UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS

ELECTRÓNICA E INDUSTRIAL

Carrera de Ingeniería en Electrónica y Comunicaciones

TEMA

"SISTEMA ALTERNATIVO DE SEGURIDAD VEHICULAR BASADO EN RECONOCIMIENTO FACIAL"

Proyecto de Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo a la obtención del título de Ingeniería en Electrónica y Comunicaciones.

SUBLÍNEA DE INVETIGACIÓN: Procesamiento digital de señales e imágenes

AUTOR: Ana Belén Amaya Arcos

PROFESOR REVISOR: Ing. Marco Jurado, Mg.

Ambato – Ecuador

Abril 2015

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: “SISTEMA ALTERNATIVO DE SEGURIDAD VEHICULAR BASADO EN RECONOCIMIENTO FACIAL” de la señorita Amaya Arcos Ana Belén, estudiante de la Carrera de Ingeniería Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe de investigación reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Abril 2015

EL TUTOR

……

Ing. Marco Jurado, Mg.

AUTORÍA

El presente trabajo de investigación titulado “SISTEMA ALTERNATIVO DE SEGURIDAD VEHICULAR BASADO EN RECONOCIMIENTO FACIAL” es absolutamente original, auténtico y personal en tal virtud, el contenido, efectos legales y académicas que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Abril 2015

……

Amaya Arcos Ana Belén

CC.: 1804251633

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes aprobó el Informe Final del trabajo de graduación titulado “SISTEMA ALTERNATIVO DE SEGURIDAD VEHICULAR BASADO EN RECONOCIMIENTO FACIAL” presentado por la señorita Amaya Arcos Ana Belén de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

…….
Ing. Vicente Morales, Mg.
PRESIDENTE DEL TRIBUNAL

……..
PhD. Gabriela Pérez
DOCENTE CALIFICADOR

……
Ing. Juan Pablo Pallo, Mg.
DOCENTE CALIFICADOR

DEDICATORIA

Este trabajo está dedicado a mis padres Guido Amaya y Amparo Arcos por su dedicación, confianza e infinito amor puesto en mí durante toda mi vida estudiantil.

A mi hijo, Michael, por ser mi motor y mi inspiración para continuar en la constante lucha del tan anhelado éxito.

A mis hermanas Evelyn y Vanessa porque siempre han estado allí en los momentos más difíciles de mi vida.

A mi familia por brindarme tantos consejos que me han convertido en una persona de bien.

A mi pareja sentimental, Renato, por ser mi apoyo incondicional, por su paciencia y comprensión.

A mí misma como una muestra de todo lo que puedo lograr con esfuerzo y dedicación.

Ana Belén Amaya Arcos

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

En la ciudad de Ambato a pesar de los incesantes esfuerzos realizados por parte de la Policía Nacional junto con la ciudadanía, no se ha logrado controlar la delincuencia; los vehículos están expuestos a ser hurtados pues ninguna alarma logra disuadir a los maleantes que evaden estos sistemas de seguridad logrando llevarse los vehículos.

En esta investigación se ha desarrollado un prototipo de un sistema de seguridad para los autos que puede ser utilizado en cualquier momento del día y está basado en el reconocimiento del rostro del conductor, para lo cual se ha generado dos bases de datos (una para el día y otra para la noche) conformadas por fotografías que corresponden al rostro de las personas autorizadas para usar el vehículo.

Para la etapa del reconocimiento se ha decidido utilizar la técnica de Análisis de Componentes Principales (ACP), que extrae las características faciales más importantes de la imagen capturada del conductor, para compararlas con las características de los usuarios autorizados y así determinar si la persona que está frente al volante pertenece o no a la base de datos.

Palabras Clave: Reconocimiento, Imagen, Facial, Seguridad.

ABSTRACT

In Ambato city despite continued efforts by the National Police along with citizenship, has not succeeded in controlling crime; vehicles are liable to be stolen because no alarm does deter criminals who evade these security systems be achieved vehicles.

This research has developed a prototype of a safety system for cars that can be used at any time of day and is based on the recognition of the driver's face, for which it has generated two databases (one for the day and one for night) made up of photographs that correspond to the faces of the people authorized to use the car.

For the stage of recognition has decided to use the technique of Principal Components Analysis (PCA), which extracts the most important facial features of the captured image of the driver, for comparison with the characteristics of authorized users to determine if the person is behind the wheel or not belongs to the database.

Keywords: *Recognition, Image, Facial, Security.*

INTRODUCCIÓN

En el presente proyecto se ha desarrollado el prototipo de un sistema de seguridad para los autos mediante el reconocimiento del rostro de conductor.

Inicialmente el sistema no permite el arranque del vehículo, pues es necesario que el usuario sea identificado, para esto se captura una imagen del rostro del conductor y se extrae un conjunto de características que mejor representen dicha imagen, para posteriormente ser comparadas con otros parámetros obtenidos de fotografías faciales de las personas autorizadas para usar el auto (almacenadas en bases de datos) y así poder determinar si la persona frente al volante puede utilizar el vehículo.

Posteriormente, la parte electrónica del sistema permite el encendido del auto, en dependencia del resultado obtenido en la fase de reconocimiento.

En el primer capítulo del proyecto se analizan estadísticas recientes respecto al robo de vehículos en el Ecuador, determinando así que los sistemas de seguridad actuales no son capaces de garantizar la protección del auto.

En el segundo capítulo se describen los diferentes sistemas de seguridad vehicular que se ofertan actualmente en el mercado, se hace una introducción a la biometría, se listan los tipos de sistemas biométricos y se detallan las principales técnicas que se emplean para realizar un reconocimiento facial.

En el tercer capítulo se explica cómo están conformadas las bases de datos que contienen las fotografías de las personas autorizadas para usar el auto, se explica cómo se desarrolla la fase de pre procesado de las imágenes y la etapa del reconocimiento facial de acuerdo a la técnica seleccionada, y finalmente se realizan pruebas del sistema para comprobar su funcionamiento.

En el cuarto capítulo se redacta las conclusiones y recomendaciones, una vez que se ha terminado el proyecto del Sistema Alternativo de Seguridad Vehicular basado en Reconocimiento Facial.

CAPÍTULO I

EL PROBLEMA

1.1 TEMA

SISTEMA ALTERNATIVO DE SEGURIDAD VEHICULAR BASADO EN RECONOCIMIENTO FACIAL

1.2 PLANTEAMIENTO DEL PROBLEMA

La seguridad es un concepto importante en lo que respecta a salvaguardar vidas y bienes materiales, pero a esta se la puede analizar desde dos puntos de vista diferentes: aquella que está orientada a la prevención de accidentes y la seguridad dirigida a evitar la ejecución de delitos como robo de propiedades y bienes.

Desde los inicios de la humanidad, el hombre siempre ha sentido la necesidad de seguridad y protección ante los distintos peligros que aquejaban su vida, con el asentamiento de las primeras civilizaciones, el objetivo de los estados que los gobernaban siempre fue administrar justicia y proveer seguridad. Conforme la sociedad va evolucionando, la delincuencia es un factor muy complejo que está en aumento, y por este motivo la búsqueda de mecanismos cada vez más

seguros siempre ha sido parte de la naturaleza humana, por eso no es extraño que los usuarios opten por diversos sistemas para proteger sus propiedades.

No se puede establecer con certeza las causas de la inseguridad, pues la delincuencia está presente en todas las clases sociales, sin ninguna distinción, aunque según se ha mencionado los últimos años en varias noticias tanto televisivas como artículos periodísticos, la delincuencia está íntimamente relacionada con algunos aspectos como bajos recursos o marginación social.

Precisamente, uno de los problemas sociales más difícil de afrontar en Ecuador es el de la inseguridad, pues ahora no solo los bienes materiales se ven expuestos sino también la propia vida de las personas ya que en un delito, al atacante no le importa herir para lograr cumplir su objetivo.

Enfocándose en el sector vehicular, en una de las ciudades con mayor afluencia de autos como lo es la capital ecuatoriana, de acuerdo a un artículo publicado en la web por la Agencia Pública de Noticias del Ecuador y Suramérica “Andes”, Pichincha redujo los índices delincuenciales del robo de autos y motos en un 37% entre enero y abril del 2014 en comparación al período de 2013, donde hubo 100 autos y 14 motos robadas ante 63 carros y nueve motos sustraídas en el 2014, asimismo, el robo de accesorios de vehículos bajó un 10% (de 108 a 97 casos) [1]. De igual manera ocurre en la provincia de Tungurahua, según menciona Ludwin Coronel, comandante de la Policía Nacional de Tungurahua, el índice delictivo ha decrecido para los años 2013 y 2014 en un 22% y 24% respectivamente, presentando una disminución de robos de carros en un 38%, de motos un 91% y de accesorios de los autos en un 34% [2].

Ante esta problemática social, cada día se van desarrollando nuevos y novedosos sistemas de seguridad para proteger los domicilios, vehículos, empresas, oficinas y hasta pequeños negocios, existiendo desde los más simples hasta los más complejos y costosos.

Según va avanzando la tecnología y la demanda de vehículos mejor equipados, se requiere mayor seguridad para proteger los nuevos y novedosos productos

que hacen parte de los automotores, por eso es necesario el uso de sistemas confiables, eficientes y difíciles de quebrantar, que garanticen su seguridad, así se podrá tener plena confianza de que el automotor no corre ningún riesgo de hurto, pues cuando una persona decide adquirir un vehículo además de analizar su equipamiento y servicios, lo que busca es una alternativa para cuidar la inversión que acaba de adquirir contra el crimen del robo de vehículos.

Actualmente, el mercado nos ofrece una infinidad de alternativas en cuanto a seguridad, pero al momento de adquirir uno de estos sistemas, no solo se debe considerar el factor económico, pues la calidad, factibilidad y sensibilidad son indicadores muy importantes que se deben analizar así como también su fácil manejo. Pero, las limitadas alternativas de seguridad vehicular, impiden que los usuarios sientan tranquilidad cuando estacionan sus vehículos en cualquier lugar de la ciudad, pues no saben en qué momento serán víctimas de la delincuencia.

1.3 DELIMITACIÓN DEL PROBLEMA

- **Área Académica**: Comunicaciones
- **Línea de Investigación**: Tecnologías de Comunicaciones
- **Sub línea de Investigación**: Procesamiento digital de señales e imágenes.

DELIMITACIÓN ESPACIAL:

El desarrollo de la investigación se llevó a cabo en la ciudad de Ambato

DELIMITACIÓN TEMPORAL:

El tiempo en el cual se realizó la presente investigación fue de diez meses a partir de la aprobación por parte del Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4 JUSTIFICACIÓN

La realidad que vive el Ecuador, específicamente la ciudad de Ambato en cuanto a la seguridad vehicular exige sistemas confiables que permitan tener pleno control sobre quien hace uso de un vehículo.

La importancia de la investigación radica en la aplicación de los conocimientos adquiridos para el diseño de un sistema seguro para los autos, brindando a sus propietarios una alternativa de seguridad para su vehículo, lo que permitirá reducir el riesgo de ser víctimas de la delincuencia.

Esta investigación se orienta a todas aquellas personas propietarias de un vehículo que no cuente con un sistema de seguridad confiable que satisfaga todas sus expectativas, pues este nuevo sistema brinda tranquilidad a los propietarios al saber que solo personas autorizadas podrán hacer uso de su automóvil.

Esta investigación genera gran impacto social en el país a pesar de que en el Ecuador ya se ha implementado el primer sistema de reconocimiento facial y de voz, pero dicho sistema únicamente servirá para reconocer la voz y rostros de periodistas y opositores del gobierno [3]; mientras que esta investigación propone utilizar esta nueva tecnología de una manera innovadora, desarrollando un sistema para la seguridad vehicular, por lo cual la gran mayoría de propietarios de automóviles, sentirán la necesidad de hacer uso de esta alternativa, debido al bajo costo que tendrá este nuevo sistema.

1.5 OBJETIVOS

1.5.1 OBJETIVO GENERAL:

Diseñar un sistema alternativo de seguridad vehicular contra robos basado en reconocimiento facial

1.5.2 OBJETIVOS ESPECÍFICOS:

- Analizar los mecanismos de bloqueo vehicular existentes
- Definir los requerimientos técnicos adecuados para el sistema de seguridad vehicular basado en reconocimiento facial
- Diseñar el prototipo del sistema de seguridad vehicular.
- Implementar el prototipo del sistema de seguridad vehicular basado en reconocimiento facial

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

2.1 ANTECEDENTES INVESTIGATIVOS

Dentro de la bibliografía revisada se ha encontrado varios documentos referentes a mecanismos de bloqueo vehicular y sistemas biométricos, que han servido de guía para el desarrollo de este proyecto.

En la investigación desarrollada por Luis Eduardo Cando Tite, bajo el tema "Bloqueo Electrónico en el encendido de un vehículo, para proporcionar un sistema de seguridad contra robos", se explica que el sistema hace uso de un módulo biométrico para el ingreso de las huellas dactilares que permitirán o no el encendido del vehículo; este sistema de bloqueo consiste en un conjunto de botones, sensores y actuadores que impiden el funcionamiento del auto, además de una pantalla LCD que ofrece la posibilidad de visualizar la actividad que se está realizando [4].

Se están desarrollando sistemas de seguridad que no hagan uso únicamente de una llave o una contraseña, ahora se pretende trabajar con sistemas que utilicen características propias del dueño del vehículo como son sus rasgos faciales. Actualmente son diversas las aplicaciones de los sistemas biométricos, ya sea

para seguridad, control de personal, acceso a lugares públicos o sitios de trabajo entre otros [5].

Revisando algunas patentes publicadas, los autores proponen sistemas de bloqueo no solo para automóviles sino también para todo tipo de vehículos, que garanticen la seguridad gracias a la identificación del conductor antes de la puesta en marcha del vehículo [6], también se pueden realizar controles de alcoholemia para prevenir accidentes, mediante la utilización de un dispositivo lector del iris de los ojos y un dispositivo alcoholímetro relacionados mediante un microprocesador que estará conectado a una base de datos, y así se podrá determinar si la persona que se encuentra en el vehículo está autorizada para hacer uso de este, caso contrario el microprocesador bloqueará el vehículo [7].

Como complemento se ha revisado también una patente en donde se explica la invención de un sistema de transmisión de datos en forma remota y digital con localización satelital desde terminales móviles o fijas con cámaras de vigilancia urbana para reconocimiento facial, y una investigación científica para así tener una clara idea de cómo implementar un sistema automático de detección y corrección de puntos característicos faciales mal marcados, obtenidos de un sistema comercial automático [8].

Todas estas fuentes proporcionan información que es de mucha utilidad para el desarrollo de este proyecto por la validez científica que poseen, de esta manera se puede tener un mejor concepto sobre el tema a investigar.

Es muy importante entonces mencionar, que las técnicas para tener pleno control sobre el vehículo en lo que a seguridad se refiere, son muchas; pero ahora se pretende modernizar estos sistemas empleando rasgos únicos del propietario del automotor, para que de esta manera no se pueda utilizar el vehículo sin la autorización correspondiente [9].

2.2 FUNDAMENTACIÓN TEÓRICA

2.2.1 SEGURIDAD VEHICULAR

La seguridad vehicular es el conjunto de elementos y sistemas ubicados en el automotor que sirven para proteger este bien material de un posible robo. Estos dispositivos dotan a los vehículos de los más altos niveles de seguridad puesto que emplean tecnología para desarrollar sistemas de seguridad cada vez más eficientes.

Para lograr cumplir con este objetivo los dispositivos deben ir evolucionando, corrigiendo falencias, mejorando características y disminuyendo costos.

2.2.2 SISTEMA DE SEGURIDAD VEHICULAR

En el mercado se presentan diversos sistemas de seguridad diseñados para vehículos, cada uno con diferentes características brindando varias alternativas para la protección de los automotores. Existen sistemas que cuando detectan la apertura no autorizada, la manipulación y los intentos de mover el vehículo mediante grúas, lanzan una señal acústica (sirena) de gran volumen acompañada de señales visuales como el destello de los intermitentes del auto, alertando del intento de robo y complicando el mismo. Por otro lado se encuentran los inmovilizadores que comparan los códigos electrónicos presentes en la llave original del auto con los códigos almacenados en la unidad de control del vehículo ECU, impidiendo el encendido cuando se lo intente realizar solo con una copia de la llave.

A pesar de la existencia de varios tipos de estas alarmas y sistemas inmovilizadores, se siguen desarrollando nuevas alternativas, dando lugar a sistemas de seguridad cada vez más sofisticados y confiables, que incluyen la identificación/autentificación personal.

Todo sistema de seguridad que sea empleado para la protección de un vehículo, basa su funcionamiento de acuerdo a alguno de los siguientes parámetros [10]:

- Apertura de puertas
- Detección de movimientos de la carrocería
- Detección de movimiento en el interior del vehículo mediante ultrasonido
- Aviso acústico de conexión-desconexión
- Mando a distancia para activar/desactivar la alarma
- Sirena
- Encendido de luces intermitentes

2.2.3 TIPOS DE SISTEMAS DE SEGURIDAD VEHICULAR

Varias alternativas en cuanto a sistemas de seguridad vehicular se ofertan actualmente, entre las cuales se puede encontrar:

- Sistemas que se activan y desactivan (sin sirena), bloqueando puertas y ventanas
- Sistemas que se activan y suenan una sirena
- Sistemas que impiden el encendido del auto bloqueando su parte eléctrica
- Sistemas con localizador, que permiten ubicar el auto por medio de un control cuando se ha olvidado donde se lo dejó parqueado
- Alarmas que por medio de un radar, detectan movimiento dentro y fuera del auto

Existen otras opciones para la protección de un vehículo, pero algunos de estos mecanismos de bloqueo resultan rústicos y antiestéticos como los que se presentan a continuación:

1. Bloqueo mediante dispositivos mecánicos, que son económicos pero no suponen mayor dificultad para ser vulnerados, sobre todo si el ladrón ya tiene experiencia con este tipo de seguridades, entre los cuales se encuentran:
   - Sistemas que bloquean el movimiento de los pedales
   - Dispositivos que unen pedales con el volante como se muestra en la figura 2.1.

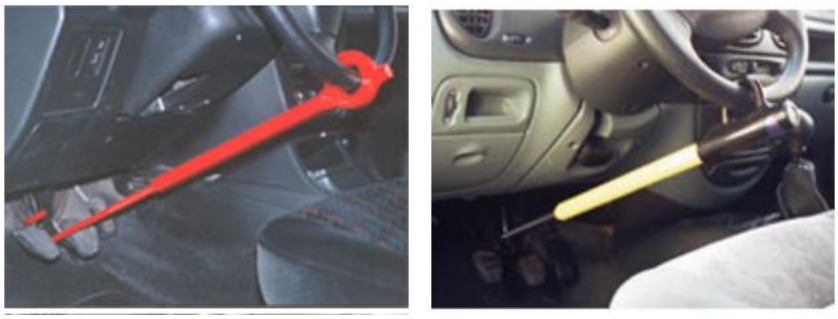


Figura 2. 1 Mecanismo de Bloqueo que une pedales con volante [13].

- Sistemas que impiden el giro del volante mediante una barra como se indica en la figura 2.2.

Figura 2. 2 Mecanismo de Bloqueo que impide giro de volante [13]

- Sistemas que unen la palanca de cambios con el freno de mano como se observa en la figura 2.3.

Figura 2. 3 Mecanismo de Bloqueo que interrumpe funciones de la palanca de cambios [13]

2. Dispositivos electrónicos que impiden el arranque

3. Localizadores (en caso de que el vehículo haya sido robado) [11].

- Sirena que avisa que el auto está en movimiento
- Localizadores mediante red GSM

- Localizadores mediante el uso de GPS.

Estas funciones corresponden a las alarmas más comunes, pero actualmente existen sistemas más sofisticadas con funciones mucho más complejas como:

- Sistema de alarma para coche con servicio de G.P.S. (Sistema de Posicionamiento Global)
- Alarma de coche con sistema anti-asalto
- Inmovilizadores

La elección de un determinado sistema se toma en función de las características que posee, su funcionalidad, nivel de seguridad costos y comodidad que ofrece.

A continuación se va a mencionar la forma en que operan estos sofisticados sistemas de seguridad vehicular.

SISTEMA DE ALARMA PARA COCHE CON SERVICIO DE G.P.S. (SISTEMA DE POSICIONAMIENTO GLOBAL): Este sistema logra acoplarse a la salida de una alarma ya conectada, cuando ésta se activa, se emite un mensaje de texto al celular del propietario con la posición exacta del vehículo. Este sistema es tan efectivo como los de uso militar (en el peor de los casos, el error puede oscilar entre los 4 y 5 metros), no presenta límite de distancia mientras el auto se encuentre dentro de la cobertura GSM.

ALARMA DE COCHE CON SISTEMA ANTI-ASALTO: Este sistema trabaja conjuntamente con el bloqueo del motor, permitiendo recuperar con facilidad el automóvil después de haber sido robado, activándose una sirena y cortando el suministro de energía al motor provocando que el auto se apague y no pueda volver a encenderse [12].

INMOVILIZADOR: Es un sistema antirrobo que inhabilita el sistema de ignición del vehículo cuando alguien intente encenderlo sin la llave original.

La Unidad de Control Electrónico (ECU) del vehículo es la encargada de proporcionar los permisos necesarios para que las funciones de encendido del auto y la inyección de gasolina o diésel funcionen.

- **CARACTERÍSTICAS DE LOS INMOVILIZADORES**

Las características de los sistemas inmovilizadores varían según las protecciones que brinden, clasificándose así en cuatro grupos:

Antirrobo de fábrica: Consiste en un sistema inhibidor de encendido basado en un chip conocido como transponder en el interior de la llave, el auto reconoce la llave y permite el encendido, caso contrario el sistema bloquea el encendido del auto, incluso si se intenta prenderlo cortando cables.

Seguridad de fábrica: Cuando este sistema se activa, bloquea las puertas y cuando alguien intenta abrirlas, la bocina empieza a sonar. La desventaja que presenta es que al ser un sistema instalado de fábrica, en la mayoría de autos es similar y además en el manual del vehículo se muestra todas las conexiones, de esta manera cualquier persona puede activarla o desactivarla.

Seguridad de Especialista: La gran ventaja es que al ser instalado por personal certificado, todas las conexiones y ubicación de los componentes del sistema, solo los conoce la persona que instala y en algunos casos el dueño del auto.

Seguimiento post-robo: Sistema que gracias al uso del GPS, realiza un seguimiento del vehículo [13].

2.2.4 SISTEMAS BIOMÉTRICOS

Siempre ha sido necesario el uso de carnets, cédulas, contraseñas o claves que permitan identificar a una determinada persona que ingresa a un lugar y así evitar ser víctimas de robos o fraudes, pero poco a poco este tipo de identificaciones han ido perdiendo su veracidad pues han podido ser vulneradas, duplicadas o simplemente robadas. Este es el motivo que ha impulsado al desarrollo de sistemas biométricos que emplean información única del usuario creando sistemas autónomos muy seguros [14].

La biometría en la actualidad se ha convertido en una ciencia muy investigada por su alta confiabilidad al momento de tratar con sistemas de seguridad, controles de acceso, identificación de personal, reconocimiento de personas entre otros sistemas que validan la identidad de una persona, mediante sus características propias como sus huellas dactilares, el iris del ojo, su voz, rasgos faciales, rasgos corporales, gestos [15].

Es necesario que la información que requiere el sistema biométrico, es decir, los rasgos personales de un individuo, cumpla con algunas cualidades para que el sistema funcione adecuadamente:

- **Permanencia**: la característica no debe cambiar con el tiempo, o hacerlo muy lentamente.
- **Unicidad**: la existencia de dos personas con una característica idéntica debe tener una probabilidad muy pequeña.
- **Universalidad**: cualquier persona debe poseer esa característica.
- **Cuantificación**: la característica puede ser medida de forma cuantitativa.
- **Mensurabilidad**: Se debe poder medir las características de la muestra de una manera rápida, fácil y precisa usando métodos no intrusivos.

Aunque en la práctica también se debe cumplir con otros aspectos como:

- **Realización**: es decir, ver la posibilidad de una identificación exacta, los recursos requeridos y los factores del entorno y de trabajo que afectan a la identificación.
- **Aceptabilidad**: que se refiere al grado de aceptación por parte de población que estaría predispuesta a aceptar el sistema de identificación.
- **Engañable**: referido a qué tan fácil resulta engañar al sistema con técnicas fraudulentas.

Varios países alrededor del mundo han adoptado los sistemas biométricos como su principal sistema de seguridad, sobre todo aquellos que trabajan con las huellas dactilares, pero como la ciencia y tecnología avanzan de manera sorprendente, ya se han desarrollado, métodos más certeros de identificación

basados en la colección de muestras de ácido desoxirribonucleico (ADN), cuyos grados de confiabilidad resultan casi infalibles, convirtiendo a los sistemas biométricos en el método más confiable de detección e identificación humana [16].

2.2.5 CLASIFICACIÓN DE LOS SISTEMAS BIOMÉTRICOS

A los sistemas biométricos se los puede clasificar de acuerdo al siguiente criterio:

- Según su tipo
- Según su tecnología
- Según su uso

A continuación se analiza de manera general cada una de estas clasificaciones de los sistemas biométricos.

❖ SISTEMAS BIOMÉTRICOS SEGÚN SU TIPO

Dentro de este grupo se encuentran los sistemas que hacen uso de la biometría estática y de la biometría dinámica.

Biometría Estática: Cuando emplea como fuente de información las características físicas de una persona: huellas dactilares, retina, color de iris, reconocimiento facial, geometría de la mano.

Biometría Dinámica: Trabaja con las características conductales de una persona, como: reconocimiento de voz, firma, letra.

❖ SISTEMAS BIOMÉTRICOS SEGÚN SU TECNOLOGÍA

Una investigación incesante por varios años ha dado como resultado una variedad de sistemas biométricos a elegir de acuerdo a la aplicación y necesidad de las personas, entre éstos se encuentran:

Reconocimiento de Huella Dactilar: que emplea como patrón las huellas o surcos de las manos conocidos como puntos de minucia y que son únicos en cada persona.

Reconocimiento de Iris y Retina: a pesar de que el iris y la retina pertenecen a un mismo órgano (ojo humano), su análisis tienen procesos diferentes.

Cuando se trabaja con el iris, es importante considerar algunos factores como el tipo de cámara digital que se emplee, el entorno y la iluminación, ya que éstos pueden afectar la efectividad del sistema.

Por otro lado, el análisis de la retina humana, utiliza los patrones de vasos sanguíneos presentes en esta, ya que al igual que las huellas dactilares, posee características únicas en cada persona.

Reconocimiento de Geometría de la mano: En este método de debe proporcionar información como el tamaño de los dedos, separación entre estos y todas las características que se puedan obtener sobre su geometría.

Reconocimiento de Firma: La escritura es capaz de proporcionar mucha información de un individuo sobre su personalidad, por este motivo, puede identificar a una persona gracias a los signos y símbolos presentes en ella.

Reconocimiento de Voz: Para identificar a una persona mediante su voz se han desarrollado varios algoritmos encargados de transformar y procesar la voz humana, pero por su grado de complejidad no son muy empleados en el ámbito de la seguridad [14].

La correcta elección del sistema biométrico depende de la aplicación que se le va a dar, así como del lugar en el que va a ser instalado. Para facilitar un poco más esta elección, la tabla 2.1 presenta un resumen de las características generales de los sistemas biométricos aquí propuestos:

Tabla 2.1 Características de los sistemas biométricos [18]

Característica	OJO (Iris)	OJO (Retina)	Huellas Dactilares	Geometría de Mano	Escritura y Firma	Voz	Cara
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Factibilidad de uso	Media	Baja	Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Alta	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

❖ SISTEMAS BIOMÉTRICOS SEGÚN SU USO

Los sistemas biométricos se han vuelto muy populares gracias a su innegable eficiencia que tanto organismos públicos como privados están haciendo uso de ellos, pero es importante mencionar el grado de aceptación que han tenido para poder clasificarlos como se muestra en la figura 2.4

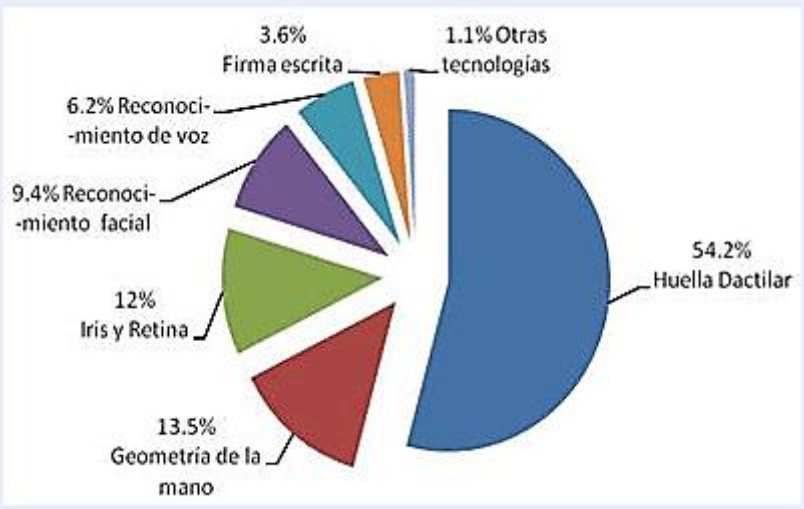


Figura 2. 4 Distribución de tecnologías biométricas según su uso [14]

❖ VENTAJAS E INCONVENIENTES DE LOS DISTINTOS TIPOS DE TECNOLOGÍA BIOMÉTRICA

Cada una de las tecnologías mencionadas, posee características favorables, entonces la elección de una u otra de estas alternativas depende únicamente del lugar en donde se desee implementarlo y de la funcionalidad que va a tener el sistema biométrico.

A continuación, en la tabla 2.2 se presenta un resumen de las ventajas e inconvenientes que presenta cada una de las tecnologías biométricas de acuerdo a una investigación desarrollada por un grupo humano pertenecientes al Observatorio de la Seguridad de la Información del Instituto Nacional de Tecnologías de la Comunicación INTECO de España en el año 2011.

Tabla 2.2 Ventajas e Inconvenientes de las tecnologías biométricas [17]

Tecnología	Ventajas	Inconvenientes
Huella dactilar	• Alto grado de madurez • Costes de implantación reducidos • Buena aceptación	• Incompatibilidad con determinados trabajos manuales
Reconocimiento de voz	• No requiere inversión en dispositivos • Posibilidad de autenticación remota	• El ruido de fondo dificulta la captura • Dificultad para reconocer ciertas formas de hablar
Reconocimiento facial	• Reconocimiento en multitudes • Identificación a media distancia • Buena aceptación	• Escasa resistencia al fraude • Unicidad limitada
Reconocimiento de iris	• Patrones muy complejos • Unicidad muy alta • Alto grado de permanencia	• Coste de implantación alto • Menor grado de aceptación
Reconocimiento de retina	• Unicidad muy alta • Alto grado de permanencia	• Precisa de total colaboración del usuario
Reconocimiento de la geometría de la mano	• Alto grado de permanencia • Facilidad de uso	• Unicidad limitada
Reconocimiento de firma	• Buena aceptación • Facilidad de uso	• Dificultad de captura por cambios de posición
Reconocimiento de escritura de teclado	• No requiere inversión en dispositivos • Posibilidad de realizar monitorización	• Tecnología emergente

2.2.6 VULNERABILIDADES DE LOS SISTEMAS BIOMÉTRICOS

De acuerdo a la investigación realizada por INTECO, además de los inconvenientes propios de cada tipo de tecnología biométrica, existen otros factores que no permiten su amplio desarrollo

En la tabla 2.3 se listan las vulnerabilidades que impiden la correcta implantación de los sistemas de reconocimiento biométrico impidiendo su eficiente rendimiento [17].

Tabla 2.3 Vulnerabilidades de las tecnologías biométricas [17]

Tecnología biométrica	Vulnerabilidades
Vulnerabilidades comunes a todas las tecnologías biométricas	• Calidad baja de los dispositivos de captura. • Ubicación inadecuada del dispositivo de captura. • Desconocimiento en la calidad o del abanico de productos y utilidades disponibles. • Falta de conocimientos técnicos del personal. • Falta de recursos (tanto de personal como económicos). • Escasa concienciación en materia de seguridad. • Percepción de ausencia de privacidad por parte de los usuarios.
Huella dactilar	• Condición del dedo en el momento de tomar la muestra: mojado, seco, manchado, etc. • Condiciones climatológicas que afectan al lector: humedad, temperatura, etc. • Condiciones de la huella: cortes, heridas o inflamaciones. • Actividad laboral: trabajos que puedan afectar a la huella, por ejemplo el uso habitual de productos químicos que puedan deteriorarla.
Reconocimiento de voz	• Enfermedades de la voz: bronquitis, faringitis, gripe, laringitis, afonías, etc. • Variación entre el dispositivo de registro y el usado en la captura de muestras. • Variación entre entornos de registro y captura de muestras (por ejemplo: interior y exterior). • Volumen del habla.
Reconocimiento facial	• Variación en el aspecto facial: peinado, vello, gafas, sombrero, etc. • Condiciones de luminosidad. • Variación en el peso. • Uso de vestimenta que puede dificultar la localización o visión de la cara (pañuelos, bufandas, etc.).
Escáner de iris y retina	• Excesivo movimiento ocular o de la cabeza. • Enfermedades oculares. • Uso de gafas. • Problemas debidos al uso de lentes de contacto (iris).
Geometría de la mano	• Uso de joyería, bisutería o abalorios. • Uso de vendajes o guantes. • Condiciones de la mano: inflamaciones en las articulaciones, heridas, etc.
Escáner de firma	• Velocidad de la firma: excesivamente rápida o lenta. • Diferente postura del sujeto durante la firma. • Firma no consistente: el sujeto varía su firma.

2.2.7 CARACTERÍSTICAS PARA IDENTIFICACIÓN PERSONAL

Algunas de las características que debe cumplir un sistema de identificación personal son [4]:

- El desempeño, característica que evalúa la efectividad del sistema en cuanto a exactitud, rapidez y robustez que se logra alcanzar en la identificación, en base a los recursos empleados.
- La aceptabilidad, factor que indica si la gente está dispuesta o no a aceptar un sistema biométrico en su vida diaria.
- La fiabilidad, que muestra el nivel de seguridad del sistema, es decir, permite conocer si el sistema es o no difícil de vulnerar.

2.2.8 SISTEMA DE PROCESAMIENTO DIGITAL DE IMÁGENES

El procesamiento digital de imágenes es una tecnología que se relaciona con las ciencias de la computación, por lo que se suele decir que el procesamiento digital de imágenes es una proyección de la inteligencia artificial formando parte de la rama de la visión artificial.

Para realizar este procesamiento es necesario el uso de algunos recursos tecnológicos, tanto en software como hardware, los que permiten la adquisición y manipulación de grandes cantidades de información espacial en forma de matrices de valores. Todo este conjunto de elementos que procesan la señal visual forman el denominado “Sistema de Procesamiento digital de Imágenes”.

Para procesar la “imagen real” que ha sido capturada se debe pasar por una serie de etapas como se muestran en la figura 2.5:

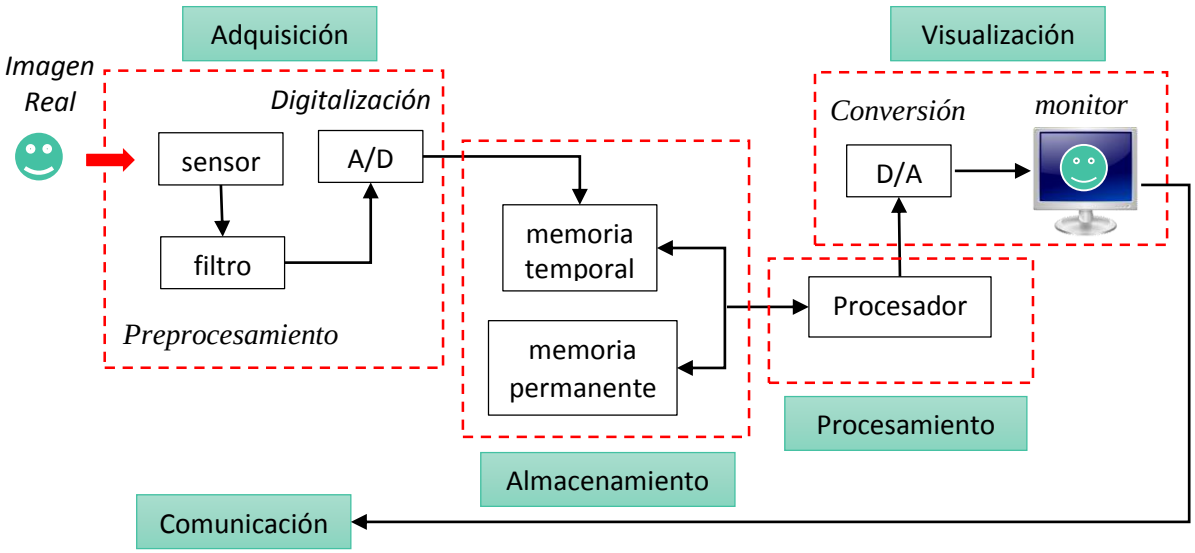


Figura 2. 5 Configuración básica de un sistema de procesamiento digital de imágenes: adquisición, procesamiento, almacenamiento, visualización y comunicación con otros procesadores [18].

2.2.9 PROCESAMIENTO DIGITAL DE IMÁGENES

El procesamiento de la imagen se emplea para mejorarla y adecuarla para una determinada aplicación, este hecho implica que la adopción de una u otra técnica para el procesamiento de la imagen van a depender del uso posterior de la misma.

Existen dos campos en los que se puede dividir los métodos de procesamiento de imágenes: los que trabajan en el dominio frecuencial, y los métodos en el dominio espacial que manipulan directamente los píxeles de la imagen.

2.2.10 RECONOCIMIENTO FACIAL

El reconocimiento facial es un proceso o aplicación controlada por un ordenador que identifica automáticamente a una persona comparando sus rasgos faciales extraídos de una imagen digital con una base de datos almacenada previamente.

Estos mecanismos son muy empleados en la actualidad presentando diversas aplicaciones como se indica en la tabla 2.4:

Tabla 2.4 Escenarios de aplicación del reconocimiento facial [18]

ÁREAS	APLICACIONES ESPECÍFICAS
Biometría	Licencia de Conducir, Programas de Derecho, Inmigración, DNI, Pasaportes, Registro de Votantes, Fraude
Control de acceso	Acceso de vehículos, facilidad de acceso, acceso a ordenadores, acceso a programas de ordenador, acceso a redes de ordenadores, acceso a programas online
Bases de datos	Catalogación y recuperación de caras, etiquetado automático de caras, clasificación de caras
Cumplimiento de la ley y vigilancia	Videovigilancia Avanzada, Control CCTV, Control Portal, Análisis Post-event, Hurto, Seguimiento de Sospechosos
Tarjetas inteligentes	Valor Almacenado, Autenticación de usuarios
Control de acceso	Acceso a Instalaciones, Acceso a Vehículos

El reconocimiento facial automatizado es un concepto relativamente nuevo, pues se introdujo en los años 60, desde entonces ha sufrido una constante evolución pues cada día van surgiendo nuevos métodos biométricos que garantizan seguridad, inviolabilidad y confiabilidad a la hora de obtener los datos [19].

Poco a poco estas técnicas han ido mejorando, incluyendo otras características como color de cabello, de ojos, grosor de labios, aumentando así la exactitud de los resultados, permitiendo desarrollar sistemas automatizados de reconocimiento facial en tiempo real.

Para realizar una determinada aplicación de reconocimiento facial, se deben cumplir diferentes etapas, una de ellas es la etapa de detección facial, que por lo general se la trabaja conjuntamente con la del reconocimiento.

Todas las etapas que componen un sistema de reconocimiento facial se lo puede apreciar en la figura 2.6.

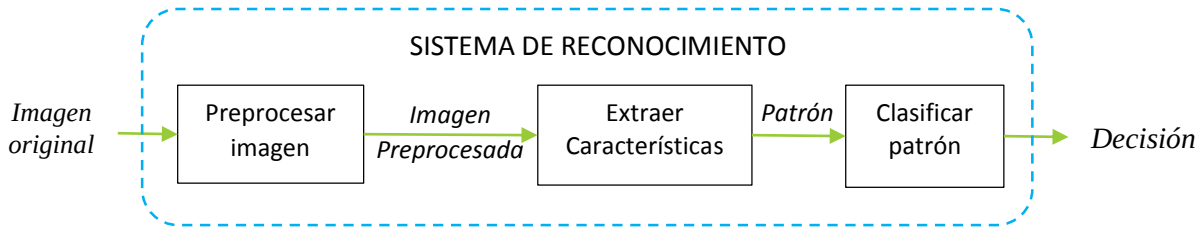


Figura 2. 6 Diagrama de bloques general de un sistema de reconocimiento facial [20]

El proceso inicia con la detección del rostro y procesado del mismo para poder extraer sus características y así compararlas con un patrón previamente almacenado, logrando finalmente tomar una decisión de acuerdo a los resultados obtenidos en la comparación.

❖ CARACTERÍSTICAS DEL RECONOCIMIENTO FACIAL

Para que la aplicación de un sistema de seguridad basado en reconocimiento facial sea efectiva, se debe considerar que los rasgos a analizarse cumplan con algunas características como [20]:

- Universalidad, indica que tan común es encontrar esta característica en todas las personas u objetos a reconocer.
- Carácter distintivo, indica si dicha propiedad, es suficientemente diferente entre un conjunto de personas u objetos diferentes.
- Permanencia, indica la estabilidad en el tiempo de dicha característica.
- Colectividad, indica si la característica es fácilmente adquirida y medida por el sistema.
- Rendimiento, indica la precisión, velocidad y coste (recursos) necesarios para llevar a cabo el reconocimiento.
- Aceptabilidad, indica en qué medida está la gente preparada para aceptar el uso de esta técnica.
- Elusión, indica la respuesta del sistema cuando alguien está tratando de engañarlo.

Pero como todo sistema de seguridad puede presentar algunas limitaciones que no lo hacen óptimo y totalmente confiable, impidiéndolo estar exento de fallas debido a las desventajas que conlleva el trabajar con rasgos faciales como:

- Orientación del rostro.
- Ruido.
- Iluminación (incluyendo interior / exterior).
- Expresión facial.

- Oclusión debido a objetos o accesorios tales como gafas de sol, sombreros…
- Vello facial.
- Envejecimiento

Aunque algunos de estos problemas pueden ser corregidos si se actualizan constantemente las bases de datos.

❖ VENTAJAS Y DEVENTAJAS DEL RECONOCIMIENTO FACIAL

El sistema biométrico facial es un sistema que presenta importantes ventajas sobre otros tipos de sistemas similares como:

- Es un sistema no intrusivo, es decir que el usuario no siente invadida su intimidad puesto que no necesita realizar ningún tipo de análisis para ser identificado
- Permite eliminar la memorización de códigos o contraseñas.
- Evita el uso de llaves, tarjetas, pasaportes, DNI, etc.

Sin embargo, existen inconvenientes que impiden que el reconocimiento facial, sea la mejor alternativa en cuanto a sistemas biométricos, como por ejemplo [18]:

- No funcionan si los individuos se presentan con algún tipo de máscara cubriendo su rostro.
- Debido a que el reconocimiento se ve afectado por las condiciones de luminosidad, rotación, enfoque de la cámara, entre otros, el sistema presenta un funcionamiento óptimo solo en condiciones de laboratorio.
- Otro inconveniente de un biométrico facial, es que en su fase de prueba se emplea una base de datos con un número bajo de individuos, comparada al número de sujetos que en la realidad debería poder analizar, si se lo implementa en lugares públicos muy grandes como estadios, aeropuertos, terminales, etc.

2.2.11 TIPOS DE TÉCNICAS DE RECONOCIMIENTO FACIAL

Para un mejor estudio de los diferentes métodos y técnicas existentes para realizar un proceso de reconocimiento facial se las ha agrupado de la siguiente manera:

- **MÉTODOS BASADOS EN IMÁGENES FIJAS:**

Según la bibliografía analizada, varias investigaciones muestran que los métodos basados en imágenes fijas son los más utilizados y desarrollados.

A este grupo pertenecen técnicas como: Análisis de Componentes Principales (ACP) o también llamada Eigenfaces, Análisis de discriminantes lineales de Fisher o Fisherfaces (FLD), Conservación de Proyecciones Locales (LPP) o Laplacianfaces, Análisis de Componentes Independientes (ACI), entre otras.

La mayoría de autores coinciden que este grupo de técnicas se ven más afectadas por condiciones luminosas antes que por posición de la cara, rotación, o presencia de accesorios en el rostro, por lo que es necesario realizar algunas correcciones a las imágenes antes de procesarlas [21].

- **MÉTODOS BASADOS EN IMÁGENES 3D**

Por otro lado están los sistemas que están basados en modelos o imágenes 3D de la cabeza de una persona los cuales intentan construir un modelo lo más descriptivo posible de la cara humana capaz de detectar con precisión las variaciones faciales; su objetivo es obtener características biométricas de las imágenes como: (distancia entre ojos, grosor de la nariz…), para realizar el reconocimiento, pero estas técnicas requieren de imágenes de gran resolución, para esto se usa un arreglo de cámaras con un escáner especializado o bien se usan tomas en 2D de la cabeza de la persona desde diferentes ángulos y así poder formar una imagen en 3D, una de las ventajas de estas técnicas es que no se ven afectadas por la pose, iluminación y gestos de las personas.

❖ MÉTODOS BASADOS EN VIDEO

Este método contempla las relaciones existentes entre los *frames* de un video. Generalmente se emplean videos de baja resolución como los que provienen de fuentes como televisión, sistemas de seguridad, video conferencias, entre otras.

En el año 2002, un informe industrial reveló que los resultados obtenidos de un sistema basado en video, no eran mejores a los presentados por un sistema de reconocimiento mediante imágenes fijas, posteriormente, el mismo informe presentado en el año 2006, ya no incluyó a este tipo de métodos dentro de las técnicas aplicables al reconocimiento facial, pero si resalta el desempeño y el avance de las técnicas basadas en imágenes fijas y en 3D [20].

Resulta complejo realizar una comparación entre estas categorías, pues cada una trabaja con bases de datos muy distintas; por una parte se encuentran las imágenes en 3D que debido al empleo de escáneres muy costosos, la cantidad de imágenes es limitado, por otro lado están los sistemas basados en video, cuyo problema es la excesiva cantidad de información que almacenan y finalmente el sistema de imágenes fijas con una extensa base de datos, por esta razón no se compara entre categorías pero si se puede comparar y elegir que técnica es la más adecuada dentro de una misma categoría; aunque varias investigaciones han demostrado que las técnicas basadas en video y en imágenes 3D no aumentan el desempeño de los sistemas de reconocimiento facial, por ser su implementación muy costosa y más compleja, quedando los sistemas basados en el empleo de imágenes fijas como la mejor alternativa para realizar un sistema de reconocimiento facial [21].

Después de este análisis, es posible mencionar algunas de las ventajas e inconvenientes de los sistemas basados en la apariencia frente a los basados en modelos, como por ejemplo [20]:

Ventajas:

- Más rápidos.
- Requieren de un menor tamaño de las imágenes.

- Menor complejidad.
- No requieren de un conocimiento previo de las imágenes.

Inconvenientes:

- Más afectados por cambios en la orientación o expresión de la cara.
- Más dificultades frente a cambios en la iluminación

2.2.12 PRINCIALES TÉCNICAS DE RECONOCIMIENTO FACIAL

Existe una amplia gama de posibles técnicas para realizar un reconocimiento de rostros, a continuación se detallan las más utilizadas:

- **ANÁLISIS DE COMPONENTES PRINCIPALES (ACP)**

Como ya se ha mencionado, el grupo de técnicas que trabajan con imágenes fijas, son las más adecuadas para realizar un sistema de reconocimiento facial, y dentro de esta categoría la técnica ACP, es la más opcionada para realizar esta tarea.

Está técnica es la base a partir de la cual se han venido desarrollando todas las técnicas existentes para el reconocimiento de rostros. También se la conoce como el método de eigenfaces o eigenvectores y fue propuesta en un inicio por Turk y Pentland en 1991 [23].

ACP es un algoritmo de reducción dimensional que permite encontrar los vectores que mejor representan la distribución de un grupo de imágenes eliminando la información que no es útil, esto se logra gracias al uso de la técnica de análisis de componentes principales maximizando la variación de la matriz de covarianza de todas las imágenes de la base de datos, entendiendo que la covarianza es el valor que representa la variación conjunta de dos variables aleatorias, permitiendo determinar la dependencia entre ambas variables.

El motivo por el cual esta técnica es la más adecuada para realizar un reconocimiento facial, se debe a la simplicidad de su algoritmo y la facilidad de

su implementación, así como el bajo coste computacional que requiere permitiendo desarrollar sistemas en tiempo real [21].

La implementación de esta técnica implica desarrollar cada uno de los pasos que se indican en la figura 2.7 pertenecientes al algoritmo de eigenfaces (ACP).

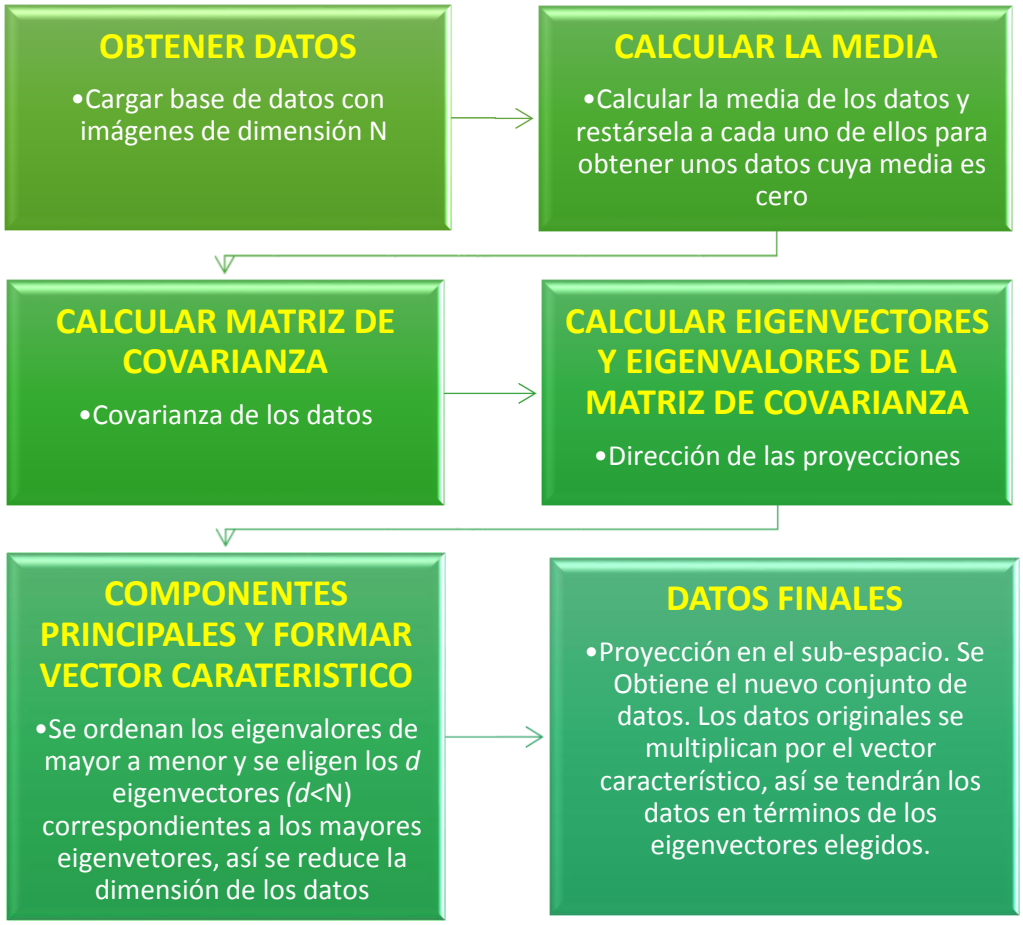


Figura 2. 7 Algoritmo ACP [18]

Otra de las cualidades de ACP, es que realiza una discriminación entre clases, es decir, todas las caras correspondientes a un mismo individuo están cerca entre sí, mientras que las imágenes correspondientes a individuos diferentes están más alejadas [20].

La aproximación PCA típicamente requiere la cara completa de frente para ser presentada cada vez; de otra forma la imagen dará un resultado de bajo rendimiento.

La técnica de PCA se basa en el algoritmo de eigenfaces con algunas modificaciones simples, por lo tanto a continuación se va a analizar cómo funciona este algoritmo.

❖ EIGENFACES

Inicialmente el algoritmo de eigenfaces fue desarrollado por Sirovich y Kirby en el año de 1897, cuyo objetivo fue encontrar la manera de emplear un número mínimo de parámetros para representar un conjunto de caras; y para conseguirlo, emplearon la técnica de PCA logrando generar ciertas imágenes similares a rostros que las llamaron eigenpictures; posteriormente fueron Turk y Pentland quienes bautizan a las eigenpictures como eigenfaces [23].

Así como cualquier color puede ser formado a partir de los colores primarios, lo mismo sucede con los rostros; cualquier cara se puede formar a partir de una combinación de caras (eigenfaces), es así que los eigenfaces son vectores de datos (eigenvectores), donde cada uno posee valores escalares conocidos como eigenvalores.

Es necesario que las imágenes cumplan con ciertas características para el buen desarrollo del algoritmo, para esto se realiza un pre-procesado a las imágenes para que todas tengan las mismas condiciones de luz, contraste, resolución y tamaño y así evitar que dos imágenes de la misma cara sean diferentes. Posteriormente se debe normalizar la línea de los ojos y de la boca, para lo cual las imágenes de entrenamiento deben estar alineadas como se indica en la figura 2.8.

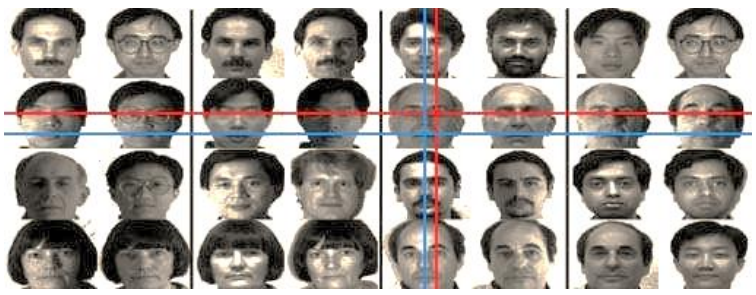


Figura 2. 8 Grupo de imágenes normalizadas a la línea de los ojos y de la boca [14]

La técnica de Análisis de Componentes Principales (PCA), permite extraer estos eigenfaces; una vez calculados se presentan como zonas luminosas y oscuras organizadas de acuerdo a un patrón específico que se ha formado con todos los rasgos faciales considerados para ser evaluados, por ejemplo habrá un patrón para evaluar la simetría, otro para determinar el tamaño de la nariz o la boca [15].

- **ANÁLISIS DISCRIMINANTE LINEAL (ADL)**

Otra de las técnicas mencionadas para el reconocimiento facial es la de Análisis Lineal Discriminante que busca obtener una separación lo más grande posible entre clases para lo cual proyecta los datos en un espacio de menor (o incluso igual) dimensión que los datos entrantes.

Es una técnica supervisada ya que para poder buscar esa proyección se debe entrenar el sistema con patrones etiquetados.

Para poder aplicar este método es necesario disponer de un conjunto de caras de entrenamiento (x) formado por un grupo de personas con distintas expresiones faciales y con diferentes vistas, todas las imágenes de caras de la misma persona están en una clase (de tamaño N), y las caras de otras personas diferentes pertenecen a distintas clases (habrá C clases), teniendo así el espacio de entrenamiento separado en grupos, además todas las imágenes del conjunto de entrenamiento deben estar etiquetadas [18].

Como se representa en la figura 2.9; en LDA el objetivo principal es maximizar la varianza entre clases, (ej. Entre usuarios) y minimizar la varianza de cada clase (Ej. De cada usuario), es decir; donde cada bloque representa una clase, hay grandes variaciones entre clases, pero pequeñas en cada clase.

Figura 2. 9 Ejemplo de seis clases usando LDA [18]

Es importante aclarar que LDA no busca en ningún momento minimizar el error de representación cometido, como se hace en PCA, pero esta técnica si se enfrenta a un problema cuando se trata con datos faciales de alta dimensión, pues surge un inconveniente cuando existen muestras de tamaño pequeño que se presentan donde hay un número pequeño de ejemplos de entrenamiento comparados a la dimensionalidad del espacio de muestra. Para realizar un reconocimiento facial usando LDA, el algoritmo que se emplea básicamente es el que se muestra en la figura 2.10.

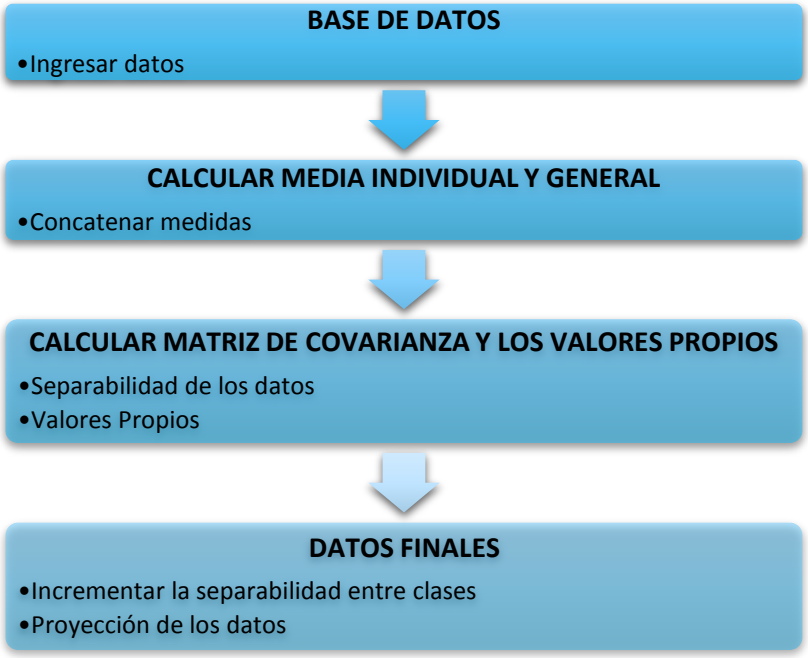


Figura 2. 10 Algoritmo LDA [18]

- **PRESERVAR PROYECCIONES LOCALES (PPL)**

La técnica de LPP del inglés Locality Preserving Projections, posee un algoritmo lineal similar al que se emplea en PCA, es rápido y útil para aplicaciones prácticas ya que reduce la dimensionalidad de los datos, pero a diferencia de PCA que conserva la estructura global de estos datos, en LPP se conserva la estructura local; con esto se logra que los "vecinos" para un dato específico sean los mismos en el espacio original que tiene alta dimensionalidad, y en el nuevo sub-espacio de baja dimensionalidad; así las imágenes pertenecientes a un mismo individuo estarán cercanas entre si y alejadas de las de otros individuos,

es decir, hay una discriminación entre clases tal como se muestra en la figura 2.11.

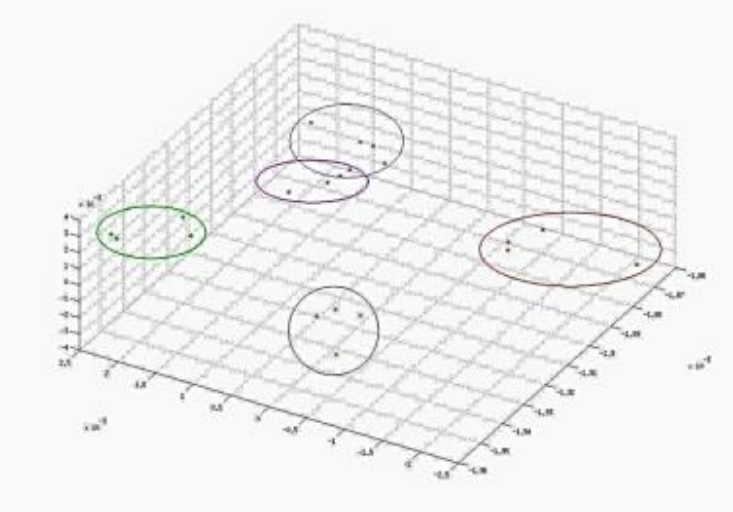


Figura 2. 11 Representación de la estructura de los datos en el nuevo subespacio, ejemplo formado por 5 personas y cuatro imágenes por persona [20]

Pero esta técnica presenta dificultad cuando se requiere recuperar los datos originales a partir de los datos proyectados al nuevo subespacio, esto se debe al hecho de hacer uso de bases no ortogonales. También surge otro problema al trabajar con matrices singulares ya que los datos de entrada tienen una mayor dimensionalidad que el número de muestras ($n >> N$), donde n son los datos y N las muestras. Este inconveniente se soluciona mediante técnicas que permitan reducir la dimensión de antes de utilizarlos de manera que $n = N$ o $n > N$ [20].

- **CORRESPONDENCIA ENTRE AGRUPACIONES DE GRAFOS ELÁSTICOS - ELASTIC BUNCH GRAPH MATCHIN (EBGM)**

Una de las grandes ventajas de esta técnica es que para poder realizar el reconocimiento de un rostro no utiliza la imagen total de la cara, sino que emplea únicamente puntos de interés.

Para implementar esta técnica se debe desarrollar dos etapas:

1. Primero se establece un modelo estadístico del rostro de la persona que se va a reconocer y se determinan los puntos de interés.
2. Después se debe extraer las características locales de cada punto para finalmente calcular la distancia entre este patrón junto con sus descriptores y el grafo almacenado de la persona a reconocer.

Al igual que sucede con todas las técnicas, es necesario normalizar las imágenes, pero para usar EBGM es necesario realizar transformaciones geométricas para poder ubicar correctamente las coordenadas de los ojos en posiciones específicas, en la figura 2.12 se presenta el grafo realizado por EBGM de una imagen de un rostro.

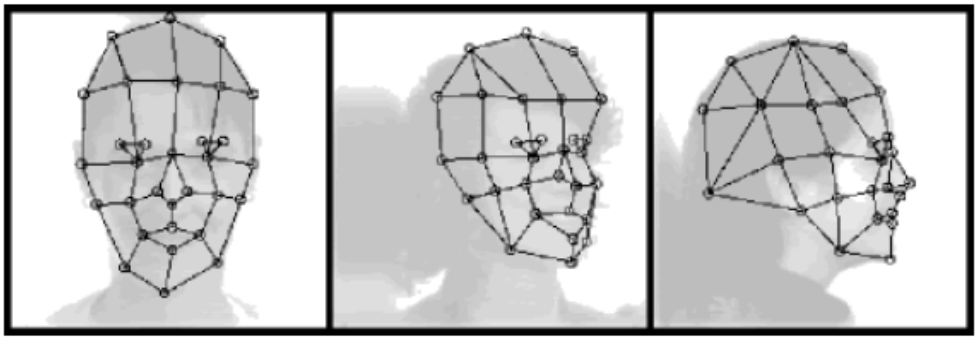


Figura 2. 12 Correspondencia entre agrupaciones de grafos elásticos [24]

El desarrollo de ésta técnica implica el uso de Wavelets Gabor que son filtros espaciales paso-banda, de esta manera se puede alcanzar los niveles máximos referentes a información de los espacios bidimensionales espacial y frecuencial de una región específica de la imagen.

Este proceso se logra mediante la operación de convolución de la región de interés con una variedad de wavelets que han sido almacenadas como máscaras dentro de matrices.

A pesar de que este algoritmo no se ve afectado por factores como la variación en la iluminación, postura y expresión, presenta mucha dificultad en localización precisa del punto de referencia

- **MODELO DE APARIENCIA ACTIVA (MAA)**

Mediante una etapa de entrenamiento, esta técnica permite reproducir un modelo estadístico de la forma y apariencia del objeto de interés. Para lograrlo se determina una malla formada por N puntos característicos conocidos como parámetros de forma, en la figura 2.13 se aprecia la forma en que trabaja MAA en cuanto a la formación de mallas.

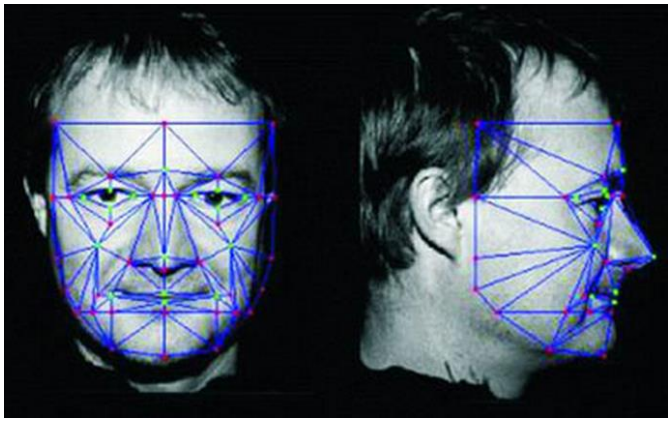


Figura 2. 13 Ejemplo de malla en MAA [24]

Posteriormente, mediante el uso de PCA se calcula los componentes principales, formando un subespacio y mediante una combinación lineal de los vectores dentro de este subespacio se puede formar cualquier instancia de la forma del modelo.

El modelo MAA es un buen método estadístico para ajustes de plantillas, el cual usa toda la información de la cara, es decir, no solo los puntos de los bordes, sino también los interiores [24].

2.2.13 SOFTWARE MATLAB

Matlab, programado originalmente por Cleve Moler a finales de la década de los 70, es un software matemático desarrollado como una herramienta de apoyo para el estudio de la Teoría de Matrices, Álgebra Lineal y Análisis Numérico, siendo el nombre de Matlab acrónimo de “MATrix LABoratory” (Laboratorio de Matrices).

Debido a las múltiples características que presenta, Matlab se ha convertido en el software más utilizado a nivel de universidades, por científicos e ingenieros, extendiéndose así sus aplicaciones.

Las nuevas ramas en las que se aplica Matlab así como el cálculo científico y las ciencias aplicadas, se han dado gracias a la implementación de *toolboxes*, librerías escritas en el lenguaje de programación propio de Matlab permitiendo resolver una mayor cantidad de problemas y la capacidad de comunicarse con otros lenguajes y dispositivos hardware.

Algunas de las áreas en donde Matlab es la herramienta de trabajo más adecuada son:

- Algebra Lineal Numérica
- Procesamiento de Señales (análisis, compresión de datos,…)
- Diseño de Sistemas de Control
- Salidas Gráficas
- Estadística
- Simulación de Sistemas Dinámicos

MATLAB brinda un entorno de desarrollo integrado (IDE); es decir, que consiste en un editor de código, un compilador, un depurador y un constructor de interfaz gráfica (GUI), además posee un lenguaje de programación propio (lenguaje M). Actualmente se encuentra disponible para diversas plataformas como: Unix, Windows, Mac OS X y GNU/Linux.

El paquete MATLAB dispone de dos herramientas adicionales que exhpanden sus prestaciones: Simulink (plataforma de simulación multidominio) y GUIDE (editor de interfaces de usuario - GUI).

❖ TOOLBOX DE PROCESAMIENTO DIGITAL DE IMÁGENES

Dentro de esta amplia gama de herramientas que brinda Matlab, la toolbox para el Procesamiento Digital de Imágenes es de gran interés para el desarrollo de este proyecto.

Esta toolbox permite trabajar con distintos tipos de imágenes emitidas desde cualquier dispositivo electrónico como: cámaras digitales, sensores satelitales y aéreos, escáneres digitales, microscopios, telescopios y otros dispositivos médicos, así como también permite manipular imágenes de distintos formatos como: JPEG, JPEG 2000, TIFF, PNG, HDF, HDF- EOS, FITS, entre otras.

Las principales funciones de las que se compone esta Toolbox son:

- Mejora y filtrado de imágenes y enfoque de imágenes borrosas
- Análisis de imágenes, incluyendo segmentación, morfología, extracción de funciones y medición
- Transformaciones geométricas y métodos de registro de imágenes basados en intensidad
- Transformaciones de imágenes, incluyendo FFT, DCT y Proyección de haz de rayos de abanico.
- Flujos de trabajo para procesar, visualizar y navegar por imágenes arbitrariamente grandes.
- Herramientas interactivas, incluyendo selecciones de ROI, histogramas y mediciones de distancias [25].

2.2.14 ARDUINO

Arduino es una placa electrónica basada en una plataforma de hardware libre que facilita el desarrollo de proyectos electrónicos debido a que posee un microcontrolador y un entorno de desarrollo para programarlo que utiliza el lenguaje de programación Processing/Wiring; existen varios tipos de placas Arduino, la placa más básica es la Arduino Uno, como se muestra en la figura 2.14.

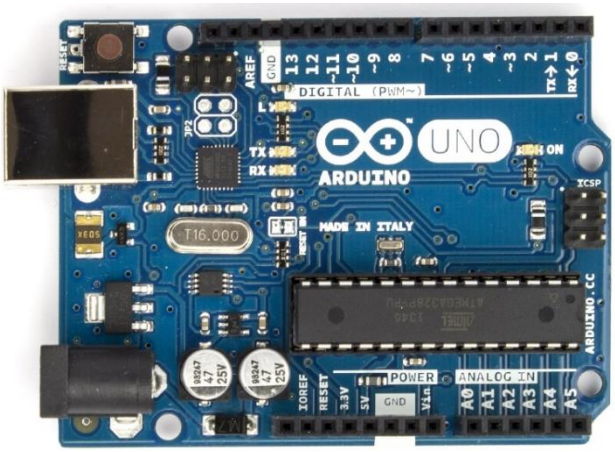


Figura 2. 14 Placa Arduino Uno [26]

Todos los programas creados en el software pueden ser cargados directamente en el microcontrolador mediante el cargador de arranque, de esta manera no es necesario el uso de un grabador de pic´s, pues la información se transmite en forma serial por el cable usb conectado a la placa.

En cuanto al hardware, la placa posee puertos de entrada/salida digitales y un bloque para entradas análogas, un resonador cerámico 16 MHz, una conexión USB, un conector de alimentación, una cabecera ICSP, y un botón de reinicio, la distribución de los pines se indican en la figura 2.15 [26]

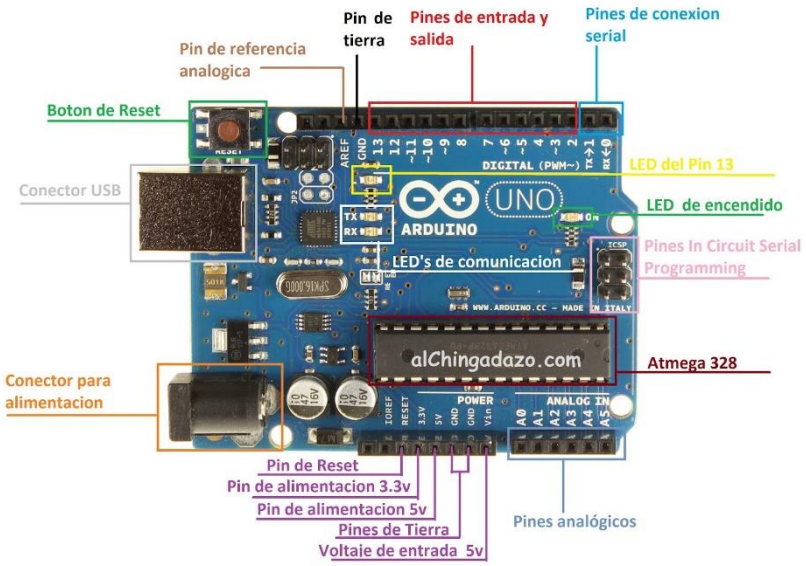


Figura 2. 15 Distribución de los pines placa Arduino Uno [26]

CAPÍTULO III

LA PROPUESTA

3.1 INTRODUCCIÓN

La sociedad actual, se enfrenta a un gran reto debido a la evolución tecnológica, pues trabajos cotidianos que normalmente los desarrollaban los seres humanos, ahora son realizados con mayor rapidez y precisión gracias a sistemas automatizados.

Grandes ciencias como la electrónica y la informática se han encargado de la creación de sistemas de seguridad cada vez más complejos y sofisticados, en donde la biometría juega un papel muy importante.

Hoy en día es común encontrar sistemas de identificación de individuos en las puertas de los domicilios, en empresas para registrar la asistencia de los empleados e incluso en los vehículos de último modelo, todo esto se debe al incremento de un mal social como lo es la delincuencia, ya que los criminales, han encontrado la forma de vulnerar las alarmas y sistemas de seguridad más comunes con una facilidad sorprendente.

Refiriéndose al sector vehicular, en la provincia de Tungurahua, el índice delincuencial se ha disminuido en cierto porcentaje, pero no se ha logrado erradicarlo por completo, ya que mientras en el año 2012 se reportaban hasta 16

carros sustraídos mensualmente, hasta el mes de junio del 2014 únicamente se han reportado 12 automotores sustraídos por mes [27].

Este notable decremento en la delincuencia se debe gracias a la instauración de nuevas estrategias policiales como la creación de diferentes UPCs (Unidad de Policía Comunitaria), la ayuda del Servicio Integrado de Seguridad ECU 911, los botones de seguridad instalados en la ciudad, y a las denuncias ciudadanas [28].

A pesar de que las estadísticas indican que se está logrando controlar la delincuencia, es necesario disponer de sistemas de seguridad confiables dentro de los automóviles pues nadie está exento de ser víctima de un robo. Por este motivo la población busca otras alternativas que les brinden mayor protección y seguridad.

La biometría se presenta como una alternativa ante esta problemática social, debido a que basa su funcionamiento en la recopilación de características (anatómicas o conductales) de un individuo para identificarlo, dichas características pueden permanecer relativamente estables con el pasar del tiempo como sucede con la huella dactilar, la silueta de la mano, patrones de la retina o el iris, lo que combinado con los equipos electrónicos y algoritmos adecuados puede convertirse en un sistema de seguridad altamente eficiente y difícil de vulnerar.

3.2 ANÁLISIS DE FACTIBILIDAD

3.2.1 FACTIILIDAD TÉCNICA

El proyecto de investigación técnicamente es factible desarrollarlo ya que los componentes electrónicos utilizados se encuentran con mucha facilidad dentro del mercado.

3.2.2 FACTIILIDAD ECONÓMICA

El desarrollo de este proyecto, económicamente es factible realizarlo por cuanto la investigadora financia el proyecto en su totalidad.

3.3 DESCRIPCIÓN GENERAL DEL SISTEMA DE SEGURIDAD

El sistema de seguridad de este proyecto funciona mediante la identificación del usuario del vehículo, usando como característica biométrica su rostro, extraído de una fotografía capturada mediante una cámara digital, para que después de ser reconocido se le permita hacer uso del automóvil, de esta manera se limita el número de personas que pueden conducir el vehículo, aumentando el nivel de seguridad.

3.4 FUNCIONAMIENTO DEL SISTEMA DE SEGURIDAD

El sistema ha sido adaptado para controlar el encendido del vehículo en base al resultado obtenido en la etapa del reconocimiento facial, su funcionamiento se puede apreciar en la figura 2.16.

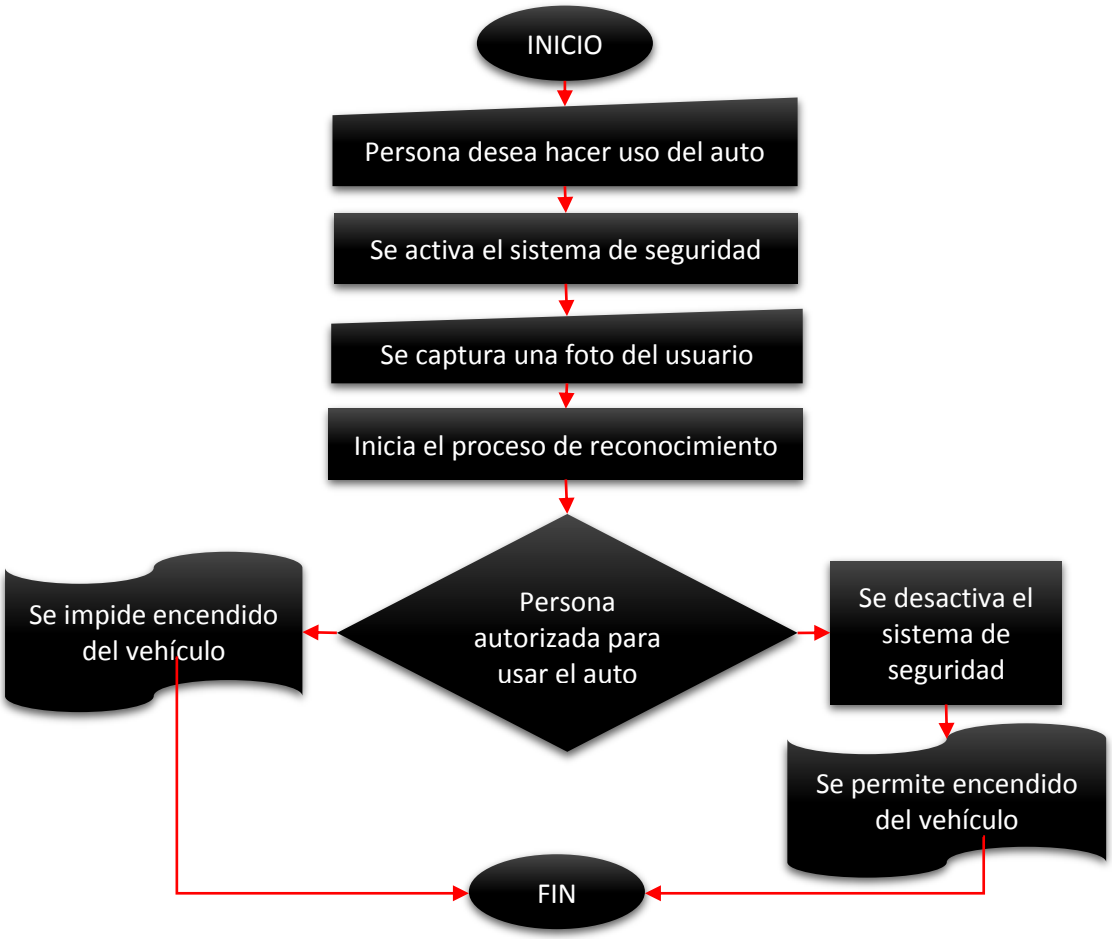


Figura 2. 16 Funcionamiento del Sistema de Seguridad Vehicular basado en Reconocimiento Facial.

Cuando una persona requiera hacer uso del auto, al tratar de encenderlo girando la llave, el vehículo no arranca debido a que el sistema de seguridad está impidiendo que el auto encienda, pues es necesario la identificación del conductor; entonces el usuario debe presionar un pulsador que inicia con el proceso de reconocimiento.

Al iniciarse la etapa de identificación, la persona frente al volante dispone de unos cuantos segundos para posicionarse dentro del recuadro rojo que se muestra en la interfaz, mientras la cámara web realiza la captura de una fotografía para iniciar con la comparación. Si el resultado del reconocimiento es positivo, es decir, que la imagen de entrada coincide con alguna de las imágenes de la base de datos, se presenta en pantalla el mensaje: “Persona autorizada, puede continuar”, y el sistema permite el paso de energía hacia el alternador para continuar con el arranque y encendido del auto; pero si el resultado es negativo y la persona no pertenece a la base de datos, se presenta el siguiente mensaje: “Error, persona no autorizada” y el usuario no puede arrancar el auto pues el sistema no lo permite.

3.5 ANÁLISIS DE REQUERIMIENTOS

3.5.1 SOFTWARE

Para llevar a cabo este proyecto es necesario de un software matemático de alto nivel que permita realizar toda la programación del algoritmo para el procesamiento digital de imágenes, por este motivo se emplea el software de Matlab 2013 como herramienta para este fin, debido a que posee el Image Processing Toolbox, una librería dedicada al tratamiento de imágenes con la ayuda de funciones y aplicaciones que permiten el análisis, visualización y desarrollo de algoritmos.

Una de las grandes ventajas del Image Processing Toolbox es la capacidad de trabajar con diversos tipos de imagen y con una resolución gigapixel, incluyendo funciones de visualización y aplicaciones que permiten explorar imágenes y vídeos, examinar una región de píxeles, ajustar el color y el contraste, crear contornos o histogramas, y manipular las regiones de interés [25].

Además se ha elegido utilizar Matlab puesto que ya se tiene conocimientos previos sobre esta herramienta informática, lo que facilita el desarrollo de la programación de los algoritmos necesarios para este proyecto.

3.5.2 HARDWARE

Para poder instalar el sistema de seguridad dentro de un vehículo, se requiere de tres dispositivos principales:

- ✓ Cámara digital con visión nocturna
- ✓ Microcomputadora
- ✓ Pantalla táctil

La microcomputadora, es la parte central del sistema pues aquí se debe cargar la aplicación para ejecutar el reconocimiento facial y es a donde se debe conectar los otros dispositivos como la cámara y la pantalla.

3.5.3 UDOO

Una excelente alternativa para el desarrollo de este proyecto, pues permite implementar proyectos que contengan hardware y software, es la placa UDOO, una minicomputadora que ofrece toda la potencia de Arduino y Raspberry Pi en un solo PCB, como se indica en la figura 2.17. La placa UDOO es un hardware libre, con plataforma de bajo coste y fácil de usar permitiendo el desarrollo de proyectos con conocimientos mínimos de hardware.

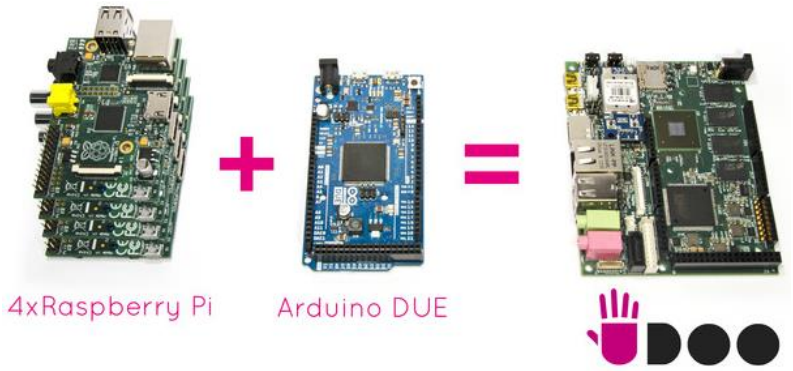


Figura 2. 17 Placa UDOO, combinación de Arduino y Raspberry Pi [29]

La elección de esta placa se basa fundamentalmente en que es compatible con todos los skeches, tutoriales y recursos disponibles en la comunidad Arduino, así

como todos los shields, los sensores y actuadores disponibles en el mercado para Arduino DUE, por lo tanto se puede lograr la conexión de la UDOO con Matlab a través de las librerías destinadas para el efecto.

Además no hay que preocuparse de buscar una cámara digital y una pantalla táctil que sean compatibles con este hardware, ya que UDOO posee módulos propios para conectar estos dispositivos directamente a la placa sin realizar ningún tipo de configuración como se aprecia en la figura 2.18 [29].

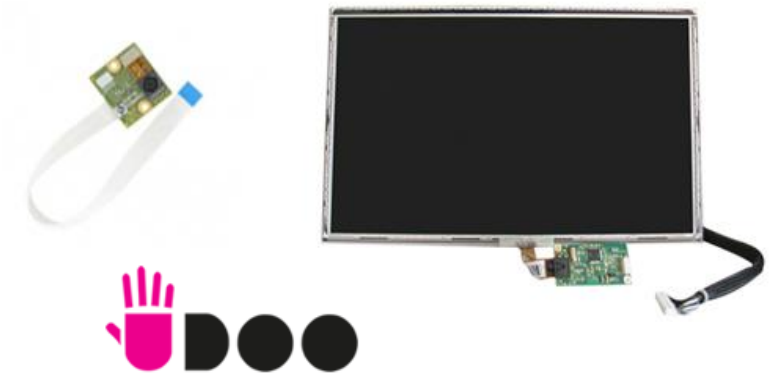


Figura 2. 18 Módulos de la Cámara y Pantalla Táctil para UDOO [29]

3.6 DISEÑO DEL SISTEMA (SOFTWARE)

3.6.1 BASE DE DATOS

Para realizar el reconocimiento facial, se ha creado dos bases de datos con las fotografías de las personas autorizadas para hacer uso del vehículo, una base de datos corresponde a las imágenes capturadas durante el día y la otra almacena las imágenes obtenidas durante la noche.

Considerando que el sistema está desarrollado para ser usado por los integrantes de una familia tipo (padre, madre y dos hijos), se han obtenido 10 fotografías por cada persona (4 individuos autorizados a usar el auto) en diferentes entornos para captar las distintas intensidades de luminosidad (ambiente no controlado), dando un total de 80 fotografías que conforman las bases de datos con las que se va a trabajar.

Todas las fotografías capturadas presentan el rostro de manera frontal, ocupando el centro de la imagen (desde el inicio de la frente hasta el final de la quijada) y tienen un tamaño de 291x400 pixeles. Al momento de evaluar el sistema desarrollado resalta la influencia del tipo de imagen que se utiliza, siendo los resultados más valederos cuando las imágenes cumplen con ciertas exigencias en cuanto a posición del individuo dentro de la fotografía, rotación, cantidad de luz, brillo y contraste. En la figura 2.19 se presentan imágenes pertenecientes a la base de datos, en las que se pueden identificar la manera correcta en que la imagen de entrada debe ser capturada.

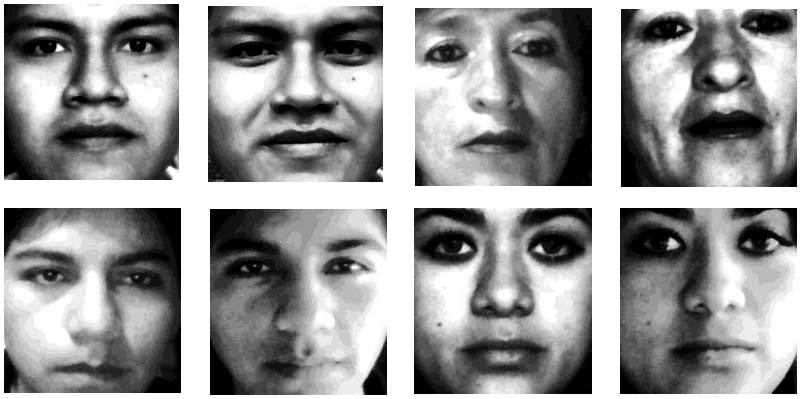


Figura 2. 19 Ejemplo de Imágenes de la base de datos

El sistema de reconocimiento facial trabaja con imágenes estáticas (fotografías) que originalmente son capturadas a color pero para su posterior análisis son convertidas a escala de grises, dichas imágenes son capturadas mediante una cámara web, pero al trabajar en un ambiente no controlado, es necesario realizar un pre procesado de las imágenes tanto a las de entrenamiento (base de datos) como a la imagen de entrada, para ajustar sus características y hacerlas lo más similares posible en lo que respecta a tamaño y luminosidad, esto debido a que la técnica empleada (PCA) para realizar el reconocimiento facial, se ve afectada por estas variables.

Cabe recalcar que el usuario debe permanecer unos cuantos segundos estático con el rostro de frente a la cámara mientras se realiza el proceso de captura, de esta manera se evita la mala orientación y expresiones erróneas en las fotografías.

3.6.2 CUADRO COMPARATIVO DE LAS PRINCIPALES TÉCNICAS PARA RECONOCIMIENTO FACIAL

Para determinar la técnica que mejor se ajusta a las necesidades de este proyecto, ha sido necesario realizar una comparación de las características principales de cada una así como de los problemas que presenta cada técnica. Toda esta información se encuentra resumida en la tabla 2.5.

Tabla 2. 5 Técnicas de reconocimiento facial

TÉCNICA	CARACTERÍSTICAS	INCONVENIENTES
PCA	• Se emplea en bases de datos pequeñas • Algoritmo sencillo • Fácil Implementación • Bajo coste computacional • Permite desarrollar sistemas en tiempo real • Realiza una reducción dimensional de los datos • Es la base de todas las técnicas de reconocimiento facial	• Al trabajar en un entorno no controlado no se tiene una misma intensidad luminosa en las imágenes lo que dificulta el reconocimiento.
LDA	• Realiza una máxima discriminación entre clases • Minimiza la varianza de cada clase • Maximiza la varianza entre clases	• Es un método supervisado, requiere entrenar el sistema con patrones etiquetados • Requiere matrices no-singulares para trabajar
LPP	• Posee un algoritmo lineal similar al que posee PCA • Rápido y útil para aplicaciones prácticas, pues reduce la dimensión de los datos	• Es un método supervisado, requiere entrenar el sistema con patrones etiquetados • Presenta dificultad al recuperar los datos originales ya que no trabaja con vectores ortogonales • Otro problema es el trabajar con datos de entrada de mayor dimensión que el número de muestras.
EBGM	• No utiliza la imagen total de la cara, solo puntos de interés. • La iluminación, expresión y postura no afectan el reconocimiento	• Requiere el uso de wavelets, generando un algoritmo complejo. • Presenta dificultad en la ubicación de los puntos de referencia
AAM	• Forma una malla con los puntos característicos del rostro. • Usa toda la información de la cara, no solo los puntos de los bordes, sino también los interiores.	• Hace uso de PCA para la extracción de características.

Después de haber realizado una intensa investigación bibliográfica respecto al reconocimiento facial y a las técnicas empleadas para su desarrollo, se ha determinado que la mejor alternativa para realizarlo es mediante el uso del algoritmo de eigenfaces con el cual trabaja la técnica de reconocimiento facial ACP (Análisis de Componentes Principales), pues en gran parte de la bibliografía consultada se menciona que este método es más versátil en cuanto a complejidad, rapidez de ejecución y resultados.

Como ya se ha analizado en apartados anteriores, esta técnica no trabaja con imágenes grandes en dimensión lo que reduce el coste computacional que implica ejecutar su algoritmo, facilitando la implementación de sistemas en tiempo real, además; el sistema de seguridad propuesto es de carácter doméstico, por lo que la base de datos no es muy extensa, como sucedería en el caso de implementar el sistema de seguridad en grandes empresas, estadios o aeropuertos, donde existe una mayor afluencia de personas, por tanto el método elegido se ajusta perfectamente a las necesidades del proyecto.

Sin importar la técnica que se use para el reconocimiento de rostros, es importante realizar un mejoramiento de la imagen preparándola para un procesamiento posterior.

Todo sistema de reconocimiento debe desarrollar las cuatro etapas que lo componen como se muestra en la figura 2.20.

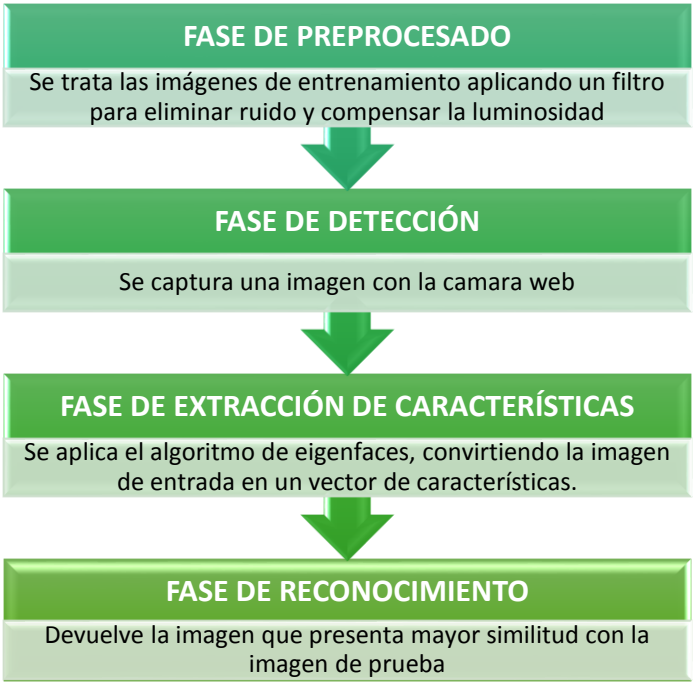


Figura 2. 20 Pasos para realizar un reconocimiento facial [18]

3.6.3 FASE DE PREPROCESADO DE LAS IMÁGENES

Para el preprocesado de las imágenes se ha realizado otro script de Matlab para que este algoritmo no interfiera con la programación del reconocimiento en cuanto a velocidad de ejecución y para poder visualizar la imagen resultante también se ha creado un nuevo GUI, tal como se aprecia en la figura 2.21.

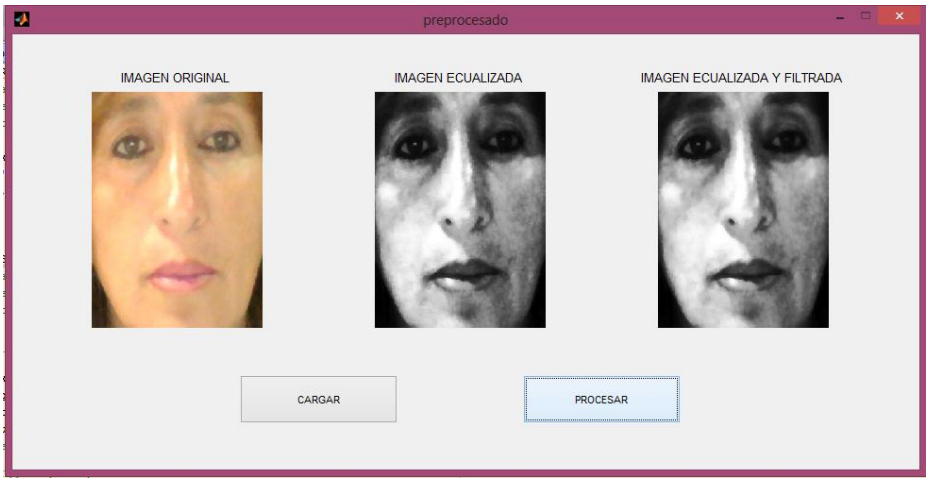


Figura 2. 21 GUI para el preprocesado de las imágenes

Todas las imágenes de entrenamiento igualmente fueron capturadas con la cámara web y almacenadas.

En esta fase se busca compensar todo aquello que puede provocar que dos imágenes de una misma persona no sean iguales, corrigiendo la luminosidad, ajustando el tamaño de las imágenes y aplicando un filtro para eliminar el ruido presente en las fotografías.

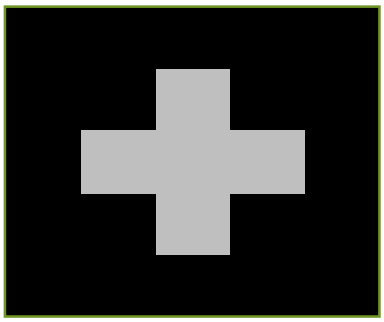
- **AJUSTE DE TAMAÑO**

Se normaliza el tamaño de las imágenes de entrenamiento a 291x400 píxeles, valores que se han elegido de manera arbitraria. Este proceso se realiza debido a que las imágenes que se han agregado a la base de datos fueron capturadas mediante la cámara web y originalmente tenían un tamaño de 480x640 píxeles, reduciendo así el costo computacional que implica el trabajar con matrices de gran tamaño. Para realizar este proceso se hace uso de las funciones de Matlab ***imcrop*** e ***imresize***.

- **ECUALIZACIÓN DEL HISTOGRAMA**

De manera general, una imagen digital se la puede conceptualizar como un conjunto de píxeles con diferentes niveles o valores de intensidad luminosa (escala de grises) o brillo asociado, formando un arreglo bidimensional de píxeles con diferente intensidad [18].

Cada elemento de esta matriz corresponde a un píxel de la imagen, como se puede apreciar en la figura 2.22:



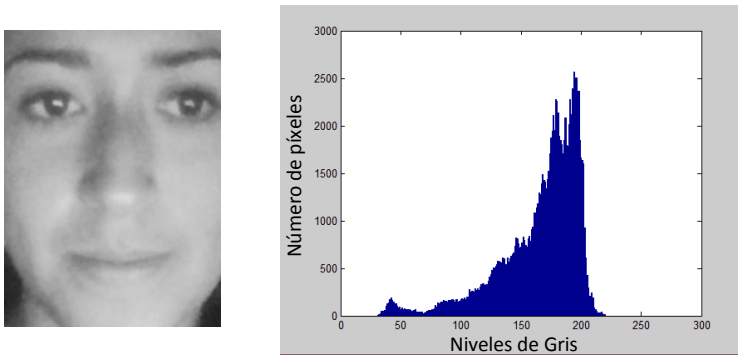
40	40	40	40	40
40	40	200	40	40
40	200	200	200	40
40	40	200	40	40
40	40	40	40	40

Figura 2. 22 a) Imagen original; b) Estructura matricial de la imagen [18]

Por consiguiente, el histograma de la imagen consiste en una gráfica donde se muestra todos los niveles de gris presentes en esa imagen r_k dentro del rango de 0 a 255 (256 tonos de gris) y la cantidad de pixeles con un determinado valor de gris n_k [30].

El ecualizado de una imagen se realiza con el objetivo de modificar su histograma mediante transformaciones de tal manera que la nueva imagen presente un histograma con una distribución uniforme, es decir, que exista el mismo número de pixeles para cada nivel de gris [31]

En la figura 2.23 que se presenta a continuación se puede observar una imagen en escala de grises y su correspondiente histograma.



a) b)

Figura 2. 23 a) Imagen a escala de grises b) histograma de la imagen

En el tratamiento de imágenes, el histograma se emplea para comparar contrastes e intensidades y permite producir cambios en una imagen tras realizar algunos procesos para alterar su histograma, uno de estos métodos es mediante la ecualización del histograma, logrando el realce y mejora de la imagen [14].

Al variar el histograma, se modifica la distribución de probabilidad hasta encontrar un determinado nivel de gris en la imagen alcanzando una función de densidad deseada que en realidad corresponde al histograma normalizado [12].

Para lograr realizar el ecualizado de la imagen se aplica la ecuación 1.

$$s_k = T(r_k) = (L-1)\sum_{j=0}^{k} p_r(r_j) = \frac{L-1}{MxN}\sum_{j=0}^{k} n_j \qquad (1)$$

Si:

$$p_r(r_j) = \frac{n_j}{MxN} \qquad (2)$$

Donde:

$L = niveles\ de\ gris\ de\ la\ imagen$

$M = ancho\ de\ la\ imagen\ en\ pixeles$

$N = alto\ de\ la\ imagen\ en\ pixeles$

$p_r = Densidad\ de\ Probabilidad$

De esta manera se logra conseguir una dispersión del histograma en un rango mayor dentro del intervalo [0, L-1].

Entonces, si se tiene una imagen cuya dimensión es de 4096 pixeles, es decir, de 64 x 64 pixeles con 8 niveles de gris, distribuidos como se indica en la tabla 2.6

Tabla 2. 6 Distribución de pixeles de una imagen a escala de grises con 8 niveles de gris

r_k $(niveles\ de\ gris)$	n_k $(\#\ pixeles\ en\ el\ nivel\ de\ gris)$	$p_r(r_k) = n_k/MxN$
$r_0 = 0$	*790*	*0,19*
$r_1 = 1$	*1023*	*0,25*
$r_2 = 2$	*850*	*0,21*
$r_3 = 3$	*656*	*0,16*
$r_4 = 4$	*329*	*0,08*
$r_5 = 5$	*245*	*0,06*
$r_6 = 6$	*122*	*0,03*
$r_7 = 7$	*81*	*0,02*

Usando la ecuación 1, se logra obtener la función de transformación para ecualizar el histograma, obteniendo los siguientes resultados:

$$s_0 = T(r_0) = (8-1)\sum_{j=0}^{0} p_r(r_j) = 1{,}33$$

$$s_1 = T(r_1) = (8-1)\sum_{j=0}^{1} p_r(r_1) = 0{,}19 + 0{,}25 = 3{,}08$$

$$s_2 = T(r_2) = (8-1)\sum_{j=0}^{2} p_r(r_2) = 0{,}19 + 0{,}25 + 0{,}21 = 4{,}55$$

$$s_3 = T(r_3) = 5{,}67$$

$$s_4 = T(r_4) = 6{,}23$$

$$s_5 = T(r_5) = 6{,}65$$

$$s_6 = T(r_6) = 6{,}86$$

$$s_7 = T(r_7) = 7$$

Todos los resultados se deben aproximar a su valor válido más cercano, por lo tanto se tiene:

$$s_0 = T(r_0) = 1$$

$$s_1 = T(r_1) = 3$$

$$s_2 = T(r_2) = 5$$

$$s_3 = T(r_3) = 6$$

$$s_4 = T(r_4) = 6$$

$$s_5 = T(r_5) = 7$$

$$s_6 = T(r_6) = 7$$

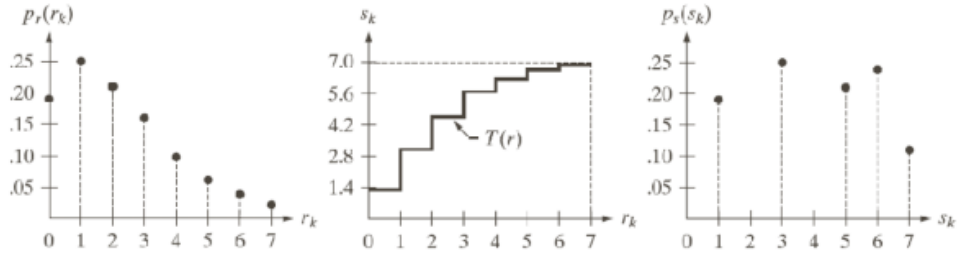
$$s_7 = T(r_7) = 7$$

En base a estos resultados se obtienen un nuevo histograma, en base a los datos mostrados en la tabla 2.7:

Tabla 2. 7 Número de pixeles de cada nivel de gris del histograma ecualizado

histograma ecualizado (niveles de gris)	*# pixeles en el nivel de gris*
$s_0 = 1$	*790*
$s_1 = 3$	*1023*
$s_2 = 5$	*850*
$s_3 = 6$	*656*
$s_4 = 6$	*329*
$s_5 = 7$	*245*
$s_6 = 7$	*122*
$s_7 = 7$	*81*

De la tabla anterior se puede deducir que, como $r_0 = 0$ ahora se ha transformado en $s_0 = 1$, hay 790 pixeles en este nuevo valor, para el nivel de gris 3, ahora se tienen 1023 puntos, así como existen 850 puntos en el nivel 5, sin embargo el nivel seis presenta 985 pixeles (656+329) y finalmente para en el nivel 7 se ubican 448 puntos (245+122+81), de esta forma el histograma queda redistribuido [31] como se indica en la figura 2.24.



a) b) c)

Figura 2. 24 a)Histograma Original b)Función de Transformación c)Histograma Ecualizado [31]

Para cumplir con este paso se ha utilizado la función ***histeq*** de Matlab.

El resultado de aplicar esta función en Matlab se puede apreciar en la figura 2.25.

a) b)

Figura 2. 25 Ecualización de las imágenes.
a) imagen original en escala de grises b) imagen ecualizada

- **FILTRO PARA ELIMINAR EL RUIDO**

Mediante el uso de filtros digitales se puede mejorar la presentación visual de una imagen, eliminando el ruido presente, o dejando pasar un solo tipo de frecuencias (altas o bajas) dependiendo del objetivo que se desea alcanzar.

Una imagen puede ser filtrada en el dominio de la frecuencia como también dentro del dominio espacial.

Cuando a una imagen se aplica filtros en el dominio de la frecuencia, se permite el paso de un rango determinado de frecuencias, para esto se modifica la transformada de Fourier mediante operaciones matemáticas.

Al trabajar en el dominio espacial, los filtros realizan operaciones directamente sobre los pixeles, modificando su valor de acuerdo al valor de los pixeles que lo rodean [18]. Dentro del dominio espacial los filtros pueden ser lineales en donde se realiza una convolución entre la imagen y una matriz que sirve como máscara y que recorre la imagen para aplicar el filtro a todos los pixeles, y los filtros no lineales utilizan la función de transformaciones de escala de gris $y=t(x)$ para pasar de un nivel de gris x a otro nivel de gris y que para esto se aplica el proceso matemático de la convolución [32].

FILTRO DE MEDIANA

Se ha elegido este tipo de filtro debido a que es excelente atenuando el ruido impulsional (sal y pimienta) presente en las imágenes, pues este tipo de ruido se presenta mucho en las fotografías capturadas en ambientes con poca iluminación como las que han sido capturadas durante la noche.

El filtro de mediana es un filtro no lineal, es decir que si se tienen dos imágenes A y B, sucede que:

mediana (A+B) ≠ mediana de (A) + mediana (B) [33]

Este filtro selecciona el valor del pixel que se encuentra en el centro una vez que la matriz correspondiente a la imagen ha sido ordenada de mayor a menor valor, entonces se toma el valor en escala de grises del pixel central, el nivel de gris de cada píxel se reemplaza por la mediana de los niveles de gris en un entorno de este píxel.

Así, después de haber ordenado la matriz, la mediana M de un conjunto de valores es tal que la mitad de los valores del conjunto son menores que M y la mitad de los valores mayores que M, tal como se aprecia en la figura 2.26 [18].

$$\begin{array}{|c|c|c|} \hline 3 & 5 & 2 \\ \hline 6 & 4 & 9 \\ \hline 1 & 8 & 7 \\ \hline \end{array} \Longrightarrow \begin{array}{|c|c|c|} \hline 1 & 2 & 3 \\ \hline 4 & \mathbf{5} & 6 \\ \hline 7 & 8 & 9 \\ \hline \end{array}$$

Figura 2. 26 Ejemplo de extracción de la mediana [18]

Así se consigue eliminar el ruido de sal y pimienta presente en las imágenes ya que estos pixeles de desplazan a los extremos y no interfiere con la información central de la imagen que es la que se necesita analizar. El inconveniente de este tipo de filtro es que la imagen se torna un poco borrosa, como ocurre con cualquier filtro pasa bajo como el de mediana o filtros no lineales como el gaussiano, pero conserva de mejor manera los bordes [12].

El comando en Matlab para aplicar el filtro de mediana es ***medfilt.***

En la figura 2.27 se puede visualizar el resultado de aplicar el filtro de mediana a una imagen que contenía ruido de “sal y pimienta”.

a) b)

Figura 2. 27 Filtrado de las imágenes.
a) imagen original con ruido b) imagen filtrada con filtro de mediana

3.6.4 FASE DE DETECCIÓN DE LAS IMÁGENES

Como ya se ha mencionado todas las imágenes, tanto las de entrenamiento (base de datos) y las imágenes de entrada han sido capturadas mediante la cámara web propia del computador; pero en caso de que se requiera utilizar una cámara externa de igual manera se lo puede realizar gracias a la librería de adquisición de imágenes que Matlab posee, así se puede utilizar cualquier dispositivo de video conectado al computador.

Esta librería posee un enfoque orientado a objetos, por este motivo primero se debe crear el objeto que permita la conexión entre MATLAB y el dispositivo de adquisición de video. Después es necesario identificar las propiedades de ese objeto, es decir del dispositivo de video, para poder controlar características importantes como: la cantidad de cuadros que se quieren almacenar y cada cuánto almacenarlos.

La programación para la adquisición de imágenes/ video en Matlab es realmente muy sencilla, basta realizar los pasos que se mencionan a continuación:

1. **Conectar e instalar la cámara:**

En caso de utilizar una cámara externa, primero se debe conectar al computador e instalar todos sus drivers y realizar una prueba con cualquier aplicación para asegurarse que la cámara funcione correctamente.

2. **Obtener información acerca del hardware**

En Matlab se debe ejecutar el comando ***imaqhwinfo*** que permite conocer los adaptadores que posee nuestro equipo (software que establece la comunicación entre el dispositivo de video y Matlab), los dispositivos de video conectados al adaptador y todos los formatos que manejan estos dispositivos.

Tras ejecutar este comando, en este caso se presentan los adaptadores: ***'gentl' 'gige' 'matrox' 'winvideo'***, que vienen cargados ya en el sistema operativo.

Los adaptadores asignan un número a cada dispositivo conectado a él, así se puede conocer a que adaptador se ha conectado la cámara, para esto es necesario ejecutar nuevamente el comando ***imaqhwinfo*** seguido del nombre del adaptador del cual se requiera obtener información [26], en este caso el adaptador a consultar es ***'winvideo'***.

Después de ejecutar estas instrucciones se observa que este adaptador tiene conectado un dispositivo al cual se le ha asignado un número para identificarlo (deviceID), tal como se muestra en la figura 2.28.

```
>> imaqhwinfo

ans =

    InstalledAdaptors: {'gentl'  'gige'  'matrox'  'winvideo'}
        MATLABVersion: '8.1 (R2013a)'
          ToolboxName: 'Image Acquisition Toolbox'
       ToolboxVersion: '4.5 (R2013a)'

>> imaqhwinfo('winvideo')

ans =

       AdaptorDllName: [1x81 char]
    AdaptorDllVersion: '4.5 (R2013a)'
          AdaptorName: 'winvideo'
            DeviceIDs: {[1]}
           DeviceInfo: [1x1 struct]
```

Dispositivo conectado
ID : [1]

Figura 2. 28 Información de Hardware (adaptadores y dispositivos conectados)

Si se realiza el paso anterior en cualquiera de los otros adaptadores como por ejemplo para el adaptador ***'matrox'*** se despliega la siguiente información como se aprecia en la figura 2.29:

```
>> imaqhwinfo('matrox')

ans =

       AdaptorDllName: [1x79 char]
    AdaptorDllVersion: '4.5 (R2013a)'
          AdaptorName: 'matrox'
            DeviceIDs: {1x0 cell}
           DeviceInfo: [1x0 struct]
```

No hay dispositivos conectados

Figura 2. 29 Información del adaptador 'matrox'

Como se indica en la figura, no existe ningún identificador de dispositivo (*deviceID*) eso quiere decir que ningún dispositivo está conectado a ese adaptador, de esta manera se puede elegir correctamente el adaptador con el que se va a trabajar.

Posteriormente se debe identificar los formatos soportados por el dispositivo de video, para esto se escribe ***imaqhwinfo('winvideo',1),*** (el número 1 corresponde al *deviceID),* tras realizar esta acción, se establece que la cámara empleada para este proyecto solo soporta el formato ***'MJPG_1280x720'.***

3. Crear el objeto de video

Para crear el objeto que nos permita trabajar en Matlab y realizar la adquisión se emplea el comando ***videoinput.***

4. Vista previa y Configuración de las propiedades del dispositivo

La visualización de la imagen de entrada se lo realiza mediante el comando ***preview,*** este comando despliega una ventana donde se puede tener una vista previa de la imagen que se desea capturar.

Gracias al objeto de video creado, se puede manipular ciertas características y ajustarlas según sean las necesidades del usuario; se puede modificar parámetros de brillo, nitidez, contraste, es decir, ajustar la calidad de la imagen.

Otra característica que se puede alterar es la del *trigger*, que puede configurarse para iniciar la captura de manera instantánea, con un retardo, realizar capturas a intervalos, o configurarlo para que el *trigger* se realice de forma manual, automática o mediante un impulso externo [34].

5. Adquisición de la Imagen

La función empleada para capturar una fotografía es ***getsnapshot;*** al ejecutar este comando, la cámara captura un *frame* y lo almacena en una variable, y con el comando ***imwrite*** se puede almacenar la fotografía en el disco duro [34].

A continuación se presenta la sección de código programado para realizar la fase de captura de la imagen.

3.6.5 FASE DE EXTRACCIÓN DE CARACTERÍSTICAS

Cada una de las imágenes de entrenamiento previamente almacenadas en la base de datos, puede matemáticamente ser representada como una matriz formada por los valores de los pixeles que la conforman (en el rango de escala de grises 0-256), por lo tanto ésta matriz tiene dimensiones NxN pixeles. Dentro de la base de datos, las imágenes almacenadas tienen una dimensión de

291x400 pixeles, por lo que se las ah redimensionado a un tamaño de 64x64 pixeles para trabajar con matrices más reducidas.

Cada una de estas matrices que representan a las imágenes de la base de datos, se las transforma a un vector columna cuya dimensión será N^2 pixeles (4096 valores) conocido como "espacio original de la imagen". La agrupación de estos vectores forma una sola matriz con una dimensión de N^2xm (327680 pixeles), siendo m el número de personas dentro de la base de datos. Esta matriz da origen a un espacio vectorial gigantesco dentro del cual se un encuentra un subespacio de menor dimensión (facespace), formado únicamente por imágenes de caras. ACP busca representar este conjunto de caras mediante vectores que las identifiquen dentro del espacio general de imágenes. Para esto primero es necesario calcular la imagen promedio de entre todas las imágenes de entrenamiento usando la ecuación 3.

$$\mu = \frac{1}{m}\sum_{i=1}^{m} x_i \tag{3}$$

Y se obtiene la diferencia entre cada vector y la media usando la ecuación 4:

$$\emptyset_i = x_i - \mu \tag{4}$$

Este paso se realiza para eliminar la información que no es útil para el reconocimiento, así se obtiene la matriz A:

$$A = [\emptyset_1, \emptyset_2, \ldots \ \emptyset_m]$$

Empleando esta nueva matriz se puede calcular la matriz de covarianza mediante la ecuación 5, esta matriz tiene una dimensión de $N^2 \, x \, N^2$

$$S = \frac{1}{m}\sum_{i=1}^{m}(\ \emptyset_i \ . \emptyset_i^T) = A \, . \, A^T \tag{5}$$

Aplicando ACP se busca un conjunto de x vectores ortonormales u_k que describen la distribución de los datos, estos vectores u_k son los eigenvectores y los valores encontrados mediante la ecuación 6,

$$\lambda_k = \frac{1}{m}\sum_{i=1}^{m}(u_k^T \ . \ \emptyset_i) \quad (6)$$

corresponden a los eigenvalores de la matriz de covarianza.

El cálculo computacional que esto implica es muy elevado, por eso si $m<N$ sólo habrá $m-1$ eigenvectores, facilitando así los cálculos y pudiendo resolver el problema utilizando combinaciones lineales de las imágenes.

Se calcula la matriz $L = A.A^T$ de dimensión mxm y se buscan los m eigenvectores v_l. Estos vectores determinan la combinación lineal de las m imágenes del conjunto de entrenamiento usando la ecuación 7:

$$u_k = \sum_{i=1}^{m} v_{Ii} \ . \ \emptyset_i \quad (7)$$

Una vez calculados los eigenvectores de la matriz de covarianza se seleccionan aquellos con autovalores más altos pues contienen mayor información de las imágenes. La elección del número de autovectores con los que se va a trabajar es muy importante, pues un número elevado supone un mayor tiempo de procesamiento y memoria para la etapa de clasificación, por otro lado un número bajo de autovectores puede no proporcionar la información necesaria para el reconocimiento [18]. Según pruebas realizadas se ha determinado 50 eigenvectores son suficientes para trabajar en la etapa de clasificación.

La reducción dimensional realizada por PCA es equivalente al número de autovectores o eigenvectores que se utilicen. Por lo tanto la imagen proyectada por PCA tendrá una dimensión de valor *d*, como se puede ver en la figura 2.30.

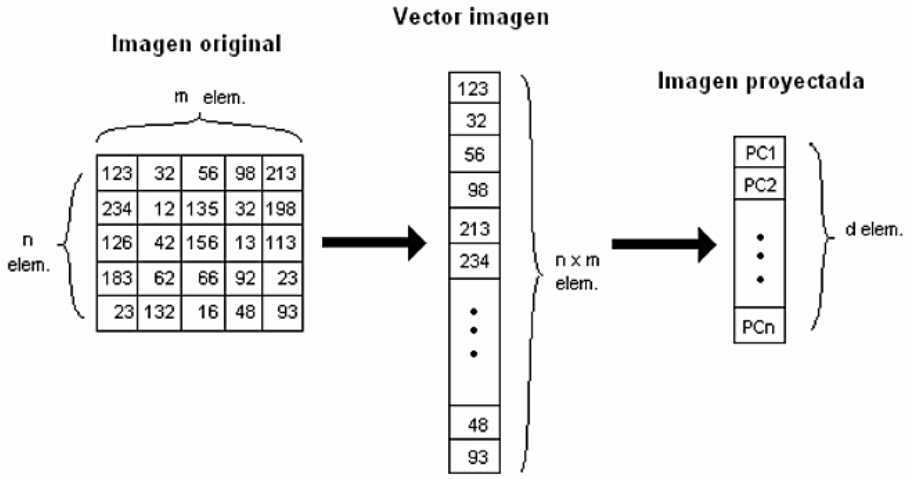


Figura 2. 30 Ejemplo de reducción dimensional al aplicar APC [21]

Los autovectores representan las componentes principales que son más comunes en imágenes de diferentes caras. La matriz de transformación, está formada por los autovectores correspondientes a los *d* autovalores más significativos [21].

3.6.6 FASE DE RECONOCIMIENTO

Después de haber obtenido el conjunto de características que mejor representen una cara humana, se lleva estas características a la etapa final del programa que es el clasificador para efectuar el reconocimiento propiamente dicho.

Las comparaciones en el clasificador se hacen mediante una medida de distancia para determinar qué tan cerca o lejos se encuentran un conjunto de características de otras, en este caso se ha hecho uso de la distancia Euclidiana.

DISTANCIA EUCLÍDEA

Las medidas realizadas en base a la distancia euclídea son aplicadas cuando los problemas a resolver no son tan complicados, por ello la distancia euclídea se considera como la distancia clásica, básica, general y la más implementada.

Se define a la distancia euclídea como el producto escalar de la diferencia de dos vectores de posición (referidos al mismo origen de coordenadas), expresado en términos más sencillos, corresponde a determinar la longitud del vector entre dos puntos tomando como centro de coordenadas un mismo punto [13].

Matemáticamente, la distancia euclídea, está definida como:

Para un espacio bidimensional, definido entre los puntos *P1* y *P2*, de coordenadas *(x1,y1) y (x2,y2)* respectivamente, tal como se indica en la figura 2.31 .

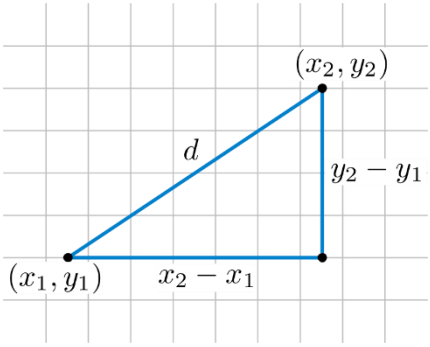


Figura 2. 31 Distancia Euclídea en un sistema bidimensional [13]

se tiene la ecuación 8 :

$$d_e(P1, P2) = \sqrt{(x2 - x1)^2 + (y2 - y1)^2} \tag{8}$$

Para un espacio euclídeo n-dimensional, la distancia entre los puntos *P=(p1,p2,...pn)* y *Q=(q1,q2,...qn)* se determina mediante la ecuación 9.

$$d_e(P, Q) = \sqrt{(p1 - q1)^2 + (p2 - q2)^2 + \cdots + (pn - qn)^2} \tag{9}$$

Generalizando, se obtiene la ecuación 10.

$$d_e(P, Q) = \sqrt{\sum_{i=1}^{n} (pi - qi)^2} \tag{10}$$

Siendo *pi* y *qi* las columnas *i-ésimas* de las matrices de características de la imagen de entrada y de la base de datos respectivamente, y *n* la anchura de la imagen.

Finalmente, para determinar la imagen correspondiente a la imagen de entrada, se determina la menor distancia euclidiana y en base a esta la imagen con mayor similitud, para lo cual se ha establecido un rango de aceptación.

En la figura 2.32 se muestra las imágenes proyectadas en el espacio vectorial y el cálculo de la distancia euclidiana desde la imagen de prueba a cada una de las imágenes de entrada.

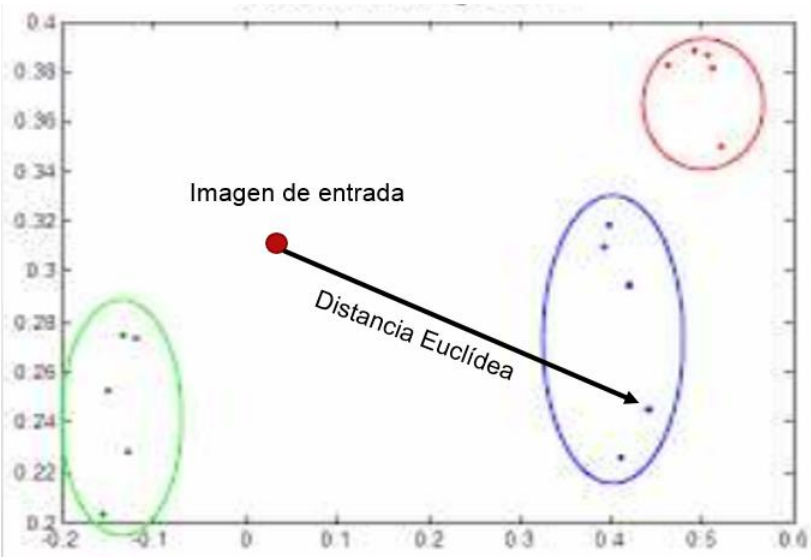
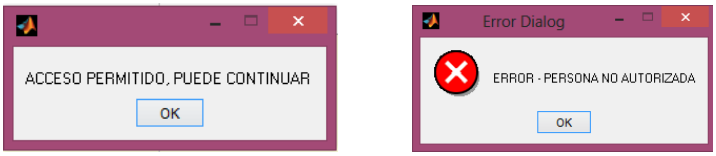


Figura 2. 32 Proyección de las imágenes en el espacio vectorial y cálculo de la Distancia Euclídea [20]

En la interfaz de usuario se presenta la imagen del sujeto reconocido por el sistema como la imagen de la persona sometida a la prueba, como se observa en la figura 2.33.

Figura 2. 33 Ejemplo de captura de una imagen y su resultado

Dependiendo del resultado, se muestra un mensaje, validando el encendido del auto o bien bloqueándolo, como se indica en la figura 2.34.



a) b)

Figura 2. 34 Cuadros de diálogo en dependencia del resultado
a) Caso positivo, se permite el uso del auto , b) caso negativo, se bloquea el uso del auto

3.7 INTERFAZ GRÁFICA DE USUARIO

Con la ayuda de Guide de Matlab, se ha creado una interfaz para ejecutar el programa de reconocimiento facial.

Se han desarrollado dos GUI, el primero corresponde a la portada en la cual se presentan algunos datos informativos como el nombre de la universidad, nombre de la facultad, título del proyecto, autor y tutor; en la parte inferior derecha se ubica un botón con el cual se da inicio a reconocimiento así como se muestra en la figura 2.35.

Figura 2. 35 GUI de la portada del programa

Una vez que se ha pulsado el botón de inicio, arranca la segunda interfaz, en ella se presenta al lado izquierdo un recuadro para la imagen de entrada y en el

lado derecho un recuadro donde se visualiza el resultado, es decir, la fotografía del personaje correspondiente a la imagen de entrada, en la parte inferior izquierda se tiene un menú para que el usuario pueda seleccionar la base de datos a utilizar de acuerdo al instante en el cual se va a capturar la imagen (día o noche); después de seleccionar una de las dos opciones la cámara se enciende automáticamente y la persona que se encuentra frente a esta dispone de cinco segundos para enfocarse adecuadamente dentro del rectángulo rojo, después se capturará la imagen que será procesada y comparada, todo esto se puede apreciar en la figura 2.36

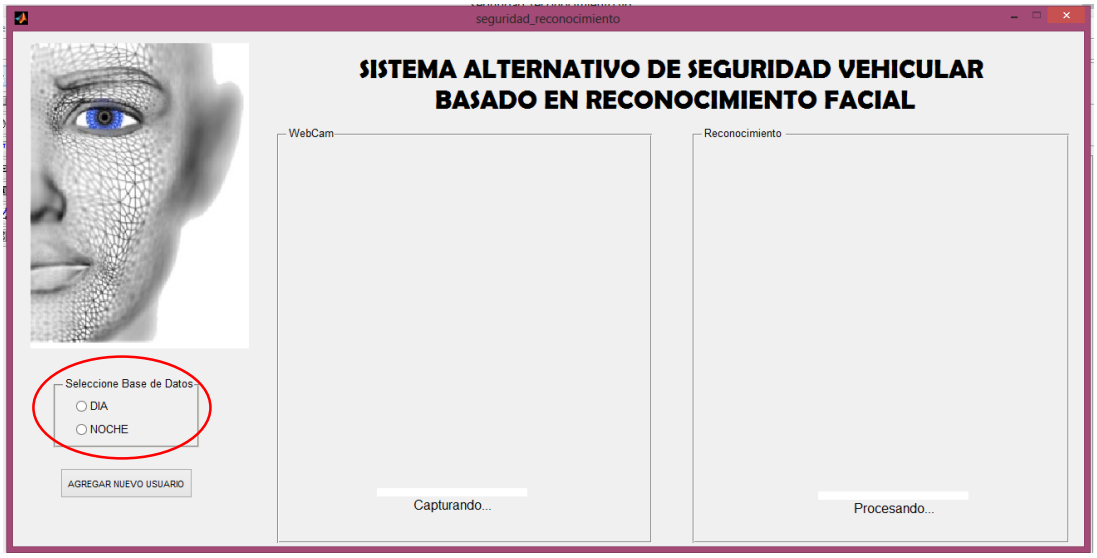


Figura 2. 36 GUI del programa de reconocimiento facial

Existe la posibilidad de agregar nuevos usuarios a las diferentes bases de datos, solo se debe presionar el botón “AGREGAR NUEVO USUARIO” como se aprecia en la figura 2.37.

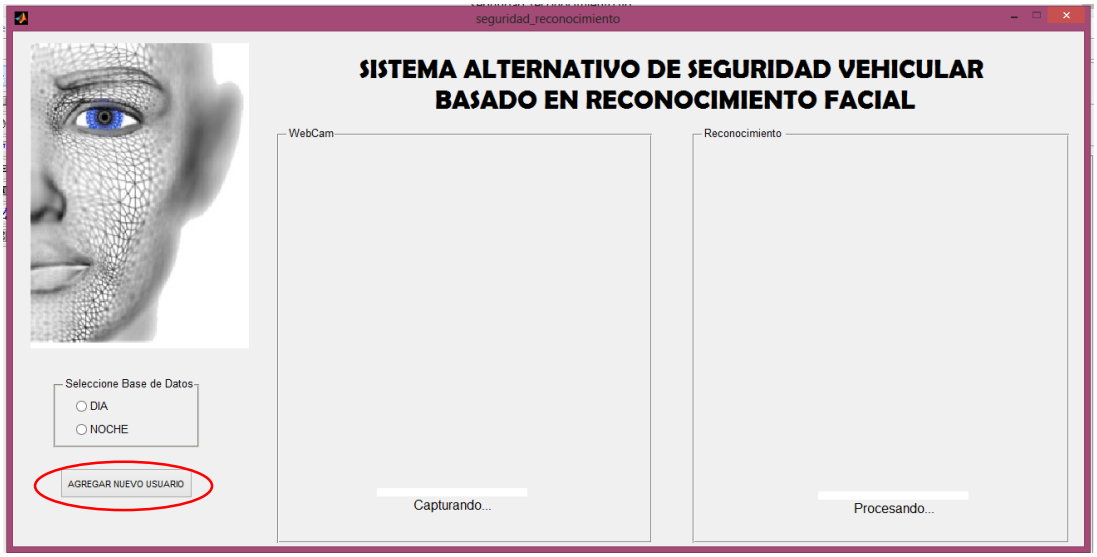


Figura 2. 37 Botón “agregar nuevo usuario”

Al presionar este botón se despliega otro GUI que permite la captura de una imagen del nuevo usuario para ser almacenada en la base de datos correspondiente, como se puede observar en la figura 2.38

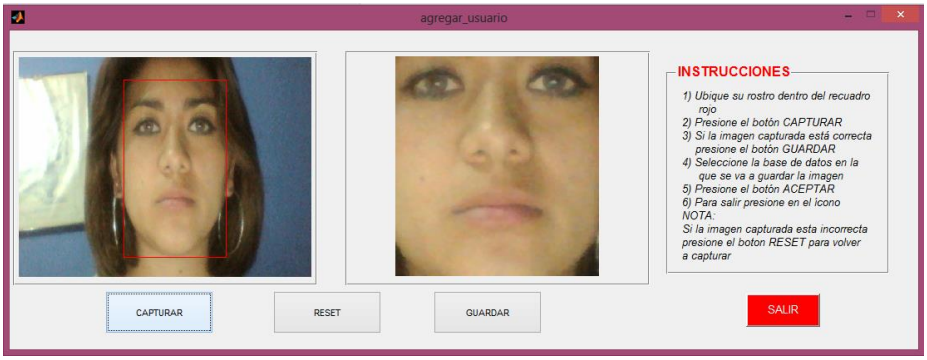


Figura 2. 38 GUI para agregar un nuevo usuario

Al pulsar el botón “GUARDAR”, se despliega una ventana que corresponde al fichero donde se encuentra el programa y las bases de datos, para almacenar la imagen del nuevo usuario se debe seleccionar la base de datos correspondiente ya sea la del día o la de noche, como se indica en la figura 2.39.

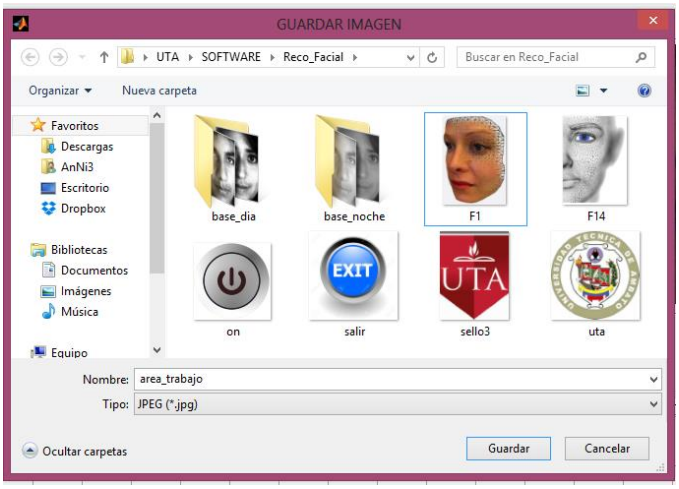


Figura 2. 39 Ventana emergente para guardar imagen del nuevo usuario

3.8 PRUEBAS DE FUNCIONAMIENTO DEL SISTEMA Y RESULTADOS

El sistema se puso a prueba para comprobar su funcionamiento, realizando varias tomas de las personas autorizadas para usar el auto.

Las pruebas se realizaron durante el transcurso de una semana en horarios distintos para cada persona, tanto para los usuarios autorizados como para las personas externas.

3.8.1 PRUEBAS REALIZADAS DURANTE EL DÍA

Las pruebas de reconocimiento facial durante el día de los usuarios autorizados se han capturado durante el transcurso de la mañana y tarde dentro del horario de 9 a.m. hasta las 6 p.m.

Para establecer los porcentajes de confiabilidad del sistema, se ha realizado 8 tomas por persona para el día, varias de capturas se muestran en las figuras 2.40 – 2.43, en las que se puede observar la imagen de entrada (fotografía izquierda) de la persona sometida a la prueba, la fotografía similar (imagen derecha) y el nombre de la persona con la cual coincide.

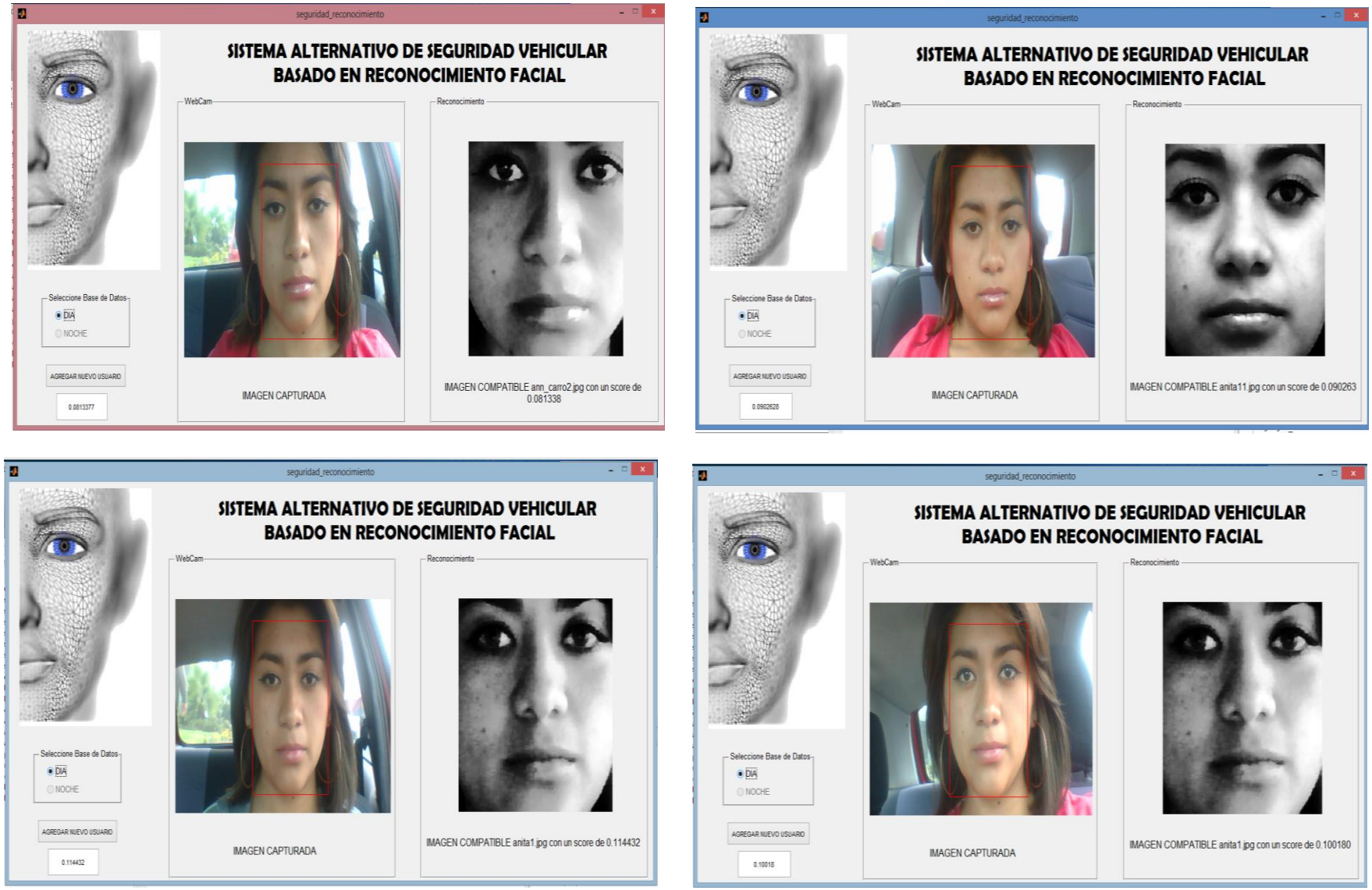


Figura 2.40 Pruebas durante el día (primera persona autorizada)

Figura 2. 41 Pruebas durante el día (segunda persona autorizada)

Figura 2. 42 Pruebas durante el día (tercera persona autorizada)

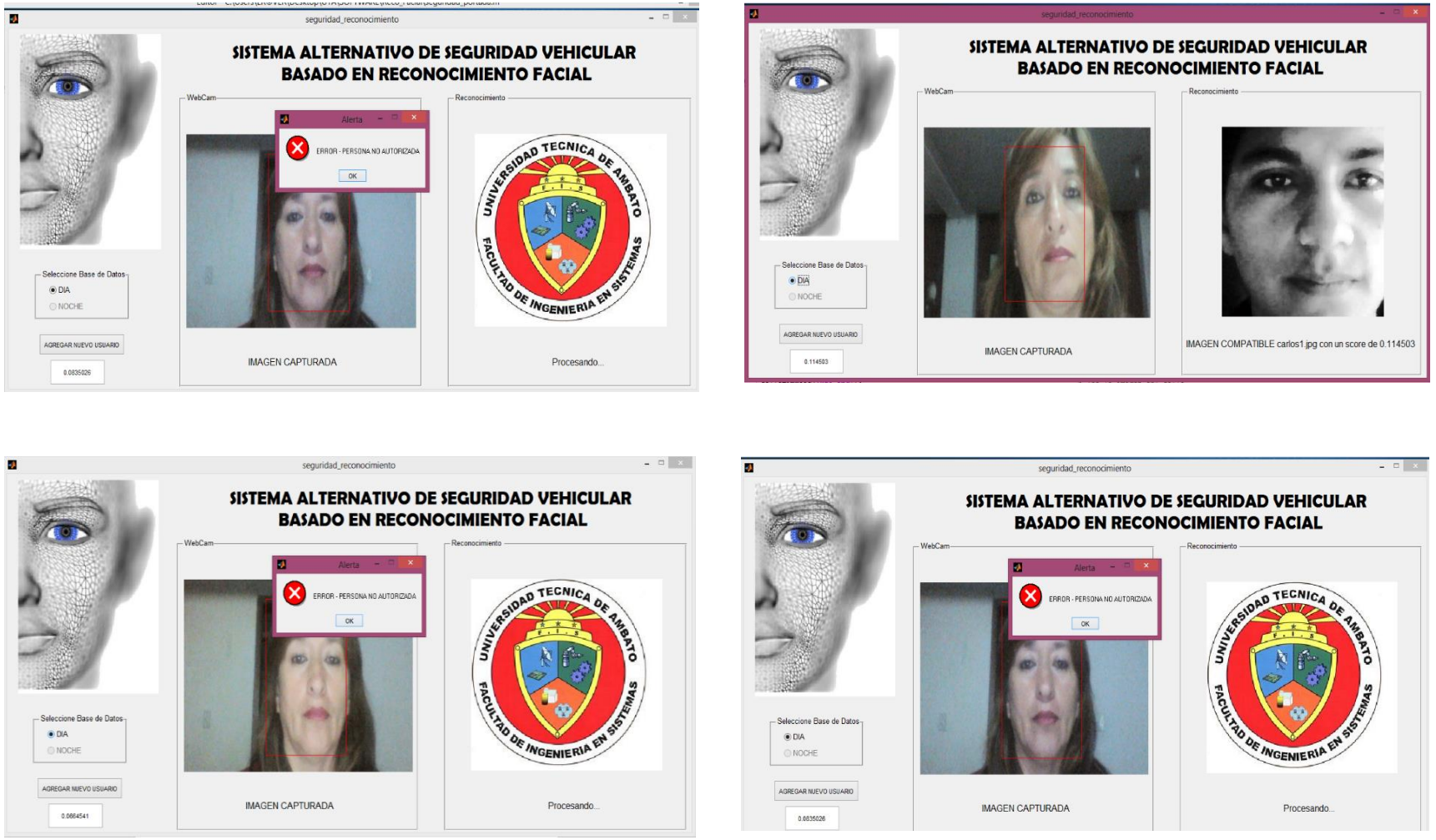


Figura 2. 43 Pruebas durante el día (cuarta persona autorizada)

3.8.2 PRUEBAS REALIZADAS DURANTE LA NOCHE

Durante una semana se han realizado las capturas de las personas autorizadas a usar el auto. Las pruebas se realizaron por la noche dentro del horario de 6 p.m hasta las 10 p.m.

Al igual que se ha realizado para el día, para comprobar el funcionamiento del sistema durante la noche se han obtenido 8 tomas por persona como se aprecia en las figuras 2.44 – 2.47.

En las imágenes presentadas se puede visualizar la imagen con la cual coincidió la imagen de entrada puesta a prueba, y en los casos de negativos donde no se encuentra una imagen similar, se presentan los mensajes de error.

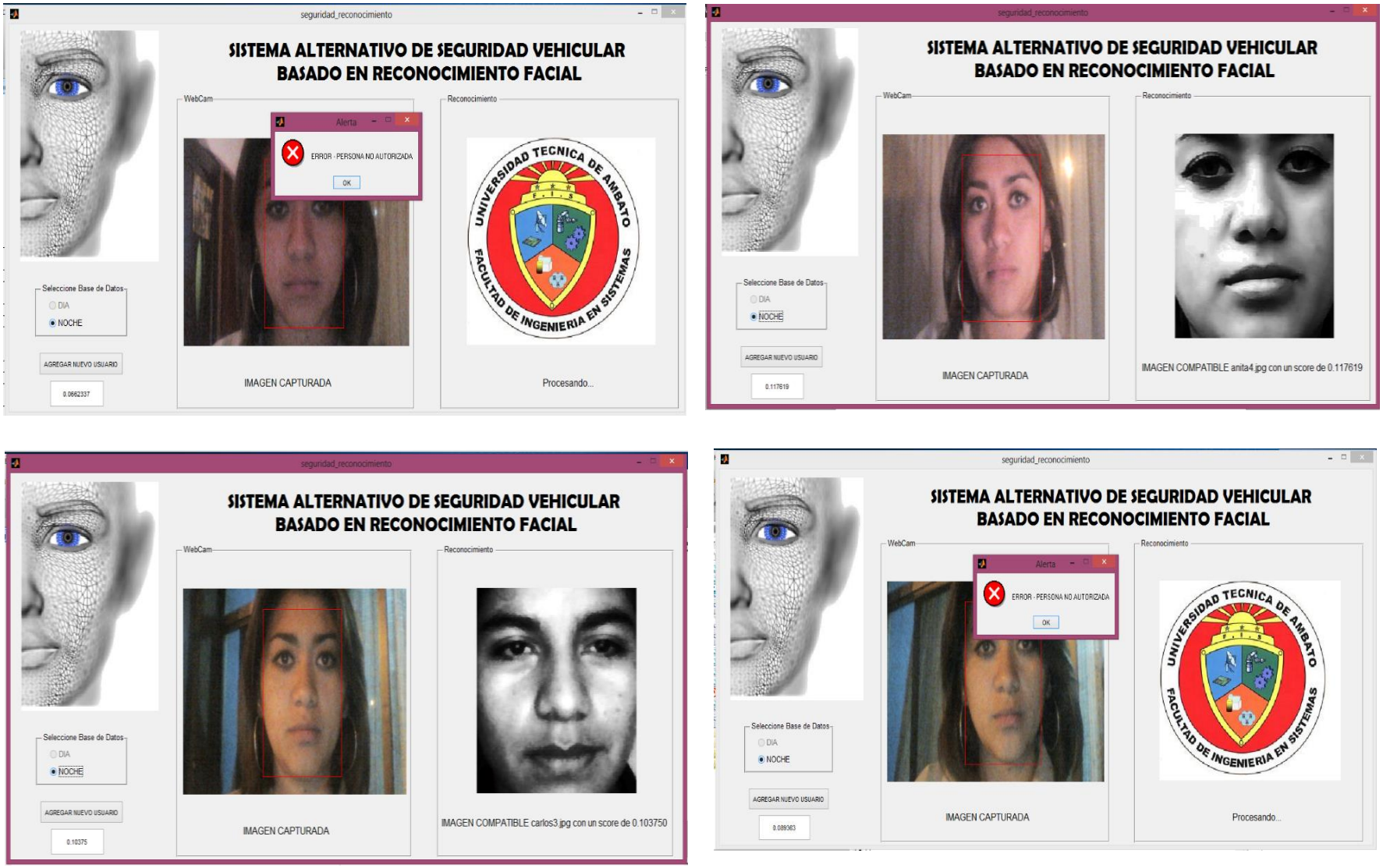


Figura 2. 44 Pruebas durante la noche (primera persona autorizada)

Figura 2. 45 Pruebas durante la noche (segunda persona autorizada)

Figura 2. 46 Pruebas durante la noche (tercera persona autorizada)

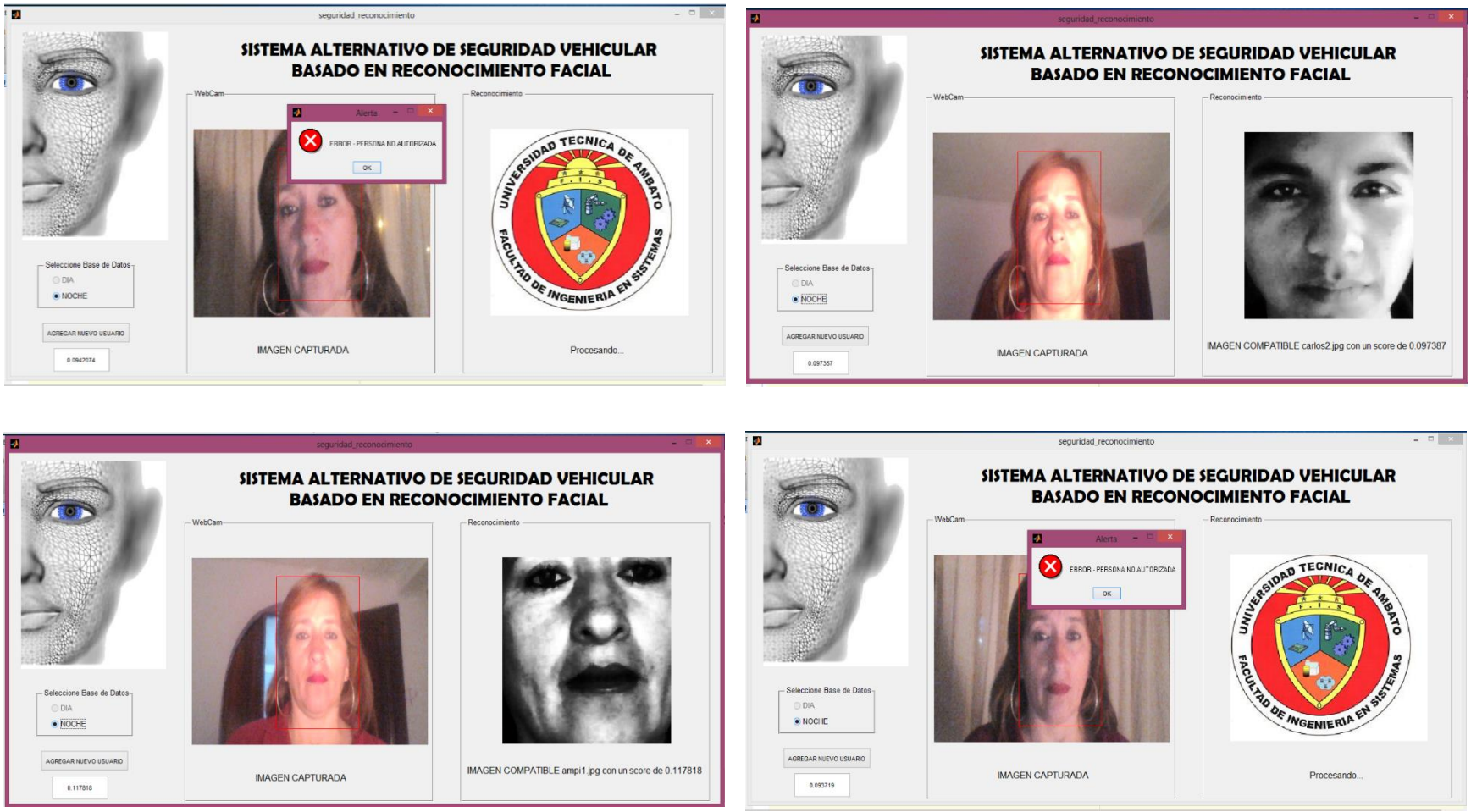


Figura 2. 47 Pruebas durante la noche (cuarta persona autorizada)

3.9 PRUEBAS REALIZADAS A USUARIOS EXTERNOS

Para comprobar cómo reacciona el sistema cuando se somete a prueba a un usuario externo a las bases de datos, se ha realizado varias capturas para poder comparar los resultados obtenidos, como se muestra en la figuras 2.48 – 2.51.

3.9.1 PRUEBAS REALIZADAS DURANTE EL DÍA

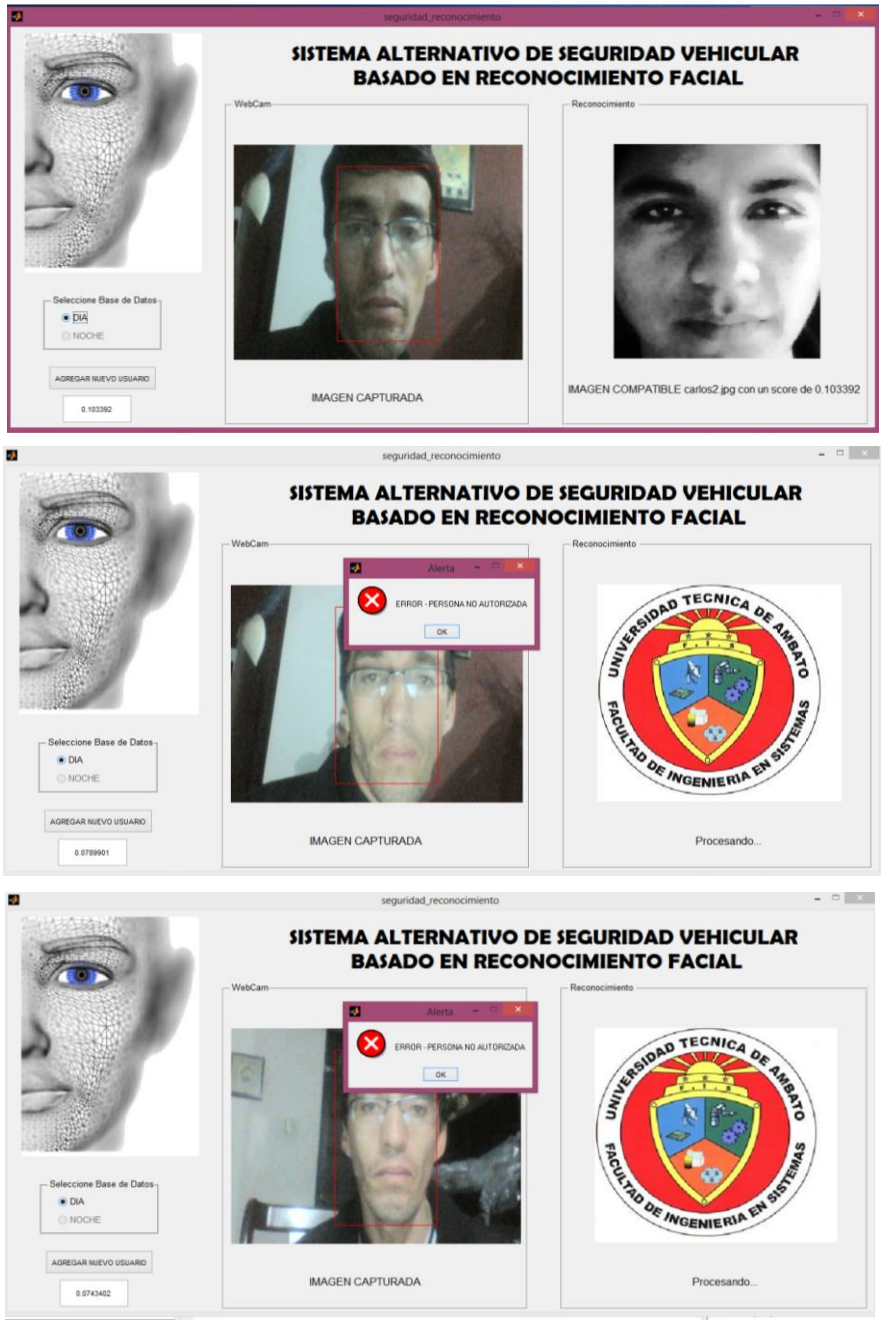


Figura 2. 48 Pruebas durante el día (primer usuario externo)

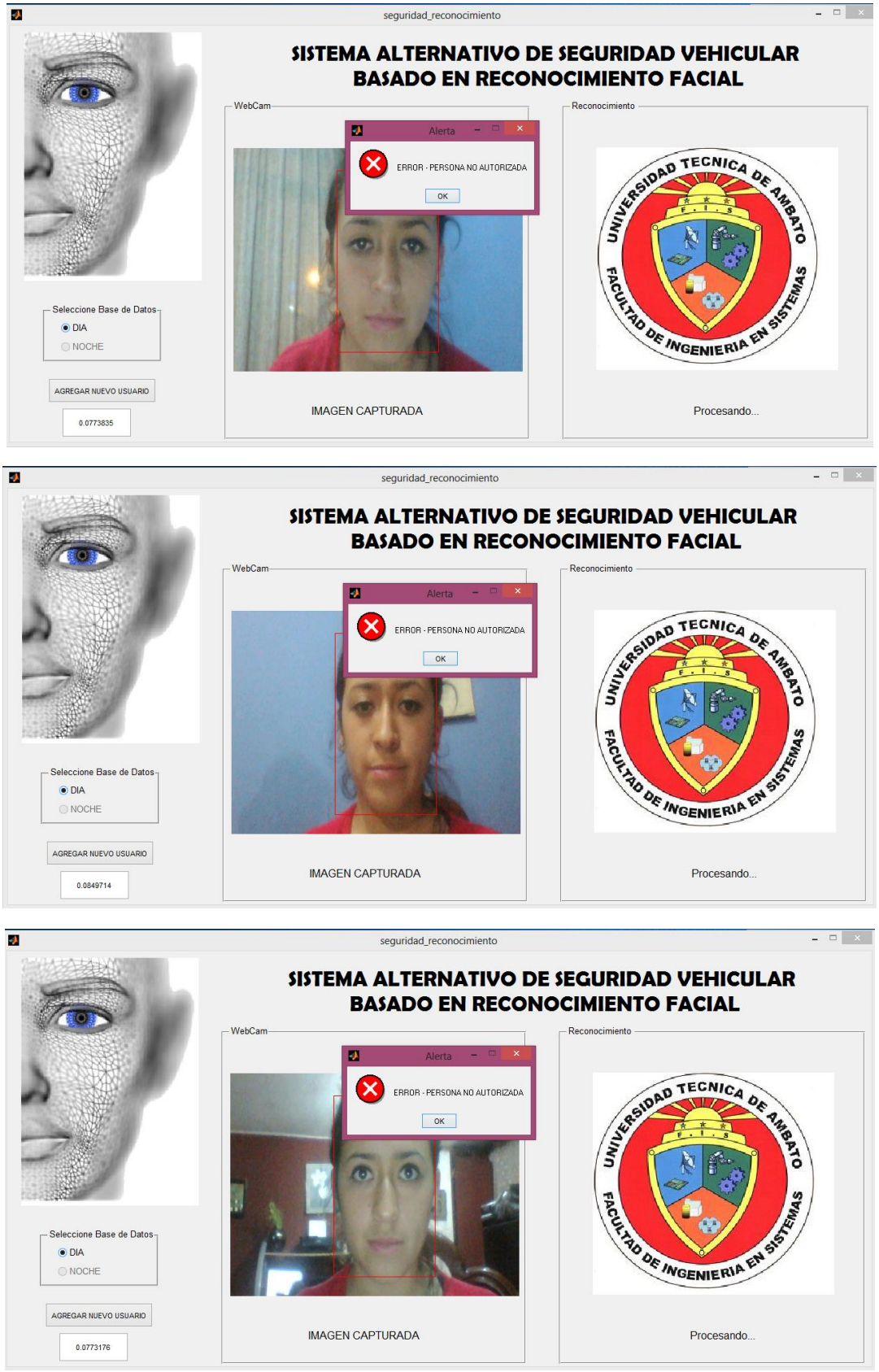


Figura 2. 49 Pruebas durante el día (segundo usuario externo)

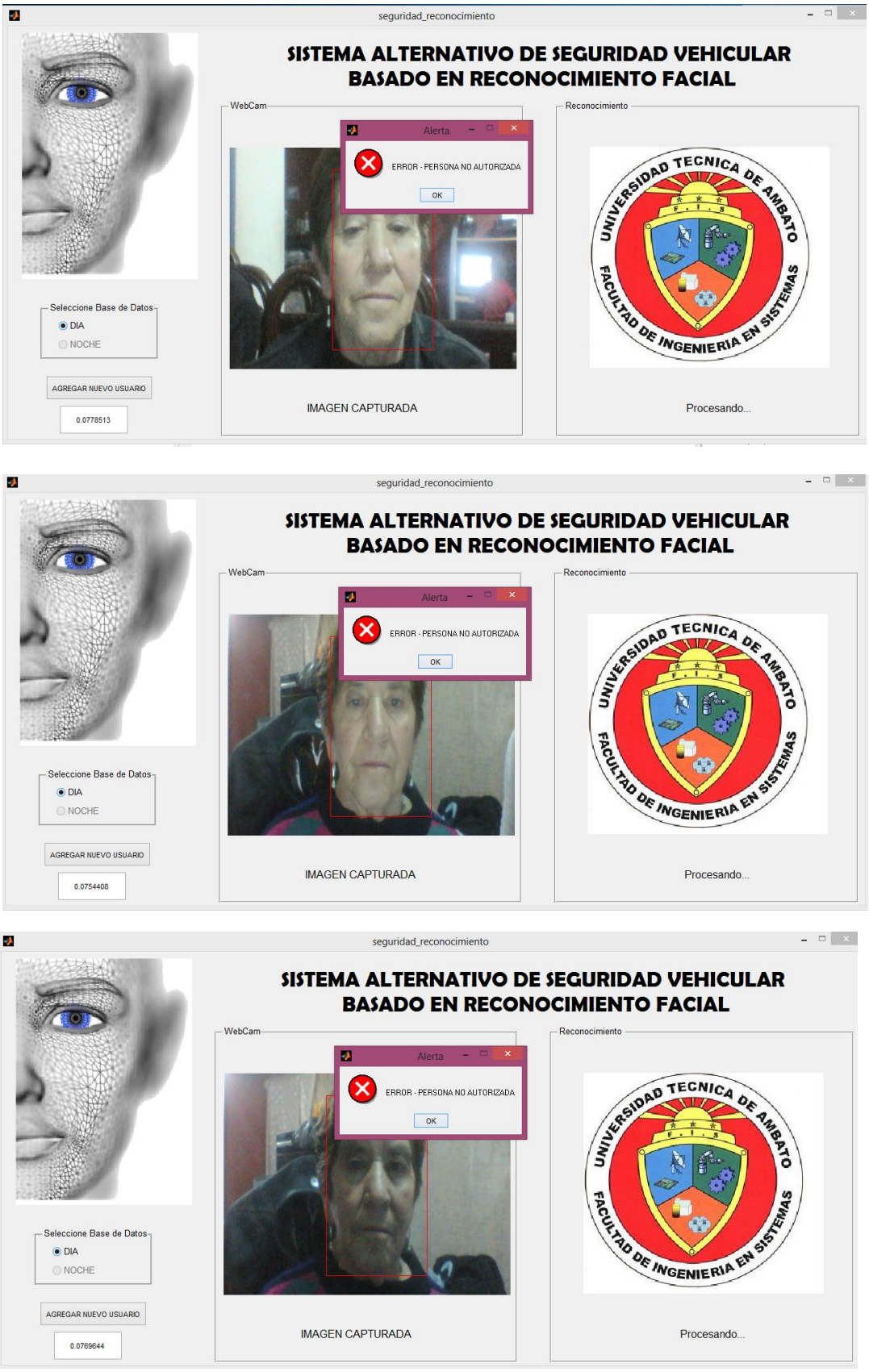


Figura 2. 50 Pruebas durante el día (tercer usuario externo)

Figura 2. 51 Pruebas durante el día (cuarto usuario externo)

3.9.2 PRUEBAS REALIZADAS DURANTE LA NOCHE

Las capturas de usuarios externos que se han realizado la prueba de reconocimiento se aprecia en las figuras 2.52 – 2.54

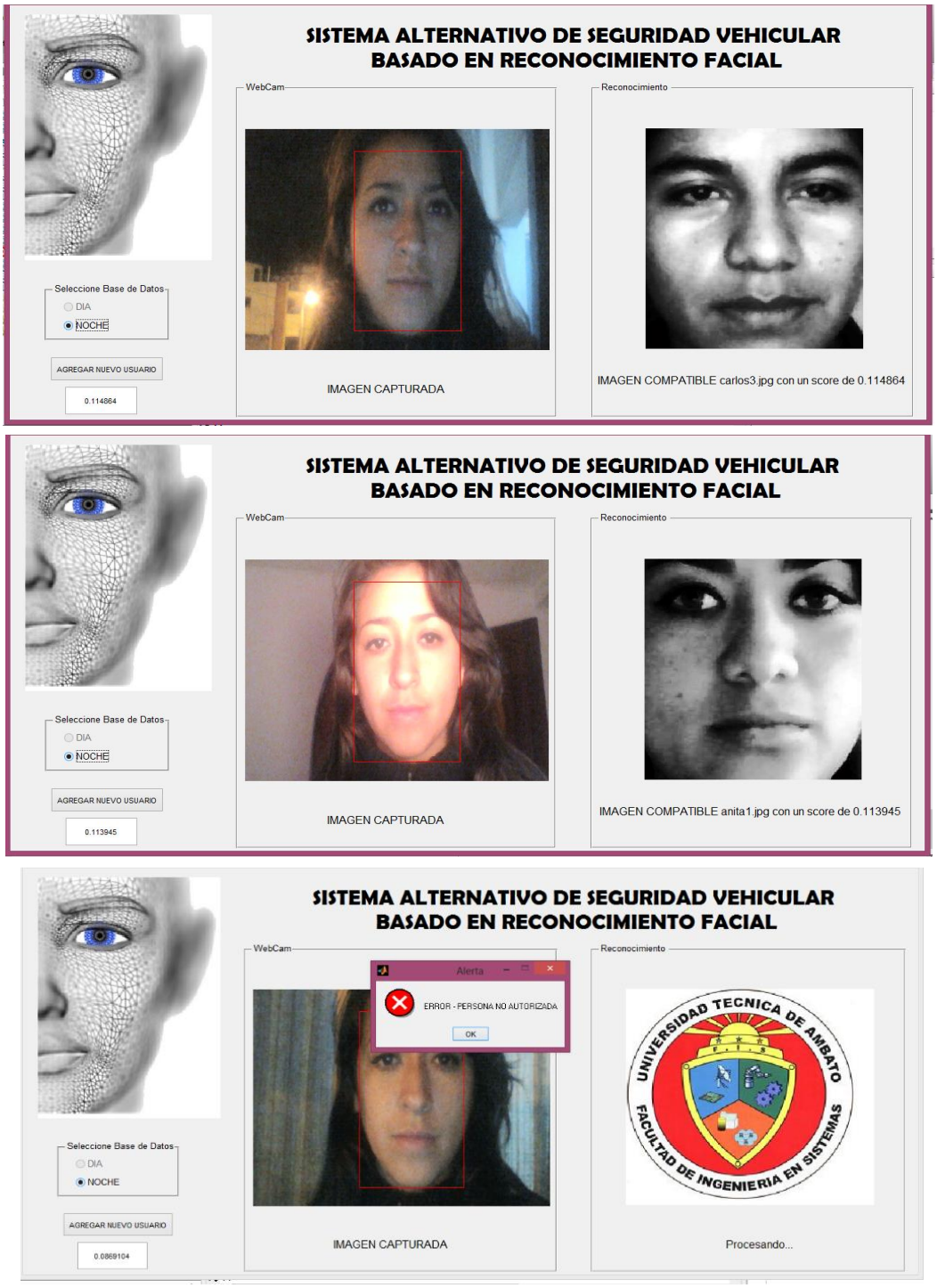


Figura 2. 52 Pruebas durante la noche (primer usuario externo)

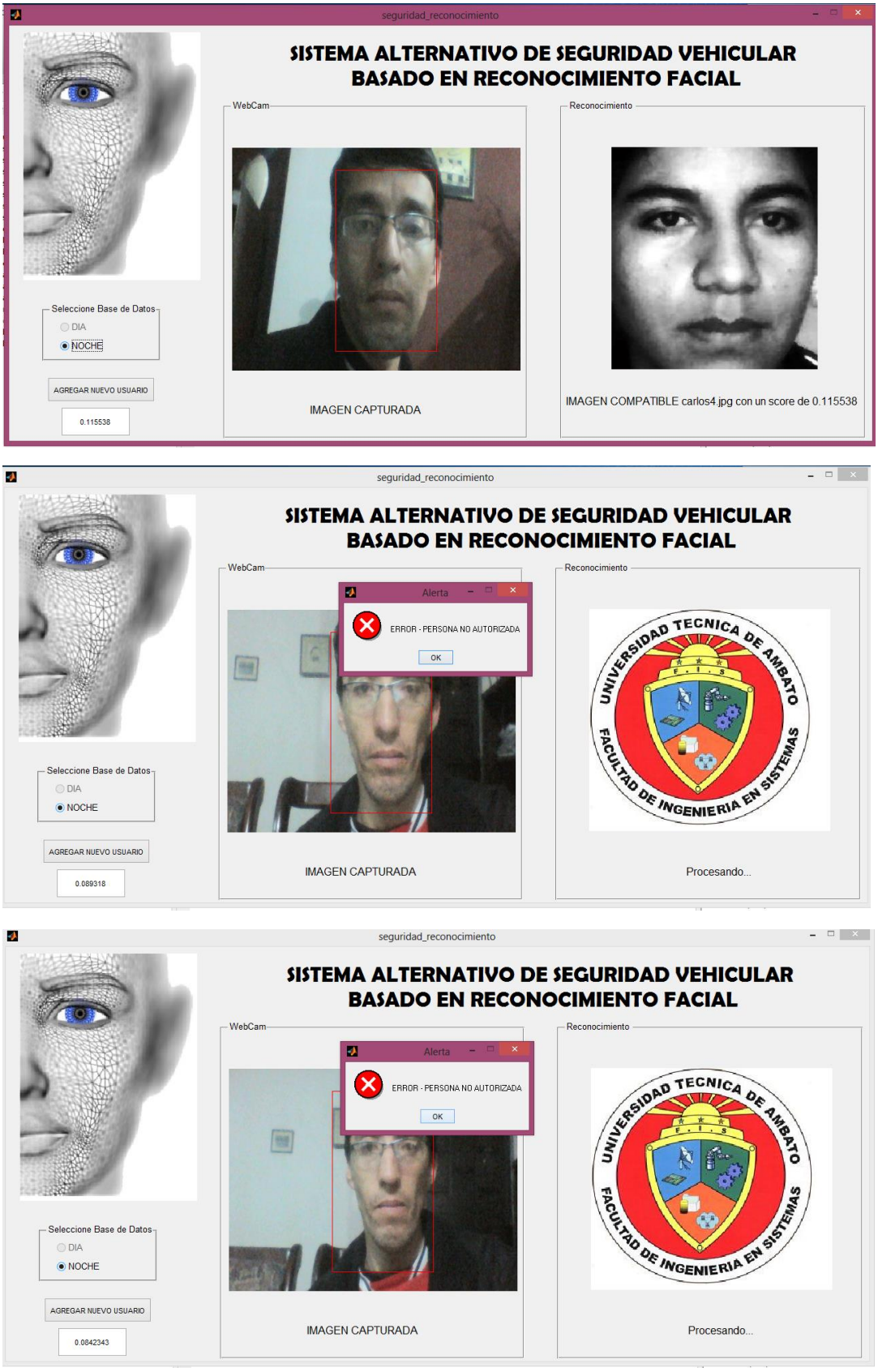


Figura 2. 53 Pruebas durante la noche (segundo usuario externo)

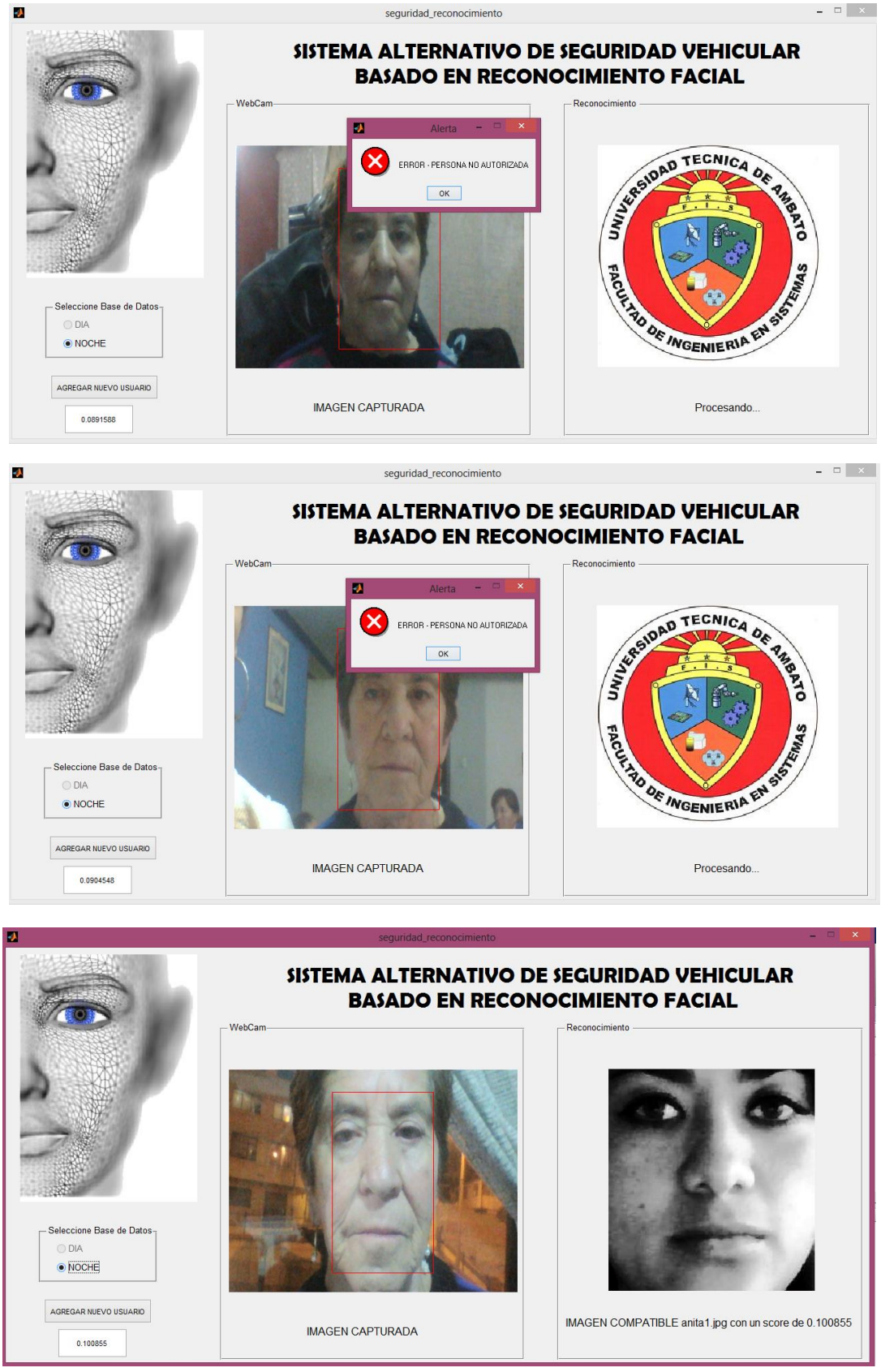


Figura 2. 54 Pruebas durante la noche (tercer usuario externo)

3.10 INTERPRETACIÓN DE RESULTADOS

El sistema ha sido sometido a varias pruebas para comprobar su eficiencia, capturando imágenes a diferentes usuarios (autorizados y externos), tanto en el día como en la noche para poder utilizar las dos bases de datos.

El sistema es capaz de arrojar cinco tipos de resultados:

- **Persona Autorizada – Permitida:** Cuando una persona autorizada es sometida a una prueba y el sistema permite el acceso (caso de éxito).
- **Persona Autorizada – No Permitida**: Cuando una persona autorizada es sometida a una prueba y el sistema no permite el acceso.
- **Persona Autorizada – Permitida/Diferente:** Cuando una persona autorizada es sometida a una prueba y el sistema permite el acceso, pero la imagen de entrada corresponde a una imagen que no es de la misma persona.
- **Persona Externa – Permitida**: Cuando un usuario externo a la base de datos se somete a una prueba y el sistema permite el acceso.
- **Persona Externa – No Permitida**: Cuando un usuario externo a la base de datos se somete a una prueba y el sistema no permite el acceso (caso de éxito).

Como resultados de la experimentación se obtienen los siguientes datos:

3.10.1 EXPERIMENTACIÓN DURANTE EL DÍA

Se capturaron 16 fotografías a los usuarios autorizados, y 12 fotografías a usuarios externos a la base de datos (28 capturas en total), posteriormente se ha determinado los resultados para cada opción de respuesta expresados en porcentajes usando la ecuación 11.

$$x = \frac{número\ de\ casos\ por\ respuesta * 100}{total\ de\ capturas\ realizadas} \qquad (11)$$

Donde x es el resultado de cada caso.

Obteniéndose los siguientes resultados:

- Persona Autorizada – Permitida: 10 casos 35,71%
- Persona Autorizada – No Permitida: 5 casos 17,86,43%
- Persona Autorizada – Permitida/Diferente: 1 caso 3,57%
- Persona Externa – Permitida: 2 casos 7,14%
- Persona Externa – No Permitida 10 casos 35,71%

3.10.2 EXPERIMENTACIÓN DURANTE LA NOCHE (PERSONAS AUTORIZADAS)

Al igual que se realizó para el día, en la noche se capturaron en total 32 fotografías a los usuarios autorizados y 9 fotos a los usuarios externos a la base de datos (41 capturas en total).

Se han determinado porcentajes de acuerdo a los valores de cada opción de respuesta mediante la ecuación 11, obteniéndose los siguientes resultados:

- Persona Autorizada – Permitida: 22 casos 53,65%
- Persona Autorizada – No Permitida: 4 casos 21,95%
- Persona Autorizada – Permitida/Diferente: 6 casos 17,03%
- Persona Externa – Permitida: 4 casos 9,75%
- Persona Externa – No Permitida 5 casos 12,19%

3.11 CONFIABILIDAD DEL SISTEMA

Después de haber determinado los resultados parciales, se procede a calcular un porcentaje de efectividad del sistema para el día y otro para la noche. Para esto se suma únicamente los porcentajes que correspondientes a los casos de éxito de acuerdo a la ecuación 12:

$$\frac{\begin{array}{r}\%\ persona\ autoriada\ permitida \\ +\ \%\ persona\ externa\ no\ permitida\end{array}}{CONFIABILIDAD} \qquad (12)$$

Gracias a las pruebas realizadas y en base a los resultados generados, el sistema ofrece un nivel de seguridad de acuerdo a lo siguiente:

CONFIABILIDAD DEL SISTEMA EN EL DÍA: 71,42%

CONFIABILIDAD DEL SISTEMA EN LA NOCHE: 65,84%

Es importante mencionar que la técnica empleada no rechaza a los usuarios que no se encuentren en la base datos, puesto que busca la imagen del rostro al que más se parece, es decir siempre habrá un sujeto semejante, la decisión de rechazo de los usuarios externos se realiza en base a la medida de la distancia euclídea.

Además, el sistema propuesto es capaz de presentar mejores resultados cuando se trabaja en condiciones de laboratorio, es decir condiciones óptimas de luz, pero al trabajar al aire libre, la luz se ve proyectada en diferentes direcciones lo que dificulta el reconocimiento.

3.12 DISEÑO DEL SISTEMA (HARDWARE)

3.12.1 ESQUEMA DE CONEXIÓN DEL SISTEMA DENTRO DEL VEHÍCULO

Como se denota en la figura, el sistema de seguridad se coloca entre la línea de alimentación entre la llave de encendido y el alternador, de esta manera se garantiza que el auto no se va a encender mientras no se realice el proceso de reconocimiento facial, pues el circuito se encuentra abierto.

No es necesario de una fuente externa, pues la alimentación para la UDOO se toma directamente de Vcc del radio del auto.

Como se puede observar en la figura 2.55, cuando el usuario requiera encender el auto, no podrá hacerlo pues la placa UDOO no permite el arranque del motor, por lo tanto la persona debe obligatoriamente identificarse mediante el reconocimiento facial.

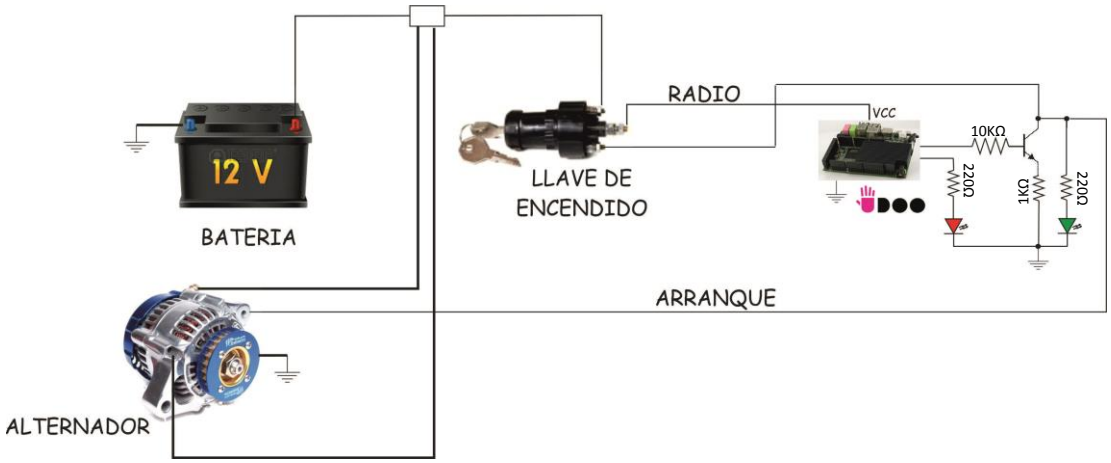


Figura 2. 55 Esquema de Conexión del sistema en el auto

Al girar la llave de encendido, la placa UDOO se energiza y automáticamente la aplicación que permite el reconocimiento se ejecuta. Si la persona es reconocida, el transistor que se encuentra conectado a una de las salidas de la placa se activa permitiendo el paso de energía hacia el alternador, pero en caso de que el conductor no sea reconocido, el transistor permanecerá abierto y el auto no encenderá a pesar de que la llave de encendido se encuentre en la posición de arranque.

Para la instalación del sistema en un auto, las conexiones se deben realizar tal como se muestra en el esquema.

3.12.2 UBICACIÓN DE LOS DISPOSITIVOS DENTRO DEL VEHÍCULO

Como se comentó anteriormente tanto la cámara como la pantalla táctil deben ir conectados a la minicomputadora (UDOO), y dentro del vehículo estos dispositivos van dispuestos de la forma en que se indica en la figura 2.56.

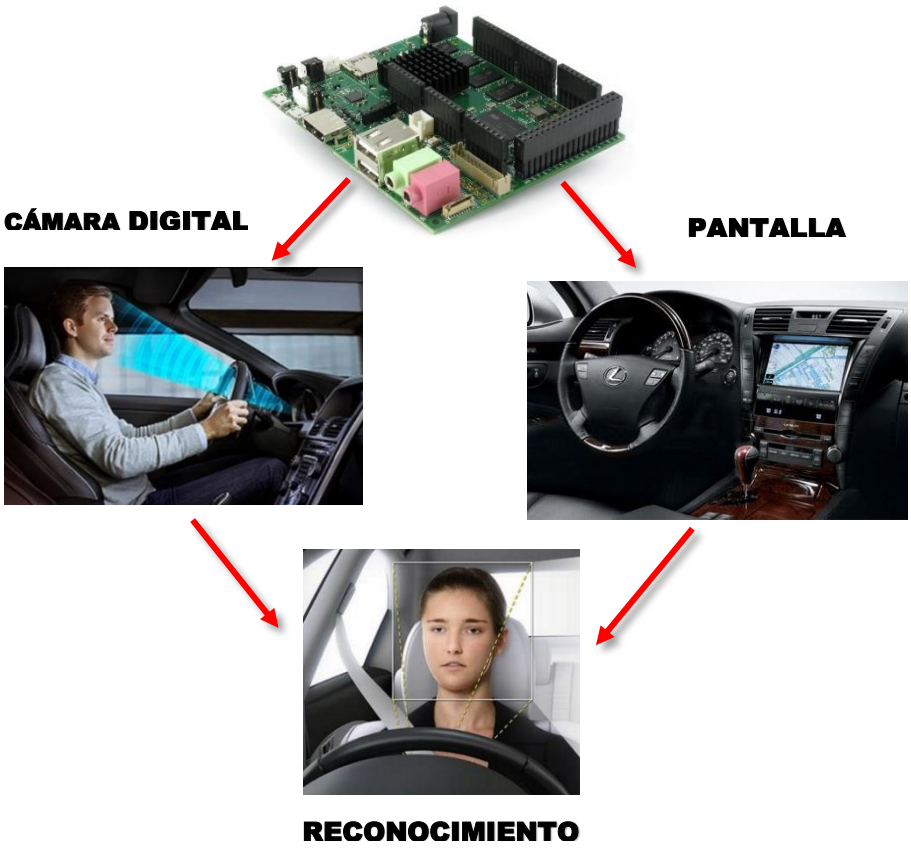


Figura 2. 56 Dispositivos del sistema de seguridad ubicados dentro del auto

3.13 DISEÑO DEL PROTOTIPO

Para realizar la implementación del prototipo del sistema de seguridad propuesto, se ha empleado una laptop HP Pavilion 14 con una cámara web HP Truevision HD integrada, con la que se ha realizado la captura de las imágenes.

Gracias a la posibilidad que Matlab ofrece para conectarse con algunos dispositivos hardware, se utilizará la placa de Arduino Uno para demostrar el funcionamiento del sistema, encendiendo un led de color verde y activando un motor DC cuando la persona sometida a la prueba de reconocimiento sea autorizada para usar el auto, de lo contrario se enciende un led de color rojo para indicar que se ha producido un error en el reconocimiento y la persona no está autorizada para hacer uso del vehículo.

3.13.1 COMUNICACIÓN ENTRE MATLAB - ARDUINO

Se puede desarrollar varios proyectos interesantes gracias a la interacción entre un GUI desarrollado en Matlab – Guide y la placa Arduino, permitiendo al usuario controlar un circuito electrónico mediante su computador y ejecutar órdenes desde este, como por ejemplo: al pulsar un botón de la interfaz gráfica empiecen a girar los servomotores de un brazo robótico, o realizar una adquisición de datos y presentarlos en una gráfica de Matlab.

Para demostrar el funcionamiento del sistema, se ha desarrollado un prototipo empleando la tarjeta electrónica de Arduino.

El giro de la llave de encendido del auto, cuando una persona requiera hacer uso de este, es simulado mediante un pulsador o un switch, como el sistema requiere que la persona sea identificada, el motor DC conectado a una de las salidas de la placa no se activa. Es necesario entonces, que el usuario presione el botón que permite la ejecución del proceso de reconocimiento facial.

Si el resultado es positivo, y la persona es reconocida, el sistema se desbloquea permitiendo que el motor DC se encienda, activando también el led de color verde, caso contrario, si el sistema no reconoce al sujeto, en pantalla se presenta un mensaje de error y un led rojo se enciende como alerta, entonces la persona nuevamente debe reiniciar el proceso de reconocimiento para poder encender el motor.

3.13.2 REQUERIMIENTOS PARA LA COMUNICACIÓN MATLAB - ARDUINO

- Es necesario tener una versión de Matlab superior a la 2014a y descargar el paquete que permite la conexión con Arduino.
- Se puede utilizar cualquier tipo de placa Arduino, pero en este caso se utiliza la placa Arduino Uno.

3.13.3 PROCEDIMIENTO PARA REALIZAR PARA LA COMUNICACIÓN MATLAB - ARDUINO

- Descargar el paquete para la conexión directamente de la página oficial de MathWorks.

- Ejecutar el Software de Arduino
- Mediante el cable USB conectar la placa Arduino Uno.
- Verificar el puerto "*COM*" del computador al cual se conectó la placa
- Dentro de la carpeta ArduinoIO que viene conjuntamente con el paquete descargado de MathWorks se encuentra un *sketch* llamado "*adiosrv.pde*'' que se debe cargar en la placa Arduino, este *sketch* permite que el Arduino comprenda las órdenes enviadas desde Matlab.
- Dentro de Matlab la carpeta ArduinoIO debe colocarse en el *Current Folder.*
- En el *Command Window* digitar *install_arduino*
- Finalmente escribir *a=arduino('COMX')*, donde *X* es el número del puerto *COM* al que se conectó la placa, entonces Matlab la reconoce e identifica todos sus pines, después de esto la conexión Matlab – Arduino ha sido establecida [35].

3.13.4 PROGRAMACIÓN DE MATLAB - ARDUINO

Para demostrar el funcionamiento del sistema, se ha desarrollado un prototipo mediante la tarjeta Arduino, encendiendo dos leds (verde y rojo), representando el permiso para usar el auto y en su defecto para impedir su uso, además del giro de del motor DC.

```
clear all;
global a;
a=arduino('COM4')
a.pinMode(8,'output');
a.pinMode(4,'output');
a.digitalWrite(4,1);
a.digitalWrite(8,0);
```

3.13.5 PRUEBA DE FUNCIONAMIENTO DE LA PLACA ARDUINO

Después de haber realizado el reconocimiento, el sistema se conecta con la placa Arduino para activar un led dependiendo del resultado.

En la figura 2.57 se indica el intento de conexión que realiza Matlab con Arduino después del reconocimiento.

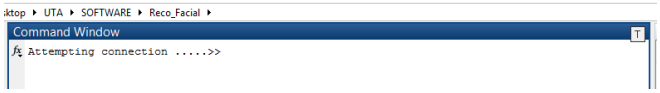


Figura 2. 57 Estableciendo comunicación entre Matlab y Arduino

Después de que se ha conseguido la conexión, Matlab reconoce la placa Arduino identificando cada uno de sus pines, como se presenta en la figura 2.58

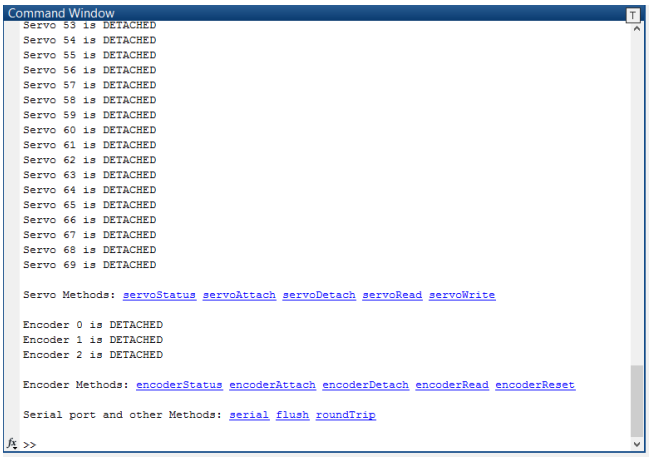


Figura 2. 18 Detectando pines de la placa Arduino

Finalmente, Arduino enciende los leds respectivos y el motor DC, dependiendo del resultado.

3.13.6 SIMULACIÓN DEL PROTOTIPO

Para demostrar su funcionamiento, el prototipo ha sido simulado en Proteus 8 Professional empleando las librerías de Arduino. Como se aprecia en la figura 2.59 el led verde esta encendido y el motor activado ya que se ha reconocido a la persona.

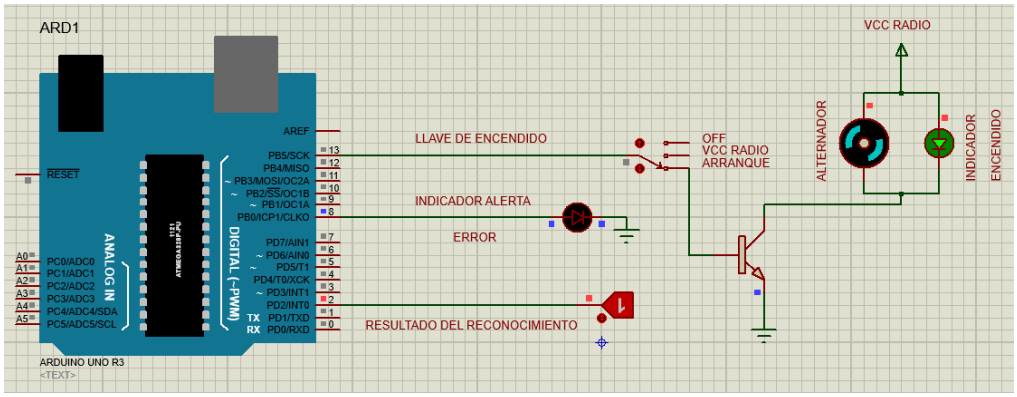


Figura 2. 59 Caso en el que la persona es reconocida

En la figura 2.60 se indica que se ha producido un error en el reconocimiento encendiendo el led rojo.

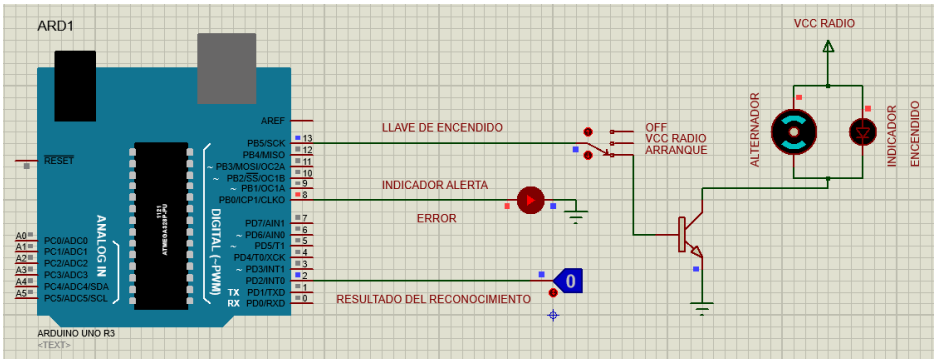


Figura 2. 60 Caso en el que la persona no es reconocida

3.14 ANÁLISIS ECONÓMICO DEL PROYECTO

El costo de los dispositivos y demás componentes necesarios para la implementación del sistema de seguridad vehicular basado en reconocimiento facial se detalla en la tabla 2.8

Tabla 2. 8 Costo de materiales para el proyecto

DESCRIPCION	CANTIDAD	VALOR UNIT.	VALOR TOTAL
Placa UDOO	1	$135,00	$135,00
Pantalla Táctil	1	$ 125,00	$ 125,00
Cámara Digital	1	$ 39,00	$ 39,00
Transistor	1	$ 0,30	$ 0,30
Fusible	1	$ 0,50	$ 0,50
Pulsador o Switch	1	$ 0,35	$ 0,35
Led (rojo, verde)	2	$ 0,10	$ 0,20
Regulador de Voltaje	1	$ 0,50	$ 0,50
Resistencias 220Ω	2	$ 0,10	$ 0,20
		TOTAL	301,05

Debido a que el sistema de seguridad basado en reconocimiento facial, corresponde a un trabajo de investigación previo a la obtención del título de Ingeniería en Electrónica y Comunicaciones, la licencia de Matlab no tiene ningún costo por ser la versión académica, pero en caso de que el sistema se requiera implementarlo a nivel industrial o empresarial, se debe cancelar el valor correspondiente a la licencia de Matlab Empresarial.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

- El encendido del vehículo únicamente se lo puede realizar mediante la identificación del usuario (si este es autorizado).
- Las pruebas de funcionamiento determinan que el reconocimiento facial se ve afectado por condiciones luminosas y posición del rostro.
- El nivel de confiabilidad del sistema es mayor durante el día ya que se puede tener una mejor iluminación del rostro, mientras que en la noche la luz presente en el ambiente es escasa dificultando el reconocimiento.
- La técnica empleada para el reconocimiento no rechaza a usuarios externos pues siempre presenta la imagen con mayor parentesco, la decisión de rechazo se realiza mediante la Distancia Euclidiana.

4.2 RECOMENDACIONES

- Se recomienda actualizar constantemente la base de datos, sobre todo cuando exista cambios en la apariencia de la persona para garantizar el reconocimiento.
- Es necesario almacenar la mayor cantidad de fotografías de cada usuario en la base de datos, de esta manera se tiene mayor posibilidad de que el reconocimiento se efectúe correctamente.
- Se debe procurar que en el reconocimiento facial efectuado por la noche, la fuente de luz refleje directamente en el rostro, ya que si se presenta por detrás de la cabeza, las imágenes serán oscuras presentado resultados erróneos.
- Es recomendable que las personas usuarias de lentes, almacenen sus fotografías en la base de datos haciendo uso de este accesorio, pues al momento de la identificación mediante el reconocimiento, se puede presentar errores por este motivo.

BIBLIOGRAFÍA:

[1] "La principal provincial del Ecuador redujo los índices delincuenciales en los primeros cuatro meses del año", 28 de mayo, 2014, Publicado por: Agencia de Noticias Andes, Disponible en: http://www.andes.info.ec/es/noticias/principal-provinciaecuador-redujo-indices-delincuenciales-primeros-cuatromeses-ano.html.

[2] "Índice delincuencial se reduce en el 24,8%", 2 de Julio, 2014, Publicado por Diario El Heraldo, Disponible en: http://www.elheraldo.com.ec/index.php?fecha=2014/0702&seccion=Policiales&noticia=42302

[3] Gallagher R, 12 de Diciembre, 2012, "Ecuador Implements "World's First" Countrywide Facial- and Voice-Recognition System",

[4] Cando L., Noviembre, 2011, "Bloqueo electrónico en el encendido de un vehículo para proporcionar un sistema de seguridad contra robos", Universidad Técnica de Ambato.

[5] Roca S., Chaparro I., 16 de octubre, 2008, "Sistema de bloqueo para automóviles y otros vehículos", Número de publicación WO2008122676 A1.

[6] Oliveras A., Roca S., Chaparro I, 2 de Febrero, 2012, "Dispositivo de identificación y seguridad por biometría ocular a corta distancia", Número de publicación WO2012013849 A1.

[7] Couch S., Knowles T., 2 de noviembre, 2005, "Alcohol impairment detection and interlock system with tester identification", Número de publicación EP 1591296 A1.

[8] Castillo P., 24 de Julio, 2008, "Sistemas de transmisión de datos en forma remota y digital y localización satelital desde terminales móviles o fijas con cámaras de vigilancia urbana para reconocimiento facial", Número de publicación WO 2008088203 A1.

[9] Chen H., 25 de Marzo, 2010, "Un método de identificación inteligente y el método para lograr terminal de reconocimiento", Número de publicación WO 2010031213 A1.

[10] “Tipos de Alarmas de Vehículos”, Disponible en: http://www.gestiexport.com/Alarmas_vehiculos/Tipos_de_Alarmas_de_vehiculos.htm

[11] “Alarmas para coches”, Disponible en: http://www.alarmasseguridad.com/tipos-alarmas/alarmas-para-coches.html

[12] “Sistemas de Inmovilización”, Repositorio ESPE, Disponible en: http://repositorio.espe.edu.ec/bitstream/21000/4157/2/T-ESPEL-0225.pdf?%20-%20zoom=81&statusbar=0&navpanes=0&messages=0

[13] Bronte S., 2008, “Sistema de Detección y Reconocimiento Facial de Conductores Mediante Sistemas de Visión Computacional”, Universidad de Alcalá.

[14] Jiménes D., Paredes G., “Análisis, Diseño e Implementación de un Prototipo de Sistema para Reconocimiento de Firmas Personales con Métodos de Visión Artificial”, mayo, 2012, Unidad Politécnica Salesiana

[15] Bauzá M., “Sistema de Autificación Facial”, Universidad de Palermo.

[16] Travieso C., Ticay Jaime, “Sistemas Biométricos”, mayo, 2011, Universidad de las Palmas de Gran Canaria. Disponible en: http://www.rcysostenibilidad.telefonica.com/blogs/documentoscatedras/files/2012/07/Catedra_telefonica_Sistemas_Biometricos.pdf

[17] Pérez P., “Estudio sobre las tecnologías biométricas aplicadas a la seguridad”, diciembre, 2011, INTECO, Gobierno de España.

[18] Gámez Carmen. “Diseño y Desarrollo de un Sistema de Reconocimiento de Caras”, Madrid, abril, 2009, Universidad Carlos III de Madrid.

[19] Blásquez L., 2013, “Reconocimiento Facial Basado en Puntos Característicos de la Cara en entornos no controlados”, Universidad Autónoma de Madrid

[20] Gimeno R., Mayo 2010, “Estudio de Técnicas de Reconocimiento Facial”.

[21] Lorente Luis, “Representación de caras mediante eigenfaces”, Ramas de Estudiantes de la IEEE.

[22] Argüello H., 22 de noviembre, 2011, “Sistemas de Reconocimiento basados en la Imagen Facial”, Universidad Industrial de Santander, Colombia.

[23] Reinoso O., Pérez C., “Reconocimiento de Objetos 3d mediante análisis PCA”, Universidad Miguel Hernández.

[24] Cortés M., marzo, 2009, “Reconocimiento de Caras Frontales Mediante la Extracción de Puntos Característicos”, Universidad Autónoma de Madrid.

[25] Laorden E., “Descripción, comparación y ejemplos de uso de las funciones de la toolbox de procesado digital de imágenes de MATLAB”, septiembre, 2012, Universidad Politécnica de Madrid.

[26] “Arduino Uno”, Disponible en: http://arduino.cc/en/Main/arduinoBoardUno

[27] “Disminuye el robo de carros en Tungurahua”, 09 de octubre, 2013, Publicado por: Diario el Telégrafo, Disponible en: http://www.telegrafo.com.ec/regionales/regional-centro/item/disminuye-el-robo-de-carros-en-tungurahua.html.

[28] “Brigadas comunitarias frenan la delincuencia”, 27 de febrero, 2013, Publicado por: Diario El Telégrafo, Disponible en: http://www.telegrafo.com.ec/regionales/regional-centro/item/brigadas-comunitarias-frenan-a-la-delincuencia.html

[29] “UDOO”, enero, 2015. Disponible en: http://elinux.org/UDOO

[30] “Introducción a las Imágenes Digitales”, Disponible en: http://alojamientos.us.es/gtocoma/pid/tema1-2.pdf

[31] “Ecualización del histograma”, Disponible en: http://es.wikipedia.org/wiki/Ecualizaci%C3%B3n_del_histograma

[32] Aguilar G., diciembre, “Procesamiento Digital de Imágenes usando filtros morfológicos”, diciembre, Escuela Politécnica Nacional, Ecuador.

[33] “Filtros”, Disponible en: http://alojamientos.us.es/gtocoma/pid/tema3-1.pdf

[34] Barrera L., “Desarrollo e implementación de algoritmos para el sistema de percepción y localización de los robots Bogobots”, 26 de abril, 2010, Instituto Tecnológico y de Estudios Superiores de Monterrey.

[35] “Enlace Arduino - Matlab”, 18 de abril, 2013, Disponible en: https://www.youtube.com/watch?v=IyeKXNQ6Kww

ANEXOS

ANEXO A

PROGRAMACIÓN PARA LA ETAPA DE PREPROCESADO DE IMÁGENES DE LA BASE DE DATOS

- function CARGAR_Callback(hObject, eventdata, handles)

```
global imagen
axes(handles.axes1)
imagen=imread('mami3.jpg');          % carga una imagen de la BD
imshow(imagen)                       % visualiza la imagen
title('IMAGEN ORIGINAL');            % título de la imagen
```

- function PROCESAR_Callback(hObject, eventdata, handles)

```
% ecualizando imagen
global imagen;
axes(handles.axes2)
imag_gray=rgb2gray(imagen)           % transforma la imagen a
                                       escala de grises
imag_ecual=histeq(imag_gray);        % ecualiza la imagen
imshow(imag_ecual)                   % visualiza la imagen
title('IMAGEN ECUALIZADA');          % título de la imagen

% aplicando filtro de mediana
axes(handles.axes3)
imag_filt=medfilt2(imag_ecual);      % aplica el filtro de mediana a
                                       la imagen ecualizada
imshow(imag_filt                     % presenta la imagen final
                                       preprocesada
title('IMAGEN ECUALIZADA Y FILTRADA');  % título de la imagen
```

ANEXO B

PROGRAMACIÓN DE LA PORTADA REALIZADA EN MATLAB

- function seguridad_portada_OpeningFcn(hObject, eventdata, handles, varargin)

```
handles.output = hObject;

boton_on = imread('on.jpg');            % se lee la imagen para el botón de
                                          encendido
set(handles.on,'Cdata',boton_on);       % carga la imagen en el elemento
                                          correspondiente de la intefaz

axes(handles.axes3)
fondo1=imread('F1.jpg');                % carga la imagen del rostro (fondo)
imshow(fondo1);                         % visualiza la imagen de rostro (fondo)

axes(handles.axes1)                     % axes para vizualizar sello uta
sello=imread('sello3.jpg');             % lee la imagen del sello
imshow(sello);                          % presenta la imagen

axes(handles.axes2)                     % axes para vizualizar sello uta
sello=imread('uta.jpg');                % lee la imagen del sello
imshow(sello);                          % presenta la imagen

% Update handles structure
guidata(hObject, handles);
```

- function on_Callback(hObject, eventdata, handles)

```
seguridad_reconocimiento;               % ejecuta el GUI para el
                                          reconocimiento facial
```

ANEXO C

PROGRAMACIÓN PARA LA ETAPA DEL RECONOCIMIENTO FACIAL

- function seguridad_reconocimiento_OpeningFcn(hObject, eventdata, handles, varargin)

```
handles.output = hObject;
axes(handles.axes11)
fondo2=imread('F14.jpg');                    % lee la imagen
imshow(fondo2);                              % presenta la imagen
%% ENCENDIDO DE CAMARA
global vid
axes(handles.axes1)
% creando y configurando el objeto de entrada para el video
vid = videoinput('winvideo', 1, 'MJPG_1280x720');
% Se obtiene el alto y ancho de los frames de video
vidRes=get(vid,'VideoResolution');
% Se obtiene el número de bandas de color de la imagen de entrada
nBands=get(vid,'NumberOfBands');
% Crea el objeto de imagen de acuerdo a los parámetros ingresados
himage= image ( zeros(vidRes(2),vidRes(1),nBands));
% Dibuja el rectángulo rojo
rectangle('Position',[520 170 300 390],'EdgeColor','r');
% Realiza el zoom a la imagen de entrada
zoom(1.5)
preview(vid,himage);                         % Permite visualizar la imagen
axes(handles.axes9)                          % axes para vizualizar sello fisei
sello=imread('sello.png');                   % lee la imagen del sello
imshow(sello);                               % presenta la imagen
 % Update handles structure
guidata(hObject, handles);
```

- function uipanel4_SelectionChangeFcn(hObject, eventdata, handles)

```
%% SELECCION DE LA BASE DE DATOS
if hObject== handles.dia

set(handles.noche,'Enable','off');
global vid                                  % presenta el sello
pause(5)
set(handles.capturando,'Visible','Off');    % Presenta el texto
CAPTURANDO
foto=getsnapshot(vid);                      % captura una fotografía
closepreview(vid);                          % detiene el video
% Presenta el texto IMAGEN CAPTURADA
set(handles.imag_cap,'Visible','On');

%% PREPROCESAR LA IMAGEN DE ENTRADA
% recorta la imagen procesada segun los parametros especificados
recorte=imcrop(foto,[540 240 260 280]);
% transforma la imagen capturada a escala de grises
imagen_gray=rgb2gray(recorte);

 %ecualizado
imag_ecual=histeq(imagen_gray);             % ecualiza la imagen

%filtrado
% aplica el filtro de mediana a la imagen ecualizada
imag_filt=medfilt2(imag_ecual);
% redimendiona la imagen al tamaño especificado
work_area=imresize(imag_filt,[64 64]);
% se guarda la imagen redimensionada
imwrite(work_area,'area_trabajo.jpg','jpg');

%% EMPIEZA EL PCA
input_dir='.\base_dia';                     % guarda la ruta de la BD
image_dims=[64,64];                         % normalizacion de las imágenes
```

```
% lista las imágenes existentes dentro de la base de datos
filenames= dir(fullfile(input_dir,'*.jpg'));
% cuenta el numero de imagenes en la estructura
num_images=numel(filenames);
%% representacion de imagenes en vectores
images=[];                                  % conjunto de caras vacio
% selecciona una imagen de la BD
for n=1:num_images
filename=fullfile(input_dir,filenames(n).name);
% se lee la imagen a convectir como vector
img=imread(filename);
img=im2double(img);                         % se pasa la imagen a double
   if n==1                                  % campo vectorial inicializado
% crea el campo vectorial de caras
   images=zeros(prod(image_dims),num_images);
    end
% redimensiona todas las imagenes de la BD
 img=imresize(img,image_dims);
% campo vectorial de caras generado
images(:,n)=img(:);
end

% calculo de la media de la matriz de covarianza
% Calcula la media de todas las imagenes
mean_face=mean(images,2);                   );
% Crea copias de la imagen media calculada
rep=repmat(mean_face,1,num_images
% Cálculo estadistico de la covarianza (info mas importante)
shifted_images=images-rep
% eigenvectores
% Se determina los componentes principales - eigenvectores (forma canonica
reducida)
[evectors,score]=princomp(images');

% Se limita el número de eigenvectores a utilizar
```

```
num_eigenvectors=50;
evectors= evectors(:,1:num_eigenvectors);            % eigenvectors sin ruido
% proyeccion de los vectores caracteristicos
features= evectors'* shifted_images;
%% DISTANCIA EUCLIDEANA Y CALCULO DE LA IMAGEN SIMILAR
% se lee la imagen con la que se va a trabajar
input_work=imread('area_trabajo.jpg');
% paso imagen a double
input_work=im2double(input_work);
feature_vec=evectors'*((input_work(:)- mean_face));
% Se calcula la distancia euclidiana inversa
imilarity_score= arrayfun(@(n)1/(1+norm(features(:,n)-feature_vec)),...
                    1:num_images);
% encuentra la imagen con mayor similitud
[match_score,match_1x]= max(similarity_score);
score_resul=match_score;
set(handles.edit2,'String',score_resul);

% muestra el resultado
% la max distancia permitida es 0.095
if score_resul>0.095
% Selecciona la imagen con mayor semejanza
foto_gan=filenames(match_1x).name;
% lee la imagen con mayor semejanza
foto_win=imread(foto_gan);
axes(handles.axes9)
% visualiza la imagen ganadora
imshow(foto_win);
% presenta un mensaje con el score resultante y el nombre de la persona con la
cual coincidió la imagen

leyenda=sprintf('IMAGEN COMPATIBLE %s con un score de %f',...
filenames(match_1x).name, score_resul);
set(handles.leyenda,'String',leyenda);
   set(handles.leyenda,'Visible','On');
```

```
   pause (3)
   clc, clear all, close all
   msgbox('ACCESO PERMITIDO, PUEDE CONTINUAR');
      clear all;
   global a;
    a=arduino('COM4')
   a.pinMode(8,'output');
   a.pinMode(4,'output');
    a.digitalWrite(8,1);
   a.digitalWrite(4,0);
 else
    pause(2)
    errordlg('ERROR - PERSONA NO AUTORIZADA','Alerta');

   clear all;
   global a;
    a=arduino('COM4')
   a.pinMode(8,'output');
   a.pinMode(4,'output');

   a.digitalWrite(4,1);
   a.digitalWrite(8,0);
 end
else                                          % else del if principal
  set(handles.dia,'Enable','off');
  global vid                                   % presenta el sello

Sonido de conteo regresivo
[Y,Fs]=audioread('conteoreg.wav');            % Agrega audio
sound(Y,Fs);                                  % Reproduce el audio
pause(5)
set(handles.capturando,'Visible','Off');      % Presenta el texto
                                                CAPTURANDO
foto=getsnapshot(vid);                        % captura una fotografía
closepreview(vid);                            % detiene el video
```

```
set(handles.imag_cap,'Visible','On');                % Presenta el texto IMAGEN
                                                       CAPTURADA

%% PREPROCESAR LA IMAGEN DE ENTRADA
% recorta la imagen procesada segun los parametros especificados
recorte=imcrop(foto,[540 240 260 280]);
% transforma la imagen capturada a escala de grises
imagen_gray=rgb2gray(recorte);
%ecualizado
imag_ecual=histeq(imagen_gray);                      % ecualiza la imagen

%filtrado
% aplica el filtro de mediana a la imagen ecualizada
imag_filt=medfilt2(imag_ecual);
% redimendiona la imagen al tamaño especificado
work_area=imresize(imag_filt,[64 64]);
% se guarda la imagen redimensionada
imwrite(work_area,'area_trabajo.jpg','jpg');
%% EMPIEZA EL PCA
% guarda la ruta de la base de datos
input_dir='.\base_noche';
% normalizacion de las imagenes
image_dims=[64,64];
% lista los imágenes existentes dentro de la base de datos
filenames= dir(fullfile(input_dir,'*.jpg'));
% cuenta el numero de imagenes en la estructura
num_images=numel(filenames);
%representacion de imagenes en vectores
images=[];                                           % conjunto de caras vacio
for n=1:num_images
    % selecciona una imagen de la BD
% se lee la imagen a convectir como vector
filename=fullfile(input_dir,filenames(n).name);
img=imread(filename);
%img=rgb2gray(img);%paso imagenes a grises
```

```
% se pasa la imagen a double
img=im2double(img);
  % campo vectorial inicializado crea el campo vectorial de caras
if n==1
images=zeros(prod(image_dims),num_images);
   end
% redimensiona todas las imagenes de la BD
img=imresize(img,image_dims);
% campo vectorial de caras generado
images(:,n)=img(:);
        end
% calculo de la media de la matriz de covarianza
% Calcula la media de todas las imagenes
mean_face=mean(images,2);
% Crea copias de la imagen media calculada
rep=repmat(mean_face,1,num_images);
% Cálculo estadistico de la covarianza (info mas importante)
shifted_images=images-rep;

% eigenvectores
% Se determina los componentes principales - eigenvectores (forma canonica
reducida)
[evectors,score]=princomp(images');
% Se limita el número de eigenvectores a utilizar
num_eigenvectors=50;
% eigenvectors sin ruido
evectors= evectors(:,1:num_eigenvectors);
% proyeccion de los vectores caracteristicos
features= evectors'* shifted_images;

%% DISTANCIA EUCLIDEANA Y CALCULO DE LA IMAGEN SIMILAR
% se lee la imagen con la que se va a trabajar
input_work=imread('area_trabajo.jpg');
% paso imagen a double
input_work=im2double(input_work);
```

```
feature_vec=evectors'*((input_work(:)- mean_face));
% Se calcula la distancia euclidiana inversa
similarity_score= arrayfun(@(n)1/(1+norm(features(:,n)-feature_vec)),...
                        1:num_images);
% encuentra la imagen con mayor similitud
[match_score,match_1x]= max(similarity_score);
score_resul=match_score;
set(handles.edit2,'String',score_resul);

% muestra el resultado
 % la max distancia permitida es 0.06
if score_resul>0.06
 % Selecciona la imagen con mayor semejanza
foto_gan=filenames(match_1x).name;
% lee la imagen con mayor semejanza
foto_win=imread(foto_gan);
axes(handles.axes9)
% visualiza la imagen ganadora
imshow(foto_win);
% presenta un mensaje con el score resultante y el nombre de la persona con la
cual coincidió la imagen
leyenda=sprintf('IMAGEN COMPATIBLE %s con un score de %f',...
          filenames(match_1x).name, score_resul);
   set(handles.leyenda,'String',leyenda);
   set(handles.leyenda,'Visible','On');
   pause (3)
   clc, clear all, close all
   msgbox('ACCESO PERMITIDO, PUEDE CONTINUAR');

   clear all;
   global a;
   a=arduino('COM4')
   a.pinMode(8,'output');
   a.pinMode(4,'output');
   a.digitalWrite(8,1);
```

```
    a.digitalWrite(4,0);
else
     pause(2)
     errordlg('ERROR - PERSONA NO AUTORIZADA','Alerta');
    clear all;
    global a;
     a=arduino('COM4')
    a.pinMode(8,'output');
    a.pinMode(4,'output');
   a.digitalWrite(4,1);
    a.digitalWrite(8,0);

end
end                                                  % end del if principal
```

ANEXO D

PROGRAMACIÓN DEL GUI PARA AGREGAR NUEVO USUARIO

- function agregar_usuario_OpeningFcn(hObject, eventdata, handles, varargin)

```
handles.output = hObject;

%% ENCENDIDO DE CAMARA
pause(1);
global vid
axes(handles.axes1)
vid = videoinput('winvideo', 1, 'MJPG_1280x720');
vidRes=get(vid,'VideoResolution');
nBands=get(vid,'NumberOfBands');
himage= image ( zeros(vidRes(2),vidRes(1),nBands
rectangle('Position',[520 170 300 390],'EdgeColor','r');
zoom(1.5)
preview(vid,himage);
axis off;
axes(handles.axes2)
axis off;
guidata(hObject, handles);
```

- function guardar_Callback(hObject, eventdata, handles)

```
% --- FUNCIÓN DEL BOTÓN "GUARDAR"
rgb = getimage(handles.axes2);
if isempty(rgb), return, end
% Guardar archivo
formatos = {'*.jpg','JPEG (*.jpg)'};
[nomb,ruta] = uiputfile(formatos,'GUARDAR IMAGEN');
if nomb==0, return, end
fName = fullfile(ruta,nomb);
imwrite(rgb,fName);
```

- function reset_Callback(hObject, eventdata, handles)

```
agregar_usuario;
```

- function capturar_Callback(hObject, eventdata, handles)

```
global vid
foto=getsnapshot(vid);
closepreview(vid);
recorte=imcrop(foto,[540 240 260 280]);
axes(handles.axes2)
imshow(recorte)
```

- function salir_Callback(hObject, eventdata, handles)

```
boton_salida = questdlg('Seguro que desea salir','salir','si','no','no')
if strcmp(boton_salida,'no')                    %si no desea  salir, continue
   return;
end
close all                                       % si desea salir cierre todo
```

ANEXO E

RESUMEN DE LAS FUNCIONES MÁS IMPORTANTES UTILIZADAS EN LA PROGRAMACIÓN DE MATLAB

SINTAXIS DEL COMANDO O FUNCIÓN	DESCRIPCIÓN
videoinput (adaptorname,deviceid,format)	Tiene tres argumentos, el primero referente al adaptador, el segundo al número de dispositivo conectado y el tercero referente al formato en el cual se tomará la imagen.
getsneapshot (obj)	Retorna una imagen instantánea desde el objeto de entrada especificado en *obj.*
medfilt2 (A)	Lleva a cabo el filtrado de mediana de la matriz *A* en dos dimensiones usando una matriz de *3x3* definida por defecto, en caso de no especificarse la dimensión de la matriz filtro.
imcrop (A, [xmin ymin width height])	Recorta la imagen *A* de acuerdo a las coordenadas especificadas, *xmin, ymin, width y height* corresponden a los vértices del rectángulo de recorte.
imresize(A, [numrows numcols])	Redimensiona la imagen o matriz *A* de acuerdo a los valores indicados en *numrows, numcols,* cambiando el tamaño de la imagen para que

	tenga el número especificado de filas y columnas preservando la relación de aspecto de la imagen.
numel (A)	Contabiliza el número de elementos dentro de la matriz *A*
mean (A)	Retorna el promedio de todos los valores que conforman la matriz *A*
princomp (A)	Lleva a cabo el análisis de componentes principales (PCA) en la matriz de datos *A* *n*-por-*p*, y devuelve los coeficientes de componentes principales
arrayfun (fun,A)	Aplica la función especificada por FUN a cada elemento de la matriz *A*
max (A)	Para los vectores, *max (A)* es el elemento más grande en *A*. Para matrices, *max (A)* es un vector fila que contiene el elemento máximo de cada columna.
sprintf (format, A, ...)	Aplica el formato a todos los elementos de la matriz *A, format* es un *string* que describe el formato para cada campo de salida.
image('PropertyName','PropertyValue',…)	Crea un objeto de imagen mediante la interpretación de cada elemento en la matriz, basándose en los datos especificados como el

	mapa de colores o directamente como valores RGB.
fullfile(foldername)	Almacena la ruta de cada uno de los archivos y carpetas existentes en *foldername* dentro de directorio.
dir('directory_name')	Enumera los archivos existentes en *directory_name*.
repmat(A,M,N)	Crea una gran matriz formada por copias de tamaño MxN de la matriz A.
histeq(image)	Mejora el contraste de las imágenes mediante la transformación de los valores en una imagen de intensidad, o los valores en el mapa de colores de una imagen indexada, por lo que el histograma de la imagen de salida coincide aproximadamente con un determinado histograma.
[Y, Fs]=audioread(filename)	Lee un archivo de audio especificado por *filename*, devolviendo los datos muestreados en Y y la frecuencia de muestreo Fs en Hertz.
sound(Y,Fs)	Envía la señal en el vector Y (con frecuencia de muestreo Fs hacia el altavoz de las plataformas

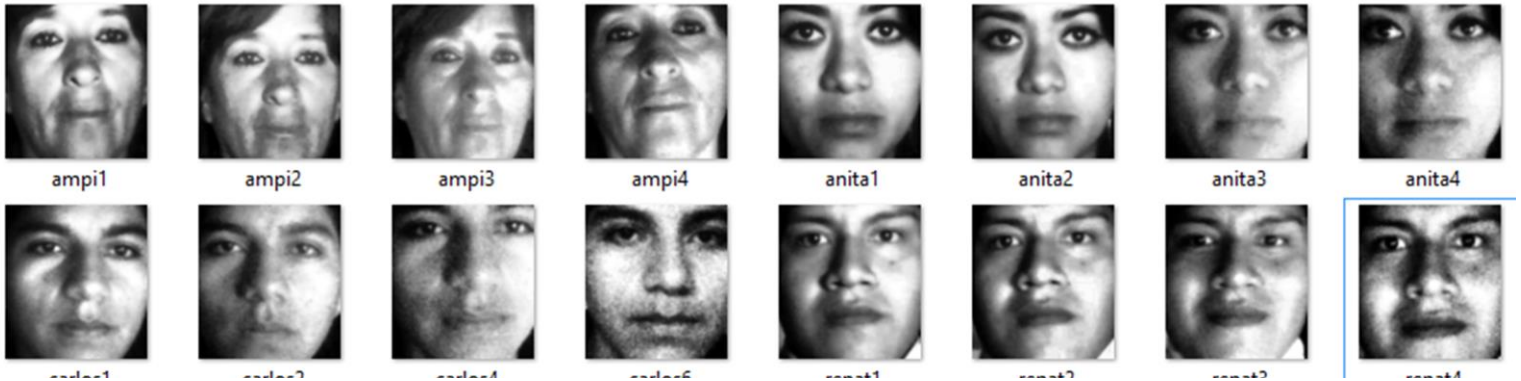
	compatibles para reproducir el sonido.
PROPIEDADES UTILIZADAS EN LA PROGRAMACIÓN	
PROPIEDAD	**DESCRIPCIÓN**
VideoResolution	Esta propiedad es un vector de dos elementos que indica el ancho y el alto de cada *frame* del video entrante. El ancho se mide en píxeles y el alto en filas.
NumberOfBands	Indica el número de bandas de color en los datos de entrada adquiridos

ANEXO F

BASES DE DATOS

FOTOGRAFÍAS DE LA BASE DE DATOS PARA EL DÍA

FOTOGRAFÍAS DE LA BASE DE DATOS PARA LA NOCHE



GLOSARIO DE TÉRMINOS Y ACRÓNIMOS

A/D	Análogo/Digital
ADN	Ácido desoxirribonucleico
CCTV	*Closed circuit televisión* - circuito cerrado de televisión
D/A	Digital/Análogo
DCT	*Discrete Cosine Transform* - Transformada Discreta de Coseno
DNI	Documento Nacional de Identidad
ECU	*Engine Control Unit* - Unidad de Control Electrónico
FFT	*Fast Fourier Transform* - Transformada Rápida de Fourier
GNU	*Gnu Not Unix* - No es Unix
GPS	*Global Positioning System* - Sistema de Posicionamiento Global
GSM	*Groupe Spécial Mobile* - Grupo Especial Móvil
GUI	*Graphical user interface* - Interfaz Gráfica de Usuario
GUIDE	*Graphical User Interfase Development Environment* - Interfase gráfica de usuario del entorno de desarrollo
HD	*High Definition* - Alta Definición
ICA	Análisis de Componentes Independientes
IDE	*Integrated Development Environment* - Entorno de Desarrollo Integrado
INTECO	Instituto Nacional de Tecnologías de la Comunicación
JPEG	*Joint Photographic Experts Group* - Grupo Conjunto de Expertos en Fotografía
LCD	*Liquid Crystal Display* - Pantalla de Cristal liquido

LDA	*Linear Discriminant Analysis* - Análisis Lineal Discriminante
LPP	*Locality Preserving Projections* - Preservar proyecciones locales
MatLab	*MATrix LABoratory* - Laboratorio de Matrices
OMSC	Observatorio Metropolitano de Seguridad Ciudadana
PCA	*Principal Component Analysis* - Análisis de Componentes Principales
PNG	*Portable Network Graphics* - Gráficos de Red Portátiles
ROI	*Return On Investment - Retorno de la Inversión*
TIFF	*Tagged Image File Format* - formato de archivo informático para imágenes.