



ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO
FACULTAD DE INFORMÁTICA Y ELECTRÓNICA
ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES
Y REDES

**“IMPLEMENTACIÓN DE UN SISTEMA DE IDENTIFICACIÓN
FACIAL UTILIZANDO PROCESAMIENTO DIGITAL DE
IMÁGENES PARA EL PERSONAL DEL BIOTERIO DE LA
FACULTAD DE CIENCIAS DE LA ESPOCH”**

TRABAJO DE TITULACIÓN

Tipo: PROPUESTA TECNOLÓGICA

Presentado para optar al grado académico de:

**INGENIERO EN ELECTRÓNICA, TELECOMUNICACIONES Y
REDES**

AUTOR: SANTIAGO SALOMÓN SALINAS LÓPEZ

TUTOR: ING. PAÚL DAVID MORENO AVILÉS PhD.

Riobamba – Ecuador

2019

© 2019, Santiago Salomón Salinas López

Se autoriza la reproducción total o parcial, con fines académicos, por cualquier medio o procedimiento, incluyendo la cita bibliográfica del documento, siempre y cuando se reconozca el Derecho de Autor.

Yo, SANTIAGO SALOMÓN SALINAS LÓPEZ soy responsable de las ideas, doctrinas y resultados expuestos en este trabajo de titulación y el patrimonio intelectual del mismo pertenece a la Escuela Superior Politécnica de Chimborazo.

Santiago Salomón Salinas López

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

**ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y
REDES**

El Tribunal del trabajo de titulación certifica que: El trabajo de investigación: Tipo: PROPUESTA TECNOLÓGICA “IMPLEMENTACIÓN DE UN SISTEMA DE IDENTIFICACIÓN FACIAL UTILIZANDO PROCESAMIENTO DIGITAL DE IMÁGENES PARA EL PERSONAL DEL BIOTERIO DE LA FACULTAD DE CIENCIAS DE LA ESPOCH”, de responsabilidad del señor SANTIAGO SALOMÓN SALINAS LÓPEZ, ha sido minuciosamente revisado por los Miembros del Tribunal del trabajo de titulación, quedando autorizada su presentación.

NOMBRES	FIRMAS	FECHA
M.Sc. Washington Luna Encalada DECANO DE LA FACULTAD DE INFORMÁTICA Y ELECTRÓNICA	_____	_____
Ing, Patricio Romero DIRECTOR DE LA EIETR	_____	_____
Ing. Paúl Moreno Avilés PhD DIRECTOR DEL TRABAJO DE TITULACIÓN	_____	_____
M.Sc. Mónica Zabala MIEMBRO DEL TRIBUNAL DEL TRABAJO DE TITULACIÓN	_____	_____

AGRADECIMIENTOS

Gracias a Dios y mi familia por todo el apoyo incondicional brindado, especialmente de mi mamá, mis hermanos, mi novia y mi papá.

Al Ing. David Moreno e Ing. Mónica Zabala, por la valiosa guía y asesoramiento no solo a lo largo del presente trabajo, si no durante todo el proceso académico universitario de los que fueron parte, demostrando su calidad humana y profesionalismo. A la Escuela Superior Politécnica de Chimborazo, por sus excelentes profesores, cuyas cátedras serán aplicadas a lo largo de mi vida profesional. Finalmente agradezco a todas las personas que colaboraron conmigo de manera directa e indirecta que sin su apoyo no habría finalizado con éxito el presente trabajo.

Inicie la universidad ignorante y termine más ignorante.

Santiago Salinas López

DEDICATORIA

El presente trabajo se lo dedico a Dios por todos los momentos que me ha brindado en la vida, a mi madre Beatriz, que con el ejemplo me enseñó a ser una persona de excelentes valores, a mi hermano Luis por ser mi mentor académico y siempre ayudarme, mi hermano Pedro por las enseñanzas de que siempre existe otro punto de vista, a mi novia Heidi que me acompañó y alentó a lo largo de todo este recorrido universitario. Se lo dedico a mi familia, a la vida, al tiempo, al amor y a la música por ser fuente de inspiración y creación de ideas.

Santiago Salinas López

TABLA DE CONTENIDO

ÍNDICE DE TABLAS.....	x
ÍNDICE DE FIGURAS.....	xi
ÍNDICE DE GRÁFICOS.....	xii
ÍNDICE DE ECUACIÓN.....	xiii
ÍNDICE DE ANEXOS.....	xiv
ÍNDICE DE ABREVIATURAS.....	xv
RESUMEN.....	xvi
ABSTRACT.....	xvii
INTRODUCCIÓN.....	1
CAPÍTULO I	
1. MARCO TEÓRICO.....	6
1.1. Reconocimiento Facial.....	6
1.2. Algoritmo de Viola – Jones.....	7
1.3. Origen del método Eigenface.....	7
1.4. Fases del Reconocimiento Facial.....	7
1.4.1. <i>Detección</i>	8
1.4.2. <i>Preprocesado</i>	8
1.4.3. <i>Extracción de características</i>	9
1.4.3.1. <i>Técnicas basadas en apariencia (Holísticos)</i>	10
1.4.3.2. <i>Principal Component Analysis (PCA)</i>	10
1.4.3.3. <i>Linear Discriminant Analysis (LDA)</i>	11
1.4.3.4. <i>Frecuency Domain Analysis</i>	11
1.4.3.5. <i>Técnicas basadas en modelos (Analíticos)</i>	12
1.4.3.6. <i>Análisis de distancias a puntos característicos</i>	12
1.4.3.7. <i>Local Binary Patterns (LBP)</i>	12
1.4.3.8. <i>Elastic Bunch Graph Matching (EBGM)</i>	13
1.4.3.9. <i>Hidden Markov Models (HMMs)</i>	13
1.4.4. <i>Comparación y decisión</i>	14

1.4.4.1.	<i>Medidas de similitud o distancias – Distancia Euclídea</i>	14
1.4.4.2.	<i>Medidas de similitud o distancias – Distancia Bhattacharyya</i>	15
1.4.4.3.	<i>Clasificadores – K-Nearest Neighbours</i>	16
1.4.4.4.	<i>Support Vector Machines (SVMs)</i>	16
1.4.5.	<i>Software Matlab</i>	16
1.4.5.1.	<i>Entorno de trabajo GUIDE – MATLAB</i>	17
1.4.5.2.	<i>MatLab Compiler</i>	17
CAPÍTULO II		
2.	MARCO METODOLÓGICO	18
2.1.	Escenario y variables de correlación	18
2.1.1.	<i>Escenario</i>	18
2.1.2.	<i>Variables de Correlación</i>	19
2.1.2.1.	<i>Luminosidad</i>	19
2.1.2.2.	<i>Posición</i>	20
2.1.2.3.	<i>Distancia</i>	20
2.2.	Metodología	21
2.2.1.	<i>Fundamentos del Análisis de Componentes Principales (PCA)</i>	21
2.2.2.	<i>Eigenfaces y PCA para la representación facial</i>	22
2.2.3.	<i>Redimensionamiento y comparación de datos</i>	23
2.3.	Software de programación	24
2.4.	Diseño del sistema de identificación facial	24
2.4.1.	<i>Etapa de entrenamiento</i>	26
2.4.1.1.	<i>Imágenes de entrenamiento</i>	26
2.4.1.2.	<i>Detección</i>	26
2.4.1.3.	<i>Preprocesado</i>	27
2.4.1.4.	<i>Extracción de Características</i>	28
2.4.2.	<i>Etapa de identificación</i>	30
2.4.2.1.	<i>Imagen de usuario</i>	31
2.4.2.2.	<i>Detección</i>	31
2.4.2.3.	<i>Preprocesado</i>	32
2.4.2.4.	<i>Proyección</i>	33
2.4.2.5.	<i>Comparación y decisión</i>	33
2.5.	Interfaz Gráfica	34

2.6.	Base de datos.....	35
2.6.1.	<i>Base de datos de control de acceso</i>	35
2.6.2.	<i>Base de Datos de Registro</i>	36
2.7.	Almacenamiento de las imágenes.....	37
2.8.	Sistema eléctrico de control de acceso	37
2.8.1.	<i>Cámara IP</i>	38
2.8.2.	<i>Configuración de una red LAN</i>	38
2.8.3.	<i>Comunicación entre Matlab y Arduino Nano</i>	39
2.8.4.	<i>Funcionamiento de la cerradura eléctrica</i>	40
2.9.	Presupuesto	40
CAPÍTULO III		
3.	PROCESAMIENTO Y ANÁLISIS DE RESULTADOS	42
3.1.	Procesamiento de pruebas y estimación umbral.....	42
3.2.	Evaluación del sistema de identificación facial.....	63
CONCLUSIONES		64
RECOMENDACIONES		65
BIBLIOGRAFÍA		
ANEXOS		

ÍNDICE DE TABLAS

Tabla 1-2: Escenario.....	18
Tabla 2-2: Funciones predeterminadas de Matlab.....	24
Tabla 3-2: Base de datos de control de acceso.....	36
Tabla 4-2: Base de datos de registro.....	36
Tabla 1-3: Características de la primera prueba.....	42
Tabla 2-3: Intentos de los usuarios registrados de la primera prueba.....	43
Tabla 3-3: Intentos de los usuarios desconocidos de la primera prueba.....	45
Tabla 4-3: Proyecciones y distancias euclídeas obtenidas en la primera prueba.....	48
Tabla 5-3: Características de la segunda prueba.....	49
Tabla 6-3: Intentos de los usuarios registrados de la segunda prueba.....	50
Tabla 7-3: Intentos de los usuarios desconocidos de la segunda prueba.....	52
Tabla 8-3: Proyecciones y distancias euclídeas obtenidas en la segunda prueba.....	55
Tabla 9-3: Características de la tercera prueba.....	56
Tabla 10-3: Intentos de los usuarios registrados de la tercera prueba.....	57
Tabla 11-3: Intentos de los usuarios desconocidos de la tercera prueba.....	59
Tabla 12-3: Proyecciones y distancias euclídeas obtenidas en la tercera prueba.....	62
Tabla 13-3: Resultados finales de las 3 pruebas realizadas.....	63

ÍNDICE DE FIGURAS

Figura 1-1: Preprocesamiento de una imagen.....	9
Figura 2-1: Eigenfaces.....	11
Figura 3-1: Fisherfaces.....	11
Figura 4-1: Vectores de distancias característicos.....	12
Figura 5-1: Imagen representada mediante EBGm.....	13
Figura 6-1: Extracción de bloques mediante HMM.....	14
Figura 7-1: Extracción de bloques de imagen facial mediante k-NN.....	16
Figura 1-2: Implementación de la cámara IP.....	20
Figura 2-2: Variaciones faciales.....	20
Figura 3-2: Distancia usuario cámara.....	20
Figura 4-2: Matriz de la etapa de entrenamiento.....	27
Figura 5-2: Matriz principal ecualizada.....	28
Figura 6-2: Promedio visual.....	28
Figura 7-2: Matriz Diferencia.....	29
Figura 8-2: Eigenfaces obtenidos.....	29
Figura 9-2: Matriz de covarianza.....	30
Figura 10-2: Detección de rostro.....	31
Figura 11-2: Rostro recortado.....	32
Figura 12-2: Ecualización del rostro.....	32
Figura 13-2: Rostro a identificar.....	33
Figura 14-2: Rostro con mayor proyección.....	33
Figura 15-2: Interfaz gráfica general del sistema de identificación.....	34
Figura 16-2: Interfaz de ingreso al sistema de identificación.....	35
Figura 17-2: Esquema del sistema eléctrico de control de acceso.....	37
Figura 18-2: Conexión entre Matlab y la Cámara IP.....	38
Figura 19-2: Router del sistema.....	39
Figura 20-2: Comunicación USB.....	39
Figura 21-2: Configuración de pines en Arduino.....	40
Figura 22-2: Cerradura eléctrica.....	40
Figura 23-2: Montaje final del sistema eléctrico.....	41

ÍNDICE DE GRÁFICOS

Gráfico 1-1: Diagrama general del sistema de reconocimiento facial.	8
Gráfico 2-1: Taxonomía del reconocimiento facial.	10
Gráfico 1-2: Diagrama de Flujo del sistema de identificación facial.....	25
Gráfico 2-2: Esquema de la etapa de entrenamiento.....	26
Gráfico 3-2: Esquema de la etapa de identificación.....	31
Gráfico 1-3: Resultados del intento uno de los usuarios registrados.	43
Gráfico 2-3: Resultados del intento dos de los usuarios registrados.....	44
Gráfico 3-3: Resultados del intento tres de los usuarios registrados.....	44
Gráfico 4-3: Resultados de los usuarios registrados de la primera prueba.	45
Gráfico 5-3: Resultados del intento uno de los usuarios desconocidos.	46
Gráfico 6-3: Resultados del intento dos de los usuarios desconocidos.....	46
Gráfico 7-3: Resultados del intento tres de los usuarios desconocidos.....	47
Gráfico 8-3: Resultados de los usuarios registrados de la primera prueba.....	47
Gráfico 9-3: Resultados generales de la primera prueba.	48
Gráfico 10-3: Resultados del intento uno de los usuarios registrados.	50
Gráfico 11-3: Resultados del intento dos de los usuarios registrados.....	51
Gráfico 12-3: Resultados del intento tres de los usuarios registrados.....	51
Gráfico 13-3: Resultados de los usuarios registrados de la segunda prueba.....	52
Gráfico 14-3: Resultados del intento uno de los usuarios desconocidos.	53
Gráfico 15-3: Resultados del intento dos de los usuarios desconocidos.....	53
Gráfico 16-3: Resultados del intento tres de los usuarios desconocidos.....	54
Gráfico 17-3: Resultados de los usuarios registrados de la segunda prueba.....	54
Gráfico 18-3: Resultados generales de la segunda prueba.....	55
Gráfico 19-3: Resultados del intento uno de los usuarios registrados.	57
Gráfico 20-3: Resultados del intento dos de los usuarios registrados.....	58
Gráfico 21-3: Resultados del intento tres de los usuarios registrados.....	58
Gráfico 22-3: Resultados de los usuarios registrados de la tercera prueba.	59
Gráfico 23-3: Resultados del intento uno de los usuarios desconocidos.	60
Gráfico 24-3: Resultados del intento dos de los usuarios desconocidos.....	60
Gráfico 25-3: Resultados del intento tres de los usuarios desconocidos.....	61
Gráfico 26-3: Resultados de los usuarios registrados de la tercera prueba.....	61
Gráfico 27-3: Resultados generales de la tercera prueba.	62

ÍNDICE DE ECUACIÓN

Ecuación 1-1: Distancia euclídea.....	14
Ecuación 2-1: Espacio euclídeo n-dimensional.	15
Ecuación 3-1: Espacio euclídeo n-dimensional.	15
Ecuación 4-1: Coeficiente de Bhattacharyya forma discreta.	15
Ecuación 5-1: Coeficiente de Bhattacharyya forma continua.....	15
Ecuación 6-1: Distancia Bhattacharyya para distribución normal.	15
Ecuación 1-2: Media General de X.....	21
Ecuación 2-2: Matriz de Covarianza.....	21
Ecuación 3-2: Combinación Lineal.....	21
Ecuación 4-2: Aproximación de la media.....	22
Ecuación 5-2: Aproximación de la Matriz de Covarianza.	22
Ecuación 6-2: Cálculo matriz V	23

ÍNDICE DE ANEXOS

ANEXO A: Código del Programa.

ANEXO B: Datasheet Arduino Nano.

ANEXO C: Configuración del Relé con Arduino.

ANEXO D: Características de la Cerradura Eléctrica.

ANEXO E: Acta de Entrega – Recepción.

ANEXO F: Manual del Sistema de Identificación Facial.

ÍNDICE DE ABREVIATURAS

PCA	Principal Component Analysis
LBP	Local Binary Patterns
EBGM	Elastic Bunch Graph Matching
HMMs	Hidden Markov Models
SVMs	Support Vector Machines

RESUMEN

El objetivo del trabajo de titulación fue implementar un sistema de identificación facial mediante el procesamiento digital de imágenes para el personal del Bioterio de la Facultad de Ciencias de la Escuela Superior Politécnica de Chimborazo. El método utilizado para el procesamiento digital de imágenes fue el método *Eigenfaces*, construido sobre técnicas de Análisis de Componentes Principales (PCA), y conjuntamente con las principales variables correlacionadas como: luminosidad, distancia usuario – cámara, posición facial, umbrales de proyección y distancia euclídea, para el almacenamiento de datos se utilizó una base de datos local y el software Matlab para desarrollar el sistema de identificación debido a que permite utilizar herramientas para el reconocimiento facial necesarios para la identificación. Se realizaron un total de 180 pruebas en 3 días diferentes con un número total de 20 usuarios, registrando 3 intentos de acceso por cada uno. El resultado final fue un porcentaje promedio del 86% de validez del sistema, registrando un 96% como máximo y un 80% como mínimo. Adicionalmente, se realizó la combinación con un sistema eléctrico para el control de apertura de una cerradura eléctrica, la cual fue implementada en la puerta del Bioterio. Se concluye que el sistema de identificación facial implementado en el bioterio de la Facultad de Ciencias tiene una eficiencia del 86% con las diferentes características establecidas de acuerdo a las variables de correlación. Se recomienda analizar el escenario respectivo para determinar el método de procesamiento digital de imagen para implementar un sistema de identificación facial.

PALABRAS CLAVE: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INTELIGENCIA ARTIFICIAL>, <RECONOCIMIENTO FACIAL>, <SISTEMA DE IDENTIFICACION FACIAL>, <CONTROL DE ACCESO>.

ABSTRACT

The objective of this thesis was to implement a facial identification system through the digital image processing for the vivarium staff at the Faculty of Science of the Higher Polytechnic School of Chimborazo. The Eigenfaces method was the procedure used for digital image processing, built on techniques of Principal Component Analysis (PCA), and together with the main variables correlated as: luminosity, user-camera distance, facial position, projection thresholds and Euclidean distance, for data storage, a local database and the Matlab software were used to develop the identification system because it allows to use the necessary facial recognition tools for identification. A total of 180 tests were carried out in three different days with a total number of 20 users, registering 3 access attempts for each one. The final outcome was an average percentage of 86% of system validity, registering a rating scale of at most 96% and at least 80%. Additionally, the combination was made with an electrical system for the controlled opening of an electric lock, which was implemented on the Vivarium door. It is concluded that the facial identification system implemented at the faculty of sciences Vivarium has an efficiency of 86% with the different characteristics established according to the correlation variables. It is recommended to analyze the respective scenario to determine the digital image processing method in order to implement a facial identification system.

KEYWORDS: <TECHNOLOGY AND ENGINEERING SCIENCES>, <ARTIFICIAL INTELLIGENCE>, <FACIAL RECOGNITION>, <FACIAL IDENTIFICATION SYSTEM>, <ACCESS CONTROL >.

INTRODUCCIÓN

Actualmente, todo tipo de información es de vital importancia para una persona y más valiosa cuando se encuentra a cargo de información sustancial de una empresa, laboratorio o institución, es por eso que en los últimos años la considera como uno de los activos más valiosos que puede poseer una institución, la información puede encontrarse a nivel virtual o a nivel físico, pero en la actualidad el mayor riesgo de la información es la suplantación de identidad mediante la identificación facial.

La identificación de un rostro es una tarea relativamente fácil para los humanos, y un claro ejemplo es el caso de los niños, quienes rápidamente aprenden a identificar o reconocer el rostro de sus padres, esto haría pensar que indicarle a una computadora a reconocer diferentes rostros mediante algoritmos es una tarea sencilla, pero desafortunadamente no es así. El reconocimiento facial es un problema que fue considerado desde las primeras etapas de visión por computadora, este problema ha sido estudiado más a fondo en los últimos años y gracias a los avances de los recursos computacionales se ha logrado implementar algoritmos más complejos utilizando diferentes métodos y técnicas, entre estas, se puede mencionar las basadas en igualamiento de plantillas llamada Eigenfaces. En este proyecto utilizamos esta técnica para realizar la identificación facial aprovechando sus diferentes características que esta técnica nos ofrece.

El desarrollo del presente trabajo de titulación está enfocado a la implementación de un sistema de identificación facial mediante el algoritmo llamado Eigenface como sistema de seguridad del bioterio de la Facultad de Ciencias de la Escuela Superior Politécnica de Chimborazo. Con el desarrollo del presente trabajo, se pretende innovar el actual sistema de vigilancia que utilizan para acceder al laboratorio permitiendo un análisis de imágenes para el reconocimiento de personas, mediante los resultados adquiridos se determinará las condiciones necesarias para el mejoramiento en cuanto a condiciones ambientales, resolución de cámaras, distancias favorables y eficiencia de los algoritmos.

ANTECEDENTES

El sistema de identificación facial utiliza el reconocimiento facial, el cual no es precisamente un fenómeno nuevo, los primeros experimentos con esta tecnología se remontan a la década de 1960, aunque, en aquel entonces, la investigación para comenzar con su desarrollo se mantuvo en secreto. (Reconocimiento facial con base en imágenes, 2016, p.4).

En el año de 1871 se realizó el primer intento de identificar a una persona comparando su rostro con un grupo de imágenes, más tarde en 1882, el criminólogo Alphonse Bertillon de origen francés uso un método que consistía en tomar medidas de todos los rasgos posibles de la cara y con esto crear una base de datos de rasgos faciales, en resumidas cuentas, el principio de identificación facial parte en registrar las medidas de varios puntos característicos del rostro de un individuo. Dado que en un rostro común se puede encontrar puntos significativos como ojos, pupilas, boca, cejas entre otros. De manera que analizando y apoyándose de cada una de las distancias obtenidas de los puntos característicos del rostro se podría identificar caras iguales (Maya Binetskaya, 2013, p.6).

La identificación facial es una técnica muy usada en la actualidad para poder tener un control de acceso a diversas áreas restringidas. Así como la búsqueda de personas, el sistema de identificación facial también es muy utilizado en diversas aplicaciones, como es en videojuegos controlados por movimiento, animaciones, realidad aumentada o cámaras fotográficas; (Cañego Nerea, 2017, p.5). La identificación facial tiene un mercado aproximado de 3 mil millones de dólares, lo cual se estima que crezca a 6 mil millones en 2021, además la vigilancia es uno de los factores fundamentales para el crecimiento, es decir que los gobiernos son los que generan el principal ingreso. De forma que se puede ver que el FBI tiene una base de datos con imágenes a más de la mitad de la población estadounidense, de forma que el solo ingresar ciertas características del habitante automáticamente tendrán la imagen de la persona, también existe el temor de varias personas, de manera que pueden usar la información para cometer actos delictivos. (Cromo, 2017)

El impacto de los sistemas de identificación facial tiene tanta difusión, ya sea desde el punto de vista de la seguridad (como lo utiliza la policía, los profesionales de seguridad y el gobierno), o como un beneficio para una organización (para reconocer a la gente en una cámara o como un medio para proteger un dispositivo con contraseña).

En Ecuador en el año de 2016 en Quito, la Escuela Politécnica Nacional realizó el diseño e implementación de un sistema de seguridad y alerta para vehículos, basado en reconocimiento facial y localización GPS, en una Raspberry Pi B plus, de manera similar en la ciudad de Riobamba en el año del 2017 se han presentado diversos proyectos similares, uno de ellos es el

procesamiento de imágenes para la identificación de personas como sistema de seguridad en zonas domiciliarias brindando seguridad y una alternativa de protección a la sociedad. Otro gran ejemplo sobre el reconocimiento facial es el diseño del prototipo de control de acceso del personal mediante reconocimiento facial en 3D para empresas públicas y privadas, el cual se implementó en la empresa pública llamada cementera de Chimborazo EP, para disminuir el tiempo de acceso al momento del ingreso y salida del lugar de trabajo obteniendo un nivel de aceptación del 90 por ciento, finalmente como último ejemplo en la ESPOCH se realizó la implementación de un sistema de control de acceso mediante reconocimiento facial para la sala de profesores de la Facultad de Informática y Electrónica mejorando la seguridad del ingreso del personal, sistema que en la actualidad no sigue vigente para la identificación de los docentes.

FORMULACIÓN DEL PROBLEMA

¿Es posible implementar en el Bioterio de la Facultad de Ciencias un sistema de identificación facial basado en el procesamiento digital de imágenes?

SISTEMATIZACIÓN DEL PROBLEMA

¿Qué técnicas del procesamiento digital de imágenes permitirá identificar las características para la identificación facial?

¿Cuáles son los elementos de una arquitectura para el reconocimiento facial?

¿En qué grado de desempeño el sistema de identificación facial ayudará al reconocimiento facial del personal del Bioterio de la Facultad de Ciencias de la Escuela Superior Politécnica de Chimborazo?

JUSTIFICACIÓN TEÓRICA

En el 2016 la Universidad de Carabobo implementó el diseño de un software de reconocimiento facial para el control de asistencia en la Escuela de Telecomunicaciones de la misma Universidad, brindando un mayor nivel de fiabilidad por medio de la detección y reconocimiento facial de todo el personal del lugar, para ello, con la ayuda de la librería OpenCV se usó la tecnología de visión artificial, captura, comparación y procesamiento digital de imágenes y de esta forma identificar a las personas. Otra de las universidades que implementaron un Sistema de Reconocimiento Facial fue la Pontificia Universidad Católica de Valparaíso, el cual integrada las librerías de

OpenCV/EmguCV, además disponía de una base de datos local la cual permitía almacenar las fotografías ya entrenadas sacadas al usuario para que en los pasos siguientes se pueda reconocer el rostro de la persona. Como último ejemplo la Universidad de Veracruzana tiene un sistema de reconocimiento facial aplicado a la toma de asistencia de los estudiantes, apoyando al docente con la automatización de esta tarea administrativa que debe realizar diariamente, este sistema se realizó con la ayuda de la herramienta de MatLab.

En los sistemas de reconocimiento de rostros en ambientes controlados se pueden modificar los factores como variaciones de iluminación, variación de pose, expresión facial, oclusión, etc. Con esto se logra obtener una alternativa de mejora a la autenticación del personal, donde se evalúa el comportamiento del sistema para poder ser utilizados en aulas o pasillos donde la afluencia de personas es mayor.

La Escuela Superior Politécnica de Chimborazo no dispone de un sistema de reconocimiento facial para poder verificar e identificar el rostro del personal del Bioterio de la Facultad de Ciencias, mediante la implementación del sistema de identificación facial se logrará optimizar tiempo y recursos, debido que se necesita obligatoriamente una persona encargada de brindar acceso al laboratorio y registrar manualmente el ingreso y salida del personal autorizado, siendo el Bioterio un lugar de gran importancia donde se realizan experimentos con animales para su análisis científico, además en el lugar existe personal estudiantil, los cuales se encuentran encargados de realizar la limpieza del lugar de manera obligatoria en horarios específicos, con el sistema de identificación facial se eliminarán los descuidos personales en caso de dejar sin seguridad la puerta de ingreso al Bioterio, previniendo posibles inconvenientes como la expulsión de virus y bacterias al exterior del laboratorio, obteniendo un control más sólido y evitando las vulnerabilidades de seguridad para el ingreso del laboratorio. El sistema de identificación facial beneficiará a estudiantes, docentes y personal de la Facultad de Ciencias de la ESPOCH.

JUSTIFICACIÓN APLICATIVA

El presente proyecto se realizará mediante las técnicas que el procesamiento digital de imágenes ofrece encontrándonos con imágenes de entradas las cuales seguirán un proceso llegando a obtener un resultado final, el cual será la identificación de una persona registrada o no registrada. El reconocimiento se dará inicio a través de una imagen capturada por una cámara para el control de acceso al bioterio de la Facultad de Ciencias, una vez realizada la detección facial se procederá a la identificación facial. Primero se creará una base de datos con imágenes de varios usuarios del bioterio, si la persona que se identifica delante de la cámara tiene acceso otorgado dentro de la

base de datos se dará una descripción del usuario, es decir, nombre de la persona y hora a la que se ha identificado. Por último, se realizará la capacitación a la persona encargada, la cual tendrá la responsabilidad de modificar la base de datos, almacenar fotografías de nuevos usuarios o negar el acceso al personal no autorizado, manteniendo sus capturas faciales en la base de datos sin ser eliminados.

OBJETIVOS

OBJETIVO GENERAL

Implementar un sistema de identificación facial utilizando procesamiento digital de imágenes para el personal del Bioterio de la Facultad de Ciencias de la Escuela Superior Politécnica de Chimborazo.

OBJETIVOS ESPECÍFICOS

- Analizar las diferentes técnicas del procesamiento digital de imágenes para implementar el sistema de identificación facial.
- Diseñar e implementar la arquitectura del reconocimiento facial.
- Evaluar el desempeño del sistema de identificación facial mediante los parámetros correlacionados encontrados.

CAPÍTULO I

1. MARCO TEÓRICO

El contenido del presente capítulo nos proporciona información de los conceptos teóricos utilizados a lo largo del proceso del desarrollo del presente trabajo de titulación.

1.1. Reconocimiento Facial

El reconocimiento facial dependiendo de la aplicación a utilizarse se encuentra dentro de dos esquemas: verificación e identificación. La verificación en el sistema de reconocimiento facial es un escenario de comparación 1:1, donde el rostro como imagen de entrada se compara directamente con el rostro de la base de datos previamente almacenada confirmando de esta manera la idoneidad de la identidad de la persona en cuestión. Por otro lado, el esquema de identificación es el reconocimiento de la identidad de una persona desconocida como información de entrada comparada con la base de datos de rostros, teniendo una comparación de 1: N, pudiendo operar bajo dos modalidades dependiendo del conjunto de datos a utilizar (Pandya et al., 2013, p.632)

- Identificación close-set. – Opera sobre un escenario donde un conjunto de datos cerrado en la que el sistema devuelve como respuesta la imagen de la persona registrada en la base de datos o a su vez la más semejante a la imagen evaluada.
- Identificación open-set. – Este tipo de identificación opera sobre un escenario donde un conjunto de datos abiertos obliga al sistema a dar como resultado una identificación de la persona evaluada o la notificación que la imagen de la persona no se encuentra registrada en la base de datos, siendo más común este sistema a nivel comercial (Kawulok, 2016, p.79).

Entre las diferentes líneas de investigación enfocado a técnicas de mejora de detección de facial, se establece dos tareas fundamentales, extracción de la características y clasificación de la expresión facial, Ekman y Friesen (1978, p.70), clasifica a las emociones en seis emociones universales básicas como son: alegría, sorpresa, tristeza, miedo, disgusto y enojo; codificadas en un sistema de codificación de acciones faciales FACS por sus siglas en inglés, derivándose dos campos de estudio, como es la clasificación de expresiones de emociones faciales, y el segundo que es la detección automática de acciones faciales. En donde la robustez de los sistemas de reconocimiento dependerá del sistema de extracción de características faciales, desarrollándose

sistemas de reconocimiento facial en tiempo real con técnicas híbridas que son los trabajos propuestos por Braathen et al. (2001, p.45).

Otros estudios se han enfocado en la detección de píxeles de piel, para discriminar los elementos que deben ser analizados y solo enfocarse en el rostro o características de piel propias de las personas, como lo presenta (Zarit, et al., 1999, p.2), realizando una comparación de cinco espacios de color y dos métodos no paramétricos de modelado de piel, métodos paramétricos, modelo gaussiano y mezcla de gaussianas.

1.2. Algoritmo de Viola – Jones

El algoritmo de Viola – Jones es un método de detección de objetos que destaca por su bajo coste computacional lo que permite ser empleado en tiempo real, su principal objetivo es la detección de rostros o reconocimiento facial donde actualmente sigue siendo utilizado, el algoritmo se basa en una serie de clasificadores denominados *Haar-like features* que se calculan a partir de una imagen integral, estos se agrupan en una cascada empleando un algoritmo de aprendizaje basado en AdaBoost para un alto rendimiento en la detección. (Viola y Jones, 2001, pp.1-2).

1.3. Origen del método Eigenface

En 1988, Sirovich y Kirby comenzaron a aplicar el álgebra lineal al problema del reconocimiento facial. Lo que se conoció como el enfoque Eigenface comenzó como una búsqueda de una representación de baja dimensión de las imágenes faciales. Sirovich y Kirby pudieron demostrar que el análisis de las características de una colección de imágenes faciales podría formar un conjunto de características básicas. También pudieron demostrar que se necesitaban menos de cien valores para codificar con precisión una imagen de cara normalizada. En 1991, Turk y Pentland ampliaron el enfoque Eigenface descubriendo cómo detectar rostros dentro de las imágenes. Esto condujo a las primeras instancias de reconocimiento facial automático. Su enfoque se vio limitado por factores tecnológicos y ambientales, pero fue un gran avance en la demostración de la viabilidad del reconocimiento facial automático. (Greer Williams, 2018).

1.4. Fases del Reconocimiento Facial

A pesar de la gran variedad de sistemas existentes, todo sistema de reconocimiento facial puede dividirse en cuatro fases principales como que se pueden visualizar en el Gráfico 1-1. La primera

fase comprende la detección y localización de la cara en la imagen para su posterior procesado. Esta fase de preprocesado se lleva a cabo para preparar el rostro mediante la alineación, escalado, recorte y ecualización de la imagen. Una vez que la imagen del rostro está preparada, se realiza la tercera fase de extracción de característica para obtener la información relevante de la imagen. Por último, se realiza la comparación donde se aplican los algoritmos de reconocimiento y se extrae una decisión respecto a la base de datos y la imagen de entrada. (Domínguez Sara, 2017, p.9).

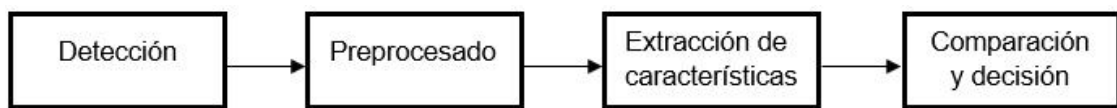


Gráfico 1-1: Diagrama general del sistema de reconocimiento facial.
Realizado por: Santiago Salinas, 2019

1.4.1. Detección

La fase de detección consiste en encontrar áreas de la imagen que contengan una cara para aislarlas del resto. Este es uno de los objetivos del trabajo, y una de las fases más importantes de la aplicación ya que una mala detección conllevaría un error en el resto de las fases. (Domínguez Sara, 2017, p.9).

Actualmente existen varios algoritmos de alto y bajo nivel que ayudan a la implementación de sistemas de identificación facial, muchos de estos algoritmos son un tanto complejos dependiendo el área a implementarse y pueden llegar a tratarse incluso hasta de redes neuronales o inteligencia artificial sofisticada, sin embargo, en el presente trabajo de titulación se va a utilizar uno de los métodos más populares y eficientes que permiten procesar la información facial de los usuarios en tiempo real.

1.4.2. Preprocesado

La etapa de procesado se lleva a cabo a partir de la información obtenida en la detección. Esta etapa realiza una serie de transformaciones geométricas sobre la imagen dejándole preparada para la correcta extracción de características. (Russ J. C., 2002, p.80) En el preprocesado se utilizan tres etapas para realizar la normalización y ordenar la imagen para su próxima etapa como se puede visualizar en la Figura 1-1.



Figura 1-1: Preprocesamiento de una imagen.

Fuente: Domínguez Sara, 2017

- **Escalado.** Para conseguir que todos los rostros de las imágenes tengan las mismas proporciones, se utiliza la distancia entre los centros de los ojos para conseguir un ratio por el cual la imagen debe ser aumentada o reducida. Esto es necesario puesto que muchas técnicas de reconocimiento requieren que todos los datos de entrada tengan el mismo tamaño (en nuestro caso la matriz de píxeles).
- **Recorte.** Una vez la imagen ha sido escalada, se procede al recorte para obtener sólo la región de interés. A todas las imágenes se les da las mismas dimensiones con el fin de que todas ellas tengan el mismo tamaño para que sea posible la comparación entre ellas.
- **Ecualización del histograma.** Las imágenes pueden presentar variabilidad en la luminosidad y en el contraste lo que produce que imágenes similares sean muy diferentes respecto al valor de intensidad de sus píxeles. Mediante la ecualización de su histograma, se pretende que las imágenes que tienen la mayor parte de sus valores de intensidad concentrados en una zona reducida del histograma pasen a extenderse por todo el rango de valores del histograma. Esto resulta en imágenes con mayor contraste y con menor variabilidad lumínica entre ellas. (Domínguez Sara, 2017, p.9).

1.4.3. Extracción de características

La extracción de características se emplea para obtener la información que resulta relevante de cara a realizar una comparación. Durante las últimas décadas se han desarrollado un gran número de algoritmos para llevar a cabo dicha extracción en el ámbito del reconocimiento facial. Como se puede ver en la Gráfico 2-1, las técnicas dependientes de pose se dividen en dos grandes grupos (Agrawala y Singhb, 2015, p.80). En primer lugar, las técnicas basadas en apariencia, que analizan la textura de la imagen a partir de la cual se aplicarán diferentes técnicas estadísticas y se extraerá la información. En segundo lugar, las técnicas basadas en modelos, que extraen las características tanto de la forma del rostro como de la textura. (Domínguez Sara, 2017, p.9).

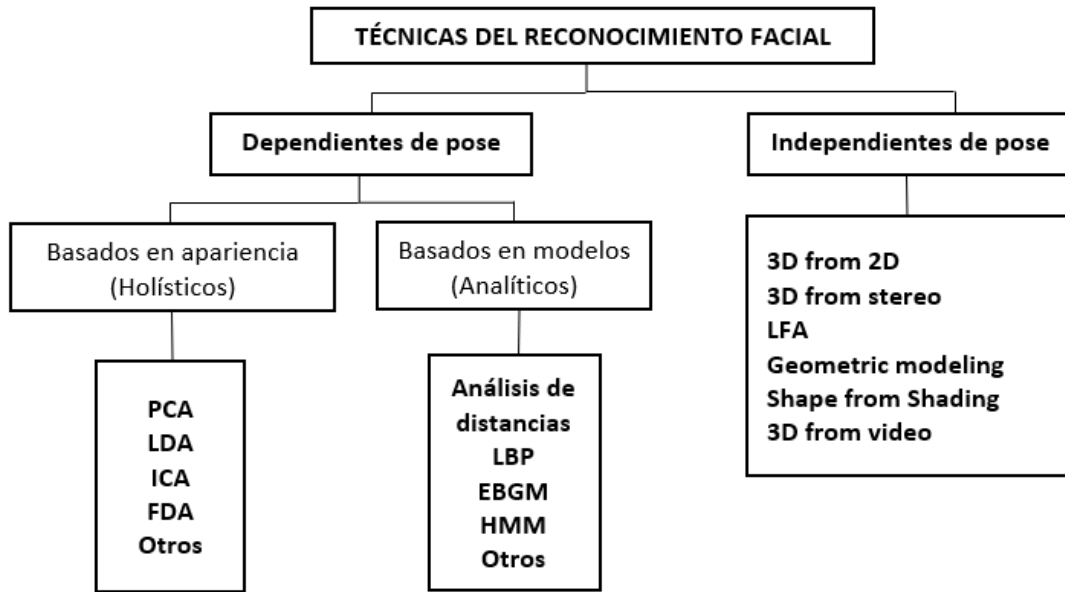


Gráfico 2-1: Taxonomía del reconocimiento facial.
Realizado por: Santiago Salinas, 2019.

1.4.3.1. Técnicas basadas en apariencia (Holísticos)

Las técnicas basadas en apariencia o también llamadas técnicas holísticas son las encargadas de convertir un problema de reconocimiento facial a un problema de análisis de espacio, en donde se aplica diferentes técnicas basadas en estadística. De este tipo de técnicas destaca su aplicabilidad en imágenes de baja resolución o mala calidad, su rapidez y ejecución (se pueden implantar en sistemas en tiempo real) o su baja complejidad. Sin embargo, también tienen varios inconvenientes. Uno de los inconvenientes es que para conseguir buenos resultados se requiere un conjunto de muestras considerable para la fase de entrenamiento. También aspectos como los cambios en la iluminación, la pose o la expresión de la cara tienen un gran impacto en los resultados finales. Dependiendo del método empleado, estos inconvenientes tendrán un impacto mayor o menor. (Domínguez Sara, 2017, p.13).

1.4.3.2. Principal Component Analysis (PCA)

El método Eigenfaces basado en Turk y Pentland, (1991, p.590) es uno de los más populares, construido sobre técnicas de Principal Component Analysis (PCA). Dicho método transforma la imagen a un subespacio (ejemplo en Figura 4-1) por el cual es posible obtener vectores de características de menor dimensionalidad sin una pérdida de información discriminativa importante.



Figura 2-1: Eigenfaces.

Fuente: Jolliffe I.T, 1986

1.4.3.3. Linear Discriminant Analysis (LDA)

Derivada de PCA, se implementó una técnica que une PCA con Linear Discriminant Analysis (LDA) denominada Fisherfaces (Belhumeur, et al., 1997, p.713), con la que se consigue mayor robustez frente a cambios de iluminación, pero resulta computacionalmente más costosa. Este método, junto con el anterior Eigenfaces, son los dos más usados en la actualidad en reconocimiento facial.



Figura 3-1: Fisherfaces

Fuente: Lee, Chen-Pang, 2009

1.4.3.4. Frequency Domain Analysis

Por último, las técnicas de análisis en el dominio de la frecuencia (Hafed y Levine, 2001, p.179) ofrecen un gran tipo de representación del rostro del individuo en función de las componentes de baja frecuencia que presentan altos niveles de energía, estas técnicas son independientes de los datos o la información por lo que no requieren de un entrenamiento. En la actualidad, existen varios algoritmos optimizados que facilitan la implementación y con un costo computacional reducido.

1.4.3.5. Técnicas basadas en modelos (Analíticos)

Las técnicas basadas en modelos tratan de obtener características biométricas de las imágenes para realizar el reconocimiento. Se tienen en cuenta aspectos como la distancia entre los ojos, el grosor de la nariz, el tamaño de la boca, etc. Estos sistemas requieren un conocimiento previo de las imágenes, además de ser más lentos y complejos que los sistemas basados en apariencia. Sin embargo, son más robustos frente a cambio de orientación o expresión de la cara y se ven menos afectados por cambios en la iluminación o las sombras. (Domínguez Sara, 2017, p.13)

1.4.3.6. Análisis de distancias a puntos característicos

Uno de los primeros sistemas de reconocimiento se basa en la técnica a partir de puntos geométricos de la cara (Cox et al., 2002, pp 2-3). A partir de la detección de diferentes puntos característicos (por ejemplo, como se muestra en la Figura 4-1 se crean vectores que contienen datos de distancias entre los mismos. Cuantos más puntos característicos son detectados, mayor número de distancias podrán ser calculadas obteniendo así mejores resultados en el reconocimiento.

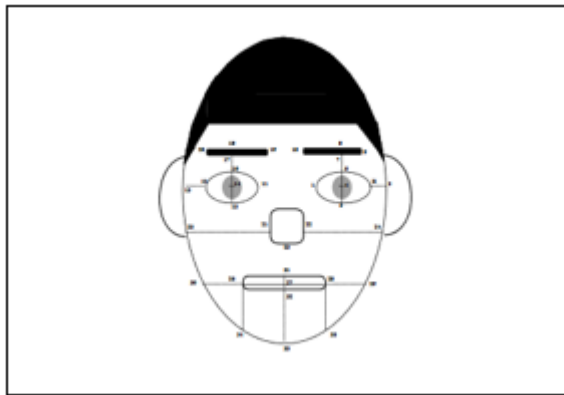


Figura 4-1: Vectores de distancias característicos.
Fuente: Cox et al., 2002, p.3.

1.4.3.7. Local Binary Patterns (LBP)

El algoritmo LBP (Ahonen et al., 2004, pp 470-471) es conocido como un buen descriptor de texturas a nivel local, utilizado en muchas aplicaciones de tratamiento de imágenes y reconocimiento de patrones. LBP etiqueta cada píxel de la imagen de acuerdo a los valores de sus píxeles vecinos. Para esto, se define un grado de vecindad y se les da el valor de 1 o 0 a estos píxeles según su nivel de intensidad sea mayor o menor que el valor del píxel central. A

continuación, se recorren los vecinos y se genera una etiqueta binaria para el píxel central. Este proceso se repite sucesivamente para todos los píxeles de la imagen.

1.4.3.8. *Elastic Bunch Graph Matching (EBGM)*

EBGM es una técnica que fue diseñada para realizar tareas de reconocimiento facial utilizando solamente algunos puntos de interés y no la cara en su totalidad, aprovechando la estructura topológica similar que estas presentan. La implementación de este algoritmo requiere el uso de las wavelets de Gabor, que son filtros paso banda que permiten alcanzar la resolución conjunta de información máxima en los espacios bidimensionales espacial y frecuencial. De esta manera, el uso de estas funciones bidimensionales proporciona una descripción de la información en frecuencia, en una región específica de la imagen. (Wiskott et al., 1997, pp 7-8)

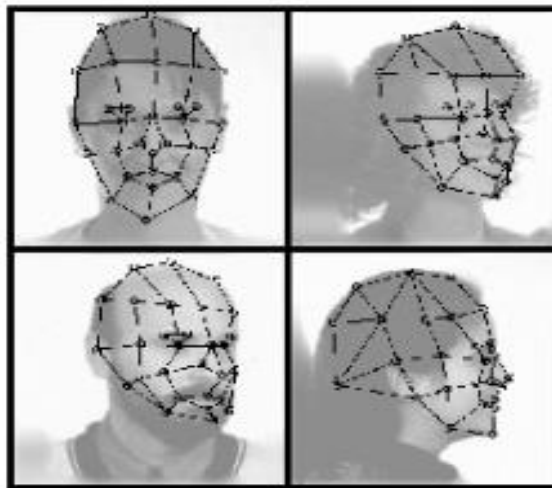


Figura 5-1: Imagen representada mediante EBGM.
Fuente: Wiskott et al., 1997, p.9

1.4.3.9. *Hidden Markov Models (HMMs)*

Los HMMs también han sido usados con éxito para el reconocimiento facial. Estas técnicas presentan robustez frente a cambios de iluminación, expresión y orientación, otorgando así una ventaja frente a los métodos holísticos. Las técnicas basadas en HMM utilizan regiones horizontales de píxeles que albergan a la frente, ojos, nariz, boca y barbilla sin obtener la posición exacta de cada rasgo. Cada una de estas regiones es asignada a un estado del HMM para el reconocimiento. (Samaria y Young, 1994, pp 37-39)

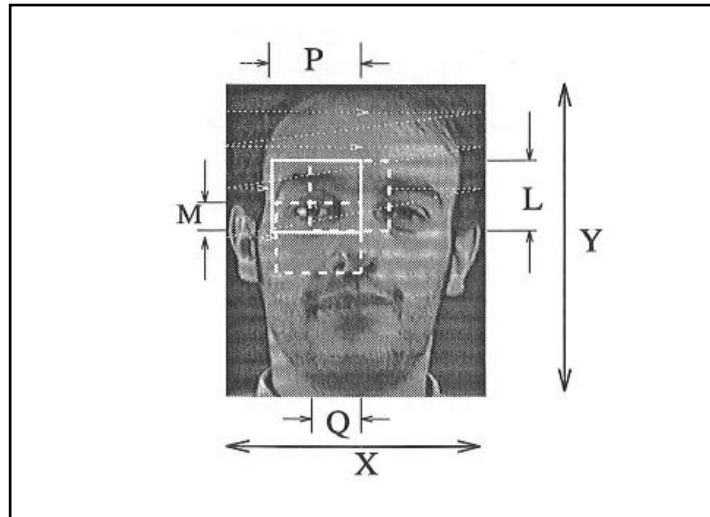


Figura 6-1: Extracción de bloques mediante HMM.
Fuente: Samaria y Young, 1994, p.40

1.4.4. Comparación y decisión

En la última fase, se compara la información extraída del rostro que se quiere reconocer con los datos que hay almacenados en la base de datos. Para obtener una puntuación por la cual tomar una decisión, existen varios métodos de comparación. En este apartado se describen algunos de los más utilizados en la actualidad. Los métodos se pueden dividir en medidas de similitud y clasificadores (Theodoridis y Koutroumbas, 2008, p.20).

1.4.4.1. Medidas de similitud o distancias – Distancia Euclídea

La distancia euclídea es una de las medidas más básicas para calcular distancias. Esta distancia se define como la distancia directa entre dos puntos en un plano. (Domínguez Sara, 2017, p.17) El ejemplo más claro es la distancia entre dos puntos en un plano de dos dimensiones de coordenadas X e Y . Si tuviéramos dos puntos P_1 y P_2 con coordenadas (X_1, Y_1) y (X_2, Y_2) respectivamente, el cálculo de la distancia euclídea entre los mismos sería:

$$d_E(P_1, P_2) = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2} \quad (1.1)$$

Ecuación 1-1: Distancia euclídea.

En general la distancia euclídea entre dos puntos $P = (p_1, p_2, \dots, p_n)$ y $Q = (q_1, q_2, \dots, q_n)$ en el espacio euclídeo n -dimensional vendría definida como:

$$d_E(P, Q) = \sqrt{\sum_{i=1}^n (p_i - q_i)^2} \quad (2.1)$$

Ecuación 2-1: Espacio euclídeo n-dimensional.

1.4.4.2. Medidas de similitud o distancias – Distancia Bhattacharyya

La distancia Bhattacharyya es una medida estadística que cuantifica la similitud entre dos distribuciones de probabilidad discretas o continuas. Está estrechamente relacionada con el coeficiente de Bhattacharyya, que es una medida de la superposición entre dos muestras estadísticas o poblaciones. Esta distancia es particularmente conocida por su bajo coste computacional y baja sensibilidad al ruido. (Vezzeti y Marcolin, 2015, p.49) Para las distribuciones de probabilidad p y q sobre el mismo dominio X , la distancia Bhattacharyya es definida como:

$$D_B(p, q) = -\ln(BC(p, q)) \quad (3.1)$$

Ecuación 3-1: Espacio euclídeo n-dimensional.

Donde BC es el coeficiente de Bhattacharyya, definido para distribuciones de probabilidad discretas y para distribuciones de probabilidad continuas. En ambos casos, $0 \leq BC \leq 1$ y $0 \leq D_B \leq \infty$

$$BC(p, q) = \sum_{x \in X} \sqrt{p(x)q(x)} \quad (4.1)$$

Ecuación 4-1: Coeficiente de Bhattacharyya forma discreta.

$$BC(p, q) = \int \sqrt{p(x)q(x)} dx \quad (5.1)$$

Ecuación 5-1: Coeficiente de Bhattacharyya forma continua.

En su formulación más simple, la distancia Bhattacharyya entre dos clases que siguen una distribución normal pueden calcularse a partir de la media μ y varianza σ^2 de las mismas como:

$$D_B(p, q) = \frac{1}{4} \ln \left(\frac{1}{4} \left(\frac{\sigma_p^2}{\sigma_q^2} + \frac{\sigma_q^2}{\sigma_p^2} + 2 \right) \right) + \frac{1}{4} \left(\frac{(\mu_p - \mu_q)^2}{\sigma_p^2 + \sigma_q^2} \right) \quad (6.1)$$

Ecuación 6-1: Distancia Bhattacharyya para distribución normal.

1.4.4.3. Clasificadores – *K-Nearest Neighbours*

El método k-NN es una técnica no paramétrica de clasificación de objetos basado en las muestras de entrenamiento más cercanas del espacio de características. El algoritmo se basa en encontrar los k vecinos más cercanos al objeto para, en función de la cantidad de estos, clasificarlo en el conjunto que tenga un mayor número de muestras cercanas. (Parveen y Thuraisingham, 2006, pp.5-9) En el ejemplo de la Figura 9-1 se analiza para $k=3$ el objeto se clasificaría como triángulo y para $k=5$ como cuadrado.

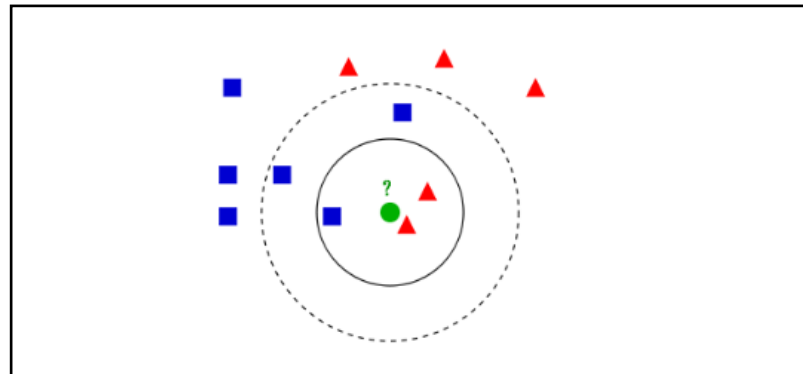


Figura 7-1: Extracción de bloques de imagen facial mediante k-NN.
Fuente: Domínguez Sara, 2017, p.18

1.4.4.4. *Support Vector Machines (SVMs)*

Los SVMs son modelos de aprendizaje usados para clasificación y regresión. El objetivo de este método es el de representar en un espacio una serie de clases y tratar de encontrar un hiperplano que divida ambas clases de una forma óptima, es decir, que la distancia entre ambas sea máxima. El cálculo de este hiperplano depende en gran medida de la distribución de las clases, es por ello, dependiendo de la técnica utilizada para extraer características, los SVMs funcionarán mejor, o en ciertos casos no serán viables. (Cortes y Vapnik, 1995, p.273)

1.4.5. *Software Matlab*

MATLAB es el nombre abreviado de “MATriz LABORatory”. Es un programa para realizar cálculos numéricos con vectores y matrices, y por tanto se puede trabajar también con números escalares (tanto reales como complejos), con cadenas de caracteres y con otras estructuras de información más complejas. Matlab es un lenguaje de alto rendimiento para cálculos técnicos, es al mismo tiempo un entorno y un lenguaje de programación. Uno de sus puntos fuertes es que permite construir nuestras propias herramientas reutilizables. Se puede crear fácilmente nuestras

propias funciones y programas especiales (conocidos como M-archivos) en código Matlab, además de agrupar en Toolbox (también llamadas librerías): colección especializada de M-archivos para trabajar en clases particulares de problemas. Matlab, a parte del cálculo matricial y álgebra lineal, también puede manejar polinomios, funciones, ecuaciones diferenciales ordinarias, gráficos. (Casado Cristina, 2007, p.4)

1.4.5.1. Entorno de trabajo GUIDE – MATLAB

El entorno de trabajo utilizado es la GUIDE de Matlab, un entorno de programación que incluye la facilidad de implementar gráficamente la interfaz de usuario para Apps personalizadas que permiten el control sencillo (mediante uso del ratón) del sistema para el usuario, eliminando la necesidad de aprender un lenguaje de programación y escribir los comandos con el fin de ejecutar una aplicación.

1.4.5.2. MatLab Compiler

MatLab Compiler permite compartir programas de MATLAB como aplicaciones independientes, Mapreduce y Spark, web apps y complementos de Microsoft y Excel, además es posible desplegar aplicaciones y complementos de forma gratuita mediante MATLAB Runtime, que se puede empaquetar con la aplicación o descargarse durante la instalación. Es posible alojar web apps basadas en Matlab mediante las herramientas que proporciona Matlab Compiler.

CAPÍTULO II

2. MARCO METODOLÓGICO

El presente capítulo aborda los diferentes procedimientos realizados para la implementación del sistema de identificación facial, como la distancia entre el usuario y la cámara siendo no mayor a 0.5 metros, el sistema se implementó mediante el método llamado *Eigenfaces*, construido sobre técnicas de análisis de componentes principales (PCA) como mejor opción de acuerdo a la comparación de métodos entre *Fisherfaces* y *Eigenfaces* a menores distancias (Granja Iván, 2018, pp.87-92), además del software necesario para la programación respectiva, los dispositivos necesarios y el tipo de comunicación esencial para el funcionamiento de una cerradura eléctrica implementada en la puerta del laboratorio o bioterio de la Facultad de Ciencias como una innovación en el sistema de seguridad y control de acceso.

2.1. Escenario y variables de correlación

2.1.1. Escenario

Las funciones que realiza el bioterio de la Facultad de Ciencias son la experimentación y reproducir con animales, como las ratas y ratones, así como la estandarización de los reactivos biológicos de los animales de experimentación. Generalmente los químicos utilizados dentro del laboratorio no son peligrosos debido a que utilizan sustancias basadas en el extracto de plantas, los cuales no son tóxicos, a pesar de esto se realiza el aseo continuo del laboratorio, existe protección personal y barreras biológicas de los animales.

Para la elaboración del escenario se realizó un registro durante 5 días, en las cuales se determinó los siguientes parámetros como el peor de los casos basado en el siguiente criterio:

Tabla 1-2: Escenario.

HORARIO	Acción de Registro	Acciones Espontáneas	Personal Autorizado
08:00 – 12:00	15	5	5
12:00 – 14:00	5	5	3
14:00 – 18:00	15	5	5
total	35	15	13

Realizado por: Salinas Santiago, 2019

El bioterio permite la capacidad máxima de aproximadamente 15 personas por lo que se toma como universo a este valor entre docentes, tesisistas, estudiantes y personal en general.

En un día laborable de 8 horas se reconoció 15 veces la acción de registro y 5 acciones espontáneas en el horario de 08:00 – 12:00 por 5 personas autorizadas, mientras que, en el horario de 12:00 – 14:00 se obtuvo 5 acciones de registro y 5 acciones espontáneas por 3 personas autorizadas, finalmente para el horario de 14:00 – 18:00 de manera similar que en la mañana se obtuvieron los mismos resultados concluyendo que la mayor afluencia del personal se encontraba en el horario de 08:00 – 12:00 y 14:00 – 18:00, toda la información indicada en la tabla anterior fue adquirida considerando el peor de los casos.

En conclusión, en un día laborable se obtuvo un total de 50 acciones que fueron realizadas por un personal aproximado de 15 usuarios, es decir, cada persona autorizada realizó en promedio 3 acciones (Registro o Espontáneo), por lo que se procedió a utilizar una población de 15 personas con 3 intentos, además se consideró añadir 5 personas adicionales para la ejecución de pruebas de falsas identificaciones, dando un total de 60 pruebas para evaluar el rendimiento del sistema.

2.1.2. Variables de Correlación

En las pruebas realizadas se determinó que existen diferentes variables de correlación las cuales influían notablemente en el proceso de identificación del sistema, para esto se realizó el control posible de dichas variables siendo las más importantes las siguientes.

2.1.2.1. Luminosidad

Dentro del algoritmo *Eigenfaces*, la luminosidad es el parámetro más importante con respecto al reconocimiento facial y a la detección del rostro para poder procesar la información en el sistema, debido a que el lugar se encontraba expuesto a la luz natural del ambiente de manera considerable se procedió a realizar la implementación de la cámara IP en posición perpendicular a la puerta de control tratando de disminuir el error de contraste al momento de realizar la detección del rostro, manteniendo uniformidad en la iluminación para la elaboración de las pruebas.



Figura 1-2: Implementación de la cámara IP.
Realizado por: Santiago Salinas, 2019

2.1.2.2. Posición

Las posiciones utilizadas para la realización de las pruebas fueron de manera frontal con ligeras variaciones de gestos optado por el estándar propuesto por la normativa ISO/IEC 19794-5.



Figura 2-2: Variaciones faciales.
Realizado por: Santiago Salinas, 2019

2.1.2.3. Distancia

La última variable de correlación es la distancia, la cual fue una medida de 30cm desde la cámara IP hacia el rostro del usuario.



Figura 3-2 Distancia usuario cámara.
Realizado por: Santiago Salinas, 2019

2.2. Metodología

2.2.1. Fundamentos del Análisis de Componentes Principales (PCA)

Se consideró un conjunto de varias imágenes cuyas dimensiones son w pixeles de ancho y h pixeles de alto, entonces el número total de componentes de estas imágenes estaría dado por una matriz de dimensiones $w \cdot h$, si se concatena las filas de esta matriz se logra obtener varios vectores, donde el conjunto de imágenes tendría una representación en el espacio vectorial de la misma dimensión.

De la misma manera si se analiza un conjunto de imágenes de rostros de varios individuos, en relación al caso anterior estas imágenes son similares, donde todos los rostros tienen los mismos elementos situados en el mismo lugar (ojos, nariz, boca), donde los pixeles o componentes están relacionados entre sí, la técnica PCA permite implementar una nueva base de vectores donde es posible generar las imágenes de los rostros logrando una aproximación.

Si se analiza un vector X de dimensión n , donde su media μ está definida por:

$$\mu = E\{X\} \quad (1.2)$$

Ecuación 1-7: Media General de X .

La matriz de covarianza del vector X está dada por Σ_X

$$\Sigma_X = E\{(X - \mu)(X - \mu)'\} = \begin{bmatrix} \sigma_{11}^2 & \sigma_{12}^2 & \dots & \sigma_{1n}^2 \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_{n1}^2 & \sigma_{n2}^2 & \dots & \sigma_{nn}^2 \end{bmatrix} \quad (2.2)$$

Ecuación 2-8: Matriz de Covarianza.

Donde σ_{ij}^2 representa la covarianza entre las componentes i e j del vector X , PCA encuentra los autovectores de X y logra expresar en la menor dimensión posible con toda la información necesaria del vector, logrando ser representado sin error mediante la siguiente combinación lineal.

$$X = \sum_{i=1}^n y_i A_i \quad (3.2)$$

Ecuación 3-9: Combinación Lineal.

Donde los vectores A_i son todos los autovectores de la matriz de covarianza, la cualidad más importante de la representación de X , es que, si se requiere representar con el menor número de componentes posibles, la mejor elección son los m autovectores de la matriz de covarianza con mayores autovalores asociados.

2.2.2. *Eigenfaces y PCA para la representación facial*

Se procedió a encontrar los autovectores de la matriz de covarianza del vector donde el objetivo primordial fue caracterizar un conjunto de N imágenes de rostros en un espacio de menos dimensiones, en el presente proyecto se consideró varias imágenes de rostros (vector X de dimensión $w \cdot h$), además de su vector media (μ), al cual se le aplicó la teoría PCA.

La media del conjunto se estimó a partir de la ecuación:

$$\mu \approx \frac{1}{N} \sum_{i=1}^N X_i \quad (4.2)$$

Ecuación 4-10: Aproximación de la media.

Además, la matriz de covarianza también se estimó a partir de:

$$\Sigma_X \approx \frac{1}{N} \sum_{i=1}^N (X_i - \mu)(X_i - \mu)' \quad (5.2)$$

Ecuación 5-11: Aproximación de la Matriz de Covarianza.

Una vez calculado la matriz de covarianza se procedió a realizar el cálculo de los autovectores, para lo cual existen diversos algoritmos que ayudan a obtener este resultado, pero la implementación de estos planteó un problema, la cantidad de recursos (memoria) necesarios para almacenar la matriz fue demasiado grande, debido a que si los vectores faciales de la base de entrenamiento son de dimensión $w \cdot h$ las dimensiones de la matriz de covarianza estimada serían de dimensiones $w \cdot h$ de ancho por $w \cdot h$ de alto. Por ejemplo, si se utiliza imágenes con dimensiones de $w = 192$ y $h = 192$, el número de elementos de la matriz de covarianza estimada sería de 192^4 , es decir, más de mil millones de elementos lo que se encuentra fuera del alcance de la computadora a implementarse.

Al trabajar con imágenes, los recursos computacionales son exagerados, por lo que Solem J. E. (2012, pp. 40-48) propone un método general y resumido para calcular los autovectores y los

autovalores de la matriz de covarianza, cuyo método se aplicó para el desarrollo del presente trabajo de titulación, el cual consistió en los siguientes pasos:

- Se expresó la matriz M_X para que las imágenes se encuentren en filas y se pueda restar su media.
- Se calculó la matriz de covarianza con un algoritmo preestablecido para que su dimensión ($N \times N$) sea manejable por el computador.
- Se procedió al cálculo de los autovalores (λ) y los autovectores (v) de la matriz de covarianza.
- Finalmente, se determinó el cálculo de la matriz V y se procedió a dividir las columnas por la raíz cuadrada del vector λ elemento a elemento.

$$V = (M_X' \cdot v)' \quad (6.2)$$

Ecuación 5-12: Cálculo matriz V .

Los autovectores fueron las N filas de la matriz obtenida, estos autovectores conseguidos son los únicos que pueden tener un autovalor distinto de cero, es decir, son las únicas que capturan información del vector X siendo fundamentales al momento de realizar el proceso de identificación facial.

Mediante el uso de este método de reducción de dimensiones compacto fue posible caracterizar a los vectores correspondientes al conjunto de imágenes faciales, estos autovectores contienen información útil y es igual al número de vectores linealmente independientes del conjunto de entrenamiento.

2.2.3. Redimensionamiento y comparación de datos

Una vez finalizado el procedimiento anterior, se obtuvo la representación en un espacio de menor dimensión dando como resultado N autovectores o *Eigenfaces* ortonormales con los cuales se logró hallar los N rostros del conjunto de imágenes.

Para realizar el proceso de identificación con el conjunto de imágenes entrenadas se analizó un rostro X , el cual tiene un vector de información Y , para hallar el rostro similar se procedió a calcular el producto escalar debido a que cada eigenface es ortonormal, al haber $N - 1$ eigenfaces la dimensión del vector de datos del rostro a identificar también tiene la misma dimensión.

La principal reducción de dimensionalidad es mediante el uso de los *Eigenfaces* con mayor autovalor asociado, logrando reducir la dimensión de la representación de los rostros sin perder calidad en la representación facial. En resumen, se utilizó una óptima representación posible de

un conjunto de N imágenes de rostros consiguiendo proyectar dichas imágenes sobre los eigenfaces con su mejor autovalor asociado.

2.3. Software de programación

El Software de programación utilizado para la implementación del presente proyecto con licencia estudiantil fue Matlab, ya que es un programa con gran potencial en el cálculo numérico con vectores y matrices muy utilizado en el desarrollo de algoritmos para la identificación facial, por lo que existen diversas librerías y herramientas muy útiles para alcanzar los objetivos de una manera eficiente.

La versión utilizada fue la R2017b, a pesar de que ya existe actualizaciones del lenguaje de programación se recomienda utilizar la versión mencionada o inferiores, debido a que actualmente existen problemas de compatibilidad con las versiones superiores a la R2018x en adelante, no obstante, en un futuro no existiría problema alguno en traspasar el presente trabajo a versiones superiores, ya que a pesar de existe diferencia internamente, la sintaxis es muy similar.

Además, mediante el uso de la técnica de Matlab Compiler se realizó la creación de un programa independiente ejecutable en el ordenador para realizar el respectivo control de acceso al Bioterio.

2.4. Diseño del sistema de identificación facial

Mediante la utilización de las funciones que la herramienta de Matlab nos ofrece se procedió a establecer un diagrama de flujo el cual se puede visualizar en el Gráfico 1-2, en el cual tenemos las siguientes características.

Las siguientes funciones son predeterminadas de Matlab y su funcionamiento esta expresado en la Tabla 2-2:

Tabla 2-2: Funciones predeterminadas de Matlab.

FUNCIÓN	PROCESO
vision.CascadeObjectDetector();	Detección de rostros.
imcrop ();	Recorte de la detección.
rgb2gray ();	Traslado de color a escala de grises.
imresize ();	Redimensionamiento de la imagen
eig ()	Cálculo de los <i>Eigenfaces</i>

Realizado por: Santiago Salinas, 2019

Por otro lado, las descripciones como normalización, proyección y la distancia euclídea se basan en las ecuaciones (2.2), (4.2), (5.2), (1.1) y (2.1), respectivamente, las cuales fueron programadas en Matlab, para mayor detalle ver Anexo A.

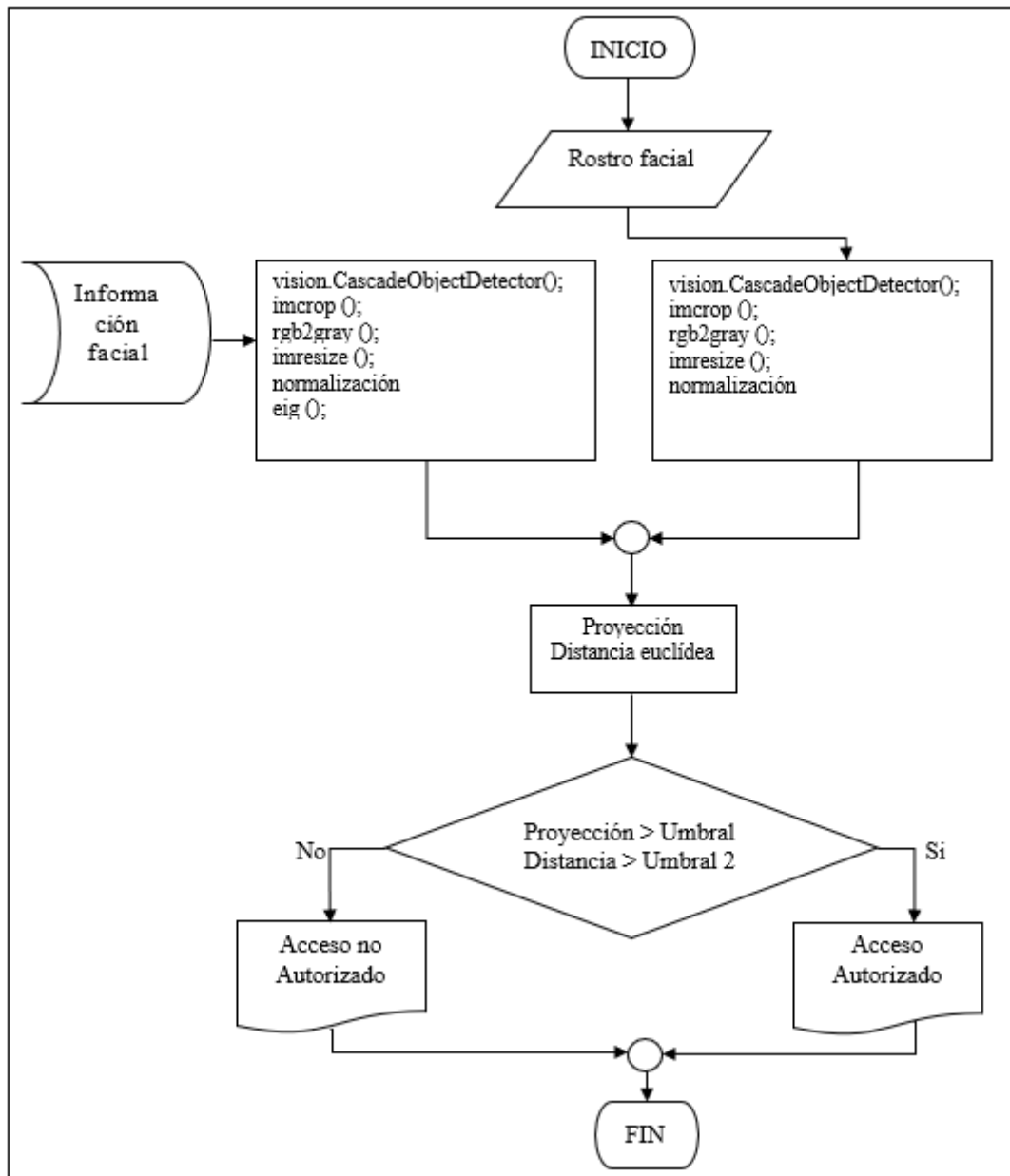


Gráfico 1-2: Diagrama de Flujo del sistema de identificación facial.

Realizado por: Santiago Salinas, 2019

Para que el sistema de identificación facial esté preparado para realizar la fase de comparación y decisión con el rostro de un individuo fue necesario adquirir las características de las imágenes de entrenamiento, para ello se procedió a preparar el sistema en la etapa de entrenamiento para posteriormente en la etapa de identificación se validó el proceso de reconocimiento e identificación del sistema.

2.4.1. Etapa de entrenamiento

En la etapa de entrenamiento se preparó al sistema para obtener los datos de los coeficientes de las imágenes de entrenamiento mediante el método combinado de *PCA – Eigenface* para lo cual se desarrolló mediante el esquema que muestra la Gráfico 2-2.

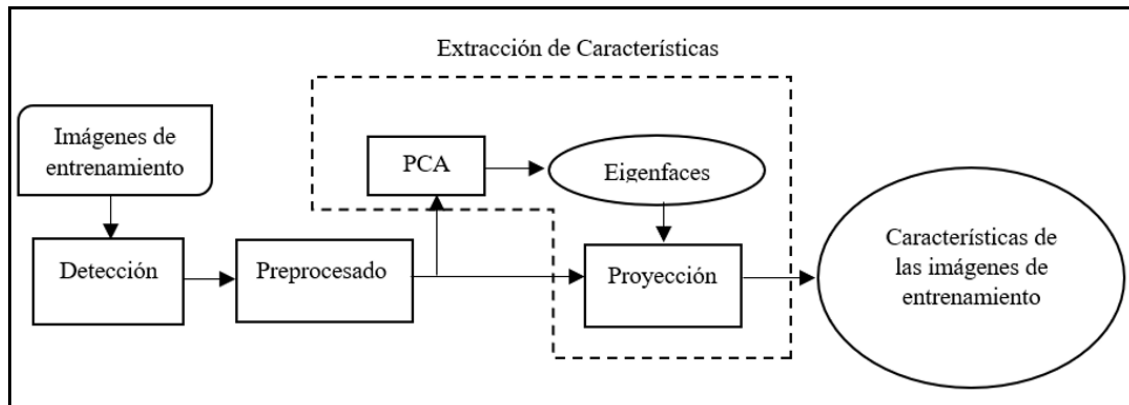


Gráfico 2-2: Esquema de la etapa de entrenamiento.

Realizado por: Santiago Salinas, 2019

2.4.1.1. Imágenes de entrenamiento

Las imágenes de entrenamiento utilizadas para el desarrollo del funcionamiento del algoritmo fueron consideradas con los mismos factores, la posición facial utilizada para adquirir las capturas fue la posición frontal del rostro, la iluminación fue controlada para todas las imágenes, el gesto utilizado fue el de seriedad y finalmente las dimensiones de las imágenes fueron de 70 píxeles de ancho por 70 píxeles de alto de acuerdo a los recursos computacionales del ordenador a implementarse optado por el formato de imagen del estándar ISO/IEC 19795-5, que define un área similar a una foto de carnet. Con estos primeros parámetros establecidos se procedió a realizar los siguientes pasos de la etapa de entrenamiento.

2.4.1.2. Detección

En la siguiente fase de la etapa de entrenamiento se procedió a realizar la detección del rostro de las personas mediante la función que Matlab nos permite usar para la detección de rostros, el cual está basado en el algoritmo de Viola – Jones previamente analizado en el Capítulo I, como se visualiza en la Figura 4-2.



Figura 4-2: Matriz de la etapa de entrenamiento.
Realizado por: Santiago Salinas, 2019

2.4.1.3. Preprocesado

En la fase del preprocesamiento se aplicó la extracción de características del rostro detectado anteriormente, al realizar el preprocesamiento la región del rostro queda completamente visible eliminando el resto de los píxeles para posteriormente realizar las operaciones de ecualización del histograma obteniendo como resultado una imagen ecualizada, como se observa en la Figura 5-2.



Figura 5-2: Matriz principal ecualizada.
Realizado por: Santiago Salinas, 2019

2.4.1.4. Extracción de Características

En la Figura 6-2 se presenta el resultado promedio de la matriz principal ecualizada para el nuevo subespacio, para esto se inicializó aplicando la teoría PCA y posteriormente se determinó las eigenfaces, después se procedió a redimensionar (70x70) cada imagen de entrenamiento preprocesada en un vector para formar una matriz con el fin de obtener dimensiones homogéneas y proceder a obtener la distancia euclídea.



Figura 6-2: Promedio visual.
Realizado por: Santiago Salinas, 2019

Posteriormente se realizó el proceso de diferencia de la matriz promedio con la matriz principal de imágenes ecualizadas, como se observa en la Figura 7-2.



Figura 7-2: Matriz Diferencia.
Realizado por: Santiago Salinas, 2019

Finalmente, para culminar el proceso de extracción de características realizamos el proceso del cálculo de los eigenfaces mediante PCA, como demuestra la Figura 8-2.

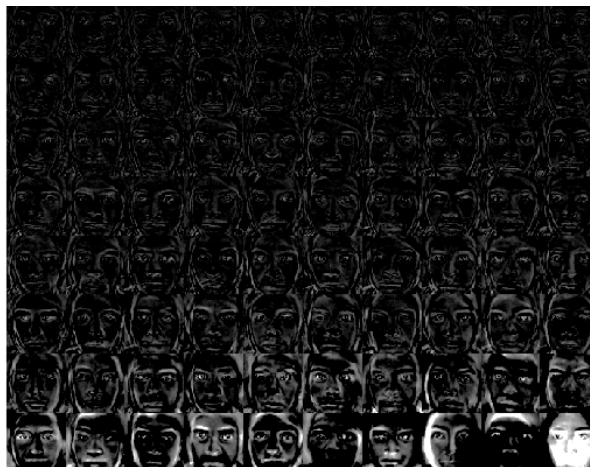


Figura 8-2: Eigenfaces obtenidos.
Realizado por: Santiago Salinas, 2019

De esta manera se obtuvieron las diferentes características de las imágenes de entrenamiento de las 15 personas, las mismas que fueron registradas en la base de datos del sistema de identificación, una vez finalizada la etapa de entrenamiento se procedió a realizar la configuración de la etapa de identificación, en la cual se repiten las etapas de detección, preprocesamiento y extracción de características.

Como siempre será mayor la dimensión de la matriz principal ($70 \times 70 \times n$, donde n es la cantidad de imágenes de entrenamiento) que el número total de imágenes (n), se logró aplicar el método compacto mencionado anteriormente, este método trabajó con la matriz de covarianza de la matriz principal de la etapa de entrenamiento, en donde se obtuvieron los autovectores y autovalores hallando así las eigenfaces.

En la Figura 9-2 se observa la matriz de covarianza, la cual indicó una comparación entre rostros, brindando una escala de colores de mayor intensidad significando alta compatibilidad y menor intensidad significando baja o poca similitud, como en el proceso pruebas se utilizaron a 15 personas de las cuales se obtenía 10 fotos de cada una, la matriz de covarianza realizó una comparación 1:150.

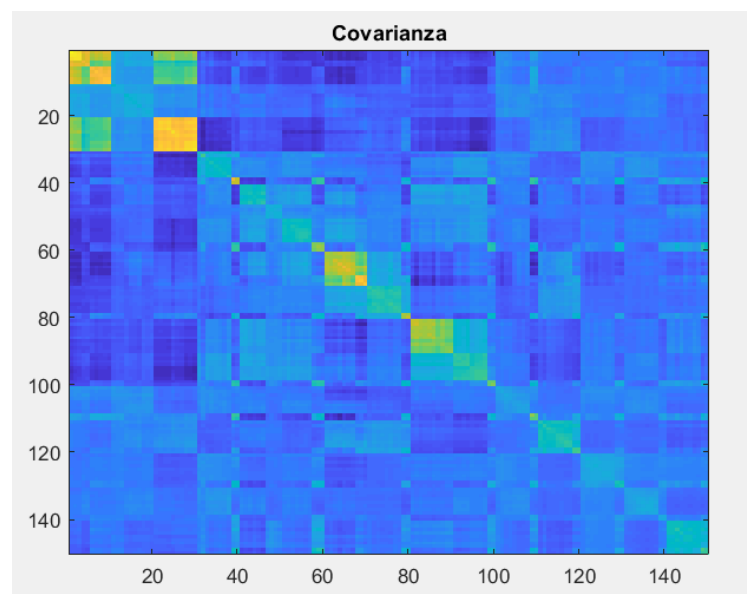


Figura 9-2: Matriz de covarianza.
Realizado por: Santiago Salinas, 2019

2.4.2. Etapa de identificación

Durante la etapa de identificación, se procedió a proyectar la imagen del usuario en la base de datos y se realizó la comparación y decisión para obtener como resultado el rostro identificado. El esquema en el que se basó la etapa de identificación se puede visualizar en la Gráfico 3-2.

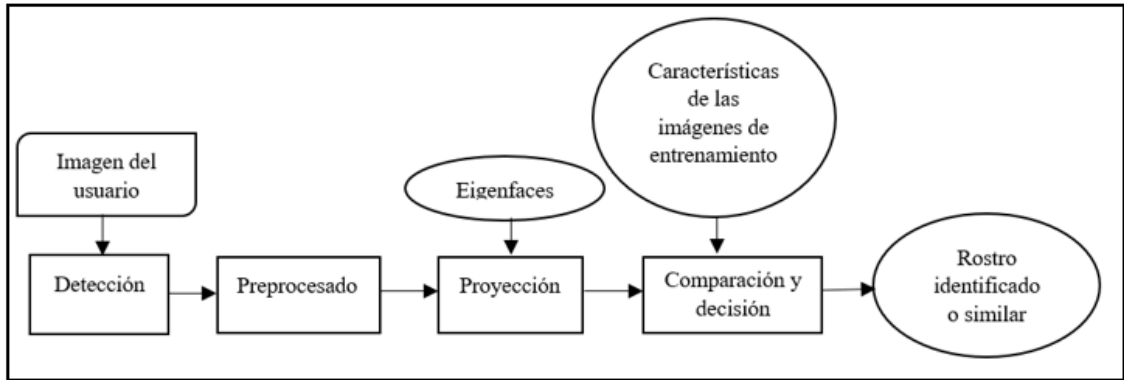


Gráfico 3-2: Esquema de la etapa de identificación.

Realizado por: Santiago Salinas, 2019

2.4.2.1. Imagen de usuario

A diferencia de la etapa de entrenamiento en la etapa de identificación se utilizó una imagen de usuario para realizar el proceso de validación del algoritmo con el respectivo sistema en tiempo real. A esta imagen se le realizó el respectivo proceso para poder identificar si la persona se encontraba o no en la base de datos del sistema.

2.4.2.2. Detección

Al igual que en la etapa de entrenamiento se procedió a realizar la detección del rostro del usuario mediante la herramienta que Matlab nos permite usar para la detección de rostros el cual está basado en el algoritmo de Viola – Jones, como se visualiza en la Figura 10-2.

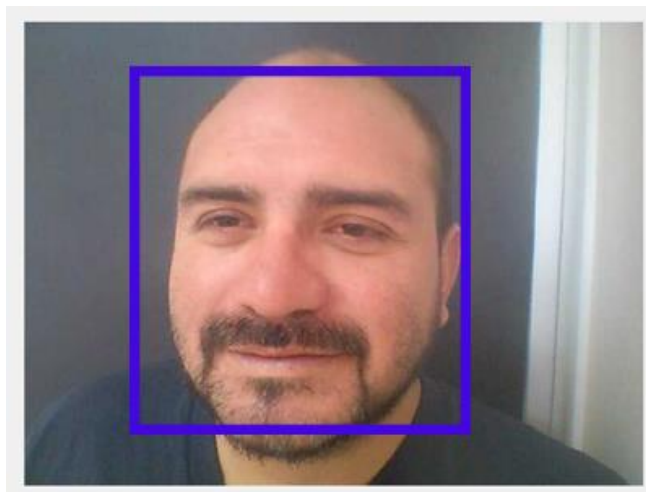


Figura 10-2: Detección de rostro.

Realizado por: Santiago Salinas, 2019

2.4.2.3. Preprocesado

En la fase del preprocesamiento de la etapa de identificación se aplicó la extracción de características del rostro detectado anteriormente, al realizar el preprocesamiento la región del rostro queda completamente visible eliminando el resto del píxeles para posteriormente realizar las operaciones de recorte y ecualización del histograma obteniendo como resultado una imagen ecualizada, esto se debe a que todas las imágenes deben cumplir una misma dimensión o tamaño para realizar la comparación entre ellas, en el caso del presente proyecto se optó por el uso de una dimensión de 70 x 70 píxeles (ancho por alto).

Una vez identificada la persona se procedió a recortar el rostro facial del usuario tal y como se observa en la Figura 11-2.



Figura 11-2: Rostro recortado.
Realizado por: Santiago Salinas, 2019

Posteriormente se realizó el proceso de ecualización del histograma con el objetivo de obtener una imagen a escala de grises lo más uniformemente posible, es decir, que el número de píxeles para cada nivel de gris sea lo más igualado posible logrando reducir los diferentes cambios de luminosidad del ambiente que afectan de manera negativa al algoritmo del sistema.



Figura 12-2: Ecualización del rostro.
Realizado por: Santiago Salinas, 2019

2.4.2.4. Proyección

Para este proceso se realizó la proyección sobre las *Eigenfaces*, en donde como primer paso se procedió a normalizar las imágenes evitando las desiguales, posteriormente se realizó el producto escalar de la imagen detectada preprocesada sobre cada una de las eigenfaces logrando proyectar en el nuevo subespacio los rostros de las imágenes de entrenamiento y de la imagen a identificar para finalmente realizar la comparación y decisión de la persona a identificarse.

2.4.2.5. Comparación y decisión

El último paso para la comparación y decisión fue determinar qué imagen del conjunto de imágenes de entrenamiento es parecida al rostro detectado, para realizar el proceso de selección se procedió a calcular la distancia euclídea con el fin de tomar la mejor decisión de similitud buscando así la proyección que más cerca este de la imagen a identificar.



Figura 13-2: Rostro a identificar.
Realizado por: Santiago Salinas, 2019



Figura 14-2: Rostro con mayor proyección.
Realizado por: Santiago Salinas, 2019

2.5. Interfaz Gráfica

Mediante el uso de la herramienta GUIDE de Matlab se procedió a realizar la programación de una interfaz gráfica en donde se realizó el proceso de ingreso de la imagen de entrada para la identificación, hora de ingreso y si el proceso de identificación y autenticación fue exitoso para acceder al bioterio.



Figura 15-2: Interfaz gráfica general del sistema de identificación.
Realizado por: Santiago Salinas, 2019

Existen 6 principales partes de la interfaz gráfica los cuales son:

- Ingreso a la base de datos
- Indicador de hora y fecha de ingreso
- Botón de reset o reinicio
- Indicador del rostro de la persona a identificarse
- Botón de Inicio para encender la cámara y adquirir la imagen
- Botón de Salida del programa

Al ingresar en la base de datos mediante el botón de ingreso, se obtuvo una nueva interfaz en la cual se realizó el proceso de entrada de información del usuario con autorización de ingreso al laboratorio o bioterio.

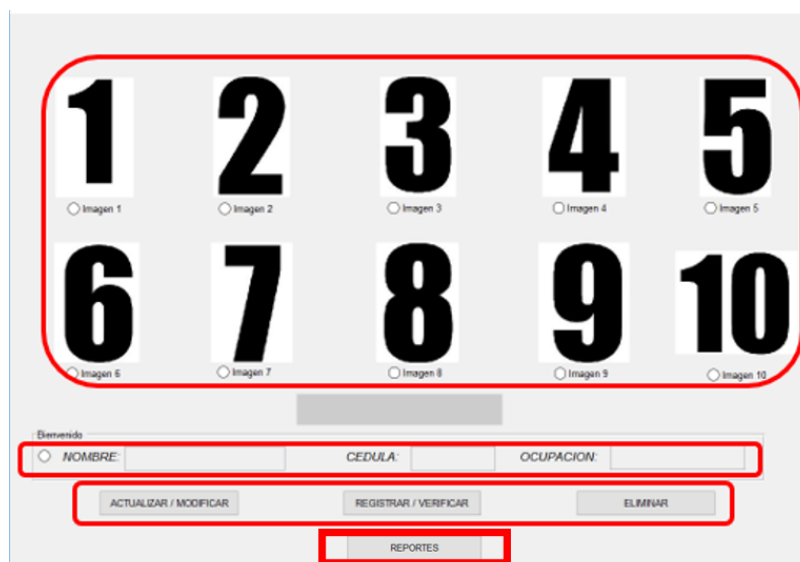


Figura 16-2: Interfaz de ingreso al sistema de identificación.
Realizado por: Santiago Salinas, 2019

El acceso a esta interfaz gráfica está programado para el personal autorizado la cual puede ingresar la información de los usuarios, en la parte superior de la interfaz se debe añadir la captura de 10 imágenes por persona, además del nombre completo, número de cédula y ocupación de la persona, esta información se almacena en una base de datos local dentro del mismo ordenador, además de la posibilidad de generar reportes de acuerdo a la necesidad del administrador.

El personal con acceso a esta interfaz tiene autorización para registrar o verificar a n usuarios en la base de datos, actualizar o modificar la información facial de un usuario o eliminar la información de este.

2.6. Base de datos

El almacenamiento de datos del sistema de identificación se dividió en dos grupos dentro de una misma base, esta información se almacenó en un archivo del formato *.xlsx*, donde los datos se dividieron de la siguiente manera:

2.6.1. Base de datos de control de acceso

En la base de datos de control de acceso se almacenó la información de los usuarios que tienen acceso autorizado para ingresar al bioterio, los parámetros almacenados fueron: número de

cédula, nombre, ocupación, fecha de creación y última fecha de modificación como se puede observar en la Tabla 3-2.

Tabla 3-2: Base de datos de control de acceso.

NUMERO	CEDULA	NOMBRE	OCUPACION	FECHA DE CREACION	ULTIMA FECHA DE MODIFICACION
0	1716456254	BENAJMIN ANDRES ROMAN SANTOS	TECNICO DOCENTE	6/6/2019 10:40	6/6/2019 10:40
1	1718305855	JEAM EDUARDO ALVARADO MENDOZA	TESISTA	6/6/2019 10:42	6/6/2019 10:42
2	0603949694	SEBASTIAN PATRICIO PACHACAMA HUILCA	TESISTA	6/6/2019 10:47	6/6/2019 10:47
3	0202026043	JHALMAR FABRIZIO ESPIN VILLAFUERTE	TESISTA	6/6/2019 10:49	6/6/2019 10:49
4	1804149282	YAHUAIRA ESTEFANIA LANDA LANDA	ESTUDIANTE	6/6/2019 11:00	6/6/2019 11:00
5	0605514546	TATIANA NICOLE OLEAS MORALES	ESTUDIANTE	6/6/2019 11:02	6/6/2019 11:02
6	1104714959	ANAHI KATHERINE CASTRO RIVAS	ESTUDIANTE	6/6/2019 11:04	6/6/2019 11:04
7	0650052616	MARIA BELEN ALLAUCA IGUASNIA	ESTUDIANTE	6/6/2019 11:06	6/6/2019 11:06
8	0605086446	VIVIANA PAMELA PACA LLUAY	ESTUDIANTE	6/6/2019 11:09	6/6/2019 11:09
9	0604563221	NATHALIA SOLEDAD TORRES LOGRONO	ESTUDIANTE	6/6/2019 11:12	6/6/2019 11:12
10	0606208197	ANTHONY JOEL CAYAMBE ASQUI	ESTUDIANTE	6/6/2019 11:20	6/6/2019 11:20
11	1804984910	VANEZA ESTEFANIA BUENAÑO TIPANTASCI	ESTUDIANTE	6/6/2019 11:27	6/6/2019 11:27
12	2200042287	FREDERICK JOSUE ANDRADE BALSECA	ESTUDIANTE	6/6/2019 11:32	6/6/2019 11:32
13	1401243496	JEAN CARLOS TIGRE MARIN	ESTUDIANTE	6/6/2019 11:36	6/6/2019 11:36
14	2300611387	LOURDES LISSETH CALVOPÍÑA VELIZ	ESTUDIANTE	6/6/2019 11:42	6/6/2019 11:42

Realizado por: Santiago Salinas, 2019

2.6.2. Base de Datos de Registro

Para realizar un control de registro de los usuarios con acceso y sin acceso autorizado se procedió a guardar la siguiente información: número de cédula, nombre, ocupación, hora y fecha de registro y si el acceso fue positivo o negativo como se visualiza en la Tabla 4-2.

Tabla 4-2: Base de datos de registro.

NUMERO	CEDULA	NOMBRE	OCUPACION	HORA DE REGISTRO	ACCESO
0	2300611387	LOURDES LISSETH CALVOPÍÑA VELIZ	ESTUDIANTE	6/6/2019 11:44	POSITIVO
1	2300611387	LOURDES LISSETH CALVOPÍÑA VELIZ	ESTUDIANTE	6/6/2019 11:44	POSITIVO
2	1401243496	JEAN CARLOS TIGRE MARIN	ESTUDIANTE	6/6/2019 11:47	POSITIVO
3	1401243496	JEAN CARLOS TIGRE MARIN	ESTUDIANTE	6/6/2019 11:48	POSITIVO
4	1401243496	JEAN CARLOS TIGRE MARIN	ESTUDIANTE	6/6/2019 11:49	POSITIVO
5	0202026043	JHALMAR FABRIZIO ESPIN VILLAFUERTE	TESISTA	6/6/2019 11:52	POSITIVO
6	2200042287	FREDERICK JOSUE ANDRADE BALSECA	ESTUDIANTE	6/6/2019 11:59	POSITIVO
7	2200042287	FREDERICK JOSUE ANDRADE BALSECA	ESTUDIANTE	6/6/2019 12:00	POSITIVO
8				6/6/2019 12:01	NEGADO
9	1804984910	VANEZA ESTEFANIA BUENAÑO TIPANTASCI	ESTUDIANTE	6/6/2019 12:03	POSITIVO
10	1804984910	VANEZA ESTEFANIA BUENAÑO TIPANTASCI	ESTUDIANTE	6/6/2019 12:03	POSITIVO
11	1804984910	VANEZA ESTEFANIA BUENAÑO TIPANTASCI	ESTUDIANTE	6/6/2019 12:04	POSITIVO
12	0606208197	ANTHONY JOEL CAYAMBE ASQUI	ESTUDIANTE	6/6/2019 12:07	POSITIVO
13	0606208197	ANTHONY JOEL CAYAMBE ASQUI	ESTUDIANTE	6/6/2019 12:07	POSITIVO
14				6/6/2019 12:08	NEGADO
15	0604563221	NATHALIA SOLEDAD TORRES LOGRONO	ESTUDIANTE	6/6/2019 12:10	POSITIVO

Realizado por: Santiago Salinas, 2019

Para el caso donde la persona no tiene autorización para ingresar al laboratorio, se realizaron pruebas de ingreso al sistema sin la autorización respectiva, es decir, sin el previo ingreso de la información a la base de datos, una vez realizada la acción de acceso no autorizado el sistema negó automáticamente el ingreso, además de registrarse una imagen de la persona desconocida para el sistema con la fecha y hora del intento.

2.7. Almacenamiento de las imágenes

Para el proceso de comparación y decisión se almacenaron los rostros en el formato de imagen *png*, además se creó un archivo general, el cual contenía dos sub archivos, uno perteneciente a las personas con autorización de ingreso y otro perteneciente a los individuos sin acceso, dentro del archivo de las personas autorizadas se encontrada una carpeta con diez imágenes por cada usuario, las cuales eran utilizadas para el respectivo proceso de identificación del sistema, mientras que en el segundo archivo se encuentra las imágenes de las personas que intentaron acceder al sistema sin tener autorización.

2.8. Sistema eléctrico de control de acceso

Como una innovación en el sistema de seguridad del Bioterio se realizó la implementación de un sistema eléctrico de control de acceso visualizado en la Figura 17-2 cuyo objetivo principal era el manejo de una cerradura eléctrica instalada en la puerta del laboratorio, para realizar este sistema de control se utilizaron los dispositivos electrónicos Arduino Nano y Relé, a continuación, se detalla el procedimiento realizado de este sistema.

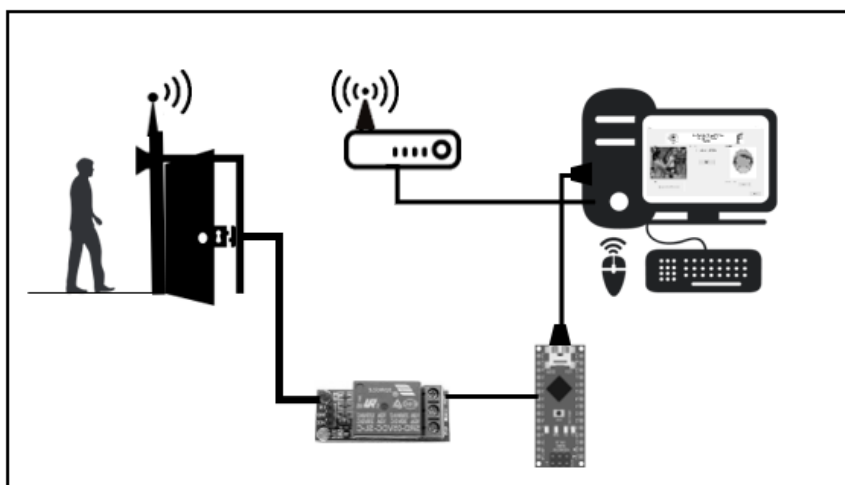


Figura 17-2: Esquema del sistema eléctrico de control de acceso.
Realizado por: Santiago Salinas, 2019

El sistema de identificación da inicio cuando el usuario acciona manualmente mediante un pulsador la ejecución del programa, esta información se envía al computador mediante el dispositivo Arduino, una vez inicializado el sistema, este se conecta inalámbricamente mediante una red LAN a la cámara IP para obtener la imagen del usuario e iniciar el proceso de identificación, cuando el programa ha detectado que la persona identificada tiene autorización se comunica con el sistema eléctrico mediante el Arduino enviando una señal para el accionamiento del relé y de esta manera abrir la cerradura eléctrica.

2.8.1. Cámara IP

Como un método de innovación en el presente proyecto se utilizó una cámara IP mediante la aplicación *IP Webcam* instalada en un teléfono inteligente, para la conexión entre Matlab y la cámara se ingresó la dirección IP dada por la red y de esta manera se estableció la comunicación para posteriormente comenzar con el proceso de identificación del usuario.

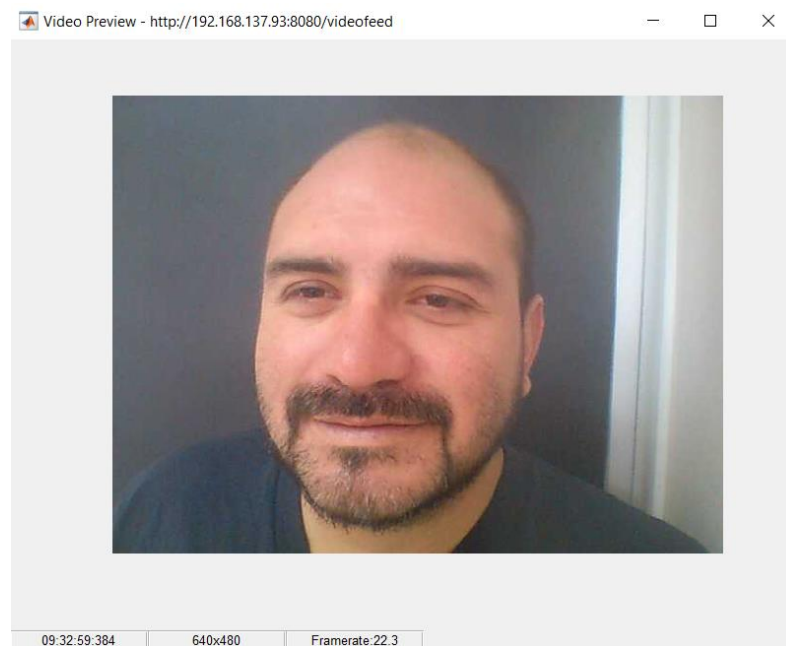


Figura 18-2: Conexión entre Matlab y la Cámara IP.
Realizado por: Santiago Salinas, 2019

2.8.2. Configuración de una red LAN

Durante la implementación del sistema se procedió a configurar una red LAN, la cual mediante el uso de un Router TP – Link WR840N se logró reducir el tiempo de transmisión de datos entre el programa de identificación facial y la cámara IP, obteniendo mejores resultados.



Figura 19-2: Router del sistema.
Realizado por: Santiago Salinas, 2019

2.8.3. *Comunicación entre Matlab y Arduino Nano*

Como primer paso para el control del sistema eléctrico se procedió a la configuración de la comunicación entre MatLab y Arduino, para esto se utilizó la comunicación mediante cable de bus universal en serie o USB, posteriormente se realizó la configuración en el software Matlab instalando los paquetes necesarios para el control del Arduino mediante Matlab, finalmente se procedió a configurar los pines de salida.



Figura 20-2: Comunicación USB.
Realizado por: Santiago Salinas, 2019

Los pines utilizados para el funcionamiento del sistema eléctrico fueron:

- Pin D12: Señal de salida para el control de accionamiento del relé.
- GND y 5V: Pines utilizados para la alimentación del relé.

2.8.4. *Funcionamiento de la cerradura eléctrica*

La comunicación y correcto funcionamiento entre el Arduino y el Relé brindó un excelente funcionamiento de la cerradura eléctrica, para la comunicación entre estos dos dispositivos se procedió a establecer que el sistema eléctrico se active en el modo normalmente abierto del relé, el cual cambiaba de estado cuando la señal de entrada del relé era verdadera y de esta manera enviar el voltaje necesario para la activación de la cerradura.

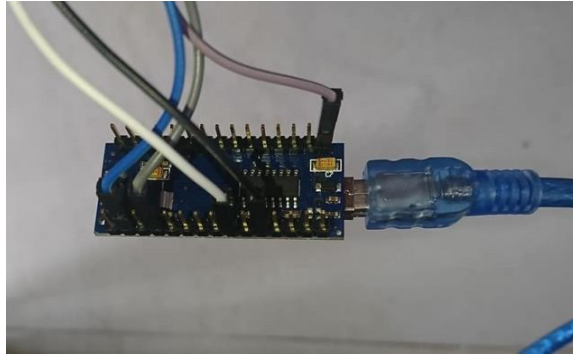


Figura 21-2: Configuración de pines en Arduino.
Realizado por: Santiago Salinas, 2019

La cerradura eléctrica trabaja a una corriente alterna de 12V AC, por lo cual se utilizó un transformador de 110V AC a 12V AC, y para el control de apertura de la cerradura se intercomunicó el transformador con el relé, donde si el pulso era positivo el relé cambiaba de estado logrando enviar el voltaje de 12V AC a la cerradura eléctrica por un intervalo de tiempo de 1 segundo (anteriormente configurado en Matlab) permitiendo así abrir la puerta del bioterio, finalmente el relé cambiaba de estado a normalmente cerrado y de esta manera se posicionaba a esperar una siguiente orden para enviar la señal de accionamiento a la cerradura eléctrica.



Figura 22-2: Cerradura eléctrica.
Realizado por: Santiago Salinas, 2019

De esta manera se logró comunicar el sistema de identificación con el sistema eléctrico para el control de acceso, posteriormente se procedió a verificar el funcionamiento general teniendo éxito en las pruebas realizadas.



Figura 23-2: Montaje final del sistema eléctrico.
Realizado por: Santiago Salinas, 2019

2.9. Presupuesto

En el presente trabajo de titulación se obtuvieron diferentes recursos, siendo el computador el de mayor costo, éste fue otorgado por la Facultad de Ciencias para la implementación del sistema, además se obtuvieron recursos adicionales con sus costos respectivos incluido la mano de obra realizada, los cuales se encuentran detallados en la Tabla 5-2.

Tabla 5-2: Presupuesto.

DESCRIPCIÓN	CANTIDAD	PRECIO
Cerradura eléctrica e infraestructura.	1	\$82
Soporte para cámara IP.	1	\$20
Teléfono inteligente	1	\$100
Sistema electrónico de control (Arduino y Relé)	1	\$10
Router TP – Link WR840N	1	\$30
Parlantes para computadora	1	\$10
Mano de Obra	1	\$60
TOTAL		\$312

Realizado por: Santiago Salinas, 2019

CAPÍTULO III

3. PROCESAMIENTO Y ANÁLISIS DE RESULTADOS

En el presente capítulo se procede a presentar los resultados estadísticos y las condiciones en las que fueron realizadas las diferentes pruebas.

3.1. Procesamiento de pruebas y estimación umbral

Basado en el escenario indicado en el Capítulo II, se realizaron 180 pruebas divididas en 3 días, de los cuales se obtuvieron los siguientes resultados.

Tabla 1-3: Características de la primera prueba.

Día 1: 06 de junio del 2019.	
Luminosidad:	Nublado.
Posición:	Frontal con ligeras variaciones faciales y pequeñas rotaciones de la cabeza.
Distancia:	0.3 m
Usuarios Registrados:	15 usuarios
Usuarios Desconocidos:	5 usuarios
Número total de usuarios:	20 usuarios
Intentos de Registro:	3 intentos
Número total de intentos:	60 intentos
Número de fotos por usuario:	10 fotos
Número total de fotos:	200 fotos
Tamaño del redimensionamiento:	70 x 70 pixeles
Umbral de proyección	0
Umbral de distancia euclídea	Sin consideración

Realizado por: Santiago Salinas, 2019.

De los intentos realizados el 06 de junio de 2019 con las características mencionadas en la Tabla 1-3, se indica los resultados en la Tabla 2-3 en donde se representa con 1 si el sistema identificó satisfactoriamente al usuario registrado, por otro lado, el 0 indica que el sistema no identificó al usuario registrado, y finalmente, en los espacios donde se encuentra un guion (-) son intentos en los cuales el sistema procedió a confundir al usuario con otro de la misma base de datos. Además de realizar las respectivas pruebas se realizaron reingresos a la base de datos debido a posiciones

faciales no válidas para el sistema, de esta manera se obtuvieron mejores resultados mostrados en la evaluación.

Tabla 2-3: Intentos de los usuarios registrados de la primera prueba.

USUARIOS REGISTRADOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	1	1	1
USUARIO 2	1	1	1
USUARIO 3	1	1	1
USUARIO 4	1	1	0
USUARIO 5	1	1	1
USUARIO 6	1	1	0
USUARIO 7	1	1	1
USUARIO 8	1	1	0
USUARIO 9	1	1	1
USUARIO 10	0	0	-
USUARIO 11	-	-	1
USUARIO 12	1	1	1
USUARIO 13	1	0	1
USUARIO 14	0	0	0
USUARIO 15	1	1	1
INTENTOS TOTALES	15	15	15

Realizado por: Santiago Salinas, 2019.

En el primer intento se determinó que, existieron 12 registros con éxito en la identificación correspondiente al 80%, 2 identificaciones sin éxito correspondiente al 13% y finalmente un registro confuso correspondiente al 7%, como indica el Gráfico 1-3.

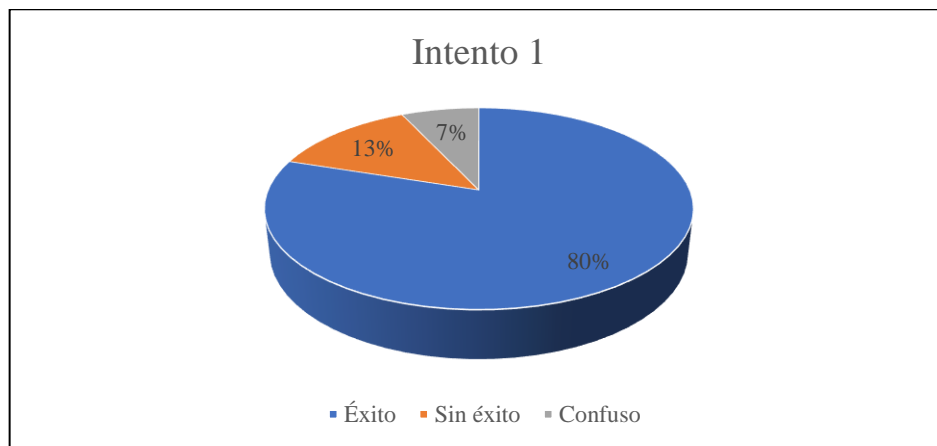


Gráfico 1-3: Resultados del intento uno de los usuarios registrados.

Realizado por: Santiago Salinas, 2019.

En el segundo intento se determinó que, existieron 11 registros con éxito en la identificación correspondiente al 73%, 3 identificaciones sin éxito correspondiente al 20% y finalmente un registro confuso correspondiente al 7%, como indica el Gráfico 2-3.

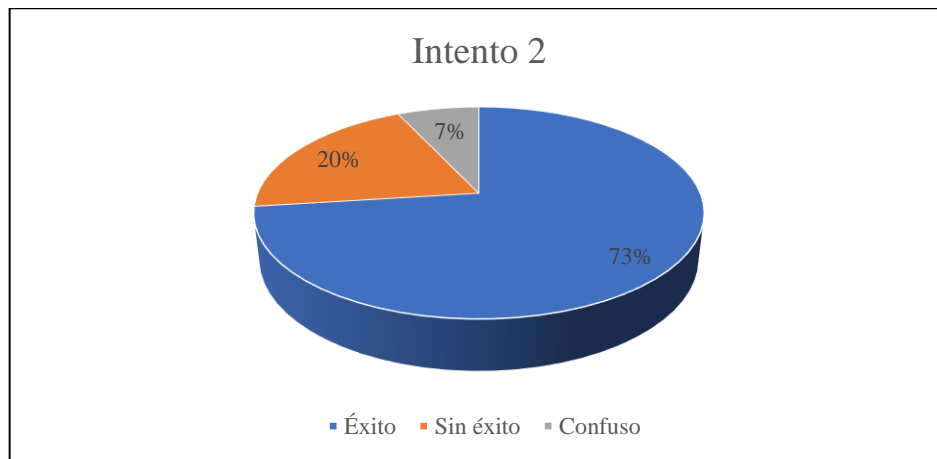


Gráfico 2-3: Resultados del intento dos de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

En el tercer intento se determinó que, existieron 10 registros con éxito en la identificación correspondiente al 66%, 4 identificaciones sin éxito correspondiente al 27% y finalmente un registro confuso correspondiente al 7%, como indica el Gráfico 3-3.

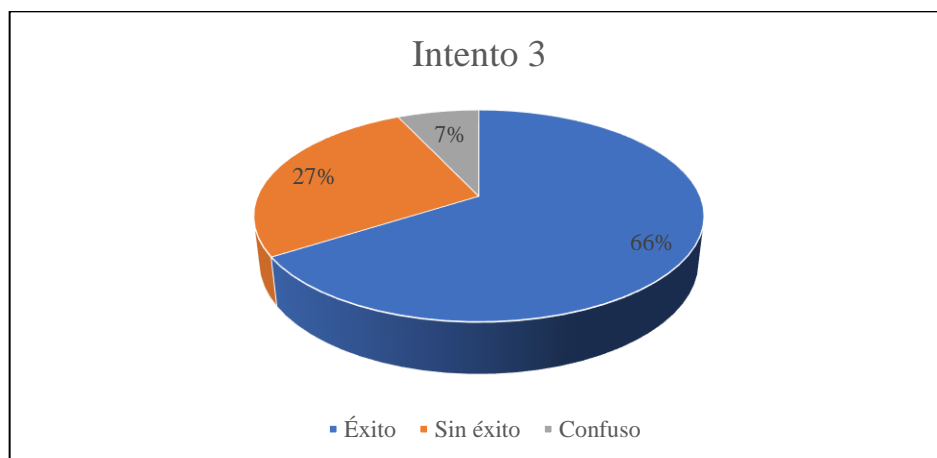


Gráfico 3-3: Resultados del intento tres de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

Del total de la primera prueba correspondiente a 45 registros perteneciente a los usuarios registrados se determinó un total de 33 registros con éxito correspondiente al 73%, además de 9 identificaciones sin éxito correspondiente al 20% y finalmente 3 registros confusos correspondiente al 7%, como indica el Gráfico 4-3.

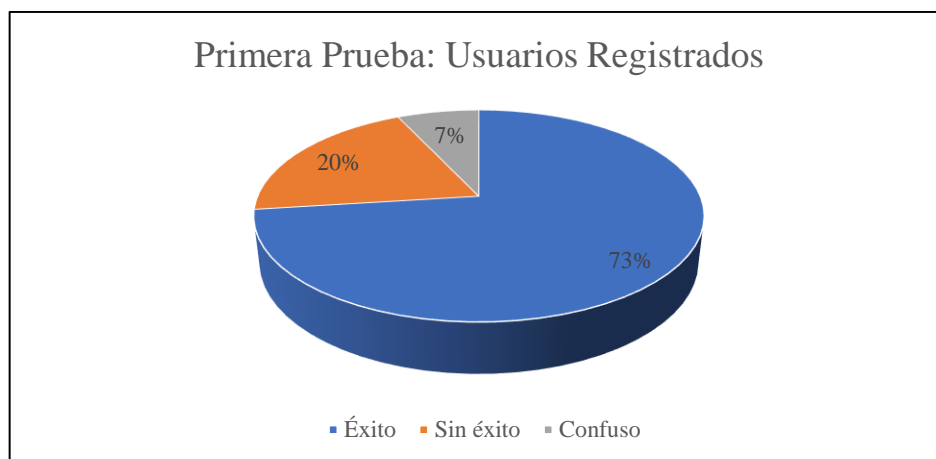


Gráfico 4-3: Resultados de los usuarios registrados de la primera prueba.
Realizado por: Santiago Salinas, 2019.

De manera similar se realizaron las pruebas para los usuarios desconocidos, en donde se representa con 1 si el sistema identificó al usuario desconocido, con 0 si el sistema no identificó al usuario y finalmente con un guion si el sistema procedió a confundir al usuario desconocido con un usuario registrado en la base de datos.

Tabla 3-3: Intentos de los usuarios desconocidos de la primera prueba.

USUARIOS DESCONOCIDOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	0	0	0
USUARIO 2	0	0	0
USUARIO 3	0	0	0
USUARIO 4	0	0	0
USUARIO 5	0	0	0
INTENTOS TOTALES	5	5	5

Realizado por: Santiago Salinas, 2019.

En el primer intento se determinó que, existieron 5 registros de identificaciones sin éxito correspondiente al 100%, cero identificaciones con éxito y cero registros confusos correspondiente al 0%, como indica el Gráfico 5-3.



Gráfico 5-3: Resultados del intento uno de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

En el segundo intento se determinó que, existieron 5 registros de identificaciones sin éxito correspondiente al 100%, cero identificaciones con éxito y cero registros confusos correspondiente al 0%, como indica el Gráfico 6-3.

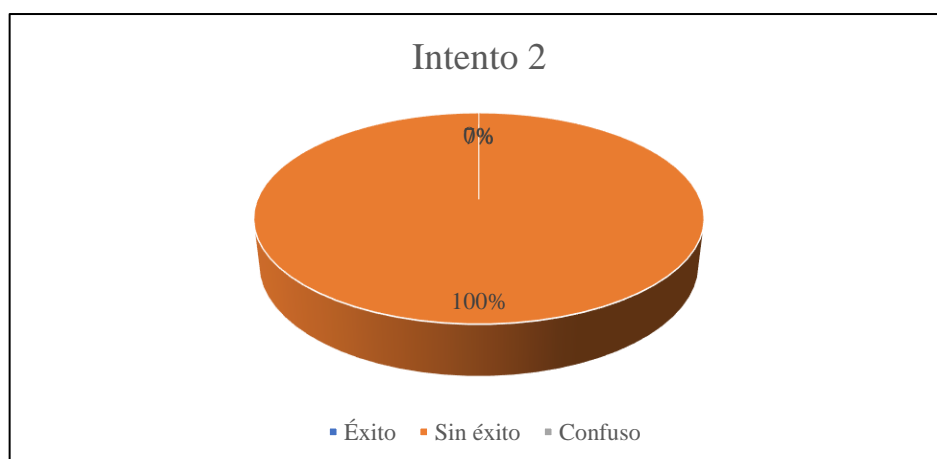


Gráfico 6-3: Resultados del intento dos de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

En el tercer intento se determinó que, existieron 5 registros de identificaciones sin éxito correspondiente al 100%, cero identificaciones con éxito y cero registros confusos correspondiente al 0%, como indica el Gráfico 7-3.



Gráfico 7-3: Resultados del intento tres de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

Del total de la primera prueba correspondiente a 15 registros perteneciente a los usuarios desconocidos se determinó un total de 15 registros sin éxito correspondiente al 100%, además de 0 identificaciones con éxito y 0 registros confusos correspondientes al 0%, como indica el Gráfico 8-3.

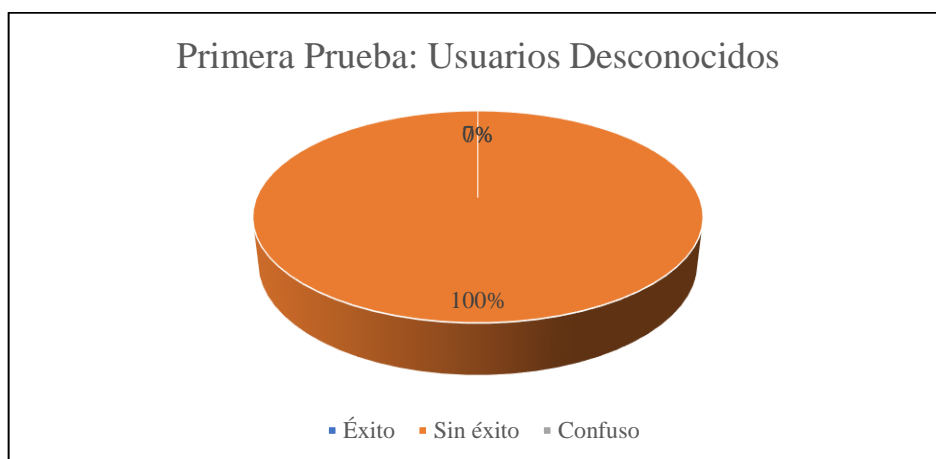


Gráfico 8-3: Resultados de los usuarios registrados de la primera prueba.
Realizado por: Santiago Salinas, 2019.

En conclusión, de la primera prueba se obtuvieron los siguientes resultados generales, tanto para usuarios registrados como para usuarios desconocidos, en la primera prueba se tuvieron 48 registros eficientes correspondiente al 80% de un total de 60 registros, además se tuvo 9 registros negados a usuarios registrados correspondiente al 15% y finalmente 3 registros confusos correspondientes al 5% de un total de 60 registros, para un clima nublado con un umbral de proyección de cero y sin considerar el umbral para la distancia euclídea.



Gráfico 9-3: Resultados generales de la primera prueba.
Realizado por: Santiago Salinas, 2019.

De las pruebas realizadas anteriormente se procedió a almacenar las proyecciones y las distancias euclídeas de cada registro para mejorar el rendimiento del sistema de identificación obteniendo los siguientes resultados.

Tabla 4-3: Proyecciones y distancias euclídeas obtenidas en la primera prueba.

ACCIÓN	PROYECCIÓN	DISTANCIA EUCLÍDEA
ÉXITO	0.79	267.97
SIN ÉXITO	-1.58	364.37
CONFUSO	0.89	273.09

Realizado por: Santiago Salinas, 2019.

De acuerdo con las proyecciones y distancias euclídeas obtenidas en la primera prueba se procedió a realizar nuevas pruebas con la consideración de un umbral de proyección de 0.79 y un umbral para la distancia euclídea de 267.97, además de otras características especificadas en la Tabla 5-3.

Tabla 5-3: Características de la segunda prueba.

Día 2: 11 de junio del 2019.	
Luminosidad:	Parcialmente Nublado.
Posición:	Frontal con ligeras variaciones faciales y pequeñas rotaciones de la cabeza.
Distancia:	0.3 m
Usuarios Registrados:	15 usuarios
Usuarios Desconocidos:	5 usuarios
Número total de usuarios:	20 usuarios
Intentos de Registro:	3 intentos
Número total de intentos:	60 intentos
Número de fotos por usuario:	10 fotos
Número total de fotos:	200 fotos
Tamaño del redimensionamiento:	70 x 70 pixeles
Umbral de proyección	0.79
Umbral de distancia euclídea	267.97

Realizado por: Santiago Salinas, 2019.

De los intentos realizados el 11 de junio de 2019 con las características mencionadas en la Tabla 5-3, se indica los resultados en la Tabla 6-3 en donde se representa con 1 si el sistema identificó satisfactoriamente al usuario registrado, por otro lado, el 0 indica que el sistema no identificó al usuario registrado, y finalmente, en los espacios donde se encuentra un guion (-) son intentos en los cuales el sistema procedió a confundir al usuario con otro de la misma base de datos.

Tabla 6-3: Intentos de los usuarios registrados de la segunda prueba.

USUARIOS REGISTRADOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	1	1	1
USUARIO 2	1	1	1
USUARIO 3	1	1	1
USUARIO 4	1	1	0
USUARIO 5	1	1	1
USUARIO 6	1	1	0
USUARIO 7	1	1	1
USUARIO 8	1	1	0
USUARIO 9	1	1	1
USUARIO 10	1	-	1
USUARIO 11	1	-	1
USUARIO 12	1	1	1
USUARIO 13	1	0	1
USUARIO 14	1	1	0
USUARIO 15	1	1	1
INTENTOS TOTALES	15	15	15

Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento uno se determinó que, existieron 15 registros con éxito correspondiente al 100%, 0 registros sin éxito y 0 registros confusos correspondientes al 0%, como indica el Gráfico 10-3.

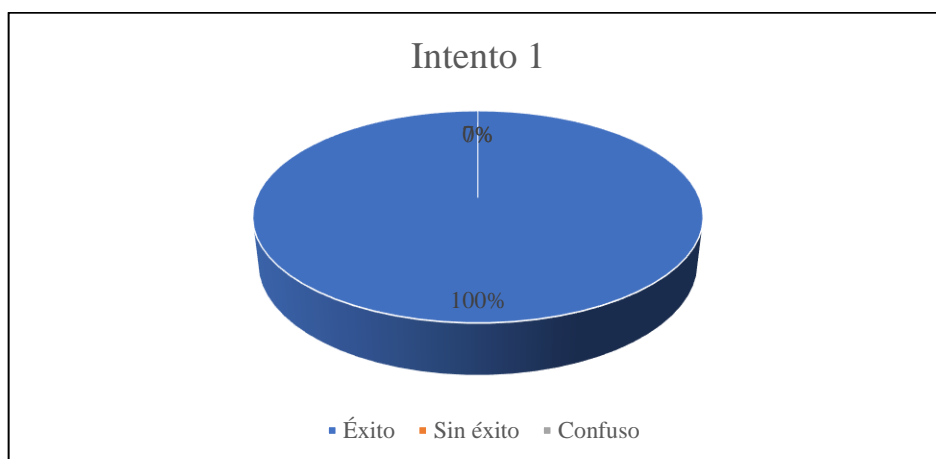


Gráfico 10-3: Resultados del intento uno de los usuarios registrados.

Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento dos se determinó que, existieron 12 registros con éxito correspondiente al 80%, 1 registro sin éxito correspondiente al 7% y finalmente 2 registros confusos correspondiente al 13%, como indica el Gráfico 11-3.

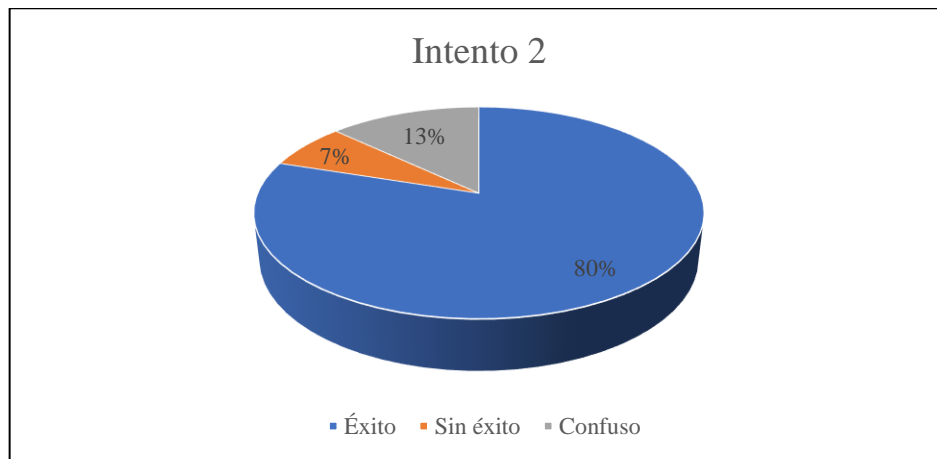


Gráfico 11-3: Resultados del intento dos de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento tres se determinó que, existieron 11 registros con éxito correspondiente al 73%, 4 registros sin éxito correspondiente al 27% y finalmente 0 registros confusos correspondiente al 0%, como indica el Gráfico 12-3.

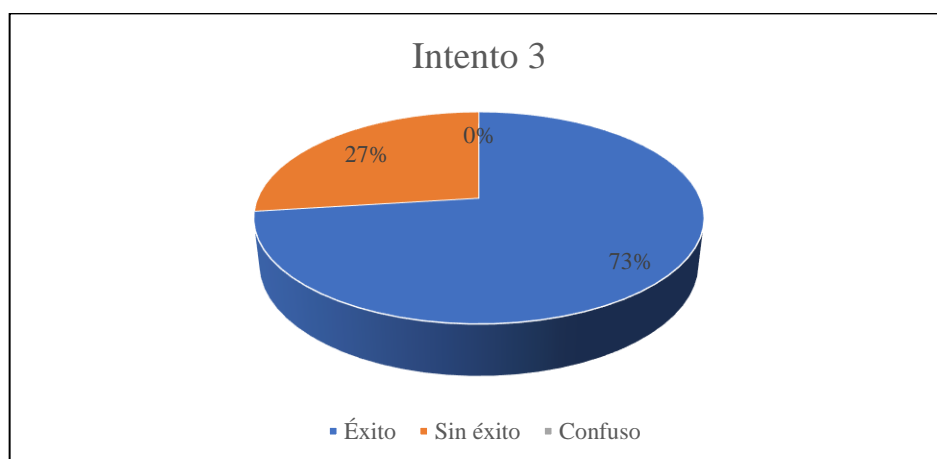


Gráfico 12-3: Resultados del intento tres de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

Del total de la segunda prueba correspondiente a 45 registros perteneciente a los usuarios registrados se determinó un total de 38 registros con éxito correspondiente al 84%, además de 5 registros sin éxito correspondiente al 12% y finalmente 2 registros confusos correspondiente al 4%, como indica el Gráfico 13-3.

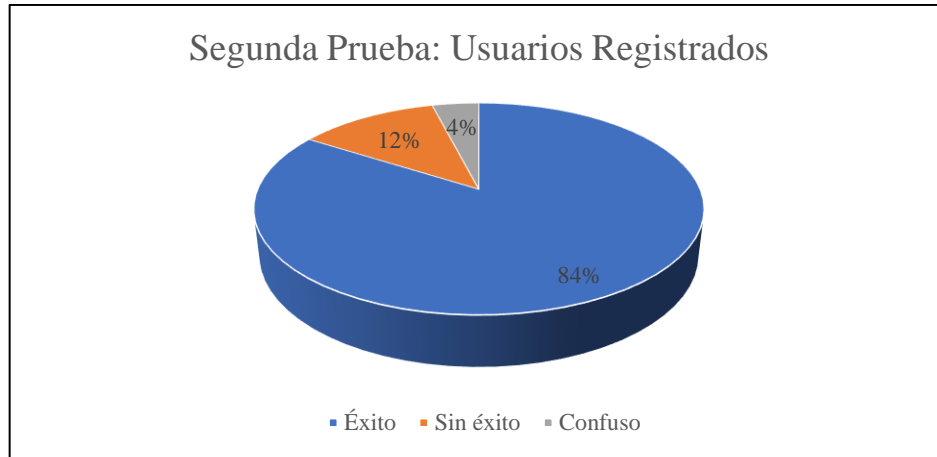


Gráfico 13-3: Resultados de los usuarios registrados de la segunda prueba.
Realizado por: Santiago Salinas, 2019.

De manera similar se realizaron las pruebas para los usuarios desconocidos, en donde se representa con 1 si el sistema identificó al usuario desconocido, con 0 si el sistema no identificó al usuario y finalmente con un guion (-) si el sistema procedió a confundir al usuario desconocido con un usuario registrado en la base de datos.

Tabla 7-3: Intentos de los usuarios desconocidos de la segunda prueba.

USUARIOS DESCONOCIDOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	0	0	0
USUARIO 2	0	0	0
USUARIO 3	0	0	0
USUARIO 4	0	0	0
USUARIO 5	0	0	0
INTENTOS TOTALES	5	5	5

Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento uno se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 14-3.



Gráfico 14-3: Resultados del intento uno de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento dos se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 15-3.

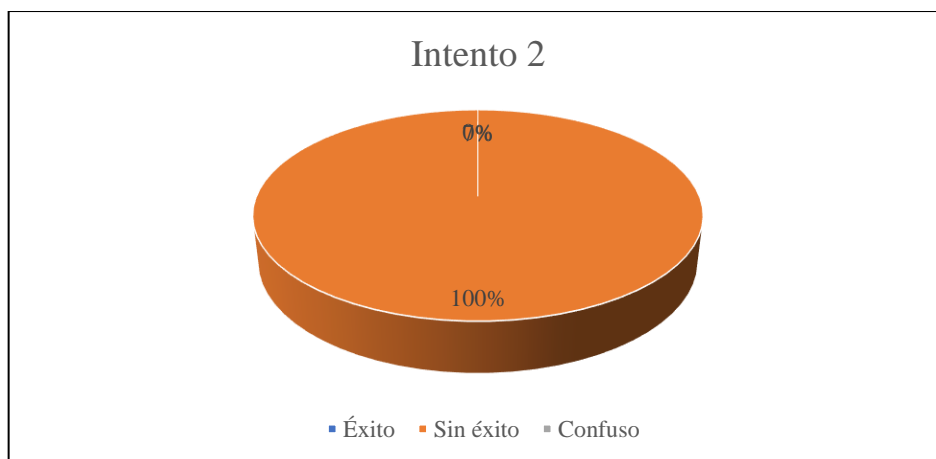


Gráfico 15-3: Resultados del intento dos de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento dos se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 16-3.



Gráfico 16-3: Resultados del intento tres de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

Del total de la segunda prueba correspondiente a 15 registros perteneciente a los usuarios desconocidos se determinó un total de 15 registros sin éxito correspondiente al 100%, además de 0 registros con éxito y 0 registros confusos correspondientes al 0%, como indica el Gráfico 17-3.

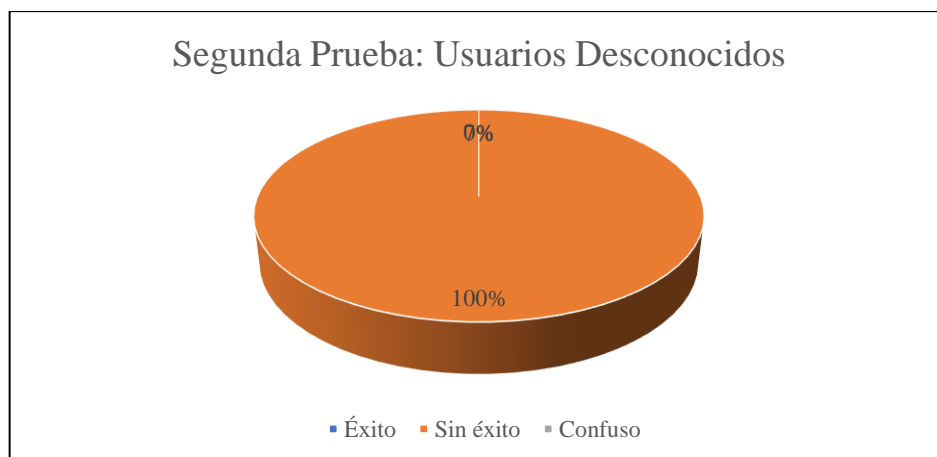


Gráfico 17-3: Resultados de los usuarios registrados de la segunda prueba.
Realizado por: Santiago Salinas, 2019.

En conclusión, de la segunda prueba se obtuvieron los siguientes resultados generales, tanto para usuarios registrados como para usuarios desconocidos, en la segunda prueba se tuvieron 53 registros eficientes correspondiente al 89% de un total de 60 registros, además se tuvo 5 registros negados a usuarios registrados correspondiente al 8% y finalmente 2 registros confusos correspondientes al 3% de un total de 60 registros, para un clima parcialmente nublado con un umbral de proyección de 0.79 y un umbral de 267.97 para la distancia euclídea.



Gráfico 18-3: Resultados generales de la segunda prueba.
Realizado por: Santiago Salinas, 2019.

De las pruebas realizadas anteriormente se procedió a almacenar las proyecciones y distancias euclídeas observadas en la Tabla 8-3.

Tabla 8-3: Proyecciones y distancias euclídeas obtenidas en la segunda prueba.

ACCIÓN	PROYECCIÓN	DISTANCIA EUCLÍDEA
ÉXITO	0.83	280.47
SIN ÉXITO	-1.65	384.73
CONFUSO	0.78	283.02

Realizado por: Santiago Salinas, 2019.

Finalmente se procedió a realizar la última prueba añadiendo los últimos resultados de los umbrales al sistema.

De acuerdo con las proyecciones y distancias euclídeas obtenidas en la segunda prueba se procedió a realizar nuevas pruebas con la consideración de un umbral de proyección de 0.83 y un umbral para la distancia euclídea de 280.47, además de otras características especificadas en la Tabla 9-3.

Tabla 9-3: Características de la tercera prueba.

Día 3: 13 de junio del 2019.	
Luminosidad:	Soleado.
Posición:	Frontal con ligeras variaciones faciales y pequeñas rotaciones de la cabeza.
Distancia:	0.3 m
Usuarios Registrados:	15 usuarios
Usuarios Desconocidos:	5 usuarios
Número total de usuarios:	20 usuarios
Intentos de Registro:	3 intentos
Número total de intentos:	60 intentos
Número de fotos por usuario:	10 fotos
Número total de fotos:	200 fotos
Tamaño del redimensionamiento:	70 x 70 pixeles
Umbral de proyección	0.83
Umbral de distancia euclídea	280.47

Realizado por: Santiago Salinas, 2019.

De los intentos realizados el 13 de junio de 2019 con las características mencionadas en la Tabla 9-3, se indica los resultados en la Tabla 10-3 en donde se representa con 1 si el sistema identificó satisfactoriamente al usuario registrado, por otro lado, el 0 indica que el sistema no identificó al usuario registrado, y finalmente, en los espacios donde se encuentra un guion (-) son intentos en los cuales el sistema procedió a confundir al usuario con otro de la misma base de datos.

Tabla 10-3: Intentos de los usuarios registrados de la tercera prueba.

USUARIOS REGISTRADOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	1	1	1
USUARIO 2	1	1	1
USUARIO 3	1	1	0
USUARIO 4	1	1	1
USUARIO 5	1	1	1
USUARIO 6	1	1	1
USUARIO 7	1	1	1
USUARIO 8	1	-	1
USUARIO 9	1	1	1
USUARIO 10	1	1	1
USUARIO 11	1	1	1
USUARIO 12	1	1	1
USUARIO 13	1	0	1
USUARIO 14	1	1	1
USUARIO 15	0	1	1
INTENTOS TOTALES	15	15	15

Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento uno se determinó que, existieron 14 registros con éxito correspondiente al 93%, 1 registros sin éxito correspondiente al 7% y 0 registros confusos correspondientes al 0%, como indica el Gráfico 19-3.

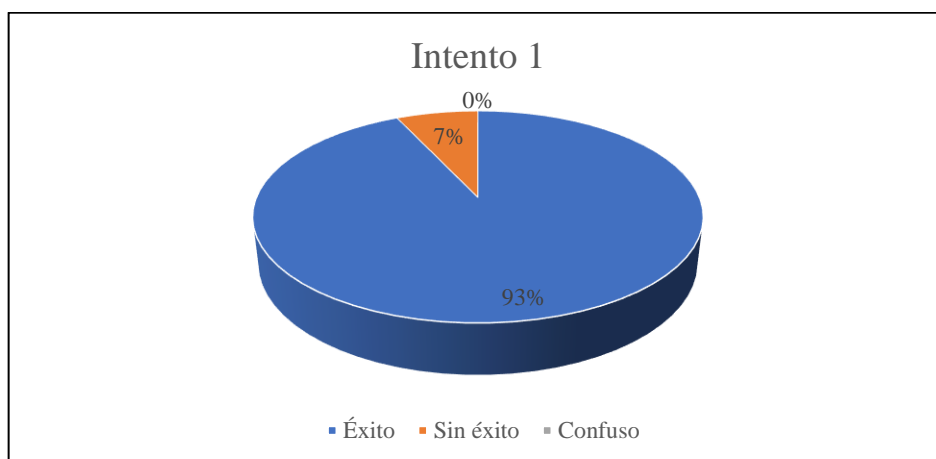


Gráfico 19-3: Resultados del intento uno de los usuarios registrados.

Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento dos se determinó que, existieron 13 registros con éxito correspondiente al 86%, 1 registro sin éxito correspondiente al 7% y finalmente 1 registro confuso correspondiente al 7%, como indica el Gráfico 20-3.

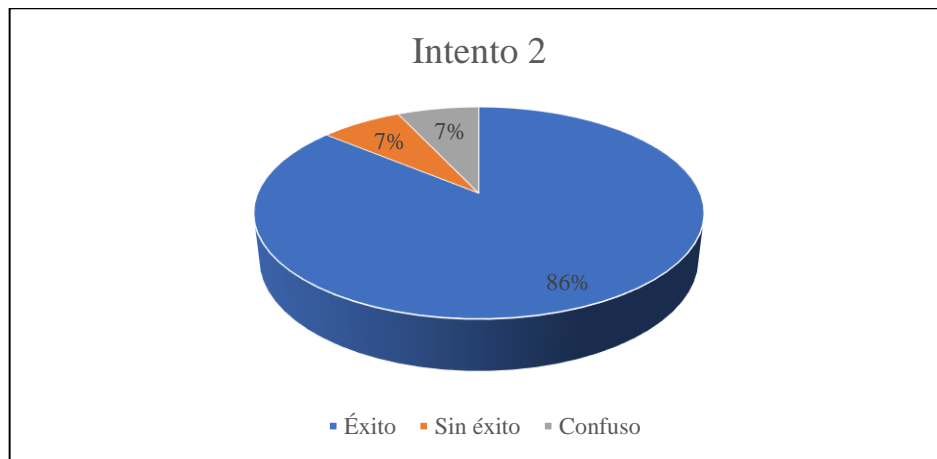


Gráfico 20-3: Resultados del intento dos de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

De un total de 15 registros realizados en el intento tres se determinó que, existieron 14 registros con éxito correspondiente al 93%, 1 registro sin éxito correspondiente al 7% y finalmente 0 registros confusos correspondiente al 0%, como indica el Gráfico 21-3.

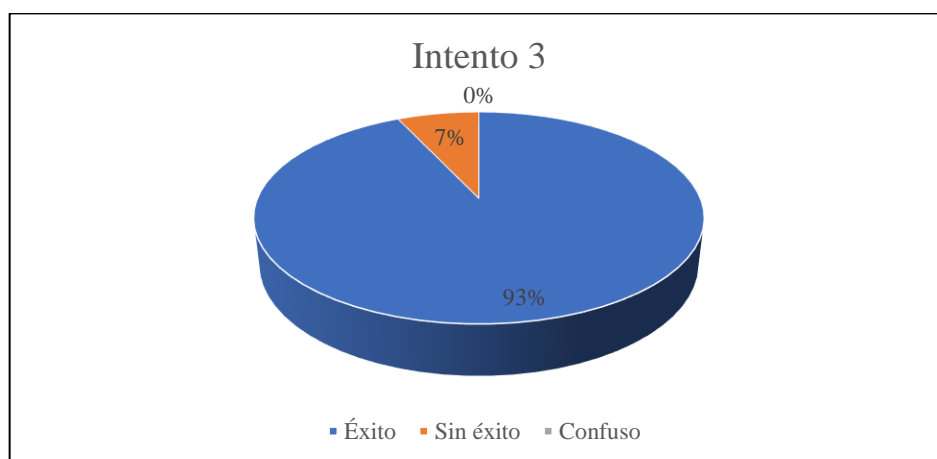


Gráfico 21-3: Resultados del intento tres de los usuarios registrados.
Realizado por: Santiago Salinas, 2019.

Del total de la tercera prueba correspondiente a 45 registros perteneciente a los usuarios registrados se determinó un total de 41 registros con éxito correspondiente al 91%, además de 3 registros sin éxito correspondiente al 7% y finalmente 1 registro confuso correspondiente al 2%, como indica el Gráfico 22-3.

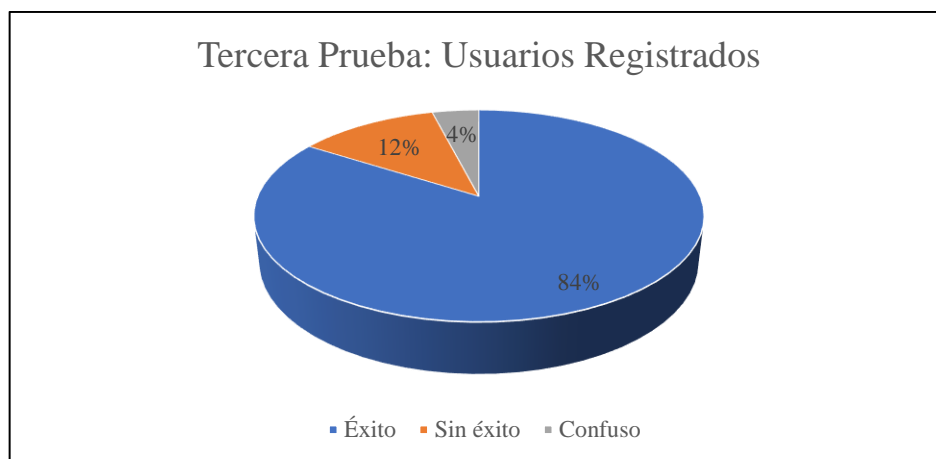


Gráfico 22-3: Resultados de los usuarios registrados de la tercera prueba.
Realizado por: Santiago Salinas, 2019.

De manera similar se realizaron las pruebas para los usuarios desconocidos, en donde se representa con 1 si el sistema identificó al usuario desconocido, con 0 si el sistema no identificó al usuario y finalmente con un guion (-) si el sistema procedió a confundir al usuario desconocido con un usuario registrado en la base de datos.

Tabla 11-3: Intentos de los usuarios desconocidos de la tercera prueba.

USUARIOS DESCONOCIDOS	INTENTO 1	INTENTO 2	INTENTO 3
USUARIO 1	0	0	0
USUARIO 2	0	0	0
USUARIO 3	0	0	0
USUARIO 4	0	0	0
USUARIO 5	0	0	0
INTENTOS TOTALES	5	5	5

Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento uno se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 23-3.



Gráfico 23-3: Resultados del intento uno de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento dos se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 24-3.

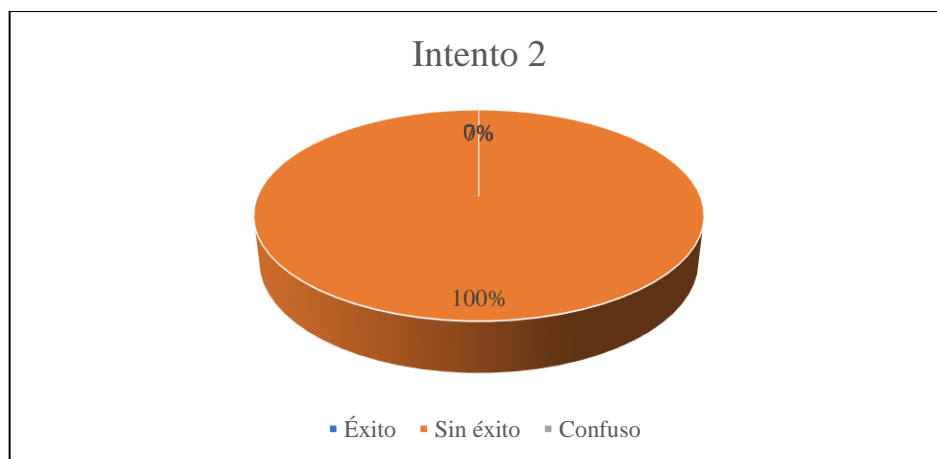


Gráfico 24-3: Resultados del intento dos de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

De un total de 5 registros realizados en el intento dos se determinó que, existieron 5 registros sin éxito correspondiente al 100%, 0 registros con éxito y 0 registros confusos correspondiente al 0%, como indica el Gráfico 25-3.



Gráfico 25-3: Resultados del intento tres de los usuarios desconocidos.
Realizado por: Santiago Salinas, 2019.

Del total de la tercera prueba correspondiente a 15 registros perteneciente a los usuarios desconocidos se determinó un total de 15 registros sin éxito correspondiente al 100%, además de 0 registros con éxito y 0 registros confusos correspondientes al 0%, como indica el Gráfico 26-3.



Gráfico 26-3: Resultados de los usuarios registrados de la tercera prueba.
Realizado por: Santiago Salinas, 2019.

En conclusión, de la tercera prueba se obtuvieron los siguientes resultados generales, tanto para usuarios registrados como para usuarios desconocidos, en la tercera prueba se tuvieron 56 registros eficientes correspondiente al 93% de un total de 60 registros, además se tuvo 3 registros negados a usuarios registrados correspondiente al 6% y finalmente 1 registro confuso correspondiente al 1% de un total de 60 registros, para un clima soleado con un umbral de proyección de 0.83 y un umbral de 280.47 para la distancia euclídea.



Gráfico 27-3: Resultados generales de la tercera prueba.
Realizado por: Santiago Salinas, 2019.

De las pruebas realizadas anteriormente se procedió a almacenar las proyecciones y distancias euclídeas observadas en la Tabla 12-3.

Tabla 12-3: Proyecciones y distancias euclídeas obtenidas en la tercera prueba.

ACCIÓN	PROYECCIÓN	DISTANCIA EUCLÍDEA
ÉXITO	0.88	268.15
SIN ÉXITO	-1.85	395.17
CONFUSO	0.79	283.45

Realizado por: Santiago Salinas, 2019.

3.2. Evaluación del sistema de identificación facial

Una vez culminado la ejecución de las pruebas se obtuvo la siguiente evaluación final, mostrada en la Tabla 13-3.

Tabla 13-3: Resultados finales de las 3 pruebas realizadas.

Acción Pruebas	ÉXITO (%)	SIN ÉXITO (%)	CONFUSO (%)	LUMINOSIDAD	UMBRAL 1	UMBRAL 2
PRIMERA PRUEBA	80	15	5	Nublado	0.79	267.97
SEGUNDA PRUEBA	84	12	4	Parcialmente Nublado	0.83	280.47
TERCERA PRUEBA	93	6	1	Soleado	0.88	268.15
PROMEDIO	86	11	3			

Realizado por: Santiago Salinas, 2019.

De las 3 pruebas realizadas con diferentes características se determinó un promedio de 86% de eficiencia del programa, siendo 96% el porcentaje más alto y 80% el porcentaje más bajo alcanzado en las pruebas, mientras que, el porcentaje promedio de negación del sistema es un 11%, siendo 15% el porcentaje más alto y 6% el porcentaje más bajo alcanzado en las pruebas realizadas, finalmente, el porcentaje promedio de confusión del sistema es de 3%, siendo 5% el porcentaje más alto y 1% el porcentaje más bajo alcanzado en las pruebas realizadas.

CONCLUSIONES

Se realizó el análisis respectivo sobre las diferentes técnicas de procesamiento de imágenes, en la cual se optó por el método *Eigenfaces* para la implementación del sistema de identificación facial, siendo el más conveniente de acuerdo a las características del escenario.

Mediante la implementación de un sistema electrónico y eléctrico se implementó la arquitectura del sistema de identificación facial, cuyo principal objetivo era el control de apertura de una cerradura eléctrica.

El desempeño del sistema de identificación facial tuvo un porcentaje promedio de validez del 86% de acuerdo a las pruebas realizadas con los principales parámetros correlacionados como luminosidad, posición, distancia, umbral de proyección y distancia euclídea.

La distancia cámara – usuario fue el parámetro más controlado por lo que no realizó gran influencia dentro de la realización de las pruebas, a diferencia de la luminosidad el cual fue el parámetro menos controlado logrando mayor influencia dentro del sistema.

Para determinar si la persona se encuentra o no en la base de datos del sistema se utilizó dos umbrales (proyección y distancia euclídea) los cuales ayudaron al reconocimiento dentro del proceso de identificación.

RECOMENDACIONES

Para el uso del método *Eigenfaces* es necesario tratar de controlar la luminosidad, si la base de captura de la foto es un material reflejante como el vidrio, se debe realizar la homologación de este debido a que los reflejos de la luz alteran el sistema.

Es de gran importancia llevar un sondeo del control de acceso de los usuarios debido a que, si existen errores progresivamente, se debería realizar el reingreso de la información facial del usuario al sistema de identificación.

Antes de seleccionar el método para la identificación facial se recomienda analizar el escenario respectivo para determinar el método más adecuado para el proceso digital de la imagen e implementar un sistema de identificación facial.

BIBLIOGRAFÍA

1. “*A SURVEY OF FACE RECOGNITION APPROACH*”, *International Journal of Engineering Vol.3* [en línea]. Gujarat – India 2013. pp.632-635. [Consulta: 25 abril 2019]. Disponible en: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.436.5320&rep=rep1&type=pdf>
2. *ADMINISTRACIÓN DE SISTEMAS OPERATIVOS EN RED.*, [en línea]. España-Barcelona: Editorial UOC 2008. pp.25-32 [Consulta: 27 abril 2019]. Disponible en: <https://books.google.com.ec/books?id=w4utLelkYgkC&printsec=frontcover&dq=inautor:%22Josep+Maria+Arqu%C3%A9s+Soldevila%22&hl=es&sa=X&ved=0ahUKEwiCpvPK5t3iAhXJslkKH8MDaMQ6wEIKTAA#v=onepage&q&f=false>
3. **AGRAWALA, A. y SINGH, Y.**, *EVALUATION OF FACE RECOGNITION METHODS IN UNCONSTRAINED ENVIRONMENTS*, 2015. [en línea]. [Consulta: 4 abril 2019]. Disponible en: <https://www.sciencedirect.com/science/article/pii/S1877050915006560>
4. “*AN APPROACH TO AUTOMATIC RECOGNITION OF SPONTANEOUS FACIAL ACTIONS*”, IEEE [en línea]., 2002, (USA) p.20 [Consulta: 4 abril 2019]. Disponible en: <https://ieeexplore.ieee.org/abstract/document/1004180>
5. **BINESTSKAYA, M.**, *RECONOCIMIENTO FACIAL EN EL ÁMBITO FORENSE*, 2013, [en línea]. [Consulta: 28 abril 2019]. Disponible en: <http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20130916MayaBinetskaya.pdf>
6. **BRAND, J. y MASON, J.S.**, “*A COMPARATIVE ASSESSMENT OF THREE APPROACHES TO PIXEL – LEVEL HUMAN SKIN –IEEE DETECTION*”, IEEE [en línea]., 2002, (España). [Consulta: 25 abril 2019]. Disponible en: <https://ieeexplore.ieee.org/document/905653>
7. **CAÑEGO N.**, *SISTEMA DE IDENTIFICACIÓN DE PERSONAS MEDIANTE RECONOCIMIENTO FACIAL APLICADO A VIDEOVIGILANCIA*, [en línea] (Trabajo de titulación) (Maestría) Universidad Politécnica de Valencia. Valencia-España 2017. pp. 20-25. [Consulta: 25 abril 2019]. Disponible en: https://riunet.upv.es/bitstream/handle/10251/86962/memoria_53258252.pdf?sequence=

1&isAllowed=y

8. **CASADO, M.C.**, *MANUAL BÁSICO DE MATLAB*, [en línea]. [Consulta: 27 mayo 2019]. Disponible en: <http://webs.ucm.es/centros/cont/descargas/documento11541.pdf>
9. *¿CÓMO FUNCIONA LA TECNOLOGÍA DE RECONOCIMIENTO FACIAL?* 2015. [blog]. [Consulta: 4 abril 2019]. Disponible en: <https://www.welivesecurity.com/la-es/2015/08/27/tecnologia-de-reconocimiento-facial/>
10. *COMPARISON OF FIVE COLOR MODELS IN SKIN PIXEL CLASIFICATION.*, 1999, [en línea]. [Consulta: 5 mayo 2019]. Disponible en: https://www.researchgate.net/publication/3823455_Comparison_of_five_color_models_in_skin_pixel_classification
11. **CORTES, C. y VAPNIK, V.**, *SUPPORT – VECTOR NETWORKS*, 1995., [en línea]. [Consulta: 27 abril 2019]. Disponible en: http://image.diku.dk/imagecanon/material/cortes_vapnik95.pdf
12. **CROMO**, 2017 [blog]. [Consulta: 3 mayo 2019]. Disponible en: <https://www.elobservador.com.uy/nota/como-funciona-el-reconocimiento-facial-2017422500>
13. **DOMÍNGUEZ, S.**, *RECONOCIMIENTO FACIAL MEDIANTE EL ANÁLISIS DE COMPONENTES PRINCIPALES (PCA)*, [en línea] (Trabajo de titulación) (Maestría) Universidad Politécnica de Sevilla. Sevilla-España 2017. pp. 30-52. [Consulta: 4 abril 2019]. Disponible en: http://bibing.us.es/proyectos/abreproy/91426/fichero/TFG_SARA_DOMINGUEZ_PAVON.pdf
14. “*EIGENFACES VS. FISHERFACES: RECOGNITION USING CLASS SPECIFIC LINEAR PROJECTION*”., *IEEE* [en línea], 2015, pp.711-720 [Consulta: 4 abril 2019]. Disponible en: <https://ieeexplore.ieee.org/document/598228>.
15. *FACE RECOGNITION BY ELASTIC BUNCH GRAPH MATCHING*, 1997, [en línea]. [Consulta: 14 abril 2019]. Disponible en: <http://www.face-rec.org/algorithms/EBGM/WisFelKrue99-FaceRecognition-JainBook.pdf>

16. *FACE RECOGNITION WITH LOCAL BINARY PATTERNS.*, [en línea], [Consulta: 4 abril 2019]. Disponible en: http://www.ee.oulu.fi/research/imag/mvg/files/pdf/pdf_494.pdf
17. *FEATURE – BASED FACE RECOGNITION USING MIXTURE – DISTANCE.*, 2002, [en línea]. [Consulta: 3 mayo 2019]. Disponible en: <https://pdfs.semanticscholar.org/7c0b/c2e15bf134a8d867415f6a4d94dcba0044c5.pdf>
18. **GREER, W.**, *BREVE HISTORIA DEL RECONOCIMIENTO FACIAL.*, 2018, [blog]. [Consulta: 4 abril 2019]. Disponible en: <https://www.facefirst.com/blog/breve-historia-del-reconocimiento-facial/>
19. **HAFED, M. y LEVINE, M.**, *FACE RECOGNITION USING THE DISCRETE COSINE TRANSFORM*, 2001, [en línea]. [Consulta: 28 abril 2019]. Disponible en: <https://link.springer.com/article/10.1023/A:1011183429707>
20. **JOLLIFFE I.T.**, *PRINCIPAL COMPONENT ANALYSIS*, SECOND EDITION, 1986., [en línea]. New York-USA: Editorial Springer-Verlag. pp.435-438 [Consulta: 14 abril 2019]. Disponible en: [http://cda.psych.uiuc.edu/statistical_learning_course/Jolliffe%20I.%20Principal%20Component%20Analysis%20\(2ed.,%20Springer,%202002\)\(518s\)_MVsa_.pdf](http://cda.psych.uiuc.edu/statistical_learning_course/Jolliffe%20I.%20Principal%20Component%20Analysis%20(2ed.,%20Springer,%202002)(518s)_MVsa_.pdf)
21. **KAWULOK.**, *ADVANCES IN FACE DETECTION AND FACIAL IMAGE ANALYSIS.*, [en línea]. Syden-Australia: Editorial Springer 2016. pp.328-333. [Consulta: 26 mayo 2019]. Disponible en: <https://www.springer.com/la/book/9783319259567>
22. **LEE, C.** *PATTERN RECOGNITION*, 2009, [en línea]. [Consulta: 4 abril 2019]. Disponible en: <https://sites.google.com/site/mesmerli/Home/wo-de-zuopin?tmpl=%2Fsystem%2Fapp%2Ftemplates%2Fprint%2F&showPrintDialog=1>
23. **LLAMAS, L.**, *MANEJAR CARGAS DE MAS DE 220v CON ARDUINO Y SALIDA POR RELÉ*, 2016, [blog]. [Consulta: 28 mayo 2019]. Disponible en: <https://www.luisllamas.es/arduino-salida-rele/>
24. **MARTÍNEZ, J.**, *LAS EMOCIONES Y SU EXPRESIÓN EN LA PRIMERA INFANCIA*, [en línea]. [Consulta: 8 mayo 2019]. Disponible en:

25. **MORENO, J.** *PROTOTIPO PARA EL CONTROL DE UNA CERRADURA ELECTRONICA POR MEDIO DE RECONOCIMIENTO FACIAL*, [en línea] (Tesis) Universidad Distrital Francisco José de Caldas. Bogotá-Colombia 2017. pp. 12-15. [Consulta: 3 mayo 2019]. Disponible en: <http://repository.udistrital.edu.co/bitstream/11349/4687/9/MorenoLatorreJimPool2016.pdf>
26. **PARVEEN, P. y THURASINGHAM, B.,** *FACE RECOGNITION USING VARIOUS CLASSIFIERS: ARTIFICIAL NEURAL NETWORK, LINEAR DISCRIMINANT AND PRINCIPAL COMPONENT ANALYSIS*, 2006, [en línea]. pp.3-8 [Consulta: 3 mayo 2019]. Disponible en: <https://www.utdallas.edu/~bxt043000/Publications/Technical-Reports/UTDCS-05-06.pdf>
27. *¿QUÉ ES EL BLOQUEO ELECTRÓNICO?* [blog]. [Consulta: 25 abril 2019]. Disponible en: <http://www.keyless-doorlock.com/sp/company-news/what-is-electronic-lock.html>
28. *RECONOCIMIENTO FACIAL CON BASE EN IMÁGENES.*, 2017, [en línea]. [Consulta: 14 mayo 2019]. Disponible en: <https://dialnet.unirioja.es/descarga/articulo/6145639.pdf>
29. **RUSS, J.,** *THE IMAGE PROCESSING*, 2002, [en línea]. [Consulta: 4 abril 2019]. Disponible en: http://www.geo.uzh.ch/microsite/rsi-documents/research/SARlab/GMTILiterature/PDF/1142_fm.pdf
30. **SAMARIA, Y.,** *FACE RECOGNITION USING HIDDEN MARKOV MODELS*, 1994, [en línea]. [Consulta: 25 abril 2019]. Disponible en: https://www.researchgate.net/profile/Ferdinando_Samaria/publication/281127745_Face_recognition_using_Hidden_Markov_Models/links/5ad706ae0f7e9b28593963a1/Face-recognition-using-Hidden-Markov-Models.pdf
31. **SOLEM, J.,** *PROGRAMMING COMPUTER VISION WITH PYTHON*, 2012, [en línea]. [Consulta: 4 abril 2019]. Disponible en: http://programmingcomputervision.com/downloads/ProgrammingComputerVision_CC_draft.pdf

32. **THEODORIDIS, S. y KOUTROUMBAS, K.**, *PATTERN RECOGNITION*, SECOND EDITION, Elsevier (USA), 2008, [en línea]. [Consulta: 14 abril 2019]. Disponible en: <http://www.cs.ukzn.ac.za/~sviriri/Books/Machine-Learning-Pattern-Recognition/book3.pdf>
33. **TURK, M. y PENTLAND, A.**, *FACE RECOGNITION USING EIGENFACES*, 1991, [en línea]. [Consulta: 12 abril 2019]. Disponible en: <https://sites.cs.ucsb.edu/~mturk/Papers/mturk-CVPR91.pdf>
34. **VEZZETTI, E. y MARCOLINI, F.**, *SIMILARITY MEASURES FOR FACE RECOGNITION*, 2015, [en línea]. [Consulta: 14 abril 2019]. Disponible en: <https://ebooks.benthamscience.com/book/9781681080444/>
35. **VIOLA, P. y JONES, M.**, *RAPID OBJECT DETECTION USING A BOOSTED CASCADE OF SIMPLE FEATURES*, Cambridge - Reino Unido 2001, [en línea]. [Consulta: 4 abril 2019]. Disponible en: <https://www.cs.cmu.edu/~efros/courses/LBMV07/Papers/viola-cvpr-01.pdf>

ANEXOS

ANEXO A: Código del Programa.

```
clear all; close all;
clc;
bd = xlsread('DATOS.xlsx', 'Hoja1', 'B2:B200');
[m n] = size(bd);

N = 70;
for i=1 : m
    st.names{i} = bd(i);
end
total_d = 1;
for i=1 : m
    chr=int2str(bd(i));
    directorio =
['C:\Users\Santiago\Desktop\tesis\imagenesprueba\' ,
chr];
    cd(directorio);
    for j=1 : 10
        chr2 = int2str(j);
        chr3 = [chr2, '_'];
        chr4 = [chr3, chr];
        jk = [chr4, '.png'];
        k = imread(jk);
        jk2=imresize(k, [N N] );
        jk3 = [chr4, 'color'];
        jk4 = [jk3, '.png'];
        k5 = imread(jk4);
        st.datta{total_d} = k5;

        st.data{total_d} = jk2;
        total_d=total_d + 1;
    end
end
cd C:\Users\Santiago\Desktop\tesis\

%% Mostrar todos los usuarios todas las fotos

z=[];
au=[];
au_color=[]; z_color=[];
for i=0:10:(m-1)*10
    for j=1:10
        au=[au st.data{i+j}];
```



```

        au_color=[au_color st.data{ i+j}];
    end
    z=[z;au];
    au=[];
    z_color=[z_color;au_color];
    au_color=[];
end
figure(1),imshow(z,'Initialmagnification','fit');title
('z org')
figure(40),imshow(z_color,'Initialmagnification','fit'
);title('COLOR')
%% compute mean

avImg=zeros(N);
for k=1:(m*10)
    st.data{k} = im2single(st.data{k});
    avImg = avImg + (1/(m*10))*st.data{k};
end
figure(2),imshow(avImg,'Initialmagnification','fit');t
itle('average')

%%
for k=1:(m*10)
    st.dataAvg{k} = st.data{k} -avImg;
end
z=[];
au=[];
for i=0:10:(m-1)*10
    for j=1:10
        au=[au st.dataAvg{i+j}];
    end
    z=[z;au];
    au=[];
end
figure(3),imshow(z,'Initialmagnification','fit');title
('PROMEDIO MATRIZ Z')

%% CALCULO MATRIZ VARIANZA Y MATRIZ A VECTOR
A = zeros(N*N,m*10);% (N*N)*M    N*N*length(m)
m=columnas BS Excel
for k=1:(m*10)
    A(:,k) = st.dataAvg{k}(:);
end
% covariance matrix small dimension (transposed)
C = A'*A;
figure(4),imagesc(C);title('Covarianza')

```

```

%% eigen vectros in small dimension
[ Veigvec,Deigval ] = eig(C);% v M* e M*M only
diagonal 4 eigen values
% eigan face in large dimension A*veigvec is eigen
vector of Clarge
Vlarge = A*Veigvec;% 2500*M*M*M =2500 *M
% reshape to eigen face
eigenfaces1=[];
for k=1:(m*10)
    c = Vlarge(:,k);
    eigenfaces1{k} = reshape(c,N,N);
end
x=diag(Deigval);
[xc,xci]=sort(x,'descend');% largest eigenval
z=[];
au=[];
for i=0:10:(m-1)*10
    for j=1:10
        au=[au eigenfaces1{i+j}];
    end
    z=[z;au];
    au=[];
end
figure(5),imshow(z,'Initialmagnification','fit');title
('eigenfaces')

%% weights
nset=m*10;% select eigen faces
for mi=1:(m*10) % image number
    for k=1:nset % eigen face for coeff number
        wi(mi,k) = sum(A(:,mi).* eigenfaces1{xci(k)}(:))
    ;
    end
end

%% PRUEBA DE RECONOCIMIENTO

figure(10);
vid=ipcam('http://192.168.137.93:8080/videofeed');
preview(vid); %visualizar camara hImage
pause(5);
foto = snapshot(vid); % CAPTURA get
faceDetector = vision.CascadeObjectDetector();
%barrido de toda la imagen encuentra rasgos rostro
imag = foto;
BBOX = step(faceDetector,imag); %encuentra rostro
posicion

```

```

%axes(handles.axes2);
imshow(imag);
pause(1);
rectangle('position',BBOX(1,:), 'edgecolor','b','linewidth',2); %encuadra zona de interes para extraccion de
caracteristicas
k=imag;
testFaceMic=imcrop(k,BBOX);
testFaceMic = rgb2gray(testFaceMic);
testFaceMic = imresize(testFaceMic,[N N]);
testFaceMic = im2single(testFaceMic);
figure(6),
imshow(testFaceMic, 'Initialmagnification','fit');
title('test face')
Aface = testFaceMic(:)-avImg(:); % normilized face

for tt=1:nsel
    wface(tt) = sum(Aface.* eigenfaces1{xc1(tt)}(:)) ;
end

% compute distance
for mi=1:(m*10)
    fsumcur=0;
    for tt=1:nsel
        fsumcur = fsumcur + (wface(tt) -
wi(mi,tt)).^2;
    end
    diferencia(mi) = sqrt(fsumcur);
end

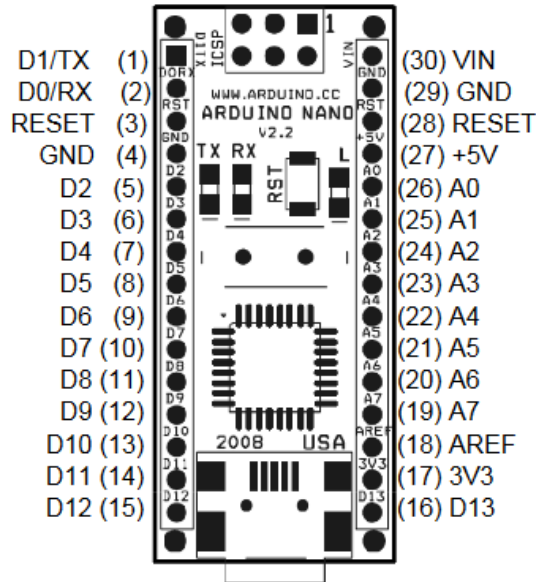
[val, in] = min(diferencia);

if (min(wface)>=0.88) && (val>=280)
    figure(7),
    imshow(st.data{in}, 'Initialmagnification','fit');
    title('La imagen reconocida es')
else
    disp('Persona Desconocida');
end
xlswrite('DATOS.xlsx', mean(wface), 'Hoja2', 'J11');

```

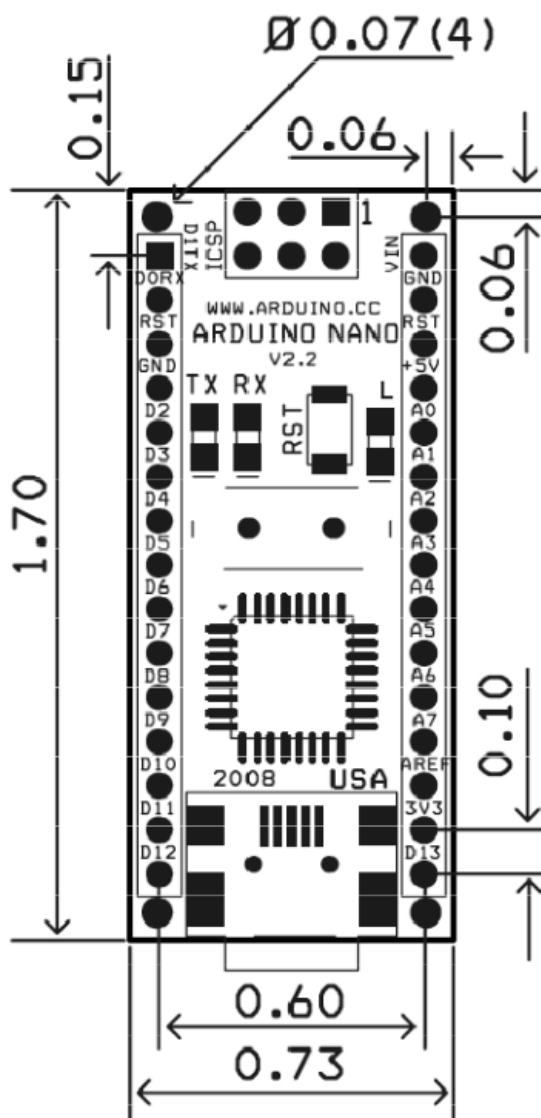
ANEXO B: Datasheet Arduino Nano.

Arduino Nano Pin Layout



Pin No.	Name	Type	Description
1-2, 5-16	D0-D13	I/O	Digital input/output port 0 to 13
3, 28	RESET	Input	Reset (active low)
4, 29	GND	PWR	Supply ground
17	3V3	Output	+3.3V output (from FTDI)
18	AREF	Input	ADC reference
19-26	A7-A0	Input	Analog input channel 0 to 7
27	+5V	Output or Input	+5V output (from on-board regulator) or +5V (input from external power supply)
30	VIN	PWR	Supply voltage

Arduino Nano Mechanical Drawing




ALL DIMENTIONS ARE IN INCHES

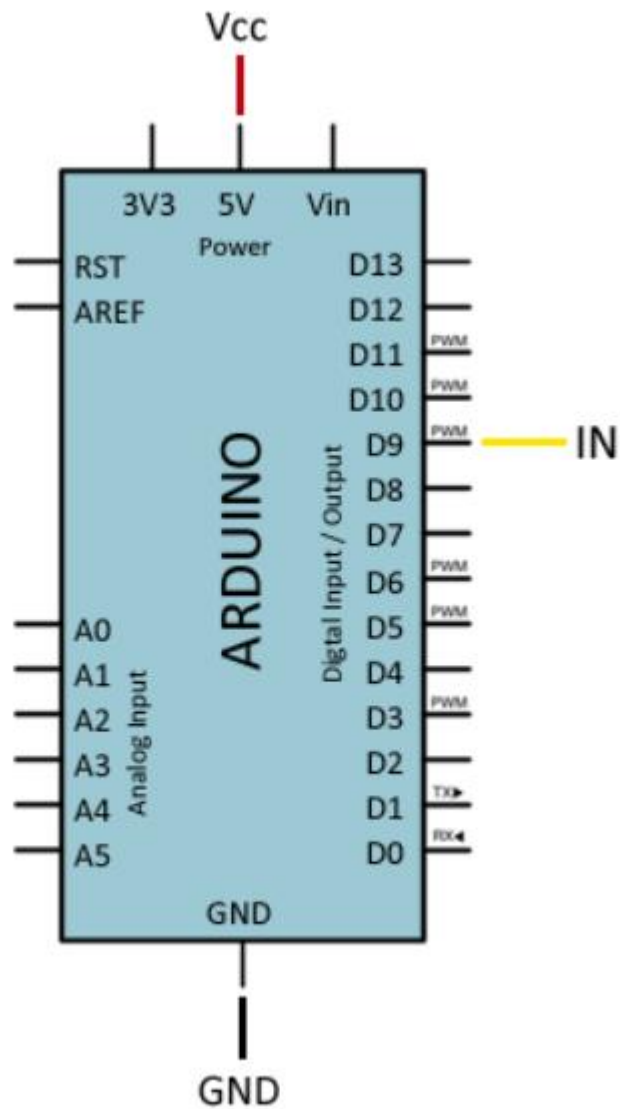
Arduino Nano Bill of Material

Item Number	Qty.	Ref. Dest.	Description	Mfg. P/N	MFG	Vendor P/N	Vendor
1	5	C1,C3,C4,C7,C9	Capacitor, 0.1uF 50V 10% Ceramic X7R 0805	C0805C104K5RACTU	Kemet	80-C0805C104K5R	Mouser
2	3	C2,C8,C10	Capacitor, 4.7uF 10V 10% Tantalum Case A	T491A475K010AT	Kemet	80-T491A475K010	Mouser
3	2	C5,C6	Capacitor, 18pF 50V 5% Ceramic NOP/COG 0805	C0805C180J5GACTU	Kemet	80-C0805C180J5G	Mouser
4	1	D1	Diode, Schottky 0.5A 20V	MBR0520LT1G	ONsemi	863-MBR0520LT1G	Mouser
5	1	J1,J2	Headers, 36PS 1 Row	68000-136HLF	FCI	649-68000-136HLF	Mouser
6	1	J4	Connector, Mini-B Recept Rt. Angle	67503-1020	Molex	538-67503-1020	Mouser
7	1	J5	Headers, 72PS 2 Rows	67996-272HLF	FCI	649-67996-272HLF	Mouser
8	1	LD1	LED, Super Bright RED 100mcd 640nm 120degree 0805	APT2012SRCPRV	Kingbright	604-APT2012SRCPRV	Mouser
9	1	LD2	LED, Super Bright GREEN 50mcd 570nm 110degree 0805	APHCM2012CGCK-F01	Kingbright	604-APHCM2012CGCK	Mouser
10	1	LD3	LED, Super Bright ORANGE 160mcd 601nm 110degree 0805	APHCM2012SECK-F01	Kingbright	04-APHCM2012SECK	Mouser
11	1	LD4	LED, Super Bright BLUE 80mcd 470nm 110degree 0805	LTST-C170TBKT	Lite-On Inc	160-1579-1-ND	Digikey
12	1	R1	Resistor Pack, 1K +/-5% 62.5mW 4RES SMD	YC164-JR-071KL	Yageo	YC164J-1.0KCT-ND	Digikey
13	1	R2	Resistor Pack, 680 +/-5% 62.5mW 4RES SMD	YC164-JR-07680RL	Yageo	YC164J-680CT-ND	Digikey
14	1	SW1	Switch, Momentary Tact SPST 150gf 3.0x2.5mm	B3U-1000P	Omron	SW1020CT-ND	Digikey
15	1	U1	IC, Microcontroller RISC 16kB Flash, 0.5kB EEPROM, 23 I/O Pins	ATmega168-20AU	Atmel	556-ATMEGA168-20AU	Mouser
16	1	U2	IC, USB to SERIAL UART 28 Pins SSOP	FT232RL	FTDI	895-FT232RL	Mouser
17	1	U3	IC, Voltage regulator 5V, 500mA SOT-223	UA78M05CDCYRG3	TI	595-UA78M05CDCYRG3	Mouser
18	1	Y1	Cystal, 16MHz +/-20ppm HC-49/US Low Profile	ABL-16.000MHZ-B2	Abracon	815-ABL-16-B2	Mouser

ANEXO C: Configuración del Relé con Arduino.



 Carga: Tensión máxima 250VAC.
Intensidad máxima 10A.

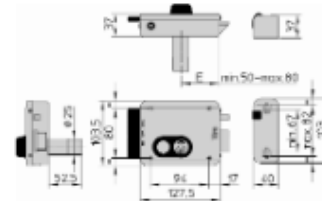
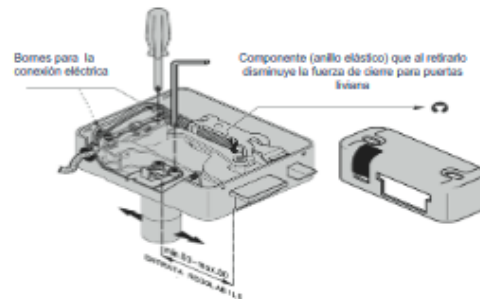


CERRADURAS ELÉCTRICAS - MADE IN ITALY



“V97” CON PULSADOR INTERIOR ENTRADA REGULABLE DE 50 HASTA 80 MM.

- Intercambiable con la mayoría de las cerraduras eléctricas de tipo europeo ya instaladas, dejando instalado el mismo recibidor metálico.
- El pestillo se autobloquea cuando la cerradura está cerrada.
- Expulsor separado del pestillo para garantizar el funcionamiento en caso de movimientos verticales (tolerancia hasta ± 6 mm) entre cerradura y recibidor.
- Por medio del giro de la llave en el cilindro interior de la cerradura, es posible:
 - ✓ desactivar o reactivar el funcionamiento del pulsador;
 - ✓ activar o desactivar la función “Cerradura Siempre Abierta”.
- Montaje muy sencillo:
 - ✓ **entrada regulable de 50 hasta 80 mm.**
(Las cerraduras eléctricas con cerrojo de la competencia no tienen esta característica);
 - ✓ **recibidor metálico con altura regulable**, con inserto en nylon, autolubrificante, alineado con el expulsor.
- Si se instala en puertas o portones livianos, es posible disminuir la fuerza de cierre retirando un anillo elástico del interior de la cerradura (como se indica en el dibujo).
- **Llaves:** de latón niquelado, de perfil Viro, 3 en dotación. Disponibles versiones con llaves de perfil Universal para la sustitución de las más comunes cerraduras eléctricas ya instaladas sin necesidad de retiro de las llaves en uso. (Cilindros ricodificables con específico kit para amaestramientos).



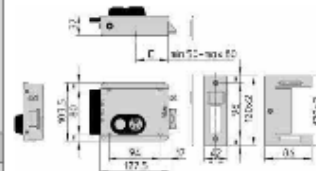
	ART. N.	Entrada regulable mm.	Dimensiones de la cerradura mm.	Cilindro interior (fijo) Art. N.	Cilindro exterior (fijo) Art. N.	Peso de la unidad gr.
Derecha	8972.1	50 ÷ 80	127,5 x 103,5	791	794	1535
Izquierda	8972.2	50 ÷ 80	127,5 x 103,5	791	794	1535

Para las versiones con llave de perfil Universal añadir al final del código artículo la sigla .UN

“V97” CON PULSANTE CON APERTURA ESTERNA



	ART. N.	Entrada regulable mm.	Dimensiones de la cerradura mm.	Cilindro interior (fijo) Art. N.	Cilindro exterior (fijo) Art. N.	Cilindro externo (suelto) Art. N.
Derecha	8973.712.1	50-60-70-80	127,5 x 103,5	791	712	1450
Izquierda	8973.712.2	50-60-70-80	127,5 x 103,5	791	712	1450



Para las versiones con llave de perfil Universal añadir al final del código artículo la sigla .UN

ANEXO E: Acta de entrega y recepción.

ESPOCH

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

Facultad de Informática y Electrónica

ACTA DE ENTREGA

FECHA : Riobamba, 26 de junio de 2019

PARA : **BQF. Benjamín Román**
Técnico Docente a cargo del Bioterio

DE : **Santiago Salinas López**
Tesisista de la Facultad de Informática y Electrónica

ASUNTO : Entrega del sistema de identificación facial.

Con la presente acta se realiza la entrega del sistema de identificación facial e infraestructura implementada en el BIOTERIO de la Facultad de Ciencias, el cual consta de lo siguiente:

DESCRIPCIÓN	CANTIDAD
Cerradura eléctrica e infraestructura.	1
Soporte para cámara IP.	1
Teléfono inteligente	1
Sistema electrónico de control (Arduino y Relé)	1
Router TP – Link WR840N	1
Parlantes para computadora	1

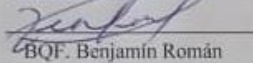
A los 51 días de la aprobación de la solicitud para la realización del tema "Implementación de un sistema de identificación facial mediante el procesamiento digital de imágenes para el personal del Bioterio de la ESPOCH" realizada por parte de señor Santiago Salomón Salinas López, tesisista de la Facultad de Informática y Electrónica, de la Escuela de Ingeniería en Electrónica Telecomunicaciones y Redes se

procede a la entrega por parte del Sr. Santiago Salinas y recepción por parte del técnico docente a cargo del Bioterio el señor BQF. Benjamín Román.

Aprovecho la oportunidad para expresar mis más sinceros agradecimientos por la oportunidad brindada.

En constancia firman:

BQF. Benjamín Andrés Román
Bioquímico Farmacéutico
Retrendado 25186 - C.I. 11711111



BQF. Benjamín Román
TÉCNICO DOCENTE A CARGO DEL
BIOTERIO



Santiago Salinas López
TESISTA FIE-EIETR

Anexo: Solicitud realizada para la implementación.

Riobamba, 29 de abril de 2019



Señor,

Dr. Edmundo Caluña

DECANO DE LA FACULTAD DE CIENCIAS

Presente. -

De mi consideración

En calidad de director de tesis del tema: "Implementación de un sistema de identificación facial utilizando procesamiento digital de imágenes para el personal del Bioterio de la Facultad de Ciencias de la ESPOCH", desarrollado por el Sr. SANTIAGO SALOMON SALINAS LOPEZ, estudiante egresado de la Facultad de Informática y Electrónica de la carrera de Ingeniería en Electrónica Telecomunicaciones y Redes, me permito solicitar a Usted muy comedidamente se sirva emitir la respectiva autorización para el acceso al bioterio y la designación de una computadora para la realización de pruebas, implementación e instalación definitiva del sistema, actividad que se llevará a cabo a partir del 6 de mayo de 2019.

En espera de ser atendido favorablemente, anticipo a Usted mis debidos agradecimientos.

Atentamente,



Ing. Paúl David Moreno PhD

ANEXO F

MANUAL DEL SISTEMA
DE IDENTIFICACIÓN
FACIAL

Riobamba – Ecuador

CONTENIDO

INTRODUCCIÓN	20
EJECUCIÓN DEL SISTEMA DE IDENTIFICACIÓN FACIAL .	21
INTERFAZ GENERAL	22
INTERFAZ DE LA BASE DE DATOS	24
INTERFAZ DE REPORTES.....	26
INGRESO A LA BASE DE DATOS A UN USUARIO	28
OBTENCIÓN DE REPORTES DEL SISTEMA	30
FUNCIONAMIENTO DEL SISTEMA ELÉCTRICO	35
RECOMENDACIONES	36

INTRODUCCIÓN

El presente Manual de procedimientos tiene como propósito contar con una guía clara y específica que garantice la óptima operación y desarrollo de las diferentes actividades del Sistema de Identificación Facial, ingreso de usuarios a la base de datos, generación de reportes y manejo general del sistema, documento que ayudará a servir como un instrumento de apoyo y mejora para el control de acceso al Bioterio, secuencial y detallada las operaciones de los procedimientos a seguir para cada actividad, promoviendo el buen desarrollo del sistema.

EJECUCIÓN DEL SISTEMA DE IDENTIFICACIÓN FACIAL

El sistema de identificación facial tiene dos maneras de ejecución, una de ellas es la ejecución por la aplicación .exe o mediante la ejecución de la programación del software comercial MatLab, como se observa en la Figura 1.

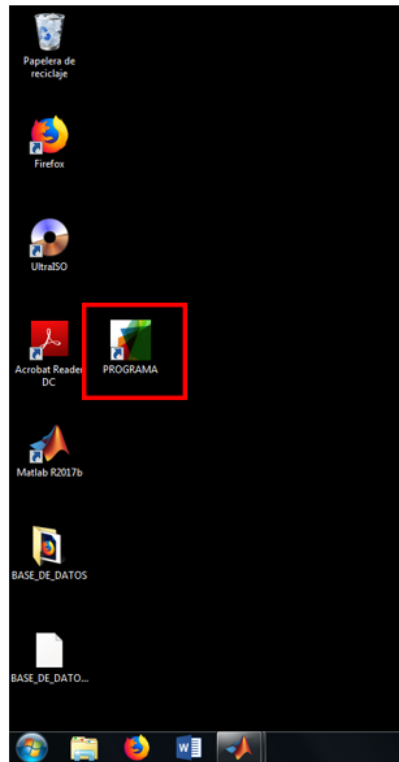


Figura 1: Programa ejecutable.

Si la ejecución del programa es por la aplicación .exe el sistema de identificación tardará unos minutos en ejecutarse, por otro lado, si el sistema es ejecutado por el software MatLab el sistema correrá de manera mas óptima de acuerdo a las características del computador.

Una vez inicializado el sistema de identificación aparecerá la interfaz general de inicio, como muestra la Figura 2.



Figura 2: Interfaz de Inicio.

INTERFAZ GENERAL

La interfaz general tiene las siguientes funciones:

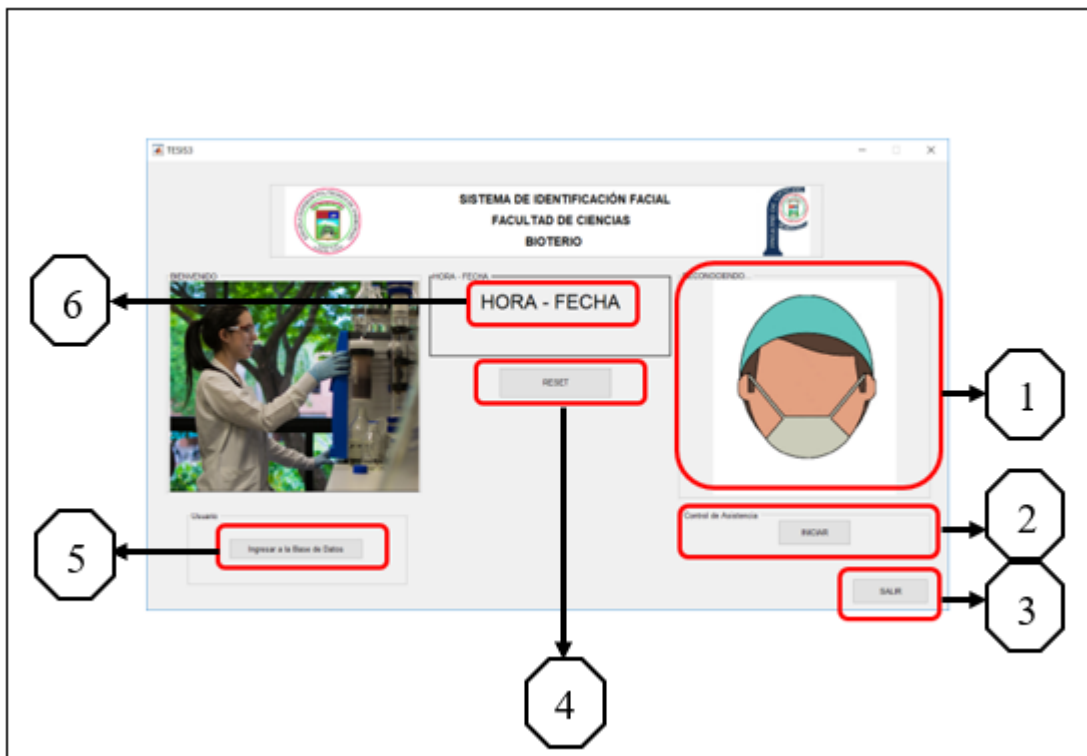


Figura 3: Funciones de la interfaz general.

En donde, las especificaciones de cada una se muestran a continuación:

- Parámetro 1: Ventana de visualización del usuario, en esta área se observa la detección del rostro del individuo para proceder con la identificación.
- Parámetro 2: Botón de INICIO, mediante esta ejecución el programa se iniciará y se procederá a enlazar con la cámara IP para obtener la imagen del usuario.
- Parámetro 3: Botón de SALIR, mediante esta ejecución el sistema de identificación se cerrará y se apagará automáticamente.
- Parámetro 4: Botón de RESET, mediante esta ejecución el sistema procede a actualizar la hora y fecha del sistema de identificación.
- Parámetro 5: Mediante este botón se procede al Ingreso de la Base de Datos, en donde se registrará a un nuevo usuario.
- Parámetro 6: Interfaz de muestro de la hora y fecha de ingreso o reinicio del sistema de identificación.

INTERFAZ DE LA BASE DE DATOS

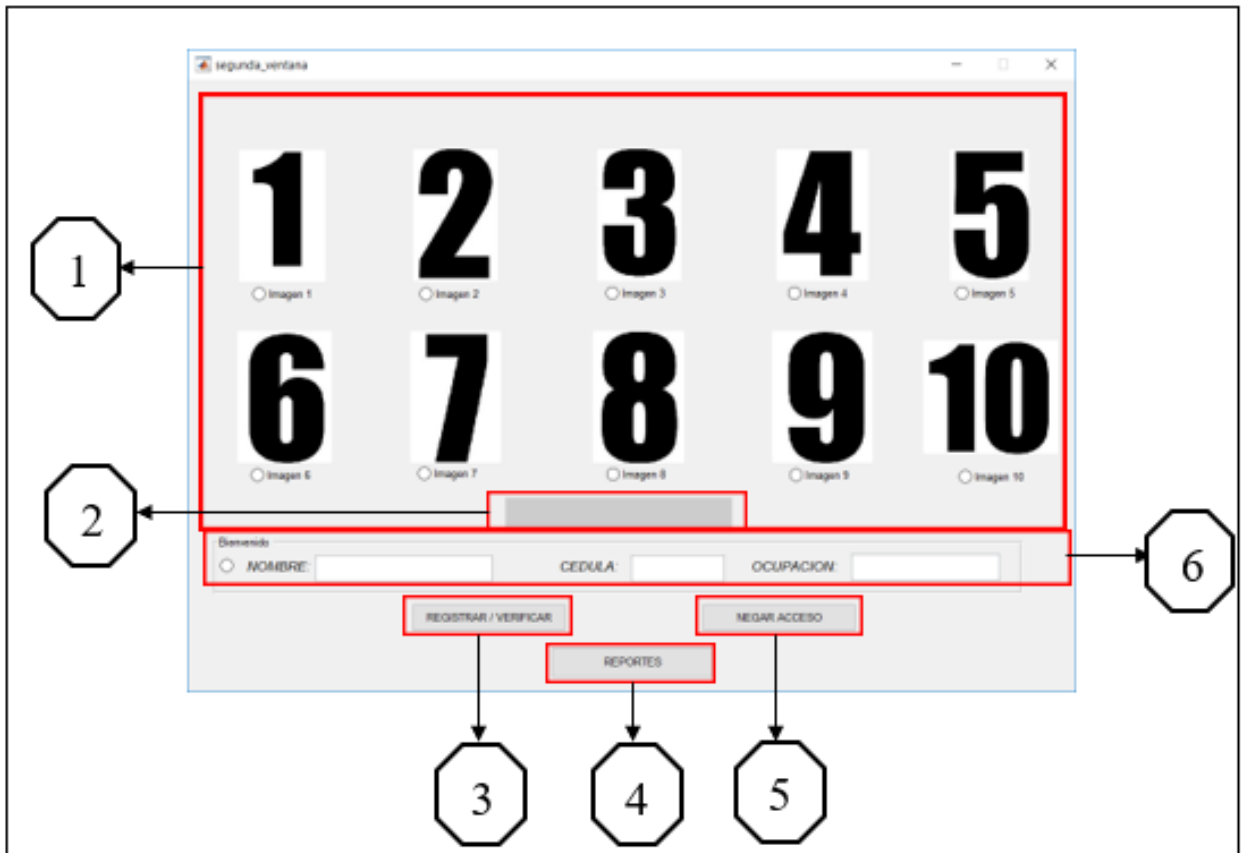


Figura 4: Funciones de la interfaz de la base de datos.

La interfaz para el ingreso de los datos de los diferentes usuarios tiene 6 parámetros importantes, a continuación, se especifica cada uno de ellos:

- Parámetro 1: Ingreso de las capturas faciales de los usuarios, en este parámetro se ingresa obligatoriamente 10 fotografías de los usuarios las cuales se van a almacenar en la base de datos local del ordenador, para el ingreso de cada rostro se presiona en el círculo en blanco, en donde el programa procederá a enlazarse a la base de datos y realizar la captura del rostro del usuario.
- Parámetro 2: Este indica una pantalla de información el cual de acuerdo a la acción realizada el sistema enviara un mensaje de confirmación, negación o error al momento de ejecutar alguna función dentro de esta interfaz.
- Parámetro 3 y parámetro 6: Ingreso de la información del usuario a la base de datos, mediante esta acción el sistema procederá a realizar el ingreso de los

parámetros como el nombre, cédula y ocupación del usuario al sistema de identificación, para posteriormente realizar las capturas de rostro del usuario.

- Parámetro 4: Para la generación de reportes o realización de filtros por búsqueda se abrirá una nueva ventana donde se desplegará una interfaz con otras funciones, las cuales se encuentran analizadas en la interfaz de reportes, detallada en el presente manual.
- Parámetro 5: Cuando un usuario registrado se le culmine el tiempo de acceso al laboratorio se realiza la negación del acceso mediante el botón de negación de servicio, cabe recalcar que la información como el nombre, cedula y ocupación, y la información facial no serán eliminados, si no, solamente se registrará la negación del acceso.

INTERFAZ DE REPORTEES

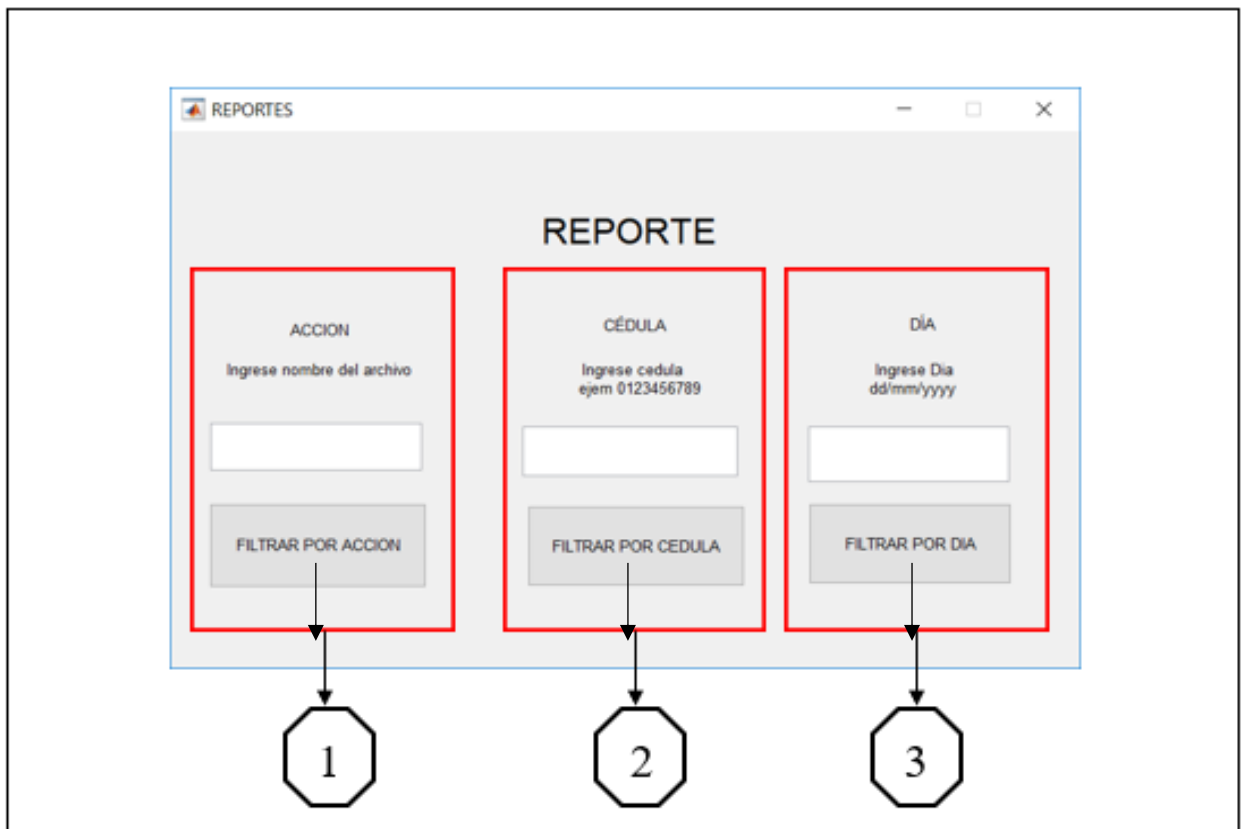


Figura 5: Interfaz de Reportes.

La interfaz de reportes de los diferentes usuarios tiene 3 parámetros importantes, a continuación, se especifica cada uno de ellos.

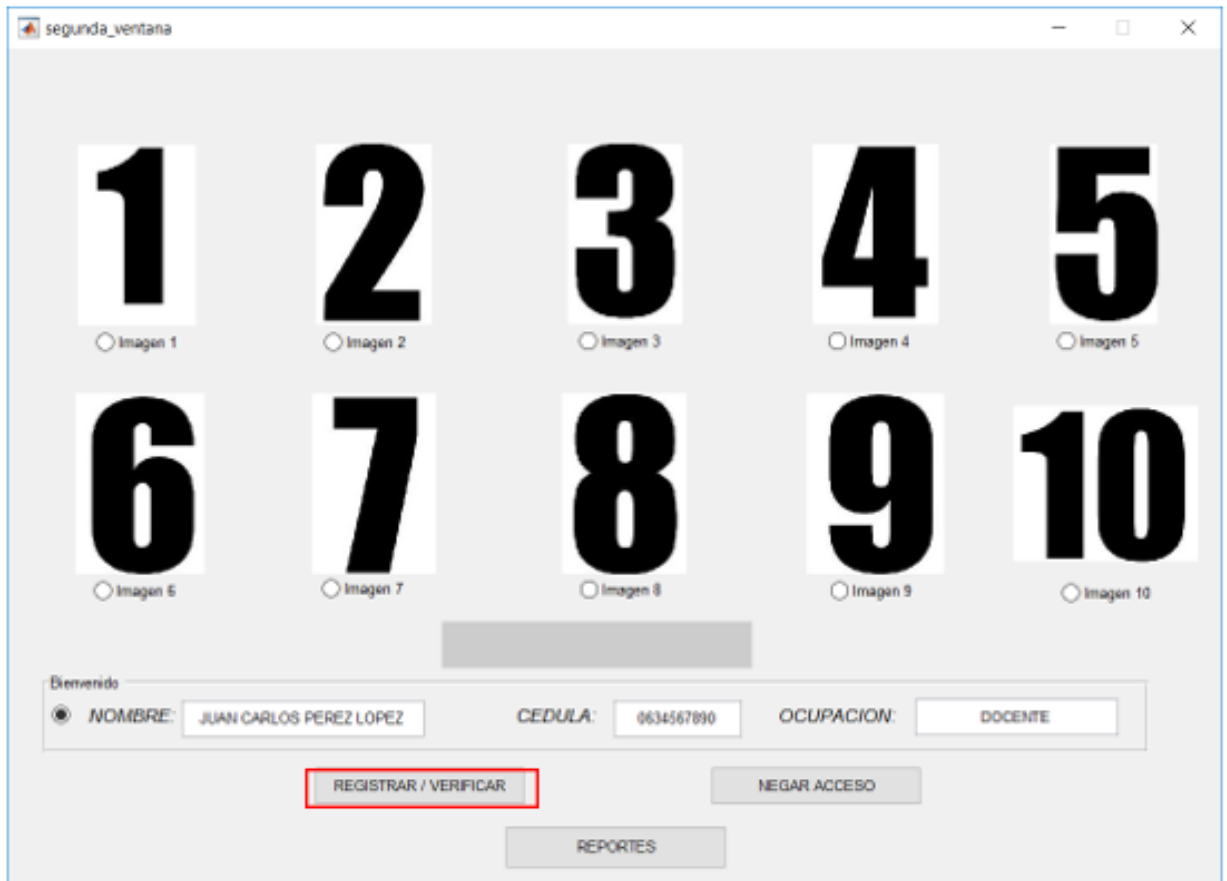
- **Parámetro 1:** Filtración por acción, este parámetro genera un archivo EXCEL .xlsx el cual contiene la información de los usuarios con acceso POSITIVO y usuarios que no se encuentren registrados en la base de datos o que ya no tengan acceso, los cuales tienen la acción NEGATIVO, los usuarios con acceso positivo se encontrarán registrados en la Hoja 1 del documento en Excel, y los usuarios con la acción negativo, se encontrarán registrados en la Hoja 2 del documento de Excel, este documento se generara de manera automática y se almacenara en el escritorio del ordenador.
- **Parámetro 2:** Filtración por numero de cédula, este parámetro genera un archivo Excel con el formato .xlsx el cual brindará información del usuario al cual pertenece el numero de cedula ingresado, dando las acciones positivas y

negativas, si el usuario ya no cuenta con acceso al laboratorio, si el numero de cédula ingresado no existe en la base de datos el sistema creará un archivo vacío el cual no contendrá ninguna información sobre la cédula ingresada, cabe recalcar que el numero de cédula ingresado es sin guion, el archivo generado se almacenará en el escritorio del ordenador.

- Parámetro 3: Filtración por día, mediante este parámetro se creará un archivo Excel con el formato .xlsx el cual contiene la información de las acciones positivas y negativas del sistema y los usuarios que ingresaron dicho día filtrado, el ingreso de la información esta dado en el formato de día, mes y año respectivamente, (dd/mm/yyyy). El archivo se creará en el escritorio del ordenador, si la fecha esta mal ingresada o no hay registros de la fecha el sistema procederá a la creación de un archivo vacío.

INGRESO A LA BASE DE DATOS A UN USUARIO

Al ingresar a un usuario a la base de datos, necesitaremos encontrarnos en la interfaz de la base de datos, para posteriormente ingresar la información del usuario.



The screenshot shows a web application window titled "segunda_ventana". At the top, there are ten large black numbers (1-10) arranged in two rows of five. Each number is centered in a white square and has a small radio button labeled "Imagen" below it. Below the numbers is a grey rectangular bar. Underneath that is a form section titled "Bienvenido" with a radio button and the text "NOMBRE: JUAN CARLOS PEREZ LOPEZ", "CEDULA: 0634567890", and "OCUPACION: DOCENTE". Below the form are three buttons: "REGISTRAR / VERIFICAR" (highlighted with a red border), "NEGAR ACCESO", and "REPORTES".

Figura 6: Ingreso de datos del usuario.

Como primer punto se realiza el ingreso del nombre, cédula y ocupación del usuario, la ocupación puede ser Tesista, Técnico Docente, Docente, Personal, etc. Cabe recalcar que el ingreso de la cédula se la realiza sin guion y el nombre con letras mayúsculas. Posteriormente se inserta la información mediante el botón REGISTRAR/VERIFICAR y el sistema nos procederá a informar si la acción tuvo éxito (Figura 7) o si en la base de datos el usuario ya se encuentra registrado (Figura 8).

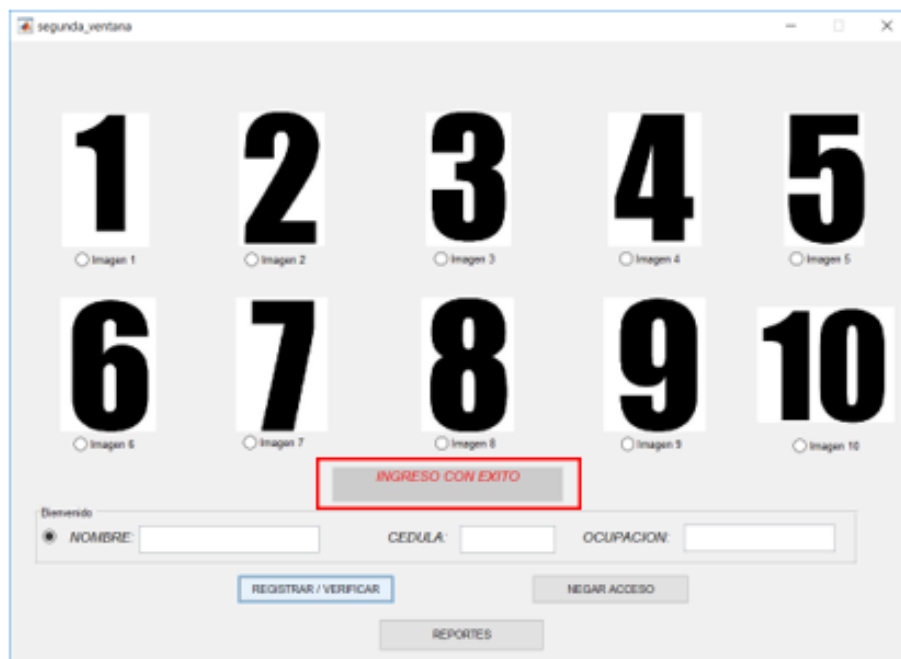


Figura 7: Confirmación del ingreso a la base de datos.

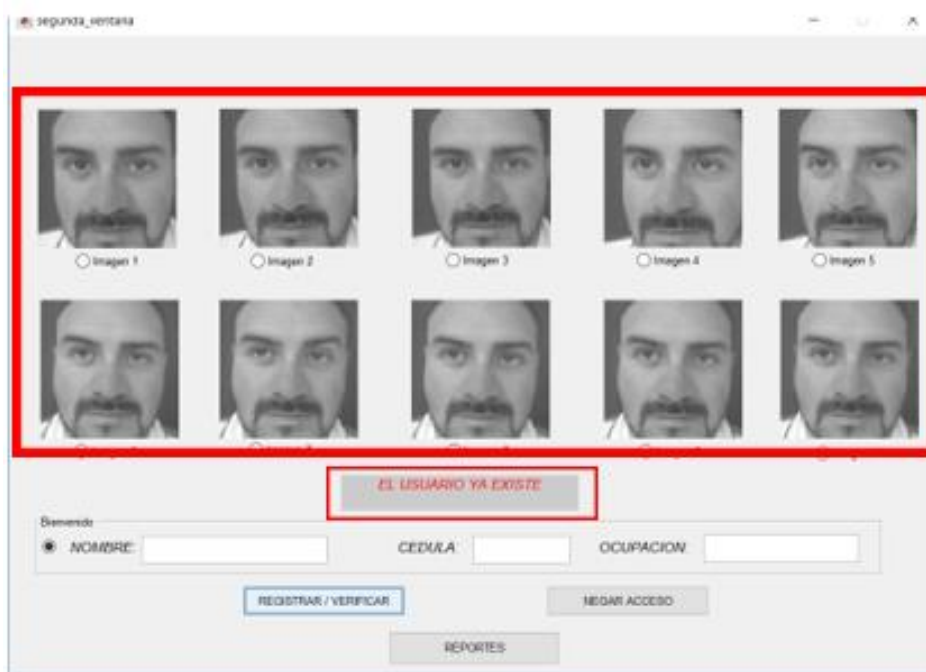


Figura 8: Verificación de usuario.

Si el usuario ingresado ya se encuentra en la base de datos, el sistema procederá a mostrar las fotografías del usuario e informar que el usuario ingresado ya existe en la base de datos, como se puede visualizar en la Figura 8.

Si el usuario no se encuentra en la base de datos (Figura 7) se procederá al ingreso de las fotos faciales de los usuarios, para esto se selecciona el botón redondo en blanco y el sistema procederá a realizar la captura de la imagen del usuario (Figura 9).

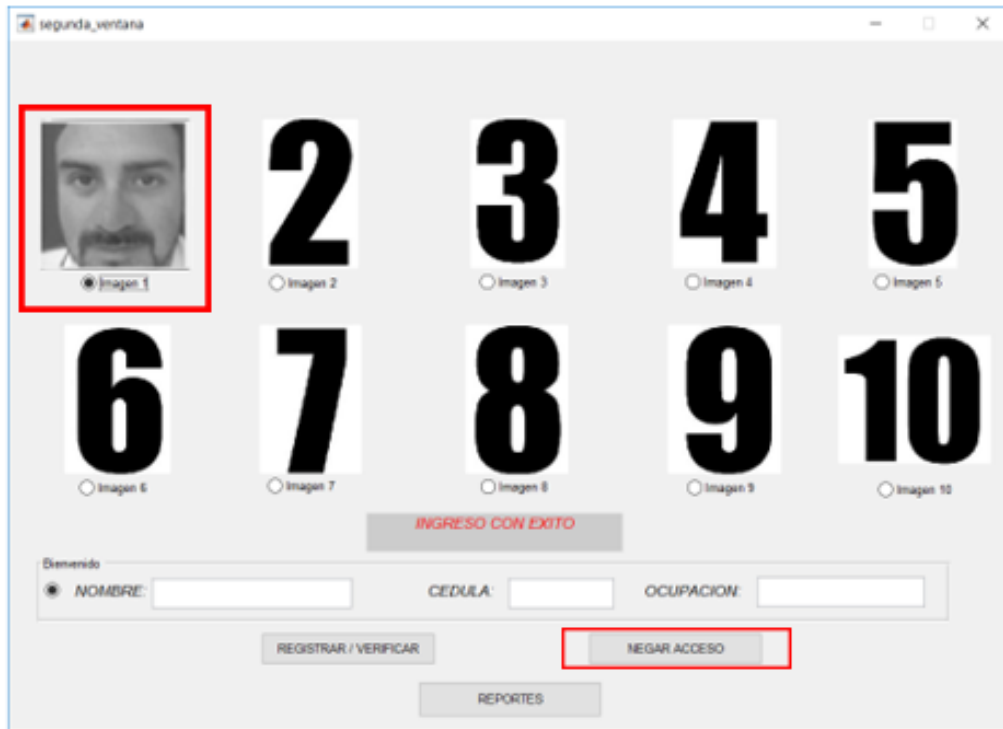


Figura 9: Ingreso de la información facial del usuario.

Si la imagen se encuentra borrosa o carece de información se procederá a realizar el reingreso de la imagen mediante la ejecución del mismo botón de captura.

Una vez ingresado las 10 fotografías se procede a cerrar la interfaz de la base de datos.

De esta manera se realiza el ingreso a la base datos a un usuario, si se desea negar el servicio al usuario registrado, se procede a ingresar la cédula y posteriormente ejecutar el botón de negar acceso y automáticamente el usuario carecerá de ingreso al laboratorio.

OBTENCIÓN DE REPORTES DEL SISTEMA

Una vez ingresado en la interfaz de la base de datos se procede a ejecutar el botón de REPORTES, como indica en la Figura 10.

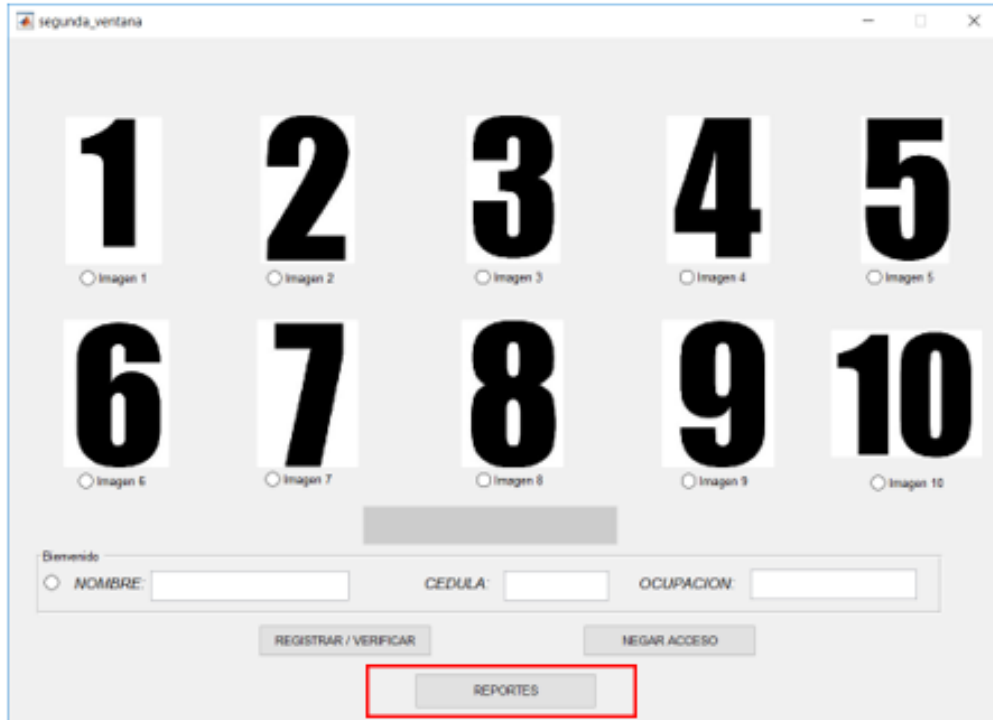


Figura 10: Acceso a la interfaz de reportes.

De esta manera se abrirá la nueva interfaz de reportes (Figura 11). En donde se procederá a ingresar la información específica, en la filtración por acción, se ingresará el nombre del archivo, este puede ser cualquier nombre que el administrador crea conveniente, y finalmente se filtra por acción, en donde, en el escritorio del ordenador se guardará el archivo con la información de las acciones realizadas (POSITIVAS Y NEGATIVAS).

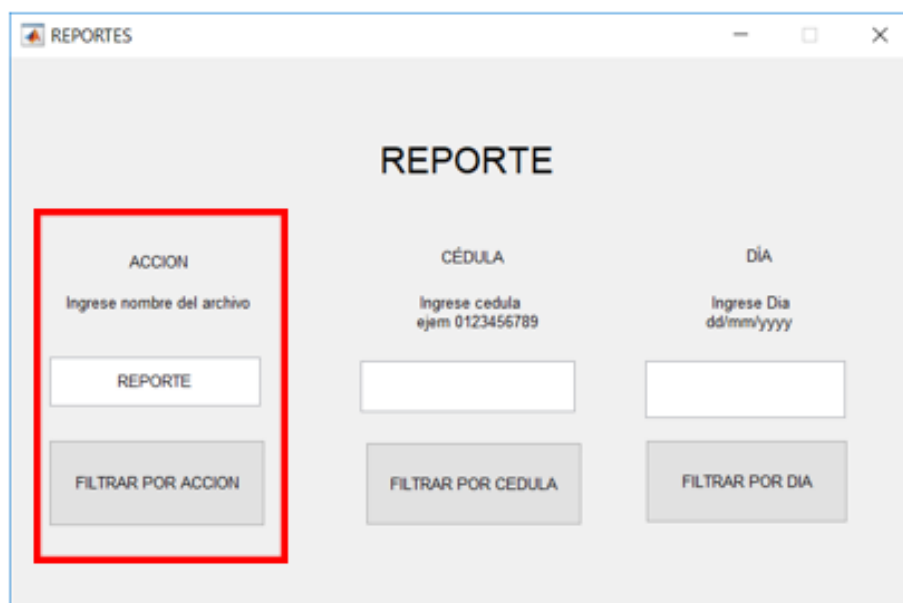


Figura 11: Filtración por acción.

El tiempo de demora de la creación del reporte tiene como estimado 40 segundos, dependiendo de la información que se encuentre en la base de datos a filtrarse. Una vez generado el archivo, en la hoja 1 se encontrarán las acciones positivas y en la hoja 2 las acciones negativas, como se puede visualizar en la Figura 12.

	A	B	C	D	E	F		A	B	C	D	E	F
76					21/06/2019 11:52	NEGADO	66			ING AIDA MI DOCENTE		21/06/2019 11:53	POSITIVO
77					21/06/2019 11:53	NEGADO	67			ING DAVID N DOCENTE		21/06/2019 11:54	POSITIVO
78					21/06/2019 11:54	NEGADO	68			ISAAC HERNANDEZ		25/06/2019 17:00	POSITIVO
79					25/06/2019 15:59	NEGADO	69			ISAAC HERNANDEZ		25/06/2019 17:01	POSITIVO
80					25/06/2019 16:00	NEGADO	70			ISAAC HERNANDEZ		25/06/2019 17:09	POSITIVO
81					25/06/2019 16:00	NEGADO	71			ISAAC HERNANDEZ		25/06/2019 17:14	POSITIVO
82					25/06/2019 16:01	NEGADO	72			ISAAC HERNANDEZ		25/06/2019 17:15	POSITIVO
83					25/06/2019 16:41	NEGADO	73			ISAAC HERNANDEZ		25/06/2019 18:46	POSITIVO
84					25/06/2019 16:48	NEGADO	74			SANTIAGO S. TESISTA		26/06/2019 8:16	POSITIVO
85					25/06/2019 16:54	NEGADO	75			SANTIAGO S. TESISTA		26/06/2019 8:22	POSITIVO
86					25/06/2019 16:54	NEGADO	76			BENJAMIN A TECNICO DO		26/06/2019 8:23	POSITIVO
87					25/06/2019 17:01	NEGADO	77			BENJAMIN A TECNICO DO		26/06/2019 8:39	POSITIVO
88					25/06/2019 17:10	NEGADO	78			BENJAMIN A TECNICO DO		26/06/2019 8:52	POSITIVO
89					25/06/2019 17:42	NEGADO	79			ISAAC HERNANDEZ		26/06/2019 9:25	POSITIVO
90					25/06/2019 18:22	NEGADO	80						
91					25/06/2019 18:23	NEGADO	81						
92					25/06/2019 18:27	NEGADO	82						
93					25/06/2019 18:27	NEGADO	83						
94			ISAAC HERNANDEZ		25/06/2019 18:29	NEGADO	84						
95			ISAAC HERNANDEZ		25/06/2019 18:31	NEGADO	85						
96			ISAAC HERNANDEZ		25/06/2019 18:33	NEGADO	86						
97			ISAAC HERNANDEZ		25/06/2019 18:45	NEGADO	87						
98					26/06/2019 8:38	NEGADO	88						
99					26/06/2019 8:41	NEGADO	89						
100			ISAAC HERNANDEZ		26/06/2019 9:26	NEGADO	90						
101					26/06/2019 9:27	NEGADO	91						
102					26/06/2019 9:30	NEGADO	92						
103							93						
104							94						

Figura 12: Reporte mediante filtrado por acción.

Para la filtración por cédula se ingresa el número sin guion y se ejecuta el botón de "filtrar por cedula", consecuentemente el archivo tendrá el nombre de la misma cédula

del usuario a filtrar es decir “0634567890” y se creará un documento Excel en donde se indicará las acciones realizadas por el usuario en el sistema de identificación facial.

The screenshot shows a web application window titled 'REPORTES'. Inside, there is a form titled 'REPORTE'. The form is divided into three columns: 'ACCION', 'CÉDULA', and 'DÍA'. Each column has a text input field and a button labeled 'FILTRAR POR [column name]'. The 'CÉDULA' column is highlighted with a red border. The input field for 'CÉDULA' contains the text '0634567890'. The 'ACCION' column has a placeholder text 'Ingrese nombre del archivo'. The 'DÍA' column has a placeholder text 'Ingrese Dia dd/mm/yyyy'.

Figura 13: Filtración por cédula.

El tiempo de demora de la creación del reporte tiene como estimado 40 segundos, dependiendo de la información que se encuentre en la base de datos a filtrarse. Una vez generado el archivo, se encontrará la información en la hoja 1, como se puede visualizar en la Figura 14.

The screenshot shows an Excel spreadsheet with the following data:

	A	B	C	D	E	F
1	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 9:47	POSITIVO	
2	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 9:49	POSITIVO	
3	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 9:51	POSITIVO	
4	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:14	POSITIVO	
5	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:33	POSITIVO	
6	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:39	POSITIVO	
7	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:41	POSITIVO	
8	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:53	POSITIVO	
9	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 10:55	POSITIVO	
10	1804630893	SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	21/06/2019 11:06	POSITIVO	
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						

Figura 14: Reporte mediante filtrado por cédula.

Para la filtración por día se ingresa el día en el formato dd/mm/yyyy y se ejecuta el botón de “filtrar por día”, consecuentemente se creará un archivo Excel en el escritorio con el nombre *reporte_fecha*, en donde se indicarán las acciones realizadas por todos los usuarios en el sistema dentro del día establecido.

Figura 15: Filtración por día.

El tiempo de demora de la creación del reporte tiene como estimado 40 segundos, dependiendo de la información que se encuentre en la base de datos a filtrarse. Una vez generado el archivo, se encontrará la información en la hoja 1, como se puede visualizar en la Figura 16.

	A	B	C	D	E	F
1			SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	26/06/2019 8:16	POSITIVO
2			SANTIAGO SALOMON SALINAS LOPEZ	TESISTA	26/06/2019 8:22	POSITIVO
3			BENJAMIN ANDRES ROMAN SANTOS	TECNICO DOCENTE	26/06/2019 8:23	POSITIVO
4			ISAAC HERNAN TENE LOPEZ	TESISTA	26/06/2019 9:26	NEGADO
5					26/06/2019 9:27	NEGADO
6					26/06/2019 9:30	NEGADO
7						
8						

Figura 16: Reporte mediante filtrado por día.

FUNCIONAMIENTO DEL SISTEMA ELÉCTRICO

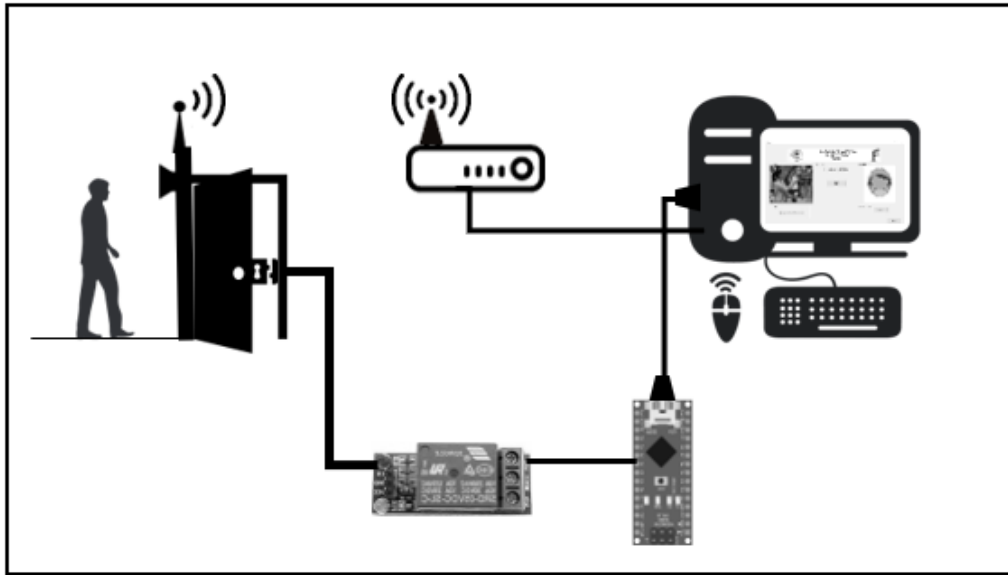


Figura 17: Esquema de funcionamiento del sistema eléctrico.

El sistema está compuesto por una cámara IP la cual está conectada de manera inalámbrica mediante un Router a la computadora u ordenador, la información es enviada a través de la conexión ethernet router – computadora, de esta manera se adquiere realiza la captura del rostro facial para posteriormente enviar una señal al dispositivo electrónico RELÉ mediante la comunicación USB del ARDUINO – COMPUTADORA. El puerto configurado para la programación es el puerto COM3 localizado al nivel inferior derecho del CPU, y de esta manera mediante la instalación eléctrica se conecta el circuito de alta potencia para el accionamiento de la cerradura eléctrica.

RECOMENDACIONES

- Evitar el ingreso de imágenes borrosas o mal capturadas al sistema debido a que durante el proceso de identificación puede causar problemas o errores al programa.
- Esperar al momento de realizar los respectivos reportes debido a que si la información a filtrar es extensa el sistema tomará mas tiempo para el proceso de filtraje.
- Realizar la ejecución del programa con el software MatLab si el ordenador tiene bajos recursos computacionales.
- Evitar e uso de otro puerto USB para la conexión Arduino – Computadora.