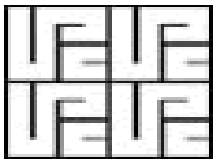
SISTEMA DE SEGURIDAD BIOMÉTRICO BASADO EN EL ANÁLISIS DE LA GEOMETRÍA DE LA MANO.

IVÁN MAURICIO ZULETA SÁNCHEZ

ERIK HELVER ZORRO JIMÉNEZ

Ing. Ana María Cagua Jiménez



UNIVERSIDAD PILOTO DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ

2015

SISTEMA DE SEGURIDAD BIOMÉTRICO BASADO EN EL ANÁLISIS DE LA GEOMETRÍA DE LA MANO.

PRESENTADO POR:

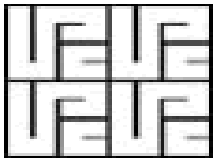
IVÁN MAURICIO ZULETA SÁNCHEZ

ERIK HELVER ZORRO JIMÉNEZ

Proyecto de grado, como requisito para optar al título de Ingeniero de Telecomunicaciones.

Docente:

Ing. Ana María Cagua Jiménez



UNIVERSIDAD PILOTO DE COLOMBIA

FACULTAD DE INGENIERÍA

PROGRAMA DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ

2015

DEDICATORIAS

En primer lugar dedicamos este trabajo de grado a Dios, pues Él es quién nos brinda la sabiduría, paciencia, salud y demás virtudes para seguir adelante cada día con nuestros trabajos, familia y todas las actividades desarrolladas a nivel personal.

Dedicamos también este proyecto de grado a cada uno de los miembros de nuestra familia, pues ellos en todo momento nos han brindado el apoyo económico y moral que requerimos para alcanzar nuestros objetivos como estudiantes y como profesionales, ya que sin ellos esto no se hubiera logrado, puesto que en todo momento nos proporcionaron el apoyo, mantuvieron la paciencia y nos sirvieron de aliento para alcanzar el desarrollo académico y que a su vez nos ha permitido llegar a esta instancia final, para alcanzar este logro tan grande a nivel personal y profesional.

AGRADECIMIENTOS

Agradecemos la contribución que ha tenido para el desarrollo de este proyecto de grado al Ingeniero Nelson Forero, quién fue nuestra mano derecha y guía inicial para la presentación de esta idea como opción de grado, ya que él fue quien nos ayudó a mejorar la idea planteada inicialmente y nos facilitó herramientas para el desarrollo de la misma; a la Ingeniera Ana María Cagua, por la dedicación, apoyo y compromiso con nosotros para el desarrollo de este documento, ya que sin ella no se habría logrado obtener eficientemente la estructura adecuada para hacer entender de manera clara y concisa lo que se expone en el contenido de este documento de proyecto de grado.

Agradecemos también a la Universidad Piloto de Colombia y al Programa Ingeniería de Telecomunicaciones, por brindarnos los conocimientos durante toda nuestra etapa de aprendizaje, por el apoyo, compromiso y enseñanzas de cada uno de los docentes del programa, ya que gracias a ellos se adquirieron las bases que se requieren para alcanzar este tan anhelado título profesional.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

1. PLANTEAMIENTO DEL PROBLEMA

En la actualidad existe una gran variedad de sistemas biométricos que ofrecen mayor seguridad para acceder a un recurso o servicio. Una opción viable que garantice el acceso exclusivo a un recurso o servicio es mediante el reconocimiento biométrico, el cual se basa en la identificación automática de un individuo basado en sus características físicas o de comportamiento, hoy en día contamos con equipos capaces de detectar a las personas a través de las manos, los ojos, las huellas dactilares, la voz, o la firma, entre otros.

Actualmente se presenta el inconveniente de que el sistema de ingreso a las instalaciones del plantel, así como a los recursos y servicios que presta la Universidad Piloto de Colombia, son demasiados vulnerables, pues no se tiene un control seguro del personal tanto administrativo como estudiantil que accede a los mismos, por lo tanto se propone utilizar un sistema de seguridad biométrico, el cual debe ser altamente seguro, con el fin de impedir la suplantación del personal o el ingreso no autorizado de personas ajenas al plantel.

2. JUSTIFICACIÓN

La seguridad biométrica es uno de los sistemas de acceso más utilizados hoy en día para el acceso a un servicio. Actualmente existen varios sistemas biométricos, la huella dactilar es uno de ellos. Sus mayores problemas radican en su dificultad para la identificación de personas mayores o trabajadores manuales. Por otro lado, los sistemas biométricos de iris presentan grandes índices de precisión y habilidad; sin embargo, los dispositivos para la captura del iris son demasiado costosos.

De este modo, un sistema biométrico basado en imágenes de la mano se convierte en una buena alternativa, obteniendo un equilibrado balance entre rendimiento y facilidad de uso. Otra de las ventajas de la geometría de la mano es la facilidad con la que pueden extraerse las principales características (medidas de longitud y amplitud y líneas principales) mediante imágenes de muy baja resolución (de ahí que los dispositivos de captura puedan resultar mucho más económicos).

Así mismo, la superficie de una impresión palmar es mayor y contiene más información que la de una huella dactilar; por lo tanto nos permite resolver el problema del bajo rendimiento, mayores costos y eficiencia que otros sistemas biométricos ofrecen.

De acuerdo a lo anterior, se quiere proponer la implementación de un sistema biométrico basado en el análisis de la geometría de la mano, el cual debe ser altamente seguro, para impedir la suplantación del personal o el ingreso no autorizado de personas ajenas al plantel.

El dispositivo biométrico que se pretende utilizar, debe contar con las características básicas que un sistema biométrico requiere para que sea óptimo, es decir, que posea un buen desempeño, aceptabilidad y fiabilidad, lo cual apuntaría a la obtención de un sistema biométrico con utilidad práctica.

3. OBJETIVOS

3.1 Objetivo General

Diseñar y validar un modelo de prototipo para un sistema de seguridad biométrico basado en el análisis de la geometría de la mano, con el propósito de contribuir en la seguridad y mejora de los procesos de ingreso y salida de instalaciones y la correcta identificación de los usuarios.

3.2 Objetivos Específicos

- ✓ Establecer el hardware y software que hará parte del sistema biométrico.
- ✓ Seleccionar e implementar el algoritmo para el sistema de reconocimiento de patrones de la geometría de la mano.
- ✓ Implementar la base de datos que permita almacenar y validar la información de los usuarios para una correcta identificación.
- ✓ Realizar una prueba piloto que permita validar el sistema de seguridad biométrico.

4. MARCO REFERENCIAL

Hoy en día sabemos que la seguridad es parte integral de nuestras vidas, es ahí donde el hombre ha venido trabajando con diferentes proyectos que aseguren nuestra vida personal y demás cosas que suelen ser importantes y requieren una protección mayor a la que por naturaleza se brinda. Por ello se denotan diferentes sistemas de control y de acceso para determinar una seguridad más confiable que puede ser por control de acceso físico, llaves electrónicas de contacto, sistemas biométricos y otros sistemas que apuntan hacia nuevas tecnologías de alta seguridad.

Sabiendo esto existe una tecnología de mayor fidelidad y de acceso intransferible de la persona como lo es la seguridad biométrica, el concepto de biometría proviene de la palabra bio (vida) y metria (medida), por lo tanto con ello se infiere que toda seguridad biométrica mide e identifica alguna característica propia de la persona[1]. Por consiguiente este tipo de tecnología de seguridad biométrica se basa en identificar y verificar aquellas características fisiológicas para validar a la persona que hace uso de ésta por medio de la coincidencia respecto a un almacenamiento de información previamente de patrones únicos, que lo que harán es independizar el proceso de autenticación al sistema de muchos a uno.

En la seguridad biométrica podemos encontrar diferentes formas de identificación biométrica como lo son huellas dactilares, iris, manos, reconocimiento facial, entre otros, los cuales son nuestra propia firma y/o identificación frente al acceso de un lugar o sistema que lo requiera. Como modelo de proceso de identificación personal hay ciertas características básicas que un sistema biométrico para identificación personal debe cumplir según la facultad de ingeniería biométrica informática de la Universidad Autónoma de México (UNAM), en su módulo de bases teóricas y sistemas biométricos *"Un sistema biométrico es un método automático de identificación y verificación de un individuo utilizando características físicas y de comportamiento precisas. Las características básicas que un sistema biométrico para identificación personal debe cumplir son: desempeño, aceptabilidad y fiabilidad. Las cuales apuntan a la obtención de un sistema biométrico con utilidad práctica".*[2]

Este tipo de seguridad se está implementando alrededor del mundo en entornos de entidades bancarias, industriales, agencias de gobierno, centro de cuidado infantil, fuerzas militares y otras.

Entre las formas de identificación biométrica la que se selecciono es la geometría de las manos, esta ha aumentado su popularidad debido a que *"Las texturas de las líneas principales, arrugas y surcos de las impresiones palmares, contienen información diferenciadora que puede ser extraída para*

[1] http://www.homini.com/new_page_5.htm
[2] http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicassistema.html

fines de verificación."[3] Por ejemplo en Japón, las personas pueden retirar dinero de los cajeros automáticos utilizando escáneres de impresiones palmares[4]y en las bibliotecas japonesas utilizan escáneres de impresiones palmares para consignar la salida de libros.[5] En el 2006, la policía del Reino Unido creó una base de datos de impresiones palmares.[6] La policía canadiense también está buscando crear tal base de datos.[7]

Es importante aclarar que hay varios sistemas biométricos que han sido infringidos por la ingeniería social, lo cual es un tema que se está tratando con urgencia y recientemente se ha demostrado que las técnicas biométricas convencionales, tales como huellas dactilares y rostro son vulnerables a recibir ataques. Estos ataques son realizados con el fin de falsificar el rasgo biométrico y de esta manera engañar al sistema. Por ejemplo, se tiene el caso de crear un dedo artificial con superficie gomosa el cual puede copiar fácilmente la huella humana y así romper la seguridad del sistema. Es un tema que en Europa es preocupante, ya que la mayoría de sus sistemas de acceso son por seguridad biométrica, se espera que el proyecto con el nombre de Tabula Rasa busque mitigar este tipo de brechas.[8]

4.1 MARCO HISTÓRICO

4.1.1 La biometría. La biometría es una ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento, esta característica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina o el iris, sin embargo los rasgos del comportamiento son menos estables, pues dependen de la disposición psicológica de la persona, por ejemplo en la firma.

Durante miles de años hemos empleado para identificarnos unos de otros, características de nuestro cuerpo tales como cara, voz, etc. Sin embargo no es hasta mediados del siglo XIX que se pone en práctica la idea de emplear diversas medidas del cuerpo humano (por ejemplo peso, estatura, longitud de

[3] Michael KO Goh, Tee Connie, et al, Multimedia University, Malaysia. "A Fast Palm Print Verification System," International Conference on Computer Graphics, Imaging andVisualisation, 2006, disponible en http://www.computer.org/portal/web/csdl/doi/10.1109/CGIV.2006.7

[4] Kenji Hall, "Biometrics: Vein Scanners Show Promise," BusinessWeek.com, 6 de febrero de 2007 http://www.businessweek.com/globalbiz/content/feb2007/gb20070206_099354.

[5]Martyn Williams, "Japanese Library to Use Palm-Vein for Book Check-Out," IDG News Service, 26 de diciembre de 2005, disponibleenhttp://www.infoworld.com/d/security-central/japanese-library-use-palm-ve...

[6] Andy McCue, "Police Get National Biometric Palm Print Database," Silicon.com, 23 de marzo de 2006 http://www.techweekeurope.co.uk/

[7] "Winnipeg Police Angling for Palm-Print Software," CBC News, 15 de enero de 2007 disponible en http://www.cbc.ca/news/canada/manitoba/story/2007/01/15/palm-print.html

[8] http://www.tabularasa-euproject.org/

los brazos, manos y pies), para la identificación de personas, naciendo formalmente lo que hoy conocemos como Biometría.[9]

4.1.2 Procesamiento de imagen. El procesamiento de imágenes es un conjunto de técnicas o mecanismos utilizados, los cuales se aplican a las imágenes digitales con el propósito de mejorar la calidad de las mismas.

Teniendo en cuenta la definición anterior, se puede evidenciar que a diferencia de los mecanismos que tiene el ser humano para captar visualmente algo, el procesamiento y captación de imágenes digitales requiere de recursos o mecanismo tecnológicos, que permitan la manipulación de la información y las características que cada una contiene. Por lo tanto, es necesario conocer que la secuencia básica para el tratamiento de imágenes digitales consta de los siguientes pasos:

- **I.** Captura de la imagen a partir de procesos físicos mediante el uso de un sensor adecuado.
- **II.** Reconstrucción para reducir ruidos y mejorar la calidad.
- **III.** Codificación, segmentación y extracción de las características.
- **IV.** Descripción y/o ilustración.

El análisis del ser humano cuando capta visualmente imágenes u objetos despliega problemas, pues el proceso de reconocimiento visual se efectúa en una gran cantidad de tiempo y está sujeto a interpretaciones incoherentes y/o incompletas. El procesamiento de imágenes que se realiza mediante máquinas inteligentes, resuelve estos problemas al poder automatizar el proceso de extracción de información útil de la imagen. Con el procesamiento de imágenes, también se puede optimizar la imagen y corregir distorsiones.

[9] http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2440/iba%C3%B1ezorozco.pdf? sequence=1

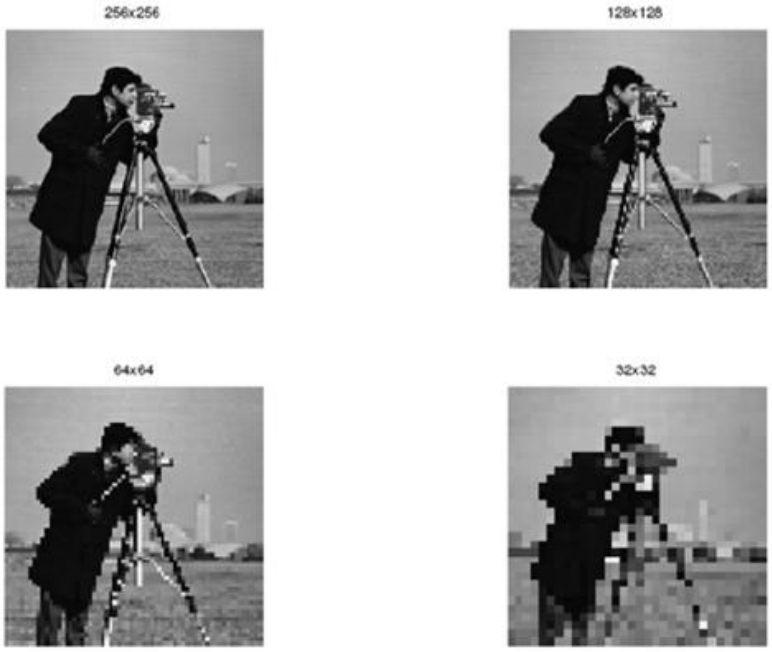


Figura 1. Imagen tomada con diferentes resoluciones.[10]

La cuantificación de la señal es el número finito de los valores de intensidad de cada píxel. Se suele emplear un byte de cuantificación por píxel, consiguiendo así 256 niveles de gris. El 0 corresponde al color negro y el 255 al blanco. Entre estos dos valores están los distintos tonos de gris. Para las imágenes en color, la cuantificación es vectorial; por cada píxel se representan tres valores. Estos tres valores dependen del sistema de representación del color: RGB (Red Green Blue) o HSV (Hue, Saturation, Value). Comúnmente se utiliza RGB con un byte por cada color consiguiendo 256 niveles o 16 millones de colores.

La profundidad de píxel es una unidad de medida binaria, cada píxel está formado por bits. Cuando decimos que la profundidad de píxel es 1, la imagen solamente tiene dos colores o dos niveles de gris. Una profundidad de píxel de 8 permite que cada pixel pueda tener 256 colores distintos o 256 niveles distintos de grises, si la profundidad de píxel es de 24 podemos llegar a 16 millones de colores distintos en cada píxel.

El número de bits por pixel determinará la gama de colores de una imagen, según lo expresado en la *Figura 2*.

[10] http://www.iit.upcomillas.es/pfc/resumenes/4aae971695c34.pdf [Pág. 27; Figura 2.8]

Figura 2. Numero de bits por pixel.[11]

Figura 3. Niveles de cuantificación de la señal de la intensidad luminosa.[12]

4.1.3 Imagen digital. Las imágenes digitales se obtienen a través de dispositivos de conversión analógico-digital como un escáner, una cámara fotográfica digital o directamente desde el ordenador utilizando cualquier programa de tratamiento de imágenes. La información digital que genera cualquiera de los medios citados es almacenada en el ordenador mediante bits (unos y ceros). Los ordenadores trabajan con información digital y con información numérica. En un ordenador la información analógica de textos, imágenes y sonidos se codifica por medio de bits.[13]

[11] http://www.ite.educacion.es/formacion/materiales/56/cd/tem0/hoja0002.htm
[12] http://www.iit.upcomillas.es/pfc/resumenes/4aae971695c34.pdf [Pág. 28; Figura 2.9]
[13] http://www.ite.educacion.es/formacion/materiales/86/cd/pdf/m2_caracteristicas_de_la_imagen_digital.pdf

4.1.4 Histograma de una imagen. El histograma de una imagen contiene la información de la probabilidad de aparición de las distintas tonalidades de color que se pueden dar en cada caso, ya que podemos trabajar en distintos tipos de colores o en escala de grises.[14]

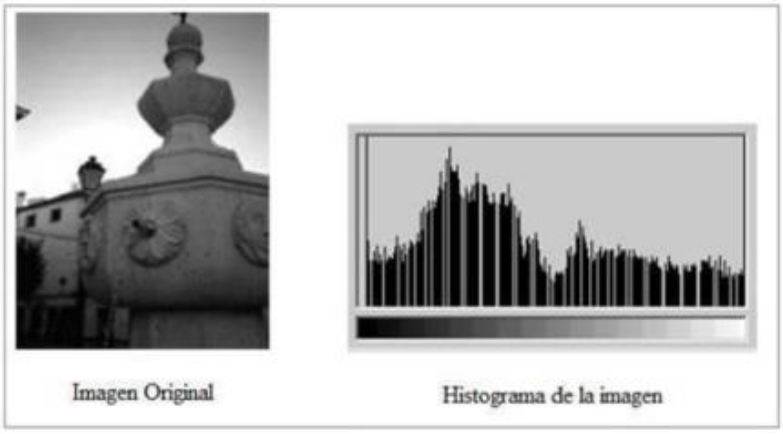


Figura 4. Imagen con su correspondiente histograma.[15]

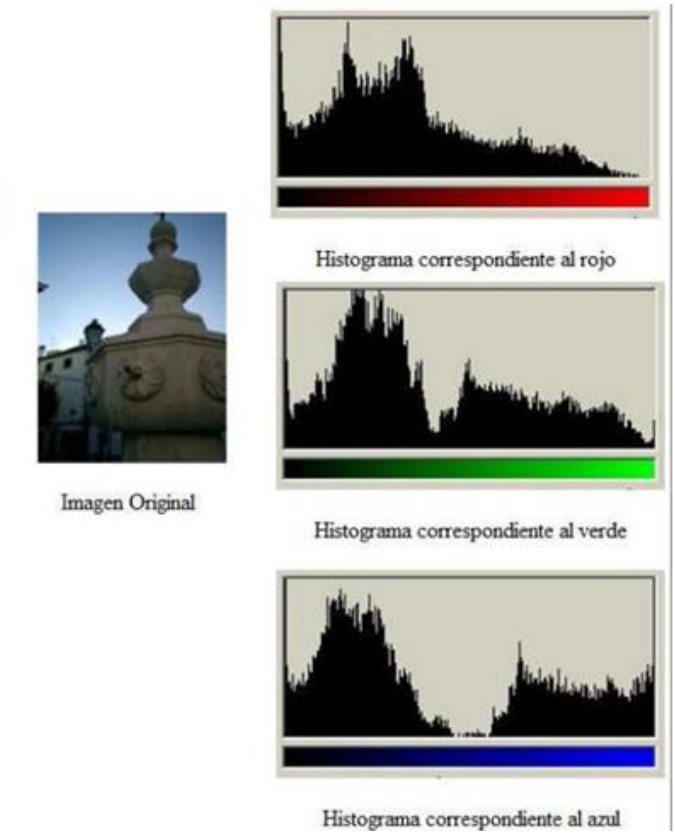


Figura 5. Imagen a color con sus respectivos histogramas RGB.[16]

[14]http://biblioteca.unet.edu.ve/db/alexandr/db/bcunet/edocs/TEUNET/2010/pregrado/Electronica/RubioB_FranklynJ/Capitulo2.pdf
[15]http://www.iit.upcomillas.es/pfc/resumenes/4aae971695c34.pdf [Pág. 32; Figura 2.10]
[16]http://www.iit.upcomillas.es/pfc/resumenes/4aae971695c34.pdf [Pág. 34; Figura 2.11]

En resumen, un histograma es un gráfico estadístico que permite representar la distribución de intensidad de los píxeles de una imagen, es decir, el número de píxeles que corresponde a cada intensidad luminosa. Por convención, el histograma representa el nivel de intensidad con coordenadas X que van desde lo más oscuro a lo más claro.

En general, se representa como un gráfico de barras en el que las abscisas son los distintos colores de la imagen y las ordenadas la frecuencia relativa con la que cada color aparece en la imagen. El histograma proporciona información sobre brillo y el contraste de la imagen, y puede ser utilizado para ajustar estos parámetros y eliminar ciertas tonalidades molestas.

4.1.5 La Webcam. Todo inicio en el área de informática de la Universidad de Cambridge a raíz de la necesidad en la que todos querían tomar café, pero la cafetera estaba en el sótano de un edificio. El dilema no era la cafetera, tampoco quien tenía que preparar más café, era quien vaciara la cafetera. Claro está que esta norma no se cumplía.

Figura 6. La cámara del café. La primer webcam de la historia.[17]

Entonces en el año 1991, Quentin Stafford-Fraser y Paul Jardetzky, diseñaron un sistema que podían conectar a una cámara y esta trasmitía una imagen de la cafetera. Así, desde la pantalla de su computadora, sabían cuándo había café y quién se lo terminaba. A este sistema se le llamó XCoffee, y después de unos meses decidieron venderlo. En 1992 salió a la venta la primera cámara web llamada XCam. La cámara que dio vida a la webcam que conocemos actualmente, fue apagada el 22 de agosto del año 2001.[18]

[17] http://www.anfrix.com/2007/05/la-camara-del-cafe-la-primer-webcam-de-la-historia/
[18] https://academiamoderna.files.wordpress.com/2014/10/l2-invencic3b3n-de-la-webcam.pdf

Figura 7. IP Webcam.[19]

El mercado actual y con el avance de la tecnología se ha llegado a crear la cámara IP en el año 1996. Con esta cámara se han logrado integrar soluciones de seguridad en diferentes entidades como lo son las industrias, laboratorios, bancos, aeropuertos y casinos, así como también se ha utilizado para aplicaciones profesionales basadas en seguridad y control remoto en tiempo real.

Básicamente por tres razones las cámaras web han tenido buen desempeño en el mercado de la tecnología: la versatilidad de las cámaras, el bajo costo de transmisión de imágenes y la alta calidad de las mismas.

4.2 MARCO CONCEPTUAL

4.2.1 Funcionamiento de un sistema biométrico. Gran parte de los sistemas biométricos ofrecen soluciones tecnológicas y funcionan basados en modelos seguros para el control de acceso e identificación de personas. Un sistema biométrico común puede funcionar de dos formas:

La primera tiene que ver con la verificación, que consiste en realizar una comparación entre un patrón biométrico capturado a través de un sistema de biometría y un patrón capturado instantáneamente, para luego verificar si un individuo es o no es, de acuerdo a las características tomadas como patrón de verificación en el sistema de verificación. Una segunda manera en que un sistema biométrico puede funcionar es mediante la identificación, es decir, mediante uno o más sistemas biométricos se realiza una comparación de los patrones almacenados en una o varias bases de datos para identificar a un individuo desconocido. Para que la identificación sea exitosa la comparación del patrón biométrico debe coincidir con los archivos almacenados dentro de la base de datos.

[19] http://www.ecrater.com/p/4079732/wireless-network-ip-webcam-security

Estos sistemas están compuestos por dos elementos, el primero captura la característica del individuo o indicador biométrico mediante dispositivos físicos. El segundo elemento está constituido por programas de computadora que interpretan dichos indicadores biométricos para garantizar o negar lo que el usuario requiera. En el caso de las huellas digitales, el individuo debe colocar su dedo en un sensor que hace una lectura matemática de su huella, después el software archivara la información como un modelo, luego cuando el usuario vuelva a acceder al sistema, volverá a repetir el procedimiento y el software determinará si la información coincide con el modelo. Este principio es el mismo para otros sistemas biométricos como los de identificación de iris o retina, la cara o la mano.[20]

La precisión de los sistemas biométricos esencialmente depende de dos cosas, lo primero tiene que ver con los cambios que cada individuo presente por accidentes o envejecimiento presentado en su fisiología, en segundo lugar, los factores externos al sistema utilizado también juegan un papel importante, por ejemplo cuando se quiere realizar una lectura de la mano o del dedo, la humedad, suciedad, el sudor o alteraciones presentadas en la piel que recubre estas partes del cuerpo, pueden alterar los resultados.

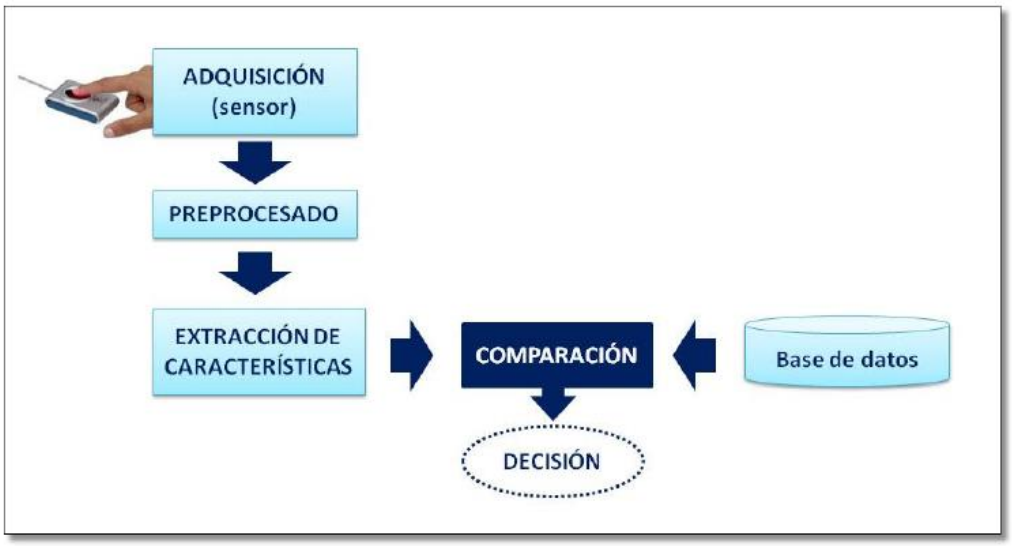


Figura 8. Funcionamiento básico de un sistema biométrico.[21]

4.2.2 Características de los sistemas biométricos. Las características en las que se basa un sistema de reconocimiento biométrico de personas son comúnmente conocidas como “rasgos biométricos”. Una posible clasificación de los rasgos biométricos es:

- **Rasgos fisiológicos:** presentan una reducida variabilidad a lo largo del tiempo pero su adquisición requiere de la cooperación de los usuarios y

[20] http://sistemasbiometria.blogia.com/2010/120301-como-funcionan-los-sistemas-biometricos.php
[21] http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20120309MariaMeridaAguilera.pdf. Capítulo 2.3. Sistemas Biométricos [Figura 2.2]

es más denso. El iris, la huella dactilar o la geometría de la mano pertenecen a este grupo.

- **Rasgos de comportamiento:** resultan menos densos pero experimentan una gran variabilidad (factores como el estado anímico, el cansancio o estrés de la persona pueden influir en la realización del rasgo biométrico) por lo que, en general, la exactitud de estos sistemas será menor. La voz, la escritura o la forma de andar son algunos ejemplos de este tipo de rasgos.

Además para que un sistema biométrico sea fiable, estos tendrán que cumplir con unos requisitos básicos, que lo que hacen es descartar o aprobar ciertas características como indicador biométrico:

I. **Universalidad:** lo tienen o lo poseen todas las personas.

II. **Unicidad:** es diferente para cada individuo, es decir, tiene la capacidad de discriminar entre una u otra persona.

III. **Permanencia:** no varía al transcurrir el tiempo.

IV. **Mensurabilidad:** puede ser capturado y medido fácilmente mediante un proceso de adquisición que no resulte denso para los usuarios.

V. **Rendimiento:** un sistema de reconocimiento cuenta con una baja tasa de error, alta velocidad y mínimo consumo de recursos.

VI. **Aceptabilidad:** cuenta con un alto grado de aceptación social.

VII. **Evitabilidad:** es difícil de vulnerar mediante algún procedimiento fraudulento, lo que indica que son sistemas demasiados seguros.

4.2.3 Clasificación de los sistemas biométricos. Los sistemas biométricos pueden ser clasificados de acuerdo al número de sus aplicaciones siendo estas dependientes de sus características. De acuerdo a esto, los sistemas biométricos pueden ser clasificados dentro de las siguientes categorías:

a) Cooperativa versus no-cooperativa. Se refiere al comportamiento del impostor en interacción con el sistema, es decir en un sistema de reconocimiento positivo es de gran interés del impostor el cooperar para ser aceptado como un usuario valido, sin embargo en un sistema de reconocimiento negativo el impostor no muestra ningún interés en cooperar con el sistema ya que él no desea ser reconocido.

b) No cubierto versus Cubierto. Si el usuario está enterado de que va a ser sometido a un reconocimiento biométrico, la operación es catalogada como no cubierta y caso contrario en donde el usuario desconoce la aplicación de esta se trata de una aplicación cubierta.

c) Habitual versus no habitual. Se refiere a la frecuencia en que el usuario se ve envuelto en una operación de reconocimiento biométrico, siendo esta una importante consideración al momento de diseñar un sistema biométrico debido a que la familiaridad de los usuarios hacia el sistema afecta la exactitud del reconocimiento.

d) Atendido versus no atendido. Situación referida al proceso de adquisición de datos biométricos en donde una aplicación es observada, guiada o supervisada por un humano. Más aun, una aplicación puede tener un registro atendido pero un reconocimiento no atendido.

e) Ambiente estándar versus no estándar. Referido a que el sistema está siendo operado en un ambiente controlado (temperatura, presión, condiciones de iluminación, etc.). Esta clasificación es también importante para el diseño del sistema, es decir un sensor biométrico más resistente va ser necesario para un ambiente no estándar.

f) Público versus privado. Referido a si los usuarios del sistema son clientes o empleados de la organización del sistema biométrico desplegado.

g) Abierto versus Cerrado. Situación presente cuando la plantilla biométrica del personal es usada para una sola aplicación o para múltiples aplicaciones.[22]

4.2.4 Sistemas biométricos actuales. Como se ha venido mencionando, en la actualidad existen mecanismos de seguridad y control basados en diferentes indicadores biométricos. A continuación se hace referencia a los sistemas de seguridad biométrica más usados y que ofrecen de manera confiable la identificación de personas, evitando la problemática antes mencionada y que actualmente está ganando aceptación a nivel mundial en todos los sectores.

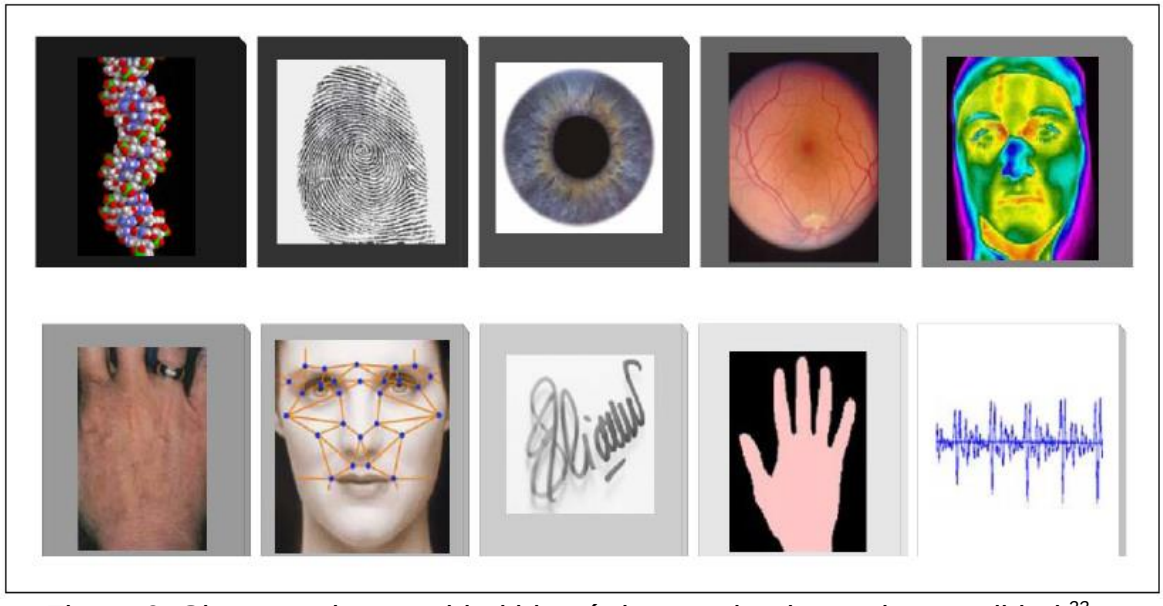


Figura 9. Sistemas de seguridad biométrica empleados en la actualidad.[23]

[22] http://132.248.9.195/ptd2008/noviembre/0636771/Index.html
[23] http://www.ptolomeo.unam.mx:8080/xmlui/handle/132.248.52.100/2440 [ibañezorozco.pdf; Pág. 9. Figura 2.1]

4.2.4.1 ADN: Es el último y único código unidimensional para un individuo. Solamente excepto para los gemelos idénticos que tienen patrones idénticos de ADN, sin embargo existen algunas limitaciones en la utilización de este identificador biométrico.

4.2.4.2 Cara: La cara es uno de los patrones biométricos más aceptables debido a que es uno de los métodos más comunes de reconocimiento para las personas usando su interacción visual. Sin embargo es muy difícil el desarrollar una técnica de reconocimiento facial que pueda tener tolerancia a efectos tales como el envejecimiento, expresiones faciales y variaciones en la posición de la cara con respecto a la cámara.

4.2.4.3 Termografía de la mano y del rostro: Los patrones de calor difundidos por el cuerpo humano son una característica del cuerpo de cada individuo y pueden ser capturados por una cámara infrarroja en un medio de no obstrucción, similar a una fotografía. Los sistemas basados en termografía son sin contacto y sin intrusión, pero sensibles a cambios en ambientes no controlados.

4.2.4.4 Geometría del dedo o la mano: Algunas características relacionadas con la mano de una persona, son relativamente particulares e invariantes en un individuo. La adquisición de la imagen requiere cooperación de la persona, ya que es necesario la captura frontal de imágenes y vistas del lado de la palma de la mano totalmente colocada sobre una superficie plana. Los requisitos para almacenar las variables o patrones tomados son muy bajos, lo que hace de este método algo muy atractivo ya que se requieren muy pocos recursos.

4.2.4.5 Iris: La textura visual del iris en un individuo es distinto para cada persona y para cada ojo. La imagen del iris es típicamente capturada mediante un sistema que no requiere el contacto y hacer esto involucra cooperación del usuario, siendo esta tecnología de reconocimiento extremadamente exacta y rápida.

4.2.4.6 Firma: La forma como una persona firma su nombre se sabe que es personal e individual, aunque el firmar requiera contacto y esfuerzo al momento de escribir, este identificador biométrico tiene una excelente aceptación en diversas transacciones legales y comerciales como método de verificación de identidad. Es un comportamiento biométrico que cambia con el paso del tiempo, ya que ésta puede variar por condiciones físicas y emocionales de cada persona.

4.2.4.7 Voz: Es un identificador biométrico aceptable en todo el mundo además de ser el único identificador biométrico que en sus aplicaciones requiere reconocimiento de la persona frente al sistema o dispositivo. No se espera que la voz sea suficientemente distintiva como para permitir la identificación de un individuo. generalmente la calidad se ve degradada en el uso de elementos externos como micrófonos, canales de comunicación y

características de digitalización, además la voz también puede verse afectada por el clima, estrés, emoción, etc., inclusive puede ser vulnerable por personas que tienen la capacidad de imitar a otras.

4.2.4.8 Huellas dactilares: Es el sistema biométrico más aceptado en todo el mundo, el cual posee características únicas de invariabilidad y unicidad.

4.2.5 Aplicaciones de los sistemas biométricos. Independientemente del sistema biométrico y la aplicación para la cual se desee adaptar, es necesario tener en cuenta algunos parámetros que nos permiten identificar y corroborar si el proceso utilizado dentro de los componentes del sistema biométrico cumple o no con lo que se espera al final de uso.

- **Registro:** La persona proporciona un documento de identificación para probar su identidad. Después la persona presenta una característica o patrón biométrico que se pueda parametrizar (por ejemplo, las yemas del dedo o de la mano) a un dispositivo de adquisición. Una o más muestras se adquieren, se codifican y se almacenan como registro de la referencia para las comparaciones futuras.

- **Verificación:** Se debe verificar que una persona es quien dice ser. Después de presentar un documento de identificación y una característica biométrica, el sistema captura los datos biométricos y genera un registro del patrón biométrico, el cual es comparado con el registro de la referencia de la persona (almacenado en el sistema durante la inscripción) para determinar si hay similitud entre los dos registros.

- **Identificación:** Se quiere identificar quién es la persona. En este caso no se presenta documento de identificación. El registro del patrón biométrico se compara contra los registros almacenados como referencia de todos los individuos listados en el sistema. Existen dos tipos de sistemas de identificación: positivo y negativo. En los positivos se determina si la persona que desea acceder está identificada en la lista del sistema. Los sistemas negativos son diseñados para asegurarse de que la información biométrica de una persona no está presente en la base de datos.

- **Falsa captura:** Una falsa comparación ocurre cuando el sistema acepta dos registros de diferentes usuarios incorrectamente como si fuese una sola identidad. Las capturas falsas pueden ocurrir cuando hay semejanzas entre las características o patrones biométricos tomados en cada uno de los individuos.

- **Falso rechazo:** Ocurre cuando un sistema rechaza una identidad válida. Ocurren porque no hay suficiente semejanza entre el registro de

inscripción y el registro del patrón biométrico tomado; esto se da a causa de envejecimiento o alguna lesión.

❖

4.3 MARCO TEÓRICO

4.3.1 Comparativo de los sistemas biométricos. No existe un sistema biométrico que sea mejor para todas las implementaciones. Se deben considerar muchos factores al momento de implementar un dispositivo biométrico, incluyendo la ubicación, los riesgos de seguridad, cantidad de usuarios establecidos, datos existentes, etc. Es también importante resaltar, que los sistemas biométricos están en distintas etapas de implementación y mejora continua con el paso del tiempo. Por ejemplo, el reconocimiento por huellas dactilares ha sido utilizado por más de un siglo, mientras que el reconocimiento por iris no tiene más de una década de utilización. Debe tenerse en cuenta también que la capacidad del dispositivo no está relacionada con cuál de ellos es el mejor, pero puede ser un indicador de las tecnologías que tienen mayor experiencia al momento de ejecutar la implementación.

			CARACTERÍSTICA						
			Universalidad	Unicidad	Permanencia	Mensurabilidad	Rendimiento	Aceptabilidad	Evitabilidad
RASGO BIOMÉTRICO	Fisiológico	Cara	ALTO	BAJO	MEDIO	ALTO	BAJO	ALTO	ALTO
		Geometría de la Mano	MEDIO	MEDIO	MEDIO	ALTO	MEDIO	MEDIO	MEDIO
		Huella Dactilar	MEDIO	ALTO	ALTO	MEDIO	ALTO	MEDIO	MEDIO
		Iris	ALTO	ALTO	ALTO	MEDIO	ALTO	BAJO	BAJO
		Oreja	MEDIO	MEDIO	ALTO	MEDIO	MEDIO	ALTO	MEDIO
	De Comportamiento	Dinámica del Tecleo	BAJO	BAJO	BAJO	MEDIO	BAJO	MEDIO	MEDIO
		Firma	BAJO	BAJO	BAJO	ALTO	BAJO	ALTO	ALTO
		Forma de Andar	MEDIO	BAJO	BAJO	ALTO	BAJO	ALTO	MEDIO
		Voz	MEDIO	BAJO	BAJO	MEDIO	BAJO	ALTO	ALTO

ALTO
MEDIO
BAJO

Tabla 1. Tabla comparativa de los sistemas biométricos. [24]

La Tabla 1 nos muestra la comparativa de los sistemas biométricos más usados en la actualidad, por tal razón se ha decidido utilizar el sistema de seguridad biométrico basado en la geometría de la mano, dado que éste sistema ofrece una mejor tasa de acierto en comparación con los demás

[24] http://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf [Pág. 11. Tabla 1]

sistemas biométricos convencionales, porque contiene la mayoría de las características de seguridad y confiabilidad que se requiere para un sistema biométrico.

4.3.2 Sistemas biométricos basados en la geometría de la mano. La utilización de sistemas biométricos puede llegar a cambiar entre aplicación y aplicación, sea cual sea que se requiera. Para establecer de qué manera me beneficiara en cuanto a seguridad, calidad y robustez, primero se debe entender y conocer cuáles son los requerimientos de operación que necesita dicha aplicación del sistema biométrico. "*La biometría puede proveer de un método automático de identificación de un individuo o de verificación de una identidad proclamada*"[25]. Previo a tomar una decisión es necesario cerciorar de que la tarea va a satisfacer las condiciones de operación necesarias.

A continuación se muestran una serie de herramientas, funciones y técnicas para la implementación de sistemas biométricos basados en la geometría de la mano, permitiendo de esta manera el desarrollo de soluciones integradas, escalables y robustas, para minimizar el costo del desarrollo y mantener todas las características y parámetros necesarios para la implementación y solución de un sistema de seguridad biométrico.

4.3.2.1 Sistemas que capturan la imagen del dorso de la mano. Este sistema adquiere las imágenes de tres maneras: mediante la banda de visible, otra en la banda de 850nm y por último en la banda de 1450nm. Para el procedimiento de captura, primero se ilumina con un bombillo que emite radiación en cada una de las tres bandas. Luego se colocan tres cámaras en la parte superior de la mano. El sistema descrito se puede observar en la *Figura 11*. Para la imagen tomada en la banda visible se usa una webcam de 640x480 pixeles. Para la imagen en la banda de 850nm se usa otra webcam de 640x480 pixeles modificada para que trabaje como infrarrojo. Para la obtención de la imagen en la banda de 1450nm se usa una cámara con un sensor de AsGaIn sensible en un rango dinámico desde 900 a 1700nm, con un lente que posee un filtro pasa-banda a 1450nm y un ancho de banda de 250nm.En la *Figura 10* se puede apreciar las imágenes capturadas.

[25] http://www.biometria.gov.ar/acerca-de-la-biometria/preguntas-frecuentes.aspx

Figura 10. Imágenes adquiridas del dorso de la mano en la banda visible (izquierda), banda 850nm (centro) y 1450nm (derecha).[26]

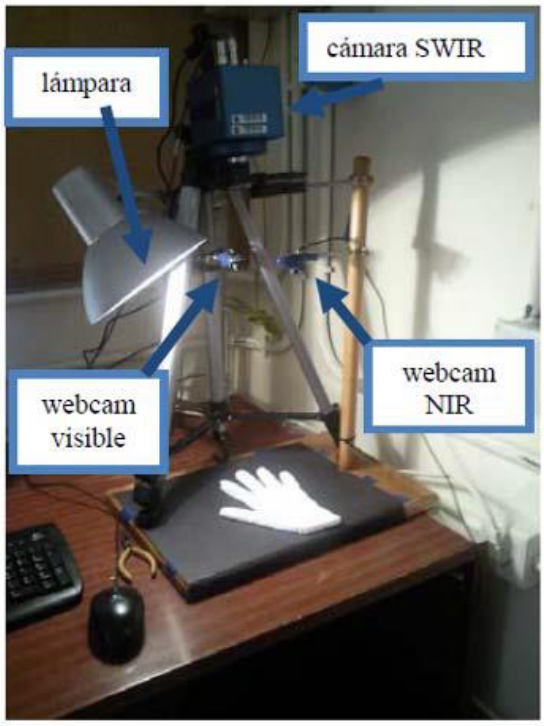


Figura 11. Sistema para capturar imágenes del dorso de la mano en las bandas visible, 850nm y 1450nm.[27]

4.3.2.2 Sistemas que capturan la palma de la mano por contacto.

[26] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 4. Fig. 1]
[27] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 4. Fig. 2]

- **Sistema mediante el escáner:** El uso del escáner es quizás el más fundamental y básico de los sistemas de biometría de la mano. Cada individuo coloca su mano sobre el escáner, con la condición de que no debe tocar los bordes del cristal del escáner y tener los dedos firmes y extendidos, como se muestra en la *Figura 12*. Mediante este sistema se pueden obtener medidas de la palma de la mano, la textura de la misma y de los dedos. En la *Figura 13* se puede observar una imagen captada utilizando este sistema.

Figura 12. Sistema de escáner para capturar la palma de la mano.[28]

Figura 13. Imagen de la mano capturada mediante el sistema de escáner.[29]

[28] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 5. Fig. 3]
[29] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 5. Fig. 4]

- **Sistema mediante el PRM233c Big Eye.** El dispositivo fue desarrollado por la empresa Hungarian Recognition, y se diseñó con el fin de capturar imágenes de los pasaportes en las bandas visible, infrarroja y ultravioleta. El dispositivo se puede apreciar en la *Figura 14*. Actualmente, este sistema es utilizado para capturar imágenes de la geometría de los dedos, es decir, solo se capturan los contornos correspondientes a estos últimos. Las imágenes son tomadas por una cámara que posee un sensor CCD (charge-coupled device) iluminando la mano con luz blanca y posteriormente con luz infrarroja. En la *Figura 15* se observa un ejemplo del funcionamiento de este sistema.

Figura 14. Dispositivo PRM233c utilizado para biometría de los dedos.[30]

Figura 15. Funcionamiento del sistema PRM233cbigeye. Imagen captada en Banda visible (izquierda) e infrarroja (derecha).[31]

- **Sistemas de captura multi-espectral sin contacto.** Estos sistemas se diseñaron con el fin de verificar a un individuo por medio de la geometría de la mano. Este sistema utiliza dos cámaras web, una designada para tomar imágenes en la banda de 850nm y la otra en la banda visible.

[30] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 6. Fig. 5]
[31] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 6. Fig. 6]

La cámara web que capta en la banda de 850nm, se utiliza para permitir observar la segmentación de la mano en entornos expuestos a mucha luz. Por lo tanto, los parámetros se ajustan a para una exposición muy pequeña de luz, brillo bajo, contraste alto y ganancia alta, con el fin de obtener imágenes saturadas donde la mano se ve brillante en primer plano y el fondo oscuro.

La otra cámara web se usa en la banda visible para obtener una imagen de la geometría de la mano, pero en esta ocasión, los parámetros se ajustan con una exposición más pequeña para que no se muestre una imagen borrosa a causa de los movimientos involuntarios de cada usuario durante la captura de la imagen.

- **Sistema con cámaras independientes.** En este sistema se coloca una cámara a unos pocos centímetros de la otra como se observa en la *Figura 16*. La cámara que funciona como infrarrojo se utiliza para segmentar la mano, de tal manera que se aumente la capacidad de discriminación del dispositivo. El funcionamiento consta de que cada usuario acerque la mano y la cámara solo obtiene la imagen de los dedos, mientras que la otra cámara, la cual trabaja en la banda visible, está puesta de forma que cuando la cámara infrarroja capture la imagen de los dedos, luego solo tome la imagen de la palma de la mano. En la *Figura 17* se observa como es la captura de una imagen de la mano mediante este dispositivo.

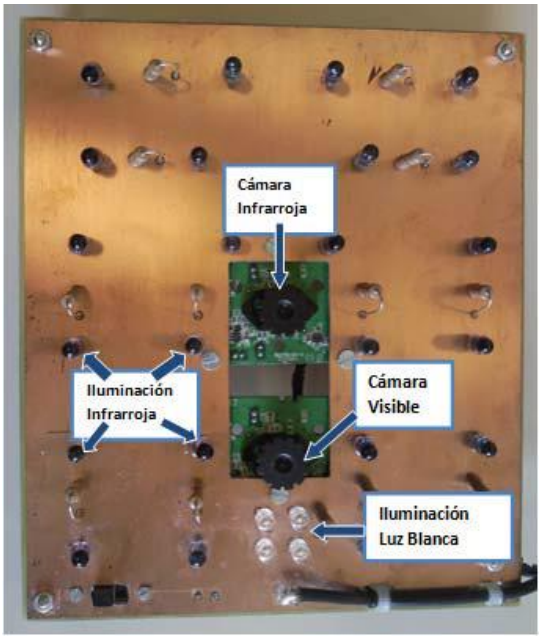


Figura 16. Sistema con cámaras independientes.[32]

[32] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 7. Fig. 7]

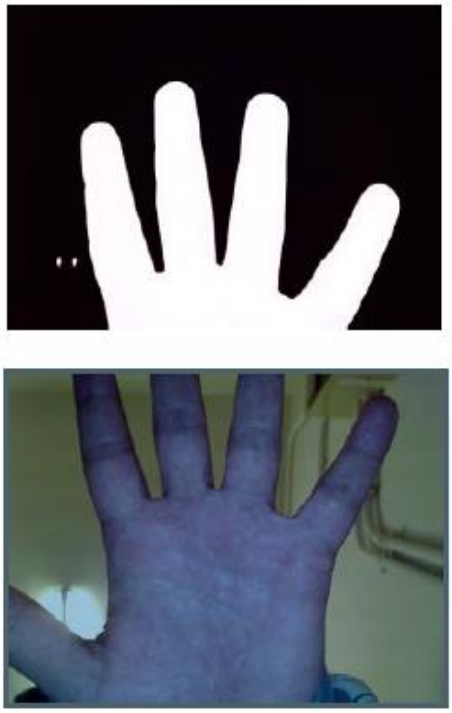


Figura 17. Imágenes obtenidas por las cámaras independientes. Arriba en banda 850nm y abajo en banda visible.[33]

4.3.2.3 Responsabilidad social y protección al usuario. La responsabilidad social es una actitud madura, consciente y sensible a los problemas de la sociedad y es una forma proactiva para adoptar hábitos, estrategias y procesos que nos ayuden a disminuir los impactos negativos que se pueden generar hacia el medio ambiente y la misma sociedad, mediante la utilización de un sistema de seguridad biométrico confiable.

La protección al usuario es un tema fundamental que se debe tratar con precaución cuando se hace uso de un sistema de seguridad biométrico, pues la privacidad de la información que se maneje debe ser extremadamente segura, ya que cada usuario está suministrando información personal (edad, género, sexo, etc.) y lo que se busca es evitar que otras personas infrinjan o se presente fraude ante el sistema.

Con el apoyo de la sociedad resulta más cómodo y factible implantar un sistema de seguridad biométrico, ya que el grado de aceptación que éste tenga depende de las características que presente y la manera como interactúe con los usuarios.

[33] http://jrbp10.unizar.es/papers/S4.C1.pdf [Pág. 7. Fig. 8]

5. METODOLOGÍA

5.1 METODOLOGÍA EMPLEADA

El procedimiento consiste en autenticar una persona que pertenezca a la Universidad Piloto de Colombia, tomando un registro fotográfico de la palma de la mano de cada usuario, de tal manera que se logre identificar el nombre (Juan, María, José,…), facultad (Telecomunicaciones, Sistemas, Civil,…) y tipo de usuario (Estudiante, Docente, Vigilante,…).

La clasificación de las manos de cada uno de los usuarios suele ser un tema interesante, debido a que se puede encontrar una gran cantidad de clases y la similitud entre estas es muy cercana, lo que hace que la sistematización sea más complicada. Este es uno de los principales problemas que se enfrentó debido a la falta de variabilidad discriminante de las manos, no quiere decir que no sea factible desarrollar una aplicación biométrica, puesto que el objetivo es realizar el reconocimiento por medio de la comprobación de algunos patrones característicos de cada mano, evitando que hayan similitudes y de esta manera se pueda determinar con exactitud a cada usuario y se eviten todos los tipos de suplantaciones posibles.

Para la captura de las imágenes se necesita una cámara de alta resolución o un scanner, posteriormente la imagen es almacenada en una base de datos, la cual está relacionada con la información personal de cada usuario para luego ser analizada. El análisis consiste en procesar la imagen de tal manera que se encuentre un patrón o característica propia de cada individuo; luego se compara la imagen con las demás imágenes almacenadas previamente que se encuentran en la base de datos.

El modelo matemático utilizado para realizar todo el estudio comparativo y de análisis de las características propias para cada imagen que se requiere analizar, se trabaja con el programa Matlab, con el cual se puede hacer el procesamiento de imágenes necesario después de la captura respectiva.

De las pruebas realizadas con diferentes métodos se define cuál de estos es el más óptimo para obtener un modelo matemático final, con el cual se va a trabajar y realizar la puesta en marcha de la aplicación y “modelo de prototipo” final.

5.2 ADQUISICIÓN DE IMÁGENES

La captura de imágenes de la palma de la mano, suelen tomarse a través de dispositivos de captura de imagen como lo son escáneres o cámaras fotográficas digitales. La calidad de la imagen adquirida de la palma de la mano depende

principalmente de la tecnología empleada por cada uno de estos dispositivos, por ejemplo los escáneres pueden adquirir imágenes de mayor resolución, pero requieren de mayor tiempo para la toma de la información, lo que implica que para aplicaciones en tiempo real no resulta eficiente. Por otra parte las cámaras digitales capturan imágenes de manera instantánea, pero la calidad y resolución pueden ser deficientes generando problemas de reconocimiento en ambientes donde puede haber variaciones en la iluminación o distorsiones provocadas por el movimiento que genera cada persona al momento de ubicar la mano.

Para nuestro “modelo de prototipo”, las imágenes fueron tomadas con una webcam HD de 720p con autofoco y referencia FaceCam 1020 del fabricante Genius (*Figura 18*), la cual se adaptó a una base en madera que nos permite tenerla fija para que cada usuario ubique la mano correctamente (*Figura 19*) sobre la superficie designada para tal propósito, tratando de evitar que hayan movimientos alternos en cualquiera de los ejes de las coordenadas y adicional a esta adecuación, cuenta con iluminación convencional para que no se presenten cambios en el ambiente de prueba.

Figura 18. Webcam HD de 720p con autofoco FaceCam 1020.[34]

[34] http://www.geniusnet.com/Genius/wSite/ct?xItem=48725&ctNode=1304

Figura 19. Prototipo donde los usuarios ubican las manos para capturar las imágenes.[35]

Las imágenes tomadas con la cámara cuentan con una resolución 1280x720, lo que nos asegura que con esta calidad se puedan discriminar adecuadamente cada uno de los patrones que se quieren analizar para cada usuario.

5.3 PRE-PROCESAMIENTO

El objetivo es conseguir a través de la captura de la imagen de la mano de cada usuario, realizar un análisis por segmentos teniendo en cuenta cuales son las características que se desean analizar, y de esta manera determinar el mejor algoritmo para desarrollar el modelo de prototipo a implementar.

En primer lugar se realiza un proceso de segmentación, el cual consta de tres etapas fundamentales: Filtrado de la imagen, Binarización y Eliminación del ruido.

En segundo lugar se realiza una etapa de tratamiento de la imagen mediante métodos matemáticos, como lo son la Transformada de Fourier, Transformada de Fourier en 2D, Autocorrelación de Imágenes y Comparación de Imágenes.

Por último se analizan las características de interés de la palma de la mano de cada usuario.

[35] http://cdigital.uv.mx/bitstream/123456789/29454/1/Vazquez%20Jimenez.pdf

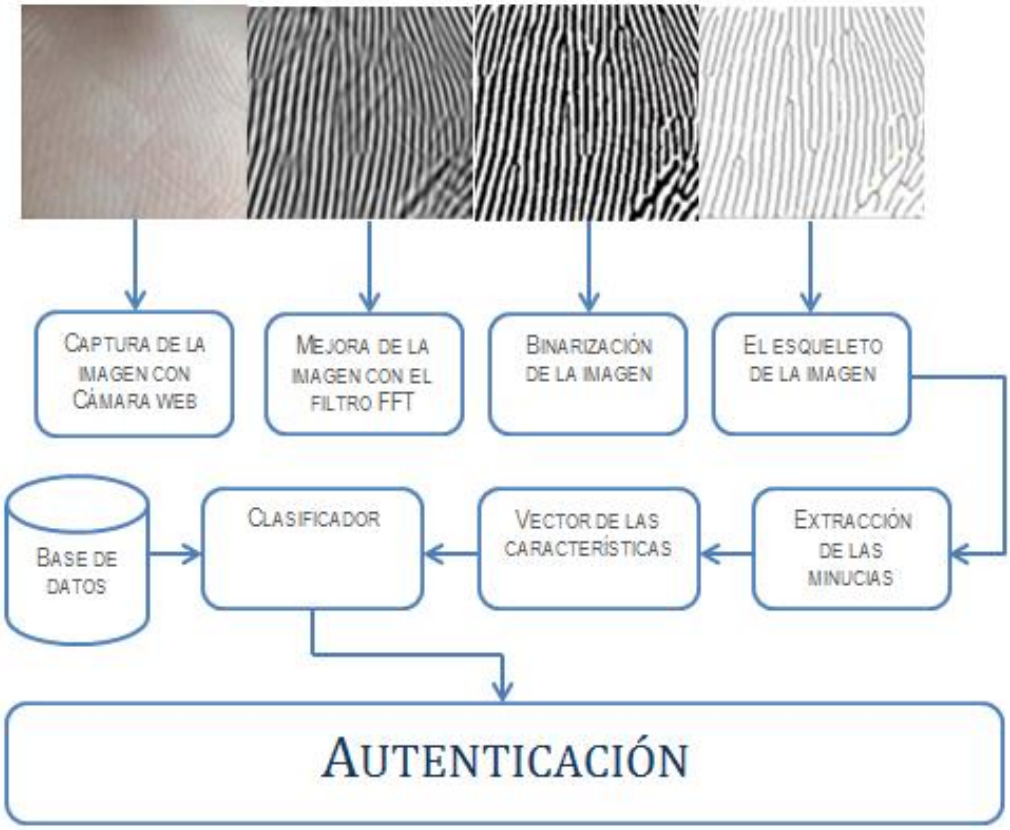


Figura 20. Diagrama de bloques del proceso de reconocimiento.[36]

5.3.1 Proceso de segmentación

5.3.1.1 Filtrado de la imagen. Las imágenes obtenidas al momento de la captura se ven afectadas por el ruido, que son variaciones aleatorias en los valores de intensidad. Por tal razón se requiere utilizar un filtro que permita eliminar esas distorsiones y a su vez afine la imagen para su posterior análisis.

Para este caso se utilizó un filtro gaussiano, el cual realiza un efecto de suavizado para mapas de bits, lo que provoca que la imagen pierda algunos detalles mínimos y de esta manera hace que la misma se vea más difuminada en los bordes, ayudando a que sea más clara o nítida.

- **Filtro gaussiano:** Una distribución gaussiana con desviación típica σ y media μ viene dada por:

[36] Fuente propia

$$\mathbf{g_\sigma(x)} = \frac{\mathbf{1}}{\boldsymbol{\sigma\sqrt{2\pi}}}\mathbf{e}^{-\frac{\mathbf{1}}{\mathbf{2}}\left(\frac{\mathbf{x-\mu}}{\boldsymbol{\sigma}}\right)^{\mathbf{2}}}$$

La convolución de la función $g_\sigma(x)$ dada en la anterior ecuación, con una señal $f(x)$ da lugar a una nueva señal suavizada $h(x)$, donde el valor en cada punto es el resultado de promediar con distintos pesos los valores vecinos a ambos lados de dicho punto. En este suavizado, la desviación típica σ juega un papel importante a la hora de controlar el grado de suavizado de este operador. Cuanto mayor sea, más se tienen en cuenta los puntos lejanos, y, por tanto, mayor será el suavizado resultante.[37]

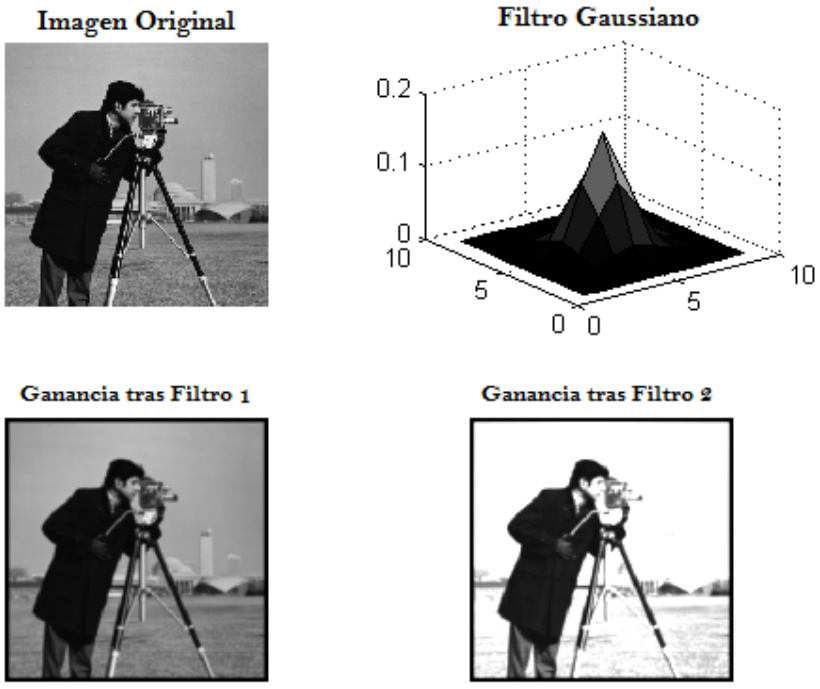


Figura 21. Aplicación de un filtro gaussiano a una imagen digital.[38]

5.3.1.2 Binarización. La binarización de imágenes digitales es una técnica de procesamiento de imágenes que consiste en un proceso de reducción de la información a dos valores binarios (blanco 1 y negro 0).

Este proceso consiste en comparar cada uno de los pixeles de la imagen con un determinado umbral, es decir que para el fondo se tomara como umbral el valor de cero (color negro) y para la palma de la mano un umbral con valor de 1 (blanco). Para nuestro caso se usa un umbral con valor de 1, el cual permite que las

[37] http://www.lpi.tel.uva.es/~nacho/docencia/ing_ond_1/trabajos_03_04/sonificacion/cabroa_archivos/pasobajo.html

[38] http://homes.di.unimi.it/~lombardi/elabImg/LinearFiltering/html/S_01_Convolution.html

sombras o manchas que aparecen en la piel no pasen a ser pixeles de fondo sino queden como pixeles de forman parte de la mano.

Entonces, como se menciona anteriormente, es necesario primero pasar la imagen a escala de grises (Filtrado de Imagen), y luego se realiza el proceso de binarización, ya que las propiedades topológicas y geométricas de la imagen al momento de reducirlas hacen que está se procese mucho más rápido.

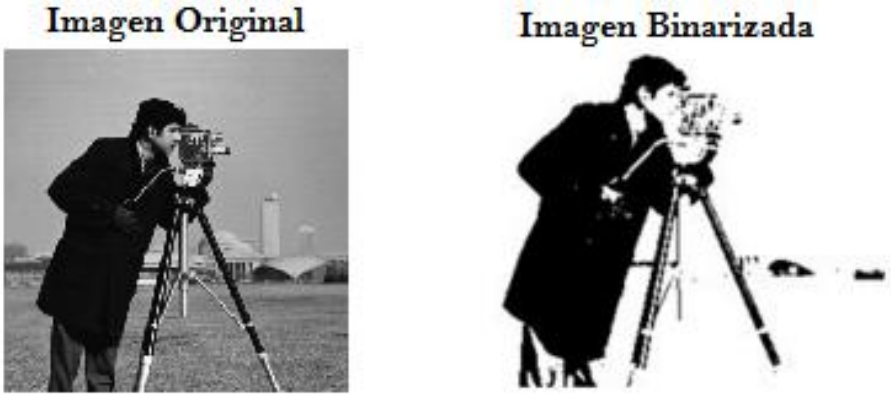


Figura 22. Binarización de una Imagen Digital.[39]

5.3.1.3 Eliminación de ruido. Luego de realizar los dos procedimientos anteriores, para eliminar el ruido se detectan las componentes de la imagen y se calcula nuevamente el tamaño de la misma. Inmediatamente de esto se procede a realizar el siguiente paso del pre-procesado.

5.3.2 Tratamiento de la imagen

5.3.2.1 Transformada de Fourier. La transformada de Fourier es una importante herramienta del procesamiento de imágenes la cual es utilizada para descomponer una imagen en sus componentes seno y coseno. La salida de la transformada representa la imagen en el dominio de Fourier o en el dominio de la frecuencia, mientras que la imagen de entrada está en el dominio espacial. Cada punto de la imagen en el dominio de Fourier representa una frecuencia particular contenida en la imagen en el dominio del espacio. La transformada de Fourier se utiliza en un amplio rango de aplicaciones, tales como análisis de imágenes, filtrado de imágenes, reconstrucción de imágenes y compresión de imágenes.[40]

[39] http://slideplayer.es/slide/1737314/
[40] http://dea.unsj.edu.ar/imágenes/recursos/Capitulo2.pdf

5.3.2.2 Transformada de Fourier de una imagen. Sea $\boldsymbol{f(x)}$ una función continúa en la variable $\boldsymbol{x}$, la transformada de Fourier de esta función indicada por $\boldsymbol{F[f(x)]}$ está dada por la ecuación:

$$\mathbf{F[f(x)] = F(u) = \int_{-\infty}^{\infty} f(x) e^{-j2\pi ux}\, dx}$$

Donde j es la raíz cuadrada de (-1) y u la variable de frecuencia. Proporcionada $F(u)$ podemos volver a hallar $f(x)$ empleando la transformada inversa de Fourier:

$$\mathbf{F[f(x)] = F^{-1}(u) = \int_{-\infty}^{\infty} f(x) e^{-j2\pi ux}\, dx}$$

Estas dos ecuaciones se denominan par de transformadas de Fourier, y existen siempre que $f(x)$ sea continua e integrable y $F(u)$ sea integrable. Estos conceptos pueden extenderse a funciones en dos dimensiones del tipo $f(x, y)$. Si la función $f(x, y)$ es continua e integrable y $F(u, v)$ es integrable, entonces existe el par de transformadas de Fourier:

$$\mathbf{F(x, y) = \iint_{\infty} f(u, v) e^{-j2\pi(ux+vy)}\, dudv}$$

$$\mathbf{F(u, v) = \iint_{\infty} f(x, y) e^{-j2\pi(ux+vy)}\, dxdy}$$

Supongamos que la función continua $f(x)$ se ha vuelto discreta en la sucesión:

$$\mathbf{\{f(X_0), f(X_0 + \Delta x), f(X_0 + 2\Delta x), \dots, f(X_0 + (N-1)\Delta x)\}}$$

Tomando N muestras separadas a una distancia, como se puede observar en la Figura 23.

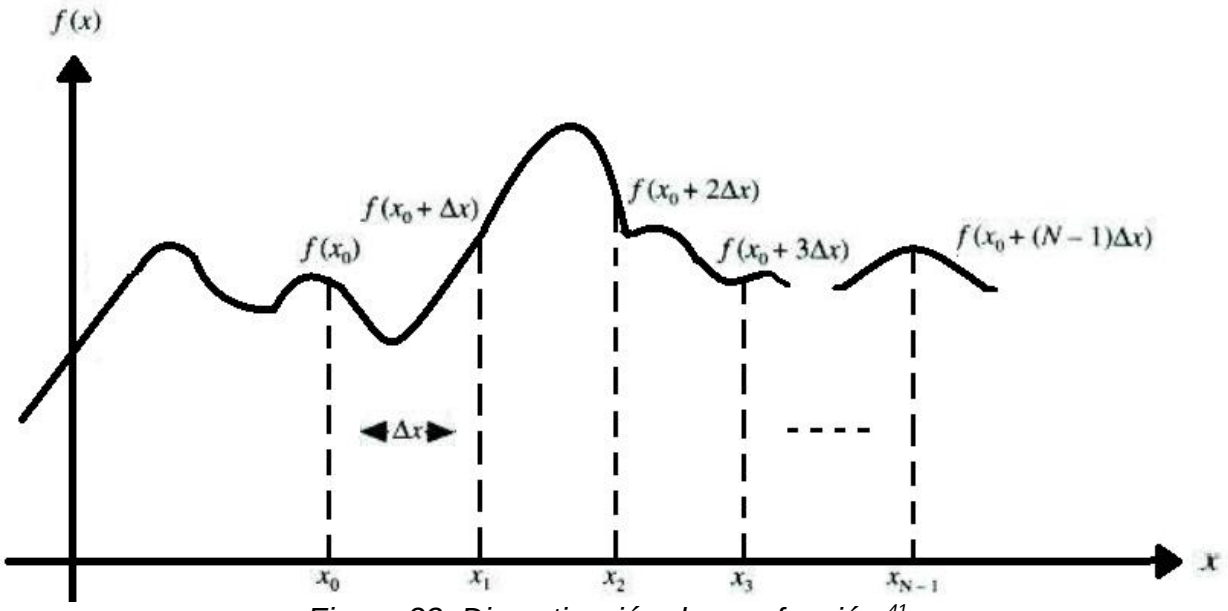


Figura 23. Discretización de una función.[41]

El par de transformadas discretas de Fourier que se emplea a las funciones muestreadas es:

$$\mathbf{F(u) = \frac{1}{N}\sum_{x=0}^{N-1} F(x)e^{-j2\pi\frac{ux}{N}}}$$

$$\mathbf{f(x) = \frac{1}{N}\sum_{u=0}^{N-1} F(u)e^{j2\pi\frac{ux}{N}}}$$

Los valores u de la transformada discreta de Fourier corresponden a las muestras de la transformación continua en los valores $0, 2, \ldots, (N-1)$. Para el caso de funciones que son discretas en dos variables el par de transformada discreta de Fourier es:

$$\mathbf{F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} f(x,y)e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}}$$

$$\mathbf{f(x,y) = \frac{1}{MN}\sum_{u=0}^{M-1}\sum_{v=0}^{N-1} F(u,v)e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)}}$$

[41] http://dea.unsj.edu.ar/imagenes/recursos/Capitulo2.pdf

Estas últimas ecuaciones son las utilizadas para trabajar con imágenes. Se formuló que una imagen puede ser constituida por medio de una función discreta $f(x, y)$, y por lo tanto es posible hallar la transformada de Fourier.

5.3.2.3 Transformada de Fourier en Dos Dimensiones (2D). De acuerdo a lo explicado anteriormente acerca de la transformada de Fourier para imágenes, es necesario tener en cuenta las siguientes consideraciones. En primer lugar, una imagen puede considerarse como una función de dos variables. Cada variable es representada en las coordenadas $\boldsymbol{x, y}$ de un pixel dado y el valor de la función es el valor del pixel. El concepto de frecuencia en el procesado de imágenes se utiliza para hacer énfasis a la frecuencia espacial, cabe recalcar que la frecuencia hace referencia a variaciones en el tiempo, pero en este caso, se refiere a la frecuencia con la que una imagen varía como una función de las coordenadas espaciales.

Con base a lo anterior, se entiende que hay una semejanza entre una imagen y su espectro de frecuencias espaciales; es decir, las imágenes que varían gradualmente tienen bajas frecuencias espaciales, y aquellas que presentan más definición en su tonalidad tienen altas frecuencias espaciales. Por consiguiente, la transformada de Fourier puede utilizarse para generar una nueva representación de la imagen basada en las frecuencias espaciales y conservando toda la información.

La representación gráfica de la transformada de Fourier de una imagen es otra imagen, en la que el eje u representa las frecuencias espaciales sobre el eje x de la imagen original, y el eje v representa las frecuencias espaciales sobre el eje y. Es de importancia saber que la componente de frecuencia más alta tiene un período igual a la anchura de un pixel, lo que refiere a que la frecuencia es de un ciclo por pixel.

En conclusión, se puede afirmar que la representación gráfica de la transformada discreta de Fourier es una imagen formada por pixeles que representan las componentes de frecuencia espacial. O de otra manera, por medio de la transformada discreta de Fourier lo que se puede hacer es reconstruir la imagen original a través de niveles de pixelación para visualizar una imagen o una sección de la misma a un tamaño en el que los pixeles individuales son visibles al ojo, permitiendo que se analice más al detalle una porción de ella.

Para finalizar, en la Tabla 2 se puede ver un resumen de las propiedades que comprende la transformada continua de Fourier bidimensional.

Operación espacial	**Operación en frecuencia**	**Comentarios**
1. Linealidad $af1(x, y) + bf2(x, y)$	Linealidad $aF1(u, v) +$	En ambos dominios aparece la linealidad. El espectro de la

Operación espacial	Operación en frecuencia	Comentarios
	$bF2(u,v)$	suma lineal de imágenes es igual a la suma lineal de los espectros.
2. Cambio de escala $f(ax,by)\left(\frac{1}{ab}\right)$	Escalado inverso $F\left(\frac{u}{a},\frac{v}{b}\right)$	Invarianza en espacio - ancho de banda. Comprimir una función espacial hace que su espectro se expanda y que se reduzca su amplitud en el mismo factor. La amplitud disminuye porque la misma energía ocupa un mayor ancho de banda. Para a=b=-1, la función espacial se invierte. Los ejes frecuenciales también se invierten, los cuales, para imágenes reales, cambian sólo sus espectros de fase.
3. Desplazamiento de la posición $f(x-a,y-b)$	Adición de fase lineal $F(u,v)\mathrm{A}\exp[-j(ua+vb)]$	Desplazar o trasladar la función espacial una cantidad x=a añade una fase 2=ua a la fase original. De la misma manera, un filtro de fase lineal produce una traslación de la imagen. El módulo del espectro es invariante a la traslación.
4. Modulación $\exp[\frac{j(u0x+v0y)}{N}]Af(x,$	Desplaza m. del espectro $F(u-u0,v-v0)$	La multiplicación de una función espacial por una sinusoide compleja hace que su espectro se traslade al centro de u0 , v0.
5. Convolución $f(x,y)g(x,y)$	Multiplicación $F(u,v)AG(u,v)$	La convolución de dos funciones espaciales corresponde al producto de los espectros individuales.
6. Multiplicación $f(x,y)Ag(x,y)$	Convolución $F(u,v)G(u,v)$	El producto de dos funciones espaciales corresponde a la convolución de sus espectros.

Operación espacial	Operación en frecuencia	Comentarios
7. Correlación $f(x,y)Bg(x,y)$	Producto conjugado $F(u,v)AG(u,v)$	La correlación de dos funciones espaciales corresponde al producto de un espectro multiplicado por el espectro conjugado de la otra función.
8. Rotación $f(x\cos 2 + y\,\text{sen}\,2, -x\,\text{sen}\,2 + y\cos 2)$	Rotación $F(u\cos 2 + v\,\text{sen}\,2, -u\,\text{sen}\,2 + v\cos 2)$	La rotación de una función de un ángulo doble hace que el espectro rote ese mismo ángulo. Ni el módulo ni la fase de los espectros son invariantes a la rotación.
9. Diferenciación $dn\ f(x,y)/dxn$	Filtro Paso Alto $(ju)n\ A\ F(u,v)$	La derivada de una función espacial en cualquier dirección corresponde a la forma de un filtro paso alto (que agudiza imágenes).
10. Integración $f(",y)\ (d")n$	Filtro Paso Bajo $(ju) - n\ A\ F(u,v)$	La integral de una función en cualquier dirección corresponde a la forma de un filtro pasabajo que va desde -4 hasta x y a su vez suaviza la imagen.

Tabla 2. Propiedades de la transformada de Fourier continua bidimensional. [42]

5.3.2.4 Correlación y Autocorrelación. La correlación es el parámetro tradicionalmente utilizado para la detección de objetos, ya que, bajo ciertas restricciones, el valor de la correlación en el origen de un objeto consigo mismo (autocorrelación) es mayor que el de la correlación con cualquier otro objeto. Para el caso discreto, la correlación entre una imagen $\boldsymbol{f(x,y)}$ y una señal a detectar $\boldsymbol{s(x,y)}$, de tamaño $\boldsymbol{M \times N}$ viene dado por:

$$\mathbf{c(m,n)} = \sum_{\mathbf{x}} * \sum_{\mathbf{y}} \mathbf{f(x,y)s(x-m,y-n)}$$

Donde $m = 0 \ldots M$ y $n = 0 \ldots N-1$ y $(*)$ significa complejo conjugado. En el caso de imágenes de gran tamaño, es conveniente efectuar esta operación en el dominio de frecuencias a través de la transformada de Fourier, utilizando como

[42] http://www.casdreams.com/cesf/FOC/FO/Transformada%20de%20Fourier.pdf

punto de partida el teorema de correlación, de forma que se puede comprobar que la operación de correlación se reduce a la multiplicación de las transformadas de Fourier de cada una de las imágenes a comparar.[43]

Mediante el método de codificación de bloques de texturas, se puede seleccionar y copiar una porción de la imagen que se quiere analizar en otra área de la imagen que contenga las mismas características, de esta manera se obtienen dos zonas de imágenes idénticas. Para detectar estas zonas en una imagen que ha sido referenciada, se debe calcular la autocorrelación de la imagen para detectar la posición y luego restar la imagen con ella misma, pero desfasada en la posición indicada al realizar la autocorrelación.

Tras realizar este procedimiento, se notaran zonas de la imagen en las que la diferencia vale cero, las cuales corresponden a las zonas copiadas. Si la totalidad de la imagen manifiesta una transformación uniforme las dos regiones se ven afectadas de igual manera, lo que implica que sigue siendo posible detectar la presencia de esas dos partes iguales.

5.3.2.5 Comparación de Imágenes. El proceso de comparación de imágenes es el resultado de realizar los procedimientos anteriormente descritos, es decir, en este proceso se debe calcular una apreciación que evalúe la similitud que existe entre las características reales e imaginarias tomadas entre las imágenes captadas de la palma de la mano de cada usuario.

Para lograr que el sistema sea invariante frente al proceso de comparación de las características que tiene cada mano para cada usuario, al finalizar el proceso de captura, el programa muestra una gráfica de correlación donde se compara la relación que existe respecto a los demás usuarios registrados y la aproximación entre las características.

5.3.3 Características de interés. Debido a que en la etapa de adquisición de las imágenes de la palma de la mano se utiliza una zona de ubicación de la palma con topes, la posición de la palma al ser capturada no es siempre la misma, esto debido a que existen usuarios que interactúan de forma diferente con la zona de ubicación de la mano al momento de tomar las imágenes, generando así tomas donde las palmas presentan variaciones en la posición.

Entonces, teniendo en cuenta que previamente se han realizado diferentes métodos matemáticos para el análisis y tratamiento de imágenes, posteriormente se analizan estas imágenes, pero teniendo en cuenta ahora la forma, tamaño y características particulares que posee cada individuo al momento de capturar la imagen de la palma de la mano.

[43] http://www.aet.org.es/congresos/xi/ten124.pdf

Ahora, de las múltiples características que se pueden realizar a través de un sistema de reconocimiento de la geometría de la mano, mediante la Transformada de Fourier en 2D (ver Sección 6.3.2), se pueden extraer la textura de la palma de la mano, es decir, se utilizará el análisis de la textura de las imágenes tomadas a la palma de la mano pre-procesadas, para generar un patrón de características que las describa y posteriormente las compare para determinar a quién pertenece (ver Figura 24).

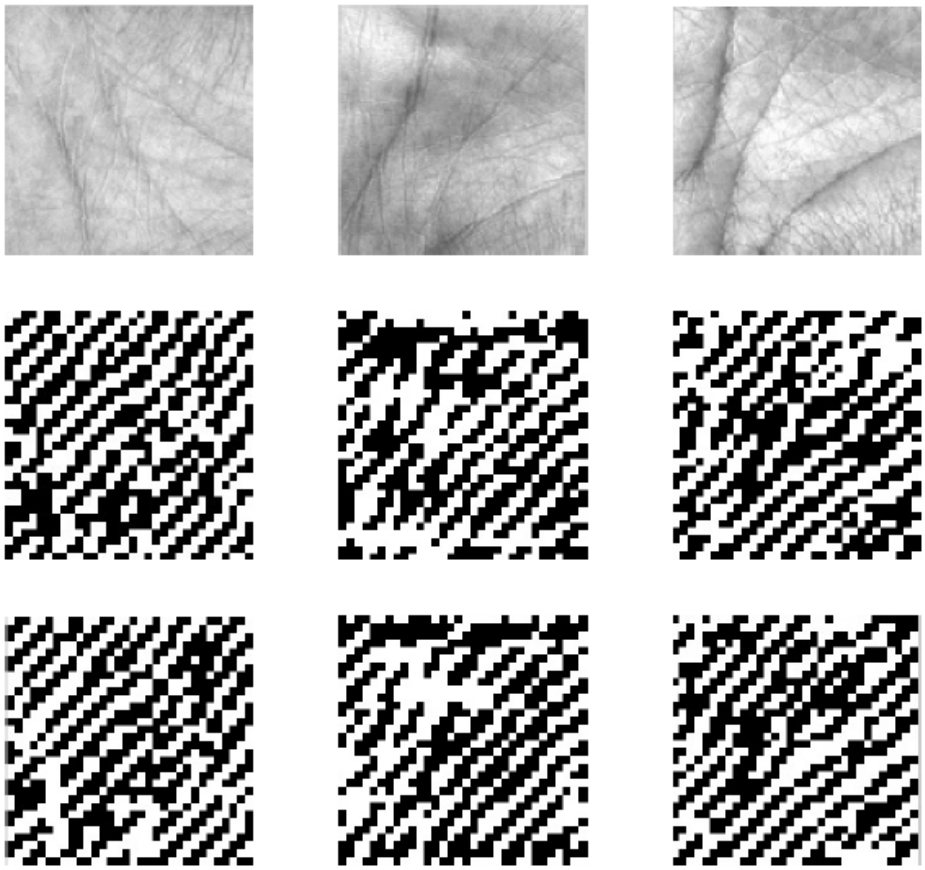


Figura 24. Características extraídas para 3 usuarios diferentes.[44]

[44] http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20120309MariaMeridaAguilera.pdf. Capítulo 4. Sección 4.3 (Extracción de Características).

6. DISEÑO Y DESARROLLO

6.1 MODELO DE PROTOTIPO

Para la obtención de las imágenes de las manos se ha diseñado una estructura en madera donde se encuentra soportada una cámara web de alta definición, mediante la cual se tomará el registro fotográfico de cada mano, permitiendo almacenarlas posteriormente en una base de datos.

La estructura donde se encuentra la cámara web de alta definición, posee un sistema de iluminación adicional para garantizar que al momento de colocar la mano sobre la estructura diseñada, donde se ubica cada una de estas, no haya sombras y en todo momento se mantenga el mismo contraste de fondo e iluminación para cada registro fotográfico. En la Figura 25 se muestra el diseño anteriormente descrito.

Figura 25. Modelo de prototipo del sistema biométrico de la geometría de la mano.[45]

[45] Fuente propia.

La estructura diseñada también permite que el usuario coloque de forma cómoda las manos sobre una base con topes (Figura 26) que se sitúa por encima de la cámara y el sistema de iluminación. Como esta estructura está diseñada con una cubierta para la colocación de las manos, la luz externa no afecta la toma de los registros fotográficos.

Figura 26. Diseño de la base con topes para posicionar la mano de cada usuario.[46]

Las imágenes tomadas tienen una resolución de alta definición (1280 x 720), lo cual permite que se obtenga un adecuado procesamiento y obtención de las características de interés de cada mano. Tras la captura de imágenes se realiza un pre-procesado de la imagen obtenida, siguiendo todo el proceso mencionado en el numeral 6.3.

Para la adquisición, el pre-procesado y análisis de las características de interés de cada mano, se ha utilizado como herramienta Matlab, que mediante un código (Ver Anexo A) se implementan todos los requerimientos para que el sistema biométrico cumpla con las necesidades y objetivos estipulados. Por medio de esta herramienta se automatiza el proceso de captura, codificación y almacenamiento de imágenes. Además de esto, el sistema biométrico diseñado a través de esta herramienta, tiene un valor agregado y es que en caso de requerirse o ser necesario, se puede realizar análisis de otros rasgos biométricos como huellas dactilares y rostros.

[46] Fuente propia

Cabe resaltar que para el desarrollo del proyecto se optó por utilizar Matlab, pues mediante este software se puede realizar el tratamiento de imágenes de una manera más eficaz, dinámica y comprensible al momento de estructurar el código. Así mismo, también se puede realizar una representación de los datos obtenidos y de igual manera se puede asociar con otros programas y dispositivos hardware. Es importante aclarar que Matlab es la herramienta más conocida y trabajada en Universidades e Institutos, lo que resulta más cómodo para encontrar asesorías o tutoriales que permitan desarrollar efectivamente este proyecto.

En la Tabla 3, se puede observar un comparativo de Matlab con otros programas que también permiten realizar tratamiento de imágenes.

Programa	**Características**	**Interfaz gráfica**	**Tratamiento de imágenes**	**Licencia**
MATLAB	- Manipulación de matrices. - Representación de datos y funciones. - Implementación de algoritmos. Creación de interfaces de usuario (GUI). - Comunicación con programas en otros lenguajes y con otros dispositivos hardware. - Funciones para visualizar datos en 2D y 3D.	- Simulink - Toolboxes	Image Processing Toolbox es la herramienta para el procesamiento de imágenes.	Licencia paga. Dos versions: - MATLAB and Simulink Student Suite - MATLAB Student
SCILAB	- Análisis numérico, visualización 2D y 3D. - Optimización, análisis estadístico, diseño y análisis de sistemas	Xcos. Es la herramienta que permite una interfaz gráfica para el diseño de modelos.	SIP es la caja de herramientas que permite el procesamiento de imágenes. SIP aún se encuentra en desarrollo.	Licencia libre.

Programa	Características	Interfaz gráfica	Tratamiento de imágenes	Licencia
	dinámicos. - Procesamiento de señales, e interfaces con Fortran, Java, C y C++			
GNU OCTAVE	- Es considerado el equivalente libre de MATLAB. - Su lenguaje puede ser extendido con funciones y procedimientos, por medio de módulos dinámicos. - Puede cargar archivos con funciones de Matlab (reconocibles por la extensión .m). - El lenguaje está pensado para trabajar con matrices, y provee mucha funcionalidad para trabajar con éstas.	- OpenGL con widgets QT. - Programación orientada a objetos	Compatible con las funciones y herramientas que maneja Matlab. Soporta librerías como OPenCv que maneja más de 500 funciones para el tratamiento de imágenes.	Licencia Libre.
LABVIEW	- Programación gráfica que facilita visualizar, crear y codificar sistemas de ingeniería. - Facilidad de uso, válido para	Es una herramienta gráfica de programación, es decir que los programas se dibujan. Los programas	IMAQ Vision es una librería para tratar aplicaciones de imagen y visión, asi como también el procesamiento	Licencia paga. Licencias de LabVIEW para la Educación Únicamente. Licencias de

Programa	Características	Interfaz gráfica	Tratamiento de imágenes	Licencia
	programadores profesionales como para personas con pocos conocimientos en programación. - Capacidad de interactuar con otros lenguajes y aplicaciones. - Herramientas gráficas y textuales para el procesado digital de señales. - Visualización y manejo de gráficas con datos dinámicos. - Adquisición y tratamiento de imágenes.	en LabView son llamados instrumentos virtuales (VIs).	de imágenes para detección de bordes y reconocimiento de patrones complejos.	LabVIEW para la Investigación Únicamente. Licencias de Multisim para la Educación Únicamente.

Tabla 3. Tabla comparativa entre software que permiten el tratamiento de imágenes.[47]

6.2 Base de datos

La base de datos que se usa para el Sistema Biométrico se hace en formato Excel, con extensión .xls o .xlsx, esto con la finalidad de que sea más interactiva y de fácil uso para aquel que administre la información que se requiere para incluir a todo el personal que se desea registrar.

> Un Libro de Excel está formado por filas y columnas las cuales dan forma a las celdas. De esta manera cada celda tiene una dirección única dentro de la hoja que está precisamente definida por la columna y la fila done está ubicada.

[47] Fuente propia

> Una hoja de un libro de Excel en sus versiones a partir del 2007 tiene una capacidad de almacenamiento de registros por filas y columnas de esta manera:
>
> Las hojas de un libro de Excel 2010 tienen un máximo de 16,384 columnas y están identificadas por letras siendo la última columna la XFD. Este máximo de columnas está presente desde la versión 2007. En Excel 2010 podemos tener hasta 1.048.576 filas lo cual nos da el espacio necesario para la mayoría de nuestras necesidades.[48]

En caso de que la base de datos realizada en Excel no sea soportada con la cantidad de registros mencionada anteriormente, se recomienda cambiar a Microsoft Access, que dentro de sus especificaciones de base de datos y capacidad de almacenamiento, contiene un máximo de 2 gigabytes, que en registros es aproximadamente 2.147.483.648.

La base de datos que guarda la información está en una tabla con nombre "Usuarios UPC.xlsx", ésta contiene la información necesaria para identificar a cada usuario (ID Registro, Nombre, Apellido, Documento, Facultad y Perfil).

El campo ID Registro tiene formato de tipo Número con propiedad de índice único dentro de la base de datos de registro, el cual es el número que debe tener asignado cada uno de los usuarios registrados. Los campos Nombre, Apellido, Facultad y Perfil tienen formato de tipo Texto, en el cual se coloca los datos de cada uno de los usuarios y que tiene como finalidad mostrar toda la información correspondiente de los mismos. El campo Documento tiene un formato de tipo Número, el cual hace referencia a la identificación propia de cada uno de los usuarios.

Para nuestro modelo de prototipo, se decidió usar una base de datos en Excel, pues mediante esta herramienta es más dinámico realizar los registros correspondientes a la prueba piloto. Así mismo, al integrarlo con Matlab, resulta más cómodo para lograr mostrar la información de los usuarios que se encuentran registrados en esta misma.

Es preciso decir que existen otras bases de datos más robustas, como lo es Microsoft Access, SQL Server, Oracle; ya que estas plataformas permiten manipular la información de una manera más segura y dinámica por medio de consultas y procedimientos almacenados asignados a unos usuarios con ciertos perfiles.

[48] https://exceltotal.com/columnas-y-filas/

6.3 Registro y Autenticación

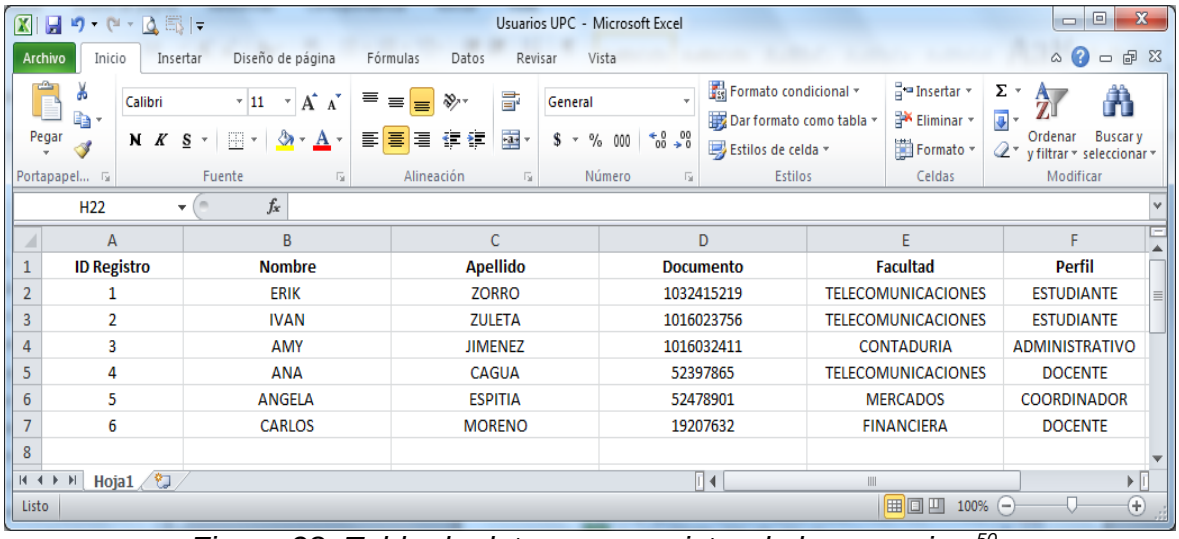
6.3.1 Fase registro

Mediante esta etapa se pretende registrar los usuarios dentro de una base de datos creada en Excel y la toma de las imágenes de la mano de cada uno de ellos, las cuales se almacenan en una carpeta propia del software que se está usando para este sistema de reconocimiento biométrico. En la Figura 27 se muestra el esquema de la etapa de registro.

Figura 27. Proceso de Registro de un Usuario.[49]

A medida que cada usuario se va registrando dentro de la base datos creada en Excel, dentro de la misma se va asignado un ID de registro con Nombre, Apellido, Documento, Facultad y Perfil (Figura 28) Posteriormente, a través de la herramienta Matlab se realiza la toma de cada imagen, en donde cada usuario debe colocar su mano cómo se mostró previamente en la Figura 26, luego la herramienta captura la imagen de la mano, extrae las características de interés (ver numeral 6.3.3), después la imagen tomada de la mano es almacenada en una carpeta propia de la herramienta Matlab y el número asignado para esta imagen debe coincidir con el número de registro en la base de datos de Excel.

[49] Fuente propia



	A	B	C	D	E	F
1	ID Registro	Nombre	Apellido	Documento	Facultad	Perfil
2	1	ERIK	ZORRO	1032415219	TELECOMUNICACIONES	ESTUDIANTE
3	2	IVAN	ZULETA	1016023756	TELECOMUNICACIONES	ESTUDIANTE
4	3	AMY	JIMENEZ	1016032411	CONTADURIA	ADMINISTRATIVO
5	4	ANA	CAGUA	52397865	TELECOMUNICACIONES	DOCENTE
6	5	ANGELA	ESPITIA	52478901	MERCADOS	COORDINADOR
7	6	CARLOS	MORENO	19207632	FINANCIERA	DOCENTE
8						

Figura 28. Tabla de datos para registro de los usuarios.[50]

6.3.2 Fase de Verificación

Esta etapa permite validar la información previamente consignada para cada uno de los usuarios que interactuó con la herramienta, es decir, esta fase autentica la identidad de la persona que intenta acceder al sistema.

La persona que se va a autenticar indica su identidad presentando al sistema su característica biométrica, que en este caso es la mano, luego un sensor se encarga de capturar la imagen de entrada presentada por cada usuario, el extractor de las características de interés se encarga de extraer estas mismas y luego son comparadas contra las características de las imágenes tomadas en la fase de registro y que posteriormente fueron almacenadas en la carpeta propia de la herramienta Matlab, para verificar la identidad.

El resultado que se obtiene mediante este proceso es encontrar que las características o al menos una de ellas, de la nueva imagen tomada, sea igual o muy similar con las que se encuentran almacenadas, y de esta manera el usuario sea aceptado, o en su defecto rechazado si la imagen tomada no coincide con ningún valor de las características de las imágenes almacenadas o si el usuario aún no ha sido registrado.

En la Figura 29 se muestra el esquema del proceso de verificación de un usuario.

[50] Fuente propia

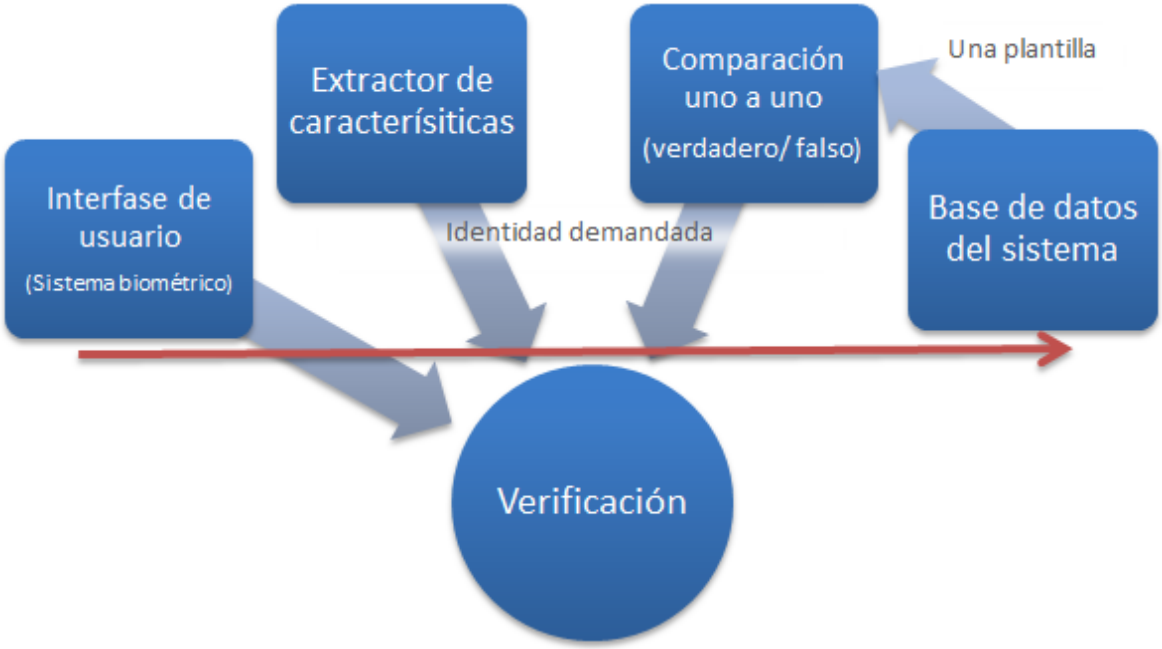


Figura 29. Proceso de Verificación de un Usuario.[51]

6.3.3 Fase de Identificación

En la etapa de identificación se realiza una combinación de las etapas previamente descritas. En este caso, cuando el usuario ha puesto su mano para que ésta sea identificada, la herramienta realiza la verificación de las características de interés almacenadas, así como también realiza una validación en la base de datos si el usuario tiene un número de registro asignado.

Por lo tanto, cuando se quiere identificar a un usuario, se le captura la imagen de la mano, si los datos previamente validados son correctos y coinciden con la información de la fase de registro entonces la herramienta procede a mostrar en detalle la información correspondiente a dicho usuario y a su vez entrega una gráfica donde se muestra el nivel de coincidencia en relación a las demás imágenes que se encuentran en la base de datos. Tal como se observa en la Figura 30.

[51] Fuente propia

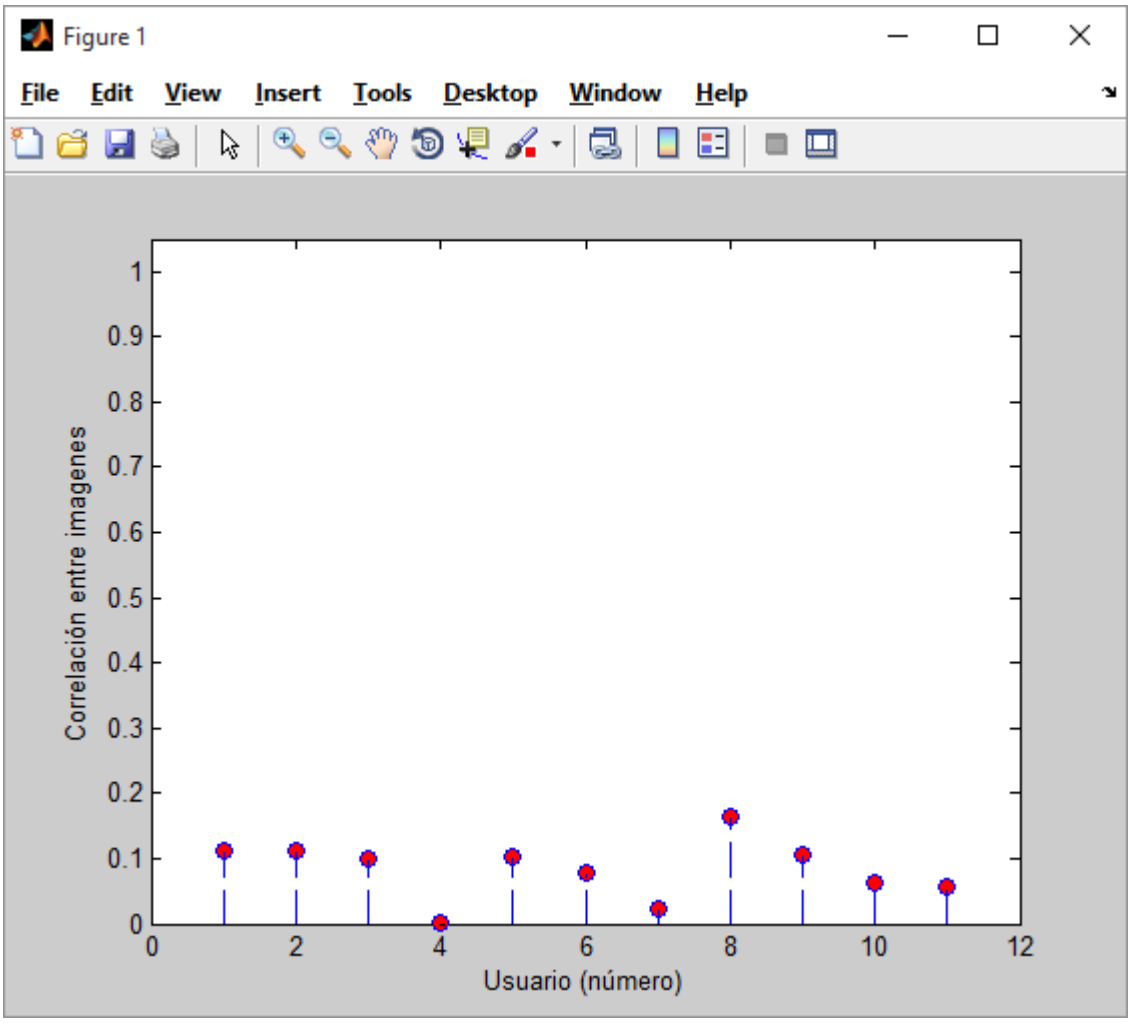


Figura 30. Tabla de correlación de las imágenes tomadas para cada usuario registrado.[52]

En caso contrario, si el usuario no presenta un registro y la información no coincide con las características de interés de la mano realizadas en la fase verificación, el usuario es rechazado y el sistema arroja un error informando (Figura 31) que no se encuentra un registro de este usuario y por lo tanto se debe realizar las fases anteriores para poder permitir la correcta identificación.

[52] Fuente propia

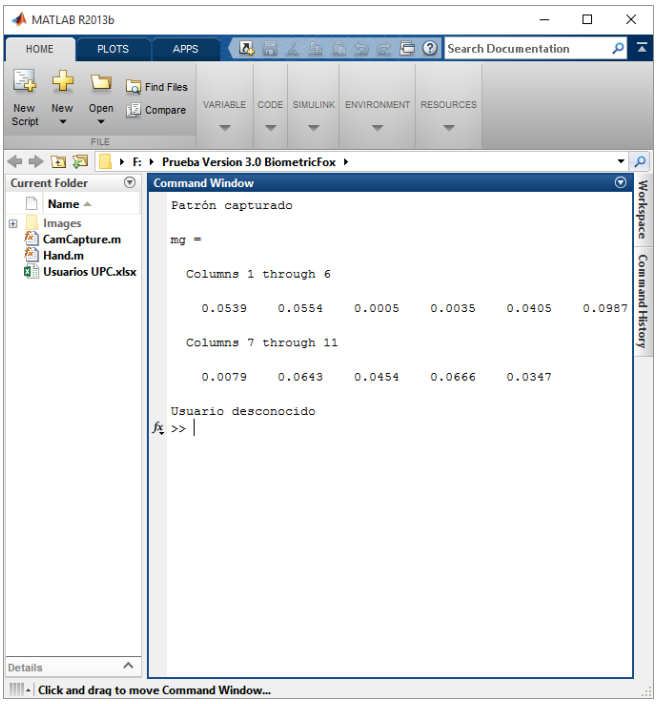


Figura 31. Error generado cuando el usuario aún no ha sido registrado.[53]

La Figura 32 muestra el esquema de la etapa de identificación de cada usuario.

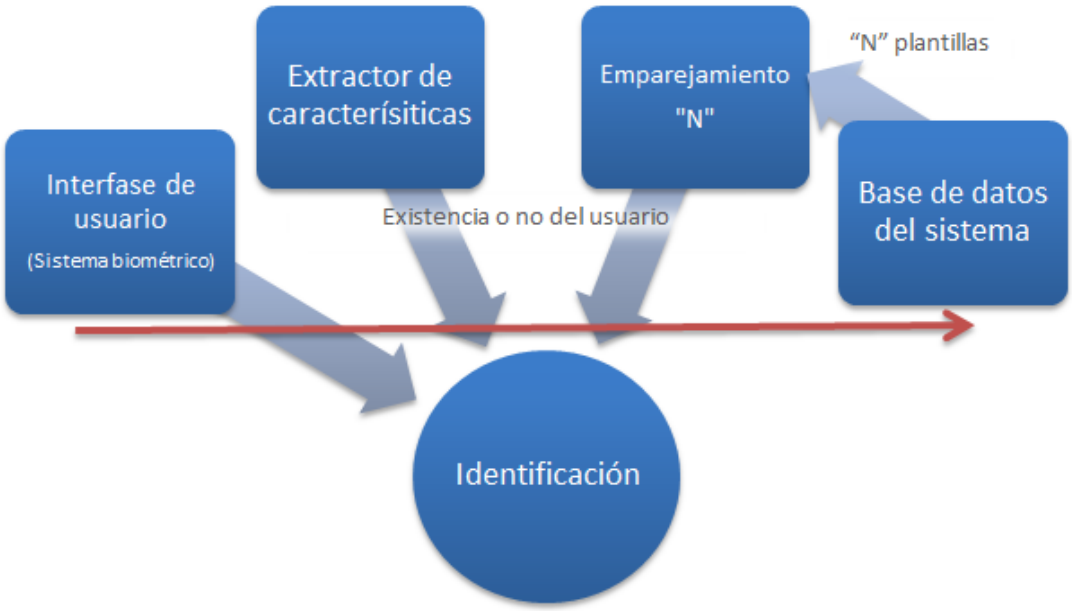


Figura 32. Proceso de identificación de un usuario.[54]

[53] Fuente propia
[54] Fuente propia

7. EXPERIMENTOS Y RESULTADOS

Para la verificación del sistema biométrico se realizaron diversos experimentos con las imágenes de las manos y aquí se presentan los más relevantes. En primer lugar se utilizó un primer segmento del programa para validar el reconocimiento de las características de la mano de cada usuario, por lo tanto se tomaron cuatro imágenes de la geometría de la mano de cada usuario y luego se ejecutó el programa para validar si había afinidad con las imágenes almacenadas dentro de la base de datos propia del sistema biométrico.

7.1 Experimentos

7.1.1 Experimento N° 1

Como se mencionó anteriormente, se capturaron cuatro imágenes de la geometría de mano para cinco usuarios diferentes, estas imágenes fueron almacenadas en una carpeta con nombre “Images” (Figura 33), que para este caso vendría siendo la base de datos propia del sistema biométrico.

El proceso fue hecho en condiciones ambientales de iluminación normal, lo que dio como resultado imágenes con una cantidad considerable de ruido, por lo tanto el proceso de identificación entre las imágenes de la geometría de la mano de cada usuario resulto ser más complejo de lo previsto. Cabe resaltar que para este experimento se tuvo también en cuenta imágenes donde la posición de la mano de cada usuario no era la más adecuada, debido a la posición que cada usuario utilizaba para posicionar la mano al momento de la captura (Figura 34).

El objetivo primordial con este experimento es comparar las imágenes capturadas y almacenadas con una captura real, simulando el acceso al sistema biométrico de un usuario y permitiendo que este sea reconocido o no por la base de datos.

Cabe resaltar, que en la ejecución de este experimento no se logró obtener un resultado adecuado, puesto que al momento de capturar la imagen, sucedió que en el proceso de identificación del usuario, la imagen capturada se parecía a la de otro ya registrado, lo que implicaba que el sistema no fuera optimo y mostrará la información errónea o para este caso la de otro usuario que no era propiamente del que quería acceder. En las Figuras 35 y 36, se puede observar el procedimiento de captura y autenticación del Usuario 1, y al momento de identificarlo el sistema muestra la información del Usuario 5.

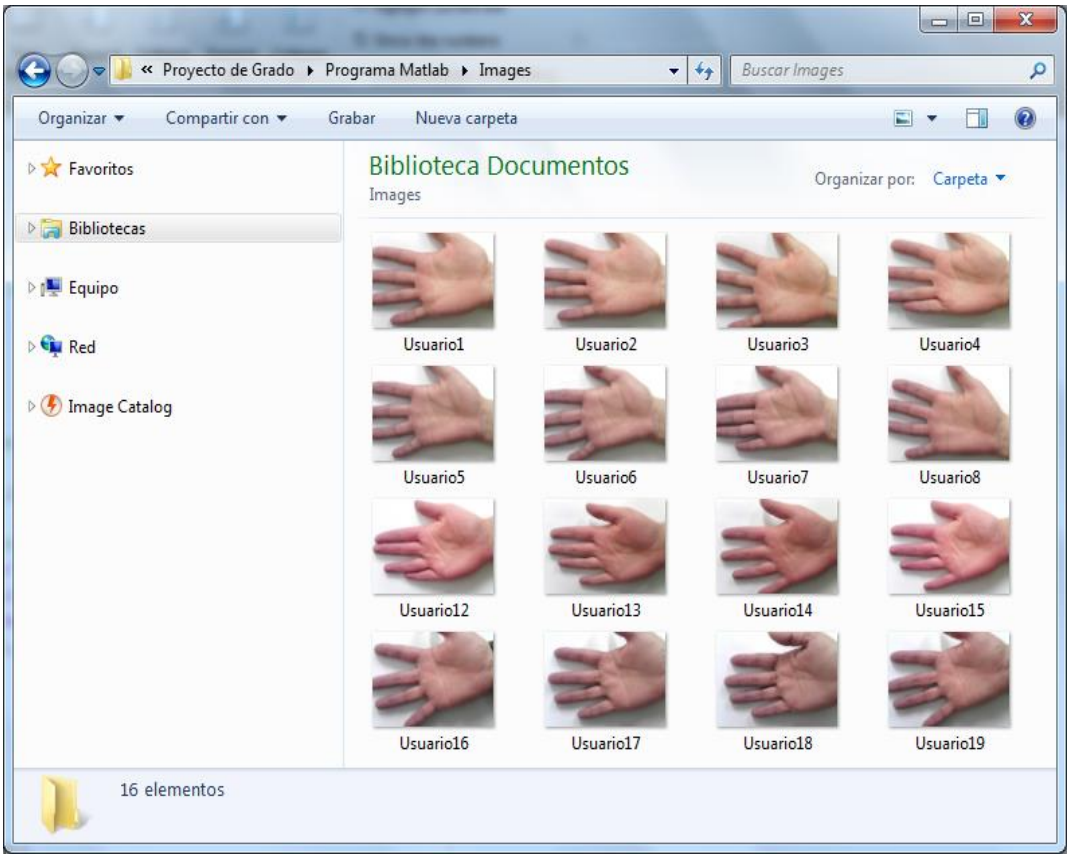


Figura 33. Carpeta "images" donde se almacenaron las imágenes de los usuarios.[55]

Figura 34. Variaciones en la posición de la mano de algunos usuarios registrados.[56]

[55] Fuente propia
[56] Fuente propia

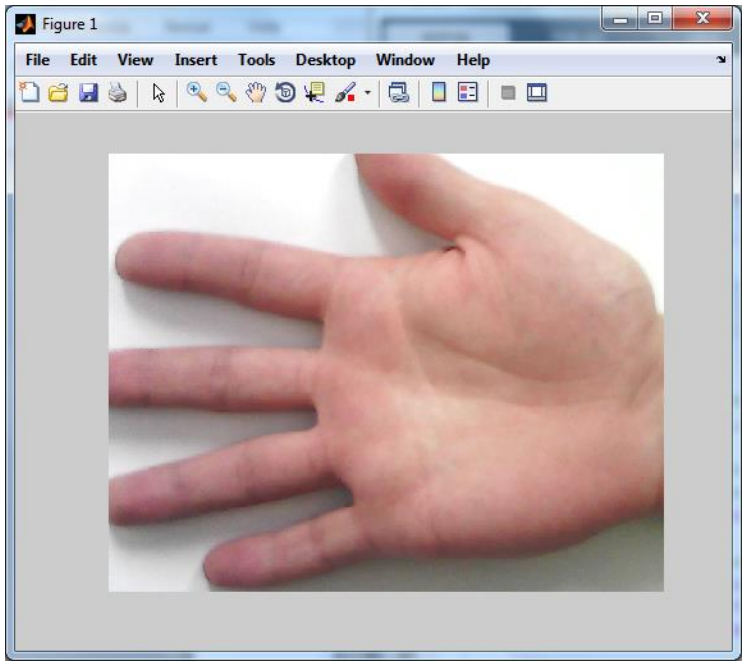


Figura 35. Proceso de captura y verificación del Usuario 1.[57]

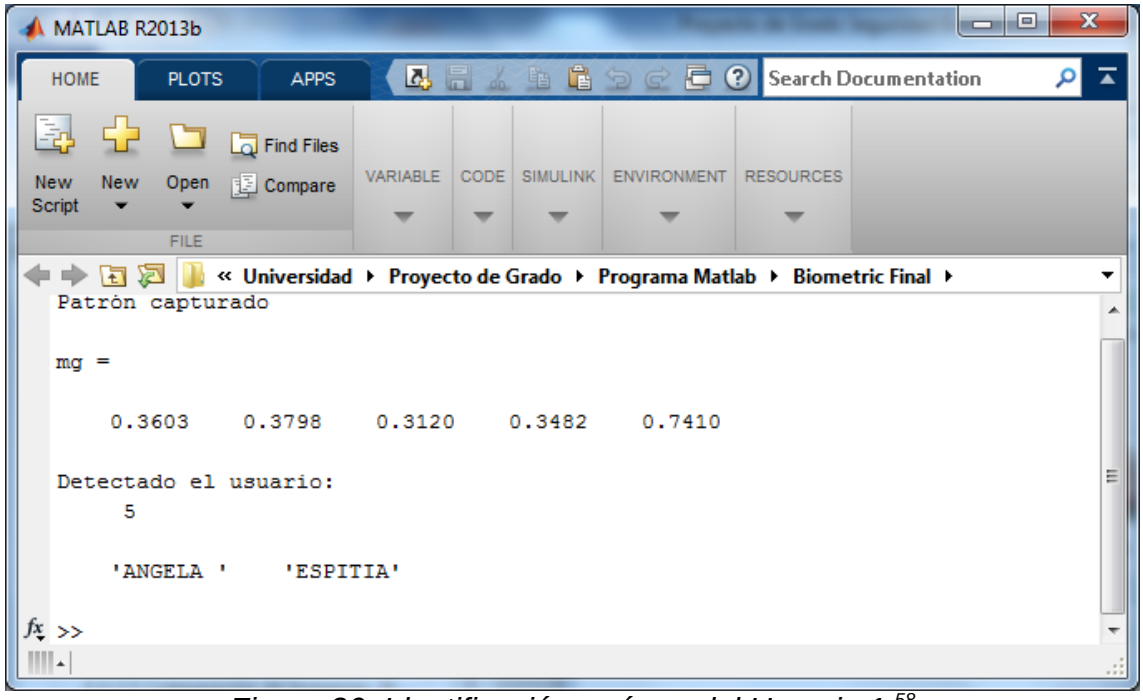


Figura 36. Identificación errónea del Usuario 1.[58]

[57] Fuente propia
[58] Fuente propia

7.1.2 Experimento N° 2

En este proceso, básicamente lo que se realizó fue un procedimiento similar al del Experimento N°1, con la diferencia de que aquí se capturaron más imágenes de la geometría de la mano solicitándole a cada usuario que mantenga una posición fija y constante de la posición de la misma, colocándola sobre una plantilla establecida de la figura de la mano (Figura 37), para poder efectuar la verificación posterior al momento de simular el acceso al sistema biométrico de cada uno.

Para este procedimiento las condiciones ambientales de luz también cambian, en el sentido de que se evita que aparezcan filtros de luz y ruido mejorando el umbral de captura de cada una de las imágenes, manteniendo una estabilidad para este tipo de condiciones.

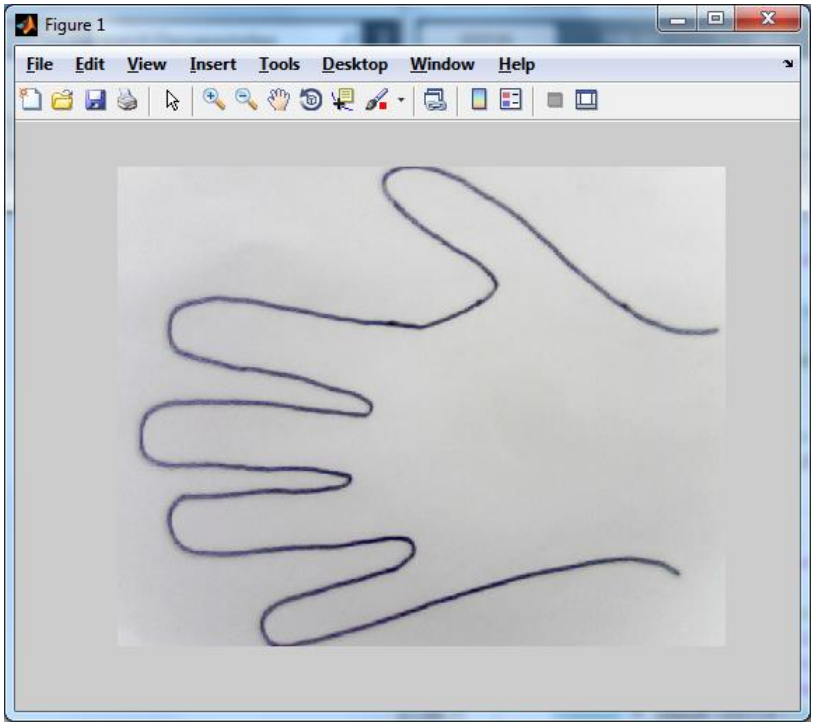


Figura 37. Plantilla de la mano utilizada para que los usuarios posicionen la mano.[59]

En la ejecución de este experimento, se mejoran los resultados en lo que respecta al posicionamiento de la mano de cada usuario, ya que como se mencionó previamente se mantiene una posición fija para la captura de la mano. El único problema con este procedimiento surgió cuando existían usuarios que tienen la mano más grande o más pequeña con respecto a la plantilla, pues al momento de

[59] Fuente propia

la captura, los contornos de las líneas negras que posee la plantilla, generaban que el programa en la etapa de pre-procesado (numeral 6.3), tomaran parte de las características a analizar, haciendo que sucediera algo similar al Experimento N° 1 en la etapa de identificación, aunque en ocasiones cuando la palma ocupaba la plantilla en su totalidad, se logra autenticar de manera efectiva al usuario. En la Figura 38 se puede observar como un usuario coloca su mano sobre la plantilla. Posteriormente, en las Figuras 39, 40 y 41 se muestran los procesos de captura, y autenticación errónea y verdadera de un usuario respectivamente.

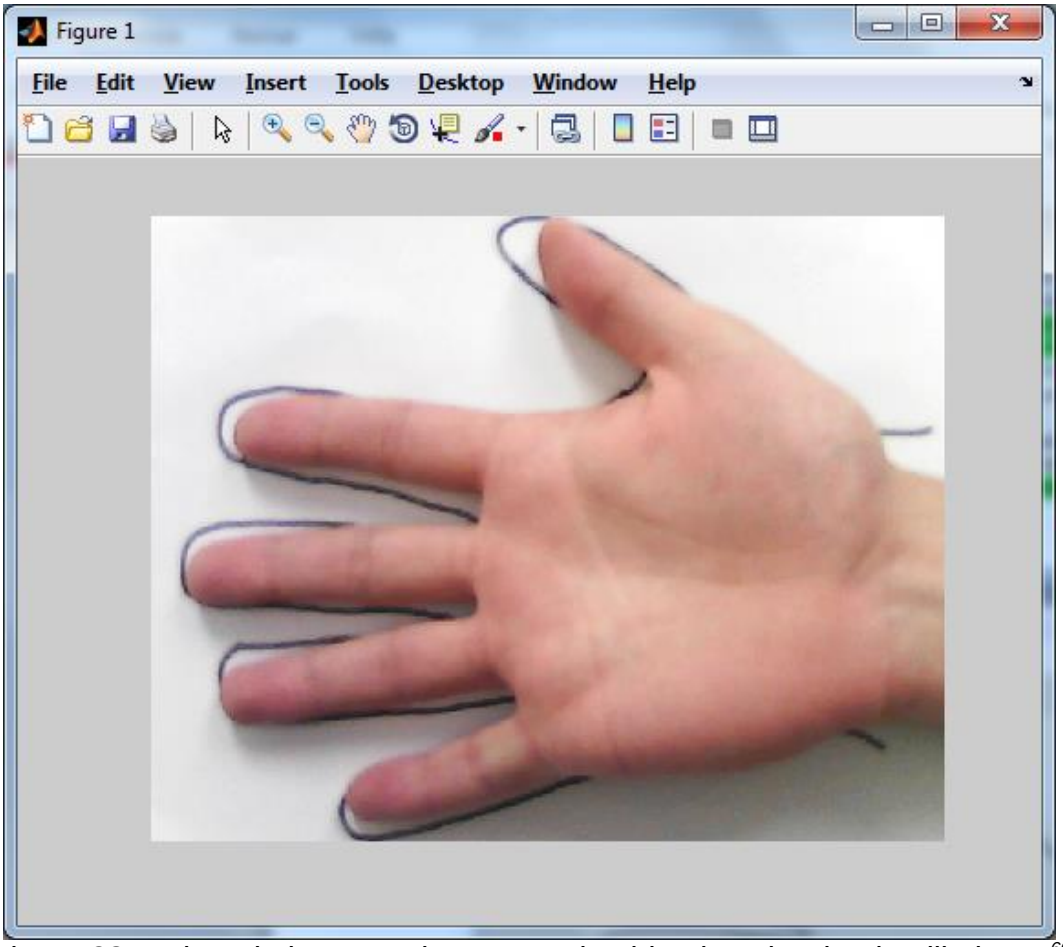


Figura 38. Palma de la mano de un usuario ubicada sobre la plantilla base.[60]

[60] Fuente propia

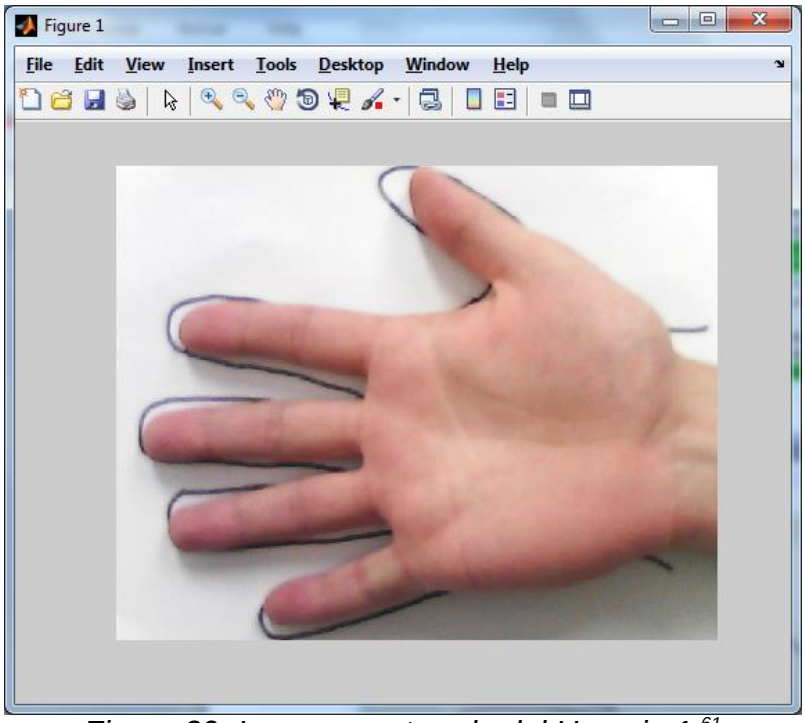


Figura 39. Imagen capturada del Usuario 1.[61]

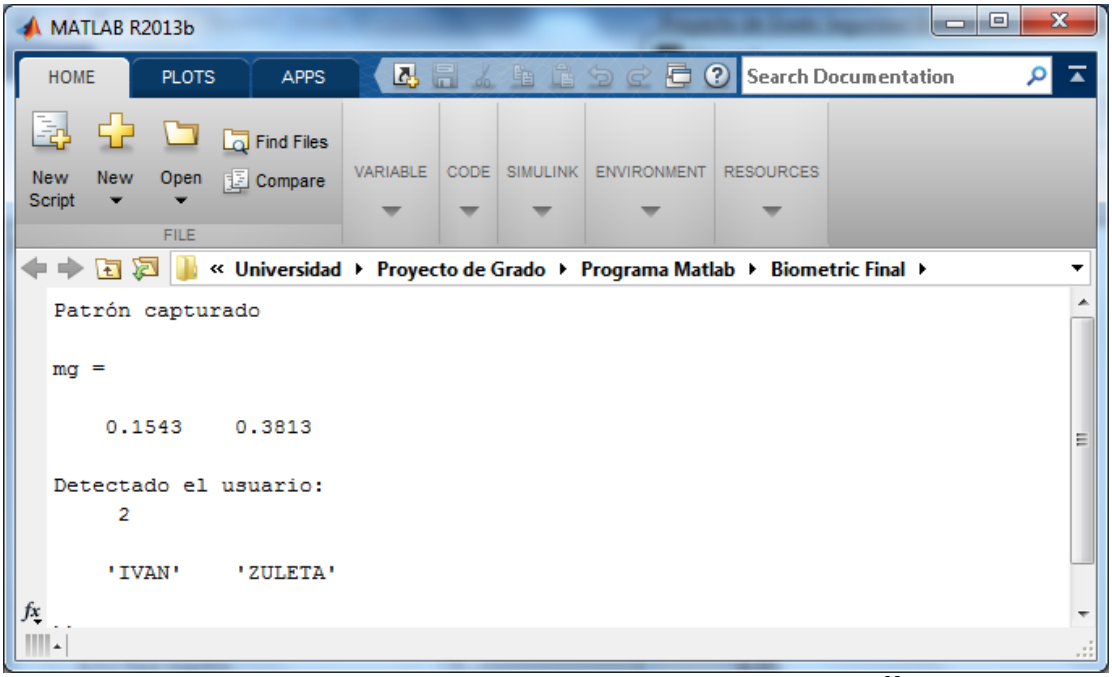


Figura 40. Autenticación errónea del Usuario 1.[62]

[61] Fuente propia
[62] Fuente propia

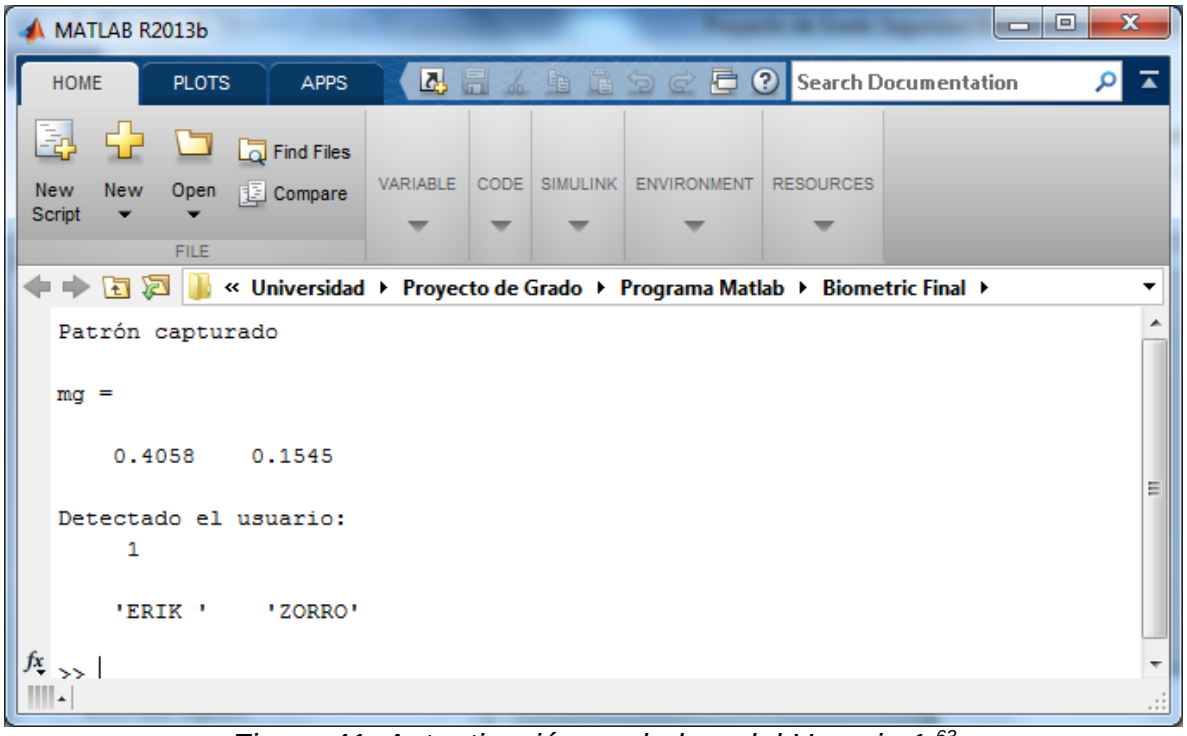


Figura 41. Autenticación verdadera del Usuario 1.[63]

7.1.3 Experimento N° 3

Teniendo en cuenta los resultados obtenidos en los experimentos previamente mencionados (Experimento N° 1 y Experimento N° 2), para este proceso, ahora se opta por diseñar un prototipo para el posicionamiento de la mano, como se muestra en la Figura 42, que permite a cada usuario mantener una posición fija, permitiendo de esta manera mejorar las condiciones para la captura y así evitar varianzas en los movimientos y posiciones de cada una de las manos referente a cada uno de los usuarios.

Para las condiciones ambientales se utilizó el mismo procedimiento del Experimento N° 2, para evitar el ruido y la aparición de filtros de luz que puedan afectar el proceso de filtrado y binarización de la imagen.

En las Figuras 43 a la 46 se muestran los procedimientos de registro, identificación y verificación de un usuario mediante el sistema biométrico desarrollado.

[63] Fuente propia

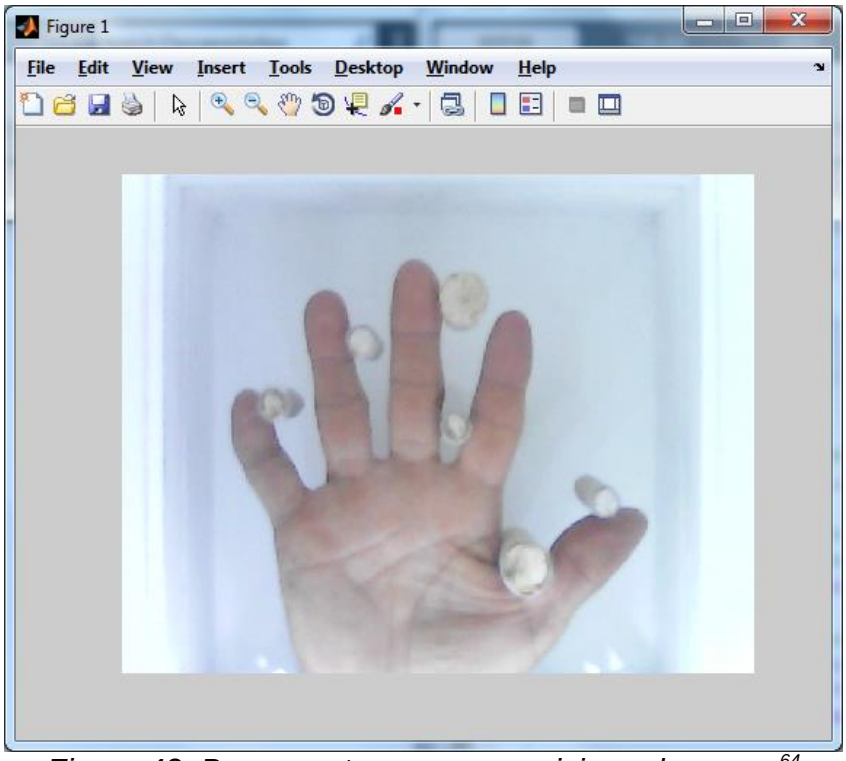
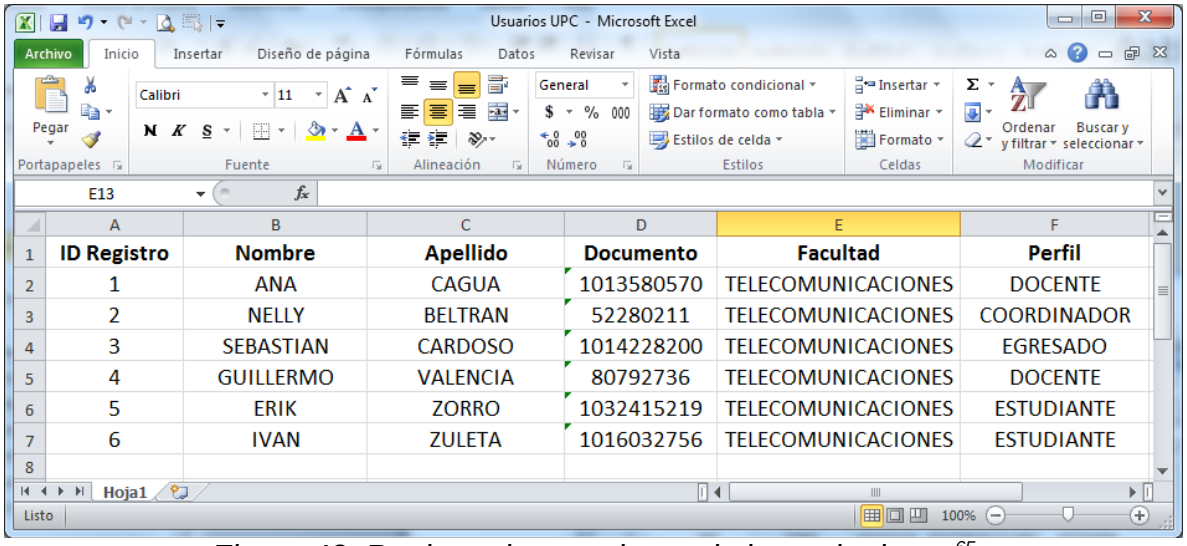


Figura 42. Base con topes para posicionar la mano.[64]



	A	B	C	D	E	F
1	**ID Registro**	**Nombre**	**Apellido**	**Documento**	**Facultad**	**Perfil**
2	1	ANA	CAGUA	1013580570	TELECOMUNICACIONES	DOCENTE
3	2	NELLY	BELTRAN	52280211	TELECOMUNICACIONES	COORDINADOR
4	3	SEBASTIAN	CARDOSO	1014228200	TELECOMUNICACIONES	EGRESADO
5	4	GUILLERMO	VALENCIA	80792736	TELECOMUNICACIONES	DOCENTE
6	5	ERIK	ZORRO	1032415219	TELECOMUNICACIONES	ESTUDIANTE
7	6	IVAN	ZULETA	1016032756	TELECOMUNICACIONES	ESTUDIANTE
8						

Figura 43. Registro de usuarios en la base de datos.[65]

[64] Fuente propia
[65] Fuente propia

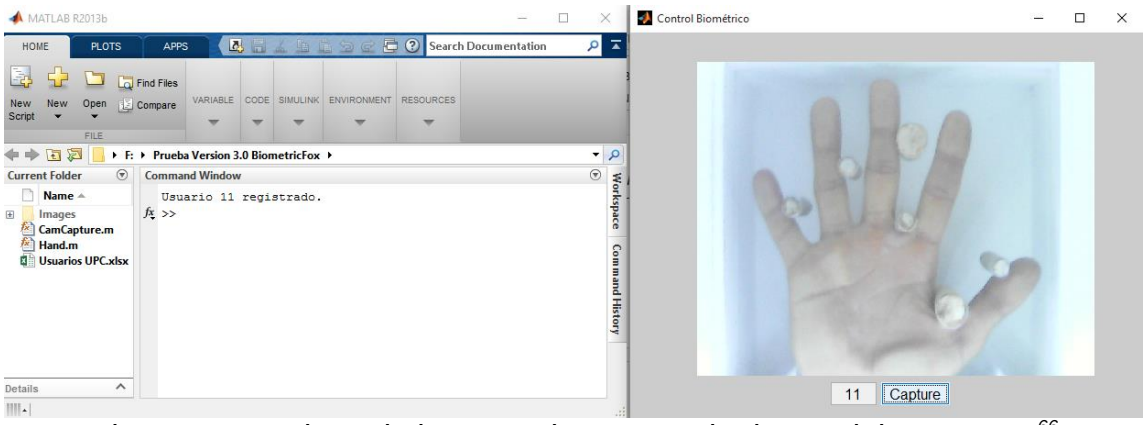


Figura 44. Registro de la mano de un usuario dentro del programa.[66]

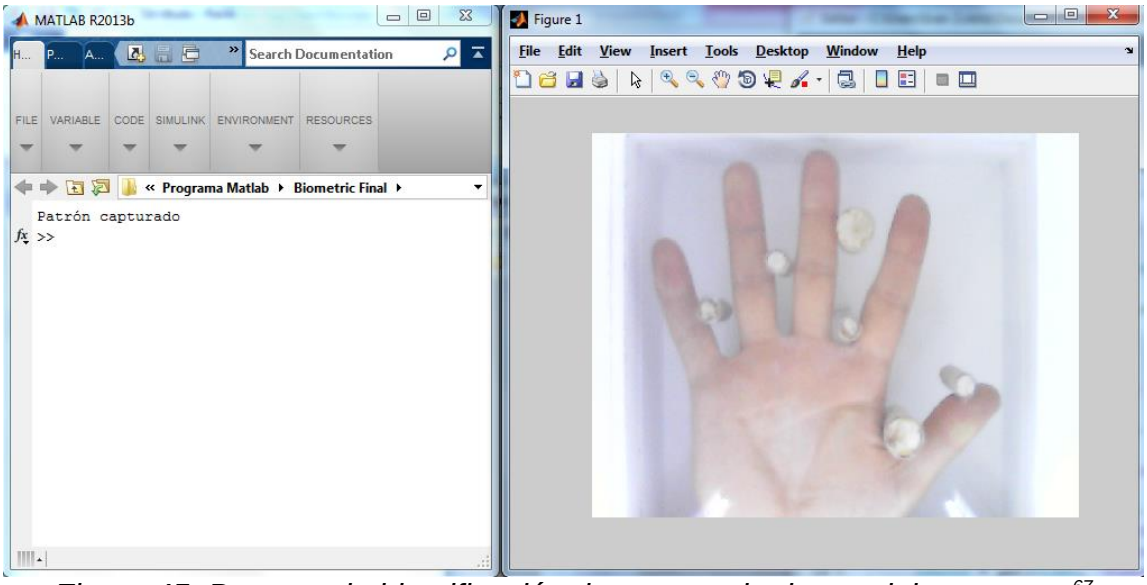


Figura 45. Proceso de identificación de un usuario dentro del programa.[67]

[66] Fuente propia
[67] Fuente propia

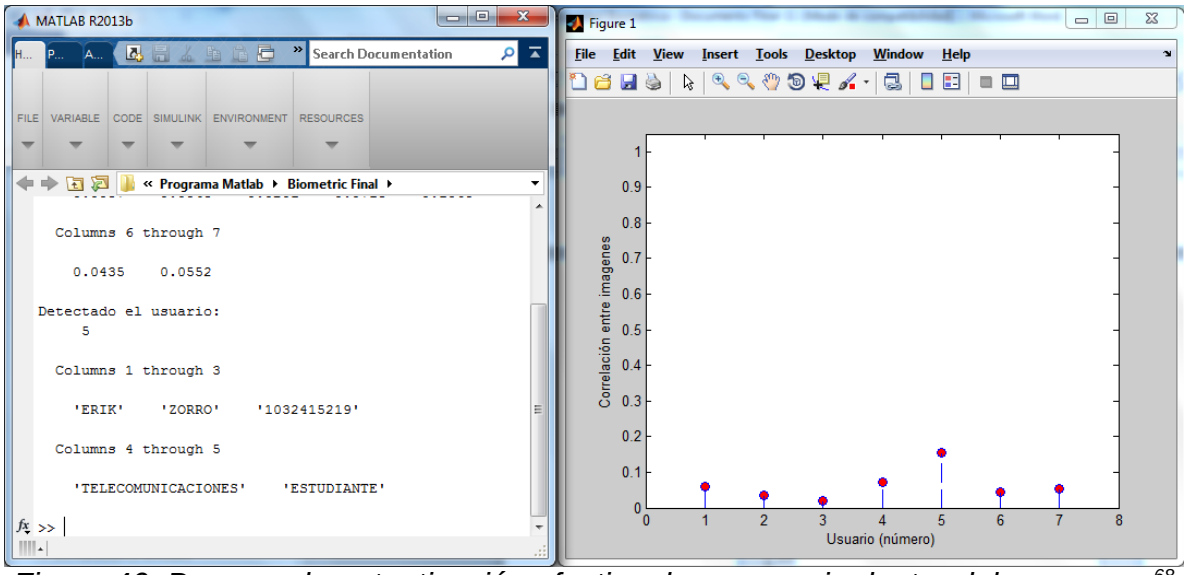


Figura 46. Proceso de autenticación efectivo de un usuario dentro del programa.[68]

7.2 Resultados

7.2.1 Resultado Final

Según las características obtenidas en los experimentos previos, se optó en primera instancia a realizar modificaciones al código en Matlab y al tamaño de la muestra, en términos generales el código permite calcular deformaciones a partir de las imágenes tomadas a cada uno de los usuarios, así como el cálculo de los desplazamientos verticales u horizontales, es decir las varianzas que cada usuario presentaba al momento de ubicar la mano sobre el prototipo base.

La técnica utilizada consiste en la maximización del coeficiente de correlación que se determina a partir del análisis de un subconjunto de pixeles. Este conjunto de pixeles se determina fijando una serie de marcadores, tal cual como se explicó en el numeral 6.3.3.

Finalmente, el sistema biométrico implementado funciona de la siguiente manera:

1) Se realiza el procedimiento de registro (ver numeral 7.3.1).
2) Para cada usuario se procede a tomar el registro fotográfico de la mano derecha.
3) Se realiza el procedimiento de identificación y verificación cuando el usuario intenta acceder al sistema (ver numerales 7.3.2 y 7.3.3).
4) El programa debe indicar si el acceso es autorizado o no autorizado.

[68] Fuente propia

Para entender mejor el funcionamiento descrito anteriormente, a continuación en la Figura 47. Se muestra el diagrama correspondiente al diseño final del sistema biométrico.

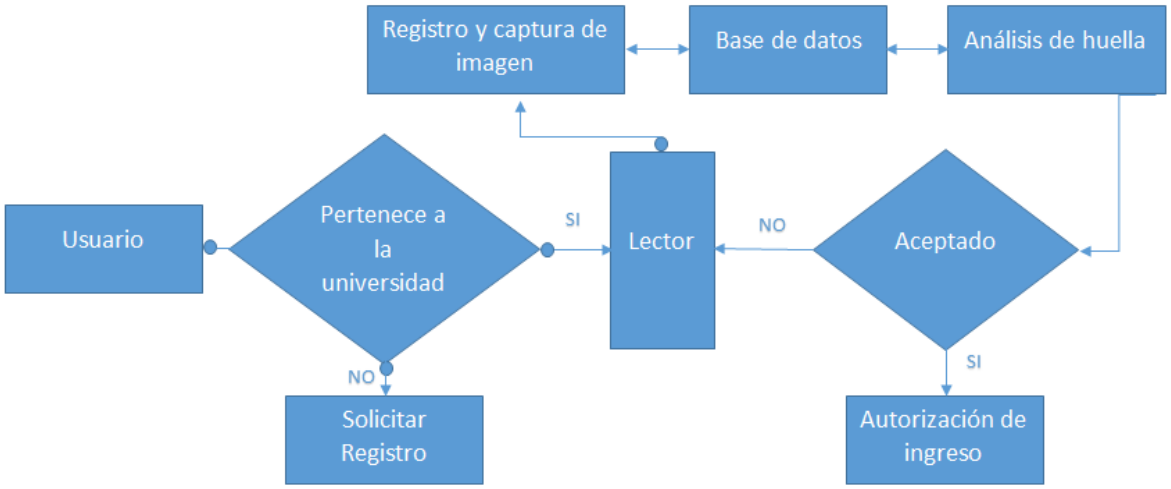


Figura 47. Diseño final del sistema biométrico implementado.[69]

7.2.2 Resultados No Esperados

Para determinar que un usuario es identificado y autenticado correctamente dentro del programa, es necesario no solo validar la información en la base de datos, sino también que al momento de la captura de la imagen (proceso de autenticación) se valide la gráfica de correlación entre imágenes, la cual debe mostrar un índice mayor al 10% (>10%) con respecto a los demás usuarios, garantizando que efectivamente si corresponde a quien intenta acceder, tal y como se observa en la Figura 46.

Todo sistema biométrico no está exento de generar errores dentro de su funcionamiento. Por lo tanto, a continuación se muestra como el programa puede llegar a fallar a pesar de que todas sus condiciones están previamente establecidas de manera correcta. En la Figuras 48 y 49 se muestra el error presentado cuando una persona no está registrada dentro de la base de datos, y se muestra la información de un usuario registrado. Pero para garantizar que este usuario no le corresponde dicha información, mediante el grafico de correlación entre imágenes, se puede ver un índice menor al 10% con respecto a los usuarios que si están registrados.

[69] Fuente propia

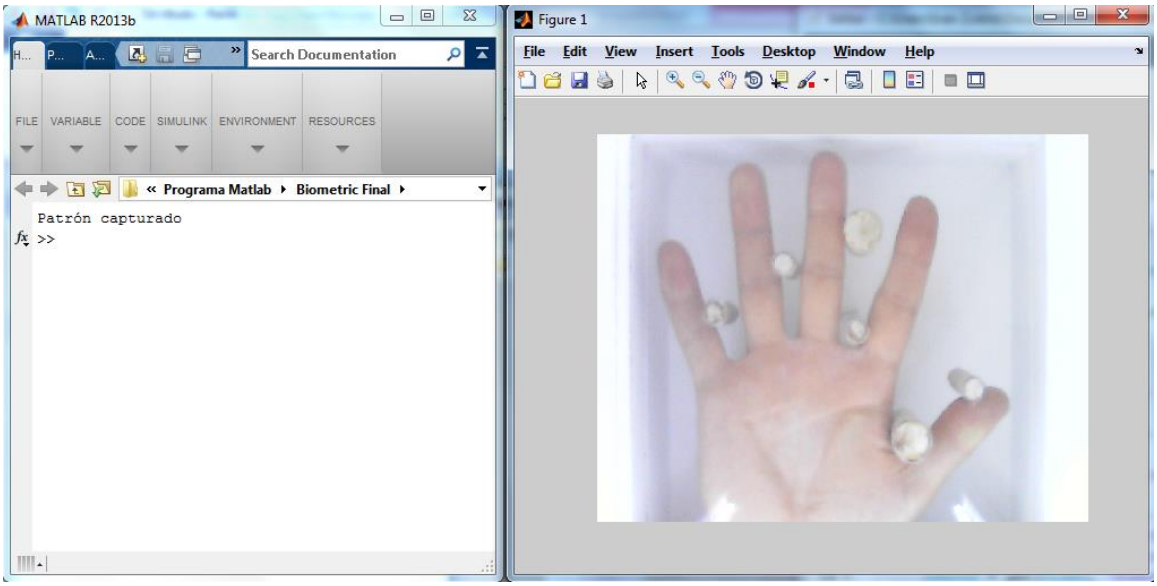


Figura 48. Identificación de un usuario no registrado en el sistema.[70]

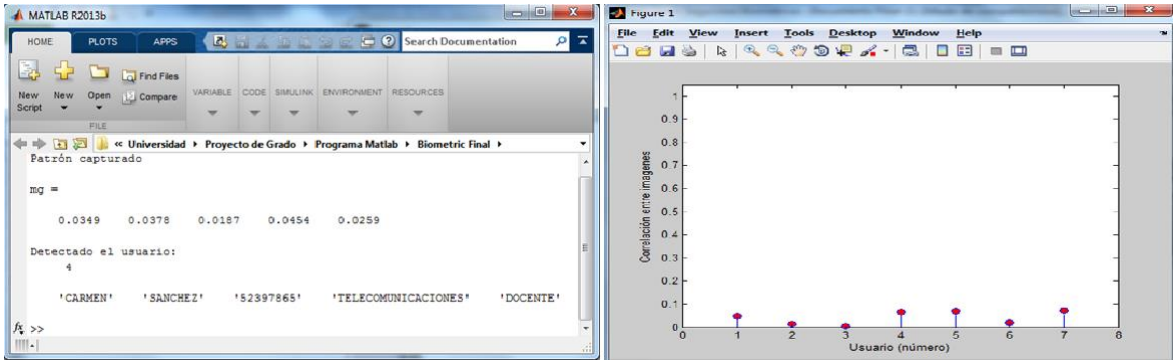


Figura 49. Información correspondiente a un usuario registrado con su índice de correlación por debajo del 10%.[71]

Otro error que se presenta, es cuando un usuario registrado en la base de datos, intenta identificarse ante el sistema, pero en la fase de autenticación muestra la información correspondiente a otro usuario. En la Figura 50 y 51 se puede observar el problema mencionado.

[70] Fuente propia
[71] Fuente propia

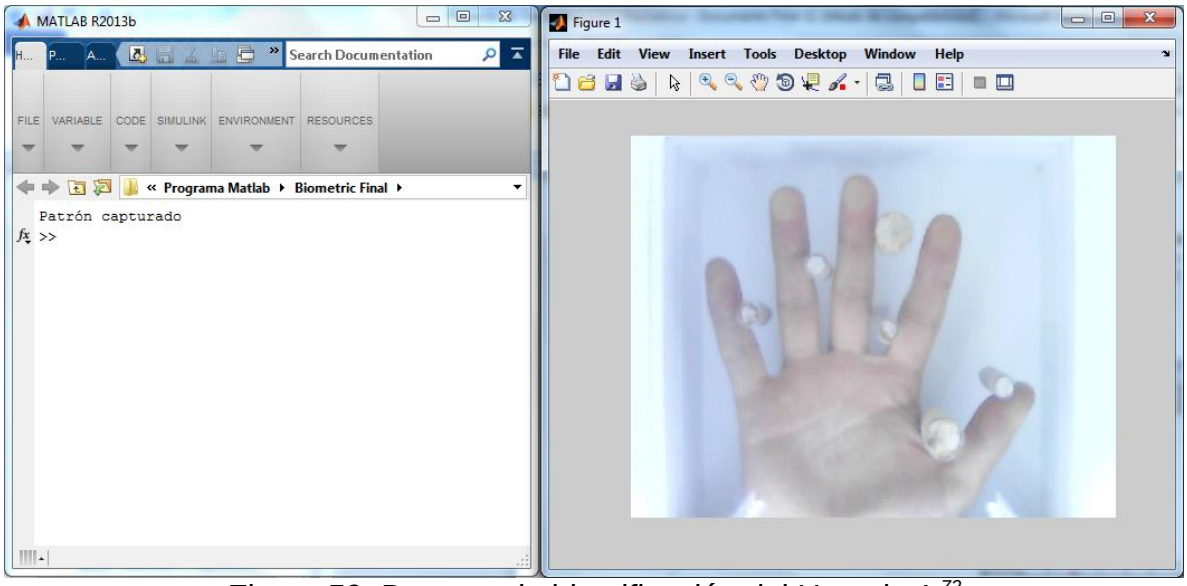


Figura 50. Proceso de identificación del Usuario 1.[72]

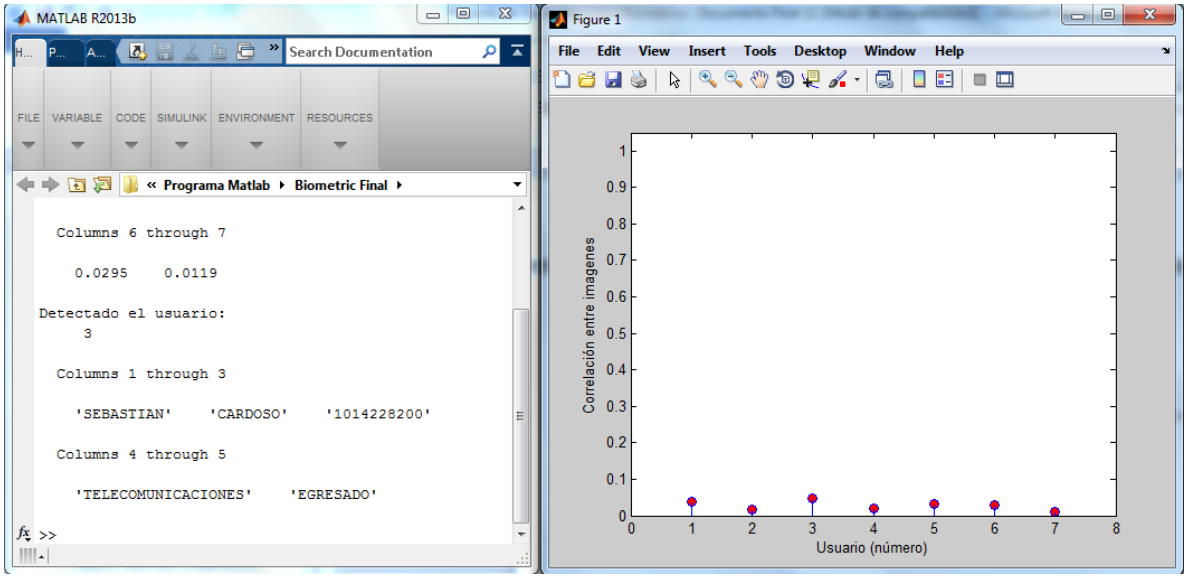


Figura 51. Error generado cuando el Usuario 1 se autentica y se muestra la información del Usuario 3.[73]

[72] Fuente propia
[73] Fuente propia

8. RECURSOS

Los recursos utilizados para el desarrollo del Proyecto de Grado se discriminan de la siguiente manera:

8.1 Recursos Humanos

N°	Profesión	Nombre
1	Tutor Guía Documentación	Ing. Ana María Cagua
2	Tutores Desarrollo Técnico	Ing. Nelson Forero
3	Tutores Externos Desarrollo Software	Ing. Rene Abadía

Tabla 4. Recursos Humanos.[74]

8.2 Materiales e Imprevistos

N°	Descripción	Costo
1	Papelería	$ 60.000
2	Tutorías	$ 130.000
3	Viáticos	$ 340.000
4	Dummy del Prototipo	$ 90.000

Tabla 5. Materiales e Imprevistos.[75]

8.3 Hardware y Software

N°	Descripción	Costo
1	Computador Portátil	$ 1.500.000
2	Cámara Web HD	$ 87.000
3	Impresora	$ 120.000
4	Licencia Software Matlab	$ 267.000

Tabla 6. Hardware y Software.[76]

[74] Fuente propia
[75] Fuente propia
[76] Fuente propia

9. CONCLUSIONES Y TRABAJO FUTURO

La necesidad de seguridad es algo que hoy en día nos importa a todos en los diferentes campos y entornos en los cuales nos vemos involucrados a diario. Por esta razón se hizo prescindible seguir ampliando y mejorando las técnicas de seguridad biométrica, debido a que cada vez el mundo se está automatizando y crece el deseo de aumentar y mejorar los métodos de identificación y de autentificación frente al fraude de identidad que actualmente se presenta.

La singularidad de la geometría de la mano de un individuo es una hipótesis en desarrollo que en el sentido matemático es difícil, más no imposible de probar. Ya que es más factible demostrar lo contrario cuando queremos encontrar dos manos idénticas. Hasta el momento no se ha encontrado dos manos idénticas que provengan de diferentes individuos.

La importancia que implicó desarrollar este proyecto, fue buscar la manera de omitir que la comunidad perteneciente a la Universidad Piloto de Colombia sigan utilizando mecanismos de acceso (tales como el carnet, tarjetas de acceso, entre otros) para permitir el ingreso a los recursos e instalaciones del plantel. Por tal motivo se determinó desplegar un mecanismo biométrico, lo que permite ser más óptimo, eficiente y dinámico para cada usuario.

A través de esta mejora se logró mostrar una metodología completa para desarrollar un sistema biométrico utilizando la geometría de la mano de un individuo, basado en las características de las líneas de contorno y las dimensiones que posee la palma de la mano. De esta manera, mediante la realización de diferentes pruebas piloto con diferentes usuarios del plantel, se comprobó que el sistema biométrico cumple satisfactoriamente, pues como se puede ver en los resultados, el sistema demuestra ser confiable, seguro y muy fácil de implementar, lo que implica que cumple con las condiciones exigidas para un sistema biométrico de alta fidelidad. Además, para la implementación del modelo de prototipo no se requirió de tecnología electrónica muy costosa y así mismo se hace eficiente el uso de recursos tecnológicos para el desarrollo sostenible.

Como trabajo futuro, respecto al almacenamiento de datos e información, es necesario implementar un sistema de almacenamiento y registro diferente al actual, ya que éste último, no se considera eficaz y seguro, debido a que puede haber pérdida de información o la manipulación errónea de la misma. En cambio, si se usa un sistema de base de datos como lo es SQL SERVER de Microsoft, permitiría integrar una mayor seguridad en la información, y además una fácil recuperación (por medio de backup) de ésta, ya que no estamos exentos a un agente externo que implique una pérdida parcial o total de la misma.

En cuanto al diseño, se pretende mejorar en lo que respecta a la interfaz gráfica para que esta sea más amigable y cómoda para el usuario final, mostrando una mejor interacción en el proceso de identificación. Adicionalmente, si con el paso del tiempo se identifican vulnerabilidades en el sistema biométrico, el código desarrollado permite tener variaciones para que los patrones y/o características que se están analizando, puedan ser modificadas para darle mayor robustez, tanto así que se podría dar una dualidad para que el sistema analice otros patrones biométricos, tales como la huella dactilar o el reconocimiento facial.

BIBLIOGRAFÍA

[1] Base de Datos Interoperable para Biometría de la Mano Ester González, Aythami Morales, Miguel A. Ferrer. Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones. Departamento de Señales y Comunicaciones. Universidad de Las Palmas de Gran Canaria. Disponible en: (http://jrbp10.unizar.es/papers/S4.C1.pdf)

[2] Electronic Privacy Information Center. Biometric Identifiers. Disponible en: (http://epic.org/privacy/biometrics/)

[3] INFOTIC Soluciones Inteligentes. Tecnología Biométrica, seguridad para móviles. Disponible en: (http://infotic.co/blog/articulo/tecnologia-biometrica-seguridad-para-moviles,461)

[4] Pablo Yglesias. Los Problemas de la Verificación Biométrica. Disponible en: (http://www.pabloyglesias.com/los-problemas-de-la-verificacion-biometrica/)

[5] Plataforma Biométrica Homini. Disponible en: (http://www.homini.com/new_page_5.htm)

[6] Privacy International. Report: Una guía de privacidad para Hispanohablantes. Chapter: Sistemas de identificación y cedulas de identidad. Disponible en: (https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes/sistemas-de-identificacion-y-cedulas-de)

[7] Revista Cloud Computing. Archivos de la Etiqueta: Seguridad Biométrica. Disponible en: (http://www.revistacloudcomputing.com/tag/seguridad-biometrica/)

[8] SBD SecurityByDefault.com.Hackeos Memorables: Sistema Biométrico con Gominolas. Disponible en: (http://www.securitybydefault.com/2009/10/hackeos-memorables-sistema-biometrico.html)

[9] UNAM - Facultad de Ingeniería Biometría Informática. Capítulo II. Bases Teóricas y Sistemas Biométricos. Disponible en: (http://redyseguridad.fi-p.unam.mx/proyectos/biometria/basesteoricas/caracteristicasindicador.html)

[10] Universidad Tecnológica Equinoccial Facultad de Ciencias de la Ingeniería Escuela de Informática y Ciencias de la Computación. Tesis: Sistema Biométrico de Reconocimiento de Huellas Digitales. Sisbiorhed. Disponible en: (http://repositorio.ute.edu.ec/bitstream/123456789/5634/1/34215_1.pdf)

ANEXOS

ANEXO A. Código Fuente Matlab CamCapture

```
function CamCapture
    clc, clear all, close all

   global video vidRes nBands hImage edit
   set(gcf,'MenuBar','none','name','Control Biométrico','numbertitle','off')

   % Información adaptador
   imaqhwinfo('winvideo',1);

   % Acceder al adpatador de video de Windows
   video = videoinput('winvideo',1,'YUY2_640x480');

   % Capturar la información de video
   set(video, 'ReturnedColorSpace', 'RGB');
   vidRes = get(video, 'VideoResolution');
   nBands = get(video, 'NumberOfBands');
   hImage = image(zeros(vidRes(2), vidRes(1), nBands) );

   % Mostrar video en ventana
   preview(video, hImage);

   % Buttons
   x=220; y=15; w=50; h=25; f=12;
   edit = uicontrol('Position',[x,y,w,h],'Style','edit','FontSize',f);
   uicontrol('Position',[x+w+5,y,1.5*w,h],'String','Capture',...
      'FontSize',f,'CallBack',@Capture);

end

function Capture(~,~)

   global video edit
   frame = getsnapshot(video);
   i = get(edit,'String');
   in = str2double(i);
```

```
    if isnan(in)
        disp('Número inválido')
    else
        filename = {'Images\Usuario',i,'.jpg'};
        filename = strjoin(filename,'');
        imwrite(frame,filename);
        fprintf('Usuario %1.0f registrado.\n', in);
    end

end
```

ANEXO B. Código Fuente Matlab Hand

```
function Hand
    clc, clear all, close all

    global n video vidRes nBands

    % Modificar numero de usuarios
    n = 11;


    % Información adaptador
    imaqhwinfo('winvideo',1);

    % Acceder al adpatador de video de Windows
    % Y escoger resolución
    video = videoinput('winvideo',1,'YUY2_640x480');

    % Capturar la información de video
    set(video, 'ReturnedColorSpace', 'RGB');
    vidRes = get(video, 'VideoResolution');
    nBands = get(video, 'NumberOfBands');

    % Mostrar video en ventana
    hImage = image(zeros(vidRes(2), vidRes(1), nBands) );
    preview(video, hImage);

    h = gcf;
    set(h,'KeyPressFcn',@KeyDown);

end

function KeyDown(obj, evt)

    global video
    x = get(obj,'CurrentCharacter');

    % Capturar y mostrar fotograma
    if x==' '
        disp('Patrón capturado')
        stoppreview(video)
        frame = getsnapshot(video);
        image(frame), axis off
```

```
        % Guardar fotograma
        imwrite(frame,'Images\capturaX.jpg');

        Reconocer

    end

end

function Reconocer

global n

A = imread('Images\capturaX.jpg');

% Supresión de frecuencias de color
Ag = rgb2gray(A);

Ag = imadjust(Ag,[0 1],[1 0]);
%imcrop(Ag);

% Transformada de Fourier en dos dimensiones
I = fft2(double(Ag));   % Matriz compleja
%surf(abs(I));


% Autocorrelación matricial
m(n+1) = mean(max(corr(I,I)));

% Comparación iterativa de imágenes
for i = 1:n
    % Cadena de caracteres con nombre de archivo
    archivo = ['Usuario',num2str(i),'.jpg'];

    % Cargar archivo de imagen temporal
    t = imread(['Images\',archivo]);

    % Supresión de frecuencias de color
    tg = rgb2gray(t);

    tg = imadjust(tg,[0 1],[1 0]);
%imcrop(tg);


    % Transformada de Fourier de imagen temporal
```

```
    Ft = fft2(double(tg));

    % Comparación iterativa con imagen capturada
    m(i) = mean(max(corr(Ft,I)));

end

% Correlación a graficar
mg = abs(m(1,1:n))
if max (mg)< 0.10
    disp('Usuario desconocido')
else

% Gráfica de Correlación
x = 1:n;
h = stem(x,mg,'fill','--'); grid off;
set(get(h,'BaseLine'),'LineStyle',':')
set(h,'MarkerFaceColor','red')

%Formato de la gráfica
xlabel('Usuario (número)');
ylabel('Correlación entre imagenes');
axis([0 n+1 0 1.05]);

[value NumUser] = max(mg);
disp('Detectado el usuario: '); disp(NumUser);

Datos(NumUser)
end
end

function Datos(NumUser)
    % Para aumentar base cambiar rango
    [Num Txt] = xlsread('Usuarios UPC.xlsx',1,'A2:F12');
    disp(Txt(NumUser,:));
end
```