Seguridad basada en la persona: Análisis de identificación biometría vascular

Aldo García 1, Isaid García 1

1 facultad de ciencias de la computación, Avenida San Claudio

72592 Puebla, México

[{isaid.garcia@alumno.buap.mx](mailto:%7bisaid.garcia@alumno.buap.mx), aldo.garciape@alumno.buap.mx}

**Abstract.** La biometría, una disciplina en crecimiento dentro del campo de la seguridad informática, se basa en la utilización de características físicas o comportamentales únicas de los individuos para su identificación. Este estudio ofrece una revisión exhaustiva de los métodos biométricos más destacados, centrándose en las características físicas como huellas dactilares, iris, geometría de la palma de la mano y reconocimiento facial. Este documento muestra los métodos biométricos, sus principios de funcionamiento y su aplicación en sistemas de seguridad informática. La comprensión de estas tecnologías es fundamental para el diseño y la implementación efectiva de sistemas de identificación biométrica seguros y confiables en una amplia gama de aplicaciones.

1 biometría como método de autentificación

La biometría es la ciencia que estudia los métodos de registro e identificación de seres humanos mediante el reconocimiento de características únicas biológicas, físicas o conductuales. Se sabe que los comerciantes chinos utilizaban las estampas de las huellas de las manos en papel con tinta como método de identificación ya en el siglo XIV. La identificación biométrica no se empezó a utilizar en occidente hasta el siglo XIX, que fue cuando comenzó su uso con fines policiales. Al principio la identificación se hacía muy elemental, confiando en la memoria, hasta que, en 1883 Alphonse Bertillon, destacado médico y estadístico y miembro de la policía parisina, desarrolló su sistema antropométrico de clasificación. Este método fue el primer sistema preciso y ampliamente utilizado para la identificación de criminales. Incluía las medidas de largo y ancho de la cabeza, largo del pie izquierdo o el largo del antebrazo del individuo, así como el registro de marcas personales como tatuajes o cicatrices.

Según los organismos de normalización ISO e IEC, la biometría es «el reconocimiento automatizado de individuos basado en sus características biológicas y de comportamiento». Estas características incluyen huellas dactilares, rasgos faciales e incluso el sonido de la voz de una persona. Los dispositivos, por su parte, son las herramientas o instrumentos utilizados para recoger y analizar datos, por lo que los dispositivos biométricos son las herramientas utilizadas para recoger y analizar estas características. [1]

Usualmente la identificación de los individuos se puede realizar a través de: objetos (carnet de identidad, tarjeta de identificación, etc.); conocimientos (claves personales, preguntas secretas, etc.); atributos conductuales (firma, forma de teclear, etc.); atributos físicos (huellas dactilares, iris, retina, rostro, etc.); otros atributos (voz, ADN, etc.). [2]

La identificación biométrica se basa en el uso de las características físicas o de comportamiento de las personas. En las décadas finales del siglo XX y en los inicios del XXI, los sistemas automáticos capaces de confirmar identidades de personas mediante técnicas biométricas han cobrado importancia. Sus tasas de error y posibilidad de fraude han hecho que entidades importantes como los órganos de seguridad del Estado y las entidades bancarias se hayan fijado en estos sistemas y los implementen en sus actividades con mayor frecuencia.[3]

Más que nuestra firma, huella digital o incluso voz, nuestra cara es la forma más fundamental de identificación. Con la tecnología ahora capaz de capturar, analizar y comparar datos sobre la distancia entre la frente y el mentón, o el contorno de las cuencas de los ojos, tomamos la aplicación del reconocimiento facial de manera muy personal. Y con razón. En la economía en línea, donde la actividad se realiza de forma remota, la autenticación e identificación confiables pueden ser difíciles de lograr. Un correo electrónico no es una prueba de identidad segura, las personas olvidan las contraseñas y los PIN, razón por la cual la atención se ha dirigido a alternativas biométricas y al potencial del reconocimiento facial.[4]

La inseguridad de ciertos datos nos lleva a pensar que para identificar a una persona no basta con una contraseña o un PIN, para realizar alguna acción importante como acceder a una cuenta bancaria o realizar una compra se deben buscar métodos que no impliquen el uso de una llave sino más bien que la llave sea el propio usuario.

## 2 Tipos de identificación biométrica

### 2.1 Reconocimiento facial

Para hablar de características que distinguen la cara de una persona del resto, podemos tomar elementos como: anchura y distancia entre elementos, color, arrugas y seguir enlistándolas hasta llegar a más de 80 características, pero los sistemas de reconocimiento no los usan todos, las características de un rostro se evalúan y se almacenan como un código numérico en una base de datos para comparar. Por lo tanto, se puede decir que el software trabaja de forma numérica y no de manera visual. El conjunto de datos que identifican a un individuo se le llama faceprint.[5]

**Figura 1.** La distancia entre los puntos nodales determina el faceprint[4]



Cuando esta tecnología era nueva, se tenían algoritmos de reconocimiento muy simples, esto daba pie a errores donde los sistemas podrían confundir 2 rostros de personas diferentes. Actualmente, este margen de error se ha reducido al punto de que estas fallas han sido mínimas, porque la forma en la que se reconocen rostros ha cambiado. El reconocimiento facial en base a imágenes 2D es una de las aplicaciones más investigadas en el reconocimiento de patrones y procesamiento de imágenes.

El procesamiento digital de imágenes o PDI son los diferentes métodos o algoritmos para editarlas mediante un ordenador. No existe aún un acuerdo Sobre los límites entre el PDI y las áreas relacionadas como el análisis de imágenes o la visión computacional, una forma de distinguir entre ambas es tomar en cuenta que los métodos de PDI hacen referencia a aplicar transformaciones utilizando operaciones primitivas como son la reducción de ruido, realce de contraste o refinamiento de una imagen, mientras que el análisis de imágenes se encarga de convertir una imagen en atributos como lo pueden ser texturas, o mediciones de objetos, esto implica la segmentación de los distintos elementos que conforman la imagen, haciendo un análisis de algún objeto en particular. Por último, la visión computacional interpreta los objetos y les asigna etiquetas según su reconocimiento, asociado con las funciones cognitivas de la vista. [6]

En el proceso de reconocimiento se utilizan algoritmos (analiza cientos de rostros y utiliza un mapeo facial que capta 100 expresiones faciales) para el procesamiento de imágenes, todas las imágenes tienen 50 x 50 pixeles de ancho y alto, y una direccionalidad de 2500 pixeles, por lo que su costo computacional aumenta.[7]

Algunos de los algoritmos de reconocimiento más eficientes de la actualidad se encuentran los siguientes:

**Métodos de concordancia holística:**

Para estos métodos es necesario tener información del rostro completo

Eigenfaces. Es un método que utiliza como datos de entrada valores de pixeles de varias imágenes faciales, y a partir de este conjunto de imágenes crea nuevas variables buscando las direcciones de varianza al original.

El método adaptativo basado en eigenespacio Evolutionary Pursuit, este hace uso de algoritmos genéticos para codificar y clasificar las imágenes

Sin embargo, la información obtenida con estos métodos puede llegar a ser poco precisa.

Teniendo en cuenta las técnicas de extracción de características se analizaron algunas de las componentes que existen:

• PCA (Principal Component Analysis)

• LDA (Linear Discriminant Analysis)

• LPP (Locality Preserving Projections)

• DCT (Discrete Cosine Transform) [8]

En la PCA es un algoritmo de reducción dimensional que permite encontrar los vectores que mejor representan la distribución y clasificación de un grupo de imágenes. El objetivo de este consiste en representar una imagen en términos de un sistema de coordenadas óptimo reduciendo el número final de componentes que tendrá la imagen.

En tanto, LDA se desempeña cuando las mediciones realizadas en variables independientes para cada observación son cantidades continuas. El objetivo es proyectar un conjunto de datos en un espacio de menor dimensión con una separabilidad de clases para evitar la sobre equipación y también reducir los costos computacionales. Cuando se trata de variables categóricas independientes, la técnica equivalente es el análisis de correspondencia discriminante.[9]

En el LPP monta gráficos que incluyen información de vecindario como el conjunto de datos. La representación de gráficos es generada por el algoritmo puede ser visto como una aproximación discreta lineal a un con que surge naturalmente de la geometría del colector.[10]

En el DCT brinda una transformación de secuencia finita de datos como la suma de funciones coseno oscilando en diferentes frecuencias.

En la DCT se obtienen las características de la imagen y luego se usan para poderlas clasificar, como se hace con PCA, por lo que la base de la DCT independientemente de las imágenes.

Etapas del Reconocimiento Facial

Al incluir los sistemas de reconocimiento facial, se rescatan cinco etapas:

1. Detección del rostro.

2. Acondicionamiento.

3. Normalización.

4. Extradición de características.

5. Reconocimiento. [11]

La detección, localiza la región facial (si existe) y la segmentación de esta del resto de la escena. El acondicionamiento localiza las componentes y la escala a la que encontramos al rostro, mediante trasformaciones geométricas.

Después, la normalización consiste en normalizar las imágenes en la etapa de preprocesado para atenuar los efectos de los cambios de iluminación, es decir, igualar en tamaño, intensidad de un rango determinado entre otras y así realizar un escalado y recortar con un rectángulo o elipse.

La determinación de características aporta información necesaria para diferenciar los rostros diferentes de las personas según sulas variaciones geométricas. Por último, el reconocimiento da el patrón facial extraído de las características y se compara con la base de datos. Si se da un 90% de similitud, entrega la identidad del rostro, o si no, se indica que es un rostro desconocido.

**Tabla 2.** Tabla que describe algunos usos que pueden tener la biometría en la vida cotidiana [12]

|  |  |
| --- | --- |
| Usos | Descripción |
| Prevención del crimen | Prevenir y reducir robo de mercancía en centros comerciales, comparando el rostro los individuos que ingresan con bases de datos privadas que contienen las plantillas previamente almacenadas de individuos que han sido acusados de hurto con anterioridad. |
| Desbloque de dispositivos | Celulares o tabletas hacen uso de esta tecnología para verificar la identidad de quien intenta acceder a ellos. |
| Mercadeo y publicidad | Estrategias de mercadeo según su audiencia objetivo, utilizando esta tecnología para identificar factores decisivos como género y edad. |
| Asistencia a personas con condición de discapacidad | Aplicaciones que alertan a las personas con discapacidad visual cuando alguien está sonriendo a través de una vibración para ayudarles a comprender mejor las situaciones sociales. |
| Redes sociales | Identificar personas en las fotos que se suben a las plataformas. |
| Diagnosticar enfermedades | Detección de enfermedades que ocasionan cambios en la apariencia de las personas. |
| Transacciones seguras | Opción de realizar transacciones únicamente con el escaneo del rostro. |

### 2.2 Reconocimiento de firmas

Es la tecnología biométrica menos problemática, en la actualidad resulta la más difundida en el mundo ya que, entre otras ventajas, es muy económica si se requiere implementar. Un sistema de este tipo solo necesita una tableta de escritura conectada al computador. El escaneo de la firma se analiza desde dos puntos de vista, siendo estos la firma en sí y el modo en que se efectúa. Los datos almacenados incluyen la velocidad, la presión, la dirección, el largo del trazado y las áreas donde el lápiz se levanta. El gran inconveniente de este método es que una persona nunca firma de manera idéntica dos veces.[13]

Las firmas pueden adquirirse de dos maneras, estática y dinámica.

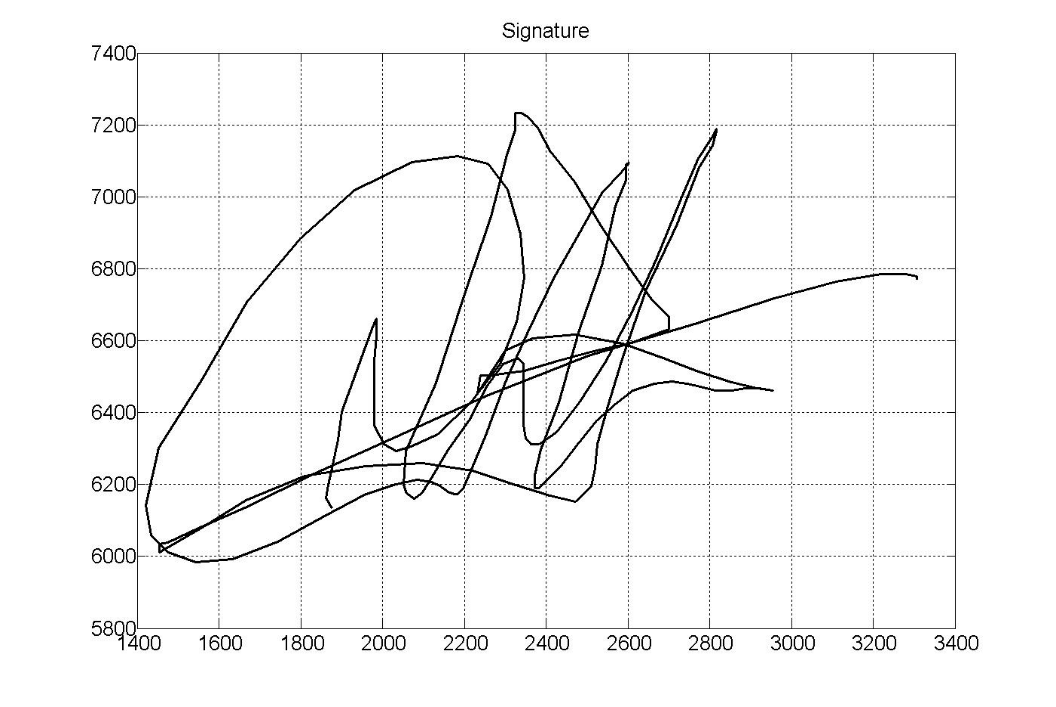
La modalidad estática implica la digitalización de una firma manuscrita a partir de una muestra obtenida en papel. Esta técnica es también conocida como off-line, convierte la firma en un formato digital sin considerar su evolución temporal.

Por otra parte, la modalidad dinámica implica capturar la firma haciendo uso de dispositivos especiales que registran la evolución temporal de varias señales generadas por el lápiz al firmar. Así como también las coordenadas posicionales, estos dispositivos pueden proporcionar información útil adicional, como lo es la presión ejercida sobre el plano de escritura y los ángulos formados entre el lápiz y superficie de escritura.[14]

Para crear un modelo de una firma esta se representa de forma paramétrica o mediante funciones, las características a tomar en cuenta para realizar una representación paramétrica son: velocidad de escritura, máxima, mínima y media. Velocidades de escritura en diferentes ejes cartesianos, duraciones globales y locales del tiempo en contacto con el bolígrafo o papel, relación de aspecto, porcentaje de pixeles y densidades de probabilidad de pixeles en distintas direcciones.

Para crear un modelo mediante funciones se debe analizar la evolución de ciertos parámetros a lo largo de la captura de la firma, por lo tanto, este método solo funciona con firmas tomadas en línea, algunas funciones temporales son: posición, precisión, fuerza y ángulos instantáneos del bolígrafo, velocidades y aceleraciones de los parámetros anteriores.[15]

**Figura 2.** Grafica de ejemplo de una firma a analizar [16]



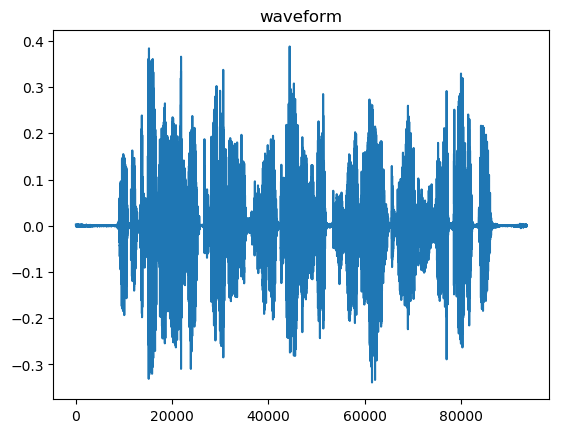
### 2.3 Reconocimiento de voz

El análisis de la voz inicia a mediados de la década de los años 60. El habla se considera como uno de los sistemas biométricos más eficaces, debido a su naturalidad. Se ha podido comprobar que los patrones con que una persona dice una palabra son únicos. El reconocimiento de voz funciona mediante la digitalización de diferentes palabras de una persona. Cada palabra se descompone en segmentos, de los cuales se obtienen 3 o 4 tonos dominantes que son capturados en forma digital y almacenados en una tabla o espectro, que se conoce con el nombre de plantilla de la voz (voice print).

En los primeros días del desarrollo de sistemas de reconocimiento de voz, se establecieron sistemas basados en diálogos discretos, donde se utilizaba un lenguaje hablado marcado por pausas y con un límite de palabras no superior a 50. Con el transcurso del tiempo, se dio inicio al trabajo en sistemas de conversaciones continuas que prescindían de pausas entre palabras, gracias a la implementación de técnicas destinadas a minimizar las discrepancias en la velocidad del habla. Con el tiempo, se introdujeron nuevas y más avanzadas técnicas, lo que llevó a los sistemas de reconocimiento de voz a desempeñar un papel significativamente más destacado en diversas industrias de renombre. [17]

Los sistemas de reconocimiento de voz tienen dos módulos principales: el de extracción y el de comparación. La extracción extrae los datos de señales sonoras de un individuo que luego se usarán para identificarlo. La comparación de características implica el reconocimiento de una persona a partir de su voz comparándola con las conocidas por el sistema. [18]

**Figura 3.** Vista grafica de ondas de sonido de una voz.[19]



### 2.4 Reconocimiento de huellas dactilares

El reconocimiento de huellas dactilares es otra de las técnicas más usadas a nivel mundial.[18] Está basado en el desarrollo realizado por John Evangelist Purkinje quien en 1823 realizó los primeros estudios de las huellas dactilares; años más tarde (1980) Sir Francis Galton comenzó sus observaciones para utilizar las huellas como identificadores personales. En el año de 1892 Galton publicó su libro "Fingerprints" en el que afirmaba que las huellas dactilares eran únicas y que no cambiaban a lo largo de la vida; Galton también estableció un sistema de clasificación de las huellas dactilares.

La huella dactilar está compuesta por crestas papilares, y surcos Inter papilares, el origen de las crestas papilares tiene sus orígenes en el aporte genético y el ambiente en el que se desenvuelve el feto, por lo tanto aunque parte de las características de la huella dactilar se forman a partir del material genético, también es cierto que factores como nutrición, presión sanguínea, líquido amniótico, temperatura y posición del feto terminan por darle forma y aspecto a la huella. [20]

**Figura 4.** Líneas de una huella dactilar.



La distintividad es la ventaja de las huellas dactilares en su uso biométrico, porque se ha comprobado que incluso en gemelos las huellas dactilares y sus patrones son diferentes, hasta ahora no hay pruebas de huellas dactilares idénticas. La permanencia es otro factor que juega a favor de las huellas, ya que es algo con lo que se nace y se mantiene hasta la muerte.

La facilidad con la que se pueden tomar muestras o registros de este tipo es más fácil que el de otros métodos, y por supuesto, conlleva también a una alta aceptación por parte de las personas a que la mayoría accede a que los bancos usen sus registros dactilares para identificar.

En la actualidad la forma más común de obtener los registros dactilares de una persona es a través de la toma de imágenes en tiempo real, a este método se le conoce como live-scan, en la mayoría de los dispositivos de la actualidad los sensores utilizados para este trabajo son: Sensores ópticos: los cuales convierten los patrones de la huella en señales digitales.

Sensores capacitivos: utilizan sensores de silicona que convierten los datos en una imagen en escala de grises de 8 bits.

Sensores de ultrasonido: esta es la tecnología más precisa para la captura de huellas dactilares, con este método se usan ondas de ultrasonido las cuales regresan imágenes de alta resolución.[21]

A pesar de que las huellas dactilares han sido un gran mecanismo de identificación también es importante reconocer los peligros y vulnerabilidades que estos podrían presentar, tal es el caso de los ataques hill-climbing, donde se generan patrones con características de huellas dactilares aleatorios, estos patrones se modifican de forma iterativa hasta llegar a un parecido al de la huella humana real. [22]

### 2.5 Reconocimiento del Iris

El uso del Iris como método de identificación biométrica no es un descubrimiento reciente, lo propuso hace más de un siglo Alphonse Bertillon (1885), quien estableció métodos de clasificación según datos recabados de personas para identificarlas. Sin embargo, no fue hasta 1987 que los oftalmólogos Leonard Flom y Aran Safir obtuvieron una patente por sus trabajos sobre estudios en el iris como medida de identificación. [23]

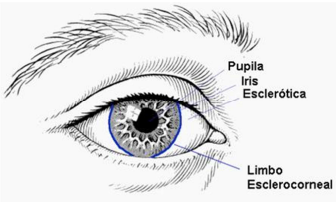
En el reconocimiento y análisis de patrones algunos métodos como el facial pueden llegar a ser inexactos o tener una gran variabilidad generando problemas para ubicar ojos, nariz, boca, etc. Incluso otros factores como gestos, maquillaje, accesorios y el envejecimiento pueden modificar la información o registros que se tenían, por eso el Iris como método de identificación biométrica es más confiable, tiene una variabilidad enorme y se mantiene casi sin cambios.

El iris es un órgano interno del ojo cuya ubicación se encuentra por detrás de la córnea y el humor acuoso, se puede decir que es aquel que diferencia el color de ojos de cada persona.

La característica más importante y que comparte en común con la huella dactilar es la morfología aleatoria de su estructura. El órgano no tiene alteración genética más allá de su forma anatómica, color y apariencia. El iris tiene más ventajas sobre las huellas digitales y otros métodos de identificación biométricos, la facilidad de registrar su imagen a ciertas distancias sin necesidad de contacto físico o intrusivo, su aleatoria estructura y su estabilidad durante la vida del individuo donde no se alterará son factores que favorecen este método biométrico.

Para tomar los registros se toma una imagen del iris de la persona. Posteriormente la imagen es procesada para ajustar su tamaño, esto debido a que el iris puede ser deformado por la dilatación de la pupila, luego la información es convertida a un código que representa el iris.

**Figura 5.** Partes externas del ojo humano



Según esto, se comparan códigos y, según el porcentaje de similitud, se confirma si el iris comparado es de la misma persona.

Como regla general el reconocimiento de personas puede trabajar de dos maneras, Autentificación o identificación, en el primero el Iris es comparado con el código de registro de la identidad y se llega a la conclusión de si ambos códigos han sido generados a partir del mismo Iris.

En el segundo, el código del iris recolectado busca coincidir en una base de datos para encontrar la identidad de la persona.

Uno de los mayores desafíos en el reconocimiento del iris es capturar una imagen de alta calidad. Este es el paso más importante dentro de todo el procedimiento, ya que afecta significativamente el desempeño del sistema en su totalidad.[24]

### 2.6 Geometría de la mano

El reconocimiento de la palma de la mano es una modalidad biométrica que usa la estructura física de la palma de la mano de una persona para fines de identificación [25].

La geometría de la palma de la mano se utiliza como un método biométrico de identificación, aprovechando las características físicas únicas de la mano. Para su análisis se hace uso de las protuberancias largas y anchas conocidas como crestas, estas se encuentran separadas por lo que conocemos como valles. (Santiago Ramírez et al., 2013) Este sistema proporciona una alta confianza en el reconocimiento de individuos al capturar imágenes de la mano mediante un escáner controlado. La iluminación adecuada y la posición precisa de los dedos son fundamentales durante la captura de imágenes. Además, se aplican técnicas de procesamiento de imágenes, como segmentación y binarización, para obtener características especiales. Estas características se analizan utilizando algoritmos como el de Euclides y la geometría plana, que proporcionan parámetros de identificación y minimizan el tiempo de reconocimiento. Los datos se almacenan en una base de datos para su posterior comparación. El proceso de autenticación implica la captura de datos, la extracción de características, la comparación con la base de datos y la toma de decisión sobre la validez del usuario. Este sistema garantiza una baja probabilidad de errores, lo que lo convierte en un método altamente seguro de autenticación biométrica.

La palma de la mano es la parte que va de la muñeca hasta el inicio de los dedos. Esta parte muestra protuberancias largas y estrechas conocidas como crestas, separadas por espacios conocidos como valles. También presenta sur- cos y arrugas. Este conjunto de características es único y permanente para cada persona, por lo que permite realizar una identificación de forma confiable.[26]

La técnica basada en geometría del dedo se puede considerar como una simplificación de la basada en contorno de la Mano.[27]

Las manos humanas están compuestas por músculos flexores localizados en la cara inferior del antebrazo, estos están unidos a falanges a través de los tendones. Los músculos extensores se hallan en la parte exterior del brazo y están unidos de forma similar. La articulación de la mano en los humanos es más compleja y delicada que la de cualquier otro animal, porque se desarrolló para manipular herramientas y utensilios.[28]

Existen múltiples formas de implementar un sistema biométrico de este tipo, por ejemplo, los sistemas biométricos en base a la captura del dorso de la mano, este sistema obtiene las imágenes de tres formas, usando una banda visible, otra banda de 850nm y por último una banda de 1450nm. El proceso de captura inicia con un bombillo el cual ilumina las 3 bandas, después de esto 3 cámaras son colocadas en la parte superior de la mano, para capturar las imágenes en la banda visible se utiliza una webcam de 640x480 pixeles. Para la imagen de la banda de 850nm se usa otra webcam de 640x480 pixeles, sin embargo, esta esta modificada para funcionar como infrarrojo. Por último, para obtener la imagen en la banda de 1450nm se utiliza una cámara con un sensor AsGaln el cual es sensible en rangos dinámicos de 900 a 1700nm.

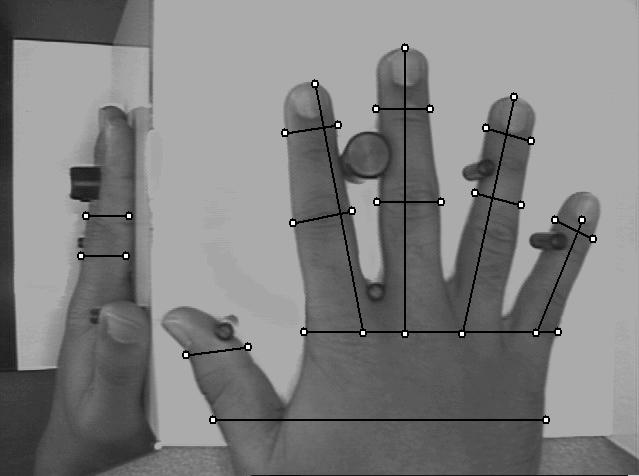
Otra forma de implementar la biometría con la geometría de la mano es en sistemas de captura por contacto, como ejemplo de los sistemas que funcionan según un escáner, el uso de los escáneres es fundamental y común. Los individuos deben colocar la mano sobre el escáner sin tocar los bordes del cristal y manteniendo los dedos firmes y extendidos.

Los sistemas multiespectral sin contacto son sistemas que fueron diseñados para la identificación por medio de la geometría de la mano sin tener contacto con el escáner, estos sistemas hacen uso de dos cámaras web, una es designada para tomar imágenes en la banda de 850nm y la otra en la banda visible. La cámara web que captura la banda 850nm es utilizada para capturar las partes de la mano que más expuestas están a la luz, su fin principal es obtener imágenes saturadas donde en el primer plano la mano se ve brillante y el fondo obscuro.

El sistema con cámaras independientes implementa una cámara a unos pocos centímetros de la mano, la cámara funciona como infrarrojo segmentando la mano para aumentar la capacidad de discriminación del dispositivo. La primera cámara se encarga de capturar imágenes de los dedos cada que el usuario acerca la mano, la otra cámara la cual trabaja con una banda visible se encarga de capturar solo imágenes de la palma de la mano.[29]

Aunque es cierto que la estructura de los huesos y las articulaciones de la mano son constantes, pero otras circunstancias, como una inflamación o una lesión, pueden variar la estructura básica de la mano dificultando la autenticación.[30]

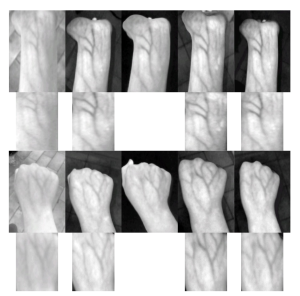
**Figura 6.** Geometría de la mano con ciertos parámetros extraídos.[31]



## 2.7 Reconocimiento a través de venas

El reconocimiento de personas mediante venas es una técnica relativamente reciente que aún no ha sido suficientemente estudiada y explotada en móviles. Hasta el momento, los dispositivos para captar las imágenes son bastante sofisticados y costosos.[32]

**Figura 7.** Fotografía de venas para su análisis[33]



Así, igual que ya está implantado el reconocimiento facial o por huella digital, se podrá implantar el sistema de comprobación por venas.

La aplicación se basa en el reconocimiento de los patrones vasculares que están formados por la estructura de los vasos sanguíneos dentro del cuerpo. Tradicionalmente, la adquisición de estos patrones vasculares se ha realizado iluminando la zona con luz infrarroja para obtener una imagen parecida a la de una radiografía. Los vasos se muestran oscuros ya que la hemoglobina absorbe la luz infrarroja y el resto de los tejidos aparecen claros.

Tanto las arterias como las venas se pueden emplear como rasgos biométricos, pero las venas son más fáciles de detectar y sus imágenes son más claras. Esto se debe a que, por un lado, hay más venas en el cuerpo humano y, por otro, están más cerca de la superficie de la piel.

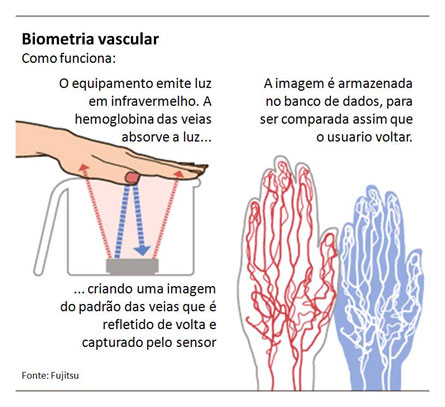
Para todo este proceso el formato de las venas es capturado a través del principio de la Transmitancia en la imagen, un proceso de diferencia de absorción de haces de luz del espectro infrarrojo (NIR – Near Infrarred y FIR - FarInfrarred), similar a la utilizada por las cámaras de circuito cerrado de televisión para su visualización en ambientes sin luz visible.

Por la composición sanguínea ferrosa, la hemoglobina presente en las venas y los capilares de la capa subcutánea absorbe más espectro infrarrojo que los tejidos musculares del cuerpo, y tienen la diferencia de absorción, de la Transmitancia.

Un sensor que detecta solo el espectro infrarrojo puede diferenciar lo que es tejido muscular y las venas y capilares. Este sensor puede ser una cámara CCD con un filtro de luz visible.

¿Cómo funciona? El equipo emite luz en infrarrojo. La hemoglobina de las venas absorbe la luz creando una imagen estándar de las venas, el cual es reflejado nuevamente y capturado por el sensor. La imagen es almacenada en el banco de datos, para ser comparada cuando el usuario vuelva a colocar su mano en el lector.[34]

**Figura 8.** Representación de cómo funciona el reconocimiento a través de infrarrojo.[34]



**Tabla 2.** Tabla que compara los diferentes tipos de identificación biométrica [35]

|  |  |  |
| --- | --- | --- |
| Técnica | Ventajas | Inconvenientes |
| Voz | Muy bajo costo ­En algunas aplicaciones puede resultar inapropiables para el usuario (por ejemplo, servicios telefónicos) | Rendimiento bajo. ­Se está estudiando el aumentar la unicidad y la estabilidad |
| Huellas | Muy estudiado/desarrollado ­Unicidad, estabilidad y rendimientos altos. ­Reconocimiento legal. ­Medio coste | connotaciones “policiales” para el usuario ­Detención de dedo vivo, depende de pruebas colaterales a la captura |
| Iris | Unicidad mayor que huella ­Gran estabilidad por protección de la córnea. ­FAR prácticamente nula. ­ Fácil detención de ojo vivo | Alto coste. ­Inicialmente incómodo para el usuario |
| Mano | Fácil uso y gran aceptación por el usuario. ­Medio coste. ­Bajo coste computacional. ­Sin connotación “policial” | unicidad y estabilidad no probadas en grandes poblaciones. ­Detención de mano viva, depende de pruebas colaterales |
| Rostro | Cómodo, e incluso inapreciable para el usuario. ­Medio coste | Sensible a cambios del sujeto (barbas, gafas, pelos.). Todavía en investigación y desarrollo |
| Firmas | Bajo costo  Fácil uso y buena aceptación | Sensible a cambios por el sujeto |

## 3 Implementacion del sistema biométrico vascular.

**3.1 Concepto:** Desarrollar una aplicación con tecnología de reconocimiento de venas para autenticar la identidad de los usuarios en escenarios, como control de acceso, autenticación de identidad en transacciones en línea y seguridad siempre.

Para desarrollar una aplicación para el reconocimiento de venas, desglosaremos cada paso de la metodología en tareas específicas, utilizando herramientas y tecnologías apropiadas.

**3.2 Metodología**

**1. Análisis de Requisitos**

Se busca crear una aplicacion que este diseñada para poder tener un metodo de verificacion basado en la tecnologia de reconicimiento de venas, esta aplicacion debe ser guiada atraves de una fotografia para la cual se comparara con venas guardadas previamente para poder verificar si se encuentra registrada y dar acceso o denegarlo.

**2. Investigación y Selección de Tecnología**

* **Sensores de Imagen:**

Flir Lepton: Seleccionado por su tamaño compacto y precisión adecuada para capturar imágenes de venas.

Seek Thermal CompactPRO: Seleccionado por su alta resolución y facilidad de uso.

* **Bibliotecas de Procesamiento de Imágenes:**

OpenCV: Seleccionada por su amplia funcionalidad y soporte comunitario.

* **Plataforma de Desarrollo:**

Python: Seleccionado para el prototipado y desarrollo de algoritmos iniciales.

Java/Kotlin: Seleccionado para la versión móvil de la aplicación.

* **Frameworks de Machine Learning:**

TensorFlow: Seleccionado para el desarrollo de modelos de reconocimiento debido a su robustez y herramientas de soporte.

* **Seguridad y Gestión de Datos:**

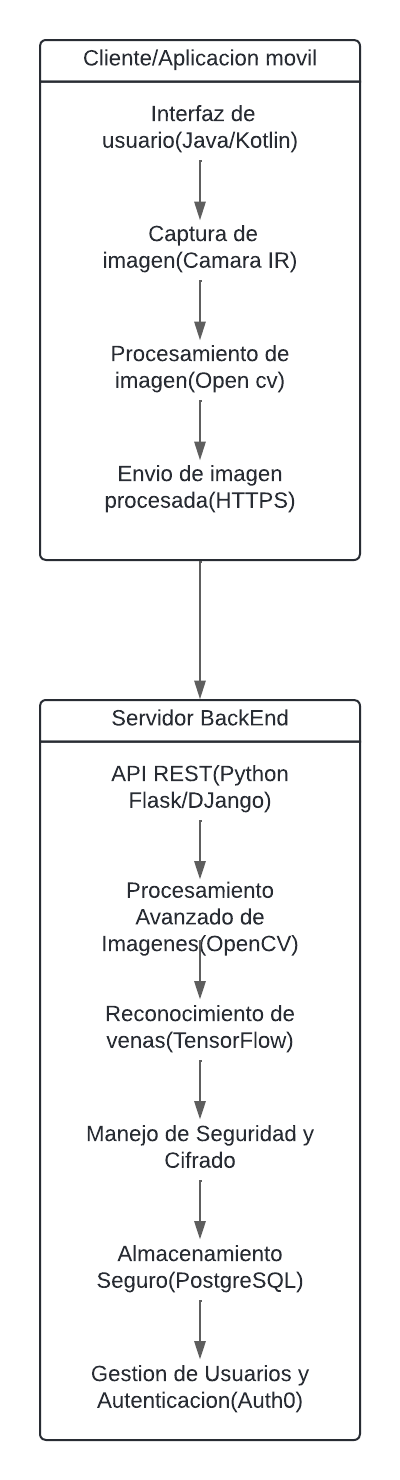
Cryptography: Seleccionado para el cifrado de datos biométricos.

Auth0: Seleccionado para la autenticación multifactor y gestión de usuarios.

**3. Arquitectura del Sistema**

**Diagrama de arquitectura.**

**Figura 9.** Diagrama de arquitectura



**Diseño de la base de Datos**

Tecnologia: PostgreSQL

### Algoritmo 1. Esquema de base de datos.

CREATE TABLE users (

user\_id SERIAL PRIMARY KEY,

username VARCHAR(255) UNIQUE NOT NULL,

password\_hash TEXT NOT NULL,

email VARCHAR(255) UNIQUE NOT NULL,

created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP

);

CREATE TABLE vein\_data (

vein\_id SERIAL PRIMARY KEY,

user\_id INT REFERENCES users(user\_id),

vein\_image BYTEA NOT NULL,

encrypted\_features BYTEA NOT NULL,

created\_at TIMESTAMP DEFAULT CURRENT\_TIMESTAMP

);

**4.- Diseño de la interfaz de usuario**

Tecnología: Java/Kotlin para la aplicación móvil

Wireframes:

* Pantalla de Inicio de Sesión

Campos: Correo Electrónico, Contraseña

Botón: Iniciar Sesión

* Pantalla de Registro

Campos: Nombre de Usuario, Correo Electrónico, Contraseña, Confirmar Contraseña

Botón: Registrarse

* Pantalla de Captura de Imagen

Botón: Capturar Imagen

Vista previa de la imagen capturada

Botón: Procesar y Enviar

* Pantalla de Resultados

Texto: Resultado del reconocimiento (éxito o fallo)

Botón: Intentar de Nuevo

**5.- Flujo de datos**

* **Captura de Imagen:**

La cámara infrarroja captura la imagen de la vena.

La imagen es procesada localmente usando OpenCV para mejorar el contraste y resaltar las venas.

* **Envío de Imagen Procesada:**

La imagen procesada se envía al servidor backend a través de una conexión HTTPS segura.

* **Procesamiento en el Servidor:**

El servidor recibe la imagen y realiza un procesamiento adicional si es necesario.

Utiliza TensorFlow para el reconocimiento de venas, comparando las características de la imagen con las almacenadas en la base de datos.

* **Manejo de Seguridad y Almacenamiento:**

Los datos biométricos y las características extraídas se cifran usando la biblioteca Cryptography.

Los datos cifrados se almacenan en PostgreSQL.

* **Gestión de Usuarios y Autenticación:**

El sistema utiliza Auth0 para manejar la autenticación multifactor y asegurar que solo usuarios autorizados puedan acceder a los datos.

**Captura y Procesamiento de Imágenes en la Aplicación Móvil (Java/Kotlin):**

### Algoritmo 2. Código de Captura y Procesamiento de Imágenes

// Captura de imagen utilizando la cámara

fun captureImage() {

val cameraIntent = Intent(MediaStore.ACTION\_IMAGE\_CAPTURE)

startActivityForResult(cameraIntent, REQUEST\_IMAGE\_CAPTURE)

}

override fun onActivityResult(requestCode: Int, resultCode: Int, data: Intent?) {

if (requestCode == REQUEST\_IMAGE\_CAPTURE && resultCode == Activity.RESULT\_OK) {

val imageBitmap = data?.extras?.get("data") as Bitmap

processImage(imageBitmap)

}

}

// Procesamiento de imagen usando OpenCV

fun processImage(image: Bitmap) {

val mat = Mat()

Utils.bitmapToMat(image, mat)

Imgproc.cvtColor(mat, mat, Imgproc.COLOR\_BGR2GRAY)

Imgproc.equalizeHist(mat, mat)

// Enviar la imagen procesada al servidor

sendImageToServer(mat)

}

**API REST en el Servidor (Python Flask):**

### Algoritmo 3. Código del API REST en el servidor

app = Flask(\_\_name\_\_)

key = Fernet.generate\_key()

cipher\_suite = Fernet(key)

@app.route('/upload', methods=['POST'])

def upload\_image():

file = request.files['image']

npimg = np.frombuffer(file.read(), np.uint8)

img = cv2.imdecode(npimg, cv2.IMREAD\_GRAYSCALE)

# Procesamiento y reconocimiento de la imagen

processed\_img = process\_image(img)

recognition\_result = recognize\_vein(processed\_img)

return jsonify({'result': recognition\_result})

def process\_image(image):

# Procesamiento de imagen con OpenCV

return cv2.equalizeHist(image)

def recognize\_vein(image):

# Uso de TensorFlow para reconocimiento

# Placeholder para el modelo

model = tf.keras.models.load\_model('vein\_recognition\_model.h5')

image = np.expand\_dims(image, axis=0)

predictions = model.predict(image)

return predictions[0].tolist()

if \_\_name\_\_ == '\_\_main\_\_':

app.run(ssl\_context=('cert.pem', 'key.pem'))

**Cifrado de Datos en el Servidor (Python):**

### Algoritmo 4. Código del Cifrado de Datos.

def encrypt\_data(data):

return cipher\_suite.encrypt(data)

def decrypt\_data(encrypted\_data):

return cipher\_suite.decrypt(encrypted\_data)

**4. Desarrollo del Prototipo**

**Configuracion del entorno de Desarrollo**

**Herramientas y Tecnologías:**

* Python: Para el desarrollo del backend y procesamiento de imágenes.
* Java/Kotlin: Para el desarrollo de la aplicación móvil.
* OpenCV: Para el procesamiento de imágenes.
* TensorFlow: Para el reconocimiento de venas.
* Flask: Para el backend.
* PostgreSQL: Para el almacenamiento seguro.
* Auth0: Para la autenticación.

**Desarrollo de la Aplicación Móvil (Java/Kotlin)**

**Captura y Procesamiento de Imágenes:**

* + Implementar la funcionalidad para capturar una imagen usando la cámara del dispositivo.
  + Procesar la imagen capturada para resaltar las venas usando OpenCV.

**Desarrollo del Backend (Python Flask)**

**API para Recepción y Procesamiento de Imágenes:**

* + Implementar un servidor Flask que reciba la imagen procesada desde la aplicación móvil.
  + Realizar procesamiento adicional en el servidor si es necesario.
  + Implementar el reconocimiento de venas utilizando un modelo de TensorFlow.

**Integración de Componentes**

**Integrar la Aplicación Móvil con el Backend:**

* + Enviar la imagen procesada desde la aplicación móvil al servidor backend.
  + Mostrar el resultado del reconocimiento en la aplicación móvil.

**5. Implementación de Algoritmos de Reconocimiento**

**Preparacion de datos**

**Recolectar y preprocesar imágenes de Venas**

### Algoritmo 5. Código para el preprocesar Imágenes

def preprocess\_image(image\_path):

image = cv2.imread(image\_path, cv2.IMREAD\_GRAYSCALE)

processed\_image = cv2.equalizeHist(image)

return processed\_image

image\_paths = glob.glob("path/to/vein/images/\*.jpg")

processed\_images = [preprocess\_image(path) for path in image\_paths]

# Guardar imágenes preprocesadas para su uso posterior

for idx, img in enumerate(processed\_images):

cv2.imwrite(f"path/to/processed/images/vein\_{idx}.jpg", img)

**Creacion del Modelo**

**Definir y Entrenar el modelo de TensorFlow**

### Algoritmo 6. Código del modelo de TensorFlow

# Definir el modelo

model = Sequential([

Conv2D(32, (3, 3), activation='relu', input\_shape=(128, 128, 1)),

MaxPooling2D((2, 2)),

Conv2D(64, (3, 3), activation='relu'),

MaxPooling2D((2, 2)),

Flatten(),

Dense(128, activation='relu'),

Dense(1, activation='sigmoid')

])

# Compilar el modelo

model.compile(optimizer='adam', loss='binary\_crossentropy', metrics=['accuracy'])

# Preparar los datos de entrenamiento

datagen = ImageDataGenerator(rescale=0.2)

train\_generator = datagen.flow\_from\_directory(

'path/to/processed/images',

target\_size=(128, 128),

batch\_size=32,

color\_mode='grayscale',

class\_mode='binary'

)

# Entrenar el modelo

model.fit(train\_generator, epochs=10)

# Guardar el modelo entrenado

model.save('vein\_recognition\_model.h5')

**Integracion del modelo**

**Cargar e Integrar el Modelo Entrenado en el Servidor Backend**

### Algoritmo 7. Integración del modelo entrenador al servidor.

def upload\_image():

file = request.files['image']

npimg = np.frombuffer(file.read(), np.uint8)

img = cv2.imdecode(npimg, cv2.IMREAD\_GRAYSCALE)

# Procesamiento de imagen

processed\_img = process\_image(img)

# Reconocimiento de venas

recognition\_result = recognize\_vein(processed\_img)

# Encriptar el resultado antes de almacenarlo

encrypted\_result = cipher\_suite.encrypt(str(recognition\_result).encode())

# Almacenar en la base de datos

store\_in\_database(encrypted\_result)

return jsonify({'result': recognition\_result})

def process\_image(image):

# Procesamiento de imagen usando OpenCV

return cv2.equalizeHist(image)

**Valacion del Modelo**

**Validar el Modelo con Nuevas Imágenes de Prueba**

### Algoritmo 8. Validación del modelo

test\_image\_path = 'path/to/test/image.jpg'

test\_image = cv2.imread(test\_image\_path, cv2.IMREAD\_GRAYSCALE)

processed\_test\_image = process\_image(test\_image)

recognition\_result = recognize\_vein(processed\_test\_image)

print(f'Resultado del reconocimiento: {recognition\_result}')

**6. Implementación de Medidas de Seguridad**

**Cifrado de Datos:**

Utilizaremos el cifrado para almacenar de forma segura los datos de las características de las venas en la base de datos.

**Uso de HTTPS:**

### Algoritmo 9. uso de HTTPS.

if \_\_name\_\_ == '\_\_main\_\_':

app.run(ssl\_context=('cert.pem', 'key.pem'))

Usaremos openssl para generar un certificado SSL y una clave privada.

### Algoritmo 10. Generacion de certificado SSL

openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 365

**Autenticacion y Autorización**

Usaremos Auth0 para manejar la autenticación y autorización de los usuarios.

**7. Mantenimiento y Actualización**

**Actualizaciones de Seguridad**

Mantener las dependencias actualizadas para proteger contra vulnerabilidades conocidas.

### Algoritmo 11. Código para actualizar dependencias

# Comando para actualizar las dependencias en un entorno Python

pip install --upgrade -r requirements.txt

# requirements.txt

Flask==2.0.1

opencv-python==4.5.2.52

tensorflow==2.5.0

cryptography==3.4.7

psycopg2==2.9.1

**Respaldo y Recuperación**

Implementar Respaldo y Recuperación de Datos:

Configurar mecanismos automáticos de respaldo de la base de datos y recuperación en caso de fallo.

### Algoritmo 12. Mecanismos de respaldo

# Script de respaldo de la base de datos PostgreSQL

pg\_dump vein\_db > vein\_db\_backup.sql

# Script de restauración de la base de datos PostgreSQL

psql vein\_db < vein\_db\_backup.sql

**Monitoreo de Seguridad**

**Implementar Monitoreo de Seguridad y Respuesta a Incidentes:**

Usar herramientas de monitoreo de seguridad para detectar y responder a posibles incidentes.

Uso de una herramienta de monitoreo de seguridad como Fail2ban para detectar intentos de intrusión

### Algoritmo 13. Configuración básica para Fail2Ban

sudo tee /etc/fail2ban/jail.local <<EOF

[DEFAULT]

bantime = 1h

findtime = 10m

maxretry = 5

[sshd]

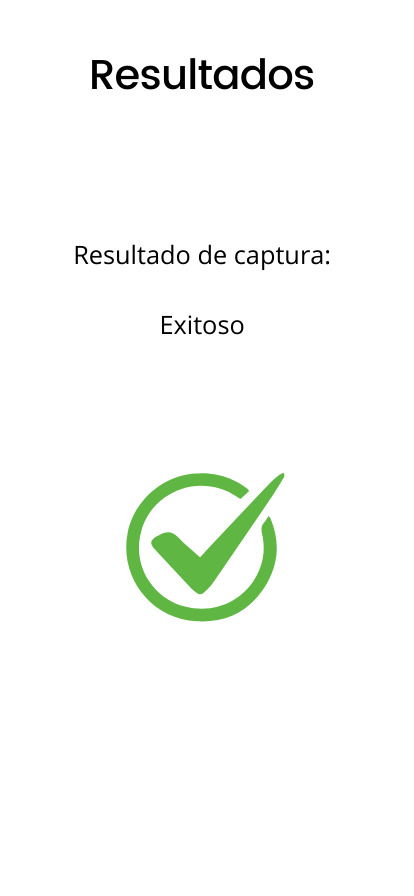
enabled = true

EOF

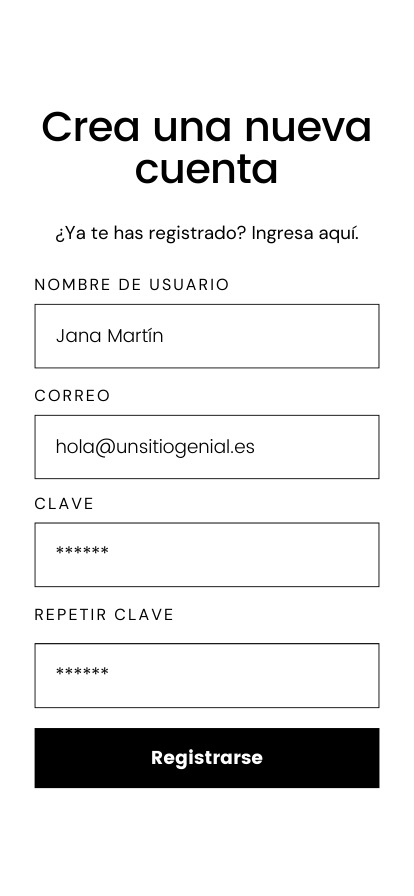
**3.3 Interfaz grafica**

Se mostrará la interfaz gráfica que se generó a partir de las ideas propuestas antes para usar la aplicación, considerando todas las características requeridas para su buen funcionamiento. Este fue un esquema hecho previamente en Canva para una fácil visualización y buen manejo de las herramientas para después ser implementado correctamente en su debido lenguaje de programación.

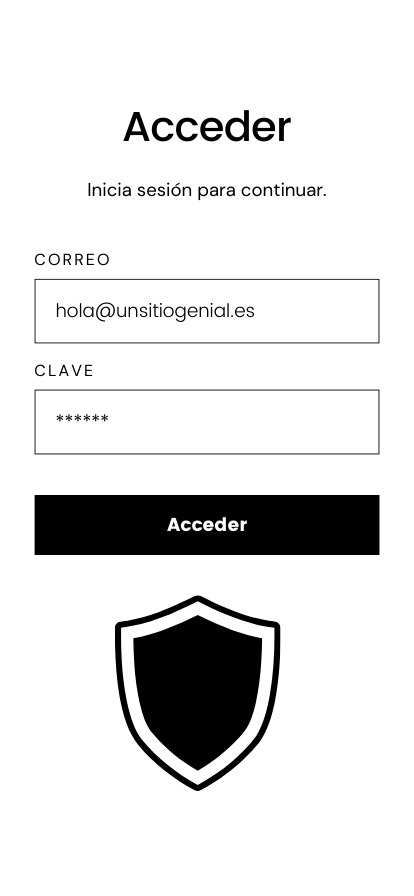
**Figura 10.** Modelo final de la pantalla de resultados



**Figura 11.** Modelo final de la pantalla de Registro.



**Figura 12.** Modelo final de la pantalla de Inicio de sesión.



**Figura 13.** Modelo final de la pantalla captura de imagen.



## 4 Conclusiones

Tras analizar muchas técnicas biométricas, desde el reconocimiento facial hasta el reconocimiento de huellas dactilares, se concluye que la biometría es poderosa y versátil para identificar y autenticar individuos.

La conclusión principal de esta investigación es que la combinación de múltiples modalidades biométricas puede ofrecer un nivel de precisión y seguridad aún mayor. La diversidad de características biométricas utilizadas garantiza que los sistemas sean más robustos frente a intentos de fraude o falsificación. Además, el uso de múltiples modalidades puede ayudar a mitigar las limitaciones inherentes de cada método individual, como la sensibilidad a cambios ambientales o la variabilidad intraclase.

Por otro lado, es crucial abordar las preocupaciones éticas y de privacidad asociadas con la implementación de sistemas biométricos. La recopilación y el almacenamiento de datos biométricos plantean desafíos en términos de protección de la privacidad y el potencial para un uso indebido de la información personal. Es necesario implementar medidas sólidas de seguridad y regulaciones adecuadas para garantizar que la información biométrica de los individuos se maneje de manera ética y responsable.

La investigación sobre biometría ha demostrado su eficacia como una herramienta poderosa para la identificación y autenticación de individuos. Su implementación debe considerarse cuidadosamente, considerando la precisión y la seguridad y las consideraciones éticas y de privacidad.

**Referencias**

1. Bodytrak. (s. f.). Guía de dispositivos biométricos para la seguridad. Bodytrak. <https://bodytrak.co/es/news/guia-de-dispositivos-biometricos-para-la-seguridad/>
2. Valdés, S., & Vallejos, S. (2020). Evaluación del rendimiento de un sistema de reconocimiento facial en condiciones desfavorables. Scielo Chile. <http://www.scielo.cl/scielo.php?script=sci_arttext&pid=S1726-569X2020000100043>
3. Baez, A., & Portilla, V. (2018). Análisis de sistemas de reconocimiento facial en tiempo real. e-Archivo UC3M. <https://e-archivo.uc3m.es/rest/api/core/bitstreams/3cfaf641-c759-41d5-9e0f-529f9393b9f4/content>
4. Thales Group. (s. f.). Reconocimiento facial. Thales Group. <https://www.thalesgroup.com/es/countries/americas/latin-america/dis/gobierno/inspiracion/reconocimiento-facial>
5. Caldera, J. & Zapico, F. (2009). Identificación facial biométrica. Profesional de la información. <https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/epi.2009.jul.11/21552>
6. Long, S. & Müller, O. (2007). Verificación biométrica automática de identidad mediante reconocimiento facial. UNL. <https://sinc.unl.edu.ar/sinc-publications/2007/LMM07/sinc_LMM07.pdf>
7. Arguello, H. (2011). Recognition Systems Based on the Facial Imagen. Revista Avances en Sistemas e Informática, 7-13. Obtenido de Researchgate: <https://www.researchgate.net/> publication/267296150\_Sistemas\_ de\_reconocimiento\_basados\_en\_la\_ imagen\_facial\_Recognition\_systems\_ based\_on\_the\_facial\_image
8. Hernández, R. G. (2010). upcommons. Obtenido de upcommons: <http://upcommons.upc>. edu/bitstream/handle/2099.1/9782/ PFC\_RogerGimeno.pdf?sequence=1
9. Raschka, S. (2014). sebastianraschka. Obtenido de sebastianraschka: http:// sebastianraschka.com/Articles/2014\_ python\_lda.html
10. Niyogi, X. É. (2002). CiteSeer. Obtenido de CiteSeer: <http://www.cad.zju.edu.cn/> home/xiaofeihe/LPP.html
11. Carrero, & et al. (2010). Obtenido de ehttp:// reconocimientofacial123.blogspot. com/2015/11/ventajas-y-desventajas. html
12. Montalva, P. B. (2023). Comparativa del rendimiento de algoritmos de reconocimiento facial en condiciones de iluminación variable. Scielo Chile. <https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122023000100003&lng=en&tlng=es>
13. Ortigoza, J. M., & Mariano, M. R. (2019). Estudio de la privacidad en sistemas biométricos: Caso de estudio reconocimiento facial. Redalyc. <https://www.redalyc.org/articulo.oa?id=84920977016>
14. Pascual, J. (2010). Uso de la firma manuscrita dinámica para el reconocimiento biométrico de personas en escenarios prácticos. Universidad de Valladolid. <https://uvadoc.uva.es/bitstream/handle/10324/130/TESIS52-100223.pdf?sequence=1&isAllowed=y>
15. Suárez, D., Herrera, E. C., & Riverón, E. M. (2007). La firma como un método biométrico de identificación. IPN, <https://www.repositoriodigital.ipn.mx/bitstream/123456789/8502/1/Azul231_original.pdf>
16. esolva.com. (s. f.). ESOLVA.COM PROYECTO Reconocimiento y verificacion de firmas manuscritas off-line. http://www.esolva.com/firmas/index\_memoria.html
17. Barrios, K., López, J., Mendieta, S., Benavides, R., & Sáez, Y. (2018). Sistema de reconocimiento de voz: un enlace en la comunicación hombre-máquina. Revista de iniciación científica. <https://d1wqtxts1xzle7.cloudfront.net/58994517/1827-Texto_del_articulo-8766-1-10-20180623_120190422-21930-1o1mjh3-libre.pdf?1555993051=&response-content-disposition=inline%3B+filename%3DSistema_de_reconocimiento_de_voz_un_enla.pdf&Expires=1713485548&Signature=BLD16-i2Kbn5i~N1N2NjTSl4AgYH4KWHikHWHGhtsnqsi5edtwSj-D--iRszA8ozbY~Uy9~9jcDPzOYTLBdGjGPAcE~PqE0SRM~Ptlt3WB~Sg94EwJyrdQQn08cV70aZoAmDJvXBEYvXBAAajPFP5fWacbI4iekvu9nZ6VD5LVlP0AScMNqddIEAXVeWZJFKS9aObUzZrdzlftyOqYlNoqY7r-yDtehn9cLwvqj0eEuIvwgP00RPohnS2Qz-65aRxL4Obpexn~L2nIZfd56lIeDPVSvD~S4jxTLgWpnoyHiGb~8qWV1BdufLhJpuJVipIWfVawe7fYoPlMoR50ojkA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA>
18. Tutorial biometría, [En línea] disponible en: <http://tutorial-biometria.galeon.com/pages/sistemas.html> (Consultado el 3 de noviembre de 2010)
19. Reconocimiento de voz: desde cero. (2019, 18 mayo). Víctor Noriega. https://victornoriega.github.io/reconocimiento-voz/
20. Carrasco, M. A., Portugal, R., & Peralta, B. (2006). Reconocimiento biométrico de audio y rostro: un sistema viable de identificación. Pontificia Universidad Católica de Chile Departamento de Ciencia de la Computación. <http://www.vizzion.cl/files/ACCA_biometria_final.pdf>
21. Vargas, A. (2013). Sistema biométrico de reconocimiento de huella dactilar en control de acceso de entrada y salida. UMNG. <https://repository.unimilitar.edu.co/>
22. Pusiol, G. (2007). Sistema de verificación de huellas digitales. Repositorio Digital UNC. <https://rdu.unc.edu.ar/bitstream/handle/11086/12/14436.pdf?sequence=1&isAllowed=y>
23. Beisner, A. (2010). Ataques tipo side-channel a sistemas biométricos de reconocimiento de huella dactilar. Universidad Autónoma de Madrid. <http://arantxa.ii.uam.es/~jms/pfcsteleco/lecturas/20100426AliciaBeisnerMunoz.pdf>
24. García, M & Ramírez, A. (2012). Avances en el reconocimiento del iris: perspectivas y oportunidades en la investigación de algoritmos biométricos. Scielo. <https://www.scielo.org.mx/pdf/cys/v16n3/v16n3a2.pdf>
25. Subcommittee on Biometrics and Identity Management, “Bio-metrics glossary,” National Science and Technology Council (NSTC), Technical report, September 2006.
26. Ramírez, E. S., González Fraga, J. Á., López, E. G., & Infante Prieto, S. O. (2013). Reconocimiento Biométrico de la Palma de la Mano Basado en el Promediado de Filtros de Correlación Simples. Difu100ci@, Revista de Difusión Científica, Ingeniería y Tecnologías, 7(2), 71-76. <http://difu100cia.uaz.edu.mx/index.php/difuciencia/article/view/75>
27. Florian, L. & Carranza, F. (2006). Reconocimiento del Iris. Advanced SourceCode.http://www.advancedsourcecode.com/reconocimientodeliris.pd
28. R. Sánchez­Reillo, C. Sánchez­Ávila, A. González­Marcos., Multiresolution Analysis and Geometric Measure for Biometric Identification. Secure Networking ­ CQRE [Secure]'99. Noviembre/Diciembre, 1999. Lecture Notes in Computer Science 1740, pp. 251­258. Springer­Verlag
29. Antelo, G. (2007). Patrones de identificación biométrica mediante geometría de la palma de la mano. Repositorio Institucional.
30. Zuleta, I. & Zorro, E. (2015). Sistema de seguridad biométrico basado en el análisis de la geometría de la mano. Unipiloto. <https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/1005/Sistema%20de%20seguridad%20biom%c3%a9trico,%20basado%20en%20el%20an%c3%a1lisis%20de%20la%20geometr%c3%ada%20de%20la%20mano.pdf?sequence=1&isAllowed=y>
31. Verificación de la geometría de la mano. (s. f.). https://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-unixsec/unixsec-html/node120.html[manooooooooooooo]
32. Instituto Nacional de Economía Social. (2018). Guía de Tecnologías Biométricas Aplicadas a la Ciberseguridad. Transparencia INAES. <https://transparencia.inaes.gob.mx/doctos/pdf/transparencia/Guias/Gu%C3%ADa_Tecnologias_biometricas_aplicadas_ciberseguridad_metad.pdf>
33. De Investigacion Use, V. (s. f.). Desarrollan un nuevo metodo de identificacion con las venas de la muñeca desde el movil. <https://investigacion.us.es/noticias/5403>
34. Anister. (2023). Vascular biometrics - Is it the future? https://www.anixter.com/es\_mx/about-us/news-and-events/news/vascular-biometrics-is-it-the-future.html
35. Ruiz Marín, M., Rodríguez Uribe, J. C., & Olivares Morales, J. C. (2009). Una mirada a la biometría. Avances en Sistemas e Informática. <https://revistas.unal.edu.co/index.php/avances/article/view/20295/21415>