

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO



INSTITUTO TECNOLÓGICO
SUDAMERICANO
Hacemos gente de talento!



ELECTRÓNICA
TECNOLOGÍA SUPERIOR

TECNOLOGÍA SUPERIOR EN ELECTRÓNICA

SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE
INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS
EN EL PERIODO ABRIL – SEPTIEMBRE 2021

PROYECTO DE INVESTIGACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
TECNÓLOGO EN LA CARRERA DE
ELECTRÓNICA.

AUTOR:

Cristian Jhoel Ramón Ordóñez

DIRECTOR:

Ing. Manuel Asdrual Montaña Blacio

Loja, Octubre 2021

Certificación del director del Proyecto de Investigación de Fin de Carrera**Ing.**

Manuel Asdrual Montaña Blacio

DIRECTOR DE INVESTIGACIÓN**CERTIFICA:**

Que ha supervisado el presente proyecto de investigación titulado “**SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021**” el mismo que cumple con lo establecido por el Instituto Superior Tecnológico Sudamericano; por consiguiente, autorizo su presentación ante el tribunal respectivo.

Loja, 13 de octubre de 2021

.....

Firma**Ing. Manuel Asdrual Montaña Blacio**

Autoría

Yo CRISTIAN JHOEL RAMÓN ORDÓÑEZ C.I. N° 1900868157 declaro ser el autor del presente trabajo de tesis titulado SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021, es original e inédito, dejando establecido que aquellos aportes intelectuales de otros autores se han referenciado debidamente en el proyecto de investigación

Loja, 13 de octubre de 2021

.....

Firma

C.I. 1900868157

Dedicatoria

El presente trabajo lo dedico primeramente a Dios quien me ha dado la sabiduría y fortaleza, a mi familia, principalmente a mi madre que ha sido el pilar fundamental en mi formación como profesional, por brindarme la confianza, consejos, oportunidad y recursos para lograr uno de mis proyectos planteados en mi vida, a mi hermano por su apoyo y compañía, a mi abuelito, que aunque no esté físicamente con nosotros forma parte de los valores inculcados a mi vida para que todo me salga bien y a todos quienes compartieron sus conocimientos para que uno de mis sueños se haga realidad.

Cristian Jhoel Ramón Ordóñez

Agradecimiento

En primera instancia agradezco a Dios y al Instituto Superior Tecnológico Sudamericano por darme la oportunidad de continuar mis estudios superiores en tan prestigiosa institución.

De la misma manera agradezco al grupo de docentes que formaron parte fundamental en mi formación académica para lograr una de mis metas como profesional.

Agradezco también a mi tutor de tesis al Ing. Manuel Asdrual Montaña Blacio por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico, así como también haberme tenido toda la paciencia del mundo para guiarme durante todo el desarrollo de la tesis.

Cristian Jhoel Ramón Ordóñez

Acta de cesión de derechos

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

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

PRIMERA. - El Ing. Manuel Asdrual Montaña Blacio, por sus propios derechos, en calidad de director del proyecto de investigación de fin de carrera; y el señor Cristian Jhoel Ramón Ordóñez; mayor de edad, por sus propios derechos en calidad de autor del proyecto de investigación de fin de carrera; emiten la presente acta de cesión de derechos.

SEGUNDA. - Declaratoria de autoría y política institucional.

UNO. – Cristian Jhoel Ramón Ordóñez, realizó la Investigación titulada **“SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021”** para optar por el título de Tecnólogo en Electrónica, en el Instituto Superior Tecnológico Sudamericano de Loja, bajo la dirección del Ing. Manuel Asdrual Montaña Blacio.

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

TERCERA. - Los comparecientes Ing. Manuel Asdrual Montaña Blacio, en calidad de director del proyecto de investigación de fin de carrera y Cristian Jhoel Ramón Ordóñez como autor, por medio del presente instrumento, tienen a bien ceder en forma gratuita sus derechos en proyecto de investigación de fin de carrera titulada

“sistema de seguridad basado en técnicas de inteligencia artificial para el control de acceso a viviendas en el periodo abril – septiembre 2021” a favor del Instituto Superior Tecnológico Sudamericano de Loja; y, conceden autorización para que el Instituto pueda utilizar esta investigación en su beneficio y/o de la comunidad, sin reserva alguna.

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

Para constancia suscriben la presente cesión de derechos, en la ciudad de Loja, en el mes de marzo del año 2021.

F. _____

Ing. Manuel Asdrual Montaña Blacio

C.I. 0706440674

F. _____

Cristian Jhoel Ramón Ordóñez

C.I. 1900868157



Declaración juramentada

Loja, 13 de octubre de 2021

Nombres: Cristian Jhoel

Apellidos: Ramón Ordóñez

Cédula de Identidad: 1900868157

Carrera: Electrónica

Semestre de ejecución del proceso de titulación: Abril – Septiembre 2021

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

“SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021”

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

Declaro bajo juramento que:

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

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

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

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

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

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente dispuesta por la LOES y sus respectivos reglamentos y del Instituto Superior Tecnológico Sudamericano de la ciudad de Loja.

Firma

Nro. Cédula 1900868157

1. Índice de Contenido

1.1 Índice de temas

Certificación del director del Proyecto de Investigación de Fin de Carrera	II
Autoría.....	III
Dedicatoria	IV
Agradecimiento	V
Acta de cesión de derechos	VI
Declaración juramentada.....	VIII
1. Índice de Contenido	1
1.1 Índice de temas.....	1
1.2. Índice de Figuras.	6
1.3. Índice de Tablas.	7
2. Resumen.....	8
3. Abstract.	9
4. Problemática.....	10
5. Tema.....	12
6. Justificación.....	13
7. Objetivos	15
7.1. Objetivo general	15
7.2. Objetivos específicos.....	15
8. Marco Teórico.....	16

8.1. Marco Institucional.	16
8.2. Marco Conceptual.	24
8.2.1. Sistema de seguridad electrónico	24
8.2.2. Evolución de los sistemas de seguridad	24
8.2.2.1. Primera Generación.	25
8.2.2.2. Segunda Generación.	25
8.2.2.3. Tercera Generación.....	25
8.2.3. Control de acceso	26
8.2.4. Inteligencia Artificial	27
8.2.4.1 Ventajas.	27
8.2.4.2 Desventajas.	28
8.2.5. Técnica de Inteligencia Artificial: Detección de Rostros.....	29
8.2.5.1 Extracción de Características.....	29
8.2.5.2. Reconocimiento.	29
8.2.6 Visión por Computadora	30
8.2.6.1. Adquisición de imágenes.....	30
8.2.6.2. Procesamiento digital de imágenes.....	30
8.2.6.3 Segmentación.....	31
8.2.6.4. Extracción de características.....	31
8.2.6.5. Reconocimiento o clasificación.....	31
8.2.7. Aplicaciones de visión por computadora	32

	3
8.2.7.1. Automoción.....	32
8.2.7.2. Alimentación.....	32
8.2.7.3. Electrónica.....	32
8.2.8 Librería OpenCV.....	32
8.2.8.1. Estructura y Características.....	33
8.2.8.2. Interfaces gráficos y herramientas.....	33
8.2.9. Trabajos relacionados.....	34
9. Diseño Metodológico.....	36
9.1. Métodos de Investigación.....	36
9.1.1. Método hermenéutico.....	36
9.1.2. Método Fenomenológico.....	36
9.1.3. Método práctico proyectual.....	37
9.2. Técnicas de investigación.....	37
9.2.1. Investigación documental.....	37
9.2.2. Observación.....	38
9.2.3. Prueba y error.....	38
10. Propuesta de Acción.....	40
10.1. Software.....	40
10.1.1. Sistema Operativo Raspbian.....	40
10.1.2. Python.....	41
10.1.3. Librería Opencv.....	42

10.2. Hardware.....	43
10.2.1. Raspberry Pi 3 Modelo B+.....	43
10.2.2. Pi Camera OV5647.....	44
10.2.3. Módulo Relé modelo KY-019.....	45
10.2.4. Mini cerradura electromagnética 12V tipo solenoide.....	46
10.2.5. Alimentación Eléctrica.....	47
10.3 Desarrollo de la Propuesta de Acción.....	47
10.3.1. Diagrama de flujo.....	47
10.3.2. Captura de video.....	49
10.3.3. Entrenamiento.....	50
10.3.4. Reconocimiento.....	50
10.3.5. Diagrama electrónico.....	52
11. Pruebas del dispositivo.....	53
11.1. Pruebas del equipo.....	53
12. Conclusiones.....	54
13. Recomendaciones.....	55
14. Bibliografía.....	56
15. Anexos.....	59
15.1. Certificado de aprobación.....	59
15.2. Autorización para la ejecución.....	60
15.3. Certificado de implementación.....	61

15.4. Certificado de aprobación del Abstract.	62
15.5. Presupuesto.....	63
15.6. Cronograma de actividades.	64
15.7. Anexo 1 (Código para capturar el video).	65
15.8. Anexo 2 (Código entrenamiento).	66
15.9. Anexo 3 (Código reconocimiento facial).	67
15.10. Anexo 4 (Resultados obtenidos).	68
15.11. Anexo 5 (Sistema de control implementado).	69

1.2. Índice de Figuras.

Figura 1. Estructura de medelo educarivo.....	22
Figura 2. Sistema de Acceso	26
Figura 3. Interfaz del sistema operativo Raspbian	41
Figura 4. Interfaz del programa Thonny Python.....	42
Figura 5. Raspberry Pi 3 modelo b+	43
Figura 6. Pi Camera modelo OV5647.....	44
Figura 7. Modelo Relé modelo KY-019	45
Figura 8. Mini cerradura electromagnetica 12V tipo selenoide.....	46
Figura 9. Diagrama general del proyecto	47
Figura 10. Diagrama de flujo	48
Figura 11. Diagrama de flujo captura de video.....	49
Figura 12. Diagrama de flujo del entrenamiento	50
Figura 13. Diagrama de flujo reconocimiento facial	51
Figura 14. Diagrama electrónico.....	52
Figura 15. Código captura de video	65
Figura 16. Código entrenamiento.....	66
Figura 17. Código reconocimiento facial.....	67
Figura 18. Usuario 1 y 3.....	68
Figura 19. Usuario 1, 2 y 3.....	68
Figura 20. Usuario 2 y 4.....	69
Figura 21. Sistema de control implementado.....	69

1.3. Índice de Tablas.

Tabla 1. Pruebas de intentos realizados	53
Tabla 2. Presupuesto	63
Tabla 3. Cronograma de actividades	64

2. Resumen

Esta investigación se fundamenta en el desarrollo de un dispositivo electrónico para prevenir robo a viviendas en la ciudad de Loja y Zamora. El objetivo de la investigación es utilizar tarjetas de software y hardware libre una de ellas es la Raspberry Pi, el dispositivo ayuda mantener nuestras viviendas seguras evitando que personas extrañas pueda extraer nuestras pertenencias.

Para analizar la información obtenida se utilizaron 3 métodos de investigación el método hermenéutico, método fenomenológico y método práctico proyectual cada uno enfocado en el análisis de diferentes medios bibliográficos como artículos, libros, para la investigación necesaria del tema y así implementar el sistema con todos los parámetros propuestos a través de pruebas de campo donde se verificó su funcionamiento.

También, se hace uso de las técnicas de investigación documental, observación y prueba y error sirviendo cada una para recopilar información importante y con ello poder seleccionar los materiales necesarios para el proyecto, finalmente la técnica de prueba y error permitió realizar pruebas de campo para verificar la programación y conexiones para el funcionamiento final del dispositivo.

Con los resultados obtenidos, se concluye que el uso de la tecnología hoy en día evoluciona constantemente permitiendo realizar nuevos proyectos para diferentes usos importantes, una muestra de ello es el desarrollo de esta investigación. Se realizaron varias pruebas de funcionamiento con un máximo de 300 imágenes de 2 usuarios y con varias personas que no se encuentran en la base de datos dando una efectividad del 80%, con ello el dispositivo está listo para utilizarlo en las viviendas.

3. Abstract.

This research is based on the development of an electronic device to prevent theft from homes in the city of Loja and Zamora. The objective of the research is to use free software and hardware cards, one of them is the Raspberry Pi, the device that helps keep our homes safe preventing in this way that strangers steal our belongings.

To analyze the information obtained, three research methods were used: the hermeneutical method, phenomenological method, and practical project method, each one focused on the analysis of different bibliographic media such as articles, books for the necessary research on the subject and thus implement the system with all the parameters.

Moreover, techniques of documentary research, observation, trial, and error were used, each one is important to collect relevant information and in this way be able to select the necessary materials for the project, finally, the trial and error technique allowed to carry out field tests to verify programming and connections for the final operation of the device.

Finally, with the results obtained, it is concluded that the use of technology nowadays is constantly evolving allowing new projects to be carried out for different important uses, a sample is the development of this research. Several functional tests were carried out with a maximum of 300 images from 2 users and with several people who are not in the database, giving an effectiveness of 80%, with the device is ready for use in homes.

4. Problemática

La visión por computadora comprende el grupo de herramientas y procedimientos que permiten obtener, procesar y examinar imágenes del mundo real con el fin que logren ser tratadas por un ordenador. Esta clase de técnicas se aplican para la categorización de las imágenes o la toma de decisiones y, a grandes rasgos, se pueden dividir en dos tipos principales, que son las supervisadas y las no supervisadas. Las principales funciones son la detección de objetos y análisis de videos. Estas tecnologías se las puede utilizar en varios proyectos interesantes ante la sociedad, uno de ellos el reconocimientos de rostros, para la aplicación de detección de intrusos (Infaimon, 2018).

La inseguridad mundial no da tregua y esa percepción se ve reflejada, con los resultados de las encuestas realizadas a 150.000 personas de 142 países, en el año 2019, las que fueron consultadas para medir la percepción en términos de seguridad, dando como resultado a Singapur como líder en el ranking mundial como país más seguro del mundo, con un puntaje de 97 puntos, mientras que, los resultados de los países latinoamericanos son los siguientes: El Salvador obtuvo un puntaje de 73 puntos, el cual lideró con una ventaja de 10 puntos por encima del promedio regional que se ubicó en 63. Los países que registraron el menor puntaje de seguridad fueron México y Venezuela, con 60 y 49, por otro lado, Brasil, República Dominicana y Bolivia, con 62 puntos, en el top cinco de los países con menor problema de inseguridad, está Argentina y Perú, con 64 cada uno; y Nicaragua, con 67 puntos y completan el top 10: Colombia y Uruguay, con un puntaje de 67 cada uno, posicionándose en las casillas 113 y 112, respectivamente. (Aristizábal Bedoya, 2019).

En el Ecuador la delincuencia constantemente afecta a los ciudadanos, cada semana se difunden videos en redes sociales con imágenes de robos, así como de

delincuentes ingresando a viviendas. Los datos de la Policía Nacional reflejan que desde el 1 de enero hasta el 6 de noviembre del 2020 se registraron 9118 delitos en la capital, en el mismo periodo del año 2019 fueron 13222, lo cual implica una reducción del 31%. Esto ha sido posible porque la policía ha implementado varias estrategias para afrontar el problema, una de ellas es la presencia de uniformados en los puntos donde se han registrado varias denuncias, otra de las medidas, fue la instalación de 1237 alarmas comunitarias y la conformación de 200 comités de seguridad (Bravo, 2020).

En la provincia de Zamora Chinchipe, la policía nacional realizó varios operativos en los meses de enero a julio de 2020 dando como resultado 870 personas detenidas involucradas en diferentes delitos, en menor número aparece la aprensión de 26 personas por robo de domicilios (Ministerio de Gobierno, 2020).

En la ciudad de Loja los robos a domicilio son uno de los principales problemas delictivos que se suscitan en estos últimos meses, según el jefe distrital de la policía nacional existen grupos de individuos que se dedican a investigar y verificar las horas de salida de sus propietarios para posteriormente cometer el delito, la policía nacional recomienda a los ciudadanos cuando salgan de sus hogares, dirigirse a un UPC cercano y pedir el servicio de encargo a domicilio, donde los uniformados se responsabilizan del inmueble y monitorean de manera periódica (Diario La Hora, 2021)

5. Tema.

Sistema de seguridad basado en técnicas de inteligencia artificial para el control de acceso a viviendas en el periodo Abril – Septiembre 2021

6. Justificación

En la elaboración de la siguiente investigación como modelo académico, se realizará la construcción de un sistema de acceso a hogares, donde se va a poner en práctica todos los conocimientos adquiridos a lo largo del proceso de formación. Además, estos proyectos ayudarán a expandir el conocimiento, y poder adquirir nuevas habilidades mediante la investigación, permitiendo implementar nuevos elementos electrónicos más sencillos de usar como interruptores eléctricos, minicomputadoras y nuevos sistemas operativos que facilitara la construcción del prototipo. Además, el presente proyecto servirá para la obtención del título de tercer nivel en la tecnología superior en electrónica del Instituto Superior Tecnológico Sudamericano.

Otro punto de interés de este proyecto de titulación de fin de carrera, es la utilización de diferentes tecnologías que se han creado en los últimos años, una de ellas es la inteligencia artificial. Esta tecnología se puede utilizar para la creación de nuevos proyectos innovadores, en esta oportunidad se la va a combinar con interruptores eléctricos con el fin de solventar una problemática social que es la seguridad en los hogares, en la actualidad es necesario incorporar este tipo de seguridad con inteligencia artificial en las viviendas con la finalidad que los dueños se sientan más seguros.

Debido al aumento de inseguridad en el país y como medida preventiva, se propone implementar un sistema de control de acceso de los ciudadanos a los hogares, donde se va a utilizar técnicas de inteligencia artificial para controlar el acceso al hogar mediante una base de datos alojada en un sistema operativo, donde se podrá observar las personas que llegan a un domicilio. Para realizar el siguiente prototipo se va a ocupar materiales que se encuentran en el mercado nacional, los mismos serán de fácil

acceso y a un precio económico, una de las ventajas es que los materiales llegan al siguiente día en un buen estado listos para comenzar a trabajar en la construcción del mismo.

7. Objetivos

7.1. Objetivo general

Elaborar un sistema de seguridad utilizando técnicas de inteligencia artificial para el control de acceso a viviendas.

7.2. Objetivos específicos

- Realizar una investigación a través de fuentes bibliográficas confiables para determinar las técnicas que se adapten a la construcción del prototipo.
- Diseñar un dispositivo de control de acceso al hogar haciendo uso de inteligencia artificial para reconocimiento de rostros.
- Implementar el prototipo en una maqueta para las respectivas pruebas de funcionamiento y corroborar la eficacia del sistema.

8. Marco Teórico.

8.1. Marco Institucional.

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO



a. RESEÑA HISTÓRICA

El Señor Manuel Alfonso Manitio Conumba, crea el Instituto Técnico Superior Particular Sudamericano, para la formación de TECNICOS, por lo que se hace el trámite respectivo en el Ministerio de Educación y Cultura, y con fecha 4 de junio de 1996, autoriza con resolución Nro. 2403, la CREACIÓN y el FUNCIONAMIENTO de este Instituto Superior, con las especialidades del ciclo pos bachillerato de:

1. Contabilidad Bancaria
2. Administración de Empresas, y;
3. Análisis de Sistemas

Para el año lectivo 1996-1997, régimen costa y sierra, con dos secciones diurno y nocturno facultando otorgar el Título de Técnico Superior en las especialidades autorizadas.

Posteriormente, con resolución Nro. 4624 del 28 de noviembre de 1997, el Ministerio de Educación y Cultura, autoriza el funcionamiento del ciclo pos bachillerato, en las especialidades de:

1. Secretariado Ejecutivo Trilingüe, y;
2. Administración Bancaria.

Con resolución Nro. 971 del 21 de septiembre de 1999, resuelve el Ministerio de Educación y Cultura, elevar a la categoría de INSTITUTO TECNOLÓGICO SUPERIOR PARTICULAR SUDAMERICANO, con las especialidades de:

1. Administración Empresarial
2. Secretariado Ejecutivo Trilingüe
3. Finanzas y Banca, y;
4. Sistemas de Automatización

Con oficio circular nro. 002-DNPE-A del 3 de junio de 2000, la Dirección Provincial de Educación de Loja, hace conocer la nueva Ley de Educación Superior, publicada en el Registro Oficial, Nro. 77 del mes de junio de 2000, en el cual dispone que los Institutos Superiores Técnicos y Tecnológicos, que dependen del Ministerio de Educación y Cultura, forman parte directamente del “Sistema Nacional de Educación Superior” conforme lo determina en los artículos 23 y 24. Por lo tanto en el mes de noviembre de 2000, el Instituto Tecnológico Sudamericano de la ciudad de Loja, pasa a formar parte del Consejo Nacional de Educación Superior (CONESUP) con Registro Institucional Nro. 11-009 del 29 de noviembre de 2000.

A medida que avanza la demanda educativa el Instituto propone nuevas tecnologías, es así que con Acuerdo Nro. 160 del 17 de noviembre de 2003, la Dirección Ejecutiva del Consejo Nacional de Educación Superior (CONESUP) otorga licencia de funcionamiento en la carrera de:

1. Diseño Gráfico y Publicidad.

Para que conceda títulos de Técnico Superior con 122 créditos de estudios y a nivel Tecnológico con 185 créditos de estudios.

Finalmente, con Acuerdo Nro. 351 del 23 de noviembre de 2006, el Consejo Nacional de Educación Superior (CONESUP) acuerda otorgar licencia de funcionamiento para las tecnologías en las carreras de:

1. Gastronomía
2. Gestión Ambiental
3. Electrónica, y;
4. Administración Turística.

Otorgando los títulos de Tecnólogo en las carreras autorizadas, previo el cumplimiento de 185 créditos de estudio.

Posteriormente y a partir de la creación del Consejo de Educación Superior (CES) en el año 2008, el Tecnológico Sudamericano se somete a los mandatos de tal organismo y además de la Secretaría Nacional de Educación Superior, Ciencia y Tecnología (SENESCYT), del Consejo Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES); así como de sus organismos anexos.

Posterior al proceso de evaluación y acreditación dispuesto por el CEAACES; y, con Resolución Nro. 405-CEAACES-SE-12-2106, de fecha 18 de mayo del 2016 se otorga al Instituto Tecnológico Superior Sudamericano la categoría de “Acreditado” con una calificación del 91% de eficiencia.

Actualmente las autoridades del Instituto Tecnológico Superior Sudamericano se encuentran laborando en el proyecto de rediseño curricular de sus carreras con el fin de que se ajusten a las necesidades del mercado laboral y aporten al cambio de la Matriz Productiva de la Zona 7 y del Ecuador.

b. MISIÓN, VISIÓN y VALORES

Desde sus inicios la MISIÓN y VISIÓN, han sido el norte de esta institución y que detallamos a continuación:

MISIÓN:

“Formar gente de talento con calidad humana, académica, basada en principios y valores, cultivando pensamiento crítico, reflexivo e investigativo, para que comprendan que la vida es la búsqueda de un permanente aprendizaje”

VISIÓN:

“Ser el mejor Instituto Tecnológico del país, con una proyección internacional para entregar a la sociedad, hombres íntegros, profesionales excelentes, líderes en todos los campos, con espíritu emprendedor, con libertad de pensamiento y acción”

VALORES: Libertad, Responsabilidad, Disciplina, Constancia y estudio.

c. REFERENTES ACADÉMICOS

Todas las metas y objetivos de trabajo que desarrolla el Instituto Tecnológico Sudamericano se van cristalizando gracias al trabajo de un equipo humano: autoridades, planta administrativa, catedráticos, padres de familia y estudiantes; que día a día contribuyen con su experiencia y fuerte motivación de pro actividad para lograr las metas institucionales y personales en beneficio del desarrollo socio cultural y económico de la provincia y del país. Con todo este aporte mancomunado la familia sudamericana hace honor a su slogan “gente de talento hace gente de talento”.

Actualmente la Mgs. Ana Marcela Cordero Clavijo, es la Rectora titular; Ing. Patricio Villamarín coronel. - Vicerrector Académico.

El sistema de estudio en esta Institución es por semestre, por lo tanto, en cada semestre existe un incremento de estudiantes, el incremento es de un 10% al 15% esto es desde el 2005. Por lo general los estudiantes provienen especialmente del cantón Loja, pero también tenemos estudiantes de la provincia de Loja como: Cariamanga, Macará, Amaluza, Zumba, zapotillo, Catacocha y de otras provincias como: El Oro

(Machala), Zamora, la cobertura académica es para personas que residen en la Zona 7 del país.

d. POLÍTICAS INSTITUCIONALES

- Las políticas institucionales del Tecnológico Sudamericano atienden a ejes básicos contenidos en el proceso de mejoramiento de la calidad de la educación superior en el Ecuador.
- Esmero en la atención al estudiante: antes, durante y después de su preparación tecnológica puesto que él es el protagonista del progreso individual y colectivo de la sociedad.
- Preparación continua y eficiente de los docentes; así como definición de políticas contractuales y salariales que le otorguen estabilidad y por ende le faciliten dedicación de tiempo de calidad para atender su rol de educador.
- Asertividad en la gestión académica mediante un adecuado estudio y análisis de la realidad económica, productiva y tecnología del sur del país para la propuesta de carreras que generen solución a los problemas.
- Atención prioritaria al soporte académico con relevancia a la infraestructura y a la tecnología que permitan que docentes y alumnos disfruten de los procesos enseñanza – aprendizaje.
- Fomento de la investigación formativa como medio para determinar problemas sociales y proyectos que propongan soluciones a los mismos.
- Trabajo efectivo en la administración y gestión de la institución enmarcado en lo contenido en las leyes y reglamentos que rigen en el país en lo concerniente a educación y a otros ámbitos legales que le competen.

- Desarrollo de proyectos de vinculación con la colectividad y preservación del medio ambiente; como compromiso de la búsqueda de mejores formas de vida para sectores vulnerables y ambientales.

e. OBJETIVOS INSTITUCIONALES

Los objetivos del Tecnológico Sudamericano tienen estrecha y lógica relación con las políticas institucionales, ellos enfatizan en las estrategias y mecanismos pertinentes:

- Atender los requerimientos, necesidades, actitudes y aptitudes del estudiante mediante la aplicación de procesos de enseñanza – aprendizaje en apego estricto a la pedagogía, didáctica y psicología que dé lugar a generar gente de talento.
- Seleccionar, capacitar, actualizar y motivar a los docentes para que su labor llegue hacia el estudiante; por medio de la fijación legal y justa de políticas contractuales.
- Determinar procesos asertivos en cuanto a la gestión académica en donde se descarte la improvisación, los intereses personales frente a la propuesta de nuevas carreras, así como de sus contenidos curriculares.
- Adecuar y adquirir periódicamente infraestructura física y equipos tecnológicos en versiones actualizadas de manera que el estudiante domine las TIC'S que le sean de utilidad en el sector productivo.
- Priorizar la investigación y estudio de mercados; por parte de docentes y estudiantes aplicando métodos y técnicas científicamente comprobados que permitan generar trabajo y productividad.
- Planear, organizar, ejecutar y evaluar la administración y gestión institucional en el marco legal que rige para el Ecuador y para la educación superior

en particular, de manera que su gestión sea el pilar fundamental para lograr la misión y visión.

- Diseñar proyectos de vinculación con la colectividad y de preservación del medio ambiente partiendo del análisis de la realidad de sectores vulnerables y en riesgo de manera que el Tecnológico Sudamericano se inmiscuya con pertinencia social.

ESTRUCTURA DEL MODELO EDUCATIVO Y PEDAGÓGICO DEL INSTITUTO TECNOLÓGICO SUPERIOR SUDAMERICANO

Figura 1

Estructura de modelo educativo.



Imagen tomada de: https://tecnologicosudamericano.edu.ec/media/Modelo-Educativo_001.jpg

f. PLAN ESTRATÉGICO DE DESARROLLO

El Instituto Tecnológico Superior Sudamericano cuenta con un plan de desarrollo y crecimiento institucional trazado desde el 2016 al 2020; el cual enfoca puntos centrales de atención:

- Optimización de la gestión administrativa
- Optimización de recursos económicos
- Excelencia y carrera docente

- Desarrollo de investigación a través de su modelo educativo que implica proyectos y productos integradores para que el alumno desarrolle: el saber ser, el saber y el saber hacer
- Ejecución de programas de vinculación con la colectividad
- Velar en todo momento por el bienestar estudiantil a través de: seguro estudiantil, programas de becas, programas de créditos educativos internos, impulso académico y curricular
- Utilizar la TIC`S como herramienta prioritaria para el avance tecnológico
- Automatizar sistemas para operativizar y agilizar procedimientos
- Adquirir equipo, mobiliario, insumos, herramientas, modernizar laboratorios a fin de que los estudiantes obtengan un aprendizaje significativo
- Rendir cuentas a los organismos de control como CES, SENESCYT, CEAACES, SNIESE, SEGURO SOCIAL, SRI, Ministerio de Relaciones Laborales; CONADIS, docentes, estudiantes, padres de familia y la sociedad en general
- Adquirir el terreno para la edificación de un edificio propio y moderno hasta finales del año dos mil quince.

La presente información es obtenida de los archivos originales que reposan en esta dependencia. (Instituto Tecnológico Superior Sudamericano, 2013)

Tlga. Carla Sabrina Benítez Torres

SECRETARIA DEL INSTITUTO SUDAMERICANO

8.2. Marco Conceptual.

8.2.1. Sistema de seguridad electrónico

Un sistema de seguridad electrónico es la interconexión de recursos, redes y dispositivos cuyo objetivo es proteger la integridad de las personas y su entorno, previniéndolas de probables riesgos y presiones externas. Las primordiales funcionalidades de un sistema de seguridad electrónico son: la detección de intrusos en el interior y exterior, el control de accesos y tráfico (personas, paquetes, correspondencia, vehículos, etc.), la vigilancia remota por medio de circuito cerrado de televisión (CCTV), detección de incendio. Asimismo, los sistemas de seguridad no únicamente sirven para proteger a los bienes, inmuebles y las personas, sino también ahorran tiempo y dinero en los procesos domésticos e industriales, al gestionar el desempeño y prevención de fallas en los mismos (Camara Nacional de Comercio y Servicios del Uruguay, 2017).

Un sistema de seguridad consta de componentes de software, hardware, dispositivos periféricos y equipo de control que van a ser controlados por un operador de seguridad. Los diseños tienen la tarea de determinar el software y hardware que se adecue a las necesidades de los consumidores. Todos los accesorios físicos están controlados por programas de aplicación, dichos programas tienen la posibilidad de implicar la utilización de una base de datos, la asignación de ciertos límites de gestión a los operadores y crear un control definido por los sensores de ambiente (Lezama, 2001).

8.2.2. Evolución de los sistemas de seguridad

Los sistemas de seguridad fueron evolucionando acorde se van desarrollando novedosas tecnologías y los usuarios exigen mejores soluciones a sus inconvenientes, con un menor tiempo de respuesta, con mayor eficiencia y con un mínimo de fallas.

Los sistemas se separan en generaciones para lograr clasificar su operatividad, esto garantizará al usuario la fiabilidad de que se cumplirá sus requerimientos con las ultimas noticias tecnologías (Lezama, 2001).

8.2.2.1. Primera Generación. La primera generación se limitaba solamente a la utilización de un dispositivo capaz de ofrecer aviso de cualquier violación y un medio que lo controlara; por ejemplo, se contaba tan solo con una alarma que emitía una señal sonora una vez que existía una interrupción en el esquema que poseía definido. El control frecuentemente era manual y el usuario debía ingresar claves o parámetros para definir que la situación que se iba a exponer era todo normal (Lezama, 2001).

8.2.2.2. Segunda Generación. La segunda generación ya consistía de un medio capaz de mantener el control de los eventos y que también podía tomar elecciones según el caso. Esto permitió que el usuario dejara de hacer eventos manuales y que además redujera el número de falsas alarmas, puesto que los dispositivos eran capaces de interpretar una situación y conceptualizar si en verdad era una situación de alarma o sencillamente una situación poco común (Lezama, 2001).

8.2.2.3. Tercera Generación. En la tercera generación, ya se implementó un medio para lograr monitorear todos los eventos que se realicen en un lugar sin que el usuario tenga que estar en la misma ubicación. Esto da flexibilidad al usuario para que paralelamente ejecute diferentes ocupaciones y puedan estar revisando el estado en que se encuentra la organización o su hogar. Además, un sistema que monitoree actividades puede llevar una bitácora de los eventos hechos a lo largo de un periodo de tiempo lo cual permiten definir situaciones de riesgo o determinar ciertas acciones que mejoren el manejo del sistema (Lezama, 2001).

8.2.3. Control de acceso

Un sistema de control de acceso se instala con el fin de autorizar la entrada a definido lugar a los individuos anteriormente autorizados y denegarlos a las que no tienen permiso de ingresar. Indudablemente a la vez que se autoriza o no el acceso a una persona particular, también puede delimitarse los horarios autorizados a ingresar al recinto (Cámara Nacional de Comercio y Servicios del Uruguay, 2017).

Los sistemas más simples, son la utilización de tarjeta de proximidad o magnética en vez de una llave para desbloquear una puerta de acceso. Esta función básica sigue siendo una de las más usadas por las organizaciones. Según la función de los paneles controladores, se puede sectorizar la empresa en zonas controladas en donde ingresan los empleados en general y zonas restringidas, como puede ser por ejemplo el área de administración y tesorería (Cámara Nacional de Comercio y Servicios del Uruguay, 2017).

Figura 2

Sistema de Acceso.



Imagen tomada de:

https://www.tecnoseguro.com/media/k2/items/cache/37a06e4a72d6cb27621f1ed829bbee81_XL.jpg

8.2.4. Inteligencia Artificial

Es la función de una máquina o sistema informática de imitar en cierta forma la conducta de la mente humana desarrollando habilidades que hasta hace poco solo estaban al alcance del cerebro humano, como la creatividad o el estudio complejo con base de datos incompletos. Se fundamenta en procesos que integran el aprendizaje, el entendimiento y la autocorrección (Tablado, 2020).

Aun cuando puede que a varios el concepto de inteligencia artificial todavía le suene a ciencia ficción, lo cierto es que ya está presente en varios entornos de la sociedad y su uso y desarrollo no deja de crecer; está se encuentra en los asistentes de voz, en los procesos de selección de candidatos, se emplea en la salud y la sanidad, en la exploración del Big Data, en los videojuegos, en los vehículos autónomos, etc. (Tablado, 2020).

Sus fines se fundamenta primordialmente en la construcción de sistemas profesionales capaces de desarrollar un comportamiento inteligente y la utilización de la inteligencia en las máquinas. Con inteligencia hacemos referencia a la sabiduría humana que incluye resolución de inconvenientes, aprendizaje y razonamiento. Tras un pequeño resumen de qué es la inteligencia artificial, vamos a ver cuáles son sus ventajas y desventajas (Transformación Digital, 2020).

8.2.4.1 Ventajas. La inteligencia artificial en los últimos años es muy utilizada por ello se da a conocer las diferentes ventajas de la inteligencia artificial las cuales son las siguientes (Transformación Digital, 2020):

- Automatización de procesos. Los robots son capaces de reproducir labores repetitivas y pensar más veloz que los humanos.
- Minimiza el error humano. Se disminuye los fallos que tenemos la posibilidad de tener los humanos gracias a nuestras propias

restricciones. Es más, la inteligencia artificial fue y es empleada para lograr identificar errores que tienen la posibilidad de ser indetectables para nuestros propios ojos. Las máquinas son más exactas.

- Mantenimiento predictivo. Por medio de la inteligencia artificial tenemos la posibilidad de hacer un mantenimiento predictivo de un equipo industrial, logrando aumentar su rendimiento y periodo de vida.
- Minimiza el tiempo de estudio de datos. Posibilita que este logro hacerse en tiempo real.
- Optimización en la toma de elecciones. Tienen la posibilidad de tomarse superiores elecciones al contar con una información mejor organizada.

8.2.4.2 Desventajas. Así como la inteligencia artificial tiene buenas ventajas también tiene sus desventajas las cuales son (Transformación Digital, 2020):

- Costo y tiempo de utilización. El gasto en inteligencia artificial es bastante alto al tratarse de aparatos complicadas con un elevado coste en mantenimiento y compostura.
- Falta de cualificación. Para lograr implantar proyectos de inteligencia artificial debería contarse con expertos que se encuentran familiarizados con la materia.
- Crecimiento de desempleo. La sustitución de humanos por máquinas está llevando a bastantes personas al desempleo a gran escala.
- Ausencia de moral. Es cierto que la efectividad es más grande, sin embargo, no son humanos, carecen de sentimientos, lo cual algunas veces podría ser inseguro debido a que no conocen ni una barrera moral.

- No existe la creatividad. Las máquinas no consideran, trabajan bajo límites, por lo cual la capacidad innovadora permanece ausente.

8.2.5. Técnica de Inteligencia Artificial: Detección de Rostros

La detección facial o rostros es el proceso de hallar una cara en imágenes o clip de videos. El algoritmo de detección de caras está basado en una funcionalidad que busca zonas rectangulares en una imagen, zonas que contengan objetos que con una alta posibilidad se parezcan a otros de un grupo de entrenamiento, devolviendo la zona rectangular de la imagen donde se han encontrado. La función consiste en escanear algunas veces la imagen y con diferentes escalas para hallar objetos parecido, pero en diferentes tamaños (Martínez Pérez & Linares Pellicer, 2012).

8.2.5.1 Extracción de Características. La extracción de propiedades tiene relación con la obtención de características o parámetros particulares de cada rostro para después poder ser clasificados. Tienen la posibilidad de tomar tres enfoques diferentes: 1) un enfoque holístico, basándose en la imagen del rostro como un todo, 2) un enfoque por medio de propiedades locales, dando mayor importancia a las diversas partes del rostro, o 3) un enfoque híbrido con base en la iniciativa de que el sistema de percepción humana combina características locales y globales para el reconocimiento (Valvert, 2006).

8.2.5.2. Reconocimiento. El reconocimiento se apoya en clasificar cada una de las propiedades extraídas de cada rostro. Esta categorización podría ser hecha de forma supervisada, en la cual un patrón de acceso es reconocido como integrante de una clase predefinida, o de forma no supervisada, donde el patrón es asignado a una clase desconocida. Aquí, cada clase es un individuo, por consiguiente, al clasificar las propiedades se está indicando a que sujeto pertenece (Valvert, 2006).

8.2.6 Visión por Computadora

El sector de visión por computadora busca explicar el mundo que vemos en imágenes y rehacer sus características como, por ejemplo: forma, iluminación y distribuciones de color. Para José Valdez, los sistemas desarrollados en visión por computadora, busca actuar con base a representaciones de una realidad, las cuales otorgan datos acerca de brillo, colores, formas (Miranda et al., 2018)

El reconocimiento de colores, formas y detección de propiedades, representan tareas increíblemente fáciles de llevar a cabo para humanos y animales; pero la implementación y emulación en sistemas automatizados genera grandes desafíos para investigadores del área. Tradicionalmente, la investigación en visión por computadora fue aplicada al sector industrial en los campos de: interacción de máquinas y su entorno, control de calidad en productos fabricados (Miranda et al., 2018).

Para entender cómo funciona la visión por computadora, se presentan las partes presentes que conforman un sistema de visión por computadora (SVC). Según el estado del arte, en lo que se refiere a SVC se puede determinar un marco general de procesos consecutivos que siguen la gran mayoría de los autores (Miranda et al., 2018).

8.2.6.1. Adquisición de imágenes. La adquisición de la imagen está al mando de cualquier transductor o grupo de transductores que por medio de la manipulación de la luz o de alguna otra forma de radiación que es emitida o reflejada por los cuerpos, se consigue conformar una representación del objeto dando sitio a la imagen, por ejemplo: el ojo humano, sensores de una cámara fotográfica o de vídeo, tomógrafos (Escalante, 2006).

8.2.6.2. Procesamiento digital de imágenes. El procesamiento digital de imágenes ha adquirido, en años actuales, un papel fundamental en las tecnologías de

la información y el cómputo. En la actualidad, es la base de una creciente variedad de aplicaciones que integran diagnóstico médica, percepción remota, investigación espacial, visión por computadora, etc. Como consecuencia directa de la reducción en el costo de las computadoras, el procesamiento digital de imágenes en la actualidad se puede hacer (aunque con ciertas limitantes) en una computadora personal (Torres, 1996)

8.2.6.3 Segmentación. Por medio de la segmentación se va a dividir la imagen en las partes u objetos que la conforman. El nivel al que se hace esta subdivisión es dependiente de la aplicación en especial, es decir, la segmentación terminara una vez que se hayan detectado todos los objetos de interés para la aplicación. Generalmente, la segmentación automática es una de las labores más complejas dentro del procesado de imagen. La segmentación va a ofrecer lugar en última instancia al éxito o fallo el proceso de análisis (Martín, 2002).

8.2.6.4. Extracción de características. La extracción de características en imágenes y secuencias de imágenes faciales, se apoya en extraer información vinculada con la activación de los diferentes músculos del rostro, esta tarea puede desarrollarse en forma universal u holística en donde se examina el rostro como un solo conjunto o localmente en donde se seleccionan zonas de interés del rostro como ojos cejas y boca (Castrillon et al., 2008).

8.2.6.5. Reconocimiento o clasificación. La finalidad de la categorización es destinar un objeto cuya clase de pertenencia es desconocida a una que haga parte de la base de entendimiento del sistema, teniendo presente los límites previamente ajustados en el clasificador. Así se recibe una métrica que define la clase asignada al objeto en cuestión. Se asignará el objeto a la clase cuya neurona de salida haya obtenido el costo mayor en la capacidad de activación (Velez et al., 2009)

8.2.7. Aplicaciones de visión por computadora

8.2.7.1. Automoción. En la zona de la automoción la utilización de sistemas de visión artificial en las industrias se corresponde primordialmente con las inspecciones en la construcción y el ensamblaje de cada una de las partes de los nuevos sistemas de seguridad. Además, se debe considerar que labores como la inspección de estampación, mecanizado, pintura y rebabas dependen directamente de grupos de visión artificial que supervisan todo el proceso (Infaimon, 2018).

8.2.7.2. Alimentación. La visión artificial industrial es un factor importante en el control de calidad de los productos alimentarios, en especial en las etapas finales. Tanto la selección de frutas como el adecuado cierre de las latas de conservación, o la preparación de productos cárnicos procesados, dependen directamente de sistemas de visión artificial que supervisan el desarrollo en cada una de sus etapas (Infaimon, 2018).

8.2.7.3. Electrónica. La zona de la electrónica pertenece a los que más se favorece del uso de la visión artificial industrial en sus procesos de construcción. La manipulación e identificación de los diversos elementos corren a su cuenta. La visión artificial tiene la función de verificar de manera eficiente la adecuada soldadura y ensamblaje de partes (Infaimon, 2018).

8.2.8 Librería OpenCV

El 13 de Junio del 2000, Intel Corporation hizo saber al mundo que estaba haciendo un trabajo con un grupo de reconocidos investigadores en visión por computador para hacer una totalmente nueva librería de estructuras/funciones en lenguaje C. Esta librería proporcionaría un marco de trabajo de grado medio-alto que ayudaría al personal docente e investigador a desarrollar novedosas maneras de interactuar con los ordenadores (Arévalo et al., 2004).

8.2.8.1. Estructura y Características. La librería OpenCV está dirigida prácticamente a la visión por computador en tiempo real. Entre sus muchas superficies de aplicación destacarían: relación hombre-máquina; segmentación y reconocimiento de objetos; reconocimiento de gestos; seguimiento del desplazamiento; composición del desplazamiento; y robots móviles, otorga varios recursos de alto nivel, que facilitan sobre forma el trabajo al cliente. Por ejemplo, proporciona filtros Microsoft® DirectShow para hacer labores tales como: calibración de la cámara, seguidores de objetos (Kalman tracker y ConDensation tracker), etc. Todos ellos tienen la posibilidad de usar en Microsoft GraphEdit para ilustrar de manera bastante fácil varias aplicaciones de visión (Arévalo et al., 2004).

8.2.8.2. Interfaces gráficos y herramientas. La librería OpenCV da diversos paquetes de alto nivel para el desarrollo de aplicaciones de visión. Todos ellos tienen la posibilidad de agrupar en librerías de C/C++ dirigidas a usuarios avanzados y en herramientas de scripting dirigidas, en esta situación, a usuarios de grado medio (ideal para entrenar con las diferentes técnicas de procesamiento de imágenes y visión). Al primer conjunto pertenecen HighGUI y CvCam, mientras que al segundo pertenecen Hawk y OpenCV Toolbox para Matlab (Arévalo et al., 2004).

HighGUI posibilita la escritura/lectura de imágenes en varios formatos (BMP, JPEG, TIFF, Pxm, SunRaster, etc.) y la captura de stream de video de capturadoras Matrox® y cámaras/capturadoras con drivers VFW/WDM (la mayor parte del mercado); la construcción de ventanas para visualizar imágenes en ellas, las ventanas HighGUI recuerdan su contenido (no se necesita llevar a cabo callbacks de repintado); y, además, nos otorga mecanismos bastante sencillos de interaccionar con ellas: trackbars, capturando el ingreso del teclado y el ratón (Arévalo et al., 2004).

CvCam nos da un exclusivo interfaz de captura y reproducción bajo Linux y Win32; callbacks para la administración de stream de vídeo o ficheros AVI y un mecanismo simple para llevar a cabo visión estéreo con dos cámaras USB o una estéreo-cámara. Hawk es un ámbito visual con el intérprete ANSI C EiC como núcleo; aguanta plugins; otorga soporte para OpenCV, IPL y HighGUI vía plugin; y soporte de video (Arévalo et al., 2004).

8.2.9. Trabajos relacionados

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

Un estudiante de la carrera de Ingeniería Eléctrica y Electrónica de la Universidad San Francisco de Quito, planteó crear un diseño e implementación de un sistema embebido de reconocimiento facial para el control de acceso usando deep learning el cual utiliza un procesador Neural Compute Stick 2. El sistema está basado en un código de reconocimiento facial desarrollado en el lenguaje de programación Python, mismo que, por medio de una cámara web, recibe las imágenes en tiempo real para realizar una comparación con los rostros guardados en una base de datos (Orna Villalta, 2019).

En la ciudad de Ibarra los estudiantes de la carrera de ingeniería en sistemas y computación de la Pontificia Universidad Católica del Ecuador, crearon un sistema de control de acceso haciendo uso de las redes neuronales artificiales para el reconocimiento facial de manera rápida a través de la extracción de propiedades tomadas de la imagen del rostro. La utilización del sistema incluye el desarrollo utilizando herramientas de hardware libre para la automatización del sistema de control de ingreso. El sistema desarrollado ha sido implantado en una organización en la ciudad de Ibarra, Ecuador, obteniéndose resultados favorables y que permiten el registro y control de ingreso a los empleados y visitantes (Ibarra-Estévez & Paredes, 2018).

Los estudiantes de la Universidad Politécnica Salesiana construyeron un prototipo para el control de accesos usando un sistema de reconocimiento facial, con esto se garantizará un nivel alto de seguridad para que los usuarios logren entrar a un definido lugar en cualquier instante, relacionando la utilización de los sistemas biométricos convencionales y prevenir cualquier tipo de vulneración. Para eso pretenda diseñar un sistema que haga uso del reconocimiento de rostros de los usuarios usando algoritmos inteligentes, los cuales se verán implementados en un programa que trabajará en conjunto con el dispositivo LattePanda, en vista a que es una tarjeta de elevado rendimiento el cual soportará toda clase de procesos a emplearse (Nacipucha Nacipucha & Frías Pérez, 2020).

9. Diseño Metodológico.

9.1. Métodos de Investigación.

9.1.1. Método hermenéutico

Hans Georg Gadamer 1995 afirma:

Que la hermenéutica, indica no únicamente el método de algunas ciencias, o el problema de una recta interpretación de lo comprendido, sino que se refiere al ideal de un conocimiento exacto y objetivo, siendo la comprensión el carácter ontológico originario de la vida humana que deja su impresión en todas las relaciones del hombre con el mundo, pues el comprender no es una de las posibles actitudes del sujeto, sino el modo de ser de la realidad como tal.

El método hermenéutico el cual ayudó a conformar un estudio completo de diferentes medios bibliográficos como son páginas web, artículos, libros, guías y varias tesis que tenga interacción al tema que se investiga, así obteniendo un pensamiento más claro en la utilización de sistemas electrónicos. Siguiendo con la selección y compra de los componentes electrónicos que se va a ocupar, analizando cada uno de ellos.

9.1.2. Método Fenomenológico

Rodríguez 2003 afirma:

Que la fenomenología de Husserl supone la necesidad de esta búsqueda razonada de la verdad; llevado por tal interés señala la obligatoriedad de mantener la actitud de ir a las cosas mismas. Actitud antes que método, porque se trata de una máxima de ética profesional filosófica y científica que nos impide a estar atentos a la donación de sentido, lo cual se trata del intento de ofrecer verdadera razón de lo real, pareciera extraña la existencia de muchos puntos de partida de las filosofías.

Aplicando el método fenomenológico se logró entender y evidenciar como las personas toman medidas de precaución para proteger sus viviendas, en sí, la mayoría no disponen de un sistema de seguridad de sus domicilios, esto puede ser por el alto costo que hoy en día se venden dichos sistemas, por lo que se pretende diseñar un dispositivo de bajo costo que se pueda adaptar a la vida cotidiana de las personas.

9.1.3. Método práctico proyectual

Munari 2010 afirma:

Que la metodología proyectual de Gui Bonsiepe se adecua al quehacer de diseñador gráfico frente al proceso de diseño y todo lo cual implica su desarrollo, a pesar de que por momentos la metodología se inclina hacia el diseño industrial, como aclara su creador, la metodología no se rige por pasos secuenciales y terminales, al contrario, el proceso de diseño se reformula.

El método práctico proyectual, consistió en la implementación de un sistema de seguridad para viviendas que mediante nuestro rostro se abra una puerta, el cual se va a implementar en una maqueta para realizar y analizar las pruebas de campo respectivas donde se verificará el funcionamiento del sistema de seguridad implementado, confirmando que cumpla los objetivos planteados y proceso adecuado del mismo.

9.2. Técnicas de investigación.

9.2.1. Investigación documental

La investigación documental de la misma forma que se la define, constituye una secuencia de procedimiento y técnicas que los trabajadores en información descubrieron y perfeccionaron durante la historia con el propósito de ofrecer

información a la sociedad, esa información se la encuentra en las bibliotecas (Tancara, 1993).

Esta técnica se utilizó para recopilar y seleccionar información precisa de diferentes artículos y páginas web, para la construcción del sistema de seguridad, además para seleccionar de manera precisa los diferentes materiales, componentes electrónicos a ocupar en el desarrollo del proyecto.

9.2.2. Observación

La observación por sí misma representa una de las maneras más sistematizadas y lógicas para el registro visual y verificable de lo cual se pretende conocer, consiste en utilizar los sentidos ya sea para explicar, examinar, o describir a partir de una perspectiva científica, válida y confiable de algún hecho, objeto o fenómeno (Campos & Martínez, 2012)

Se propuso utilizar esta técnica aplicando la observación directa en el campo de investigación para obtener las primeras respectivas a la problemática a resolver, recoger datos relevantes y sobre todo verificar los posibles escenarios para la implementación del sistema.

9.2.3. Prueba y error

Prueba y error es una metodología de obtención de conocimiento, reparación o solución de problemas en la cual se prueba una probabilidad y después se comprueba si sirve o no. En el caso de que el resultado no sea el deseado, se intenta con una nueva alternativa, y de esta forma, hasta obtener un resultado positivo (Enciclopedia Online, 2018).

La técnica de prueba y error se la aplicó para realizar las diversas conexiones electrónicas y programación. Para realizar la programación se necesita concentración, amplios conocimientos y excelente habilidad en la manipulación de componentes

electrónicos, logrando así un sistema idóneo para poner a prueba. Esto se comprueba a través de la interacción del sistema y un miembro de la familia en sus pruebas de campo.

10. Propuesta de Acción.

En la presente sección se evidencia la solución para abordar la problemática planteada, que versa en la creación de un sistema de seguridad para control de acceso a viviendas, indicando con el análisis de los materiales a utilizar tanto en software y hardware.

10.1. Software.

En este apartado se describe todo lo relacionado con los programas que se usan para llevar a cabo la programación del sistema de seguridad.

10.1.1. Sistema Operativo Raspbian

Sistema operativo que utiliza la Raspberry Pi, para su funcionamiento se aloja en una tarjeta micro SD para realizar las configuraciones de instalación y proceder con el funcionamiento. Es uno de los sistemas operativos más utilizados para tarjetas Raspberry Pi en todas sus distribuciones (Víctor & HackLab, 2016).

Existen tres versiones de sistema operativo; versión completa la cual ocupa 4GB de almacenamiento, además incluye un software recomendado preinstalado, la versión estándar no requiere de mucho almacenamiento, tiene incluido un escritorio gráfico y la versión lite es más ligera, pero hay que tomar en cuenta que solo tiene el sistema operativo sin escritorio gráfico.

Para la creación del prototipo se ocupa la versión estándar, porque cuenta con una escritorio o interfaz gráfica intuitiva y fácil de usar. Permite la configuración gráfica del idioma, seguridad, nombre del equipo y conectividad a redes, en la Figura 3 se puede visualizar como es el escritorio del sistema operativo Raspbian una vez instalado.

Figura 3

Interfaz del sistema operativo Raspbian.

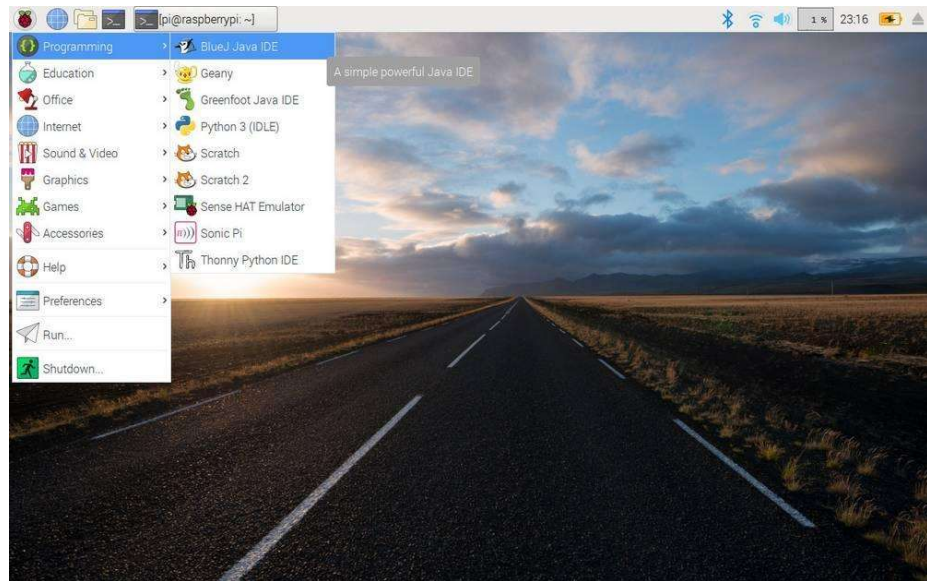


Imagen tomada de: <https://www.softzone.es/app/uploads-softzone.es/2020/01/Raspbian.jpg>

10.1.2. Python

Python es un lenguaje, simple, claro y fácil por su sintaxis; el tipado dinámico, el gestor de memoria, la gran proporción de librerías disponibles y la potencia del lenguaje, entre otros, hacen que desarrollar una aplicación en Python sea sencillo, muy eficaz, lo cual es más relevante. (González Duque, 2014). En la tarjeta Raspberry Pi tiene preinstalado un editor de códigos llamado Thonny Python el mismo es una nueva IDE de programación más sencilla para principiantes donde es fácil crear nuevos proyectos, entre sus características se destacan las diferentes formas de recorrer el código, la evaluación paso a paso de la expresión y un modo para explicar los conceptos de referencias, en la figura 4 se observa como es la interfaz del programa Thonny Python.

Figura 4

Interfaz del programa Thonny Python.

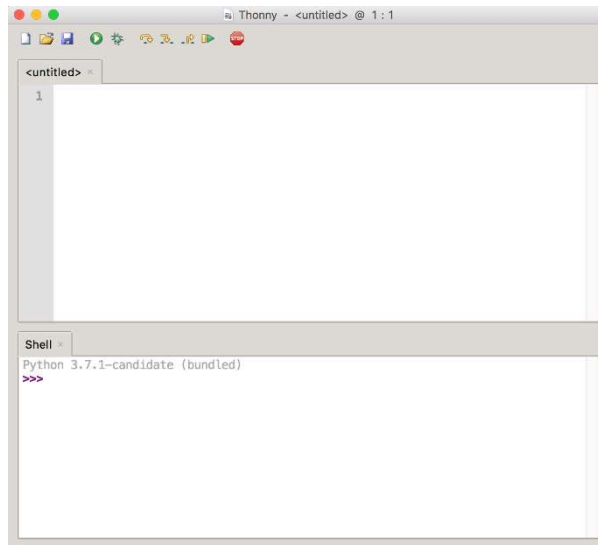


Imagen tomada de: https://files.realpython.com/media/Screenshot_2018-10-20_11.03.57.d46d970db1e6.png

10.1.3. Librería Opencv

Es una librería de software libre y gratuita, puesto que se distribuye bajo licencia BSD (Berkeley Software Distribution), que permite sea utilizada libremente en varios proyectos con propósitos comerciales y de investigación, siempre y cuando, cumpla con las condiciones de la licencia, está optimizada para ser usada bajo procesadores Intel, sin embargo, puede ser utilizada bajo cualquier otro tipo de procesadores y puede tomar más recursos de procesadores multinúcleo. Las librerías OpenCV tienen la posibilidad de instalarse tanto bajo Linux como bajo Windows (Viera Maza, 2017).

La librería de opencv permite identificar múltiples características de objetos, personas y animales. Con el uso de esta herramienta y característica específica para identificación de rostros permite discernir entre personas que estén alojadas en una base de datos, se utiliza la versión 4.1.0. para Raspberry.

10.2. Hardware.

En este apartado se da conocer todos los materiales de la parte física que se usan para el armado del sistema de seguridad por control de acceso.

10.2.1. Raspberry Pi 3 Modelo B+

Es una placa electrónica que se basa en el concepto de hardware libre, existen varios tipos y modelos de Raspberry Pi, en esta oportunidad se habla de la Raspberry Pi 3 modelo b+, se alimenta con 5v, tiene 40 pines los cuales 24 pines son GPIO, cuenta con un conector CSI (Interfaz Serie para Cámaras) para cámara, entre otras características (Rodríguez, 2018)

Para el desarrollo del prototipo la Raspberry Pi se la utiliza como el controlador del sistema, donde va almacenar la información y procesar, dicha información se la obtiene de la cámara, se envía los datos directamente a la pantalla donde se puede observar en tiempo real lo que la cámara está captando, en la Figura 5 se muestra la arquitectura física de la raspberry pi modelo b+ y también detalla las partes que posee.

Figura 5

Raspberry Pi 3 modelo b+.

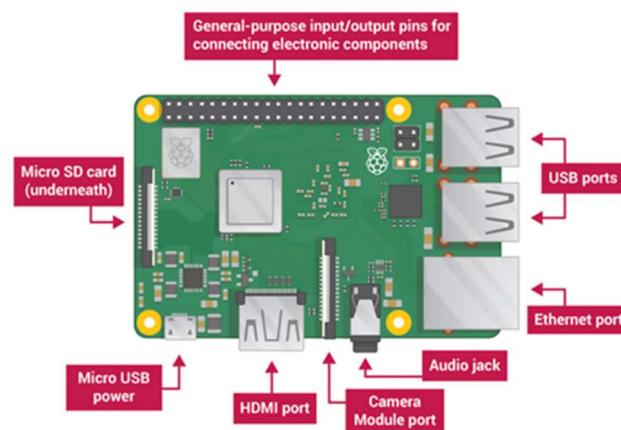


Imagen tomada de: <http://canaltic.com/blog/wp-content/uploads/2020/07/raspi004.png>

10.2.2. Pi Camera OV5647

Es un módulo oficial de Raspberry lanzado en 2016, cuenta con un sensor IMX219 de Sony con 5 y 8 megapíxeles, es capaz de tomar fotografías y grabar videos a altas resoluciones(1080p) pero sacrificando fps (30 FPS), sin embargo, si se graba a una resolución más baja ganamos más FPS (720p a 60 FPS, 480p a 60/90 FPS), es compatible con cualquier modelo de Raspberry Pi y cuenta con varias bibliotecas de terceros que han sido creadas para ella, una de las más importantes es la biblioteca PiCamera Python (Dioniz Rodríguez, 2020).

Para capturar las imágenes se usa la cámara de 5 mega píxeles de resolución nativa de alta calidad con lente fijo, también se puede utilizar este tipo de cámara en la noche, se conecta a través de interfaz dedicada CSI (Interfaz Serie para Cámaras), por su CSI es más rápida la transferencia de imágenes con respecto a una webcam convencional, en la Figura 6 se puede evidenciar como es la Pi camera.

Figura 6

Pi Camera modelo OV5647.

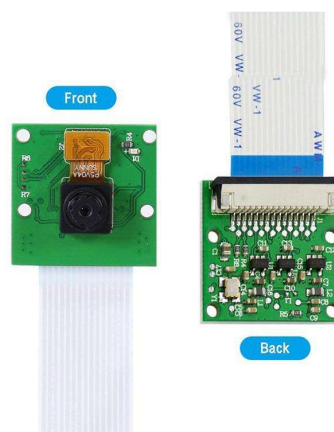


Imagen tomada de:

https://img.joomcdn.net/86d06a5558d1f7bf5303f8abcb6811a1672116da_original.jpg

10.2.3. Módulo Relé modelo KY-019

El relé es un dispositivo para gestionar voltajes y corrientes como los que se encuentran en la red eléctrica, se trata sencillamente de un interruptor eléctrico que puede encender y apagar enviando señales a partir de una placa Arduino o cualquier otro controlador similar (Procerquisa, 2016).

El módulo relé está compuesto de una Resistencia de $1M\Omega$, un LED, un diodo rectificador (1N4007) y un relé de 5VDC capaz de manejar arriba de 250 VAC y 10A, en el lado de la corriente continua de la placa, hay 3 pines para señal, voltaje y tierra, en el lado de la corriente alterna existen 3 conectores, NC (normalmente cerrado), Común y NO (normalmente abierto.)

El relé se ocupa para la activación de la cerradura eléctrica, el mismo que estará activo para mantener la puerta cerrada, cuando la persona que va ingresar al domicilio es autorizada por el sistema de reconocimiento de rostros este le permitirá ingresar, se desactivará el relé y se abre la puerta, en la Figura 7 se muestra una imagen de cómo está constituido el módulo relé.

Figura 7

Módulo Relé modelo KY-019.



Imagen tomada de: https://uelectronics.com/wp-content/uploads/2017/06/AR0037_KY019_V5.jpg

10.2.4. Mini cerradura electromagnética 12V tipo solenoide

La cerradura electromagnética se usa como medio de apertura en lugares donde el ingreso debe ser limitado (control de acceso). El ejemplo más claro es una empresa, donde la recepcionista, frente al ruido del timbre contesta; y si la persona que se encuentra en la entrada puede recibir el permiso para ingresar, entra en juego este dispositivo de apertura de puertas (Ramos Fernández, 2018).

Esta cerradura eléctrica tipo solenoide tiene un diseño delgado que da seguridad y estabilidad en su uso, es de bajo consumo y es bastante eficaz para cerrar donde se necesite; es simple de instalar, por ejemplo, para un sistema de cierre automático de alguna puerta. Este solenoide tiene un lingote con un corte inclinado, normalmente está con bloqueo activo para que no se pueda abrir la puerta (por lo que el lingote está expandido) y no utiliza ningún voltaje en este estado. Una vez que se aplica voltaje el lingote se contrae para que no sobresalga más y la puerta se pueda abrir de forma fácil, en el proyecto se la utilizó para poder abrir la puerta automáticamente, en la Figura 8 se presenta como se compone la cerradura electromagnética.

Figura 8

Mini cerradura electromagnética 12V tipo solenoide.

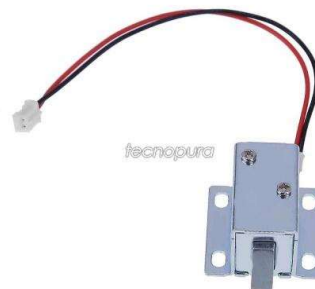


Imagen tomada de: <http://www.tecnopura.com/wp-content/uploads/mini-cerradura-electromagnetica-12v-tipo-solenoid-0.jpg>

10.2.5. Alimentación Eléctrica

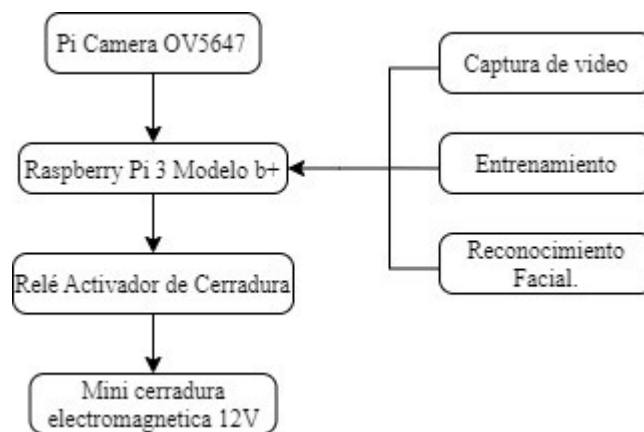
Se utilizan dos fuentes de alimentación la de 5V_{DC} para encender la Raspberry y un adaptador de 110V_{AC} a 12V_{DC} para el control de la cerradura electromagnética, se separan las fuentes debido a que el control de la cerradura utiliza mayor corriente.

10.3 Desarrollo de la Propuesta de Acción.

En este apartado se da a conocer todos los procesos que se lleva a cabo para la elaboración final del prototipo, para proceder con sus pruebas respectivas y obtener resultados, en la Figura 9 se muestra el diagrama general de la construcción de todo el proyecto.

Figura 9

Diagrama general del proyecto.



A continuación, se describe el diagrama de flujo del programa desarrollado usando el software Python con el editor Thonny Python.

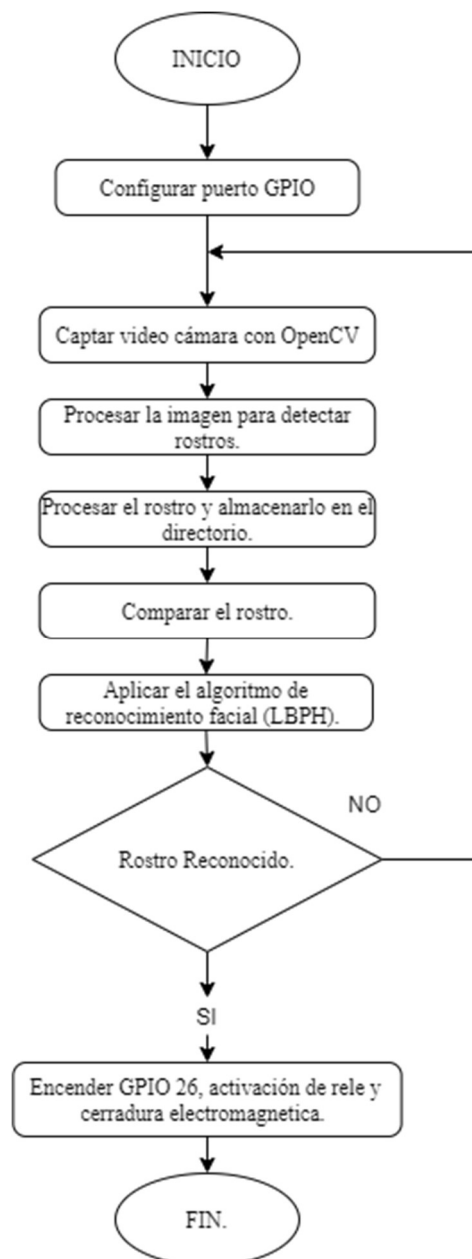
10.3.1. Diagrama de flujo

El control inicia con la configuración de los puertos GPIO para el acceso de la Raspberry Pi a la cámara, cuando se inicia el programa la librería opencv lee las imágenes captadas de la cámara, para procesar (detectar, recortar, cambiar tamaño, ecualizar, etc) una imagen primero debe detectar un rostro, un rostro valido es cuando detecta correctamente una cara de persona, se almacena en el directorio creado para comparar los rostros transformados en histogramas con el algoritmo de

reconocimiento facial LBPH, cuando detecta un rostro que se encuentra almacenada en el directorio, se activa el relé enviando el pulso a la cerradura electromagnética para abrir, caso contrario cuando detecta un rostro desconocido el relé no se accionará y se repetirá todo el procedimiento hasta que detecte un rostro válido, en la figura 10 se observa el diagrama general del control.

Figura 10

Diagrama de flujo.

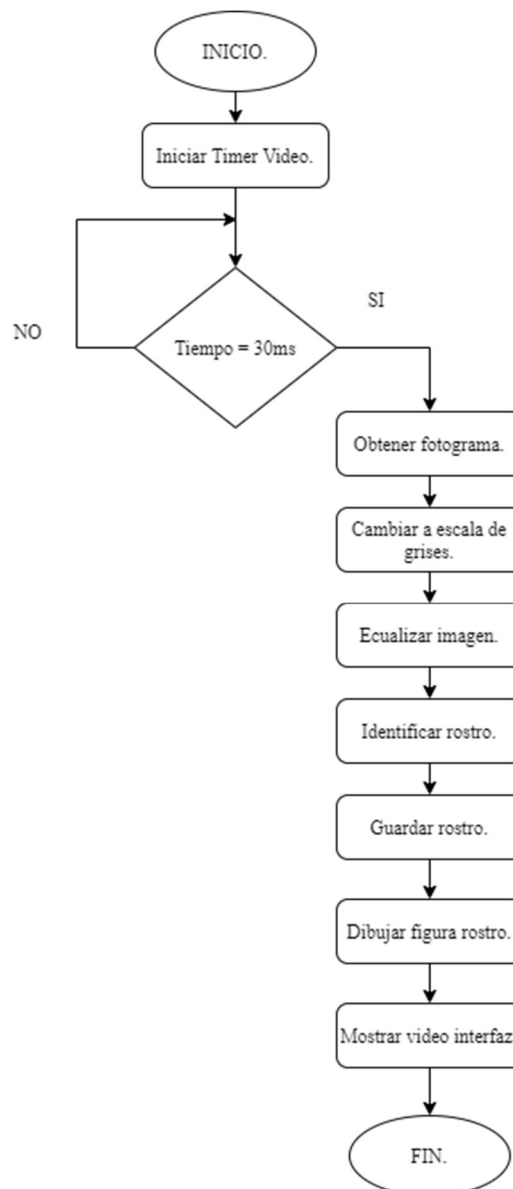


10.3.2. Captura de video

Se enciende el control de acceso e inmediatamente comienza a grabar el video, cada 30 fps (fotogramas por segundo) obtiene un fotograma, el cual debe ser cambiado a escala de grises porque los clasificadores que reconocen los rasgos trabajan exclusivamente a escala de grises, para luego ir ecualizando e ir identificando los rasgos de cada trama, en la Figura 11 se muestra el diagrama de flujo de la captura de video, referirse a los Anexo 1 donde se muestra el código.

Figura 11

Diagrama de flujo captura de video.

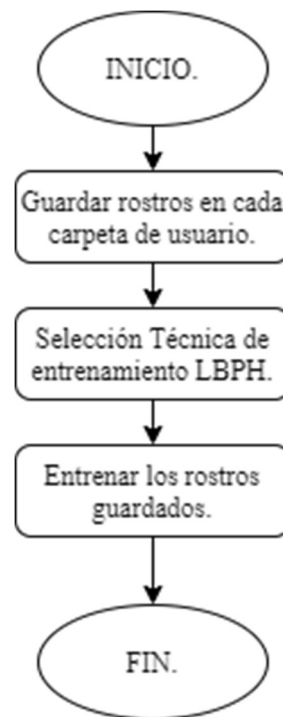


10.3.3. Entrenamiento

Esta función entrena todos los rostros almacenados de cada usuario, después de guardar cada rostro valido en las carpetas de cada usuario se selecciona la técnica de entrenamiento LBPH, cuando se aplica el algoritmo de entrenamiento todo queda almacenado en la memoria de la Raspberry Pi y queda todo listo para su uso, en la Figura 12 se puede observar el diagrama de flujo del entrenamiento, en el apartado de Anexo 2 se muestra el código que se utilizó para entrenar el sistema.

Figura 12

Diagrama de flujo del entrenamiento.



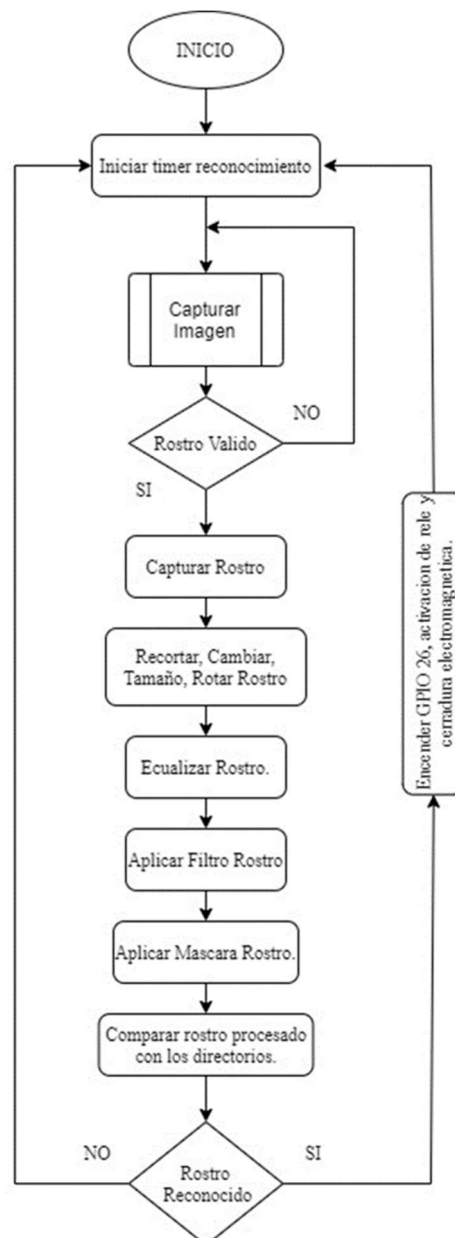
10.3.4. Reconocimiento

La librería OpenCV cuenta con una clase para utilizar el algoritmo de reconocimiento facial LBPH (patrones locales binarios), el reconocimiento comienza con un tiempo de espera para capturar imágenes y verificar si existe un rostro valido, cuando no encuentra un rostro vuelve a capturar imágenes, caso contrario prosigue con el siguiente paso que es el procedimiento de imágenes que ya se explicó en el

punto 10.3.1, luego el algoritmo compara el rostro procesado, cuando el rostro capturado no se encuentra en la base de datos creada anteriormente la puerta se mantiene cerrada, si el rostro captado es reconocido por el sistema automáticamente se abre la puerta de la vivienda, en la Figura 13 se muestra el diagrama de flujo del reconocimiento, en el apartado de Anexo 3 se observa el código que se utilizó para el funcionamiento del reconocimiento facial.

Figura 13

Diagrama de flujo reconocimiento facial.

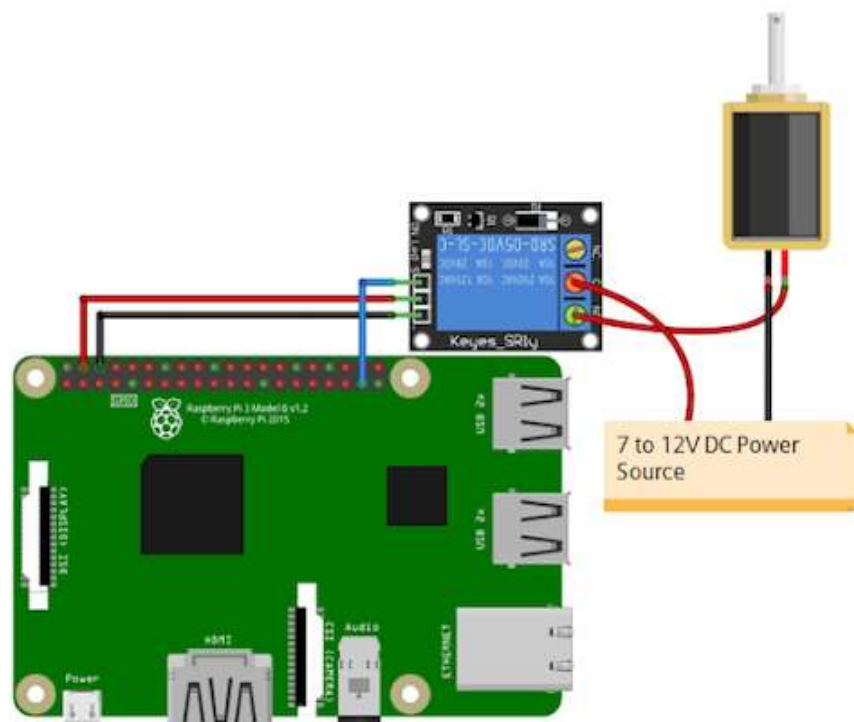


10.3.5. Diagrama electrónico

En la Figura 14 se muestra el diagrama electrónico del circuito proyecto, primero se conecta la alimentación al puerto micro USB para la Raspberry Pi, segundo se conecta la cámara en el conector CSI que tiene la tarjeta, tercero se conecta un relé en la parte de corriente continua la señal se conecta al puerto GPIO 26, el positivo a un puerto de 5 voltios, el negativo a un puerto GND de la tarjeta, de la parte de corriente alterna se conecta un cargador de 12 V_{DC} al común del relé, finalmente el positivo de la cerradura electromagnética se conecta al NO (normalmente abierto) del relé y el negativo de la cerradura se conecta al GND del cargador.

Figura 14

Diagrama electrónico.



11. Pruebas del dispositivo.

11.1. Pruebas del equipo.

Para realizar las respectivas pruebas del equipo se registraron dos usuarios dentro del control de acceso, estas personas son madre e hijo que van hacer el ingreso a la vivienda, tomando en cuenta que “SI” es uno lógico y “NO” es cero lógicos, en la Tabla 1 se puede observar los intentos realizados y los aciertos obtenidos de cada usuario.

Tabla 1

Pruebas de intentos realizados.

USUARIOS.	INTENTOS.			
	1	2	3	4
1	SI	SI	SI	SI
2	SI	SI	SI	SI
USUARIOS QUE NO SE ENCUENTRAN EL LA BASE DE DATOS.				
3(D)	SI	SI	SI	SI
4(D)	NO	NO	NO	NO

Los resultados de los intentos para ingresar a la vivienda fueron satisfactorios con un porcentaje del 80%, cada uno de los usuarios tiene archivado 300 fotos en la memoria de las Raspberry Pi, también se realizaron intentos de ingresos con personas que no están registradas en la tarjeta.

En la parte de las pruebas realizadas con desconocidos el usuario 3 tiene un aparecido con el usuario 1, en cambio con el usuario 4 no lo reconoce lo detecta como desconocido y no le permite el acceso, con el usuario 1 y 2 los reconoce sin ningún problema dando el acceso al hogar, en el Anexo 4 se explica los resultados obtenidos.

12. Conclusiones.

- Se utilizó la tarjeta Raspberry Pi 3 para el desarrollo del proyecto por sus características relacionadas a visión artificial ya que tiene mejores ventajas como codificación de video, CPU, procesador y cumple con las especificaciones a nivel de hardware y software, además de capacidades para implementación de algoritmos de procesamiento digital de imágenes.
- Se utilizó el algoritmo LBPH (patrones binarios locales) porque este algoritmo es más robusto con respecto a otros con reconocimiento facial ante cambios de iluminación porque dentro de sus capacidades esta la identificación de los ojos, nariz y boca, ecualización de los niveles de gris, para posteriormente guardar las imágenes en las carpetas de cada usuario, cabe destacar que el reconocimiento al usuario es más rápido y con menos errores.
- Se realizaron las respectivas pruebas de funcionamiento con varios intentos de acceso, con el que se obtuvo un porcentaje del 80% identificando rostros, el usuario 1 y 2 tiene 300 imágenes cada uno guardadas en la tarjeta, también se realizaron pruebas con otras personas que no se encuentran registradas en el sistema la cual no permite el acceso pero cabe destacar que el hermano del usuario 1 lo detecta como si fuera el, con estos resultados se observa que el dispositivo está listo para uso en las viviendas.

13. Recomendaciones.

- En la investigación de artículos confiables también se encontró que se puede implementar los algoritmos Eigenface o Fisherface y realizar una comparación con el algoritmo LBPH, para determinar cuál de los algoritmos es más eficiente.
- Si se desea incrementar el almacenamiento para crear un directorio con una gran cantidad de usuarios se recomienda utilizar una tarjeta micro SD de clase 10 de 32 gigabits de almacenamiento, ya que en la tarjeta se instala el sistema operativo y se guardan las imágenes de los rostros.
- Al momento de realizar las pruebas de funcionamiento tomar en cuenta la iluminación del lugar, cuando el dispositivo se encuentra con poca luz no detecta ningún rostro, cabe destacar cuando el prototipo funcione en la noche el mismo debe tener iluminación extra.

14. Bibliografía.

- Arévalo, V., González, J., & Ambrosio, G. (2004). La Librería de Visión Artificial OpenCV. Aplicación a la Docencia e Investigación. *Base Informática*, 40, 61–66.
- Aristizábal Bedoya, M. P. (2019). Venezuela y México son los primeros países latinoamericanos en el índice de inseguridad. *La Republica*.
- Bravo, D. (2020). La estadística señala menos delitos, pero la inseguridad no cede. *El Comercio*.
- Camara Nacional de Comercio y Servicios del Uruguay. (2017). *Sistema Seguridad Electrónico*.
- Campos, G., & Martínez, N. E. L. (2012). La observación, un método para el estudio de la realidad. *Xihmai*, 7(13), 45–60.
- Castrillon, W. A., Alvarez, D. A., & López, A. F. (2008). Técnicas de extracción de características en imágenes para el reconocimiento de expresiones faciales. *Scientia et Technica*, 14(38), 7–12.
- Diario La Hora. (2021). *Robos a domicilios, el delito mas frecuente en Loja*.
<https://www.pressreader.com/ecuador/la-hora-loja/20210624/281479279381812>
- Enciclopedia Online. (2018). *Prueba y error | Qué es, Definición y Concepto*.
<https://enciclopediaonline.com/es/ensayo-y-error/>
- Escalante, B. (2006). *Procesamiento Digital de Imágenes*. http://lapi.fi-p.unam.mx/wp-content/uploads/PDI_Cap1_Introduccion.pdf
- Ibarra-Estévez, J., & Paredes, K. (2018). Redes neuronales artificiales para el control de acceso basado en reconocimiento facial. *Revistapuce*.
<http://www.revistapuce.edu.ec/index.php/revpuce/article/view/140>

- Infaimon. (2018). *Visión por computador: qué es y cuáles son sus usos más comunes*.
<https://blog.infaimon.com/vision-computador-soluciones-permite/>
- Lezama, L. (2001). *Modelado de dispositivos para un sistema de seguridad implementado tecnología Jini*.
http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/lezama_1_a/capitulo1.pdf
- Martínez Pérez, J. V., & Linares Pellicer, J. J. (2012). Sistema de reconocimiento facial y realidad aumentada para dispositivos móviles. *3c Tic, 1*, 7–16.
- Martin, M. (2002). *Técnicas clásicas de segmentación de imagen*.
<http://www.kramirez.net/wp-content/uploads/2012/05/segmenclasica.pdf>
- Ministerio de Gobierno. (2020). *Cuatro delitos en Zamora no reportan detenidos*.
<https://www.ministeriodegobierno.gob.ec/cuatro-delitos-en-zamora-no-reportan-detenidos/>
- Miranda, J. C., Luis, J., Noguera, V., & Gonzalez, L. (2018). *CLASIFICACIÓN AUTOMÁTICA DE NARANJAS POR TAMAÑO Y POR DEFECTOS UTILIZANDO TÉCNICAS DE VISIÓN POR COMPUTADORA*.
<https://www.researchgate.net/publication/326551993>
- Moreno Latorre, J. P. (2016). *Prototipo para el control de una cerradura electrónica por medio de reconocimiento facial*.
<https://repository.udistrital.edu.co/handle/11349/4687>
- Nacipucha Nacipucha, C. A., & Frías Pérez, J. J. (2020). *Diseño de un Prototipo de Control de Acceso a través de Reconocimiento Facial Mediante la Creación de un Algoritmo Basado en Software Libre Utilizando lattepanda*.
<https://dspace.ups.edu.ec/handle/123456789/19626>
- Orna Villalta, G. D. (2019). *Diseño e implementación de un sistema embebido de reconocimiento facial para el control de acceso usando deep learning*. Quito.

<https://repositorio.usfq.edu.ec/handle/23000/8862>

Tablado, F. (2020). *Inteligencia artificial: Definición, tipos y aplicaciones*.

<https://protecciondatos-lopdd.com/empresas/inteligencia-artificial/>

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

Torres, A. D. (1996). Procesamiento digital de imágenes. *Perfiles Educativos*, 72.

<https://www.redalyc.org/pdf/132/13207206.pdf>

Transformación Digital. (2020). *Ventajas y desventajas de la Inteligencia Artificial*.

<https://www.winecta.com/ventajas-desventajas-inteligencia-artificial/>

Valvert, J. R. (2006). Métodos y técnicas de reconocimiento de rostros en imágenes digitales bidimensionales. *Final Project, Universidad de San Carlos de Guatemala*.

Velez, N., Erazo, J., & Loaiza, H. (2009). Sistema de clasificación de imágenes basado en técnicas de reconocimiento de patrones aplicado en termografía y robótica. *El Hombre y La Máquina*, 33, 45–52.

<http://www.redalyc.org/articulo.oa?id=47812225005>

Dioniz Rodríguez, A. (2020). *Transmisión digital con cámara óptica para comunicaciones VLC basada en Raspberry Pi*.

González Duque, R. (2014). *Python para todos*. N/A.

Procerquisa. (2016). Tutorial 14: Uso de Relé. *Curso de Arduino*, 3.

Ramos Fernandez, P. (2018). *Sistema de control de llave digital con raspberry PI 3*.

Rodriguez, E. (2018). *Raspberry Pi: todo lo necesario para iniciarse como maker desde cero*.

Víctor, S. G., & HackLab, A. (2016). *Introducción a Raspberry Pi*. Obtenido de <http://hacklabalmeria.net/recursos/intropi.pdf>.

Viera Maza, G. I. (2017). *Procesamiento de imágenes usando OpenCV*.

15. Anexos.

15.1. Certificado de aprobación.

VICERRECTORADO ACADÉMICO



Loja, 06 de julio del 2021

Of. N° 131-V-ISTS-2021

Sr. Ramón Ordóñez Cristian Jhoel
ESTUDIANTE DE LA CARRERA DE ELECTRÓNICA DEL ISTS

Ciudad

De mi consideración:

Por medio de la presente me dirijo a ustedes para comunicarles que una vez revisado el proyecto de investigación de fin de carrera de su autoría titulado **“SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021”**, el mismo cumple con los lineamientos establecidos por la institución; por lo que se autoriza su realización y puesta en marcha, para lo cual se nombra como director de su proyecto de fin de carrera (el/la) Ing. Manuel Asdrual Montaña Blacio.

Particular que le hago conocer para los fines pertinentes.

Atentamente,

Ing. Germán Patricio Villamarín Coronel Mgs.



VICERRECTOR ACADEMICO DEL ISTS
c/c. Estudiante, Archivo

15.2. Autorización para la ejecución



INSTITUTO TECNOLÓGICO
SUDAMERICANO
Hacemos gente de talento!



ELECTRÓNICA
TECNOLOGÍA SUPERIOR

Yo, Ing. Oscar Geovanny Jiménez con documento de identidad 1103571590, coordinador de la carrera de Electrónica del Instituto Superior Tecnológico Sudamericano de la ciudad de Loja a petición verbal del interesado.

AUTORIZO

A Cristian Jhoel Ramón Ordóñez con cedula de identidad Nro. 1900868157, estudiantes del sexto ciclo de la carrera de Electrónica del “Instituto Superior Tecnológico Sudamericano”; para que realicen su proyecto de investigación de fin de carrera titulado: “SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021” para lo cual nos comprometemos en entregar a los estudiantes la información necesaria hasta que culmine dicho proceso.

Loja, 13 de septiembre del 2021

Ing. Oscar Jiménez

C.I. 1103571590

15.3. Certificado de implementación



INSTITUTO TECNOLÓGICO
SUDAMERICANO
Hacemos gente de talento!



ELECTRÓNICA
TECNOLOGÍA SUPERIOR

Loja, 13 de octubre del 2021

Ing. Manuel Asdrual Montaña Blacio

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

CERTIFICO

Que el Sr Cristian Jhoel Ramón Ordóñez con cédula 1900868157 han venido trabajando en el Proyecto de fin de carrera titulado “SISTEMA DE SEGURIDAD BASADO EN TÉCNICAS DE INTELIGENCIA ARTIFICIAL PARA EL CONTROL DE ACCESO A VIVIENDAS EN EL PERIODO ABRIL – SEPTIEMBRE 2021”; el mismo que se encuentra a la presente fecha en un 100% culminado según los requerimientos funcionales planteados. Lo certifico en honor a la verdad para los fines pertinentes y a solicitud del interesado.

Ing. Manuel Asdrual Montaña Blacio

TUTOR SEMINARIO DE PROYECTOS DE INVESTIGACIÓN DE FIN DE CARRERA

15.4. Certificado de aprobación del Abstract.



CERTF. N° 006-JG-ISTS-2021
Loja, 05 de Octubre de 2021

*El suscrito, Lic. Jordy Christian Granda Feijoo, Mgs., **COORDINADOR-DOCENTE DEL ÁREA DE INGLÉS - CIS DEL INSTITUTO SUPERIOR TECNOLÓGICO "SUDAMERICANO"**, a petición de la parte interesada y en forma legal,*

C E R T I F I C A:

*Que el apartado **ABSTRACT** del Proyecto de Investigación de Fin de Carrera del señor RAMON ORDOÑEZ CRISTIAN JHOEL estudiante en proceso de titulación periodo Abril - Noviembre 2021 de la carrera de ELECTRÓNICA; está correctamente traducido, luego de haber ejecutado las correcciones emitidas por mi persona; por cuanto se autoriza la presentación dentro del empastado final previo a la disertación del proyecto.*

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

English is a piece of cake!

Lic. Jordy Christian Granda Feijoo, Mgs.
COORDINADOR-DOCENTE DEL ÁREA DE INGLÉS ISTS - CIS



Checked by:

Lic. Jordy Christian Granda Feijoo, Mgs.
ENGLISH TEACHER

15.5. Presupuesto.

El presente proyecto de investigación tiene un presupuesto, de los materiales a utilizar en el mercado del mercado nacional.

Tabla 2.

Presupuesto.

PRESUPUESTO			
Material	Precio unitario	Unidades	valor total
Raspberry Pi3 Modelo B+	74.80	1	74.80
Cámara 5MPX 1080p	12.40	1	12.40
Módulo relé 1 Canal 5V	2.90	1	2.90
Cargador 110V/12V a 1A	5.15	1	5.15
Cerradura Eléctrica con Solenoide 12v	12.00	1	12.00
Construcción de maqueta	60.00	1	60.00
Varios	20.00	1	20.00
Total, presupuesto			187.25

15.7. Anexo 1 (Código para capturar el video).

Figura 15

Código para capturar el video.

```
import cv2
import os
import imutils
import picamera

with picamera.PiCamera() as picam:
    picam = picamera
    picam.resolution = (480, 480)
    picam.framerate = 30

personName = 'Fanny Ordoñez'
dataPath = '/home/pi/Prueba/imagenes'#Cambia a la ruta donde hayas almacenado Data
personPath = dataPath + '/' + personName

if not os.path.exists(personPath):
    print('Carpeta creada: ',personPath)
    os.makedirs(personPath)

picam = cv2.VideoCapture(0)
faceClassif = cv2.CascadeClassifier(cv2.data.haarcascades+'haarcascade_frontalface_default.xml')
count = 0
while True:
    ret, frame =picam.read()
    if ret == False: break
    rame = imutils.resize(frame, width=640)
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    auxFrame = frame.copy()
    faces = faceClassif.detectMultiScale(gray,1.3,5)
    for (x,y,w,h) in faces:
        cv2.rectangle(frame, (x,y), (x+w,y+h), (0,255,0),2)
        rostro = auxFrame[y:y+h,x:x+w]
        rostro = cv2.resize(rostro, (150,150),interpolation=cv2.INTER_CUBIC)
        cv2.imwrite(personPath + '/rostro_{}.jpg'.format(count),rostro)
        count = count + 1
    cv2.imshow('frame',frame)
    k = cv2.waitKey(1)
    if k == 27 or count >= 300:
        break

picam.release()
cv2.destroyAllWindows()
```

15.8. Anexo 2 (Código entrenamiento).

Figura 16

Código entrenamiento.

```
import cv2
import os
import numpy as np

dataPath = '/home/pi/Prueba/imagenes'#Cambia a la ruta donde hayas almacenado Data
peopleList = os.listdir(dataPath)
print('Lista de personas: ', peopleList)

labels = []
facesData = []
label = 0

for nameDir in peopleList:
    personPath = dataPath + '/' + nameDir
    print('Leyendo las imágenes')

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

face_recognizer = cv2.face.LBPHFaceRecognizer_create()
# Entrenando el reconocedor de rostros
print("Entrenando...")
face_recognizer.train(facesData, np.array(labels))
# Almacenando el modelo obtenido
face_recognizer.write('modeloLBPHFace.xml')
print("Modelo almacenado...")
```

15.9. Anexo 3 (Código reconocimiento facial).

Figura 17

Código reconocimiento facial.

```
import cv2
import os
import picamera
import RPi.GPIO as GPIO

relay_pin = 26
GPIO.setmode(GPIO.BCM)
GPIO.setup(relay_pin, GPIO.OUT)
GPIO.output(relay_pin, 0)

with picamera.PiCamera() as picam:
    picam = picamera
    picam.resolution = (480, 480)
    picam.framerate = 30

dataPath = '/home/pi/Prueba/imagenes' #Cambia a la ruta donde hayas
almacenado Data imagePaths = os.listdir(dataPath)
print('imagePaths=', imagePaths)

face_recognizer = cv2.face.LBPHFaceRecognizer_create()

# Leyendo el modelo
face_recognizer.read('modeloLBPHFace.xml')

picam = cv2.VideoCapture(0)

faceClassif = cv2.CascadeClassifier(cv2.data.harcascades+'haarcascade_frontalface_default.xml')

while True:
    ret, frame = picam.read()
    if ret == False: break
    gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
    auxFrame = gray.copy()

    faces = faceClassif.detectMultiScale(gray, 1.3, 5)

    for (x,y,w,h) in faces:
        rostro = auxFrame[y:y+h,x:x+w]
        rostro = cv2.resize(rostro, (150,150), interpolation= cv2.INTER_CUBIC)
        result = face_recognizer.predict(rostro)
        print(result)
        if result[1] < 75:
            GPIO.output(relay_pin, 1)
            cv2.putText(frame, '{}'.format(imagePaths[result[0]]), (x,y-25), 2, 1.1, (0,255,0), 1, cv2.LINE_AA)
            cv2.rectangle(frame, (x,y), (x+w,y+h), (0,255,0), 2)
        else:
            GPIO.output(relay_pin, 0)
            cv2.putText(frame, 'Desconocido', (x,y-20), 2, 0.8, (0,0,255), 1, cv2.LINE_AA)
            cv2.rectangle(frame, (x,y), (x+w,y+h), (0,0,255), 2)

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

    if k == 27:
        break

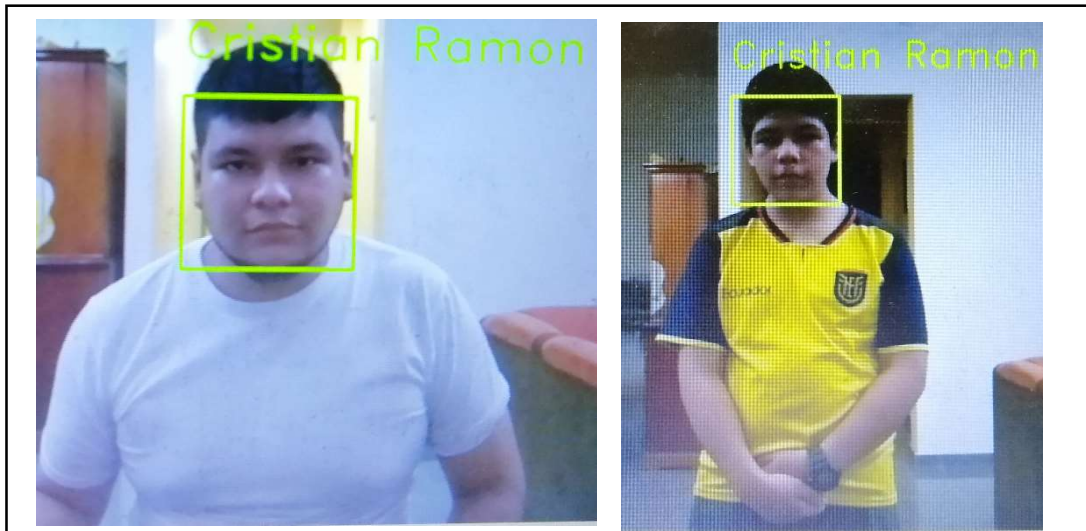
picam.release()
cv2.destroyAllWindows()
```


15.10. Anexo 4 (Resultados obtenidos).

En la Figura 18 se observa que el usuario 3 lo detecta como si fuera el usuario 1, dada la casualidad que ambos rostros son parecidos.

Figura 18

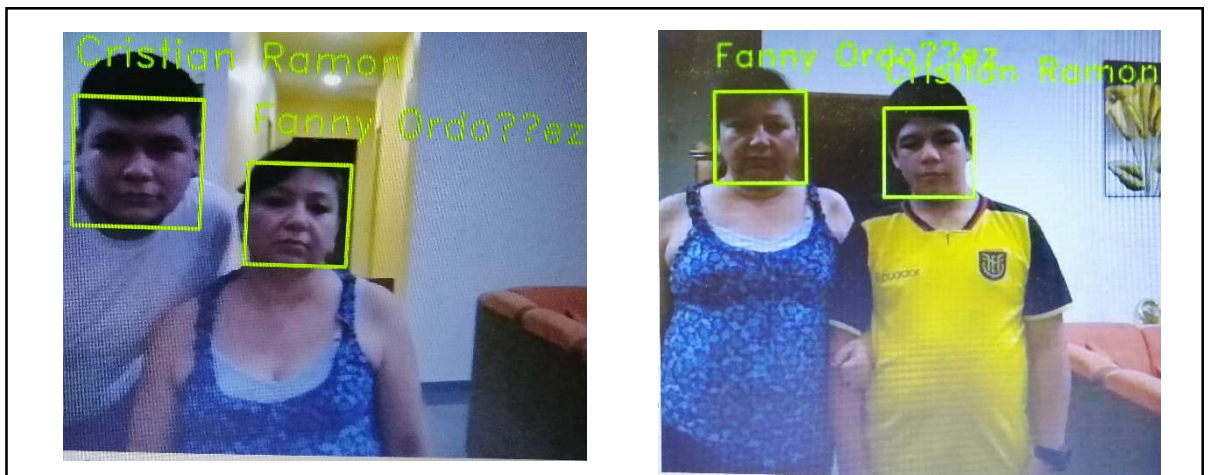
Usuario 1 y 3.



En la Figura 19 se hacen pruebas con el usuario 2, dando como resultado que con el usuario 1 se abre normalmente la prueba, pero también se abre con el usuario 3 detectándolo como si fuera el usuario 1.

Figura 19

Usuario 1, 2 y 3.



Finalmente, en la Figura 20 se realiza una última prueba con una persona desconocida dando como resultado que no se abre la puerta así sea que se encuentre un usuario registrado en la base de datos.

Figura 20

Usuario 2 y 4.



15.11. Anexo 5 (Sistema de control implementado).

Figura 21

Sistema de control implementado.

