Sistemas

Biométricos

César Tolosa Borja
Álvaro Giz Bueno

1.Introducción

Este trabajo tiene como objetivo mostrar los diferentes tipos de sistemas biométricos existentes para el reconocimiento de una característica exclusiva de una persona, mostrando la evolución de los sistemas biométricos a lo largo de la historia así como las tendencias futuras de los mismos.

Un sistema biométrico en general consta de componentes tanto hardware como software necesarios para el proceso de reconocimiento. Dentro del hardware se incluyen principalmente los sensores que son los dispositivos encargados de extraer la característica deseada. Una vez obtenida la información del sensor, será necesario realizar sobre ella las tareas de acondicionamiento necesarias, para ello se emplean diferentes métodos dependiendo del sistema biométrico utilizado. Por ello se han descrito los principales tipos de sistemas biométricos existentes:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

Para cada uno de estos sistemas se ha descrito su funcionamiento y algunas de las técnicas que se utilizan para procesar los datos obtenidos a partir de los sensores.

Los sistemas biométricos se han desarrollado como respuesta a la creciente demanda de seguridad existente en la actualidad y aunque algunos de ellos son altamente fiables, ningún sistema es efectivo al 100%, y estos sistemas también son susceptibles de ser engañados.

2.Concepto de Biometría

Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La forma de la cara, la geometría de partes de nuestro cuerpo como las manos, nuestros ojos y tal vez la más conocida, la huella digital, son algunos rasgos que nos diferencian del resto de seres humanos.

El concepto biometría proviene de las palabras bio (vida) y metría (medida), por lo tanto con ello se infiere que todo equipo biométrico mide e identifica alguna característica propia de la persona. Biometría es el conjunto de características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad del individuo, lo cual incluye huellas digitales, reconocimiento del iris, geometría de la mano, reconocimiento visual y otras técnicas.

La medición biométrica se ha venido estudiando desde tiempo atrás y es considerada en la actualidad como el método ideal de identificación humana.

2.1.Evolución histórica

En realidad, si entendemos este concepto en términos muy amplios, podemos decir que la biometría se practica desde el principio de los tiempos y, de hecho, nosotros mismos la practicamos muchas veces a lo largo del día sin casi darnos cuenta. Por ejemplo, cuando descolgamos el teléfono y escuchamos la voz de nuestro interlocutor, nuestro cerebro trata de comprobar si esa voz se parece a cualquiera de las muestras que tiene almacenadas en su memoria y que ha ido recopilando a lo largo de nuestra vida. Si nuestro cerebro encuentra similitudes suficientes entre alguno de sus recuerdos y lo que está escuchando en ese momento, entonces reconocemos a la persona que nos ha llamado. Si no, asumimos que estamos ante alguien a quien no conocemos. Del mismo modo, los animales reconocen a otros animales, incluidos los seres humanos, por características biométricas tales como el olor, el tacto o el timbre de la voz.

Por tanto, aunque se podría pensar en la biometría como una ciencia-ficción futurista, los principios básicos de la biometría eran comprendidos y utilizados miles de años antes. Esta comprobado, que en la época de los faraones, en el Valle del Nilo (Egipto) se utilizaban los principios básicos de la biometría para verificar a las personas que participaban en diferentes operaciones comerciales y judiciales.

Muchas son la referencias de personas, que en la antigüedad, han sido identificados por diversas características físicas y morfológicas como cicatrices, medidas, color de los ojos, tamaño de la dentadura...Esta clase de identificación se utilizaba, por ejemplo, en las zonas agrícolas, donde las cosechas eran almacenas en depósitos comunitarios a la espera de que sus propietarios dispusieran de ellas. Los encargados de cuidar estos depósitos debían identificar a cada uno de los propietarios cuando estos hicieran algún retiro de su mercadería, utilizando para esta tarea principios básicos de biometría como eran sus rasgos físicos.

Luego, en el siglo IXX hubo un pico de interés por parte de investigadores en criminología, cuando intentaron relacionar características físicas con tendencias criminales. Esto resulto en una variedad de equipos de medición y gran cantidad de datos recogidos. Los resultados no eran concluyentes, pero la idea de medir las características físicas de un individuo parecía efectiva y el desarrollo paralelo de la identificación de huellas digitales se convirtió en la metodología internacional para identificación utilizada por las fuerzas policiales de todo el mundo.

Con este fondo, no es sorprendente que por muchos años haya existido una fascinación con la posibilidad de usar la electrónica y el poder de microprocesadores para automatizar la verificación de identidad por parte de individuos y organizaciones tanto en el ámbito militar como comercial. Varios proyectos fueron comenzados para ver el potencial de la biometría, y uno de estos proyectos eventualmente llevó a la creación de un abultado y extraño lector de geometría de mano. El éxito de su funcionamiento motivó a sus diseñadores a refinar el concepto. Eventualmente, una pequeña compañía y un mucho mas pequeño y mas desarrollado lector de geometría de mano fue introducido al mercado y se convirtió en uno de los pilares de la industria biométrica.

Paralelamente, otras metodologías biométricas como la verificación de huellas digitales eran constantemente mejoradas y refinadas al punto de convertirse en equipos confiables y fácilmente desplegados. En años recientes, también se ha visto interés en el

escaneo de iris y reconocimiento facial, técnicas que ofrecen el potencial de no necesitar contacto, a pesar de que existen otros pormenores con respectos a estas técnicas.

La ultima década ha visto a la industria de la biometría madurar de un pequeño grupo de fabricas especialistas tratando de sobrevivir, a una industria global que comienza a tener un crecimiento significativo y está destinada a tener un rápido crecimiento al momento que aplicaciones en gran escala comienzan a aparecer en el mercado.

2.2. Necesidad de Biometría y Objetivos

Durante todo el siglo pasado han sido muchas las empresas que han concentrado sus esfuerzos en desarrollar sistemas biométricos para garantizar su seguridad, así como lo han hecho los propios Departamentos de Defensa de varios países.

Encontrar un sistema infalible e inequívoco para reconocer personas es el objetivo último de la biometría.

Hoy en día contamos con una gran variedad de equipos capaces de identificar a las personas a partir de la información de alguna parte de su cuerpo como las manos, la retina, el iris, los dedos, las huellas dactilares, la voz, o la firma. Incluso se está investigando en la posibilidad de crear un sistema basado en el ADN.

Restringido a través de su historia por su costo elevado, una función cuestionable y proveedores transitorios, la identificación biométrica está experimentando ahora una aceptación creciente, no sólo en aplicaciones de alta seguridad tales como bancos e instalaciones gubernamentales, sino también en clubes de salud, la Villa Olímpica en Atlanta en 1996, control de clientes del seguro social y acceso a oficinas y plantas comerciales e industriales. Los costos han sido reducidos a un nivel razonable y la función y contabilidad de los dispositivos es hoy día satisfactoria.

De esta forma con los sistemas biométricos que reconocen las características singulares de las huellas digitales, por ejemplo, se logra evitar fraudes en la banca, en el sistema de salud por suplantación de pacientes, controlar el acceso en el desplazamiento de seres humanos al interior de las empresas, tiempos desperdiciados, accesos no deseados; sin necesidad de utilizar contraseñas, carnes, tarjetas magnéticas u otros medios de identificación vulnerables. Esto hace que los sistemas biométricos sean el medio más rápido y seguro mediante la utilización de la huella digital como validador de operaciones y de control de acceso.

2.3. Funcionamiento de un sistema biométrico

Un equipo biométrico es aquel que tiene capacidades para medir, codificar, comparar, almacenar, transmitir y/o reconocer alguna característica propia de una persona, con un determinado grado de precisión y confiabilidad.

La tecnología biométrica se basa en la comprobación científica de que existen elementos en las estructuras vivientes que son únicos e irrepetibles para cada individuo, de tal forma que, dichos elementos se constituyen en la única alternativa, técnicamente viable, para identificar positivamente a una persona sin necesidad de recurrir a firmas,

passwords, pin numbers, códigos u otros que sean susceptibles de ser transferidos, sustraídos, descifrados o falsificados con fines fraudulentos.

La identificación biométrica es utilizada para verificar la identidad de una persona midiendo digitalmente determinados rasgos de alguna característica física y comparando esas medidas con aquéllas de la misma persona guardadas en archivo en una base de datos o algunas veces en una tarjeta inteligente que lleva consigo la misma persona. Las características físicas utilizadas son huellas digitales, huellas de la voz, geometría de la mano, el dibujo de las venas en la articulación de la mano y en la retina del ojo, la topografía del iris del ojo, rasgos faciales y la dinámica de escribir una firma e ingresarla en un teclado.

El funcionamiento de estos sistemas implica de la necesidad de un potente software con unas fases diferenciadas en las cuales intervienen diferentes campos de la informática, como son: el reconocimiento de formas, la inteligencia artificial, complejos algoritmos matemáticos y el aprendizaje. Éstas son las ramas de la informática que desempeñan el papel más importante en los sistemas de identificación biométricos; la criptografía se limita a un uso secundario como el cifrado de los datos biométricos almacenados en la base de datos o la trasmisión de los mismos.

Los escáners de huellas digitales y equipos de medición de geometría de la mano son los dispositivos más corrientemente utilizados. Independiente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico.

3. Sensores biométricos

En lo que a sensores para sistemas biométricos se refiere, aunque hay diferentes fabricantes, hablando en términos generales se utiliza el mismo sistema de captación de la característica deseada, es decir, para reconocimiento de iris se emplea una cámara o para reconocimiento de voz un micrófono. El único campo donde parece existir una mayor variedad de métodos es en el de captación de huella dactilar.

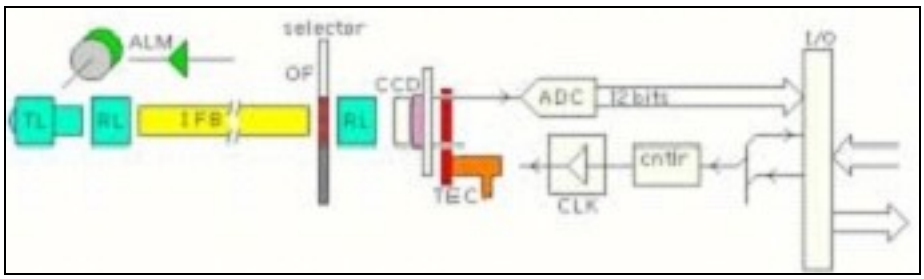
A continuación se muestran diferentes tipos de sensores:

- Sensores Ópticos

El método óptico es uno de los más comunes que suele estar formado por cámaras de vídeo de tipo CCD. Estos sensores se emplean tanto en reconocimiento de huella dactilar como de ojo.

El corazón de la cámara es un circuito integrado tipo CCD (Dispositivo de Carga Acoplada). Este dispositivo consiste de varios cientos de miles de elementos individuales (píxeles) localizados en la superficie de un diminuto CI.

En la siguiente figura se puede observar el diagrama correspondiente a una cámara de este tipo:



Cada píxel se ve estimulado con la luz que incide sobre él (la misma que pasa a través de los lentes y filtros de la cámara), almacenando una pequeña carga de electricidad. Los píxeles se encuentran dispuestos en forma de malla con registros de transferencia horizontales y verticales que transportan las señales a los circuitos de procesamiento de la cámara (convertidor analógico-digital y circuitos adicionales). Esta transferencia de señales ocurre 6 veces por segundo.

En la siguiente figura podemos apreciar un dispositivo comercial de este tipo de CI:

- Sensores Termoeléctricos

El método termoeléctrico es menos común. Actualmente sólo existe en el mercado el Atmel Fingerchip™ para reconocimiento de huella dactilar.

El Fingerchip™ utiliza un sistema único para reproducir el dedo completo "arrastrándolo" a través del sensor. Durante este movimiento se realizan tomas sucesivas (slices) y se pone en marcha un software especial que reconstruye la imagen del dedo. Este método permite al Fingerchip™ obtener una gran cualidad, 500 puntos por imagen impresa de la huella dactilar con 256 escalas de gris.
El sensor mide la temperatura diferencial entre las crestas papilares y el aire retenido en los surcos. Este método proporciona una imagen de gran cualidad incluso cuando las huella dactilares presentan alguna anomalía como sequedad o desgaste con pequeñas cavidades entre las cimas y los surcos de la huella. La tecnología termal permite también su uso bajo condiciones medioambientales extremas, como temperaturas muy altas, humedad, suciedad o contaminación de aceite y agua.

Además, también cuenta con la ventaja de autolimpiado del sensor, con lo que se evitan las huellas latentes. Se denomina así a las huellas que permanecen en el sensor una vez utilizado, lo cual puede ocasionar problemas no sólo en las lecturas posteriores sino que permite que se copie la huella para falsificarla y acceder así al sistema. De hecho, este método de arrastre que utiliza la tecnología basada en el calor hace que el Fingerchip esté por encima de otras tecnologías. El Fingerchip™ funciona con bajas temperaturas, alto porcentaje de humedad, etc.

Otra ventaja es la reproducción de una imagen grande de alta cualidad y siempre un sensor limpio. La desventaja es que la cualidad de la imagen depende un poco de la habilidad del usuario que utiliza el escáner. La segunda desventaja es el calentamiento del sensor que aumenta el consumo de energía considerablemente.

Este calentamiento es necesario para evitar la posibilidad de un equilibrio térmico entre el sensor y la superficie de la yema dactilar.

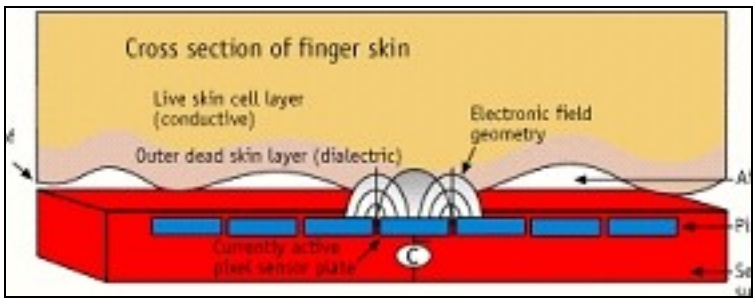
El elevado volumen de diseño del escáner permite que su precio sea bajo ya que en el proceso de manufacturación se necesita menos silicona.

- Sensores Capacitivos

El método capacitivo es uno de los más populares para reconocimiento de huella dactilar. Al igual que otros escáner, genera una imagen de las cresta y valles del dedo. En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos conductores cubiertos por una capa aislante. La capacitancia en cada plato sensor es medida individualmente depositando una carga fija sobre ese plato.

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor, tendremos un efecto de solapamiento sobre los platos (píxel) vecinos, lo que provocará que el área sensor aumente de tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen.

Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos optimas en la piel. Cuando el dedo esta sucio, con frecuencia no existirá aberturas de aire en valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento.



Entre las empresas líderes en este sector se encuentran: Infineon, Verdicom, Sony y ST Microelectronics.

- Sensores E-Field (de Campo Eléctrico)

El sensor de campo eléctrico funciona con una antena que mide el campo eléctrico formado entre dos capas conductoras (la más profunda situada por debajo de la piel del dedo). La tecnología basada en los campos eléctricos afirma ser útil para cualquiera y poder trabajar bajo cualquier condición, por dura que ésta sea, del "mundo real", como por ejemplo piel húmeda, seca o dañada.

Esta tecnología para reconocimiento de huella dactilar origina un campo entre el dedo y el semiconductor adyacente que simula la forma de los surcos y crestas de la superficie epidérmica. Se utiliza un amplificador under-píxel para medir la señal. Los sensores reproducen una imagen clara que se corresponde con mucha exactitud a la huella dactilar y que es mucho más nítida que la producida por sensores ópticos o capacitivos. Esto permite a la tecnología de campo eléctrico la lectura de huellas que otras tecnologías no podrían

En la tecnología de campo eléctrico, la antena mide las características de la capa subcutánea de la piel generando y detectando campos lineales geométricos que se originan en la capa de células de la piel situada bajo la superficie de la misma.

Esto contrasta con los campos geométricos esféricos o tubulares generados por el sensor capacitivo que sólo lee la superficie de la piel. Como resultado, huellas que con sensores capacitivos son casi imposibles de leer, se pueden reproducir con éxito por sensores de tecnología de campo eléctrico.

Desde hace poco existe también un sensor más fuerte basado en esta tecnología que saldrá al mercado en pocos meses.

Una desventaja es la baja resolución de la imagen y el área pequeña de imagen lo que produce un índice de error alto (EER).

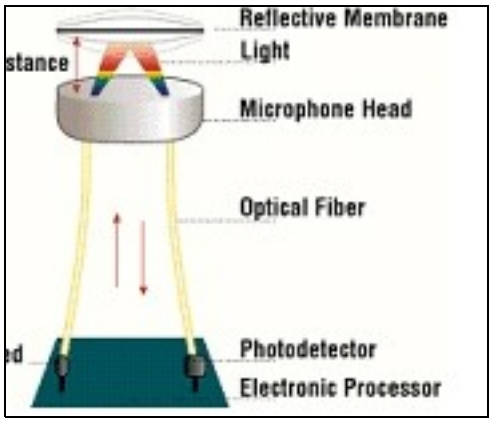
- Sensores sin contacto

Un sensor sin contacto funciona de forma similar al sensor óptico. Normalmente con un cristal de precisión óptica a una distancia de dos o tres pulgadas de la huella dactilar mientras se escanea el dedo. La yema del dedo se introduce en un área con un hueco. Una desventaja a tener en cuenta es que a través de este hueco pueden llegar polvo y suciedad hasta el cristal óptico con la correspondiente distorsión de la imagen. Otro punto es que las huellas escaneadas son esféricas lo que origina un complejo algorítmico mucho más complejo.

- Micrófonos ópticos unidireccionales

La luz de un diodo es emitida sobre una membrana reflectora a través de fibra óptica. Cuando las ondas de sonido golpean a la membrana, ésta vibra; cambiando así las características de la luz reflejada.

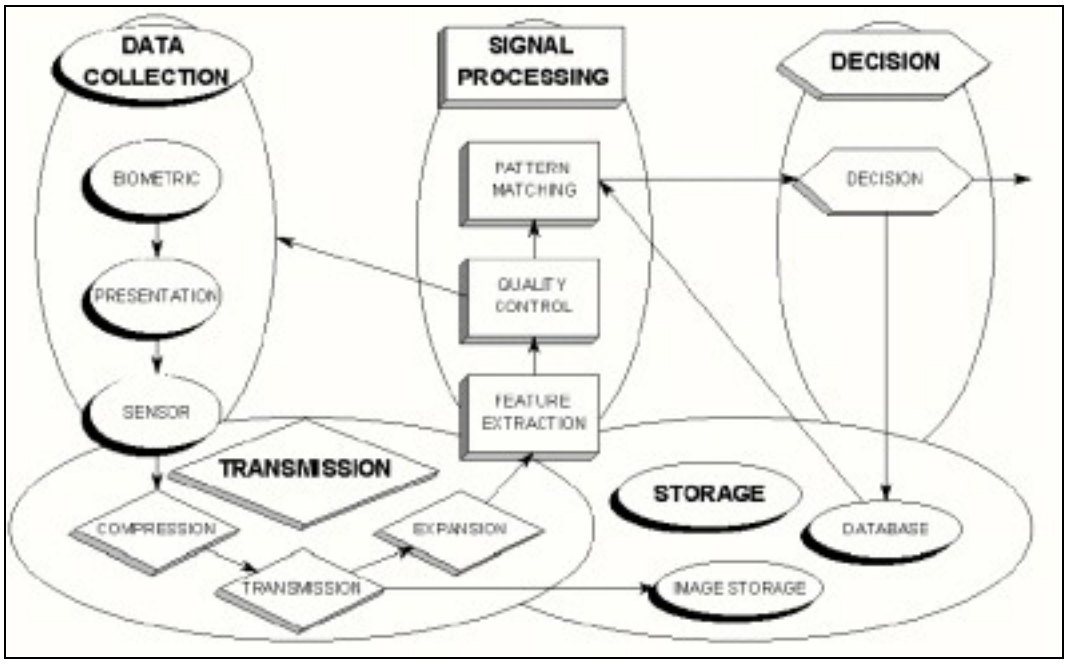
Un foto-detector registra la luz reflejada que en conjunto con una electrónica de procesamiento obtiene una representación precisa de las ondas de sonido. Es utilizado en reconocimiento de voz.



4. Procesamiento de la información

Aunque estos dispositivos se basan en tecnologías muy diversas, si se consideran de forma genérica se puede considerar un sistema biométrico genérico de identificación, dividido en cinco subsistemas: recolección de datos, transmisión, procesado de señal, decisión y almacenamiento de datos.

La siguiente figura muestra de manera esquemática estos cinco subsistemas y como se relacionan entre sí:



1. Recolección De Datos

Los sistemas biométricos comienzan con la medida de una característica del comportamiento o fisiológica. La clave de todos los sistemas es la hipótesis subyacente que la característica biométrica medida es distintiva entre los individuos y en un cierto plazo repetible para el mismo individuo.

Es decir, las características deben variar en gran magnitud entre individuos, pero deben variar muy poco para cada individuo de medida a medida. Los problemas en medir y controlar estas variaciones comienzan en el subsistema de la colección de datos. La característica del usuario se debe presentar a un sensor. Según lo observado ya, la presentación de la característica biométrica al sensor introduce un componente del comportamiento.

Los cambios inevitables en el comportamiento afectarán la capacidad de repetición y la distinción de la medida.

Si un sistema pretende ser abierto, presentación y sensor deben ser estandarizados para asegurar que la característica biométrica recogida sea la misma que recogería otro sistema para el mismo individuo.

2. Transmisión

Algunos, pero no todos, los sistemas biométricos recogen datos en una localización pero se almacenan y/o procesan en otra. Tales sistemas requieren la transmisión de datos. Si está implicada una gran cantidad de datos, la compresión es fundamental, a fin de requerir poco ancho de banda y poco espacio para su almacenamiento.

El cuadro anterior muestra la compresión y la transmisión que ocurren antes de procesar de señal y del almacenamiento de la imagen.

En tales casos, los datos comprimidos transmitidos o salvados se deben descomprimir antes de que sean usados. El proceso de la compresión y de la descompresión causa generalmente pérdida de la calidad en la señal restablecida.

La técnica de compresión usada dependerá de la señal biométrica. Un campo de investigación interesante consiste en encontrar, para una técnica biométrica dada, métodos de la compresión con impacto mínimo en el subsistema del proceso de señal. Si un sistema es abierto, los protocolos de la compresión y de la transmisión deben ser estandarizados de modo que cada usuario de los datos pueda reconstruir (aunque con pérdida de la calidad) la imagen original.

Los estándares existentes actualmente son: para la compresión de la huella digital (WSQ), de las imágenes faciales (JPEG), y de los datos de la voz (CELP).

3. Procesado De Señal

Adquirida y transmitida una característica biométrica, debemos prepararla para corresponder con otra. El cuadro anterior divide el subsistema de proceso de señal en tres tareas: extracción, control de calidad, y concordancia con el modelo.

La primer meta es analizar el modelo biométrico verdadero de la presentación y las características del sensor, en presencia de las pérdidas por ruido y de señal impuestas por la transmisión.

La segunda meta, es preservar el modelo biométrico para que esas calidades que sean distintivas y repetibles, y desechar las que no lo sean, o sean redundantes.

En un sistema de reconocimiento de la voz, se deseará encontrar las características, tales como los lazos armónicos en las vocales, que dependen solamente del hablante y no de las palabras que son habladas.

Y, desearemos centrarnos en esas características que deberán ser invariantes incluso si el hablante está resfriado o no está hablando directamente en el micrófono.

Hay muchos acercamientos matemáticos para realizar estos procesos. En general, la extracción de la característica es una forma de compresión irreversible, significando esto que la imagen biométrica original no se puede reconstruir de las características extraídas.

En algunos sistemas, la transmisión ocurre después de la extracción de la característica para reducir el requisito de mínimo ancho de banda.

Después de la extracción de la característica, o quizá antes o durante, desearemos controlar si la señal recibida del subsistema de colección de datos tiene la calidad requerida, a fin de solicitar si es necesario una nueva muestra del usuario.

El desarrollo de este proceso de "control de calidad" ha mejorado sensiblemente el funcionamiento de los sistemas biométricos en los últimos años.

El propósito del proceso de concordancia con el modelo es comparar una muestra actual con la característica de una muestra salvada, llamada un modelo, y enviar al subsistema de decisión la medida cuantitativa de la comparación.

Las distancias raramente, serán fijadas en cero, pues siempre habrá alguna diferencia relacionada con el sensor o relacionada con el proceso de transmisión o con el comportamiento propio del usuario.

4. Decisión

La política del sistema de decisión dirige la búsqueda en la base de datos, y determina los "matching" o los " no-matching" basándose en las medidas de la distancia recibidas de la unidad de procesado de señal.

Este subsistema toma en última instancia una decisión de "acepta/rechaza" basada en la política del sistema. Tal política podría ser declarar un "matching" para cualquier distancia más baja que un umbral fijo y "validar" a un usuario en base de este solo "matching", o la política podría ser declarar un "matching" para cualquier distancia más baja que un umbral dependiente del usuario, variante con el tiempo, o variable con las condiciones ambientales.

Una política posible es considerar a todos los usuarios por igual y permitir sólo tres intentos con una distancia alta para el "matching" para luego volver una medida baja de la distancia.

La política de decisión empleada es una decisión de la gerencia que es específica a los requisitos operacionales y de la seguridad del sistema. En general, bajar el número de no-matching falsos se puede negociar contra levantar el número de matching falsos.

La política óptima del sistema depende de las características estadísticas de las distancias de comparación que vienen de la unidad de "matching " del modelo y de las penas relativas para el matching falso y el no-matching falso dentro del sistema.

En cualquier caso, en la prueba de dispositivos biométricos, es necesario evaluar el funcionamiento del subsistema de procesado de señal con independencia de las políticas puestas en ejecución mediante el subsistema de decisión.

5. Almacenamiento

El subsistema restante que se considerará es el del almacenamiento. Habrá una o más formas de almacenamiento a usar, dependiendo del sistema biométrico. Los modelos de la característica serán salvados en una base de datos para la comparación en la unidad de matching.

Para los sistemas que realizan solamente una correspondencia "uno a uno", la base de datos se puede distribuir en las tarjetas magnéticas llevadas por cada usuario. Dependiendo de la política del sistema, no es necesaria ninguna base de datos centralizada.

Aunque, en esta aplicación, una base de datos centralizada se puede utilizar para detectar tarjetas falsificadas o para reeditar tarjetas perdidas sin recordar el modelo biométrico.

Los requisitos de velocidad del sistema dictan que la base de datos esté repartida en subconjuntos más pequeños, tales que cualquier muestra de la característica necesita solamente ser correspondida con la de los modelos salvados en una partición. Esta estrategia tiene el efecto de aumentar velocidad del sistema y de disminuir matching falsos a expensas de aumentar la tasa de no-matching falsos. Esto significa que las tasas de error del sistema no son constantes con el aumento del tamaño de la base de datos y, además, esta relación no es lineal.

Por lo tanto, las estrategias para particionar la base de datos representan una decisión bastante compleja.

Si existe la posible necesidad de reconstruir los modelos biométricos a partir de los datos salvados, será necesario el almacenamiento de datos sin procesar.

El modelo biométrico, en general, no es reconstituible a partir de los datos salvados. Además, los modelos son creados usando algoritmos propietarios de extracción de características, propios de cada fabricante.

El almacenamiento de informaciones en bruto permite cambios en el sistema o de equipamiento sin que sea necesario registrar nuevamente a todos los usuarios.

Estos cinco pasos se refieren a la captación y verificación de una característica biométrica determinada de una persona pero para que el sistema sea capaz de verificar dicha característica es necesario un paso previo a estos cinco en el que la persona debe registrarse en el sistema ("enroll en inglés"). Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como, por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia ("reference template" en inglés.) El modelo de referencia debe ser guardado en una base de datos, una tarjeta inteligente ("smart card" en inglés), o en algún otro lugar del cual será extraído en cualquier ocasión futura para realizar la verificación.

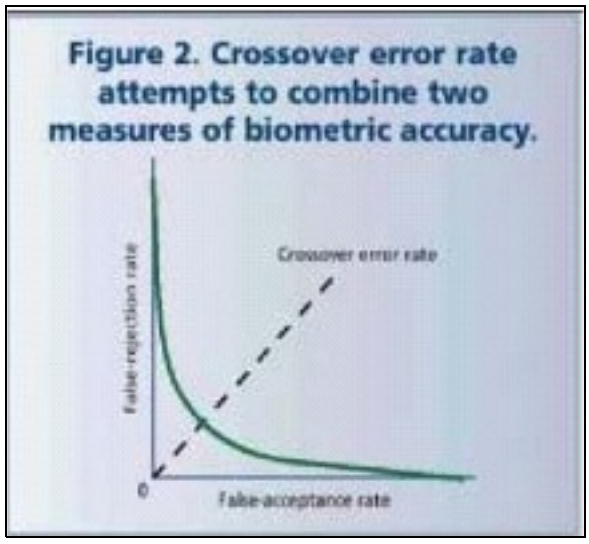
A pesar de que es poco probable obtener dos tomas iguales aún del mismo individuo, a causa de diferencias ambientales y otras condiciones en el momento de la captura, el sistema aún debe poder funcionar correctamente. La mayoría de los algoritmos de

comparación generan un ámbito para cada ensayo de comparación el cual es cotejado dentro de determinados umbrales antes de ser aceptados o rechazados.

Es en este punto donde entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación. Por tasa de falso rechazo (False Rejection Rate, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por tasa de falsa aceptación (False Acceptance Rate, FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad: estamos proporcionando acceso a un recurso a personal no autorizado a acceder a él.

Cada proveedor de tecnología biométrica configura la/el falsa/o aceptación / rechazo de forma diferente.

La figura siguiente muestra esta relación de compromiso.

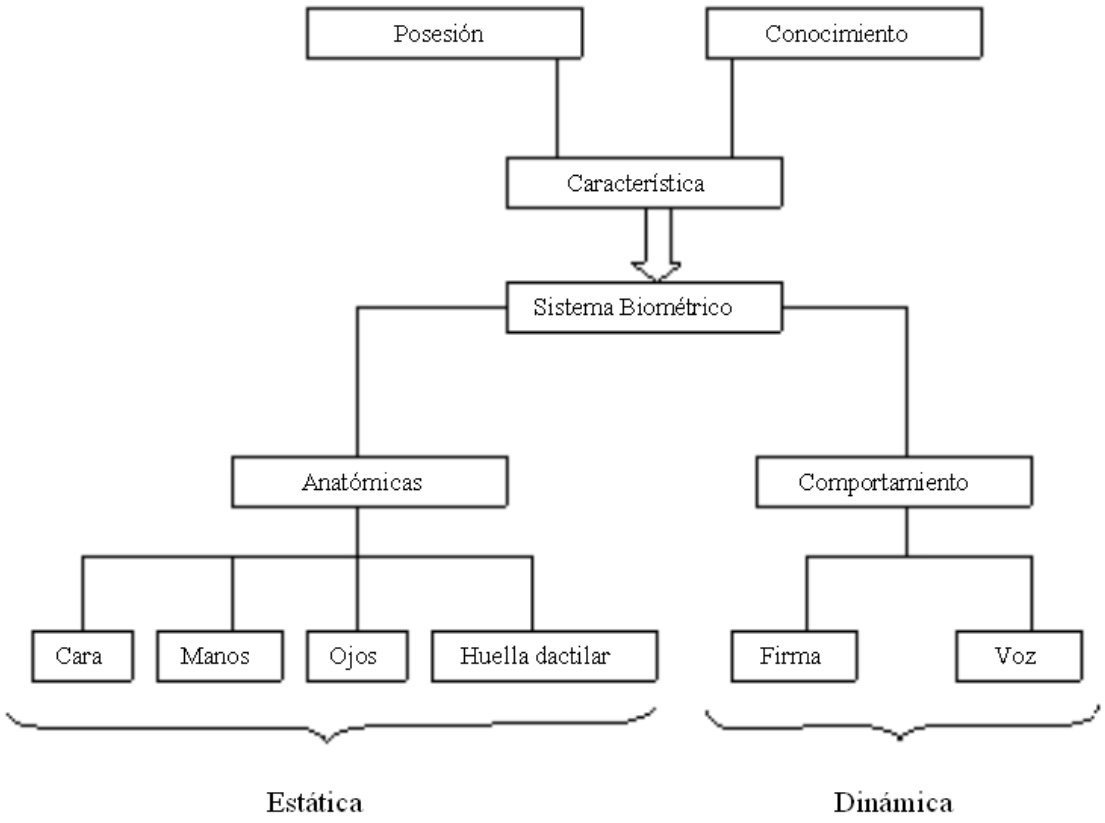


Como puede observarse, si el umbral es demasiado bajo, se vuelve demasiado fácil para una persona no autorizada ser aceptada por el sistema, en cambio si el umbral está demasiado alto, personas autorizadas pueden llegar a ser rechazadas.

5. Clasificación de los sistemas biométricos

Aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento (por ejemplo la medición de la biometría basada en huella digital variará de acuerdo a la manera en que se coloca el dedo), la clasificación de las técnicas biométricas facilita su estudio. La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual



Sin tener en cuenta la clasificación anterior, las técnicas biométricas se pueden clasificar atendiendo a cual es la característica observada y aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mesurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), tradicionalmente ha estado basada en seis grandes grupos:

- Reconocimiento de la huella dactilar
- Reconocimiento de la cara
- Reconocimiento de iris/retina
- Geometría de dedos/mano
- Autentificación de la voz
- Reconocimiento de la firma

Cada sistema biométrico utiliza una cierta clase de interfaz para recopilar la información sobre la persona que intenta acceder. Un software especializado procesará esa información en un conjunto de los datos que se pueden comparar con los modelos de los usuarios que se han introducido previamente al sistema. Si se encuentra un "matching" con la base de datos, se confirma la identidad de la persona y se concede el acceso.

En la siguiente tabla se muestra una comparativa de sus rasgos más generales:

	Ojo - Iris	Ojo - Retina	Huellas dactilares	Geometría de la mano	Escritura - Firma	Voz
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Alta	Alta	Alta
Prevención de ataques	Muy Alta	Muy alta	Alta	Alta	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta
Estabilidad	Alta	Alta	Alta	Media	Media	Media
Identificación y autenticación	Ambas	Ambas	Ambas	Autenticación	Ambas	Autenticación
Estándars	-	-	ANSI/NIST, FBI	-	-	SVAPI
Interferencias	Gafas	Irritaciones	Suciedad, heridas, asperezas ...	Artritis, reumatismo ...	Firmas fáciles o cambiantes	Ruido, resfriados ...
Utilización	Instalaciones nucleares, servicios médicos, centros penitenciarios	Instalaciones nucleares, servicios médicos, centros penitenciarios	Policía, industrial	General	Industrial	Accesos remotos en bancos o bases de datos
Precio por nodo en 1997 (USD)	5000	5000	1200	2100	1000	1200

5.1. biometría estática

- **Huella dactilar**

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

EN EXCLUSIVA. Las huellas dactilares son una característica exclusiva de los primates.

Identificando patrones

A simple vista, el patrón que siguen las líneas y surcos de una huella se puede clasificar según tres rasgos mayores: arco, lazo y espiral. Cada dedo presenta al menos una de estas características. Por otro lado, en determinados puntos las líneas de la huella dactilar se cortan bruscamente o se bifurcan. Estos puntos reciben el nombre de minucias, y juntos suman casi el 80% de los elementos singulares de una huella.

LAZO

ESPIRAL

ARCO

Todo esto da lugar a un patrón complejo único para cada individuo, distinto incluso en gemelos idénticos. En concreto, se estima que la probabilidad de que dos personas tengan las mismas huellas dactilares es aproximadamente de 1 en 64.000 millones.

Cuando se digitaliza una huella, los detalles relativos a las líneas (curvatura, separación,...), así como la posición absoluta y relativa de las minucias extraídas, son procesados mediante algoritmos que permiten obtener un índice numérico correspondiente a dicha huella. En el momento en que un usuario solicita ser identificado, coloca su dedo sobre un lector (óptico, de campo eléctrico, por presión,...) y su huella dactilar es escaneada y analizada con el fin de extraer los

elementos característicos y buscar su homóloga en la base de datos. El resultado es un diagnóstico certero en más del 99% de los casos.

Las técnicas utilizadas para la comparación de la huella dactilar se pueden clasificar en dos categorías:

La **técnica de puntos Minutia** primero encuentran estas minucias y posteriormente procede a su colocación relativa en el dedo.
Es difícil extraer los puntos de las minucias exactamente cuando la huella dactilar es de baja calidad. También este método no considera el patrón global de crestas y de surcos.

El **método correlación** puede superar algunas de las dificultades de la comparación por puntos Minutia; sin embargo, tiene algunos inconvenientes propios. Las técnica de correlación requieren una localización precisa de un punto de registro y se ve afectada por el desplazamiento y rotación de la imagen.

Clasificación de la Huella

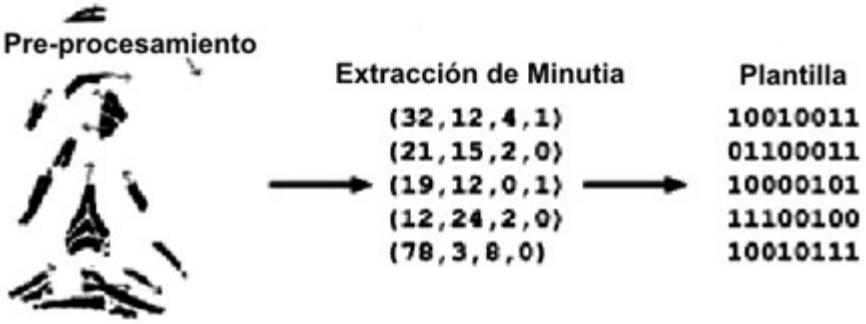
La clasificación de las huellas dactilares es una técnica consistente en asignar a una huella uno de los varios tipos previamente especificados en la literatura y registrarla con un método de indexación de las direcciones. Una huella dactilar de entrada es primeramente clasificada a un nivel grueso en uno de los tipos:

- *Whorl*
- *Lazo derecho*
- *Lazo izquierdo*
- *Arco*
- *Tented el arco*

, y entonces, en un nivel más fino, se compara con el subconjunto de la base de datos que contiene solamente ese tipo de huella dactilar. Se utilizan algoritmos desarrollados para identificar a cual de estos tipos de pertenece una huella en concreto.

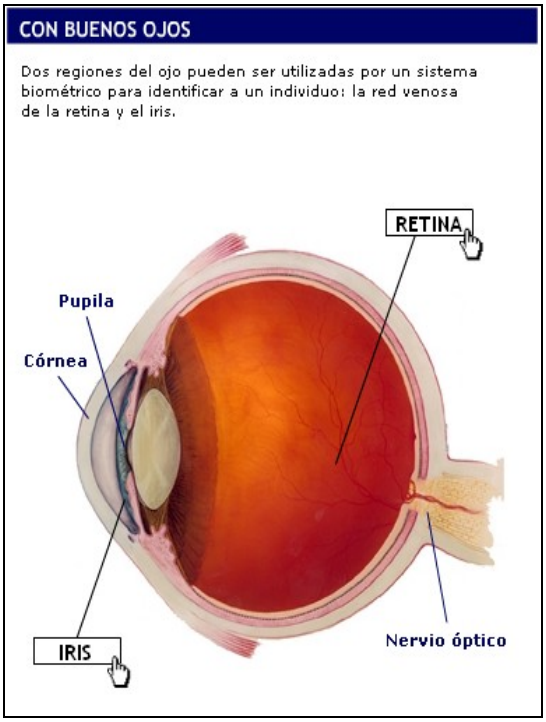
Realce de la Huella

Un paso crítico en la clasificación automática de la huella dactilar está en extraer mediante un algoritmo las minucias de las imágenes de la huella dactilar de la entrada. El funcionamiento de un algoritmo de extracción de las minucias confía totalmente en la calidad de las imágenes de la huella dactilar de la entrada. Para asegurarse de que el funcionamiento de un sistema automático de identificación/verificación de huella dactilar sea robusto con cierta independencia de la calidad de las imágenes de la huella dactilar, es esencial incorporar un algoritmo del realce de la huella dactilar en el módulo de la extracción de las minucias. De este modo se puede mejorar de forma adaptativa la claridad de las estructuras de la cresta y del surco de las imágenes de las huella dactilares de entrada.


Pre-procesamiento
Extracción de Minutia
Plantilla
(32,12,4,1)
(21,15,2,0)
(19,12,0,1)
(12,24,2,0)
(78,3,8,0)
10010011
01100011
10000101
11100100
10010111

- **Reconocimiento de iris**

El **iris** es una membrana coloreada y circular que **separa las cámara anterior y posterior del ojo**. Posee una apertura central de tamaño variable, la pupila. Las fibras musculares del iris la constituyen dos músculos, el esfínter del iris y el dilatador de la pupila



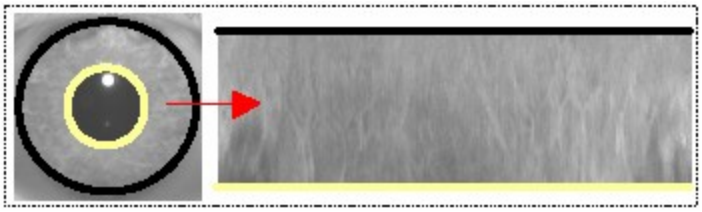
El iris está **constantemente activo** *permitiendo así a la pupila dilatarse* (midriasis) *o contraerse* (miosis). Está función tiene su objetivo en la **regulación de la cantidad de luz que llega a la retina**.

Se trata de la estructura indivisible del cuerpo humano más distintiva matemáticamente. En sus 11 milímetros de diámetro cada iris concentra **más de 400 características** que pueden ser usadas para identificar a su propietario (*criptas, surcos, anillos, fosos, pecas, corona en zig-zag*,…). Cuenta con un número de puntos distintivos 6 veces superior al de una huella dactilar.

Hay que tener en cuenta que el iris no cambia a lo largo de la vida, y que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes. Asimismo, se trata de un órgano interno protegido -por la córnea y el humor acuoso- pero visible externamente a una distancia de hasta un metro. Las lentes de contacto y las gafas no afectan a la identificación. Y, por si todo esto fuera poco, los sistemas basados en el reconocimiento de iris son veinte veces más rápidos que cualquier otro sistema biométrico.

Funcionamiento

El procedimiento, base de los dispositivos actuales, resulta extraordinariamente sencillo. Basta con colocarse frente a una cámara, con los ojos correctamente alineados en su campo de visión. La cámara genera una imagen que es analizada por medio de los algoritmos de Daugman para obtener el ***IrisCode*** personal, un patrón único del iris que apenas ocupa 256 bytes de información. Tan reducido tamaño permite una rápida búsqueda de su homólogo en una base de datos hasta identificar a su propietario.



Para la codificación del patrón del iris, usualmente se realiza una conversión de la imagen del iris de coordenadas cartesianas a polares para facilitar la extracción de información, al pasar de una forma circular a una rectangular. A la nueva representación, se le aplican filtros

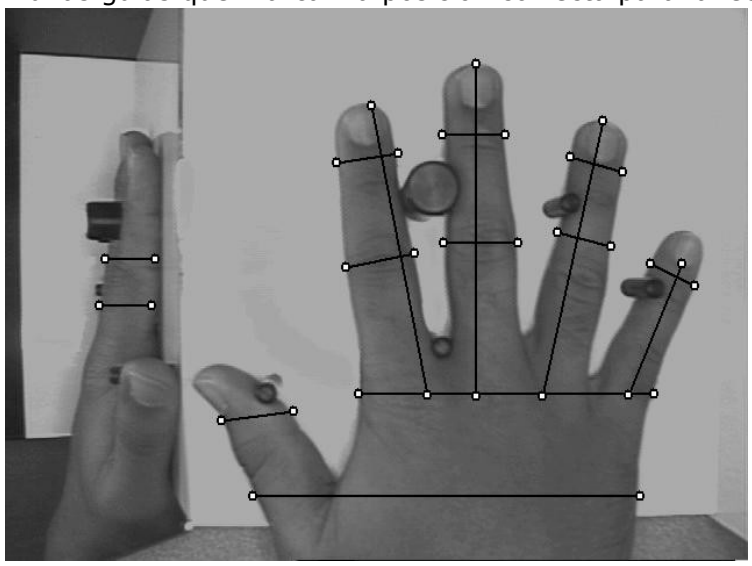
multicanal, ya sean de Gabor, Fourier o Wavelet, para extraer los coeficientes que finalmente conformaran el código del iris.

- **Geometría de la mano**

La **forma de la mano** puede ser de gran valor en biometría. A diferencia de las huellas dactilares, la mano humana no es única, y sus características individuales no son suficientes para identificar a una persona. Sin embargo, su perfil resulta útil si el sistema biométrico lo combina con imágenes individuales de algunos dedos, extrayendo datos como las longitudes, anchuras, alturas, posiciones relativas, articulaciones,… Estas características se transforman en una serie de patrones numéricos que pueden ser comparados. Su principal aplicación es la verificación de usuario.

Los sistemas de autenticación basados en el análisis de la geometría de la mano son sin duda los más rápidos dentro de los biométricos: con una probabilidad de error aceptable en la mayoría de ocasiones, en aproximadamente un segundo son capaces de determinar si una persona es quien dice ser.

Cuando un usuario necesita ser autenticado sitúa su mano sobre un dispositivo lector con unas guías que marcan la posición correcta para la lectura.



Una vez la mano está correctamente situada, unas cámaras toman una imagen superior y otra lateral, de las que se extraen ciertos datos (anchura, longitud, área, determinadas distancias...) en un formato de tres dimensiones. Transformando estos datos en un modelo matemático que se contrasta contra una base de patrones, el sistema es capaz de permitir o denegar acceso a cada usuario.

Quizás uno de los elementos más importantes del reconocimiento mediante analizadores de geometría de la mano es que éstos son capaces de aprender: a la vez que autentican a un usuario, actualizan su base de datos con los cambios que se puedan producir en la muestra (un pequeño crecimiento, adelgazamiento, el proceso de cicatrizado de una herida...); de esta forma son capaces de identificar correctamente a un usuario cuya muestra se tomó hace años, pero que ha ido accediendo al sistema con regularidad. Este hecho, junto a su rapidez y su buena aceptación entre los usuarios, hace que los autenticadores basados en la geometría de la mano sean los más extendidos dentro de los biométricos a pesar de que su tasa de falsa aceptación se podría considerar inaceptable en algunas situaciones:

no es normal, pero sí posible, que dos personas tengan la mano lo suficientemente parecida como para que el sistema las confunda. Para minimizar este problema se recurre a la identificación basada en la geometría de uno o dos dedos, que además puede usar dispositivos lectores más baratos y proporciona incluso más rapidez.

- **Reconocimiento Facial – Escaner de Rostro**

Introducción

Un sistema de reconocimiento facial es una aplicación dirigida por ordenador para identificar automáticamente a una persona en una imagen digital mediante la comparación de determinadas características faciales en la imagen y en la base de datos facial.

El reconocimiento facial automatizado es relativamente un concepto nuevo. Desarrollado en los años 60, el primer sistema semiautomático para reconocimiento facial requería del administrador para localizar rasgos (como ojos, orejas, nariz y boca) en las fotografías antes de que este calculara distancias a puntos de referencia en común, los cuales eran comparados luego con datos de referencia.

El método más común utiliza una cámara para capturar una imagen de nuestra cara, que es analizada en función de ciertos 'puntos clave', como la distancia entre los ojos o la anchura de la nariz.

Funcionamiento

El primer paso en el reconocimiento facial es la adquisición de una imagen real o una imagen bidimensional del objetivo. El sistema determina la alineación de la cara basándose en la posición de la nariz, la boca, etc. En una imagen en 2D no debe estar más desplazada de 35 grados. Después de la alineación, orientación y ajuste de tamaño, el sistema genera una plantilla facial única (una serie de números) de modo que pueda ser comparada con las de la base de datos.


INAMOVIBLES. Puntos clave de la estructura de tejidos duros del rostro.

Un factor importante en los sistemas de reconocimiento facial es su capacidad para distinguir entre el fondo y la cara. El sistema hace uso de los picos, valles y contornos dentro de un rostro (los denominados **puntos duros** del rostro) y trata a estos como nodos que puedan medirse y compararse contra los que se almacenan en la base de datos del sistema. Hay aproximadamente 80 nodos en un rostro de los que el sistema hace uso (entre ellos se incluye el largo de la línea de la mandíbula, la profundidad de los ojos, la distancia entre los ojos, la forma del pómulo, la anchura de la nariz...).

Los nuevos sistemas de reconocimiento facial hacen uso de imágenes tridimensionales, y por lo tanto son más precisos que sus predecesores. Al igual que en los sistemas de reconocimiento facial en dos dimensiones, estos sistemas hacen uso de distintas características de un rostro humano y las utilizan como nodos para crear un **mapa del rostro humano en tres dimensiones** de la cara de una persona. Empleando algoritmos matemáticos similares a los utilizados en búsquedas de Internet, la computadora mide las distancias entre determinados puntos de la muestra en la superficie del rostro. Estos sistemas en 3D tienen la capacidad de reconocer una cara incluso cuando se encuentra girada 90 grados. Por otra parte, no se ven afectados por las diferencias en la iluminación y las expresiones faciales del sujeto.

Otros sistemas de reconocimiento facial

Ciertos softwares interpretan cada imagen facial como un conjunto bidimensional de patrones brillantes y oscuros, con diferentes intensidades de luz en el rostro. Estos patrones, llamados ***eigenfaces***, se convierten en un algoritmo que representa el conjunto de la fisionomía de cada individuo. Cuando un rostro es escaneado para su identificación, el sistema lo compara con todas las *eigenfaces* guardadas en la base de datos.

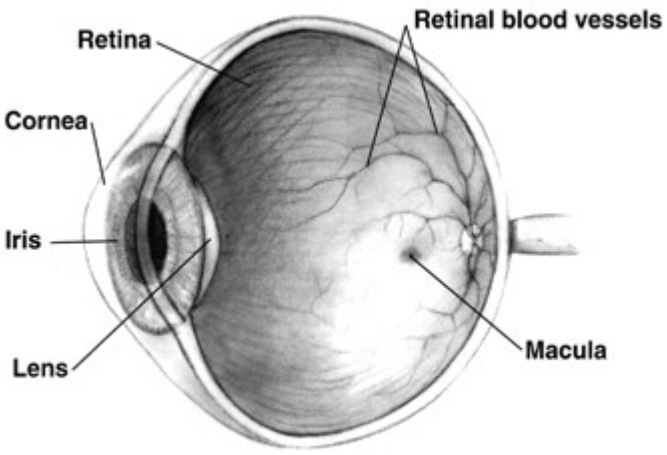
Este tipo de sistemas esta sujeto a limitaciones, como las condiciones ambientales en el momento de capturar la imagen. Así, aunque normalmente interpreta correctamente los cambios de luz en interiores, su funcionamiento al aire libre, con luz natural, es todavía una asignatura pendiente. También la posición de la cabeza y la expresión del rostro pueden influir en el "veredicto".

Un robot que se queda con tu cara

La compañía japonesa de seguridad Alsok ha presentado su nuevo **robot especializado en seguridad** y con muy buen ojo. Conectado a la base de datos fotográfica de la policía y dotado de un **sistema de reconocimiento facial**, este ser cibernético es capaz de reconocer a un delincuente entre una multitud de personas.
Cuando el robot **reconoce a una persona** buscada por la ley, automáticamente **le hace una fotografía, enviándosela a la policía al instante**. El año que viene, este robot nipón empezará a trabajar **a modo de pruebas patrullando en aeropuertos y centros comerciales**. Y es que es en este tipo de lugares donde la gran concurrencia de personas dificulta mucho las labores de videovigilancia.

- **Reconocimiento del Retina**

La **retina** es la capa más interna de las tres capas del globo ocular. Es el tejido sensible a la luz (fotorreceptor) que se encuentra en la parte posterior interna del ojo y actúa como la película en una cámara: las imágenes pasan a través del cristalino del ojo y son enfocadas en la retina. La retina convierte luego estas imágenes en señales eléctricas y las envía a través del nervio óptico al cerebro.
Los sistemas basados en las características de la retina analizan la capa de vasos sanguíneos localizados en la parte posterior del ojo.



Esta técnica requiere del uso de una fuente de luz de baja intensidad para desvelar el modelo único de la retina (irrepetible en otros individuos, como las propias huellas digitales), lo que le convierte en una de las más seguras tecnologías biométricas de "identificación" de individuos. El escaneo retinal puede ser sumamente preciso pero requiere que el usuario mire en un receptáculo y enfoque la vista hacia un punto específico, lo que redunda en un proceso intrusivo y un contacto cercano con el dispositivo de lectura. Su uso no resulta conveniente cuando se utiliza lentes.

El lector escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

Acceso Físico y Acceso Virtual

En la actualidad, la mayor aplicación de la biometría se produce en la seguridad física, para controlar el acceso a zonas restringidas. Las tecnologías biométricas permiten que el control de acceso sea automático, generalmente a través de esquemas de "verificación" de identidad.

Para el acceso a servicios virtuales, como certificaciones digitales en comercio electrónico o banca virtual, se están desarrollando sistemas biométricos que manejen la identificación remota del usuario, particularmente a través del internet. La biometría permitirá incrementar los niveles de seguridad que al momento están basados en simples claves de usuario. Las claves proporcionan solamente un mínimo de control de acceso a los datos en las redes, y la biometría es definitivamente el siguiente nivel.

5.2 biometria dinamica

- **Dinámica del tecleo**

El principal mecanismo de interacción de una persona con un ordenador es el teclado. Uno de los dispositivos de comportamiento biométrico es el análisis "key-stroke", también llamado "typing biometrics". Este último comportamiento biométrico se refiere a la velocidad con que un individuo emplea el teclado para introducir su identificación o User ID y su clave de acceso o password, lo cual puede ser indicativo de la autenticidad del usuario.

En la actualidad, la utilización de este método se vincula, fundamentalmente, a la seguridad informática y, concretamente, al uso de Internet, para aplicaciones de comercio electrónico.

Los antecedentes históricos de esta dinámica de tecleo se hallan en los primeros sistemas de telégrafos de los EE.UU., en los que se comenzó a observar la capacidad de los operadores para identificarse entre sí, en diferentes estaciones, gracias al ritmo de las pulsaciones del código morse que cada uno de ellos generaba al transmitir mensajes codificados.

Adquisición
Una muestra del tecleo en biometría está representada por el conjunto de información que un ordenador puede capturar de una secuencia de teclas pulsadas por un usuario en el teclado de una PC. En el momento de la captura de la muestra, se tendrá en cuenta:

• Tiempo entre pulsaciones (latencias): se mide el intervalo entre la pulsación de una tecla y la siguiente, dentro de una determinada secuencia de tecleo.
• Tiempo de pulsaciones (duraciones): en una pulsación específica, se mide cuánto tiempo se mantiene presionada una tecla.
• Una vez obtenidas la latencia y la duración en el tecleo, se hace un patrón estadístico y se determina una firma de tecleo para cada usuario.

Ventajas
• Bajo costo.
• No requiere de equipamiento especial.
• No es intrusivo en absoluto.
• Puede cargar un alto número de usuarios en el sistema.

Desventajas
• No es muy utilizado en el mercado.
• FA y FR son de 0,1%, pero debe complementarse con el sistema de ID y password.
• Está sujeto a alteraciones de los usuarios por lesiones sufridas en las manos.

- **Firma manuscrita:**

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además de la forma de firmar, las características dinámicas (por eso se les suele denominar Dynamic Signature Verification, DSV): el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo...

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución (aparte de una concienciación de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decrementa su seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

Por lo tanto, en lo referente al reconocimiento de firma, existen dos líneas de investigación claramente diferenciadas: reconocimiento de firma estática (off-line) y reconocimiento de firma dinámica (on-line). La principal diferencia entre ambas líneas radica en la información de firma de partida para el reconocimiento.

Técnicas de Reconocimiento Off-Line

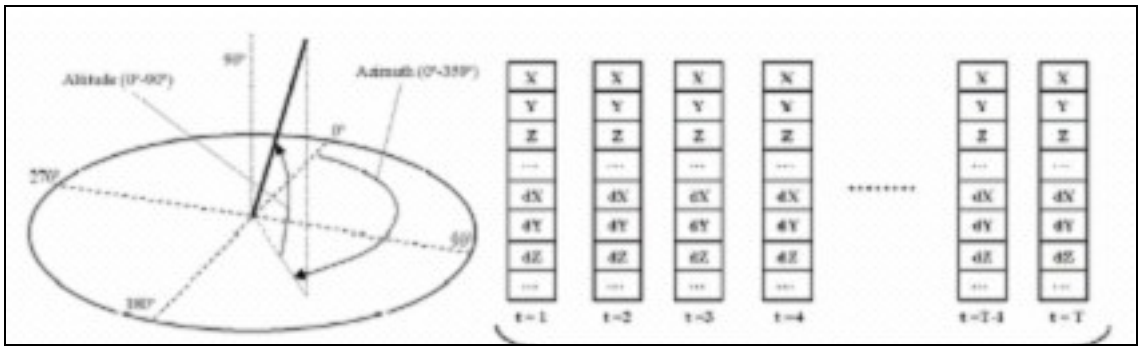
En este campo, el reconocimiento parte de firmas realizadas previamente, por lo que la única información de que se dispone es la imagen de la firma (adquisición mediante escáner). Esto va a determinar tanto las características extraídas de la firma (aproximaciones de la geometría de la firma mediante polígonos, relación de aspecto, distribución granulométrica, localización de inicio y final de trazos, concavidad de los trazos, centro geométrico de la firma o inclinación de los trazos verticales (slant), etc.), como las técnicas de procesado de la información adquirida (técnicas de procesado de imágenes en general: filtrados, umbralización, wavelet, etc.).

Técnicas de Reconocimiento On-Line

A diferencia del reconocimiento off-line, ahora la información de la firma se adquiere durante la realización de la misma por el firmante. El proceso de adquisición requerirá por tanto el empleo de dispositivos especiales, como tabletas digitalizadoras,

etc. Esto hace que los sistemas on-line dispongan de información temporal de la misma (duración total, duración de levantamientos respecto a la total, posiciones, velocidades y aceleraciones instantáneas, velocidades y aceleraciones de escritura máximas, mínimas y medias, posiciones relativas entre levantamientos y/o contactos con el papel, etc.). Además, puesto que la adquisición en estos sistemas suele consistir en el muestreo periódico de características de la firma durante la ejecución de la misma (posiciones vertical y horizontal, presión instantánea, etc.), las técnicas de procesado aplicadas a la información adquirida, son típicas de señales unidimensionales (filtrado, escalado de amplitudes, etc.).

En resumen, se podría decir que la principal diferencia entre ambas líneas de trabajo reside en la simultaneidad entre los procesos de realización de la firma y adquisición de la información para el reconocimiento. Como se puede imaginar, puesto que los sistemas on-line disponen de mayor información para realizar el reconocimiento (información estática y dinámica), serán más eficientes en lo referente a verificación de firmantes. Además, como el firmante realiza su firma de forma automática (se podría decir que el movimiento de la mano durante la ejecución de la firma es un movimiento no supervisado o pseudorreflejo) la información dinámica no es fácilmente falsificable por un impostor, y menos aún si para entrenarse en la realización de la falsificación



dispone de una imagen de la firma, donde no se conoce ni la dinámica del movimiento durante la ejecución original de la firma, ni la secuencia ordenada de trazos.

Tableta digitalizadora

Para realizar el reconocimiento de la firma on-line se puede recoger la misma con una tableta digitalizadora que proporciona posición X, posición Y, presión y ángulos de Acimut e Inclinación del bolígrafo, a una tasa de muestreo determinada en pps (puntos por segundo).

Antes de extraer características relevantes de la información adquirida de manera instantánea, es necesario realizar un preprocesado de dicha información para desechar información irrelevante, corregir valores erróneos y establecer valores comunes de referencia para todas las firmas capturadas. Los diferentes tipos de preprocesado que se le aplica a la información adquirida se describen a continuación:

- Alineación del punto inicial: El principal objetivo de esta tarea es extraer información independiente de la posición en la tableta donde se ha recogido la firma. Para conseguir esto se establece como origen de coordenadas el primer punto recogido en la firma, es decir, todas las firmas se alinearán con respecto al punto inicial. Esto permite un correcto proceso de matching.

- Segmentación de la firma: Esta tarea realiza automáticamente la decisión de si un punto determinado es o no información válida para el proceso.

Además de las cinco parámetros que se obtienen de manera instantánea a partir de la tableta digitalizadora, es posible derivar otros parámetros que permiten sacar partido de toda la información dinámica que contiene el proceso de firma. Es posible determinar la velocidad y aceleración de variación de cada parámetro lo cual deriva en un sistema más robusto y preciso.

Además de la extracción de nuevos parámetros también se utilizan algunas técnicas de normalización para establecer valores de referencia, limitar rangos dinámicos, etc.

Con esta información, tanto los parámetros dinámicos extraídos directamente como los adicionales extraídos a partir de los anteriores, se modela el proceso de firma mediante Modelos Ocultos de Markov.

Propiedades magnéticas

Otro dispositivo que se puede utilizar para el reconocimiento y validación de firmas es el basado en propiedades magnéticas de alambres amorfos. Estos alambres tienen la capacidad de cambiar su magnetización cuando están sujetos a esfuerzos pequeños de compresión-tensión, por lo que pueden usarse como transductores magnetoelásticos de este tipo de esfuerzos a señales eléctricas. El dispositivo consiste en una pluma convencional entre cuya punta y base se sujeta el alambre amorfo. El arreglo incluye una pequeña bobina de inducción, la cual detecta los cambios de magnetización producidos por los movimientos de la mano del firmante al ejecutar su rúbrica (esfuerzos de tensión-compresión), generándose así una señal eléctrica manejable. El reconocimiento de la firma consiste de tres etapas: adecuación, entrenamiento y reconocimiento; cada una de ellas involucra tanto electrónica analógica como digital.

En la etapa de adecuación, la señal se filtra, se amplifica y se homogeniza el nivel de las componentes espectrales de la señal dentro del ancho de banda en estudio. Posteriormente se digitaliza la señal empleando un convertidor A/D y un filtro digital de preénfasis. Asimismo, se caracteriza el ruido de fondo para tener una referencia que determine la parte de la señal que pertenece a la firma, obteniéndose así umbrales de energía que indican el momento para comenzar a digitalizar la señal. En la etapa de entrenamiento se digitaliza varias veces un mismo tipo de firma y se guardan en archivos para análisis posterior. Este análisis consiste en la extracción de patrones de la señal, mediante técnicas como la autocorrelación, análisis de predicción lineal, segmentación y cuantización vectorial. De esta forma se obtienen los prototipos o centroides de la firma en estudio, los cuales a su vez son características significativas de la señal (energía o coeficientes LPC por cada trama estudiada). Una vez obtenidos los patrones, se almacenan en la memoria del sistema. En la etapa de reconocimiento, se captura una firma a validar, la cual es sometida al mismo proceso de extracción de patrones, aplicándose ahora una técnica de comparación basado en la medida de distancia entre los patrones obtenidos y los previamente almacenados. En función de dicha distancia se valida o rechaza la firma.

- **Reconocimiento de voz:**

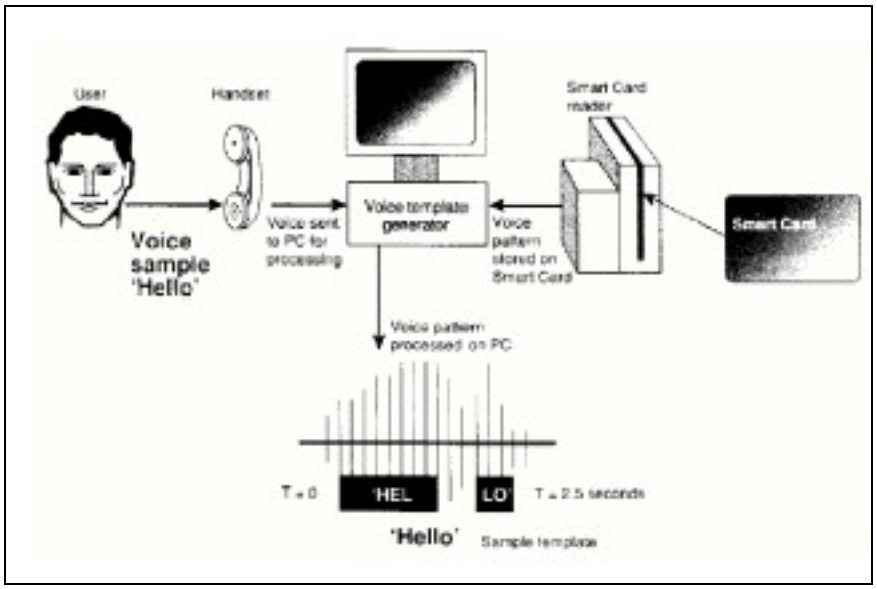
La voz es otra característica que las personas utilizan comúnmente para identificar a los demás. Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares.

En los sistemas de reconocimiento de voz no se intenta reconocer lo que el usuario dice, sino identificar una serie de sonidos y sus características para decidir si el usuario es quien dice ser. Para autenticar a un usuario utilizando un reconocedor de voz se debe disponer de ciertas condiciones para el correcto registro de los datos, como ausencia de ruidos, reverberaciones o ecos; idealmente, estas condiciones han de ser las mismas siempre que se necesite la autenticación.

Cuando un usuario desea acceder al sistema pronunciará unas frases en las cuales reside gran parte de la seguridad del protocolo; en algunos modelos, los denominados de texto dependiente, el sistema tiene almacenadas un conjunto muy limitado de frases que es capaz de reconocer: por ejemplo, imaginemos que el usuario se limita a pronunciar su nombre, de forma que el reconocedor lo entienda y lo autentique. Como veremos a continuación, estos modelos proporcionan poca seguridad en comparación con los de texto independiente, donde el sistema va `proponiendo' a la persona la pronunciación de ciertas palabras extraídas de un conjunto bastante grande. De cualquier forma, sea cual sea el modelo, lo habitual es que las frases o palabras sean características para maximizar la cantidad de datos que se pueden analizar (por ejemplo, frases con una cierta entonación, pronunciación de los diptongos, palabras con muchas vocales...).

Conforme va hablando el usuario, el sistema registra toda la información que le es útil y mediante el análisis de los sonidos que emitimos, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, cuando termina la frase, ya ha de estar en disposición de facilitar o denegar el acceso, en función de la información analizada y contrastada con la de la base de datos. El principal problema del reconocimiento de voz es la inmunidad frente a replay attacks, un modelo de ataques de simulación en los que un atacante reproduce (por ejemplo, por medio de un magnetófono) las frases o palabras que el usuario legítimo pronuncia para acceder al sistema. Este problema es especialmente grave en los sistemas que se basan en textos preestablecidos: volviendo al ejemplo anterior, el del nombre de cada usuario, un atacante no tendría más que grabar a una persona que pronuncia su nombre ante el autenticador y luego reproducir ese sonido para conseguir el acceso; casi la única solución consiste en utilizar otro sistema de autenticación junto al reconocimiento de voz. Por contra, en modelos de texto independiente, más interactivos, este ataque no es tan sencillo porque la autenticación se produce realmente por una especie de desafío-respuesta entre el usuario y la máquina, de forma que la cantidad de texto grabado habría de ser mucho mayor - y la velocidad para localizar la parte del texto que el sistema propone habría de ser elevada -. Otro grave problema de los sistemas basados en reconocimiento de voz es el tiempo que el usuario emplea hablando delante del analizador, al que se añade el que éste necesita para extraer la información y contrastarla con la de su base de datos; aunque actualmente en la mayoría de sistemas basta con una sola frase, es habitual que el usuario se vea obligado a repetirla porque el sistema le deniega el acceso (una simple congestión hace variar el tono de voz, aunque sea levemente, y el sistema no es capaz de decidir si el acceso ha de ser autorizado o

no; incluso el estado anímico de una persona varía su timbre...). A su favor, el reconocimiento de voz posee la cualidad de una excelente acogida entre los usuarios,



siempre y cuando su funcionamiento sea correcto y éstos no se vean obligados a repetir lo mismo varias veces, o se les niegue un acceso porque no se les reconoce correctamente.

Elementos de un reconocedor de voz

El reconocimiento de voz generalmente consta de los tres pasos siguientes:

- Preprocesamiento
- Reconocimiento
- Comunicación

Preprocesamiento de la señal de voz

Los sonidos consisten en cambios de presión del aire a través del tiempo y a frecuencias que podemos escuchar. Estos sonidos pueden ser digitalizados por un micrófono o cualquier otro medio que convierte la presión del aire en pulsos eléctricos. La voz es un subconjunto de los sonidos generados por el tracto vocal. En el procesamiento de la señal se extraen las características que utilizará posteriormente el reconocedor. En el proceso de extracción de características se divide la señal de voz en una colección de segmentos. Posteriormente, se obtiene una representación de características acústicas más distintivas para cada segmento. Con estas características obtenidas, se construye un conjunto de vectores que constituyen la entrada al siguiente módulo. Una de las representaciones más usadas son los coeficientes Linear Predictive Coding (LPC) y los coeficientes Mel-Frecuency Cepstrum Coefficients (MFCC).

Un reconocedor debe extraer de la señal acústica solo la información que requiere para poder reconocer una frase. Para ello la señal se muestrea a cierta frecuencia, se cuantiza y posteriormente se crean vectores de características. Estas últimos son las que utiliza el reconocedor.

Reconocimiento

En la etapa de reconocimiento se traduce la señal de entrada a su texto correspondiente. Este proceso se puede llevar a cabo de diversas formas utilizando enfoques como Redes Neuronales Artificiales (RNA) y Modelos Ocultos de Markov (HMM), entre otros.

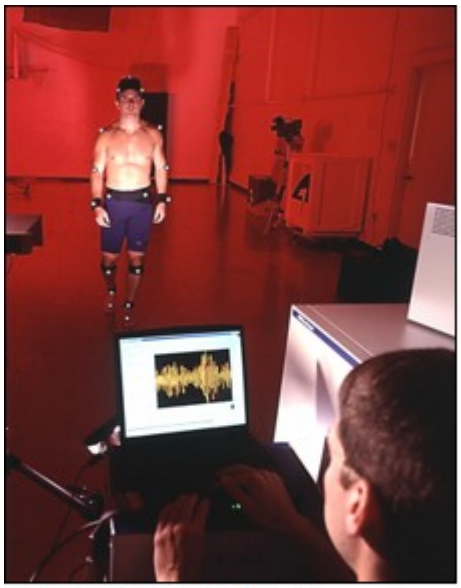
Comunicación

El resultado de la etapa de reconocimiento será enviado al sistema que lo requiere.

Cabe de todas formas hacer una mención aparte al reconocimiento biométrico de la voz como sistema eficaz para la identificación remota. Es decir, cuando una persona desea realizar una transacción o acceder a unos datos, desde, pongamos, un teléfono móvil, el reconocimiento biométrico de la voz puede ser una herramienta muy útil, y hasta muy segura si se añaden sistemas de verificación basados en desafíos dinámicos, y el registro inicial (Enrollment) se ha hecho correctamente.

- **Cadencia del paso:**

Huellas dactilares, iris, palma de la mano, voz, firma… La mayoría de las características individuales que usan los sistemas biométricos descritos hasta ahora requieren cierta proximidad o, incluso, contacto físico del individuo con un dispositivo.



HASTA LOS ANDARES. La forma de caminar de cada sujeto permite su identificación.

Esta restricción desaparece cuando la característica que se analiza es el **modo de andar**. Hace tiempo que los científicos habían observado que los seres humanos son capaces de identificar a alguien familiar por su forma de caminar. Y, aunque aún no se ha demostrado que el patrón sea totalmente único, el interés de su aplicación en sistemas de identificación es indudable. "Necesitamos esta tecnología para reconocer a los malos chicos **a distancia**", asegura John Geisheimer, ingeniero del Instituto de Investigación Tecnológica de Georgia, un centro pionero en esta tecnología.

Las principales dificultades estriban en los parámetros que influyen en nuestra forma de caminar, como el calzado, el suelo sobre el que caminamos, el nivel de cansancio del viandante, las lesiones o incluso el paso del tiempo. Por eso, de momento, se plantea su uso en combinación con otros sistemas en aplicaciones como seguridad en aeropuertos y edificios gubernamentales.

Por otro lado, un grupo de investigadores finlandeses ha desarrollado una aplicación alternativa de esta tecnología en teléfonos móviles y ordenadores portátiles. Su gaitcode (literalmente "código del paso") registra y memoriza en tres dimensiones los movimientos del propietario certificado del aparato mientras lo lleva a cuestas, de tal forma que si el dispositivo no reconoce al usuario que lo transporta, exige una contraseña para activarse. En caso de que sea falsa, el aparato y todas sus aplicaciones quedan bloqueados. Sin duda, son motivos suficientes para disuadir a cualquier ladrón.

6. Aplicaciones de los Sistemas Biométricos

La necesidad de seguridad se ha disparado con el auge de Internet, las compras on-line, las transacciones bancarias vía web o los atentados del 11 de Septiembre. La Biometría se erige como el futuro de los sistemas de seguridad y su desarrollo en los últimos años ha experimentado un crecimiento geométrico respecto a otras tecnologías de seguridad. Su eficacia potencial la hacen especialmente interesante en determinadas áreas, en las que ya se empiezan a emplear algunos sistemas biométricos.

- Entidades financieras: Es quizá uno de los sectores más preocupados históricamente por la seguridad, para evitar fraudes y pérdidas de dinero. Por ello algunas entidades ya han empezado a apostar fuertemente por los sistemas biométricos. En bancos como el Bank of America y en instituciones financieras como VISA o MasterCard ya se han implementado sistemas de reconocimiento manual y del iris para hacer frente a las grandes pérdidas debidas en parte a la poca seguridad que presentan los sistemas utilizados hasta ahora.

- Comercio electrónico y banca electrónica. Ésta ha sido una de las áreas que más ha crecido en los últimos años, y la que más ha influido en el desarrollo de nuevos sistemas de seguridad, hasta el punto de que la idea en este sector es reducir los precios de venta de los dispositivos de reconocimiento biométrico hasta que acaben formando parte del PC, integrados incluso dentro de un ratón o del teclado, o de otro tipo de equipos, como teléfonos móviles o PDA. Hay incluso investigaciones basadas en la idea de reconocer la huella dactilar al tiempo que el individuo teclea.

- Turismo y viajes. El reciente endurecimiento de varios gobiernos sobre la normativa para acceder a la zona de libre tránsito de los aeropuertos han generado la necesidad de buscar otros métodos de seguridad diferentes a los actuales. Estas aplicaciones se verán con mayor detalle mas adelante.

- Acceso a sistemas. Si a nivel local este sistema puede resultar muy beneficioso para la seguridad de las empresas, sus posibilidades serían enormes si se crease una base de datos biométricos global que permitiese identificar también a los clientes o a los mensajeros con el fin de que nadie ajeno a las actividades de la empresa pudiera franquear la entrada.

- DNI electrónico. Éste sería sin duda el salto definitivo a la tecnología biométrica: Un DNI biométrico que supondría la eliminación de tarjetas, sustituidas por ejemplo por el iris de su titular.

Como ya se ha mencionado anteriormente en lo que a seguridad en los aeropuertos se refiere hay diferentes aplicaciones que ya están funcionando hoy en día en diferentes aeropuertos del mundo:

- El aeropuerto británico de Heathrow, fue el escogido para realizar la implantación de un sistema de reconocimiento del iris y permite la identificación de los usuarios en tiempo real a través de un banco de datos previamente recogido. El sistema de biometría aplicado a la identificación se basa en ciertos

elementos morfológicos únicos y propios de cada persona, de manera que sólo la presencia física del usuario permite acceder al sistema. Tras realizar el correspondiente examen, el dispositivo biométrico se comunica con los ordenadores del aeropuerto y de la línea aérea para simplificar el control de pasaportes y el resto de registros rutinarios.
En este programa piloto participaran más de 2000 ciudadanos norteamericanos que asiduamente pasan los controles de aduanas de este aeropuerto. En un principio se les seguirá pidiendo el pasaporte pero según fuentes del servicio británico de inmigración esperan poder confiar plenamente en el examen biométrico.

- IBM y el grupo holandés de gestión de aeropuertos Schiphol han firmado un acuerdo para ofrecer tanto a líneas aéreas como a aeropuertos un innovador y rápido sistema de seguridad basado en tecnología de escaneo del iris del ojo humano. Este nuevo sistema estará basado en el ya existente "Automatic Border Pasaje" desarrollado por el grupo holandés en el aeropuerto de Ámsterdam. El sistema identifica y verifica la identidad de los viajeros a través del escaneo en tiempo real del iris, conectado a una base de datos encriptada que está almacenada en una tarjeta inteligente. El aeropuerto Schiphol de Ámsterdam es el primer aeropuerto del mundo en emplear este novedoso e instantáneo sistema de control de embarque. Con este acuerdo, IBM y el grupo Schiphol trabajarán conjuntamente para poner en el mercado la nueva solución de identificación de pasajeros en aeropuertos y líneas aéreas. Además, IBM integrará todos los sistemas, proveerá el hardware y el software necesarios y ayudará al grupo Schiphol a modificar su sistema para desarrollar nuevas soluciones que satisfagan todas las necesidades de los usuarios potenciales.
  Asimismo, IBM trabaja con Schiphol para mejorar la seguridad biométrica de este sistema de modo que pueda utilizarse no sólo para la identificación de pasajeros sino también para el etiquetado, comprobación de los pasajes, acceso y embarque. Además se tiene previsto el desarrollar algunos componentes que faciliten accesos seguros y el transporte a los empleados de los aeropuertos. El sistema procesa los datos de 4 o 5 personas por minuto, tiene una alta fiabilidad y puede tomar decisiones rápidas sobre si la persona es quien dice ser o no.

- Desde 1999, el aeropuerto de Ben Gurion (Tel Aviv) es considerado uno de los más seguros del mundo gracias a "Express Entry", un sistema de control de accesos que emplea la tecnología biométrica y que ha sido desarrollado por la empresa EDS.
  El sistema cuenta con 32 quioscos de inspección automática ubicados en las distintas terminales del aeropuerto. Por el momento, estos puestos pueden ser utilizados por todos aquellos ciudadanos israelíes que, al darse de alta en el sistema "Express Entry", dispongan de una tarjeta de crédito emitida en Israel, sus datos hayan sido validados por la base de datos del Gobierno israelí, y que en el momento de suscribir el servicio hayan enviado una muestra de las características biométricas de su mano. Esta muestra es la que el sistema utilizará posteriormente para verificar, con un gran nivel de seguridad, la identidad del pasajero.
  La descripción del funcionamiento del sistema es muy sencilla: en primer lugar, el pasajero se identifica mediante la lectura de los datos de su tarjeta de crédito. Una vez que el sistema lo autoriza, se abre la puerta de acceso. En este

momento, el pasajero debe introducir su mano en el lector biométrico, el cual mide su tamaño y forma y compara esta lectura con la "muestra" archivada en la base de datos de "Express Entry". Al mismo tiempo, el sistema envía una petición de información a la base de datos del Gobierno israelí acerca de la identidad del pasajero. Ambas informaciones se cruzan, y si son correctas, se permite el acceso al pasajero. De lo contrario, una alarma alerta al servicio de seguridad del aeropuerto del posible pasajero sospechoso. Todo ello en algo menos de 20 segundos.
El software que utiliza este innovador sistema de control de accesos, diseñado por Recognition Systems Inc, tiene un margen de error del 0,2%. Desde su implantación, el sistema "Express Entry" recoge una media de 50.000 entradas mensuales.

- Alguna de sus aplicaciones más interesantes de reconocimiento de iris se ha llevado a cabo en cajeros automáticos para verificar la identidad de los clientes de un banco, como es el caso del nuevo dispensador puesto en marcha recientemente por Argentaria en una de sus sucursales de Madrid.
  Se trata de un cajero automático que, diseñado por la compañía NCR, incorpora un sistema de reconocimiento del iris que sustituye a la tradicional identificación mediante el número secreto personal o PIN. Para realizar cualquier transacción, el cliente ha de situarse frente a este cajero, el primero de este tipo instalado en España, para que el sistema de identificación del iris lo reconozca.
  El sistema, por tanto, fotografía el ojo y transforma la imagen en dígitos. Una vez convertida en un código, esa información es contrastada con los datos almacenados en el archivo, que confirma si el usuario es o no el propietario de la tarjeta. El sistema genera así una imagen digital del iris del cliente y graba la tarjeta de banda magnética o chip con la nueva funcionalidad integrada. De esta forma, se obtiene una gran seguridad en cuanto al acceso a datos financieros ya que, si la huella del iris del usuario no coincide con la existente para ese cliente, no se le ofrece ese servicio.

  El Royal Bank de Canadá es otra de las entidades que dispone de un cajero automático de este tipo, desarrollado por NCR. Denominado Stella, este dispensador es capaz de reconocer al usuario, saludarlo por su nombre, escucharlo, hablarle, ofrecerle un menú personal con sus servicios y funciones favoritos, e incluso felicitarle en el día de sus cumpleaños si decide realizar cualquier transacción financiera en esa fecha. Las nuevas tecnologías en las que se basa Stella incluyen la biometría o el sistema de reconocimiento de iris, el reconocimiento de voz -que permite hablar con el terminal como con un empleado del banco-, y un sistema integrado capaz de comunicarse con el teléfono móvil del usuario y descargar la información de las últimas operaciones realizadas en el asistente personal digital (PDA).

  Por tanto, las posibilidades que ofrece esta nueva tecnología son apreciadas por la mayor parte de sus usuarios.

  De hecho, la aceptación del sistema de reconocimiento del iris en las pruebas piloto de cajeros automáticos que NCR tiene instalados en el banco británico Nationwide Building Society ha sido masiva.

Según un estudio realizado por Pegram Walters Group, realizado entre 1.000 clientes durante seis meses en el Reino Unido, la totalidad de los usuarios de este dispensador consideran que el sistema es fiable y seguro.

Otros lugares en los que se han empleado distintos sistemas biométricos de seguridad son:

- Huella Digital:
  - Control de acceso a áreas en el Pentágono
  - Acceso a computadoras de redes financieras en Italia
  - Automated Banking Terminal en Australia
  - Aduana y inmigración en Ámsterdam
  - Control de acceso Expo'92 Sevilla

- Mano:
  - San Francisco Intl Airport (control acceso operaciones)
  - Lotus (visitantes fuera de áreas reservadas)
  - University of Georgia (alimentos consumidos)
  - Carcel en Jessup
  - Aeropuerto Kenneddy y Newark (inspección automática de pasaporte y control de personas que se registraran como pasajeros frecuentes)
  - Cámara de Diputados y Senado en Colombia para evitar fraude en las votaciones

7. Conclusiones

Los presentados hasta aquí son los sistemas biométricos principales actualmente en uso y desarrollo, pero no son los únicos. Al igual que en muchos otros campos, la tecnología sigue avanzando tanto en la mejora de las técnicas utilizadas en los sistemas ya existentes como en el desarrollo de nuevas técnicas. Esto es consecuencia de una demanda cada vez mayor de seguridad en un gran número de campos.

El futuro de los sistemas biométricos se ven reflejado en diferentes aspectos que se muestran a continuación.

7.1.Costos Más Bajos

Lo único que se puede decir con certeza acerca del futuro de la industria de biométricos es que está creciendo.

Hoy en día los sistemas biométricos tienen un lugar importante en una sorprendente variedad de aplicaciones, más allá de controlar el acceso. Inmigración, control de asistencia, asilos, guarderías y centros de atención médica, programas de beneficencia y puntos de venta son solo unas cuantas de las aplicaciones donde se utilizan biométricos.

Del incremento en las ventas definitivamente resultará una reducción en los costos, tal y como ha sucedido con la reducción del precio del poder de procesamiento en las computadoras.

7.2. Incremento en la Precisión

Cuando los sistemas biométricos hicieron su aparición en aplicaciones de alta seguridad, su consideración principal era mantener afuera a quién no estaba autorizado. Se prestó poca atención a dejar entrar a los que estaban autorizados. Para esas aplicaciones, una tasa baja de Falsa Aceptación era el requerimiento más importante.

A medida que estos sistemas se fueron moviendo a aplicaciones comerciales, la Tasa de Falso Rechazo fue tomando importancia. Algunos bancos lo dejaron claro al sugerir que un biométrico apropiado para verificación de tarjetas de crédito necesitaría una Tasa de Falso Rechazo de 1: 100,000 y una Tasa de Falsa Aceptación de 5%.

Las Tasas de Falsa Aceptación requeridas para dispositivos comerciales de control de acceso son severas, pero la necesidad de Tasas de Falso Rechazo también deben ser bajas. Para un uso extendido de biométricos a nivel comercial se requerirán bajas Tasas de Falso Rechazo en sistemas intuitivos y fáciles de usar.
Últimamente los fabricantes han dedicado una gran energía a esta área del desarrollo y continuarán haciéndolo.

7.3. Nuevas Tecnologías

Las ventas no son la única parte de la industria biométrica que está creciendo. El número de tcnologías y fabricantes también se está expandiendo. Algunas casas están explorando tecnologías con nuevos atributos fisiológicos para identificación, mientras que otras están mejorando tecnologías actualmente en uso.

El reconocimiento facial ha recibido una buena cantidad de atención en estos últimos años. La gente identifica fácilmente a otras personas por su cara, pero automatizar esta tarea no es para nada sencillo. Mucho del trabajo en esta área se ha dedicado a capturar la imagen facial. Una compañía está experimentando con una técnica única: examinar el patrón térmico creado por los vasos sanguíneos en el rostro.

Otra tecnología nueva examina el patrón de las venas y arterias en la palma de la mano y algunas compañías están desarrollando sistemas que identifican individuos por la huella de toda la palma de la mano. Inclusive se está desarrollando una "nariz electrónica" que pueda distinguir personas por su olor.

8. Técnicas para burlar dispositivos biométricos

Como es de esperarse no existe ninguna técnica de autenticación que sea cien por cien segura. Los dispositivos biométricos no son la excepción

Científicos japoneses de la Universidad de Yokohama usaron gelatina común para crear dedos y huellas dactilares falsas y así burlar los sistemas de seguridad - no solo consiguieron hacer esto (con resultados positivos en 80% del test) sino que además desarrollaron un método para obtener falsificaciones muy convincentes de huellas digitales marcadas en vasos y otros vidrios.

Para obtener los moldes de dedos falsos, inicialmente un equipo de investigadores usaron la gelatina (no en estado liquido) recién colocada en un molde y dedos de goma normalmente usados por fabricantes de modelos. Cada proceso tarda unos pocos minutos y cuesta menos de 30 reales.

Para retirar las huellas de los vasos, los científicos usaron pegamento sobre los detritos del cuerpo que son dejados por el sudor y por las células humanas en el vidrio. Después de fotografiar con cámara digital la huella grabada en el pegamento, ellos usaron el Photoshop para enfatizar las diferencias entre los surcos y las ondulaciones.

Después, esta imagen fue transferida a una lamina fotográfica revestida de cobre, que a su ves fue usada para crear el molde tridimensional de un dedo falso con huellas digitales. En este proceso, una vez más los científicos japoneses consiguieron engañar los sistemas de seguridad biométrico en el 80% de las veces.

Bibliografía

Algunos de los enlaces que han servido como fuente de documentación para el trabajo son:

http://www.biotech.aikons.com/Huella/teoria/huella_t.htm

http://tecnociencia.es/monograficos/biometria/biometria2.html

http://www.tec-mex.com.mx/promos/bit/bit0903-bio.htm

http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

http://biometrics-on.com/es/reconocimiento-biometria-facial-escaner-de-rostro.asp

http://www.mundogar.com/ideas/reportaje.asp?ID=14904

http://www.infochannel.com.mx/infovar/noticiasvars.asp?id_nota=13621&ids=1