VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

SISTEMA DE CONTROL DE ACCESO POR BIOMETRÍA

"BIOMETRIC ACCESS CONTROL SYSTEM"

Marquez Moreno Ingrid Julieth[1], Niño Garzón Michael Johanes[2], Luengas Contreras Lely Adriana[3]

Resumen: En el presente documento se describe un prototipo de un control de acceso para instalaciones que requieran autentificación de los individuos que ingresen y salgan de ella. El modelo se compone de tres partes: reconocimiento de huella dactilar y facial, una base de datos y una interfaz gráfica web. El protocolo de autentificación debe validar reconocimiento de huella dactilar y facial, ambas deben de ser positivas para tener un resultado verdadero y permitir el acceso, los datos que se validan han sido previamente registrados. Por medio de la interfaz gráfica web el usuario puede conocer el tiempo que lleva dentro la instalación, hora de ingreso. El prototipo se implementó en una Raspberry pi 3.

Palabras clave: Autentificación positiva y negativa, huella dactilar, reconocimiento facial.

Abstract: In the present document a prototype of an access control is described for installations that require authentication of the individuals entering and leaving it. The model consists of three parts: fingerprint and facial recognition, a database and a web graphical interface. The authentication protocol must validate fingerprint and facial recognition, both must be positive to have a true result and allow access, the data that is validated have been previously recorded. Through the web graphical interface the user can know the time it takes inside the installation, time of entry. The prototype was implemented in a Raspberry pi 3.

Keywords: Positive and negative identification, fingerprint, facial recognition.

[1] Estudiante Tecnología en Electrónica (Ciclos Propedéuticos). Universidad Distrital Francisco José de Caldas – Facultad Tecnológica. Email: ijmarquezm@correo.udistrital.edu.co
[2] Estudiante Tecnología en Electrónica (Ciclos Propedéuticos). Universidad Distrital Francisco José de Caldas – Facultad Tecnológica. Email: mjniñog@correo.udistrital.edu.co
[3] Ingeniera Electrónica, Magister en ingeniería eléctrica, Esp. En pedagogía y docencia universitaria, Universidad Distrital Francisco José de Caldas – Facultad Tecnológica. E-mail:

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

1. INTRODUCCIÓN

Existen situaciones donde es indispensable reconocer con certeza la identidad del usuario para poder acceder a un servicio o sitio, y es imposible realizar una investigación profunda sobre la veracidad de la identidad. Los sistemas de control de acceso cuentan con un protocolo de seguridad en la entrada y salida del usuario, los sistemas más tradicionalistas involucran el ingreso de una contraseña, tarjeta de identificación o código de barras, estos suelen presentar fallas por suplantación. Un sistema acceso debe ser único e intransferible algo que con los métodos anteriores no se logra en un cien por ciento.

Se implementó un sistema de acceso por biométrica, donde se sensan dos características físicas únicas que cada persona posee, la huella dactilar y las características faciales, estas dos peculiaridades en conjunto funcionan como reconocimiento y autentificación para tener acceso (entrada y salida) a un servicio o sitio en específico.

El presente documento muestra la metodología empleada para realizar el diseño del sistema descrito. En el apartado dos está el estado del arte, en el tres el marco teórico. En el apartado cuatro el desarrollo del proyecto. En el quinto lugar los resultados. En el sexto y último lugar las conclusiones.

2. ESTADO DEL ARTE

Alrededor del mundo y en Colombia se han realizado diferentes proyectos donde utilizan un control de acceso biométrico, para distintas actividades o servicios. Para iniciar el proyecto propuesto se realizó el estado del arte del tema encontrando algunos documentos que se citan a continuación.

BIOMETRIC ACCESS CONTROL FOR DIGITAL MEDIA STREAMS IN HOME NETWORKS. En este documento se puede ver el extenso campo de aplicaciones que puede tener un control de acceso biométrico y reconocimiento facial, con una retransmisión inalámbrica para contenido de IP-TV, donde los usuarios son agregados por un usuario maestro y este logra identificar los miembros que ese encuentra sentados en el sofá [1].

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

USING A BIOMETRIC SYSTEM TO CONTROL ACCESS AND EXIT OF VEHICLES AT TSHWANE UNIVERSITY OF TECHNOLOGY. Las huellas dactilares también funcionan como reconocimiento y autentificación para la entrada de un establecimiento, en este documento implementaron el reconocimiento de huella dactilar para entrar al campus de una universidad, la huella es escaneada, cifrada y luego enviada a una base de datos de huellas dactilares para su almacenamiento, la hora y fecha del automovilista que ingresa también se registran junto con la huella dactilar [2].

USING A BIOMETRIC SYSTEM TO CONTROL ACCESS AND EXIT OF VEHICLES AT SHOPPING MALLS IN SOUTH AFRICA. En este caso usan la huella dactilar como un comprobante de pago, donde la persona que se encontraba dentro del centro comercial ha pagado exitosamente su factura del parqueadero, y puede sacar del establecimiento su carro, sin necesidad de mostrar factura alguna, solo con escanear su dedo el sistema le informa a la persona encargada de la salida que este ha realizado su pago [3].

RECONOCIMIENTO DE IMÁGENES FACIALES ORIENTADO A CONTROLES DE ACCESO Y SISTEMAS DE SEGURIDAD. Se implementó un sistema de reconocimiento facial al interior de una plataforma de desarrollo embebida llamada Raspberry Pi, proporcionando una solución portable, con costo reducido y la posibilidad de actualizaciones del sistema de reconocimiento sencillas, sin la necesidad de modificar el hardware del dispositivo [4].

SISTEMA DE AUTENTICACIÓN FACIAL MEDIANTE LA IMPLEMENTACIÓN DEL ALGORITMO PCA MODIFICADO EN SISTEMAS EMBEBIDOS CON ARQUITECTURA ARM. La idea principal de este proyecto fue implementar un sistema de acceso por medio de reconocimiento facial implementado en un hardware de arquitectura abierta [5].

El proyecto realizado adjunta dos métodos de reconocimiento biométrico: huella dactilar y facial, para validar el ingreso y salida de una instalación, implementado en una plataforma embebida. Esto crea una diferencia con respecto a los proyectos anteriormente mencionados que solo implementan un método de reconocimiento biométrico.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

3. MARCO TEÓRICO

3.1 Sistemas biométricos

Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas o biometría estáticas como lo son la geometría de la mano, la huella dactilar, la forma facial, el iris, la retina, el patrón vascular de la manos y dedos, etc. Y por otro lado están las características del comportamiento precisas o biometría dinámica como lo son el reconocimiento de la voz, firma, la dinámica del tecleo, cadencia del paso y conducta gestual. Las características biométricas son inherentes a la persona, es decir, están unidas inseparablemente a cada persona.

La ventaja de los sistemas biométricos esta por una parte en la comodidad del usuario, estas características siempre están con la persona sin la posibilidad de olvidar o perder. También en el aumento de la seguridad, estas no se pueden trasmitir de forma deliberada [6].

Un sistema de reconocimiento biométrico se basa en 3 procesos:

1. Inscripción: Sistema de adquisición que se encarga de proporcionar la señal biométrica que caracteriza al individuo. Tras la adquisición de la señal biométrica se procede a la extracción de las características del rasgo biométrico del individuo, dichas características se expresan de una forma univoca y compacta la identidad del individuo
2. Base de datos: El patrón biométrico extraído por el módulo de inscripción es almacenado en la base de datos del sistema de reconocimiento.
3. Reconocimiento: Se encarga de establecer la identidad del individuo que accede al sistema, para ello, tras la adquisición del rasgo biométrico del individuo, se extraen las características y se obtiene el patrón biométrico que, posteriormente, es comparado con los patrones almacenados en la base de datos. Los resultados de dichas comparaciones son cuantificados y valorados, permitiendo así la toma de decisiones respecto a la identidad del individuo en función del grado de similitud obtenido [7].

3.2 La huella dactilar

La huella dactilar es un rasgo particular de cada individuo, cuyo origen tiene lugar durante la etapa fetal y permanece inmutable a lo largo de toda la vida. La huella dactilar permite, además, discriminar perfectamente a los diferentes individuos y su grado de aceptabilidad es relativamente alto [7].

Las huellas dactilares son la reproducción de la epidermis de la parte posterior de los dedos de la mano. Una huella dactilar está formada por un conjunto de líneas que se denominan crestas (líneas oscuras) y valles (líneas claras), como se muestra en la figura 1. Este conjunto de líneas que forman las huellas dactilares pueden asemejarse a patrones o texturas que se pueden analizar de diferentes maneras dependiendo del grado de detalle [8].

Figura 1. Características de la huella dactilar [9].

3.2.1 Procesamiento de huellas dactilares

El procesamiento de reconocimiento de huellas tiene diferentes etapas:

Adquisición: En esta etapa se toma una muestra de la huella dactilar de un sujeto.

Pre-procesado: La imagen obtenida en la etapa de adquisición se trata en función de las necesidades de los algoritmos de extracción y comparación que se vayan a utilizar. **Extracción de características**: Se extrae la información relevante de las huellas para su posterior comparación.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

Comparación: Se comparan las características extraídas para determinar si las dos muestras pertenecen al mismo individuo. Existen algoritmos que no necesitan extracción de características y por tanto realizan directamente la comparación [8].

3.3 Características faciales (cara)

La cara es el rasgo biométrico más utilizado por la mayoría de las personas para reconocer a un individuo. Aunque es un rasgo cuya característica de unicidad es menos que la de la huella dactilar o el iris, su gran aceptabilidad y universalidad han contribuido a la investigación y desarrollo.

3.3.1 Técnicas de reconocimiento

Estas técnicas abarcan, tanto las aplicaciones en las que el reconocimiento se realiza a partir de imágenes de la cara estáticas, donde las condiciones de adquisición puede ser controladas, como las aplicaciones en las que el reconocimiento se realiza a partir de imágenes en movimiento, donde la cara es extraída de la escena, y donde las condiciones de adquisición no son controladas.

Las condiciones de variabilidad del proceso de adquisición, que aparecen en el reconocimiento facial de imágenes estáticas, son: el fondo de la imagen, la distancia individuo- cámara, la expresión facial, el gesto, el habla, la aparición de artefactos naturales (barba, bigote, etc.) y artificiales (maquillaje, gafas, etc.), la iluminación, la edad, etc. En general, el reconocimiento de cara con estas imágenes es más eficiente que el reconocimiento con imágenes en movimiento.

En un contexto más amplio, el reconocimiento de cara involucra dos etapas:

La detección y localización de la cara: La detección de cara se basa en el establecimiento previo de un modelo de la misma. Durante el proceso de detección se comparan diferentes zonas de la imagen con dicho modelo de cara. El grado de similitud obtenido tras la comparación determina la existencia o no existencia de la cara en la imagen.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

Extracción de características y reconocimiento del individuo: Se extraen las características de las caras obtenidas en la etapa anterior, y se procede a la identificación del individuo que se desea reconocer [7].

3.4 OpenCV

OpenCV (Open Source Computer Vision) es una biblioteca de funciones de programación dirigida principalmente a la visión por ordenador en tiempo real. Esta biblioteca es una multiplataforma gratuita para su uso bajo la licencia *BSD* de código abierto [10]. Para algoritmos de detección y reconocimiento fácil se usa esta librería.

3.5 Raspberry pi 3

Consiste de un computador de placa reducida, capaz de correr distintos tipos de sistemas operativos incluyendo sistemas operativos embebidos; ofrece herramientas de gran utilidad para este tipo de proyectos, figura 2. El software es Open Source, siendo su sistema operativo oficial una versión adaptada de Debian, denominada Raspbian. [11].

3.5.1 Cámara de la Raspberry Pi 3

La placa de cámara Raspberry Pi de alta definición (HD) de 8 megapíxeles se conecta a cualquier Raspberry Pi o Compute Module para crear fotografías y vídeo HD. Utiliza el sensor de imagen IMX219PQ de Sony que ofrece imágenes de vídeo de alta velocidad y alta sensibilidad, figura 3. Dispone también de funciones de control automático como el control de exposición, el balance de blancos y la detección de luminancia [12].

Figura 2. Raspberry Pi 3 [12]

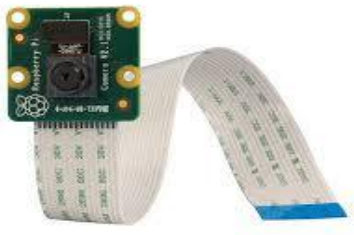

Figura 3.Cámara de la Raspberry Pi 3 [12]

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

4. DESARROLLO DEL PROYECTO

4.1 Descripción

El proyecto que se describirá a continuación, realiza una autentificación dactilar y facial de un individuo, el cual tiene que efectuar un registro previo donde se guarda su información correspondiente y realizar la carga de datos en el sistema, para que el usuario pueda realizar su validación en el sistema. Al ejecutar una validación positiva y el usuario ingresa a la instalación se guardaran los datos de ingreso (hora y fecha) en una base de datos, estos se podrán visualizar en una interfaz gráfica web, sino es así y el usuario sale de la instalación los datos de ingreso anteriormente guardados se borraran. Por medio de comandos auditivos y visuales se le informa al usuario que función debe ejecutar según el proceso seleccionado.

En la figura 4 se observa el diagrama de bloques desarrollado para la elaboración del control de acceso por biometría. El control cuenta con 4 bloques fundamentales: Autentificación de huella dactilar, Autentificación facial, bloque de control, interfaz gráfica web, serán descritos a continuación.

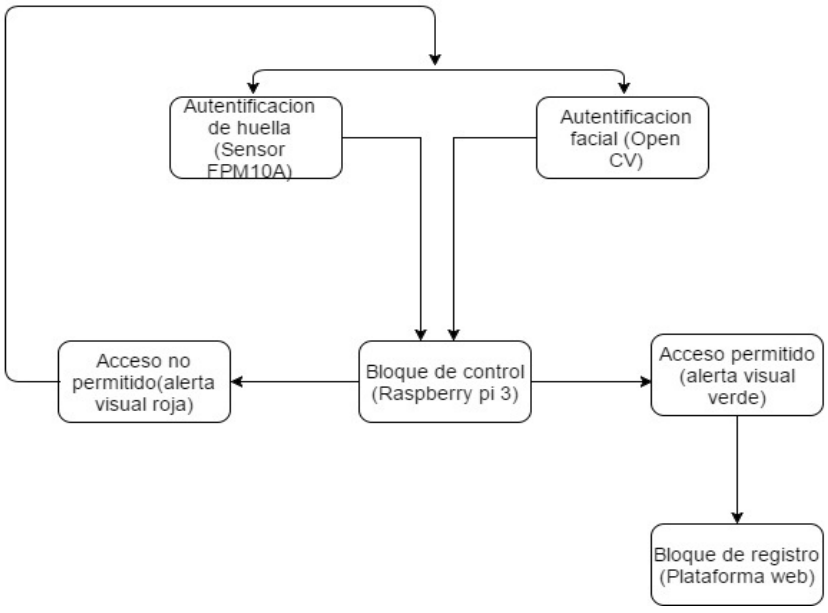

Figura 4. Diagrama de bloques

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

4.1.1 Autentificación de huella

La autentificación de huella está compuesta por el módulo FPM10A, figura 5,que incluye un sensor de huella dactilar óptico, un chip DSP, y una Uart de comunicación serial. Este también cuenta con dos buffers en los cuales se pueden leer y escribir, por medio de instrucciones, la información de estos buffers no se almacenan después de que el modulo se apaga. Se escogió este módulo por su facilidad de conexión con cualquier micro controlador o sistema con TTL en serie, y su disponibilidad de adquirir en el mercado local.

Figura 5.Módulo FPM10A [13]

Se utilizó la librería “pyfingerprint” para Python, la cual permite la conexión, transmisión y recepción de los datos. El módulo FPM10A se comunica por el protocolo de comunicación RS232, maneja por defecto una velocidad de 57600 bps, con un formato de trama de 10 bits, un bit de inicio, datos de 8 bits y un bit de parada, sin paridad. La Raspberry pi 3 solo le da instrucciones al módulo, y el modulo respuestas a la Raspberry, por medio de paquetes hexadecimales, el cual tiene el siguiente formato:

Tabla 1.Formato del paquete de datos

Encabezado	Dirección	Identificador de paquete	Longitud del paquete	Contenido del paquete (instrucción/dato/parámetro)	Chequeo de suma

Para inicializar el modulo primero se le debe de enviar la instrucción de verificación de contraseña (por defecto = 0x00000000), si esta es correcto, este nos permitiría seguir ejecutando las tareas que necesitemos. Para registrar la huella, primero se lee la huella del

individuo, se le extraen la características y se guardan en el buffer 1 del módulo, se hace la verificación que esta no se encuentre registrada, si es así se procede otra vez a leer la huella del individuo, se extraen la características y se guardan en el buffer 2. Se comparan los resultados de los dos buffers, si estos son iguales, se procede a guardar la plantilla de la huella, en la memoria flash del módulo y retornar el número de serie con la que quedo almacenada (posición). Para la autentificación de la huella se realiza el mismo procedimiento anterior, con la diferencia que solo se toma una sola muestra de la huella, donde sus características se guardaran en el buffer 1, y estas se comparan con las que se encuentran guardadas en el módulo, dando un resultado positivo o negativo. En la eliminación de la huella solo se debe de ingresar la posición en donde quedo guardada la huella, el modulo retornara un dato booleano, si el numero ingresado corresponde a una posición (numero) valida.

4.1.2 Autentificación facial

Está compuesto por la implementación de OpenCV, una herramienta de adquisición y tratamiento de imágenes, esta librería consta básicamente de tres tipos de algoritmos: Eigenfaces, Fisherfaces y local Bynary Pattrerns Histograms). Se implementó el algoritmo de eigenfaces, el cual está basado en la técnica de análisis de componentes principales (PCA o ACP) la cual busca principalmente reducir la dimensionalidad de un grupo de datos buscando destacar y utilizar como punto de comparación las características no compartidas y que representan la mayor variación en un grupo de datos. Eigenfaces usa un gran conjunto de imágenes digitalizadas de rostros humano, tomados con condiciones de iluminación similares y las alinea a la altura de los ojos y boca, entonces son redimensionados a la misma resolución, y a partir de la aplicación de PCA se pueden extraer los suficientes datos de la imagen eigenfaces resultante, figura 6, que sirvan como punto de comparación contra nuevos grupos de datos o imágenes.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

Figura 6. Ejemplo de aplicación de eigenfaces[11]

Se utilizó una base de datos la cual permite generar una imagen eigenfaces de características negativas para su comparación, figura 7. En este caso se ha tomado la base de datos de rostros de AT & T desarrollada en Abril de 1992.

Figura 7. Imagen eigenfaces negativa

Se realizo en Python 2 a través de varios scripts que desarrollan tareas específicas, estos se invocan en un script central llamado Global.py, las necesidades de la autentificación facial son: 1. captura y almacenamiento de nuevos rostros 2. Comparación y autentificación de rostros.

El sistema se doto con una cámara de la Raspberry pi, la cual permite ofrecer mejor calidad en la imagen tomada.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

1. Captura y almacenamiento de nuevos rostros: Se integra en un script llamado Capturepositives.py que consiste en capturar y recortar las imágenes, de tal manera que sean imágenes en escala de grises que permitan una óptima creación de una imagen eigenfaces. Primero se inicializa la cámara, creando un objeto camera dentro del script, donde toma una foto, la cual posteriormente es convertida a escala de grises y verifica que la imagen obtenida pertenezca a la de un rostro humano, de lo contrario repite el proceso hasta obtener la de un rostro humano.

```
camera = config.get_camera()
image = camera.read()
image = cv2.cvtColor(image, cv2.COLOR_RGB2GRAY)
result = face.detect_single(image)
```

Recorta la imagen a una medida que depende del 'result'

```
x, y, w, h = result
```

y la guarda en un directorio previamente establecido. Este proceso se repite 4 veces para cada sujeto que se registre en el sistema.

2. Comparación y autentificación de rostros: Se debe crear una nueva imagen eigenfaces de características positivas a partir de las fotos capturadas en el proceso anterior (script capturepositives.py) para que permita una comparación con los datos de las nuevas imágenes entrantes, se ejecuta el script train.py, que se basa en leer todas las imágenes guardadas como positivas y las imágenes guardadas como negativas, generando un nuevo archivo eigenfaces positivo y lo guarda en un directorio específico.

Una vez se tiene el nuevo archivo eigenfaces de características positivas se dispone a solucionar la comparación de rostros, realiza la toma de una nueva foto, la convierte a escalas de grises, verifica que sea un rostro humano, y realiza la comparación de los datos obtenidos contra los del modelo, si estos se encuentran por debajo de 3500, que es el tresh hold, un valor de confiabilidad previamente establecido, el rostro es conocido como positivo.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

4.1.3 Bloque de control

La Raspberry pi 3, se encarga de hacer el control de 4 tareas: registro, autentificación, eliminación y actualización de datos del usuario, enviándole las funciones correspondientes a los bloques de autentificación de huella dactilar y facial. El usuario interactúa con el bloque de control por medio de una LCD que visualiza el menú inicial y el paso a paso a seguir en cada bloque, también recibe indicaciones por medio de comandos de voz, un teclado, que le permite ingresar los datos correspondientes para poder acceder a cada tarea y una alerta de iluminación (verde= positiva y roja=negativa) según el acceso que se obtenga.

En la figura 8 se puede apreciar el diagrama de flujo, que se tuvo en cuenta en la implementación del código en la Raspberry Pi 3.

1. El registro se encarga de guardar la huella en el módulo FPM10A, las 4 diferentes muestras del rostro (fotografías) del usuario, la posición en la que quedo guardada la correspondiente huella en el módulo, el ingreso del usuario y clave, las dos últimas para poder acceder a la interfaz gráfica de la página web, exceptuando la huella y los rostros, los demás datos se guardan en MySQL, donde se puede modificar y obtener los datos desde Python o PHP.
2. La autentificación compara las huellas y rostros, con las que ya se han registrado posteriormente, si la comparación es positiva para ambos bloques, tendrá un acceso permitido, sino es así será un acceso negativo.
3. La eliminación se encarga de eliminar la huella, usuario y clave que fueron proporcionados en el registro.
4. La actualización de datos, básicamente esta función es para el administrador y aplicable para el reconocimiento facial, al realizar un registro de una nueva persona, los datos guardados (fotos) deben ser actualizados para la creación de una nueva imagen eigenfaces positiva, más o menos está tarda de 5 – 10 minutos, este tiempo depende del total de personas que se encuentren registradas.

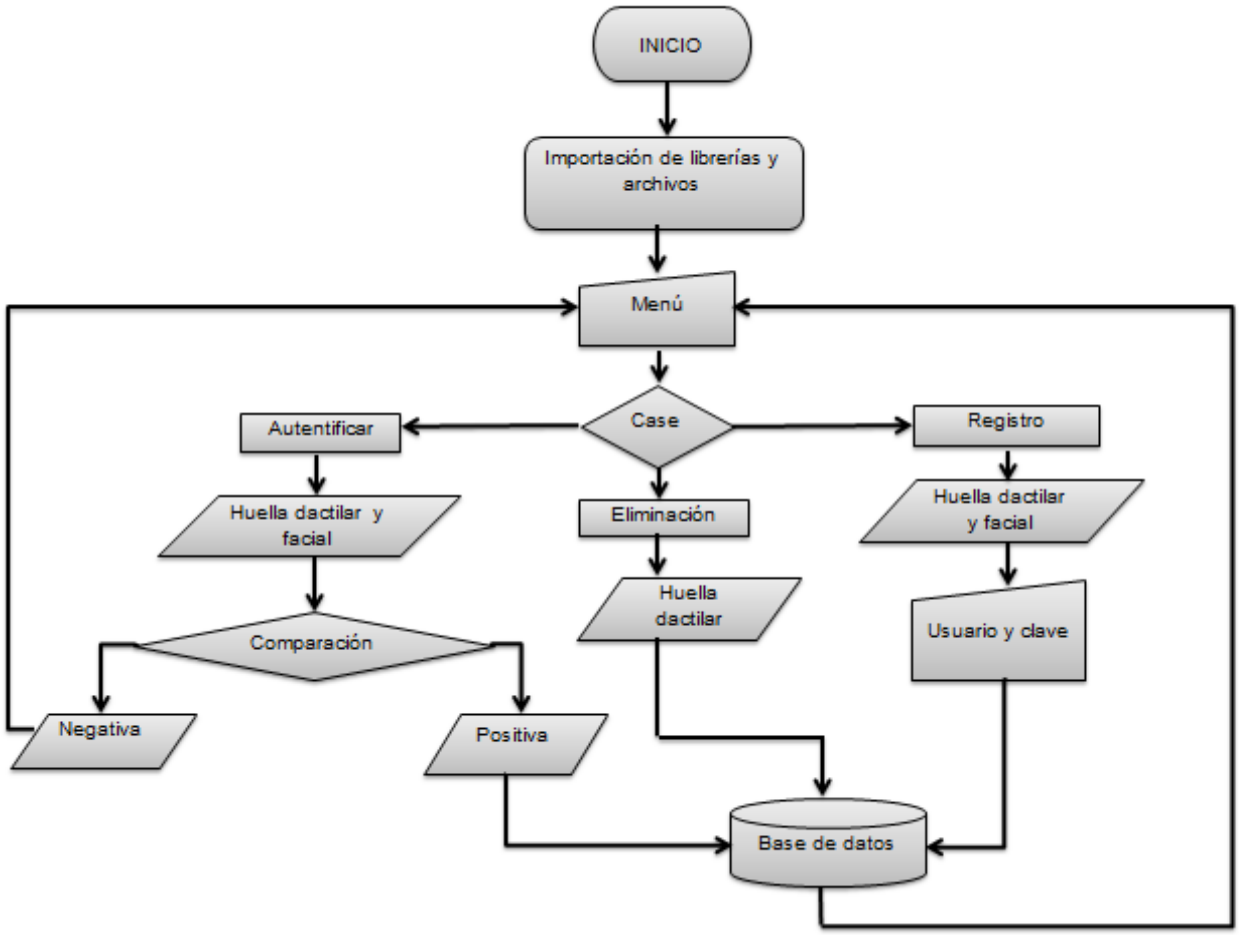

Figura 8. Diagrama de flujo del bloque de control

4.1.4 Interfaz gráfica web

Se creó una plataforma de aplicaciones LAMP (***L****inux****A****pache****M****ySQL****P****HP*), se incluyen 3 software Open Source. EL servidor web HTTP, se crea por medio del programa Apache, este crea un servidor con la dirección IP de la *Raspberry PI 3* y permitirá subir los datos a Internet de una forma segura y confiable, y a través de PhpmyAdmin se puede administrar la base de datos MySQL a través de la interfaz web, PHP. La página web se desarrolló con HTML, PHP, JavaScript, y CSS, en la figura 9, se puede observar la página principal.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

Figura 9. Página principal

Esta permite ingresar un usuario y clave, si son correctas y el usuario se encuentra dentro del sistema lo redirige a una secunda página, figura 10.

Figura 10.Página Secundaria

Esta muestra la fecha y hora del ingreso al sistema, y el tiempo que lleva en esta, sino es así, le informara por una alerta visual del porque no puede ser re direccionado, en la figura 11 se encuentra el diagrama de flujo del funcionamiento de la interfaz gráfica web.

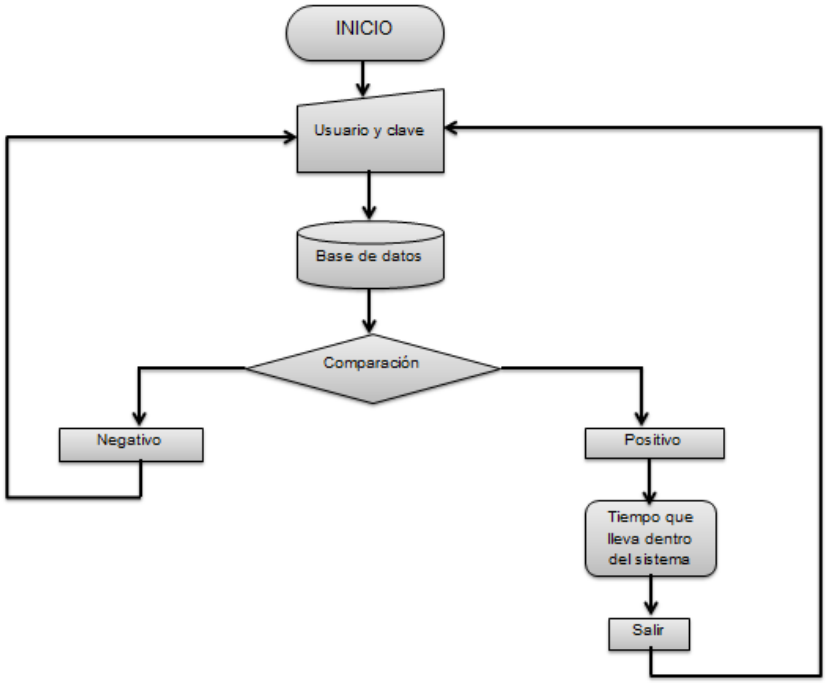

Figura 11. Diagrama de flujo de la interfaz gráfica web

4.2 Prototipo final

El prototipo final cuenta con dos partes, la de control y una cabina para tener un entorno estable de luminosidad.

4.2.1 Parte de control

La parte de control cuenta con una Raspberry pi 3, la cámara de la Raspberry pi, el módulo FPM10A, una LCD de 20*4, los cuales están incorporados en una caja, un teclado y un bafle que se encontraran en el exterior. Como se puede observar en la figura 12.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

Figura 12.Prototipo final

4.2.2 Cabina

Se realizó una cabina con dimensiones de 70 * 70 cm de ancho y 180 cm de alto, la cual se encuentra cubierta por un plástico negro, donde su propósito es impedir el traspaso de la luz exterior hacia el interior, figura 13. Esta se encuentra iluminada con una cinta led blanca, que está distribuida en los cuatro lados de la parte superior. Y cuenta con una base en el eje 'y' donde se encontrara la parte de control, esta base es movible en el eje 'y' para comodidad del usuario dependiendo de su estatura, figura 14.

Figura 13. Cabina parte externa

Figura 14. Cabina parte interna

5. PRUEBAS Y RESULTADOS

Las pruebas realizadas se dividen en cinco partes, funcionamiento del FPM10A, acceso a MySQL desde python y PHP, autentificación facial en entornos sin luminosidad constante, autentificación facial con luminosidad constante y las realizadas con el prototipo final.

5.1 Funcionamiento del FPM10A

Se realizaron pruebas con diferentes individuos, los cuales realizaron el proceso de guardar su huella en el módulo y luego autentificarse, se observaron varios factores externos, que influyeron en el reconocimiento de la huella por el módulo, uno fue el tamaño del dedo, el módulo posee dificultad de reconocimiento cuando esta es muy ancha, lo cual logra sobresalir por la ventana de detección de la imagen del módulo, este problema se obtiene cuando se quiere autentificar con el dedo pulgar, lo más aconsejable es realizar la autentificación con los dedos índice o corazón, ya que permite una posición más cómoda al usuario al momento de acercar el dedo al módulo y se puede realizar un detección del 100%. También la posición del dedo, este tiene que cubrir toda la ventana de detección de la imagen del módulo y tienen que estar derecho, si el dedo esta ladeado o no cubre toda la superficie, el modulo no lograr hacer ningún reconocimiento, el dedo debe de estar limpio y seco, ya que si este no se encuentra asi, el sensor no podrá leer bien la imagen del dedo o simplemente obtendrá una imagen diferente a la huella original.

El módulo tiene un tiempo de respuesta de cerca de 5 segundos, en la que se demora tomando la imagen, realizar las debidos procesos, y enviado la información pertinente a la Raspberry Pi 3, este tiempo no se ve afectado si el modulo se encuentra saturado o no, el modulo tiene una capacidad para guardar 100 huellas, cada huella la guarda en diferentes posiciones comenzando desde la posición más cercana al cero que se encuentre desocupada.

5.2 Acceso a MySQL desde Python y PHP

Se realizaron diferentes pruebas de acceso a MySQL desde Python, modificando, insertando y eliminando datos de las tablas que se encuentran en la base de datos, comprobando los

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

resultados desde la terminal, donde se puede abrir MySQL y observar las modificaciones en cada tabla. Desde PHP, se le realizaron la misma prueba que en Python, en ambas pruebas se obtuvieron resultados positivos y con un tiempo de respuesta muy bajo, lo cual no retrasa la ejecución de todo el programa. Cabe descartar que la página web solo se puede visualizar y ejecutar desde la red local en la cual se encuentra la Raspberry conectada.

5.3 Autentificación facial en entornos sin luminosidad constante

Se realizaron varias pruebas en un entorno de luminosidad variable en el tiempo, estas pruebas fueron ejecutadas en un cuarto que contaba con una ventana grande por donde entraba una gran iluminación natural y tenía también iluminación artificial, el primer paso que se realizó, el individuo debió registrarse, las fotos que se obtuvieron de este paso se guardan, para luego generar una nueva imagen eigenfaces positiva.

Validando la autentificación facial a distintas horas del día con el mismo individuo, se obtuvieron principalmente resultados negativos. Esto se debe a las condiciones de luz de la habitación que están cambiando, se observaron tres acciones dos de ella que incidían constantemente:

1. Se consiguieron resultados positivos, esto se mantuvieron en un trascurso de tiempo de más o menos 1 hora después del registro realizado, donde las condiciones de luz eran semejantes al del previo registró.

2. Se obtuvieron resultados negativos, este lograba detectar el rostro, pero al momento de examinar la comparación, esta daba negativa, ya que esta imagen pudo ser más oscura o iluminada, que las que se tomaron en el previo registro.

3. No se detectaron rostros, no toma ninguna muestra (fotografía), el lugar en donde se estaban realizando las pruebas la luz artificial era muy débil e insuficiente para que el rostro de la persona o el sitio se encontraran bien iluminados, también se pudo provocar por el mal posicionamiento de la cámara, esta debe ir más o menos a la altura de los ojos de la persona.

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

5.4 Autentificación facial en entornos con luminosidad constante

Se realizaron pruebas en un entorno con una luminosidad constante, en este caso se trabajó con la cabina mencionada anteriormente, se realizaron los mismos pasos, primero el registro y después la autentificación. Se obtuvieron resultados positivos en la mayoría de los casos, con autentificación positiva. Las acciones que más incidieron en el trascurso de la prueba fueron dos:

1. Autentificación positiva, después del registro, se procedió hacer varias autentificaciones en distintas horas del día, y diferentes días, sin modificar el registro inicial, y se obtuvieron autentificaciones positivas.

2. No se detectaron rostros, este problema en esta ocasión se seguía debiendo al mal posicionamiento de la cámara con respecto a la persona, el cual es más fácil de resolver en el momento.

5.5 Prototipo final

Observando las pruebas anteriores, cabe destacar que para un buen funcionamiento del proyecto, este debe encontrarse en condiciones de luz constantes. Ya mencionado anteriormente se realizó una cabina para mantener estas condiciones de luz estables, para que no hubiera problemas en la autentificación facial. Para arreglar el problema del posicionamiento de la cámara, o que el usuario no se encuentre en la posición adecuada, se agregaron comandos de voz, para dar información al usuario de lo que debe hacer y lo que está sucediendo en cada proceso. En el prototipo final se encuentran todos los procesos funcionando en uno solo. En esta prueba se realizaron el registro de 3 personas diferentes, en lo cual cada uno debía de registrarse y luego autentificarse. Para el registro primero se guarda la huella dactilar del individuo, luego de esto se procede a tomar las debidas fotografías, y por ultimo un registro de usuario y clave que la persona proporcionada ella misma por medio de un teclado. Al registrarse los 3 individuos, se pasó a la actualización de datos. Después se procedió a que cada uno se autentificara, con la misma rutina primero la huella dactilar y después la facial. De esta prueba cabe recalcar 2 acciones:

VISIÓN ELECTRÓNICA
16/04/2017
Fecha de recepción:
Fecha de aceptación:

1. Se pudo observar que algunas personas no situaron bien la cámara para que tomara las fotos, por medio de los comandos de voz se le informo a la persona que no se estaban capturando fotos, y podían arreglar esta situación, para completar el proceso.

2. En todas las pruebas se obtuvieron resultados positivos, tanto en la autentificación dactilar, facial y en la interfaz gráfica web, donde cada uno de ellos pudo ingresar con su usuario y clave, donde les mostraba su hora de ingreso y el tiempo transcurrido.

Se pudo comprar el registro de las personas que se encuentran en el sistema, en la figura 15 se observa la tabla de registro esta se obtuvo de MySQL, la base de datos que es utilizo, la cual se visualizó por medio de la consola de la raspberry, la figura 16 se visualizan la tabla de las personas que se encuentran dentro del sistema pero desde la interfaz gráfica web, en la cual esta solo la puede ver el administrador.

```
21 rows in set (0.00 sec)

mysql> select Posicion,Usuario,Clave, Bandera from login2;
+----------+-----------+-------------+---------+
| Posicion | Usuario   | Clave       | Bandera |
+----------+-----------+-------------+---------+
|        0 | michael   | 1234        | si      |
|        1 | Ingrid    | 2017        | No      |
|        2 | Aleja     | Aleja       | No      |
|        3 | cristian  | 987         | si      |
|        4 | paola     | 20141573015 | si      |
|        5 | Fabian    | 1995        | si      |
|        6 | esneyder  | 2895        | No      |
|        7 | manuel    | 1478        | No      |
|        8 | kevin     | vimek       | No      |
|        9 | esmeralda | flor        | si      |
|       10 | antonio   | 2017        | si      |
|       11 | luz       | marina      | No      |
|       12 | andrea    | nea         | No      |
|       13 | jhony     | mora        | No      |
|       14 | cart      | cart        | No      |
|       15 | karol     | asdf        | No      |
|       16 | yerson    | usagui      | No      |
|       17 | alejo     | qwer        | No      |
|       18 | samuel    | samuel      | No      |
|       19 | fernada   | mafe        | No      |
|       20 | David     | udfjc       | No      |
+----------+-----------+-------------+---------+
21 rows in set (0.00 sec)

mysql>
```

Figura 15. MySQL

Posicion	Usuario	Estado	Hora	Fecha
0	michael	Adentro de la instalacion	20:5:45	2017-11-7
1	Ingrid	Afuera de la instalacion		
2	Aleja	Afuera de la instalacion		
3	cristian	Adentro de la instalacion	21:10:52	2017-11-9
4	paola	Adentro de la instalacion	21:15:5	2017-11-9
5	Fabian	Adentro de la instalacion	21:18:25	2017-11-9
6	esneyder	Afuera de la instalacion		
7	manuel	Afuera de la instalacion		
8	kevin	Afuera de la instalacion		
9	esmeralda	Adentro de la instalacion	20:40:5	2017-11-9
10	antonio	Adentro de la instalacion	20:48:48	2017-11-9
11	luz	Afuera de la instalacion		
12	andrea	Afuera de la instalacion		
13	jhony	Afuera de la instalacion		
14	cart	Afuera de la instalacion		
15	karol	Afuera de la instalacion		
16	yerson	Afuera de la instalacion		
17	alejo	Afuera de la instalacion		
18	samuel	Afuera de la instalacion		
19	fernada	Afuera de la instalacion		
20	David	Afuera de la instalacion		

Figura 16.Pagina del administrador

En pruebas más generales se realizaron autentificaciones con personas que se encontraban registradas y con las que no, cuando una persona que no ha sido registrada en el sistema trata de autentificarse este le suministra un error visual, figura 17, en la figura 18 se puede distinguir cuando una persona que está registrada accede al sistema.

Figura 17. Acceso denegado

Figura 18. Acceso positivo

También se ejecutaron pruebas con la interfaz gráfica web, accediendo a esta con datos erróneos, figura 19. Para lograr acceder a la plataforma el usuario debe encontrarse dentro de la instalación, sino es así se muestra una aviso del por el cual no puede acceder a esta, figura 20.

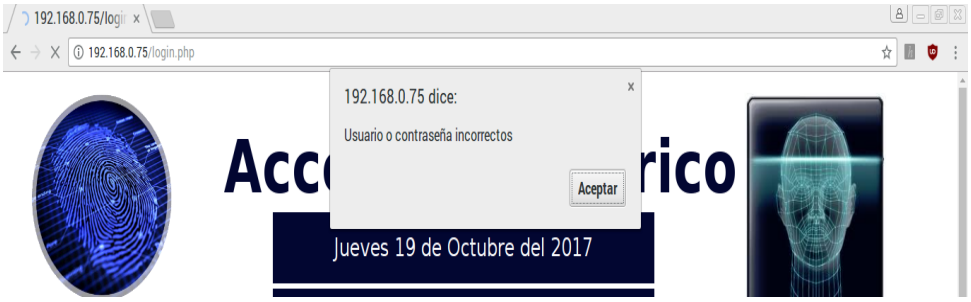

Figura 19. Usuario y contraseña erróneos

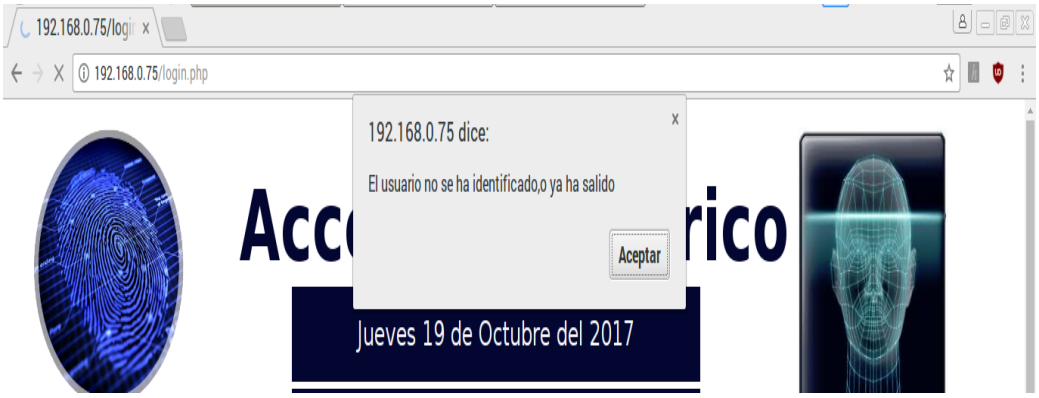

Figura 20. Usuario fuera de la instalación

6. CONCLUSIONES

Después de finalizada la construcción y realizadas las pruebas necesarias al prototipo de acceso biométrico, se puede concluir que:

- Para un correcto funcionamiento del prototipo este debe instalarse en un ambiente estable o controlable de iluminación, para que no haya problemas en la autentificación facial.
- Implementado otro tipo de código para el reconocimiento facial, se puede lograr obtener una autentificación facial para rostros artificiales (gafas, gorros) y no solo rostros naturales, como se efectúa en el proyecto.
- El proceso de registro y reconocimiento de huella dactilar se ve altamente afectado por las dimensiones que posea el sensor encargado de dicha tarea, tanto así que las huellas que superen las dimensiones del sensor presentan problemas para su registro y reconocimiento.
- Es de vital importancia tener una conexión constante y segura a internet que permita hacer la subida de la base de datos a la interfaz gráfica web; de lo contrario el prototipo generara errores en este proceso.

- Durante el desarrollo del proyecto se pudo concluir que al extraer desde el sensor la imagen digital de la huella y vectorizarla, podría llegarse a comunicar dos sensores FPM10A que compartan una base de datos de registro de huellas.
- Según los resultados obtenidos, se puede decir que el proyecto cuenta con un 98% de confiabilidad en la autentificación de los usuarios, pero un poco demorado para él usuario que no puede completar exitosamente el proceso de registro y autentificación a la primera vez, esto se ve afecto por situaciones externa, principalmente por el mal posicionamiento de la huella y el estado de esta (si está sucia o humedad).

Perspectivas y sugerencias

Para el mejoramiento futuro del prototipo de acceso por biometría se podría implementar diferentes sensores, donde se logren controlar la luz y el ambiente de luminosidad, obtener la altura del individuo para controlar la posición de la cámara y así lograr un funcionamiento eficiente de la autentificación. Adicionalmente poder comunicar más de dos sensores biométricos para tener una mayor cantidad de espacio de almacenamiento y cobertura incluso extraer la huella del módulo y guardarla en una base de datos externa.

REFERENCIAS

[1] P. Corcoran, C. Iancu, F. Callaly, and A. Cucos, “Biometric Access Control for Digital Media Streams in Home Networks,” *Consumer Electronics, IEEE Transactions on*, 2007.

[2] R. T. Hans, “Using a biometric system to control access and exit of vehicles at Tshwane University of Techonology,” *2014 4th International Conference on Engineering Technology and Technopreneuship, ICE2T 2014*, 2015. [Online]. Available: http://ieeexplore.ieee.org.bdigital.udistrital.edu.co:8080/document/6914180/?part=1.

[3] R. T. Hans, “Using a biometric system to control access and exit of vehicles at shopping malls in South Africa,” *2014 4th International Conference on Engineering Technology and Technopreneuship, ICE2T 2014*, 2015. [Online]. Available: http://ieeexplore.ieee.org.bdigital.udistrital.edu.co:8080/document/7006236/?part=1.

[4] D. C. P. PLAZAS, “RECONOCIMIENTO DE IMÁGENES FACIALES ORIENTADO A CONTROLES DE ACCESO Y SISTEMAS DE SEGURIDAD.,” 2015. [Online]. Available: http://repository.udistrital.edu.co/bitstream/11349/2230/1/PlateroPlazasDonovanCamilo2015.pdf.

[5] J. C. P. O. Andres Ernestos Lopez Sandoval, Cyntia Menndoza Martines, Luis Angel Reyes Cruz, Edgar Alejandro Rivas Ariza, Juan Manuel Ramos Arreguien, “Sistema de Autenticación Facial mediante la Implementación del algoritmo PCA modificado en Sistemas embebidos con arquitectura ARM,” *La Mecatronica Mex.*, vol. 4, no. 2, pp. 53–64, 2015.

[6] M. K. Karl-Heinz Dietsche, *Manual de la tecnica del automovil*, Cuarta edi. Germany: Robert Bosch GmbH, 2005.

[7] D. Simón Zorita, “Reconocimiento Automático Mediante Patrones Biométricos de Huella Dactilar,” *Tesis Doctoral*, 2003. [Online]. Available: http://oa.upm.es/79/1/09200327.pdf?iframe=true&width=80%25&height=80%25.

[8] A. Lindoso Muñoz, “Contribución al reconocimiento de huellas dactilares mediante técnicas de correlación y arquitecturas hardware para el aumento de prestaciones,” 2009. [Online]. Available: http://e-archivo.uc3m.es/handle/10016/5571.

[9] Daniel, “Fime - ITS,” *Presentacion inicial*, 2012. [Online]. Available: http://danimtzc.blogspot.com.co/2012/08/presentacion-inicial_14.html.

[10] P. K. anatoly;Kornyakov K. Victor., “Realtime Computer Vision with OpenCV,” *Queve*, pp. 40–56.

[11] RS Components, “Raspberry Pi 3 Model B: Technical Specifications,” p. 2, 2015.

[12] “PCCOMPONENTES,” Raspberry pi 3 – camara. [Online] Available: https://www.pccomponentes.com/raspberry-pi-camara-v2

[13] “ELECTRONILAB,” *Sensor Biometrico Huella digital -FPM10A*. [Online]. Available: https://electronilab.co/tienda/sensor-biometrico-lector-huella-digital-fpm10a/.