presentada sobre el par trenzado es un mejor de bloqueo

ante interferencias, la desventaja está en su dificultad para el manejo pues es un cable rígido y su menor tasa de transmisión.

Fibra óptica: está compuesto por un filamento de vidrio muy delgado en su centro rodeado de vidrio de aleación diferente, esto permite la reflexión y difracción del haz de la luz que ingresa por la fibra permitiendo así el envío de información. Su velocidad de transmisión es muy alta, permite el envío de datos a largas distancias sin producirse la perdida de información, su principal desventaja es el alto costo. (C. Francisco,2002, pág. 32)

2.1.5.2 *Medios Inalámbricos*

Conocidos también como medios no guiados su principal característica es la transmisión de datos mediante ondas sin la utilización de cableado, se propagan mediante radiofrecuencia e infrarrojo. En esta clasificación tenemos las siguientes:

Bluetooth: esta tecnología permite la conexión de dispositivos en una distancia no mayor a diez metros. En un sistema inmótico se lo puede utilizar para la monitorización de las imágenes captadas por las cámaras o para control de alarmas desde un Smartphone.

ZigBee: Al igual de bluetooth esta tecnología está orientada a rede inalámbricas de área personal (WPAN), la principal diferencia frente a la tecnología anterior es su área de cobertura la cual se extiende de 10 a 75 metros. Además, tiene la capacidad de ahorro de energía al poder entrar en modo dormido donde es capaz de reducir su consumo energético. Por ello es utilizado en el campo de la inmótica para la instalación en sensores. (Cupueran, M.; Ortiz, J. 2015, pág. 56)

Infrarrojo: es un estándar donde se define la transmisión y recepción mediante rayos en el espectro infrarrojo. Esta transmisión se utiliza comúnmente en mandos a distancia. Actualmente está cada vez más en desuso por el abaratamiento de las tecnologías de radiofrecuencia a pesar de tener la ventaja de ser inmune a interferencias electromagnéticas. (C. Francisco,2002, pág. 12)

WIFI: Actualmente es la más utilizada debido a su velocidad de transmisión de datos y su ancho de banda cada vez mayor. Principalmente utilizada en redes de área local (WLAN), la conexión de los dispositivos se rige bajo los estándares IEEE 802.11y su velocidad está definida por las variantes conformadas por 802.11 a/b/g/n/ac.

2.1.6 *Protocolos de comunicación*

La elección del protocolo de comunicación dentro de un sistema es quizá el factor más importante, pues será el encargado de dar el formato a los mensajes los cuales contendrán los datos enviados desde los sensores hacia los controladores o actuadores. Para esto es importante tomar en cuenta la interconectividad entre protocolos, pues en varios casos existen protocolos incapaces de comunicarse con otros.

Los protocolos se dividen en dos grandes grupos:

El primero conformado por los protocolos estándares, los cuales son capaces de interconectarse con otros los cuales se encuentran dentro de este mismo grupo, su gran ventaja radica en la posibilidad de cualquier fabricante puede crear aplicaciones o dispositivos basados en estos protocolos, lo cual posibilita el abaratamiento de los costos, pues se tendrá una variedad de productos o dispositivos más amplia, para un mejor entendimiento se lo puede comparar con un software libre. (J. Maestre,2015, pag.55)

El segundo grupo conformado por protocolos propietarios, la principal diferencia frente a los anteriores se da en la falta de interconexión, lo cual indica la no comunicación con ningunos otros protocolos. Tienen la ventaja de un costo reducido frente al grupo anterior, sin embargo, la vida útil de este protocolo está ligada con la vida útil de la empresa, si esta desaparece los sistemas los cuales hayan sido desarrollados por las misma no podrán ser actualizados quedando cada vez más obsoletos. Además, los fabricantes no podrán desarrollar nuevos productos basados en este protocolo, dando como resultado una escaza variedad de dispositivos a ser utilizados, estos dependerán de la empresa desarrolladora del protocolo.

A continuación, se realizará una pequeña descripción de algunos protocolos utilizados en el campo de la inmótica:

2.1.6.1 *Tecnología X-10*

Los elementos que pueden integrar esta tecnología son los actuadores, controladores, el medio de transmisión, los receptores y los sensores. Este sistema, comunica a los transmisores y receptores enviando y recibiendo señales sobre la línea de energía, las transmisiones X-10 se sincronizan con el paso por cero de la corriente alterna, las interfaces a la línea de poder proporcionan una onda de 60Hz, con un retraso máximo de 100µs desde el paso por cero de la corriente alterna, el máximo retraso entre el comienzo del envío y los pulsos de 120KHz es de 50µs, la transmisión

completa de un código X-10 necesita once ciclos de corriente, divididos en tres grupos, donde los dos primeros ciclos representan el código de inicio, los cuatro siguientes ciclos representan el denominado código de casa (letras A-P) y los siguientes cinco ciclos representan el código numérico (1-16) o el código de función (encender, apagar, aumento de intensidad, etc.). (J. Maestre,2015, pag.55)

Este bloque completo se transmite siempre dos veces, separando cada 2 códigos por tres ciclos de la corriente, excepto para funciones de regulación de intensidad, éstos se transmiten de forma continua (por lo menos dos veces) sin separación entre código

Una de las principales ventajas de X-10 reside en que no es necesaria la instalación de nuevos cables para conectar dispositivos ya que usa la propia línea eléctrica de la vivienda, lo que convierte a X-10 en una opción muy barata para el diseño de instalaciones domóticas no muy complejas. Cualquier fabricante puede crear dispositivos X-10, así como venderlos, pero sin embargo debe utilizar los circuitos del fabricante escoces que creó la tecnología. Eso no significa que sea un protocolo propietario y además el royalty de estos circuitos integrados es muy bajo comparado. (J. Maestre,2015, pag.56)

2.1.6.2 *Protocolo Z-WABE*

Es un protocolo inalámbrico estandarizado su implementación es sencilla, utiliza topología en malla con un máximo de dispositivos conectados de 232 con una separación entre ellos de 20 metros en el interior de la edificación y en el exterior la separación debe ser de 30 metros.

Dentro de las principales ventajas tenemos el consumo de energía es bajo y tiene un gran alcance de señal, además su ancho de banda es bajo. Al ser un protocolo estándar es capaz de conectarse con dispositivos, productos y equipos de diversos fabricantes, solo es necesario la instalación de módulos Z-WABE. (J. Maestre,2015. pág. 102)

2.1.6.3 *Protocolo BACnet*

Tiene la capacidad de conectarse con dispositivos, productos y equipos de varios fabricantes, la configuración de estos equipos tiene un grado de dificultad medio. Además, todos los dispositivos deben estar conectados a una misma red.

BACnet está basado en un modelo denominado “cliente-servidor” y sus mensajes se denominan “demandas de servicio”, una máquina cliente envía un mensaje de demanda de servicio a una

máquina servidor, la que realiza el servicio e informa los resultados al cliente, este protocolo proporciona una arquitectura escalonada en la cual existe una estación de trabajo en el extremo superior que controla el siguiente escalón, este controla al siguiente, y así sucesivamente, esta red escalonada requiere de entradas (Gateway, convertidor de datos efectiva) para traducir el protocolo usado por las redes de trabajo y los muchos protocolos que pueden usar los equipos escalones abajo, estas entradas son dispositivos de elevado costo que elevan el precio total del sistema, así como su administración y mantenimiento. (J. Huidobro, R. Millán, 2010, pág. 137)

2.1.6.4 *Protocolo LonWorks*

Es un protocolo estándar muy comúnmente utilizado para edificaciones tanto de pequeña como gran envergadura, es principalmente utilizado en aplicaciones como sistemas de control de grandes edificios, aeropuertos entre otros, no se recomienda su uso en sistemas residenciales pues su costo es elevado y para estos existen otras tecnologías más baratas.

Consiste en un conjunto de dispositivos inteligentes conocidos como nodos los cuales se comunican atreves de un medio físico al cual están conectados y comparten un protocolo en común. Nos brinda la capacidad de programar a estos nodos con el fin de realizar una acción luego de cumplir una o varias condiciones. (J. Maestre,2015, pag.60)

La característica que también se debe tomar en cuenta es la velocidad de mediante la cual la información es transmitida de un elemento o dispositivo a otro dentro de la red; las principales causas o factores que afectan esta velocidad de transmisión son, el medio por el cual se transmiten, y el protocolo de comunicación por el cual se comunican. Los sistemas inmóticos se pueden diseñar para utilizar un único protocolo de comunicación, con diferentes medios de transmisión, teniendo en cuenta que la velocidad de transmisión está dada por el medio de transmisión, mas no por el protocolo por el cual se están comunicando. (J. Maestre,2015, pag.61)

2.1.6.5 *KNX*

Es el más usado por todo el continente europeo, fue desarrolla con el fin de contar con un protocolo estandarizado para el uso en edificios, consta de tres formas de funcionamiento las cuales se detallará a continuación:

A-mode: conocido como modo automático (automatic mode), es esta forma de funcionamiento los equipos vienen previamente programados y operan bajo la filosofía Plug&Play, en la cual un

dispositivo puede ser utilizado inmediatamente después de su conexión a la red de alimentación no es necesario ninguna programación extra. (J. Huidobro, R. Millán, 2010, pág. 137, pág. 126)

E-mode: conocido como modo fácil (easy mode), los dispositivos de esta funcionalidad vienen programados desde la fábrica, pero a diferencia de la anterior forma es necesario una pequeña programación sencilla la cual se la realiza a través de un controlador o mediante micro interruptores en el mismo dispositivo.

S-mode: conocido como modeo sistema (system mode), aquí los todos los dispositivos deben ser instalados antes de ser configurados, este es el modo de funcionamiento más difícil pues para su programación es necesario conocimientos avanzados en programación, por lo tanto, solo la red solo podrá ser configurada por un experto. (J. Huidobro, R. Millán, 2010, pág. 137, pág. 127)

Otra de la ventaja es la variedad de medios de transmisión utilizados por KNX los cuales son los siguientes: par trenzado tipo 0, par trenzado tipo 1, ondas portadoras, radio frecuencia e internet protocolo.

2.2 Vision Artificial

2.2.1 Definición

Visión artificial es el campo de la tecnología mediante el cual se pretende emular el sentido de la vista de un ser humano, con el fin de desarrollar sistemas capaces de tomar decisiones dependiendo de la información extraída de imágenes tomadas de un ambiente.

En el campo de la visión artificial el uso de cámaras o cualquier otro dispositivo de adquisición de imagen reemplaza a la visión de una persona, estos serán los encargados de adquirir imágenes, las cuales entrarán a una etapa de procesamiento con el fin de obtener sus propiedades físicas o rastros característicos con los cuales el sistema realizara una toma de decisiones con respecto a estas.

La principal finalidad de la visión artificial es dotar a la máquina la capacidad para ver lo que ocurre en el mundo real, y así poder tomar decisiones para automatizar cualquier proceso.

2.2.2 *Etapas de un sistema de visión artificial*

Captura: con la ayuda de un acamara o cualquier otro dispositivo se adquieren una imagen o un conjunto de imágenes del ambiente en donde se pretende trabajar.

Preprocesador: se elimina las partes de la imagen donde no se encuentra el objeto o atributo necesario para el análisis, además, se realiza el resaltado de las características principales de la imagen.

Segmentación: divide la imagen en secciones iguales para un mejor procesamiento.

Reconocimiento: de acuerdo a las características principales de la imagen se decide si esta contiene o no el objeto o atributo a ser reconocido en el sistema.

2.2.3 *Aplicaciones*

La visión artificial va ganando campos de aplicación día tras día, esto debido a su eficiencia y flexibilidad para adaptarse a cualquier área de trabajo es así en la actualidad se la viene combinando con otras áreas de la tecnología como domótica, inmótica, drones, robots, etc.

El amplio espectro de aplicaciones cubierto por la visión artificial, se debe a que permite extraer y analizar información espectral, espacial y temporal de los distintos objetos. La información espectral incluye frecuencia (color) e intensidad (tonos de gris). La información espacial se refiere a aspectos como forma y posición (una, dos y tres dimensiones). La información temporal comprende aspectos estacionarios (presencia y/o ausencia) y dependientes del tiempo (eventos, movimientos, procesos). (Juárez, Rodríguez, 2017)

A continuación, se mencionará algunas aplicaciones del a visión artificial:

Medición o calibración: mediante visión artificial es posible obtener características de un determinado objeto como su área, longitud, espesor, etc. Esto se podría aplicar para asegurar un determinado objeto tenga las medidas especificadas en su etapa de diseño, eliminando la necesidad de tener una persona realizando esta medición manualmente.

Detección de fallas: utilizado mucho en la industria para la supervisión de los productos terminados, para asegurar una perfecta presentación en los productos sin fallas en su forma física

ni acabados asegurando cumplir las características dadas a cada producto en la etapa de diseño. (V. Artificial, 2012)

Verificación: enfocado también a productos terminados de la industria o productos agrícolas de manera de asegurar a los consumidores un producto en excelentes condiciones. En la actualidad esta aplicación se da principalmente en la verificación de los sembríos agrícolas de manera de poder evitar la pérdida de los mismo por plagas u otros factores.

Reconocimiento: principalmente orientado a reconocer personas de acuerdo a sus rasgos característicos u objetos de acuerdo a sus formas geométrica especifica muy utilizado en sistemas de seguridad o bandas clasificadores de productos. (V. Artificial, 2012)

Identificación: se puede identificar objetos de acuerdo a un símbolo un color o cualquiera otra característica por ejemplo reconocer un producto de acuerdo a su código de barra.

Análisis de localización: es posible mediante visión artificial poder obtener la posición exacta de un objeto o una persona en un ambiente especifico. Por ejemplo, obtener la posición de un robot pez en un acuario controlado.

2.3 Reconocimiento Facial

Es una aplicación mediante la cual es posible reconocer una o varias personas basándose en las características únicas que se encuentran presentes en el rostro y comparándolo con una base de datos, para ello es necesario contar con una cámara para realizar la captura de la imagen del sitio donde se pretende realizar el reconocimiento, un procesador el cual ligado a un código programado en el mismo analizará la imagen digital captura.

2.3.1 *Detección de Rostros*

En un sistema de reconocimiento facial es importante como primer paso a realizar es la verificación de que en la escena captada por la cámara se encuentre presente el rostro de la persona, para ellos en la actualidad se cuenta con varios algoritmos capaces de realizar esta tarea, a continuación, se detallara dos de los más importantes.

2.3.1.1 *AdaBoost Algoritmo de Viola Jones*

Se basa en un método de aprendizaje automático mediante el cual es capaz de realizar el reconocimiento de un determinado objeto mediante el procesamiento de imágenes a gran velocidad y con promedios muy elevados en su detección. Usa AdaBoost como algoritmo de aprendizaje para ellos forma un clasificador fuerte combinando una gran cantidad de clasificadores débiles. Además, realiza tres contribuciones en este campo de la tecnología. (E. David, J. Peter,2015, pág. 11-12)

- Propone una nueva representación de una imagen, llamada imagen integral.
- Un algoritmo de aprendizaje.
- Un método para combinar e incrementar en cascada clasificadores más complejos.

El objetivo de utilizar la llamada imagen integral es conseguir realizar el procesamiento de una manera más rápida puesto que ya no se trabajará con valores de intensidad, sino que la imagen pasará a estar formada por sub imágenes construidas a través de operaciones básicas. Esto creara una matriz sobre la cual se realizarán los cálculos al recorrer las sub imágenes en diferentes escalas sobre la imagen original a esto se lo conoce como características Haar-Like. (C. Andres. 2017, pág. 25-27)

En la imagen 8-1 se representa las referencias que se pueden tomar para calcular cualquier suma rectangular.

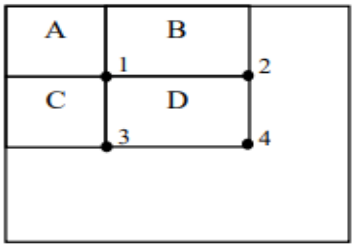


Figura 8-2: Suma rectangular

Fuente: C. Andres. 2017

Para obtener el valor de la suma rectangular en D se lo puede realizar de la siguiente manera, el valor de la imagen integral en el punto 1es la suma de los pixeles del rectángulo A, el valor en el punto 2 son los pixeles de A+B, en el punto 3 es A+C, y en el punto 4 es A+B+C+D. El resultado final puede darse como (4+1) - (2-3). (Aispuro, Paul, C. 2016)

Al aplicar las características Haar-Like en este proceso se logra realizar la detección de rostros en tiempo real y de una manera muy rápida y eficaz. Figura 9-1.

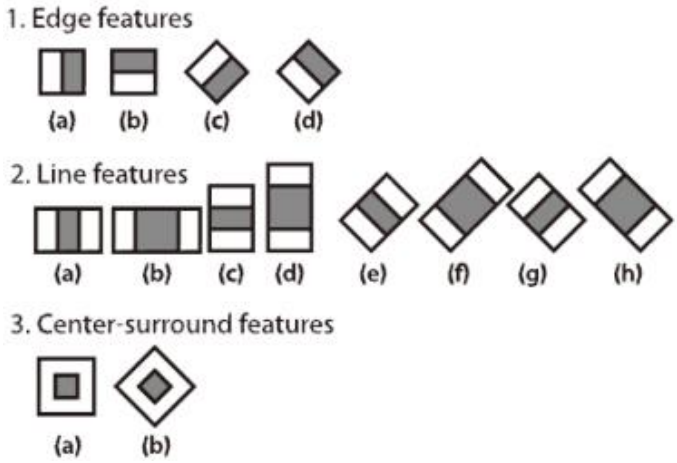


Figura 9-2: Características Haar-Like

Fuente: Z. Xin, G. Thomas, S, Jafar. 2017

Los clasificadores que se utilizan para la detección de un rostro deben ser entrenado con anterioridad basándose en la característica Haar-Like y aplicándolos en cascada sobre una región para poder verificar la presencia de un rostro una vez que cada uno de los clasificadores detecten su presencia, esto ayuda a desechar rápidamente las regiones de la imagen que no contengan un rostro en ella. (Z. Xin, G. Thomas, S, Jafar. 2017, pág. 101-102)

2.3.1.2 *Eigenfaces*

Este algoritmo se basa en un conjunto se rostros ya conocidos con los cuales se va a comparar la imagen de entrada para verificar la presencia de un rostro en el sitio de análisis. (S. Liliana, P. Luiggi, 2016. pág. 34)

El proceso de reconocimiento es el siguiente:

- Se define el conjunto de rostros que se los va utilizar para el entrenamiento de algoritmo y se calcula los eigenfaces de cada uno, esto definirá el espacio de rostros.
- Al encontrar un nuevo rostro se calcula los pesos basados en la imagen de entrada y los n eigenfaces comparando la imagen de entrada con los eigenfaces de los rostros de almacenamiento.
- Para determinar si la imagen de entrada es una cara se revisa si esta concuerda con el espacio de rostros.
- Si se determina que la imagen de entrada es una cara se realiza la comparación para saber si es persona conocida o desconocida.

- Si se detecta una misma cara desconocida varias veces se calcula el patrón de peso y se la incorpora al espacio de rostros.

La principal ventaja de este algoritmo es que es capaz de aprender a reconocer nuevas caras de manera autónoma.

2.3.2 *Métodos para reconocimiento facial*

Se clasifican en dos grupos: métodos holísticos son los que utilizan como entrada la imagen de todo el rostro y métodos basados en características locales los cuales toman como entrada las características principales del rostro como son ojos, nariz o boca tomando en cuenta la geometría, posición y apariencia. (V. Darío, 2012, pag.18)

2.3.2.1 *Métodos Holísticos*

Análisis de Componentes principales (PCA)

Este método se basa en un sub espacio de imágenes también conocido como eigenfaces descrito anteriormente, en donde una imagen de n x n pixeles es representada como una matriz de dimensiones NxN píxeles, donde cada píxel posee un valor de intensidad diferente que se obtiene al transformar la imagen del tipo RGB a escala de grises. Las imágenes están formadas por coordenadas: I(x,y).

La idea principal del método es encontrar los vectores que mejor representen la distribución de las imágenes, los cuales definen un sub-espacio correspondiente a las imágenes de rostros de seres humanos. Ese sub-espacio es llamado espacio de rostros. El proceso comienza con una imagen de rostro I(x,y) que se puede representar en dos dimensiones N x N (matriz de valores de intensidad de 8-bits). (V. Darío, 2012, pag.18)

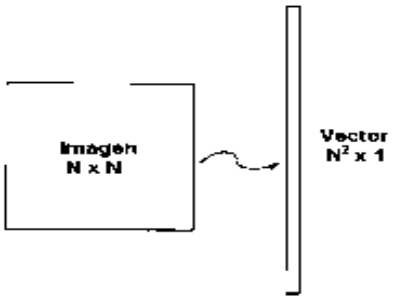


Figura 10-2: Imagen NxN transformada a vector N^2x1

Fuente: (V. Darío, 2012)

El objetivo del análisis de componentes principales es encontrar los vectores que mejor almacenen la distribución de las imágenes de rostros en el espacio completo de imágenes.

Análisis Lineal Discriminante (LDA)

LDA es conocida como una aproximación estadística que consiste en clasificar muestras de clases desconocidas basadas en ejemplos de entrenamiento con clases conocidas, esta técnica maximiza la varianza entre clases y minimizar la varianza entre cada clase. (Pereyra, p. 44).

En la figura 11-2 se puede observar que hay grandes variaciones entre clases y a la vez pequeñas en cada clase.

Figura 11-2: Ejemplo de seis clases usando LDA

Fuente: (D. Moreno, 2020)

Esta técnica consiste en discriminar de forma lineal las características de los rostros. Para lo cual obtiene las características con mayor información en las caras para su luego clasificarlas. Este proceso se hace mediante la extracción de características basadas en proyección, al encontrar el espacio subyacente que mejor discrimina entre las clases y posteriormente se clasifica. El objetivo es minimizar la separación dentro de una misma clase a la vez que se maximiza la separación entre clases diferentes. (D. Moreno, 2020, pág. 168)

Análisis de Componentes Independientes (ICA)

El algoritmo ICA toma en cuenta los estadísticos de orden superior con lo cual se obtiene una representación de los datos más independiente y, por tanto, potente. Halla un conjunto de bases de forma que minimiza las dependencias de órdenes superiores para conseguir que la información proyectada sobre dicha base sea estadísticamente independiente. (V. Miguel, 2014, pág. 5).

Máquinas de vectores de Soporte (SVM)

Las máquinas de vectores soporte (SVM) fueron introducidas por Vapnik (1990) y sus colaboradores Boser (1992), Cortes & Vapnik (1995). Originariamente las SVMs fueron pensadas para resolver problemas de clasificación binaria, actualmente se utilizan para resolver otros tipos de problemas como regresión, agrupamiento, multi clasificación. También han sido utilizadas con éxito en diversos campos, tales como visión artificial, reconocimiento de caracteres, categorización de texto e hipertexto, clasificación de proteínas, procesamiento de lenguaje natural, análisis de series temporales. (V. Miguel, 2014, pág. 5)

SVM permite determinar si un vector de entrada pertenece o no a un grupo definido disponiendo de dos posibles grupos y cada vector de entrada pertenece a un grupo, para lo cual busca un plano que separe los puntos pertenecientes a cada categoría. En la figura 10-1 se puede ver el plano de separación que es representado por una línea continua y los puntos más cercanos al plano de separación pertenecen a la línea discontinua y forman el llamado vector soporte. (Gonzáles, 2015, p. 12)

2.3.2.2 *Métodos basados en características locales*

Modelo de Apariencia Activa (AAM)

Se basa en la adaptación de un modelo estadístico creado durante una fase de entrenamiento a partir de una serie de puntos de referencia. Para cada imagen se crea una malla de puntos característicos y adopta la forma y apariencia del objeto de la región de interés, después para todas se realiza un análisis PCA para obtener las variaciones y poder obtener la malla modelo que luego se aplicara para la extracción como se puede ver la figura 11-1. (Zapatero, 2016, p. 9).

Figura 12-2: Método AAM

Fuente: (Zapatero, 2016, p. 9)

Modelado 3D

Esta técnica utiliza una malla en 3D para identificar los puntos clave hallando los puntos de máxima curvatura en los perfiles. Dichos puntos y su relación entre ellos son luego representados en un grafo.

Elastic Bunch Graph Matching (EBGM)

Este algoritmo usa grafos en estrella apoyado en la técnica de grafos en 2D, esto debido a que los rostros comparten una estructura topológica similar, cuyos nodos son puntos clave (ojos, narices,) y las aristas las distancias entre ellos. (D. Sara, 2017, pag.16).

La técnica de EBGM se desarrolla básicamente en dos etapas: la primera consiste en ajustar un grafo de puntos principales a la cara del individuo como se puede ver en la figura 12-1, utilizando para ello un modelo estadístico de dicho grafo; la segunda etapa extrae características locales en dichos puntos y halla la distancia entre el grafo obtenido y sus descriptores al grafo almacenado de la persona a identificar. Dependiendo de la distancia encontrada, se ratifica o no la identidad del individuo.

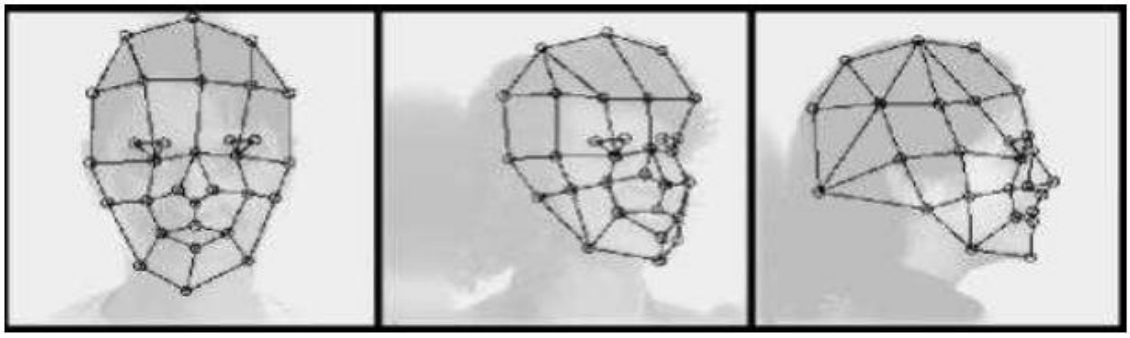


Figura 13-2: Método EBGM

Fuente: (Zapatero, 2016, p. 9)

Modelo Oculto de Markov (HMM)

Un HMM puede ser considerado como la red bayesiana más simple, están basados en la propiedad de Markov por el cual la distribución de probabilidad de un proceso del valor futuro de una variable únicamente depende de su valor presente, independientemente de los valores pasados de la misma. Se trata de un modelo en el cual el estado de cada nodo es desconocido, es decir, está oculto. (Zapatero, 2016, p. 17)

Patrones Binarios Locales (LBP)

Es utilizado para detectar todo tipo de objetos basados en texturas, invariante ante cambios de iluminación y capaz de detectar movimiento. Este sistema es capaz de extraer la estructura local de una imagen a partir del entorno de cada uno de los pixeles que lo conforman, el proceso consiste en ir comparando el valor de cada pixel con el de sus vecinos distribuidos en una circunferencia a su alrededor. (Zapatero, 2016, p. 6-7)

2.4 Seguridad Biométrica

Con el continuo avance de la tecnología, es posible contar con sistemas de vigilancia más fiables y eficientes, mediante los cuales se puede brindar una mejor seguridad a los recursos de una persona, sociedad o empresa.

Además, brinda herramientas de identificación más fiables. Es así, podemos encontrar sistemas de seguridad basados en contraseña, números de PIN, firmas digitales y los más actuales que utilizan las características únicas de partes del cuerpo de una humano como llaves de seguridad ya sea para acceder a un lugar físico, para fichar en el trabajo, para efectuar una transacción bancaria o para realizar una compra.

2.4.1 *Definición*

Definimos la biometría como la parte de la biología que estudia en forma cuantitativa la variabilidad individual de los seres vivos utilizando métodos estadísticos. Es una tecnología que realiza mediciones en forma electrónica, guarda y compara características únicas para la identificación de personas. (B. Cristian, 2020)

La forma de identificación consiste en la comparación de características físicas de cada persona con un patrón conocido y almacenado en una base de datos, de esta forma permitirá el control de acceso físico, incluso es aplicable como método de identificación y acceso a sistemas operativos y aplicaciones. Las características biométricas de una persona son intransferibles a otra, por lo que hace a estos sistemas muy seguros. (J. Costas, 2014, pág. 153)

Un sistema biométrico típico se compone de cinco componentes integrados: según NATIONAL SCIENCE AND TECHNOLOGY COUNCIL (NSTC) se utiliza un sensor para recopilar los datos y convertir la información a un formato digital, algoritmos de procesamiento de señales que

realizan actividades de control de calidad y el desarrollo de una plantilla biométrica, un componente de almacenamiento de datos que mantiene la información de las nuevas plantillas biométricas, que son comparadas con un algoritmo de coincidencia cuyo fin es comprar la nueva plantilla biométrica almacenada. Finalmente, se realiza un proceso de decisión (ya sea automatizado o manual) que utiliza los resultados correspondientes para tomar una decisión a nivel de sistema. (G. Andrea, G. Diana,2017, pág. 20)

En la figura 14-2 se presenta los diferentes tipos de biometrías que son utilizados por los sistemas de seguridad.

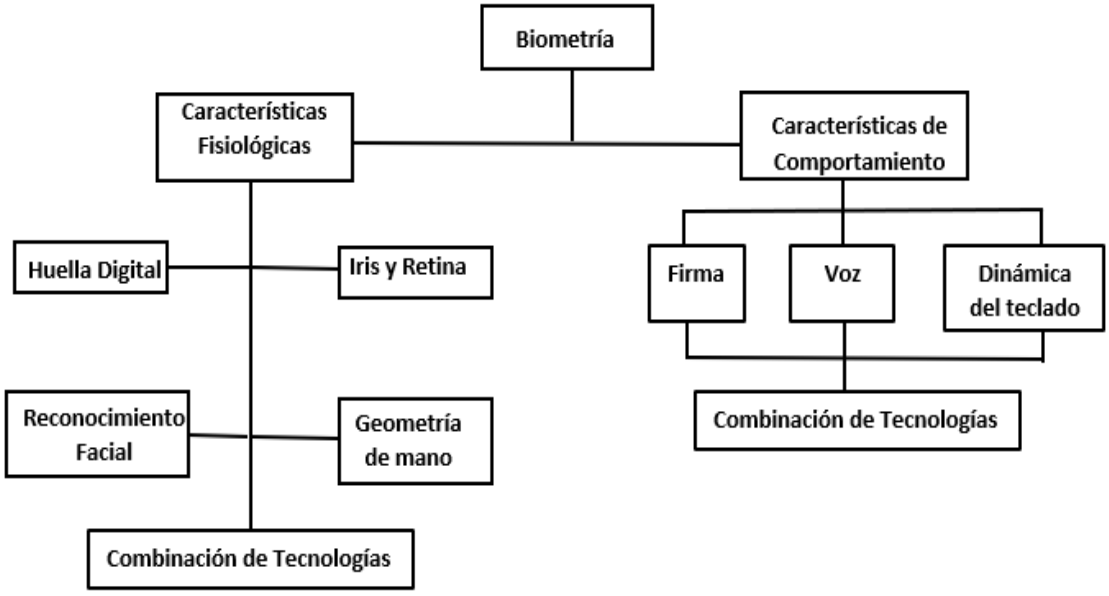


Figura 14-2: Tipos de Biometría

Fuente: A. Juan, B. Lucas, 2014

2.4.2 *Clasificación de los sistemas Biométricos*

2.4.2.1 *Reconocimiento huella digital*

Cada persona cuenta con una distribución diferente de líneas oscuras y claras, así como más de 30 pequeños relieves llamados minucias en cada uno de sus dedos, es por ello que el método de seguridad biométrica por huella digital está basado en la idea que dos personas no pueden tener más de 8 minucias iguales, en la década pasado este tipo de sistema fue considerado el más seguro, eficaz y fiable. (G. Andrea, G. Diana,2017, pág. 25)

Otra característica por el cual ha sido altamente utilizado es el beneficio calidad/precio pues a pesar de su alto nivel de seguridad los costos de los dispositivos utilizados son muy accesibles. En la figura 15-1 se observa las características propias de una huella dactilar.

Figura 15-2: Reconocimiento de huella

Fuente: G. Andrea, G. Diana,2017

Las técnicas basadas en minucias y la huella dactilar son las más estudiadas y cuenta con mayor número de algoritmos para su análisis. Todos los sensores de huellas dactilares tratan de generar una imagen digital de la superficie del dedo, esta imagen tiene normalmente una resolución de píxel de 500 dpi. La generación de imagen puede ser diferente para cada tipo de sensor. (G. Andrea, G. Diana,2017, pág. 25)

2.4.2.2 *Reconocimiento de Iris*

Es un método intrusivo mediante el cual se utiliza el iris del ojo como llave de seguridad, es el método más eficiente en la actualidad, la coincidencia entre iris de una persona a otra tiene una probabilidad de casi cero entre 200 millones, sim embargo sus principales desventajas están en la iluminación al momento de realiza la lectura, pues el tamaño del iris varía dependiendo de la cantidad de luz que exista en el ambiente.

El Autor Borja, indica que "cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag…). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar". (G. Andrea, G. Diana,2017, pág. 26)

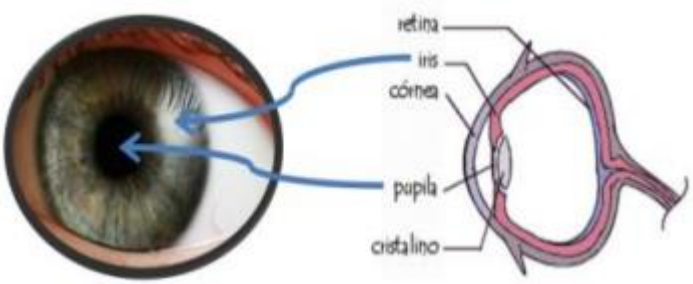


Figura 16-2: Características del iris humano

Fuente: Giraldo, Gomez,2017

2.4.2.3 *Reconocimiento facial*

Según National Science and Technology Counci describe: "El reconocimiento facial está basado en rasgos (geométrico) y lo visual (fotométrico), en el desarrollo de los avances del reconocimiento facial los investigadores desarrollaron algoritmos para obtener precisión según los más estudiados son: Análisis de componentes principales (Principal Components Analysis, PCA), Análisis lineal discriminante (Linear Discriminant Analysis, LDA), y Correspondencia entre agrupaciones de grafos elásticos Elastic Bunch Graph Matching, EBGM)". (G. Andrea, G. Diana,2017, pág. 28)

Esta tecnica se basa en las caracteriticas de las secciones principales de la cara como son los ojos, nariz, labios y cejas su forma geometrica, disposicion, longitud, etc. La ser un metodo no intrusivo es muy utilizado pues en la mayoria de las ocasiones el usuario no se entera que esta siendo identificado.

2.4.2.4 *Geometría de la mano*

Un lector es el dispositivo en el cual el usuario introduce su mano para identificarse, el dispositivo es capaz de captar imágenes de la parte superior, así como el lateral de la mano y obtener las características propias como son anchura, longitud, distancias entre puntos y líneas propias de la misma.

Este tipo de sistemas es considerado como el más rápido para la autentificación y su margen de error es en algunos casos aceptable, sin embargo, es posible que dos usuarios tengan características similares en sus manos por lo que la cantidad de falsas lecturas es elevada. (Gómez, 2014, pag.128)

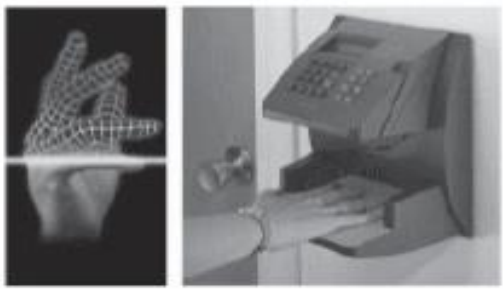


Figura 17-2: Biometría geometría de la mano

Fuente: Gómez, 2014

2.4.2.5 *Reconocimiento de Voz*

Se basa en el análisis espectral de las ondas sonoras que emite una persona, es decir, descompone la voz en las distintas componentes de frecuencia, pues esto depende de las características de los diferentes partes del cuerpo que intervienen en el habla. También se puede tener en cuenta otras características de la voz como son la velocidad o la inflexión al hablar. (Gómez, 2014, pag.124)

Existen dos procesos dentro del reconocimiento por voz en el primero el usuario debe repetir una frase almacenada dentro de la base de datos del dispositivo de reconocimiento, para ello cada usuario tiene una frase destinada exclusivamente para él, este procedimiento es altamente riesgoso puesto que está sujeto a que un tercero realice una grabación y la reproduzca ante el identificador. El segundo proceso tiene un mayor grado de seguridad pues el sistema genera un conjunto de palabras aleatorias las cuales el usuario debe repetir para ser identificado.

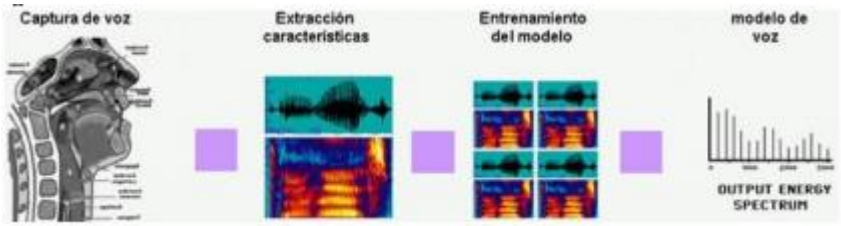


Figura 18-2: Reconocimiento de voz

Fuente: G. Andrea, G. Diana,2017

2.4.2.6 *Reconocimiento de firma*

Este sistema biométrico está tipificado como dinámico, el objetivo de este sistema es confirmar la identidad de una persona mediante el análisis de la firma manuscrita, aunque la firma sufre ligeras variaciones, la naturalidad del movimiento al firmar y el número de repeticiones hace que se pueda determinar y reconocer un patrón.

El reconocimiento de la firma, es apropiado para validar la emisión de mensajes, cheques, transacciones bancarias, el reconocimiento de huella dactilar es la que más implementaciones tiene, es un mecanismo de identificación más usado, pero es el más intrusivo, por lo cual genera más indisponibilidad a las personas, puesto que deberá contribuir para la captura de las huellas. (G. Andrea, G. Diana,2017, pág. 33)

2.5 Software

Actualmente se puede encontrar en el mercado varios paquetes de software mediante los mediante los cuales es posible realizar el procesamiento de imágenes. A continuación, se mencionará algunos de ellos.

2.5.1 *Matlab*

Es un paquete de software orientado al uso en la ingeniería y el campo científico, su precisión al momento de realizar cálculos complejos y su potente capacidad de procesamiento y la facilidad al momento del aprendizaje de su lenguaje de programación lo hace uno del software más utilizado en la actualidad al momento de trabajar con operaciones matemáticas, matrices entre otras. (MatWorks)

Figura 19-2: Logo software MATLAB

Fuente: Giraldo, Gomez,2017

El lenguaje MATLAB está basado en matrices que es la forma más natural del mundo para expresar computacionalmente. Los gráficos incorporados facilitan la visualización y el conocimiento de los datos. La basta biblioteca de cajas de herramientas preconstruidas le permite comenzar de inmediato con los algoritmos esenciales a su dominio. El entorno de escritorio invita a la experimentación, exploración y descubrimiento. Estas herramientas y capacidades de MATLAB están todas rigurosamente probadas y diseñadas para trabajar juntos. (MatWorks)

MATLAB es uno del software más utilizado en el procesamiento de imágenes pues cuenta con herramientas toolbox preconstruidas con las cuales el usuario puede realizar distintas operaciones sobre las imágenes.

2.5.2 *Python*

Es un interpretador de funciones que permite usar le lenguaje en forma interactiva. Los lenguajes interactivos interaccionan de mejor manera con el usuario a través de una ventana y también mediante programas que pueden desarrollarse y probarse a medida que son construidos. Esta interacción facilita el aprendizaje del lenguaje y mejora la productividad. A diferencia de los programas compilados los cuales deben ser terminados antes de ser probados. (Rodríguez, 2016, pág. 52)

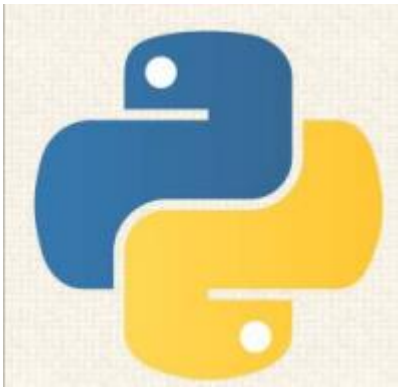


Figura 20-2: Logo software Python

Fuente: Rodríguez, 2016

Entre las principales características de este software se tiene:

- Es un lenguaje interpretado. Usa conceptos de otros lenguajes como Modula-3, Lisp, entre otros.
- Se puede instalar en plataformas Windows, Linux, entre otros. Con pocos cambios en su forma de instalación.
- Es software libre y de código abierto con licencia GLP (General Public License). Se puede instalar, modificar y distribuir proporcionando el código fuente. Las licencias GLP no ofrecen garantías sin embargo al ser código abierto una gran cantidad de usuarios lo utiliza y los errores son detectados rápidamente.

Con respecto al campo de procesamiento de imágenes, uno de los objetivos de la visión artificial abierta (OpenCV) es proporcionar una infraestructura accesible y sencilla. La biblioteca OpenCV

contiene funciones utilizadas en distintas áreas de la visión por computador, como es la inspección de productos, identificación de personas u objetos en movimiento, reconocimiento de rostros humanos en una imagen, imágenes médicas, seguridad, interfaces de usuario, reconstrucción 3D, robótica, etc (Viera, 2019, pág. 49)

2.5.3 *QT*

Qt es un framework creado por la compañía Trolltech para la creación de aplicaciones e interfaces multiplataforma. La función más conocida de Qt es la creación de interfaces de usuario, también realiza otras funciones como facilitar determinadas tareas de programación (manejo de sockets, soporte de programación multihilo, etc.), comunicar bases de datos, manejar cadenas de caracteres, y también para el desarrollo de programas sin interfaz gráfica.

Una característica muy importante y distintiva de Qt son las señales y slots, que sirven para la comunicación entre los objetos de una aplicación. Los widgets de Qt poseen señales y slots predeterminados, pero es posible desarrollar widgets personalizados con determinadas señales y slots. (Viera, 2019, pág. 50)

QT tiene dos componentes:

Qt Designer: es una herramienta para el diseño y desarrollo de interfaces gráficas de usuario (GUI). Con esta herramienta, el código de programación se integra fácilmente y se pueden modificar las propiedades de cualquier elemento. Presenta una paleta con botones, widgets, ítems, contenedores para la creación de la interfaz. Es importante mencionar que los widgets pueden agruparse utilizando señales y slots.

Qt Creator: es un entorno de desarrollo integrado (IDE) multiplataforma que utiliza el lenguaje C++ e integra otras dos herramientas: Qt Assistant y Qt Designer. Una de las mayores ventajas de este entorno es que permite que un conjunto de desarrolladores comparta un proyecto por medio de varias plataformas de desarrollo como son Microsoft Windows, Mac OS X, Linux, Symbian, MeeGo, (Viera, 2019, pág. 51)

CAPITULO III

3 MARCO METODOLOGICO

3.1 Propuesta Metodológica

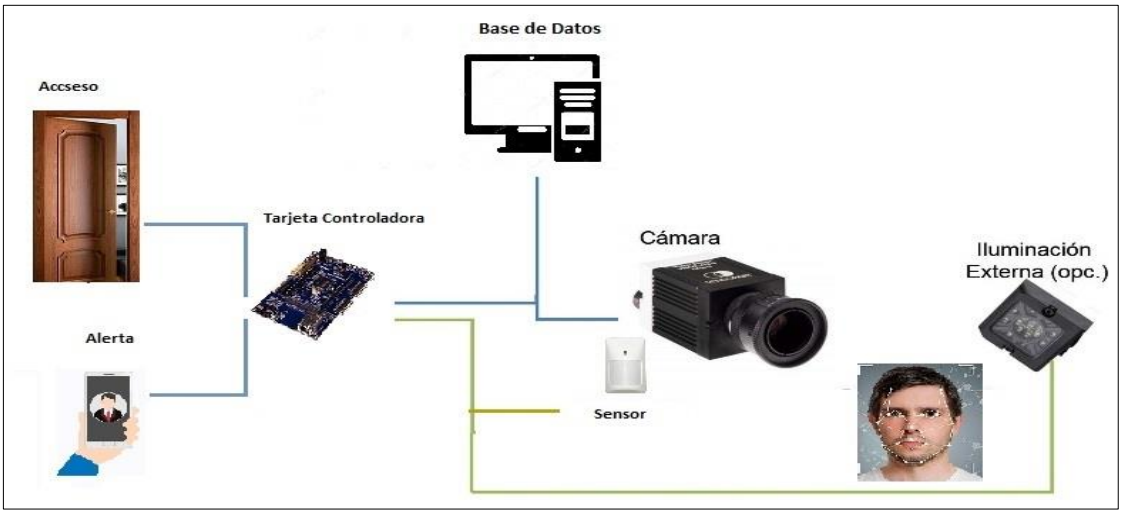


Figura 1-3: Funcionamiento del sistema

Realizado por: Pañi Cristian,2020x|x

En la figura 1-3 se presenta mediante un gráfico el proceso que llevó acabo el prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas. Se utilizó la metodología experimental pues a partir de la problemática se trabajó para el cumplimiento de los objetivos planteados. La recolección de información se la realizó utilizando el modo bibliográfico para ello se dividió el tema del trabajo de titulación en sub tema principales como son: domótica e inmótica, visión artificial y seguridad, utilizando fuentes de información como son libros, revistas, artículos científicos, tesis de pre y posgrado, etc.

3.2 Requerimientos de Hardware y Software del Sistema

Basado en el planteamiento del prototipo de sistema inmótico, y tras un previo análisis se obtuvo como requerimientos de software los siguientes: un sistema operativo ligero de manera que no ocupe mucho espacio en el almacenamiento y que sea compatible con la placa controladora que se utilizó. Un lenguaje de programación de programación potente además que brinde facilidades en el procesamiento imágenes y control de sensores. Para la creación de la app se necesitó un software mediante el cual se pueda desarrollar aplicaciones capaces de ejecutarse sobre cualquier

dispositivo móvil. Un sistema de gestión de base de datos para el almacenamiento de la información de cada usuario. Además, una plataforma web capaz de recibir imágenes desde el lenguaje de programación y enviar a la aplicación móvil.

Con respecto a hardware los requerimientos son los siguientes: una placa controladora con capacidad de procesar imágenes en tiempo real además de leer las señales emitidas por sensores y enviar comandos hacia los actuadores de manera que realicen una acción. Una cámara con la suficiente resolución para tomar una captura clara del rostro de una persona. Dos sensores, el primero capaz de detectar movimiento y enviar una señal con el objetivo de encender la cámara, el segundo un sensor que pueda conocer cuando una puerta está siendo vulnerada mediante golpes y dar a conocer la lectura al controlador. Una cerradura electromagnética encargada de asegurar la apertura o cierre de una puerta.

3.3 Descripción del Funcionamiento del Sistema

3.3.1 *Operación General del Sistema*

La figura 2-3 presenta por medio de un diagrama el funcionamiento general del trabajo de titulación, la fase de reconocimiento facial es controlado por medio del sensor de movimiento el cual emite la señal para el encendido de la cámara, la misma que es la encargada de recoger las imágenes que posteriormente son procesadas.

El sensor de impacto es el encargado de brindar un nivel más alto de seguridad, puesto que, al activarse en caso de una posible irrupción a la fuerza, emite un comando haciendo que la cámara tome una captura del actual frame y el mismo es enviado al usuario por medio de una aplicación móvil.

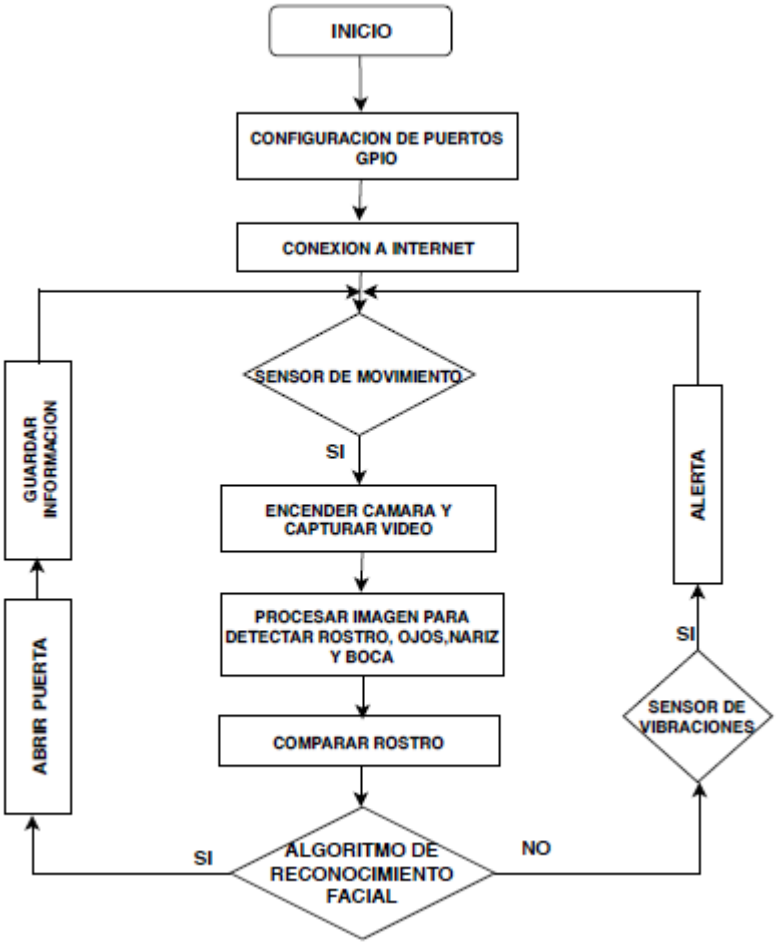


Figura 2-3: Diagrama General de funcionamiento

Realizado por: Pañi Cristian,2020

3.3.2 *Proceso de Captura de la Imagen*

Obtenida la captura de la imagen se realizó un procesamiento aplicando operaciones como conversión a escala de grises, normalización lo que me permitió resaltar los atributos de la imagen, para finalmente conocer si existió un rostro en la imagen y si esto es verdadero obtener los puntos característicos de las principales zonas de la cara. En la figura 3-3 se puede observar el diagrama de este proceso.

Figura 3-3: Proceso capturar imagen

Realizado por: Pañi Cristian,2020

3.3.3 *Proceso de Tratamiento de la Imagen*

Si se detectó un rostro en la imagen se aplica diferentes procesos para que se realice el guardado de la una imagen que contenga únicamente el recorte del rostro. En la figura 4-3 se muestra un diagrama que contiene el proceso descrito.

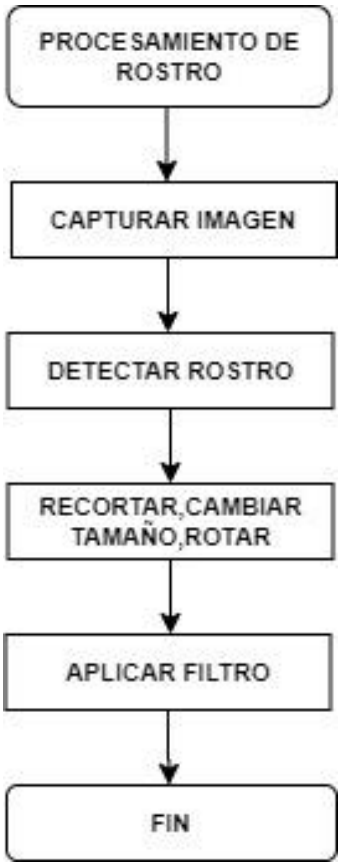


Figura 4-3: Obtención del rostro de la imagen

Realizado por: Pañi Cristian,2020

3.3.4 *Proceso de Identificación por Reconocimiento Facial*

La fase de reconocimiento se activa una vez que se ha confirmado que existió un rostro en la imagen, consistió en comparar el rostro detectado con la base de datos creada con las caras de las personas autorizadas, si el rostro detectado coincide con alguien de la base de datos se concede el acceso. En la figura 5-3 se puede observar el proceso de esta fase.

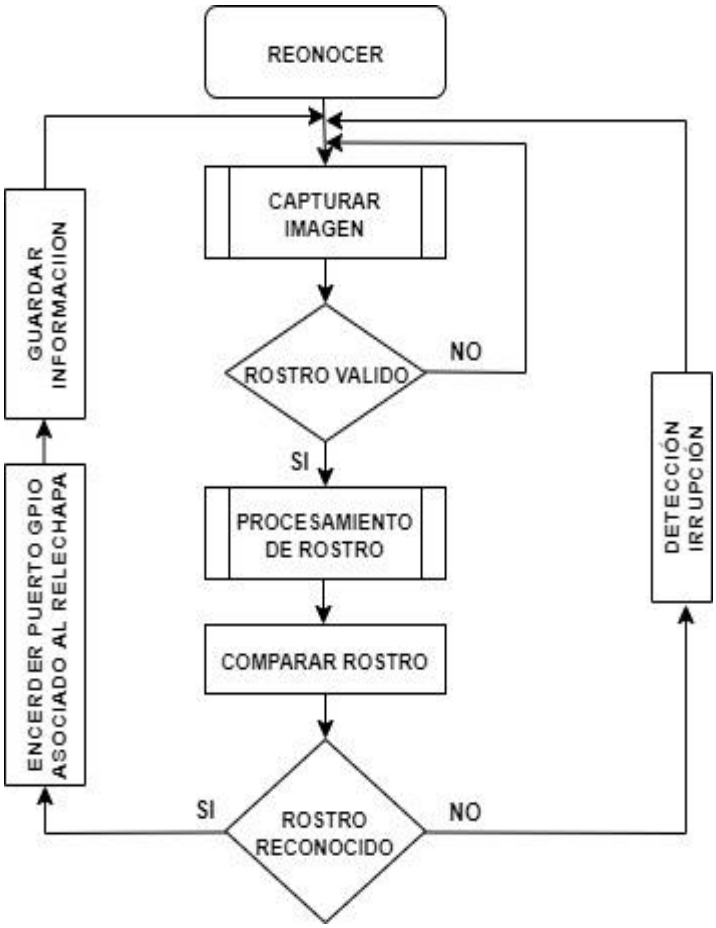


Figura 5-3: Fase de Reconocimiento

Realizado por: Pañi Cristian;2020

3.4 Elementos de Hardware del Prototipo

3.4.1 *Raspberry Pi*

Fue la encargada de realizar el procesamiento de los datos y variables que se manejan tanto en la parte de software y hardware del prototipo, es por ello que se procedió a investigar los diferentes modelos existentes en el mercado, dando como resultado la comparación presentada en la tabla 1-3.

Tabla 1-3: Comparación entre características de los modelos de Raspberry

CARACTERISTICAS	**MODELOS**			
	Raspberry Pi 1	**Raspberry Pi 2**	**Raspberry Pi 3**	**Raspberry Pi 3+**
Chip	BCM 2835	BCM2836	BCM2837	BCM2837 BO
Procesador	ARM1176JZF-S a 700MHz	ARM Cortex A7 a 900MHz quad-core	ARM Cortex A53 a 1.2GHz quad-core	ARM Cortex A53 a 1.4GHz quad -core

Procesador Grafico	Video Core IV 250MHz	Video Core IV 250MHz	Video Core IV 400MHz	Video Core IV 400MHz
Memoria RAM	256 MB SDRAM	1 GB SDRAM	1 GB SDRAM	1 GB SDRAM
Video	HDMI 1.4	HDMI 1.4	HDMI 1.4	HDMI 1.4
Puerto USB	1	4	4	4
Almacenamiento Integrado	SD	MicroSD	MicroSD	MicroSD
Red	Ninguna	10/100 Ethernal vía hub USB	WiFi 802.11n	WiFi 802.11n
Bluetooth	No	No	Bluetooth 4.1	Bluetooth 4.2

Fuente: Raspberry.org,2020

Realizado: Cristian Pañi,2020

Analizadas las características presentadas se optó por elegir el modelo raspberry Pi 3+ para el control del prototipo, esto debido a que presenta características más robustas. Las mismas que se muestra en la tabla 1-3.

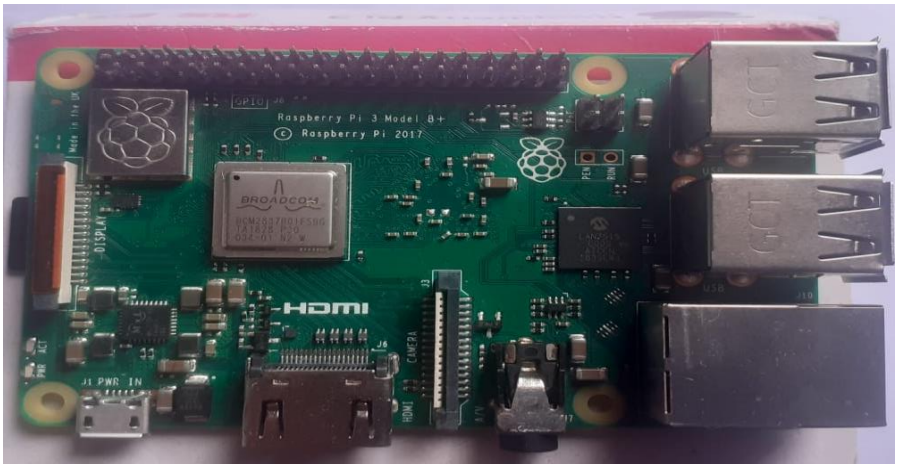


Figura 6-3: Rasberry Pi 3 b+

Realizado por: Pañi Cristian,2020

3.4.2 *Sensor de Movimiento CoMET RK210PR y Sensor de golpe RK600S*

Estos sensores fueron seleccionados debido a sus características, como son rango de lectura compatibilidad con la tarjeta controladora escogida, modo de envió de datos, precio, etc.

La raspberry pi 3+ no cuenta con entradas de señales analógicas por ello quizá la principal característica que se observó en estos dos sensores es que son de tipo digital de manera que los datos emitidos por los mismo pueden ser leídos de forma directa por la raspberry.

En lo que respecta al sensor movimiento presentado en la figura 7-3, fue configurado para que su área de detección no sea muy extensa con el fin de que la cámara utilizada para la toma de imágenes no permanezca activa todo el tiempo.

Figura 7-3: Sensor CoMET RK210PR

Realizado por: Pañi Cristian, 2020

El sensor de golpe RK600S presentado en la figura 8-3, fue el encargado de detectar posibles irrupciones por la fuerza en el área restringida que se resguarda, la activación de este sensor dio como resultado la captura de una imagen de la persona o personas que tratan de irrumpir, esta imagen puedo ser observada por el usuario mediante una aplicación Android que fue diseñada para dicho fin.

Figura 8-3: Sensor de golpe RK600S

Realizado por: Pañi Cristian, 2020

Es importante mencionar que los pines no cuentan con ninguna protección hacia la placa de la raspberry, esto significa que se debió tener mucho cuidado con los voltajes que se ingresaron por los mismo, su voltaje máximo permitido es de 3.3V DC, un voltaje mayor al mencionado puede provocar el daño de toda la tarjeta controladora.

3.4.3 *Cerradura Electromagnética ZKLM-2802*

La cerradura electromagnética ZKLM se instaló en la puerta de entrada del área que se está controlando, se optó por una cerradura de 600 libras con el fin de obtener un mayor grado de

seguridad. El voltaje de operación de este dispositivo es de 12 voltios por lo que se hizo necesario el uso del relé que controlara si la cerradura esta activa o no.

En la figura 9-3 se presenta la cerradura electromagnética ZKLM-2802.

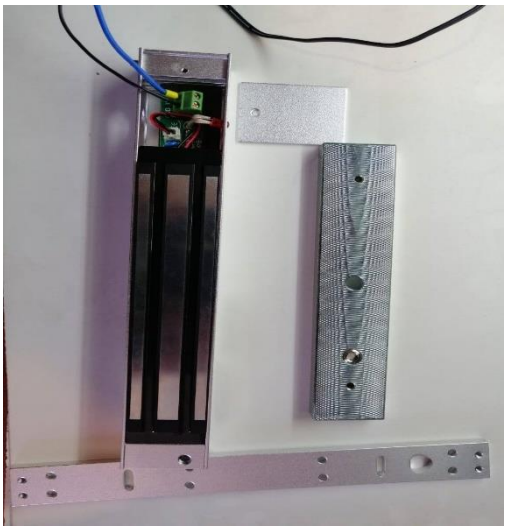


Figura 9-3: Cerradura electromagnética

Realizado por: Pañi Cristian,2020

3.4.4 *Elección de la cámara para el prototipo*

En la tabla 2-3 se presentan las características de tres modelos de cámaras que se las analizó para la elección de la cámara.

Tabla 2-3: Comparación entre modelos de cámaras

CAMARAS			
PRODUCTOS	**VENTAJAS**	**DESVENTAJAS**	**COSTO**
BRIO ULTRA HD PRO WEBCAM	Videoconferencias 4K Ultra HD (hasta 4096 x 2160 píxeles a 30 fps) Compatible con raspberry Campo visual: Diagonal: 90° Horizontal: 82,1° Vertical: 52,2°	Trabaja a resoluciones que no son compatibles con raspberry Es necesario redimensionar las imágenes que genera para utilizarlas.	Costo del dispositivo 300 dólares.
DRIVERLESS	Resolución compatible con raspberry. Compatible con raspberry.	Rango de enfoque 3cm Resolución 640x480. Cuenta con una resolución muy baja.	Costo del dispositivo 15 dólares.
	Desarrollada para uso en placa raspberry pi.	No se puede utilizar a una distancia mayor a 30 cm	

MODULO DE CAMARA RASPBERRY PI	Captura de vídeo a resoluciones de 1080p30, 720p60 y 640x480p90 Resolución de alta calidad	de la placa raspberry debido al tamaño de su bus de conexión	Costo del dispositivo 18 dólares.

Realizado: Cristian Pañi,2020

Basándose en la anterior tabla expuesta se tomó la decisión de usar el módulo de cámara de raspberry pi, debido principalmente a la compatibilidad con la placa raspberry y su bajo costo.

3.4.5 *Conexiones del prototipo*

En la Figura 10-3 se presenta los diferentes dispositivos los cuales conformaron el prototipo final, así como, las conexiones entre ellos y con la tarjeta controladora raspberry pi 3 b+.

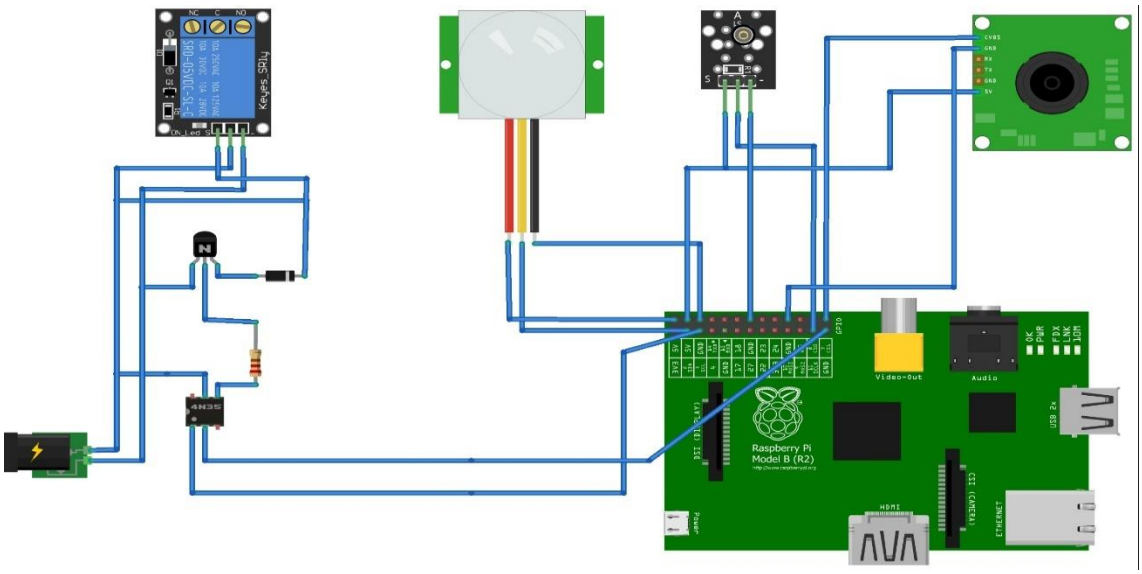


Figura 10-3: Conexión de los dispositivos del prototipo

Realizado por: Pañi Cristian,2020

El circuito consta de dos etapas la primera ubicada en la parte superior derecha de la figura 10-3, consta de la conexión de los sensores y cámara hacia la raspberry, como se conoció en la fase de investigación, estos dispositivos son compatibles con la tarjeta, sin embargo, las señales que emiten o reciben necesitan una etapa previa de acondicionamiento.

La segunda etapa del circuito está ubicada en la parte izquierda de la figura 10-3, tiene como objetivo realizar un acondicionamiento de la señal emitida desde la raspberry hasta la chapa eléctrica, la misma que fue encargada de conceder o no la entrada hacia el área restringida.

Para que la chapa eléctrica entre en funcionamiento necesitó una alimentación de 12V DC por este motivo fue necesario la construcción de un circuito de aislamiento del voltaje anterior hacia la placa controladora raspberry pi 3 b+ pues la misma es extremadamente sensible a voltajes superiores a los recomendados para su funcionamiento.

El circuito aislador antes mencionado consta de un optoacoplador(4n35), un transistor npn(2n222), un diodo rectificador(1n40000), y un par de resistencias, las conexiones se muestran en la figura 11-3 mediante una simulación en el software de diseño Proteus 8.7.

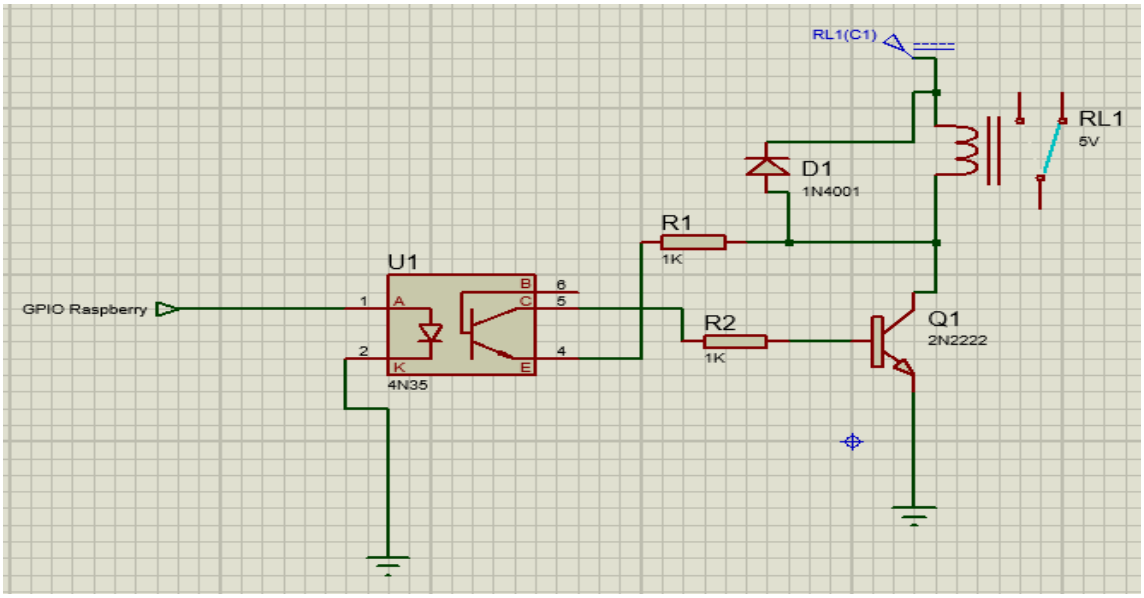


Figura 11-3: Circuito de protección

Realizado por: Paña Cristian,2020

Además de dar protección a la placa del controlador el circuito que se presenta en la figura 11-3, tuvo como objetivo proveer el suficiente voltaje y corriente para excitar el relé el cual fue el encargado de activar o desactivar la cerradura electromagnética.

Como se puede evidenciar en el datasheet de la raspberry el voltaje de operación de los pines de entrada/salida de propósito general (GPIO) es de 3.3v, además la raspberry no cuenta con una protección de los pines hacia la placa en general por lo que si se da un mal uso o se introduce un voltaje superior al antes mencionado puede ocasionar el daño de la placa controladora.

Otro proceso a realizar es el tratamiento de la señal que emite los sensores (detección de movimiento, y de lectura de golpe), esto fue necesario puesto que los mismos tienen alimentación de 12v DC. Para ello en el contacto común del sensor se ingresó 3.3V DC emitidos por la

raspberry y en el contacto abierto es donde se conecta el puerto GPIO que es el encargado de la lectura del estado.

Con este proceso se aseguró que la placa controladora no reciba un voltaje superior al que soporta, así como, una correcta lectura del estado del sensor pues actúa como un simple switch que solo tiene dos estados posibles 0 o 1.

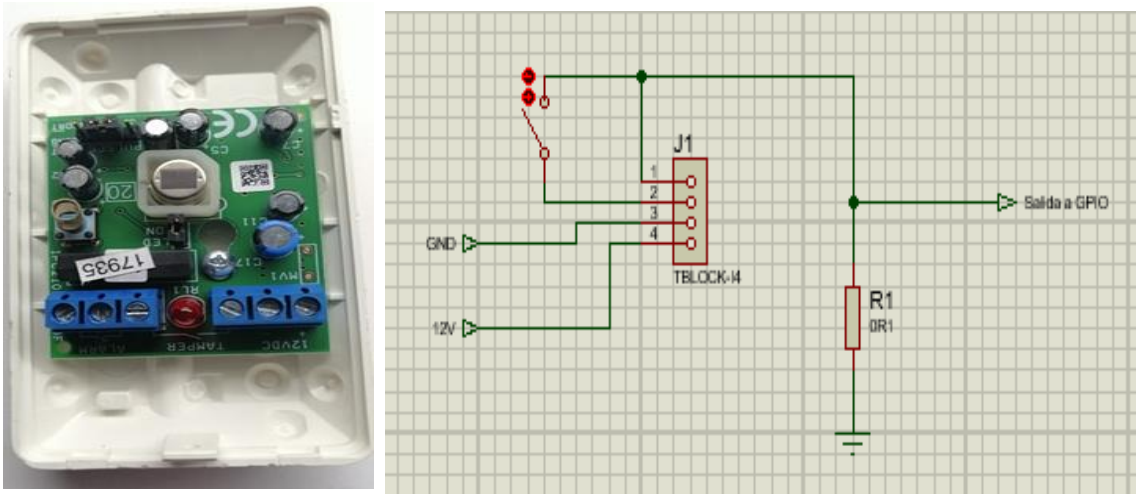


Figura 12-3: Proceso de tratamiento de la señal emitida por el sensor

Realizado por: Pañi Cristian,2020

3.5 Elementos de Software del Prototipo

3.5.1 *Análisis comparativo entre el algoritmo utilizado para reconocimiento facial con los existentes*

En la tabla 3-3 se presentan las principales ventajas y desventajas de los algoritmos que se investigaron antes del desarrollo del presente trabajo. La investigación se centró en cuatro de los principales algoritmos utilizados para conseguir el reconocimiento facial de una persona mediante visión artificial.

Tabla 3-3: Ventajas y desventajas en los algoritmos de reconocimiento facial.

ALGORITMOS PARA RECONOCIMIENTO FACIAL			
ALGORITMOS	**VENTAJAS**	**DESVENTAJAS**	**OBSERVACIONES**
EIGENFACE	Diseñado para la detección de rostros. Utiliza dos procesos para una mejor eficiencia: Extrae toda la información relevante del rostro Representa imágenes faciales de manera eficiente. Requiere un bajo consto en procesamiento	No recomendado para un análisis de imágenes en tiempo real. Además, la expresión facial al momento del reconocimiento debe ser la misma que en las imágenes usadas para conjunto de muestra.	El algoritmo necesita de un entrenamiento para realizar la identificación. Mientras mayor sea el número de imágenes para el entrenamiento mejor será su porcentaje en reconocimiento.
REDES NEURONALES CONVOLUCIONALES	El tiempo necesario para el reconocimiento es corto. El nivel de eficiencia en reconocimiento es elevado	El costo en procesamiento al momento de realizar el entrenamiento es excesivamente alto. Requiriere un volumen de pruebas sobre los datos	El algoritmo necesita de un entrenamiento para realizar la identificación.
YOLO	El porcentaje en acierto en reconocimiento es muy elevado. Se puede tomar como partida un fichero de pesos ya creado.	Al ser un tipo de red neuronal convolucional presenta las mismas desventajas que el anterior	El algoritmo necesita de un entrenamiento para realizar la identificación.
LBPH	Requiere un bajo costo de procesamiento. Presenta gran robustez respecto al cambio de expresiones faciales y orientación del rostro.	Sensible a cambios de iluminación. Requiere aplicación de filtros para mejorar las características de la imagen antes de realizar el entrenamiento.	El algoritmo necesita de un entrenamiento para realizar la identificación. Mientras mayor sea el número de imágenes para el entrenamiento mejor será su porcentaje en reconocimiento.

Realizado por: Pañi Cristian,2020

Al realizar la comparación entre ventajas y desventajas de los algoritmos investigados se optó por el uso del algoritmo basado en LBPH, tomando como principales referencias el bajo costo en

procesamiento computacional, así como que, al momento de realizar el proceso de reconocimiento de la persona ubicada frente a la cámara, tanto sus expresiones facial y orientación del rostro no influyen en gran medida como pasa en el algoritmo basado en Eigenfaces.

En relación al costo en procesamiento el prototipo diseñado tiene la capacidad de ingresar nuevos usuarios al sistema, por este motivo el uso de redes neuronales convolucionales o YOLO, no es recomendable debido a que para su entrenamiento es necesario contar con un dispositivo con potentes procesadores.

3.5.2 *Desarrollo sobre Python*

La programación de las diferentes acciones del prototipo se realizó en Python, para ello como primer paso fue necesario instalar todas las librerías necesarias, entre las más importantes se tiene la librería para manejo de imágenes, cámara y parámetros propios para reconocimiento de caracteres llamada Opencv, así como, la librería necesaria para la construcción de la GUI llamada TKinter, entre otras. Las librerías necesarias se muestran en la figura 13-3.

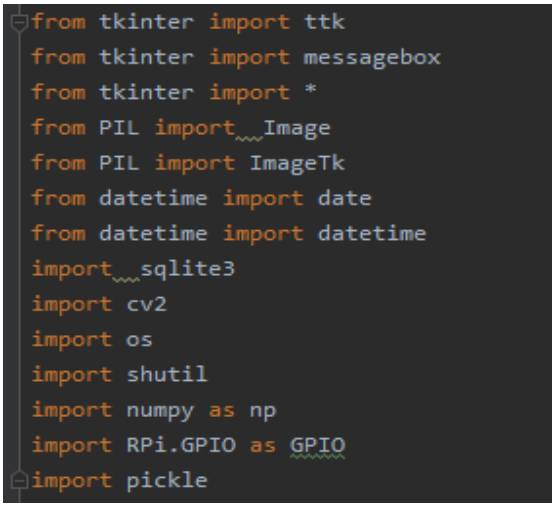


Figura 13-3: Librerías necesarias en Python

Realizado por: Pañi Cristian,2020

Para un mejor manejo y comprensión el código se hizo uso de funciones dentro de las cuales está programado cada acción necesaria. En la figura 14-3 se puede observar el procedimiento.

```
#FUNCION CONSTRUCCION DE VENTANA DE INICIO
def ventanaini(self):...

#FUNCION PARA ABRIR CAMARA
def leccamara(self):...

 #FUNCION VALIDACION DE CONTRASEÑA
def valcontra(self):...

#FUNCION CONSTRUCCION DE VENTANA USUARIO
def ventanausu(self):...

#FUNCION CREAR CARPETA ALMACENAR IMAGENES
def crear(self):...

#FUNCION TOMAR FOTOS PARA INGRESO NUEVOS USUARIOS
def tomarfot(self):...

#FUNCION ENTRENAMIENTO DE LA RED
def entrenamiento(self):...

#FUNCION RECONOCIMIENTO DE USUARIOS
def reconocimiento(self,cam):...

#FUNCION LECTURA CAMARA VENTANA USUARIOS
def leccamarausu(self):...
```

Figura 14-3: Esquema de la programación usada

Realizado por: Pañi Cristian,2020

El procedimiento de programación es el siguiente:

Se creó una GUI, la cual fue diseñada para una mejor interacción entre el usuario y el prototipo, la misma consta de dos ventanas, en la primera se realiza la lectura de la cámara utilizada para el reconocimiento de la persona que desea ingresar al ambiente controlado por el prototipo, así como, una tabla en la cual se registran la información del usuario al que se dio permiso para el ingreso. También se puede encontrar la opción para el ingreso hacia la segunda ventana, en la misma que se debe ingresar una contraseña que solo el administrador del sistema conoce. En la figura 15-3 se presenta esta ventana.

Figura 15-3: Ventana Reconocimiento

Realizado por: Pañi Cristian,2020

La segunda ventana está orientada al ingreso, actualización, y eliminación a usuarios, así como, el botón de entrenar el cual está orientado a realizar el entrenamiento de la red, esta acción se la debe realizar luego de haber ingresado o eliminado a un usuario. Al pulsar sobre el botón de

agregar se activan los campos en donde se debe ingresar los datos del nuevo usuario que se quiere ingresar en la base de datos, los mismo que son: nombre, cedula, edad y cargo; además realiza la captura de fotos necesarias para el entrenamiento del algoritmo lo que hace posible que el nuevo usuario pueda ser reconocido. En la figura 16-3 se puede apreciar esta ventana.

Figura 16-3: Ventana Usuarios

Realizado por: Pañi Cristian,2020

3.5.3 *Desarrollo sobre SQLITE*

La base de datos fue diseñada con dos tablas: USUARIOS y CONSULTA. Para la creación de la misma se utilizó una variante del conocido motor de base de datos de Lenguaje de Consulta Estructurado (SQL) basado en lenguaje C conocido como SQLite

La primera es donde se almacena los datos: nombre, cedula, edad y cargo de los diferentes usuarios que conforman el local, negocio, empresa, etc. Para evitar el ingreso de datos incoherentes en cada uno de los campos al momento de crear la tabla se define el tipo de variable la cual puede ser entera o cadena.

En la figura 17-3 se presenta el código que se utilizó en Python para crear la base de datos, así como las tablas que contiene, en la figura 18-3 se muestra la estructura de la base de datos con la ayuda del software DB Browser.

```
conexion= sqlite3.connect("TESIS_BASE")
curso=conexion.cursor()
curso.execute("CREATE TABLE USUARIOS (NOMBRE VARCHAR(50), CEDULA INTEGER(10), EDAD INTEGER(3), CARGO VARCHAR(30))")
curso.execute("CREATE TABLE CONSULTA (NOMBRE VARCHAR(50), CEDULA INTEGER(10), EDAD INTEGER(3), CARGO VARCHAR(30), FECHA STRING(25))")
conexion.close()
```

Figura 17-3: Código usado para crear la base de datos

Realizado por: Pañi Cristian,2020

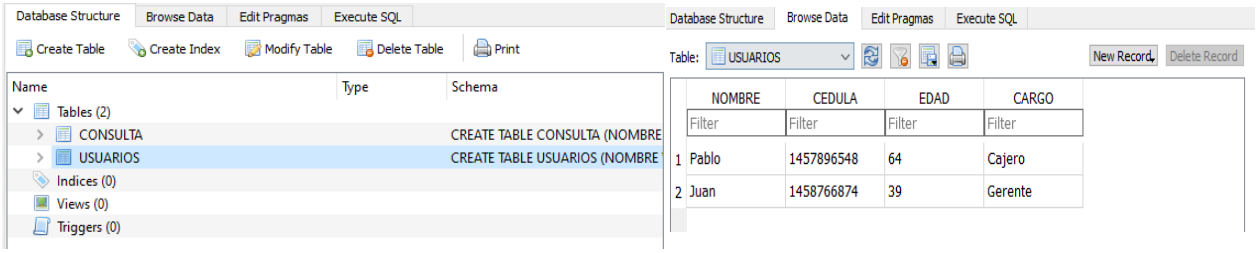


Figura 18-3: Estructura de la base de datos

Realizado por: Pañi Cristian,2020

3.5.4 *Desarrollo sobre Firebase*

Se lo configuró para la recepción de una imagen enviada desde la placa raspberry con la ayuda de Python y trasmitir la misma hacia la app de Android. Dicha imagen es la captura producida cuando el sensor de golpe se activa. Esta aplicación funciona como alerta sobre posibles irrupciones.

El primer paso es la configuración de firebase, para ello en un navegador web se ingresa al siguiente link https://firebase.google.com/?hl=es, en la parte superior derecha se encuentra la opción ir a consola, al ingresar a la misma se tiene la opción de crear un nuevo proyecto, al escoger esta opción se puede encontrar el código que se utiliza para hacer la conexión con python, esto se observa encontrar en la figura 19-3.

Se procedió a copiar este código al script principal de python encargado de realizar todas las acciones que conforman el prototipo de sistema inmótico basado en reconocimiento facial usando visión artificial, para controlar el acceso en áreas restringidas.

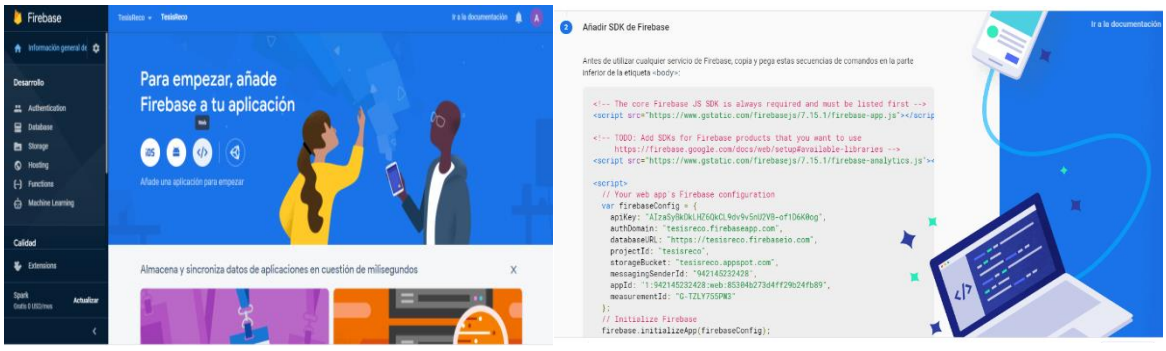


Figura 19-3: Plataforma Firebase (Izquierda), Código de conexión (Derecha)

Realizado por: Pañi Cristian,2020

La programación en python firebase junto con el manejo del sensor asociado al mismo para la captura de imagen descrita anteriormente se presenta en la figura 20-3.

```
config = {
    "apiKey": "AIzaSyB8oksc-g_n8dZLhqDvcR-7IYFR3FMr2Ak",
    "authDomain": "pruebaimg-bc4ae.firebaseapp.com",
    "databaseURL": "https://pruebaimg-bc4ae.firebaseio.com",
    "projectId": "pruebaimg-bc4ae",
    "storageBucket": "pruebaimg-bc4ae.appspot.com",
    "messagingSenderId": "940926118216",
    "appId": "1:940926118216:web:c1219215c128c25b40ab7d",
    "measurementId": "G-RRK9ZSEGYV"
}
golp= 24
GPIO.setup(golp, GPIO.IN)
lecgolp=GPIO.input(golp)
time.sleep(1)
if lecgolp:
    img_name = "sospechoso"
    cv2.imwrite(os.path.join("Peligro",  img_name + ".jpg"), marco)
    firebase=pyrebase.initialize_app(config)
    dir_fire="Peligro/foto.jpg"
    dir_local="sospechoso.jpg"
    alamace.child(dir_fire).put(dir_local)
```

Figura 20-3: Código Python manejo de firebase

Realizado por: Pañi Cristian,2020

3.5.5 *Desarrollo sobre Android Studio*

Para la creación de la app se utilizó Android Studio, el cual es uno de los principales softwares para la creación de aplicaciones móviles tanto para uso académico como para la comercialización, es importante importar un modelo de un dispositivo móvil antes de empezar a programar, esto ayudara a realizar un mejor diseño de la estructura de la aplicación.

A continuación, se procedió a realizar el diseño y programación de la app. Como primer paso como se mencionó se diseñó la estructura de la aplicación, este proceso es muy similar a cualquier programación orientada a objetos, lo cual da una vista previa a cómo será la versión final. En la figura 21-3 se presenta una parte del código utilizado.

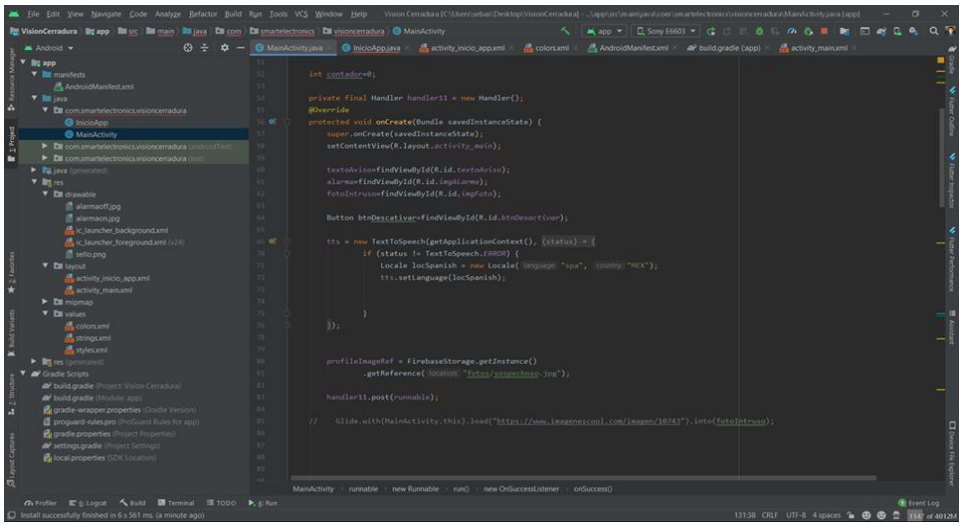


Figura 21-3: Código Android Studio

Realizado por: Pañi Cristian,2020

Para la conexión de Android Studio y Firebase se necesitan dos parámetros, el primero es la dirección URL del proyecto creado en la plataforma Firebase y el segundo es la contraseña del mismo, todos estos datos se obtienen en el proceso de creación del proyecto en la plataforma web mostrado en la figura 19-3.

En las figuras 22-2 y 23-2 se presenta la aplicación móvil finalizada que forma parte del sistema.

Figura 22-3: Pantalla de bienvenida.

Realizado por: Pañi Cristian,2020

Figura 23-3: Pantalla de lectura de la imagen

Realizado por: Pañi Cristian,2020

3.6 Funcionamiento del Sistema Desarrollado

3.6.1 *Ventana de Reconocimiento*

Al ejecutar el sistema se despliega la primera ventana en la cual se realiza el reconocimiento de la persona que está frente a la cámara, si el individuo está en la lista de aprobados, se le permite el ingreso y se guarda en la tabla consulta de la base de datos la información detallada correspondiente a ese usuario, la cual que consta de nombre, cedula, edad, cargo, además de la fecha y hora de ingreso. En la figura 24-3 se presenta esta ventana.

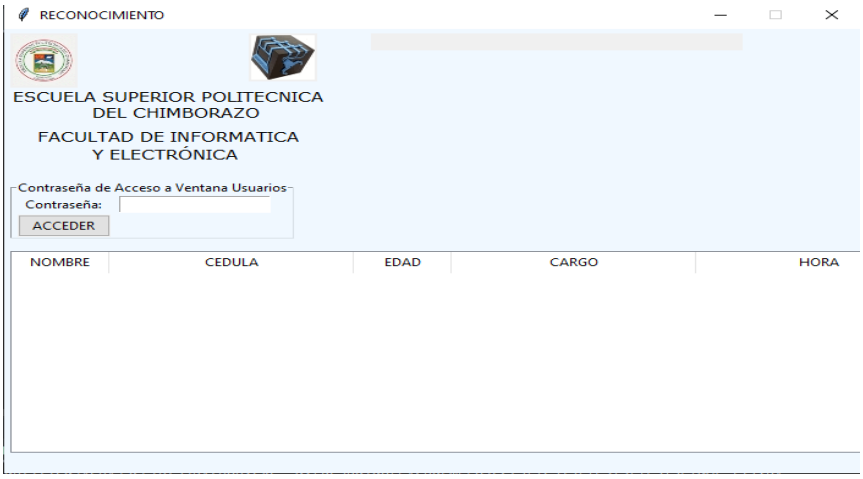


Figura 24-3: Ventana de reconocimiento

Realizado por: Pañi Cristian,2020

El interfaz de la cámara se activa una vez que el sensor de movimiento detecto una persona, como se ve en la imagen esta ventana además contiene un cuadro de texto donde el encargado de controlar el sistema puede acceder a la ventana usuarios. En el registro que se encuentra en la parte inferior de la ventana se visualiza la información de las personas las cuales se le permitió ingresar al lugar. En la figura 25-3 se observa la ventana con la interfaz de cámara encendida.

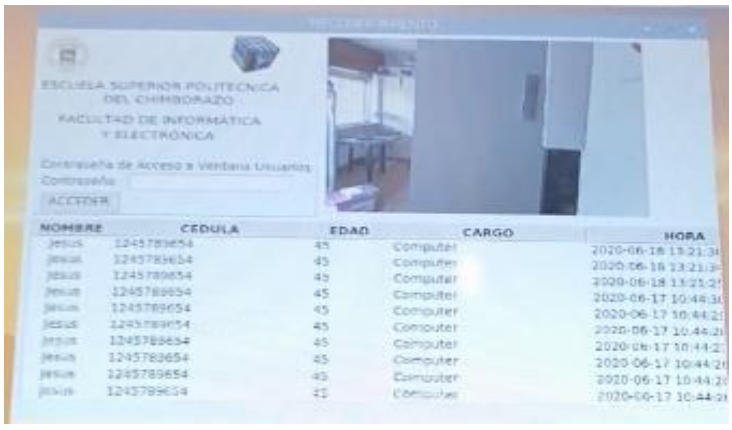


Figura 25-3: Ventana de reconocimiento cámara activada

Realizado por: Pañi Cristian,2020

El almacenamiento de la información a la base de datos de las personas que ingresan se las realiza solo cuando se les da el permiso de acceso, este permiso está programado según el cargo o puesto que ocupe el empleado o usuario. En la figura 26-3 se presenta la parte del código que realiza esta acción.

```
if ecar == 'Gerente' or ecar == 'gerente':
    print("Acceso a Todo")
    consulta = 'INSERT INTO CONSULTA VALUES(?,?,?,?,?)'
    parametros = (enom, eced, eedad, ecar, hora)
    self.runbasecons(consulta, parametros)
    self.consultcons()

if ecar == 'Tecnico' or ecar == 'tecnico':
    print("Acceso Area de Trabajo")
    consulta = 'INSERT INTO CONSULTA VALUES(?,?,?,?,?)'
    parametros = (enom, eced, eedad, ecar, hora)
    self.runbasecons(consulta, parametros)
    self.consultcons()

if ecar == 'Cajero' or ecar == 'cajero':
    print("Acceso Caja")
    consulta = 'INSERT INTO CONSULTA VALUES(?,?,?,?,?)'
    parametros = (enom, eced, eedad, ecar, hora)
    self.runbasecons(consulta, parametros)
    self.consultcons()
```

Figura 26-3: Código permisos de acceso

Realizado por: Pañi Cristian,2020

Una vez ingresado la contraseña de acceso a la ventana usuarios se obtiene la siguiente imagen figura 27-3.

3.6.2 *Ventana de Usuarios y agregar usuarios*

Figura 27-3: Ventana Usuarios

Realizado por: Pañi Cristian,2020

En esta ventana se puede realizar las diferentes acciones con la base de datos como es el ingreso de nuevos usuarios, actualización de datos o incluso eliminar un usuario. En las figuras 28-3, 29-3, 30-3,31-3 se puede observar el proceso de agregar un nuevo usuario.

Figura 28-3: Ingreso de información del usuario

Realizado por: Pañi Cristian,2020

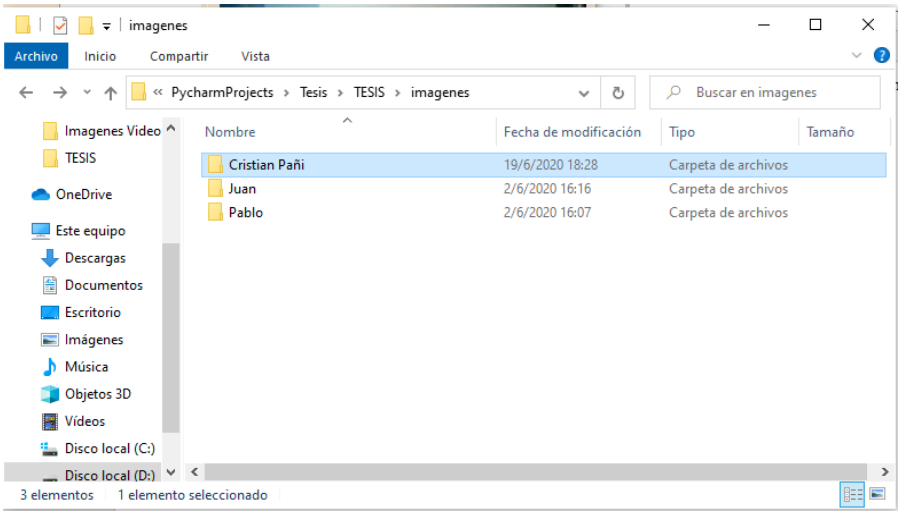


Figura 29-3: Crear carpeta

Realizado por: Pañi Cristian,2020

Al presionar en el botón de agregar que se encuentra en la ventana usuarios, se ejecuta el comando para crear una carpeta, dentro de la cual se alojaran las capturas del rostro de la persona la cual es ingresada al sistema. Una vez terminado el proceso de captura y almacenamiento de imágenes se observa un aviso de usuario agregado.

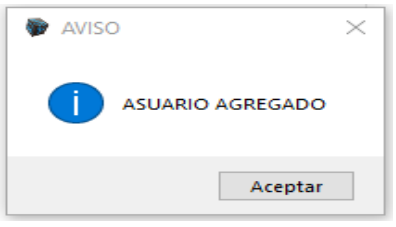


Figura 30-3: Aviso

Realizado por: Pañi Cristian,2020

El número de imágenes del rostro que se capturan es de mil imágenes, para una mejor detección y reconocimiento al momento de realizan la captura se aplican filtros y se realiza un cálculo para obtener las coordenadas del parte de la imagen que contiene el rostro y de esta forma se almacena solo el recorte del rostro para realizar el entrenamiento.

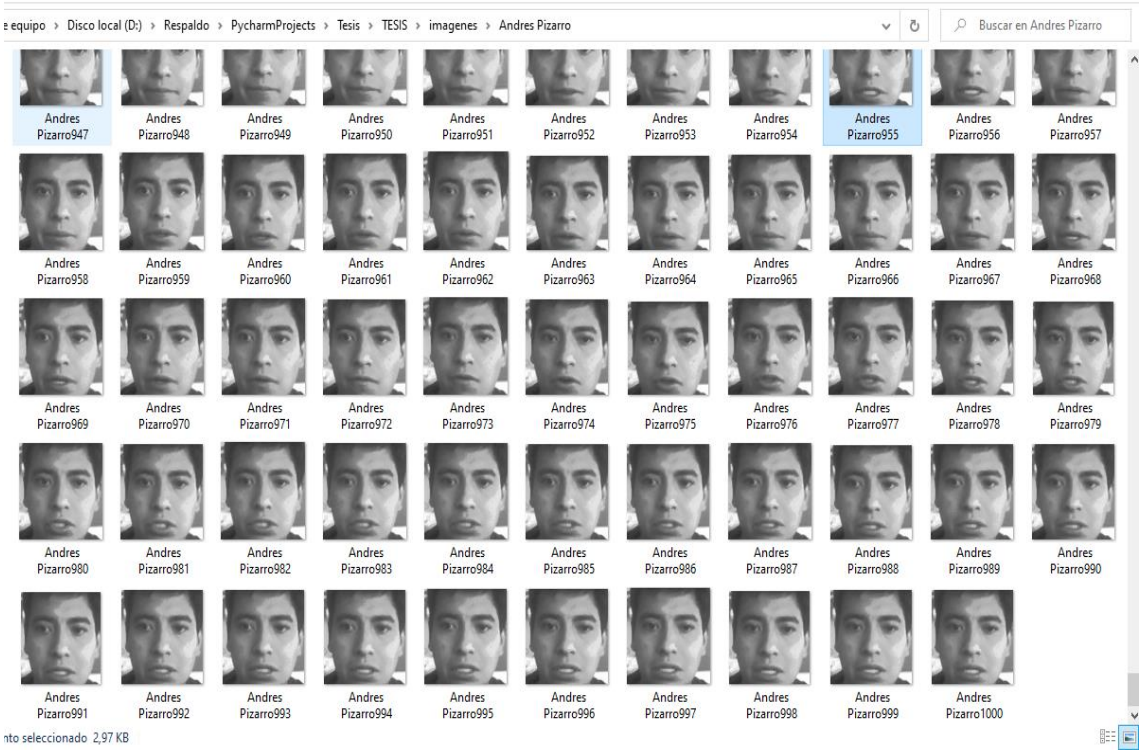


Figura 31-3: Capturas del rostro tomadas

Realizado por: Pañi Cristian,2020

3.6.3 *Proceso de entrenamiento*

Cada vez que se agregue o elimine un usuario es necesario realizar el entrenamiento del algoritmo encargado del reconocimiento, esto se lo realiza para que el nuevo usuario pueda ser reconocido o a su vez el usuario que se ha eliminado ya no sea reconocido, para ello se pulsa sobre el botón entrenar en la ventana de usuarios del sistema. En las figuras 32-3 y 33-3 se observa en proceso de entrenamiento.

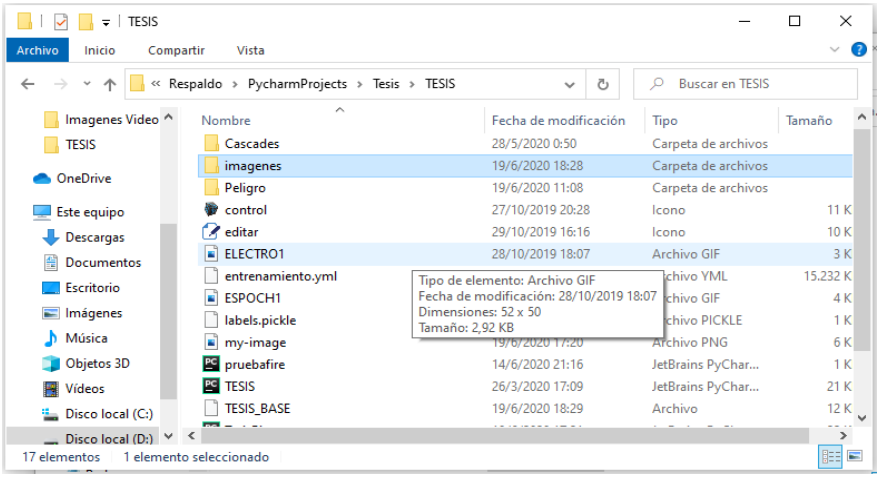


Figura 32-3: Archivos generados

Realizado por: Pañi Cristian,2020

Al terminar el proceso de entrenamiento se genera dos archivos el primero llamado entrenamiento.yml el cual contiene información sobre los rasgos únicos y personales de cada usuario y otro archivo llamado labels.pickle dentro del cual esta las etiquetas o nombres que se enlazaran con la imagen de cada usuario.

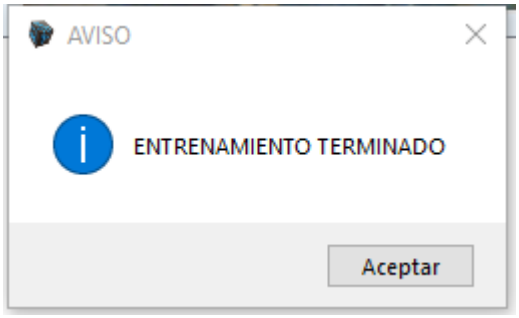


Figura 33-3: Archivos generados

Realizado por: Pañi Cristian,2020

Como al agregar un usuario, una vez termino el proceso de entrenamiento se lanza un aviso de entrenamiento terminado como notificación para el usuario.

3.6.4 *Envío de Imagen a Aplicación Móvil*

El sensor de golpe fue configurado para activarse cuando la puerta recibe un impacto en su superficie, una vez activado envía un comando para que el sistema realice una captura mediante la cámara en tiempo real. La imagen tomada es enviada a la plataforma web firebase. Esto se muestra en la figura 34-3.

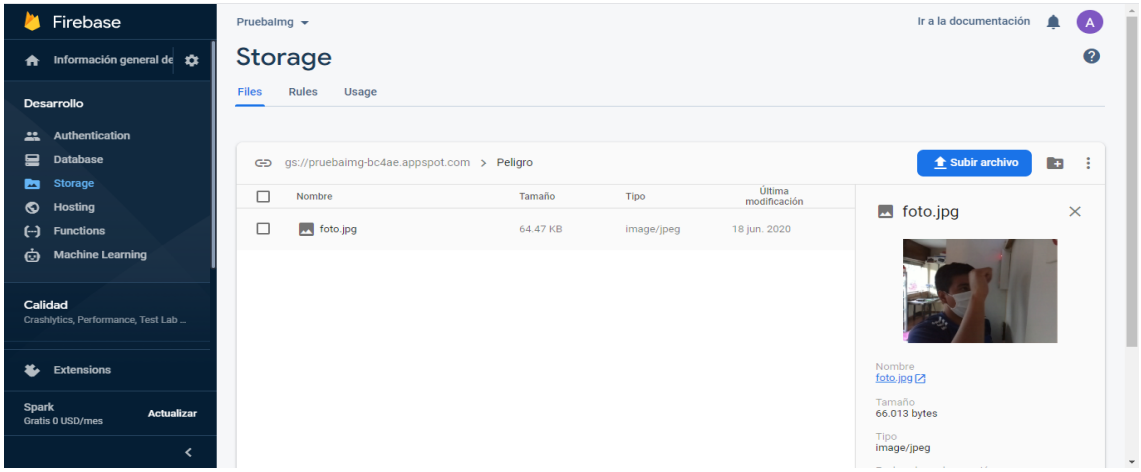


Figura 34-3: Imagen en Firebase

Realizado por: Pañi Cristian,2020

Una vez almacena la imagen en firebase, la aplicación móvil está programada para leer la misma y mostrarla acompañada de una alerta por voz. Se puede observar en las figuras 22-3 y 23-3.

CAPITULO IV

4 RESULTADOS, ANALISIS Y DISCUSIÓN

4.1 Pruebas de detección y reconocimiento en diferentes condiciones de iluminación

El cambio de iluminación es uno de los principales inconvenientes en los sistemas basados en reconocimiento, por ese motivo se realizó una investigación sobre los diferentes métodos que se pueden utilizar para evitar que este factor influya lo menos posible.

Como uno de los métodos encontrados es la aplicación de filtros en la imagen, se realizó este proceso antes de realizar la captura del rostro para el entrenamiento, así como, antes del proceso de reconocimiento. Una vez aplicados los filtros se realizó las siguientes pruebas.

El ambiente en el que se instaló el sistema está expuesto directamente al cambio de iluminación del trascurso del día, por este motivo se tomó como medias de referencia: soleado (alta iluminación, parcialmente nublado (iluminación media), nublado (baja iluminación).

Tabla 1-4: Pruebas de detección y reconocimiento bajo cambio de iluminación

Referencia	Numero de Pruebas	Detección	Reconocimiento	Error
Soleado	10	9	8	1
Parcialmente Nublado	10	10	9	1
Totalmente Nublado	10	9	7	2

Realizado por: Pañi Cristian,2020

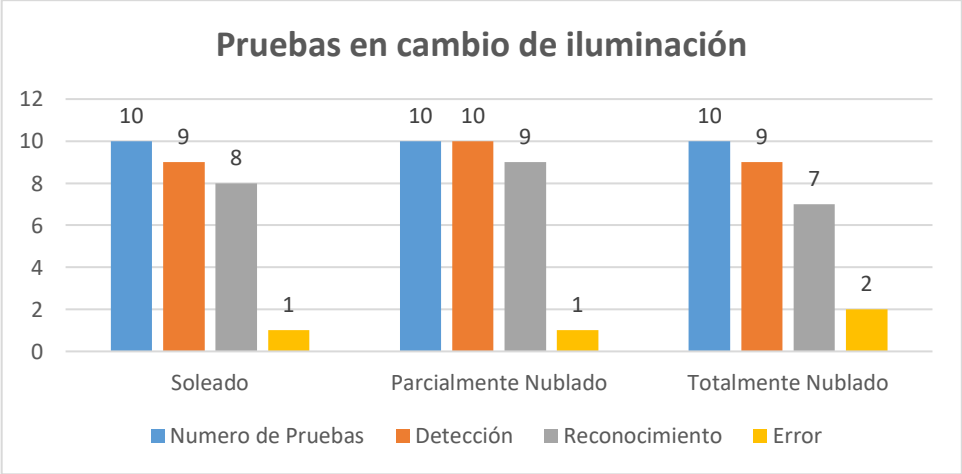


Gráfico 1-4: Gráfico pruebas con cambio de iluminación

Realizado por: Pañi Cristian,2020

El uso de cámaras con mayor o menor resolución es capaz de afectar los datos presentados en la gráfica 1-4. La distancia del usuario a la cámara no se tomó como medida de referencia ya que este factor puede ser manejado desde el código que controla el sistema, esto se realizó controlando el tamaño de rostro presente en la imagen que puede ser aceptado por el sistema.

4.2 Pruebas de Reconocimiento Facial

El reconocimiento del personal es la base del presente trabajo de titulación es así que para este aspecto se destinó una gran cantidad de tiempo hasta lograr que se lo realice de la mejor manera posible.

Las pruebas realizadas se basaron en el número de captura del rostro tomadas del usuario para el entrenamiento, se puedo verificar que un número pequeño de imagen tomadas conlleva a que el usuario no sea reconocido esto es debido a que el algoritmo de reconocimiento no cuenta con las suficientes características para especificar que usuario es el que está al frente de la cámara. Por lo contrario, un numero de muestras muy alto solo consumirá mayores recursos de la placa controladora sin brindar un beneficio mayor. En la tabla y grafica 2-3 se presenta los resultados.

Tabla 2-4: Pruebas de Reconocimiento

Nº de imágenes tomadas	Nº de pruebas	Acierto	Porcentaje
50	50	3	6%
100	50	8	16%
250	50	17	34%
500	50	30	60%
1000	50	46	92%
2000	50	46	92%

Realizado por: Pañi Cristian,2020

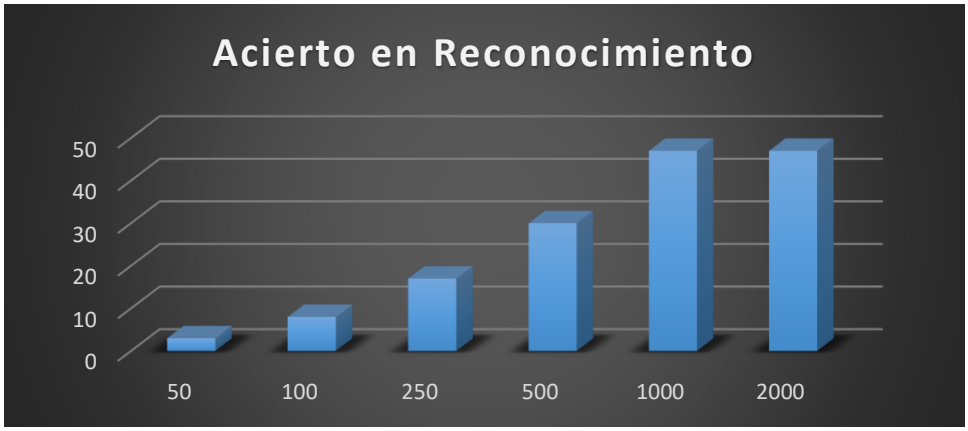


Gráfico 2-4: Número de reconocimientos correctos en base a las capturas

Realizado por: Pañi Cristian,2020

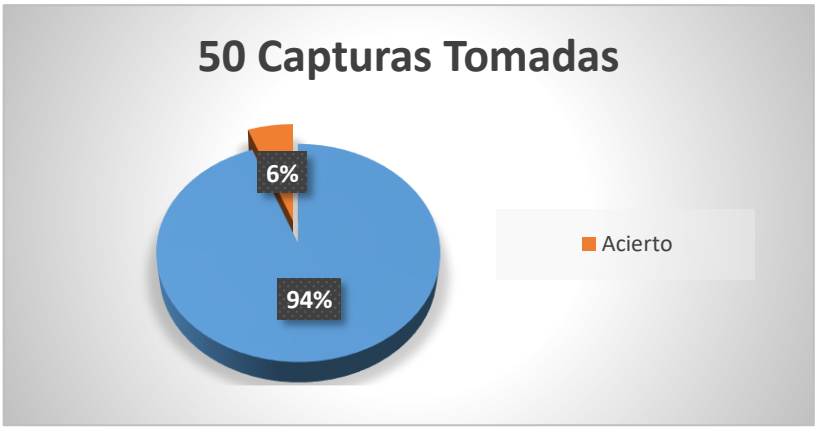


Gráfico 3-4: Resultado 50 muestras

Realizado por: Pañi Cristian,2020

Analizando el grafico 3-3, se observó que con un numero de 50 muestras tomadas del rostro del usuario, el porcentaje de aciertos en el reconocimiento es de tan solo 6%, dicho porcentaje no es aceptable para ningún sistema de reconocimiento. Además, como dato adicional se tomó el tiempo de captura de las imágenes que dio 6.33 segundos.

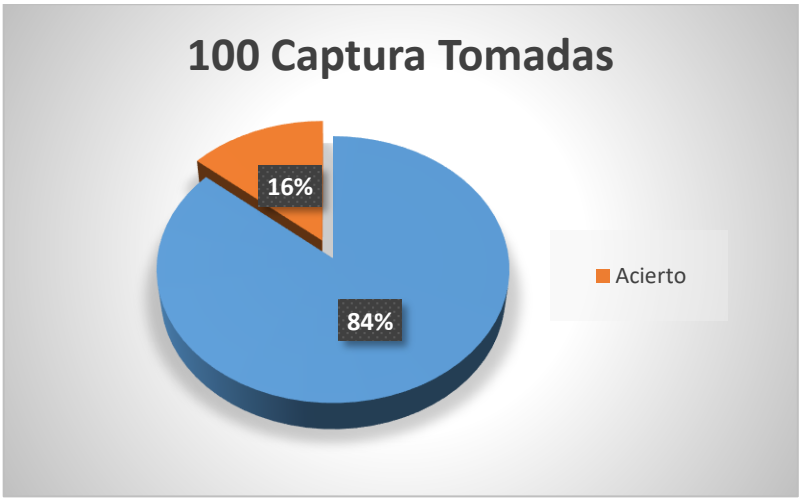


Gráfico 4-4: Resultado 100 muestras

Realizado por: Pañi Cristian,2020

El grafico 3-3 muestra el resultado del proceso de reconocimiento con un total de 100 capturas tomadas, se observó que el porcentaje de aciertos es del 14% un porcentaje demasiado bajo para que el sistema realice las acciones correctamente. El tiempo que se tardó en capturar las 100 muestras fue de 12.57 segundos.

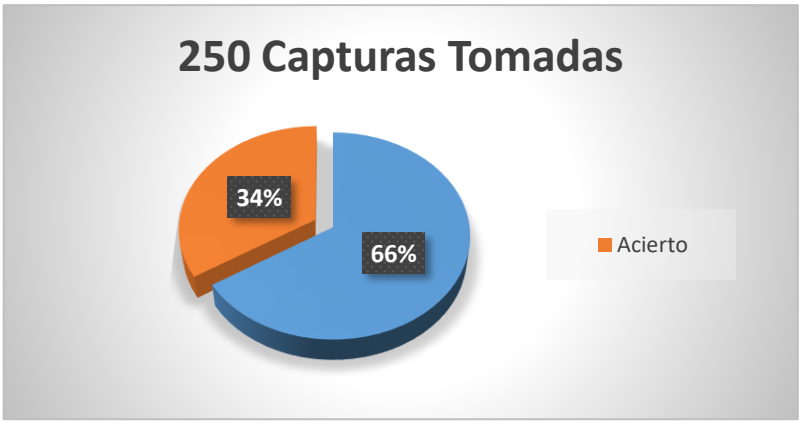


Gráfico 5-5: Resultado 100 muestras

Realizado por: Pañi Cristian,2020

De el gráfico 4-3 se pudo deducir que, con 250 capturas, el porcentaje de reconocimiento es de 34% dicho porcentaje es todavía bajo para realizar un sistema de reconocimiento. El tiempo que se tardó en la captura de las imágenes es de 18.97 segundos.

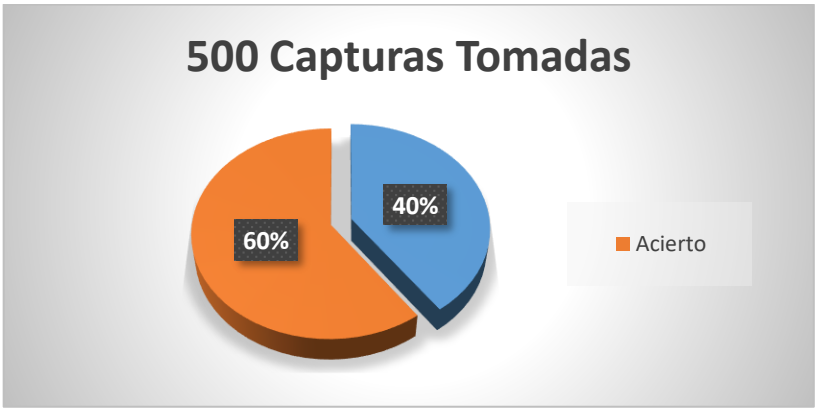


Gráfico 6-4: Resultado 500 muestras

Realizado por: Pañi Cristian,2020

Con 500 muestras capturas tomadas el porcentaje de aciertos en reconocimiento es de 70% para un sistema de reconocimiento se lo puede utilizar, sin embargo, para un sistema de seguridad todavía es bajo ya que puede dar acceso a personas incorrectas. El tiempo de captura fue de 40.08 segundos.

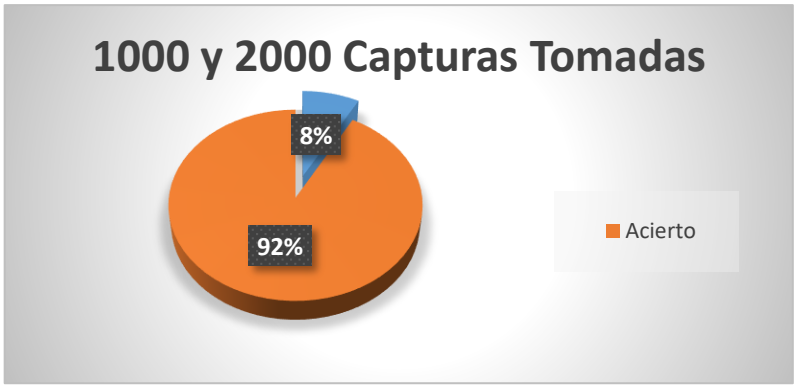


Gráfico 7-4: Resultado 1000 muestras

Realizado por: Pañi Cristian,2020

Como se puede observar en las pruebas realizadas el número de aciertos con 1000 y 2000 imágenes capturadas no difiere en un porcentaje significativo, es por ello que se procedió a poner los mismos datos en ambos casos dando como resultado la gráfica 7-4. Sin embargo, el tiempo que tarda en capturar las imágenes si tuvo un cambio significativo es así que para 1000 imágenes se tardó 1.08 minutos y para 2000 imágenes se tardó 2.04 minutos.

Para que el sistema no conceda el acceso a personas equivocadas se programó un método por número de veces que se reconoció a la misma persona, para que la cerradura magnética de la puerta se abra.

El tiempo que llevó el proceso de entrenamiento para un total de 9000 imágenes que se pudo medir fue de 4.18 minutos. Lo que equivale tener en la base de datos 9 usuarios a ser reconocidos.

4.3 Análisis de la Funcionalidad del Prototipo

La implementación del prototipo se lo realizó en uno de los locales de una pequeña empresa de la ciudad llamada Smart Electronic, las pruebas se realizaron con el personal perteneciente a la misma.

El proceso se realizó de manera de observación experimental, analizando los diferentes procesos que realiza el prototipo como son: reconocimiento, lectura del sensor de movimiento, lectura del sensor de vibración o golpe, captura y envió de la imagen hacia la aplicación móvil. Los resultados se presentan en la tabla 4-4 y la gráfica 8-4.

Tabla 3-4: Pruebas de Funcionamiento

Nº Prueba	Reconocimiento	Sensor Movimiento	Sensor Vibración	Aplicación
1	X	X	X	X
2	X	X	X	X
3	X	X	X	X
4	X	X	X	X
5	X	X	X	X
6	X	X	X	X
7	X	X	X	X
8	X	X	X	X
9		X	X	X
10	X	X	X	X
11	X	X	X	X
12	X	X	X	X
13	X	X	X	X
14	X	X	X	X
15	X	X	X	X
16	X	X	X	X
17	X	X		
18	X	X	X	X
19	X	X	X	X
20	X	X	X	X
21		X	X	X
22	X	X	X	X
23	X	X	X	X
24	X	X	X	X
25	X	X	X	X

Realizado por: Pañi Cristian,2020

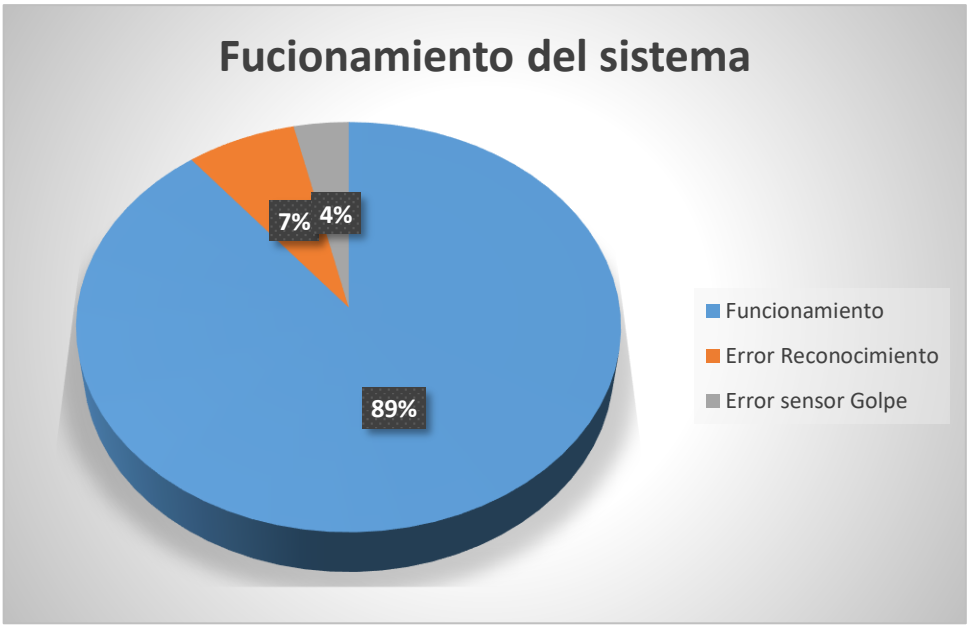


Gráfico 8-4: Funcionamiento del sistema.

Realizado por: Pañi Cristian,2020

En la gráfica 7-3 se puede observar que una vez se hicieron las pruebas del prototipo en su totalidad con todos sus sensores y actuadores el porcentaje de funcionamiento del sistema fue del 89%, mientras que el porcentaje de error en Reconocimiento fue de 7% y el porcentaje de error del sensor de vibración o golpe fue de 4%. El sensor de lectura de presencia no genero errores en todas las pruebas se activó de una manera correcta. No se tomó en cuenta el error de envío de la imagen hacia la aplicación pues esta depende del que el sensor de vibración se active y siempre que lo hizo la imagen llego de una manera correcta hacia la aplicación.

4.4 Análisis de costos

En la tabla 4-4 se presenta los costos que tuvieron los diferentes dispositivos que conforman el prototipo. No se tomaron en cuenta costos de dispositivos que se dañaron en el transcurso de la elaboración del trabajo de titulación.

Tabla 4-4: Costos del Prototipo

MATERIALES	CANTIDAD	PRECIO UNITARIO ($)	PRECIO TOTAL ($)
Raspberry pi 3 b+, carcasa, disipador y cargador	1	125	125
Módulo de cámara raspberry pi NoIR V2 5MP	1	50	50
Cerradura electromagnética ZKTeco LM-280 280Kg	1	90	90
Sensor de movimiento CoMET RK210PR	1	30	30
Sensor de golpe RK600S	1	30	30
Componentes electrónicos (optoacoplador, resistencias, transistores, diodos, cableado, etc.)	-	30	30
Impresión 3D	1	50	50
TOTAL			405

Realizado por: Pañi Cristian,2020

4.5 Comparación del Prototipo con Productos Comerciales.

En la tabla 5-4 se presenta las características de los diferentes dispositivos existentes en el mercado los mismo que son capaces de realizar el control de acceso mediante reconocimiento facial.

Tabla 5-4: Ventajas y desventajas de los productos existentes en el mercado

PRODUCTOS EXISTENTES EN EL MERCADO			
PRODUCTOS	**VENTAJAS**	**DESVENTAJAS**	**COSTO**
HANVON FACEID F710X	Control de asistencia. Control de Acceso Capacidad para 500 usuarios.	La información solo se puede ver desde el terminal. La alarma es local. Más utilizada para control de asistencia.	Costo del dispositivo 490 dólares.

	Alarma si se quitan los tornillos para abrir el dispositivo.		
FACIAL COOL-A	Control de asistencia. Control de acceso. Capacidad 800 usuarios. Se puede exportar los datos mediante dispositivo USB.	No cuenta con un sistema de alarma. Buen reconocimiento facial utiliza varios puntos característicos de la cara. Diseñado para control de asistencia y tiempo.	Costo del dispositivo 530 dólares.
FACE PASS	Control de asistencia Control de Acceso. Capacidad para 400 usuarios. Sensor infrarrojo para autoencendido.	No tiene un sistema de alarma. Reconocimiento facial basado en los puntos característicos superiores del rostro.	Costo del dispositivo 450 dólares.
UFACE4	Control de asistencia. Control de Acceso. Capacidad para 300 usuarios. Alerta de apertura de puerta mediante app. .	No cuenta con un sistema de alarma. Reconocimiento facial utilizando puntos característicos de los ojos	Costo del dispositivo 350

Realizado por: Pañi Cristian,2020

Al comparar el precio del prototipo diseñado en el presente trabajo de titulación con los dispositivos existentes, se llegó a la conclusión que el prototipo se encuentra en el rango de precio de los mismos. Pero con mejores ventajas debido a que es capaz de superar las desventajas que estos presentan entre las más importantes, el prototipo es capaz de alertar cuando se produzca una irrupción por la fuerza, esta alerta podrá ser conocida por el usuario en cualquier parte pues se utiliza una aplicación móvil la misma que se puede observar en las figuras 22-3 y 23-3 , para darla a conocer, así mismo, el método utilizado para reconocimiento facial usa los puntos característicos presentes en todo el rostro para autentificar al usuario.

Actualmente el prototipo es capaz de almacenar una cantidad de 200 usuarios, y controlar el acceso a dos áreas, lo mismo que al realizar una comparación en función de costos el dispositivo más barato descrito en la tabla 6-4, el mismo que no es el más seguro para controlar dos áreas el costo sería aproximadamente de 700 dólares una cantidad superior al precio costo del prototipo desarrollado.

CONCLUSIONES

En la investigación realizada previo al diseño e implementación del prototipo, se estudiaron 4 de los principales algoritmos que existen en la actualidad utilizados en el reconocimiento facial. Luego de un análisis de cada uno de ellos se decidió utilizar el LBPH debido a las ventajas que presenta. Además, se optó por elegir programación basada en lenguaje Python y ejecutado sobre un sistema Raspbian instalado en una placa Raspberry PI 3 b+.

El sistema inmótico se diseñó para que la cámara no permanezca encendida todo el tiempo mediante el uso de un sensor de movimiento que activa la captura de video únicamente cuando es requerido. Además, Para tener una mayor seguridad ante intrusiones forzadas en el área restringidas se hizo uso de un sensor de golpe o vibraciones, el cual envía una señal para realizar una captura de imagen en tiempo real para luego enviarla hacia la plataforma web firebase y posteriormente ser recibida por la aplicación móvil.

Como sistema de transmisión de señales desde la placa controladora hasta los sensores de vibración, movimiento y el actuador que es la chapa electromagnética se decidió utilizar cable par trenzado, debido a sus características y bajo costo.

El entrenamiento se lo realizo haciendo uso de mil imágenes, esto con el fin de obtener una identificación optima de cada usuario del sistema, en las imágenes se tiene el rostro de la persona con múltiples expresiones faciales y diferente orientación del rostro, además se concluyó que el proceso de captura de imágenes se lo debe realizar donde estará ubicado el prototipo esto con el fin de evitar un gran cambio en el factor de iluminación. El proceso de entrenamiento se lo debe realizar únicamente al añadir o eliminar un usuario.

Al analizar los datos arrojados por las pruebas se puede deducir que el prototipo cumple con los requerimientos que se planteó en el diseño. Durante las pruebas de funcionamiento se determinó que el prototipo tiene una eficiencia del 89%. Cabe recalcar que se registraron errores en el sensor de golpe, y que su incidencia podría disminuir haciendo uso de un sensor que tenga mayor sensibilidad hacia vibraciones o golpes.

RECOMENDACIONES

Para una buena eficiencia en identificación se recomienda el uso de cámara con una mayor resolución ya que de no ser así el porcentaje de detección y reconocimiento presentado en este documento puede variar de forma negativa causando que el prototipo no cumpla los requerimientos presentados al momento del diseño.

Si se hace uso de sensores que manejen un voltaje de alimentación superior al recomendado para la operación en los pines GPIO de la placa Raspberry, se recomienda implementar etapas de acondicionamiento de la señal para evitar sobrevoltajes o daños a la placa.

Es necesario la implementación de un circuito de protección desde la parte de control de la cerradura electromagnética que funciona con un voltaje de 12V DC hacia la placa Raspberry, uno de los componentes mejor diseñados para este propósito es el uso de un driver compuesto por un circuito integrado optoacoplador.

Es importante mencionar que, si se instala el sistema en un negocio, empresa, industria, etc. Se debe implementar un sistema de respaldo de energía para mantener activo el control de acceso o a su vez utilizar una cerradura eléctrica pues se pueden abrir con una llave si se produce estos inconvenientes, a diferencia de la cerradura electromagnética utilizada, la cual únicamente se puede controlar su apertura o cierre mediante la manipulación del voltaje de alimentación.

GLOSARIO

Algoritmo: Conjunto ordenado de operaciones sistemáticas que permite hacer un cálculo y hallar la solución de un tipo de problemas**.** (Oxford Languajes, s.f.)

Aplicación móvil: Una aplicación móvil es un programa que usted puede descargar y al que puede acceder directamente desde su teléfono o desde algún otro aparato móvil – como por ejemplo una tablet o un reproductor MP3. (ups,2018)

Artificial: Que ha sido hecho por el ser humano y no por la naturaleza. Que no se ajusta a lo que ya hay en la naturaleza. (Oxford Languajes, s.f.)

Arquitectura: Técnica y estilo con los que se diseña, proyecta y construye un edificio o un monumento. (Oxford Languajes, s.f.)

Biometría: Aplicación de métodos estadísticos y cálculo en el estudio de los fenómenos biológicos. (Oxford Languajes, s.f.)

Electromagnética: Parte de la física que estudia las relaciones entre el magnetismo y la electricidad. Magnetismo producido por una corriente eléctrica. (Oxford Languajes, s.f.)

Escala de grises: La escala de grises o valor, en artes gráficas y bellas artes, es el sistema ordenado y gradual que cubre un rango limitado de valores de luminosidad entre el blanco, el gris y el negro. (ups,2018)

Interfaz Gráfica: La Interfaz gráfica de usuario, también conocida como GUI (Graphical User Interface), es un programa que hace las veces de intermediario entre usuario y máquina. (ups,2018)

Protocolo: Conjunto de reglas de formalidad que rigen los actos y ceremonias diplomáticos y oficiales. Conjunto de reglas de cortesía que se siguen en las relaciones sociales y que han sido establecidas por costumbre. (Oxford Languajes, s.f.)

Prototipo: Primer ejemplar que se fabrica de una figura, un invento u otra cosa, y que sirve de modelo para fabricar otras iguales, o molde original con el que se fabrica. (Oxford Languajes, s.f.)

Topología: Ciencia que estudia los razonamientos matemáticos, prescindiendo de los significados concretos**.** (Oxford Languajes, s.f.)

Reconocimiento: Acción de reconocer o reconocerse. (Oxford Languajes, s.f.)

BIBLIOGRAFIA

ALABUELA, M. & MAÑAY, C. "DISEÑO DE INGENIERÍA INMÓTICA DE LABORATORIOS DEL BLOQUE 3 – SEDE QUERI DE LA UNIVERSIDAD DE LAS AMÉRICAS" (Trabajo de Titulación) (Pregrado). Universidad de las Américas. Quito-Ecuador. (2018), [En línea]. [Consulta: 16 de octubre del 2019]. Disponible en: http://dspace.udla.edu.ec/handle/33000/8967

ÁLVAREZ, K. & PALAGUACHI, I. "DISEÑO DE UN MÓDULO DIDÁCTICO PARA SISTEMAS DE CONTROL DOMÓTICO CON APLICACIONES DE VIDEO VIGILANCIA SUPERVISADO POR UN TELÉFONO MÓVIL". (Trabajo de Titulación) (Pregrado). Universidad Politécnica Salesiana. Guayaquil-Ecuador. (2015), [En línea]. [Consulta: 10 de octubre del 2019]. Disponible en: https://dspace.ups.edu.ec/handle/123456789/10377

APRENDER SOBRE ELECTRÓNICA. Diferencia Entre Los Transistores NPN y PNP electrónica. [Entrada de blog]. (2017), [Consulta: 22 de octubre del 2019]. Disponible en: http://www.learningaboutelectronics.com/Articulos/Diferencia-entre-transistores-NPN-y-PNP.php

CEDOM. Que es Domótica. [En línea] (2018). [Consulta: 10 de octubre del 2019]. Disponible en: http://www.cedom.es/sobre-domotica/que-es-domotica

CERVANTES, F. "ESTUDIO DE LOS MEDIOS DE TRANSMISION EN REDES COMPUTACIONALES MIXTAS (ALAMBRICA – INALAMBRICA)". (Trabajo de Titulación) (Pregrado). Universidad Técnica del Norte. Barrranquilla-Colombia (2002), [En línea]. [Consulta: 07 de noviembre del 2019]. Disponible en: http://repositorio.utn.edu.ec/bitstream/123456789/1112/1/04%20ISC%20004%20Tesis%20Final.pdf

CEVALLOS, A. "DETECCIÓN DE ROSTROS EN ESCENAS DE VIDEO UTILIZANDO HERRAMIENTAS GPU-CUDA". (Trabajo de Titulación) (Pregrado). ESPE. Quito-Ecuador (2017), [En línea]. [Consulta:27 de noviembre del 2019]. Disponible en: https://repositorio.espe.edu.ec/bitstream/21000/12780/1/T-ESPE-053701.pdf

CORTIJO, S. "Diseño e implementación de una interfaz de domótica asistencial basado en realidad aumentada". (Trabajo de Titulación) (Pregrado). Universidad Carlos III de Madrid. Madrid-España. (2015), [En línea]. [Consulta: 16 de octubre del 2019]. Disponible en: https://e-archivo.uc3m.es/handle/10016/23817

CUPERAN, M. & ORTIZ, J. "DISEÑO E IMPLEMENTACIÓN DEL SISTEMA INMÓTICO EN EL EDIFICIO DE EDUCACIÓN TÉCNICA DE LA UNIVERSIDAD TÉCNICA DEL NORTE". (Trabajo de Titulación) (Pregrado). Universidad Técnica del Norte. Barranquilla-Colombia. (2015), [En línea]. [Consulta: 27 de septiembre del 2019]. Disponible en: http://repositorio.utn.edu.ec/handle/123456789/5019

ESPINOZA, D.; JORQUERA, P. "Reconocimiento Facial". (Trabajo de Titulación) (Pregrado). Universidad Católica de Valparaíso. Valparaíso-Chile. (2015), [En línea]. [Consulta: 27 de noviembre del 2019]. Disponible en: http://opac.pucv.cl/pucv_txt/txt-1000/UCD1453_01.pdf

FERNÁNDEZ, M. Medios de Transmisión Redes de Datos. (Trabajo de Titulación) (Pregrado). Universidad de Cádiz. Cádiz-España. (2017), [En línea]. [Consulta: 07 de noviembre del 2019]. Disponible en: https://rodin.uca.es/xmlui/bitstream/handle/10498/16867/tema05_medios.pdf

FLORES, M.; CANTOS, G. & MONARD, J. Implementación de Sistema Inmótico: Estudio de Protocolos de Comunicación. ISSN: 1390-6399. DOI: 10.31095/irr.v0i8.7. Guayaquil-Ecuador (septiembre,2016), [En línea]. [Consulta: 27 de septiembre del 2019] Recuperado de: http://revistas.uees.edu.ec/index.php/IRR/article/view/7

GALLARDO, E. & SÁNCHEZ, E. "DISEÑO Y CONSTRUCCIÓN DE UN SISTEMA DE AUTENTIF ICACIÓN CON RECONOCIMIENTO FACIAL MEDIANTE PROCESAMIENTO DE IMÁGENES CON LA UTILIZACIÓN DE SOFTWARE L IBRE Y TECNOLOGÍA RASPBERRY PI". (Trabajo de Titulación) (Pregrado). ESPE. Quito-Ecuador. (2016), [En línea]. [Consulta: 02 de octubre del 2019]. Disponible en: http://repositorio.espe.edu.ec/xmlui/handle/21000/10591

GIRALDO, A. & GÓMEZ, D. ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS. (Tesis) (Maestría). Universidad Abierta y a Distancia. Ciudad de Mexico-Mexico. (2017), [En línea]. [Consulta: 10 de octubre del 2019]. Disponible en: https://repository.unad.edu.co/handle/10596/14348

MAESTRE, J. *Domótica para ingenieros*. 1ra Edición. Madrid, España. Ediciones Parainfo S.A. (2015), [En línea]. [Consulta: 10 de noviembre del 2019]. Disponible en: books.google.com.ec/books?id=BAHsBgAAQBAJ&pg=PA101&dq=protocolos+de+comunicacion+domotica&hl=es&sa=X&ved=2ahUKEwjJ6Z6D1q_qAhXikOAKHZ3IDywQ6AEwAnoECAYQAg#v=onepage&q=protocolos%20de%20comunicacion%20domotica&f=false

MDA SECURITY. Sistemas de control de Acceso. [Entrada de blog]. (2016). [Consulta: 10 de noviembre del 2019]. Disponible en: http://www.mdasecurity.net/sistema-de-control-de-acceso.html

MORO, M. *Infraestructuras de redes de datos y sistemas de telefonía*. 1ª Edición. Madrid España.

PARAINFO S.A. (2016). [Consulta: 10 de noviembre del 2019]. Disponible en: books.google.com.ec/books?id=lkBhTrHLBlEC&pg=PT15&dq=libros+TIPO+DE+TOPOLOGIAS+DE+REDES&hl=es&sa=X&ved=2ahUKEwjxr564u6_qAhXLUt8KHfsFB3cQ6AEwAXoECAQQAg#v=onepage&q=libros%20TIPO%20DE%20TOPOLOGIAS%20DE%20REDES&f=false

PÉREZ, E. "SISTEMA DOMOTICO CON TECNOLOGÍA ARDUINO PARA AUTOMATIZAR SERVICIOS DE SEGURIDAD DEL HOGAR". (Trabajo de Titulación) (Pregrado). Universidad Cesar Vallejo. Trujillo-Perú. (2016), [En línea]. [Consulta:27 de septiembre del 2019]. Disponible en: http://revistas.ucv.edu.pe/index.php/INNOVACION/article/view/985/772

PLATERO, D. "RECONOCIMIENTO DE IMÁGENES FACIALES ORIENTADO A CONTROLES DE ACCESO Y SISTEMAS DE SEGURIDAD". (Trabajo de Titulación) (Pregrado). Universidad Distrital "Francisco José de Caldas. Bogotá-Colombia. (2015), [En línea]. [Consulta: 22 de octubre del 2019]. Disponible en: http://repository.udistrital.edu.co/handle/11349/7359

PREKSHA, V. Home Automation Market by Application (Lighting, Safety & Security, HVAC, Entertainment, and Others), Type (Luxury, DIY, Managed, and Mainstream), and Technology (Wired and Wireless) - Global Opportunity Analysis and Industry Forecast, 2017-2023. (2017), [En línea]. [Consulta: 27 de septiembre del 2019]. Disponible en: https://www.alliedmarketresearch.com/home-automation-market

QUINDE, I. "DISEÑO DE UN SISTEMA INMÓTICO PARA CONTROL, MONITOREO, SEGURIDAD Y AHORRO ENERGÉTICO EN EL CAMPUS DE INGENIERÍA Y ARQUITECTURA DE LA UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA SEDE AMBATO". (Tesis) (Maestría). Escuela Superior Politécnica del Chimborazo- Riobamba-Ecuador. (2017), [En línea]. [Consulta: 27 de septiembre del 2019]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/6167

RIVERA, J. *Fundamentos de Redes Informáticas*. 2ª Edición. Carolina del Sur, Estados Unidos. Create Space. (2016). [Consultado: 02 de octubre del 2019]. Disponible en: books.google.com.ec/books?id=gGTkDAAAQBAJ&printsec=frontcover&dq=libros+TIPO+DE+TOPOLOGIAS+DE+REDES&hl=es&sa=X&ved=2ahUKEwjxr564u6_qAhXLUt8KHfsFB3cQ6AEwAnoECAYQAg#v=onepage&q&f=false

SOFTWARELAB.ORG. "Que es URL y para qué sirve". [Entrada de Blog.] (2020). [Consulta: 12 de mayo del 2020]. Recuperado de: https://softwarelab.org/es/url/

SOLIS, L. & PUGA, L. Control de Seguridad Biométrico de Reconocimiento F acial como Caso de Estudio Implementación en el Área Administrativa de la Facultad de Ingeniería de la Universidad Católica de Santiago de Guayaquil". (Trabajo de Titulación) (Pregrado). Universidad Católica de Santiago de Guayaquil. Guayaquil-Ecuador. (2016), [En línea]. [Consulta: 22 de octubre del 2019]. Disponible en: http://192.188.52.94:8080/handle/3317/6737

SEGU.INFO. Seguridad Física – Sistemas Biométricos. [Entrada de blog] (2018). [Consulta: 22 de octubre del 2019]. Recuperado de: https://www.segu-info.com.ar/fisica/biometricos

TRAPIELLA, R. "DESARROLLO Y EVALUACIÓN DE TÉCNICAS DE VISIÓN ARIFICIAL APLICADAS A UN PROBLEMA DE ROCONOCIMIENTO FACIAL". (Tesis) (Maestría). Escuela Técnica Superior de Ingeniería Informática. Málaga-España (2018), [En línea]. [Consulta: 02 de octubre del 2019].

VALVERDE, G. Paradigma Semiótico y Reconocimiento Facial. Universidad Técnica Salesiana. Trabajo presentado en Conferencia CITIS – Congreso Salesiano de Ciencias, Tecnologías e Innovación para la sociedad 2014. Guayaquil, Ecuador. (noviembre, 2014), [En línea]. [Consulta: 27 de octubre del 2019]. Disponible en: https://www.researchgate.net/publication/280556949_Paradigma_Semiotico_y_Reconocimiento_Facial

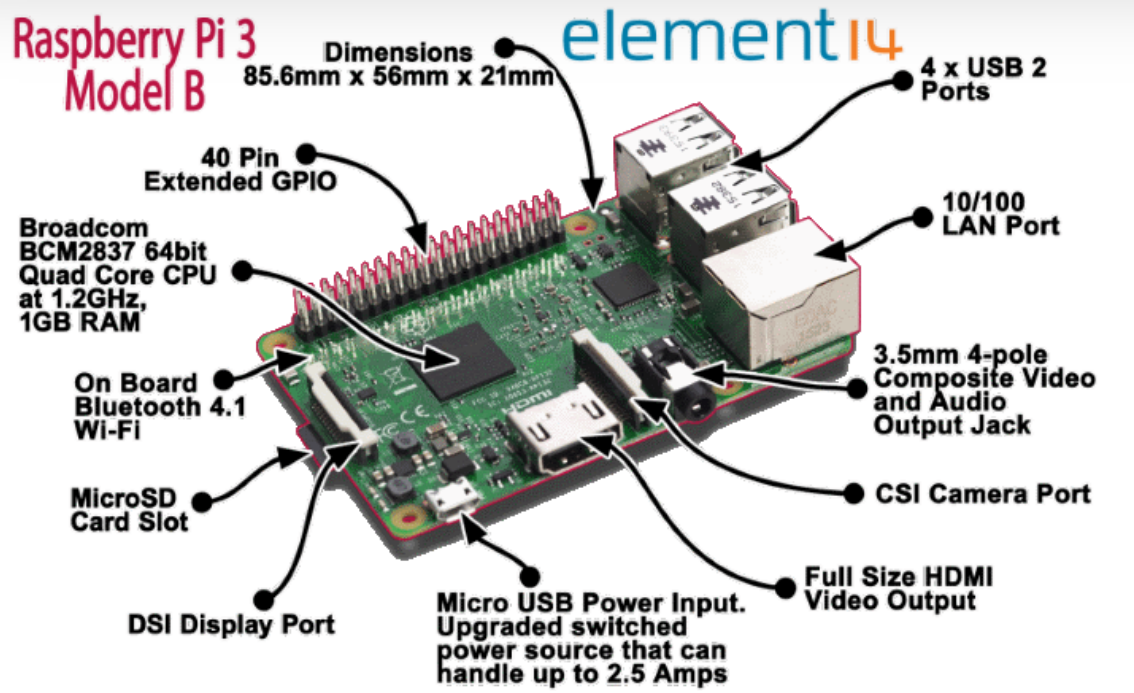
VÁZQUEZ, M. "Sistema de Reconocimiento Facial Mediante Técnicas de Visión Tridimensional". (Tesis) (Maestría). Centro de Investigaciones en Óptica, A.C. Nuevo León-México. (2014). [En línea]. [Consulta: 29 de noviembre del 2019]. Disponible en: https://cio.repositorioinstitucional.mx/jspui/handle/1002/436

VILLALÓN, D. "DISEÑO E IMPLEMENTACIÓN DE UNA PLATAFORMA DE SOFTWARE PARA RECONOCIMIENTO FACIAL EN VIDEO". (Trabajo de Titulación) (Pregrado). Universidad de Chile. Santiago-Chile. (2012), [En línea]. [Consulta: 27 de noviembre del 2019]. Disponible en: http://repositorio.uchile.cl/bitstream/handle/2250/112271/cfvillalon_dd.pdf?sequence=1&isAllowed=y

ZAPATERO, D. HERRAMIENTA DE RECONOCIMIENTO FACIAL DE EMOCIONES EN ANDROID". (Trabajo de Titulación) (Pregrado). Universidad Técnica del Norte. Barranquilla-Colombia. (2016), [En línea]. [Consulta:16 de octubre del 2019]. Disponible en: http://oa.upm.es/44722/3/TFG_DIEGO_ZAPATERO_OLMEDILLO.pdf

ANEXOS

Anexo A: Características y especificaciones de la Raspberry pi 3 b+

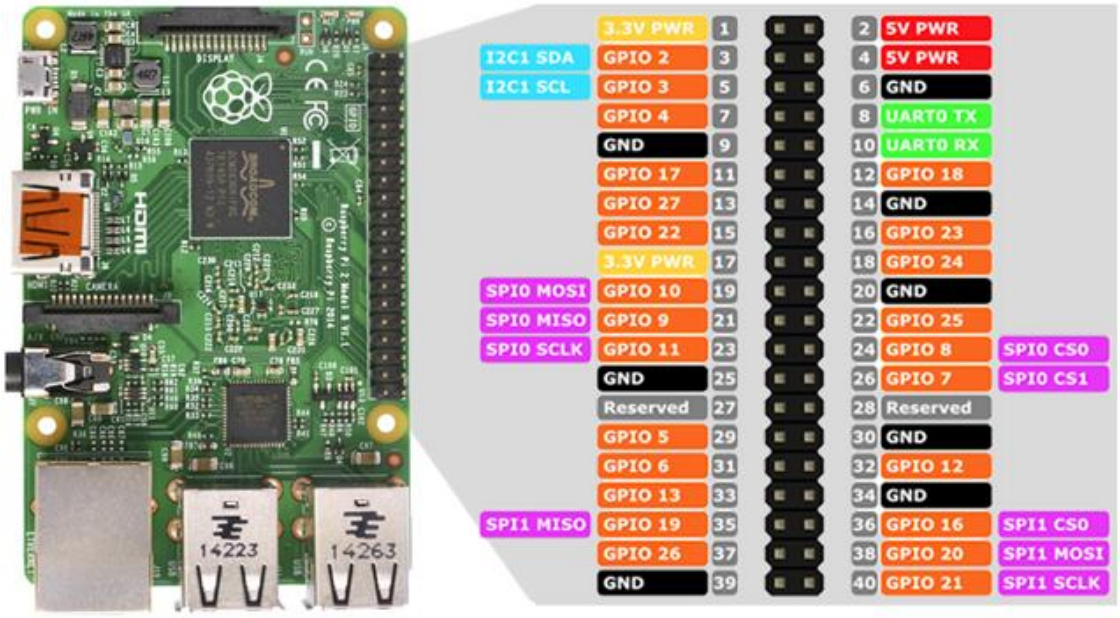


Fuente: Giraldo, Gomez,2017

Especificaciones

- Broadcom BCM2837B0, Cortex-A53(ARMv8) 64-biy SoC @ 1.4GHz
- 1 GB LPDDR2 SDRAM
- 2.4GHz y 5GHz IEEE 802.11.b/g/n/ac wireless LAN, Bluetooth 4.2 BLE
- Gigabit Ethernet over USB 2.0 (maximum throughput 300 Mbps)
- Extended 40-pin GPIO header
- Full-size HDMI
- USB 2.0 ports
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- 4-pole stereo output and composite video port
- Micro SD port for loading your operating system and storing data
- 5V/2.5A DC power input
- Power-over-Ethernet (PoE) support (requires separate PoE HAT)

Anexo B: Distribución de Pines GPIO en raspberry pi



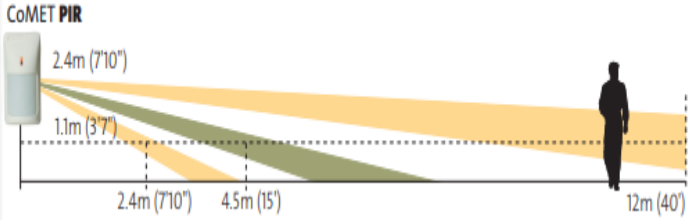
Existen dos maneras para numerar los pines:

Modo GPIO: La numeración de los pines concuerda con la posición que tienen los mismas en la placa.

Modo BCM: La numeración se la lleva acabo de acuerdo con el chip Broadcom que está instalada en la placa controladora.

BOARD	GPIO		GPIO	BOARD
01	3.3v DC Power		DC Power 5v	02
03	GPIO02 (SDA1 , I²C)		DC Power 5v	04
05	GPIO03 (SCL1 , I²C)		Ground	06
07	GPIO04 (GPIO_GCLK)		(TXD0) GPIO14	08
09	Ground		(RXD0) GPIO15	10
11	GPIO17 (GPIO_GEN0)		(GPIO_GEN1) GPIO18	12
13	GPIO27 (GPIO_GEN2)		Ground	14
15	GPIO22 (GPIO_GEN3)		(GPIO_GEN4) GPIO23	16
17	3.3v DC Power		(GPIO_GEN5) GPIO24	18
19	GPIO10 (SPI_MOSI)		Ground	20
21	GPIO09 (SPI_MISO)		(GPIO_GEN6) GPIO25	22
23	GPIO11 (SPI_CLK)		(SPI_CE0_N) GPIO08	24
25	Ground		(SPI_CE1_N) GPIO07	26
27	ID_SD (I²C ID EEPROM)		(I²C ID EEPROM) ID_SC	28
29	GPIO05		Ground	30
31	GPIO06		GPIO12	32
33	GPIO13		Ground	34
35	GPIO19		GPIO16	36
37	GPIO26		GPIO20	38
39	Ground		GPIO21	40

Anexo C: Sensor de Movimiento CoMET RK210PR



Especificaciones	CoMET **PIR**	CoMET **PET**
Inmunidad a mascotas	Pequeños roedores	Perros de hasta 20 Kg, 2 gatos o varios roedores
Cobertura a una altura de 2.4m(7'10")	12m X 12m (40' x 40')	8m (26') 90°
Voltaje de operación	9 a 16V regulados	
Consumo de corriente	12mA a 12V	
Contacto de Alarma	50mA, 24V, N.C	
Contacto de Tamper (Versiones con Tamper)	100mA, 24V, N.C	
Tiempo de Alarma	Mínimo: 2,2 Segundos	
Contador de Pulsos	Para 1, 2, o 3 Pulsos	
Compensación de temperatura	Automática, Controlado por termistor	
Filtrado Optico	Protección contra luz blanca, Lentes pigmentados	
Inmunidad a la RF (10 MHz a 1 GHz)	20V/m	
Temperatura de operación	-5 to 50°C (23 a 122°F)	
Temperatura de almacenaje	-20 to 55°C (-4 a 131°F)	
Dimensiones	89 x 52 x 39 mm (3.5 x2.0 x 1.5 inch)	

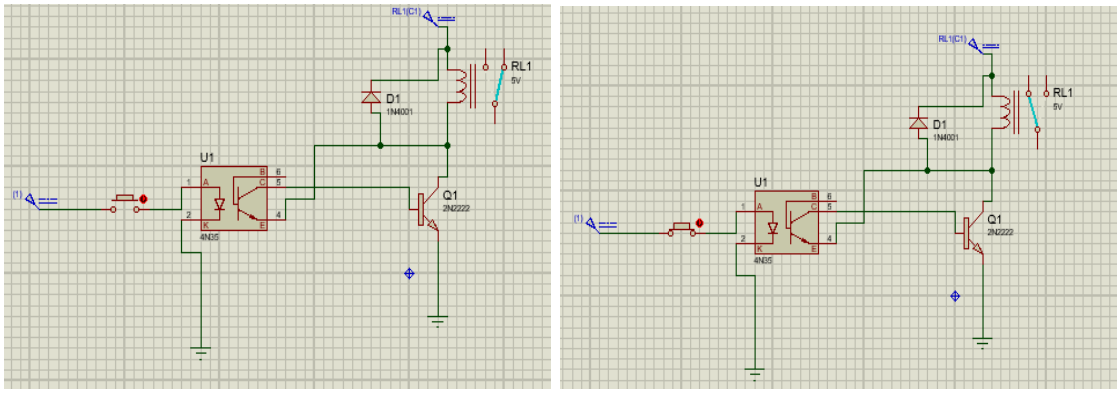
Fuente: argseguridad

ANEXO D: Sensor de golpe RK600S

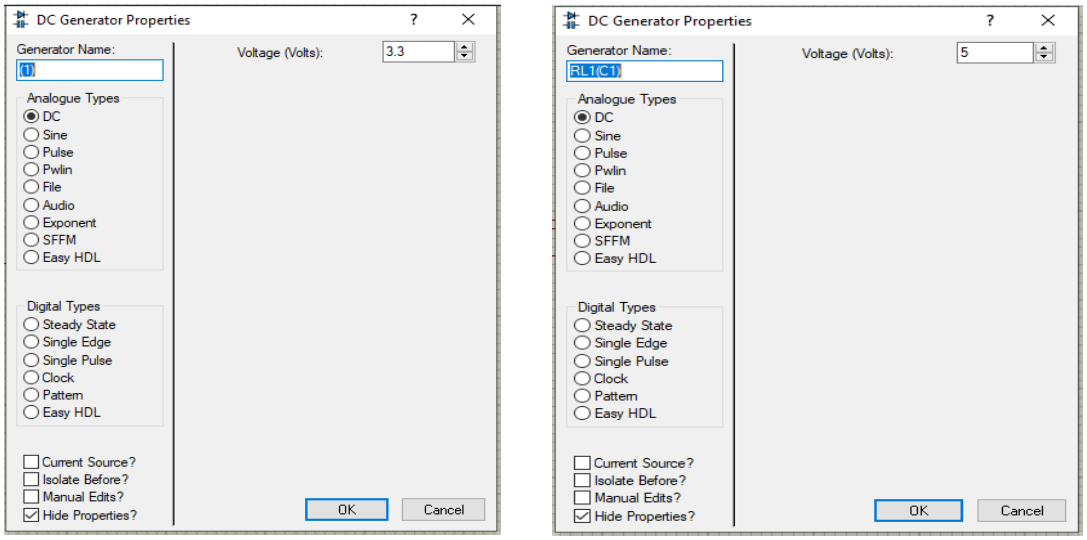
Especificaciones Técnicas	
Consumo de corriente	12.5 mA.
Temperatura de funcionamiento	-20 ° C a 60 ° C.
Humedad máxima	95% sin condensación.
Ajuste de sensibilidad	potenciómetro de fase dual.
Indicador tricolor LED	Naranja-over-sensible, verde: alarma y calibración correcta, rojo: menos sensible.
Relé de alarma:	100mA a 24VDC, NC.
Sabotaje relé	500mA a 24VDC, NC.
Hora de alarma	2,5 segundos.
Modos de retención	Cualquiera o primero para enganchar modos de funcionamiento.
N ° máximo de unidades en bucle AnyLatch	80
Max no de une el primero en Latch loop	10
Protección Falsa alarma	el procesamiento de señales microprocesador digital y reducción de ruido con el plano del terreno máxima
Descarga electrostática	No hay falsas alarmas hasta 8 kV
Inmunidad a RF	40 V / m de 80 MHz a 1 GHz.
Dimensiones de la caja	25 x 28 x 95mm

Fuente: pcel.com

Anexo E: Simulación del circuito de protección de la parte de potencia



Los voltejes que se utilizaron para la simulación fueron: el primero ubicado en la parte izquierda es de 3.3 V DC el cual es el valor que genera un pin GPIO de la placa raspberry, el segundo voltaje es de 5V DC que es el voltaje que necesita el dispositivo relé para accionarse.



Anexo F: Código manejo de base de datos en python

Como se mencionó en el capítulo dos se utilizó una función para cada acción que realice el código.

```
#FUNCION PARA ENLAZAR TABLA DE USUARIOS
def runbaseusu(self, consulta, parametros=()):
    with sqlite3.connect(self.dbreconocimiento) as db:
        self.cursor = db.cursor()
        resultados = self.cursor.execute(consulta, parametros)
        db.commit()
    return resultados
```

```
#FUNCION PARA EJECUTAR CONSULTA EN LA TABALA USUARIOS DE LA BASE DE DATOS
def consultausu(self):
    # Limpiamos la tabla
    recorr = self.tabla.get_children()
    for element in recorr:
        self.tabla.delete(element)
    consulta = 'SELECT * FROM USUARIOS'
    dbfilascon = self.runbaseusu(consulta)
    for row in dbfilascon:
        self.tabla.insert('', 0, text=row[0], values=(row[1], row[2], row[3]))
```

```
#FUNCION PARA AGREGAR NUEVO USUARIO
def agregar(self):

    if self.validacion():
        self.tomarfot()
        consulta = 'INSERT INTO USUARIOS VALUES(?,?,?,?)'
        parametros = (self.name.get(), self.cedul.get(), self.edad.get(), self.cargo.get())
        self.runbaseusu(consulta, parametros)

        self.name.delete(0, END)
        self.cedul.delete(0, END)
        self.edad.delete(0, END)
        self.cargo.delete(0, END)
        messagebox.showinfo("AVISO", "ASUARIO AGREGADO")

    else:
        messagebox.showinfo("ERROR", "TODOS LOS CAMPOS DEBEN SER COMPLETADOS")
```

```python
#FUNCION PARA ELIMINAR UN USUARIO DE LA BASE DE DATOS
def EliminarUsuario(self):
    try:
        self.tabla.item(self.tabla.selection())['text']

    except IndentationError as e:
        messagebox.showinfo("ADVERTENCIA","SELECCIONE UN USUARIO")
        return
    name=self.tabla.item(self.tabla.selection())['text']
    consulta='DELETE FROM USUARIOS Where NOMBRE=?'
    self.runbaseusu(consulta,(name, ))
    shutil.rmtree("imagenes" + "/" + name)
    messagebox.showinfo("AVISO","USUARIO ELIMINADO")
    self.consultausu()
```

```python
#FUNCION PARA EDITAR DATOS DE USUARIO
def editusu(self):
    try:
        self.tabla.item(self.tabla.selection())['text']

    except IndentationError as e:
        messagebox.showinfo("ADVERTENCIA","SELECCIONE UN ASUARIO")
        return
    namean = self.tabla.item(self.tabla.selection())['text']
    cedant=self.tabla.item(self.tabla.selection())['values'][0]
    edan = self.tabla.item(self.tabla.selection())['values'][1]
    caran = self.tabla.item(self.tabla.selection())['values'][2]

    self.name.insert(0,namean)
    self.cedul.insert(0,cedant)
    self.edad.insert(0,edan)
    self.cargo.insert(0,caran)
```

ANEXO G: Código crear Interfaz en Python

```
#FUNCION CONSTRUCCION DE VENTANA USUARIO
def ventanausu(self):
    self.camara.release()
    #self.wind.destroy()
    self.wind.iconify()
    #self.wind.withdraw()
    self.usuarios= Toplevel()
    self.usuarios.geometry("565x395+300+50")
    self.usuarios.config(bg="antique white")
    self.usuarios.title("USUARIOS")
    self.usuarios.iconbitmap("user.ico")
    self.usuarios.resizable(0, 0)
# CREAMOS CONTENEDOR PARA INGRESO DE INFORMACION
self.ingreso = LabelFrame(self.usuarios, text='Informacion de Usuario Nuevo')
self.ingreso.place(x=5,y=5)
#ingreso.grid(row=0, column=1, columnspan=1, pady=10,sticky="w")
self.ingreso.config(bg="antique white")
self.ingreso.config(bd=1)
self.ingreso.config(relief="groove")
#ingreso.pack()

#CAMARA VENTAN SUSUARIOS
self.width, self.height = 350, 700
self.camarausu = cv2.VideoCapture(0)
self.camarausu.set(cv2.CAP_PROP_FRAME_WIDTH, self.width)
self.camarausu.set(cv2.CAP_PROP_FRAME_HEIGHT, self.height)
self.panelu = ttk.Label(self.usuarios, width=50)
self.panelu.place(x=235, y=5)
# self.panel.grid(row=1,column=6,padx=2)
self.leccamarausu()
```

```
# Crear entrada para nombre de usuario
Label(self.ingreso, text='Nombre: ',bg="antique white").grid(row=1, column=0)
# Crear Input
self.id= StringVar()
self.name = Entry(self.ingreso,textvariable=self.id)
self.name.focus()
self.name.grid(row=1, column=1,padx=5,pady=2)
# Entrada Cedula Usuario
Label(self.ingreso, text='Cedula: ',bg="antique white").grid(row=2, column=0)
self.cedul = Entry(self.ingreso)
self.cedul.grid(row=2, column=1,padx=5,pady=2)
# Entrada edad usuario
Label(self.ingreso, text='Edad: ',bg="antique white").grid(row=3, column=0)
self.edad = Entry(self.ingreso)
self.edad.grid(row=3, column=1,padx=5,pady=2)
# Entrada Cargo usuario
Label(self.ingreso, text='Cargo: ',bg="antique white").grid(row=4, column=0)
self.cargo = Entry(self.ingreso)
self.cargo.grid(row=4, column=1,padx=5,pady=2)
#Creamos Boton para agregar informacion
self.guardar= ttk.Button(self.ingreso, text='AGREGAR', command=self.agregar).grid(row=6, column=0, sticky="se",padx=5,pady=2)
```

Anexo H: Código tomar fotos en python

```
faceCascade = cv2.CascadeClassifier(cascPath)
face_id = self.name.get()
count = 0
if not os.path.exists("imagenes" + "/" + face_id):
    car = os.mkdir("imagenes" + "/" + face_id)

while (True):
    _, imagen_marco = self.camarausu.read()

    grises = cv2.cvtColor(imagen_marco, cv2.COLOR_BGR2GRAY)
    filtro = cv2.equalizeHist(grises)
    scaleFactor = 1.2
    minNeighbors = 5
    minSize = (filtro.shape[0] // 5, filtro.shape[1] // 5)

    rostro = faceCascade.detectMultiScale(filtro, scaleFactor, minNeighbors, minSize=minSize)

    for (x, y, w, h) in rostro:
        cv2.rectangle(imagen_marco, (x, y), (x + w, y + h), (255, 0, 0), 4)
        count += 1
        cv2.imwrite(os.path.join("imagenes", face_id, face_id + str(count) + ".jpg"), filtro[y:y + h, x:x + w])

    if count >= 2000:

        break
```

Anexo I: Código reconocimiento en python

```
reconocimiento.read("entrenamiento.yml")

etiquetas = {"nombre_persona": 1}
with open("labels.pickle", 'rb') as f:
    pre_etiquetas = pickle.load(f)
    etiquetas = {v: k for k, v in pre_etiquetas.items()}
con = 0

while True:
    for (x, y, w, h) in rostros:
        # print(x,y,w,h)
        roi_gray = filtro[y:y + h, x:x + w]
        roi_color = marco[y:y + h, x:x + w]

        # reconocimiento
        id_, conf = reconocimiento.predict(roi_gray)
        if conf >= 50 and conf < 80:
            # print(id_)
            # print(etiquetas[id_])
            font = cv2.FONT_HERSHEY_SIMPLEX

            nombre = etiquetas[id_]
            con + 1

            if conf > 80:
                # print(conf)
                nombre = "Desconocido"
```

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

DIRECCIÓN DE BIBLIOTECAS Y RECURSOS PARA EL APRENDIZAJE Y LA INVESTIGACIÓN

UNIDAD DE PROCESOS TÉCNICOS

REVISIÓN DE NORMAS TÉCNICAS, RESUMEN Y BIBLIOGRAFÍA

Fecha de entrega: 02/10/2020

INFORMACIÓN DEL AUTOR
Nombres – Apellidos: CRISTIAN ANDRÉS PAÑI PIZARRO
INFORMACIÓN INSTITUCIONAL
Facultad: INFORMÁTICA Y ELECTRÓNICA
Carrera: INGENIERÍA ELECTRÓNICA EN CONTROL Y REDES INDUSTRIALES
Título a optar: INGENIERO EN ELECTRÓNICA, CONTROL Y REDES INDUSTRIALES
f. Analista de Biblioteca responsable: