Una mirada a la biometria

A glance to the biometric

Milton Ruiz Marín, Ing.; Juan Carlos Rodriguez Uribe, Est. & Juan Carlos Olivares Morales, Ing.
Universidad del Magdalena
mamancana@gmail.com; jcrodriguezu@gmail.com; kisjuan@gmail.com

Recibido para revisión: 14 de Febrero de 2008, aceptado 25 de Agosto de 2009, versión final 4 de Septiembre de 2009

Resumen— La Identificación Biométrica, es decir, el reconocer a una persona por alguna característica biofísica o de comportamiento, está tomando cada vez más importancia en la actualidad; su importancia radica en las limitaciones de los sistemas actuales de identificación personal, los cuales en su mayoría, están restringidos al uso de dispositivos externos como tarjetas inteligentes y claves personales. La biometría está basada en el principio de que cada individuo es único y posee rasgos físicos distintivos (rostro, huellas digitales, iris de los ojos, etc.) o de comportamientos (la voz, la manera de firmar, etc.), los cuales pueden ser utilizados para identificarla o validar restricciones de acceso. En los últimos años las aplicaciones de la biometría han aumentado y, partiendo de la identificación, se ha llegado a la utilización de sistemas de seguridad de alta complejidad y a otros usos, como el de las armas con identificación biométrica y en medicina para detección de algunas patologías.
En este artículo se presenta una introducción general a la Biometría, comentando las diversas etapas de que se compone un Sistema de Identificación Biométrica, así como un recorrido por las principales técnicas utilizadas en la actualidad.

Palabras Clave— Biometría, Sistema, Patrón, Identificación, Huella, Reconocimiento.

Abstract— The Biometric Identification, recognizing a person by some biophysics characteristic or of behaviour, is becoming increasingly important today. its importance lies in the limitations of current systems for personal identification, which mostly are restricted to using external devices like smart cards and personal codes. The biometry is based on the principle of which each individual is unique and owns distinguishing physical characteristics (face, fingerprints, rainbow of the eyes, etc) or of behaviors (the voice, the way to sign, etc), which can be used to identify it or to validate access restrictions. In the last years the applications of the biometry have increased and, based on the identification it has been the use of security systems of high complexity and other uses, such as weapons with biometric identification and medical screening for some diseases.
This article presents a general introduction to biometrics, commenting on the various stages that make up a biometric identification system and a tour of the main techniques used today.

Keywords— Biometry, System, Pattern, Identification, Tread, Recognition.

I. INTRODUCCIÓN

Desde la antigüedad, el hombre ha tratado de controlar el acceso a lugares, o a información que considera valiosa, también desde siempre hemos tratado de identificar a las personas que nos rodean o que pertenecen a nuestro mismo clan; los sobres lacrados con el sello real, el conocimiento de un santo y seña, la utilización de una vestimenta especifica, la posesión de una llave o de una clave han permitido desde siempre el acceso a lugares restringidos. En la sociedad digital, se han sustituido los objetos de antaño por contraseñas, números PIN, certificados digitales, firmas digitales y tarjetas inteligentes.

Sin embargo estos objetos o datos pueden ser robados, falsificados, filtrados o deducidos. Es fácil adivinar la contraseña o conocer el numero PIN de una persona. Lo que nos lleva a pensar que para permitir autenticar a una persona, ya sea para acceder a un lugar físico, para efectuar una transacción bancaria o para realizar una compra se deben buscar métodos que no dependan de una "llave" determinada, sino que la propia persona sea la llave que le permita autenticarse. Es aquí donde entra la biometría.

La biometría es un área de investigación ampliamente estudiado ya que desde hace varios siglos los seres humanos nos hemos identificado por medio de este sistema, lo que sí ha

estado en constante evolución son las tecnologías y los sistemas que basan en datos biométricos la identificación de las personas; en general, el concepto de biometría proviene de las palabras bio (vida) y metría (medida) lo que significa que los sistemas o equipos biométricos miden e identifican alguna característica propia, tanto física como de comportamiento de una persona. Esto ha dado pie a utilizar estas mediciones como metodologías de seguridad que permiten el reconocimiento de características físicas intransferibles de las personas para su identificación [1].

El presente trabajo se centra en explicar las generalidades de los sistemas biométricos y de las características físicas y de comportamiento más utilizadas en dichos sistemas para después hacer un recorrido por las aplicaciones prácticas más sobresalientes y por último terminar con las conclusiones generales del tema.

II. SISTEMAS BIOMETRICOS

Según el Diccionario de la Real Academia Española, se define BIOMETRÍA como "Estudio mensurativo o estadístico de los fenómenos o procesos biológicos". Esta definición se hace más específica cuando se utiliza el término de Biometría dentro del campo de la Identificación de Personas. Según el Biometric Consortium, la Biometría son métodos automáticos de reconocimiento de una persona basados en características fisiológicas o de comportamiento [2]. Expuesto de una forma más simple, la Biometría consigue reconocer a una persona mediante una imagen de su rostro o mediante la impresión de su huella dactilar.

Como es lógico, la capacidad de identificación biométrica es algo innato en los seres vivos, ya que poseen la característica de reconocer a sus semejantes. Pero la Biometría como ciencia de estudio de la individualidad de las personas, nace seriamente a finales del siglo XIX. Es entonces cuando en Europa se extendió con gran éxito el sistema francés de Identificación Antropométrica de Bertillon [3 - 6], en el que se realizaban numerosas medidas del cuerpo de una persona. Fue precisamente un experto en este sistema, Sir Francis Galton, quien realizó a finales del siglo XIX estudios muy detallados sobre la huella dactilar, estudiando su estabilidad, unicidad y morfología. Sus trabajos, complementados por los de Vucetich, Henry, Hershel y Faulds (cada uno de forma independiente), consiguieron que la identificación por huella dactilar fuera aceptada y se convirtiera en el método de identificación biométrica más utilizado por la policía mundial.

La evolución de la tecnología, así como la dificultad, en muchas ocasiones, de captar la huella de una persona y, por supuesto, el progreso por parte de los supuestos criminales de evitar su posible identificación mediante esos métodos, han puesto a pensar en nuevas vías para realizar la identificación biométrica, desarrollándose diversas soluciones alternativas, como las basadas en voz, rostro, etc. [7]

Etapas en un sistema de identificación biométrica

Las técnicas de identificación biométrica son muy diversas, ya que cualquier elemento significativo de una persona es potencialmente utilizable como elemento de identificación biométrica. Sin embargo, incluso con la diversidad de técnicas existentes, a la hora de desarrollar un sistema de identificación

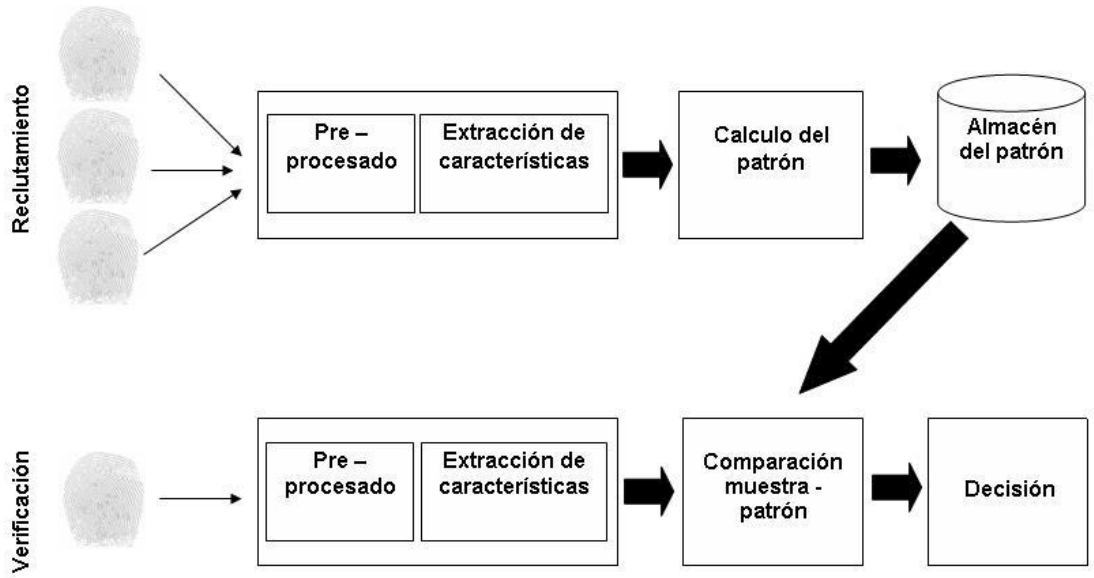


Figura 1: Etapas en un Sistema de Identificación Biométrica **[7]**

biométrica, se mantiene un esquema totalmente independiente de la técnica empleada. Los sistemas, tal y como se puede ver en la **Figura 1**, se basan en dos fases totalmente diferenciadas:

a. Reclutamiento: en esta fase, se toma una serie de muestras del usuario, y se procesan, para posteriormente extraer un patrón, el cual se almacenará y será el conjunto de datos que caracterizará a ese usuario. Si se captura más de una muestra, el patrón suele ser el resultado de una media de las características obtenidas. Este proceso se hace de forma supervisada, es decir, existe una persona encargada de controlar cómo se produce la captura de los datos, así como de asegurar la identidad de la persona que se está reclutando en el sistema. Además, se aprovecha esta fase para enseñar al usuario cómo funciona el sistema y aclararle todas las dudas que pudiera tener.

b. Utilización: una vez que se tiene almacenado el patrón del usuario, éste puede utilizar el sistema con normalidad, y sus características son comparadas con el patrón almacenado, determinando el éxito o fracaso de esa comparación.

Pero como se observa en la **Figura 1**, cada una de las fases mencionadas, está basada en una serie de bloques que hacen que las características biológicas o de comportamiento del individuo acaben siendo un elemento que lo identifique. Estas fases son:

• **Captura:** se toman los datos biofísicos o de comportamiento del sujeto. La toma de los datos depende, evidentemente, de la técnica biométrica empleada, también se pueden encontrar muchas variaciones una misma técnica biométrica. Por ejemplo, la huella dactilar puede ser obtenida por cámara de vídeo, ultrasonidos, efecto capacitivo sobre un semiconductor o exploración por láser. Esta fase es muy importante ya que en ella está contenida la interfaz hombre-máquina y el sensor para la captura de la información biométrica, esto repercute directamente en el rendimiento del sistema biométrico ya que un diseño pobre de la interfaz puede resultar en una tasa alta de fallos al adquirir la información **[8]**. Una forma de medir la eficiencia de esta fase es con el error de adquisición (Tasa de error de adquisición, o FTA) el cual denota la proporción de veces en la que el dispositivo de captura falla al adquirir la característica biométrica.

• **Pre-procesado:** en este bloque se adecuan los datos capturados para facilitar el tratamiento que tiene que realizar el siguiente bloque. Este bloque se encarga, dependiendo de la técnica, de tareas como: reconocer el inicio de una frase y medir el ruido de fondo, binarizar y hacer una extracción de bordes de la imagen, localizar la muestra, rotarla y ampliarla (o reducirla), para que se encuentre entre los márgenes que reconoce el algoritmo siguiente, etc.

• **Extracción de Características:** se puede considerar el bloque más significativo de la técnica a utilizar. En esta fase, los datos son procesados y un conjunto de características discriminatorias son extraídas para representar los rasgos medidos, estas características forman una *plantilla* [4] la cual es almacenada en una base de datos para su posterior uso. Es en este bloque en el que se fundamenta la capacidad del sistema de distinguir entre sujetos. Sin embargo, debido a distintas aproximaciones al problema, este bloque puede seguir orientaciones muy diversas, e incluso contradictorias, para la misma técnica, creándose distintos métodos dentro de una misma técnica. Por otro lado, en algunas ocasiones, el desconocimiento sobre las características que se deben extraer, lleva a utilizar técnicas basadas en Redes Neuronales, que mediante entrenamiento de las mismas, se intentan adecuar a los resultados esperados.

• **Comparación:** una vez extraídas las características de la muestra capturada, se han de comparar éstas con las previamente almacenadas, es decir, el patrón o plantilla. Lo más importante que hay que dejar claro cuando se habla de este bloque, es que no se trata de una comparación binaria (o de igualdad), sino que la variación de las muestras, por diferencias en la captura o leve variación de las características de sujeto, hacen que la comparación dé como resultado un puntaje ó probabilidad de semejanza. Por tanto, para determinar el éxito o fracaso de la comparación, habrá que determinar un umbral *n* de tolerancia en esa probabilidad. La comparación puede estar basada en cada una de las distintas posibilidades que ofrece la Teoría de Reconocimiento de Patrones **[9]**: Métricas como la Distancia Euclídea, Distancia de Mahalanobis o Distancia de Hamming ó Estadísticas utilizando funciones de distribución, clasificadores bayesianos, o técnicas basadas en modelado de problemas como Redes Neuronales, Modelos de Mezclas de Gausianas, etc. Sobre los conceptos expuestos cabe hacer un par de puntualizaciones. La primera de ellas tiene que ver con la elección del umbral, ya que si éste se incrementa, hará que el sistema se "relaje" y permita una mayor probabilidad de accesos por parte de personas no autorizadas (Tasa de Falsa Aceptación, o FAR), mientras que si se disminuye, el sistema se volverá muy restrictivo, aumentando la probabilidad de rechazo de personas autorizadas (Tasa de Falso Rechazo, o FRR). Por lo tanto, la elección del umbral dependerá del grado de seguridad, y amigabilidad hacia el usuario, que se le quiera dar al sistema. Estos dos valores (FAR y FRR) pueden ser observados de una mejor manera en una gráfica de compensación de error (*Detection Error Tradeoff, o DET*) la cual muestra FRR contra FAR en varios valores del umbral *n* en escala de la desviación normal como se ve en la Figura 2.

El modo en el que se hace el reclutamiento no es tampoco trivial. En algunas técnicas basta una única toma de los datos, mientras que en otras puede ser necesario tomar varias muestras y en distintas sesiones (días o semanas), tal y como ocurre, por ejemplo, en los sistemas basados en voz. A todo esto habrá que añadir que si el reclutamiento resulta muy pesado, los usuarios del sistema tenderán a rechazar el sistema de identificación, por lo que habrá que buscar una solución de compromiso entre la comodidad del usuario, y la obtención de un patrón óptimo. En

el reclutamiento también se presenta un tipo de error conocido como error de reclutamiento (Tasa de error de reclutamiento, o FTE) el cual indica la proporción de usuarios que no pueden ser enrolados correctamente en el sistema biométrico.

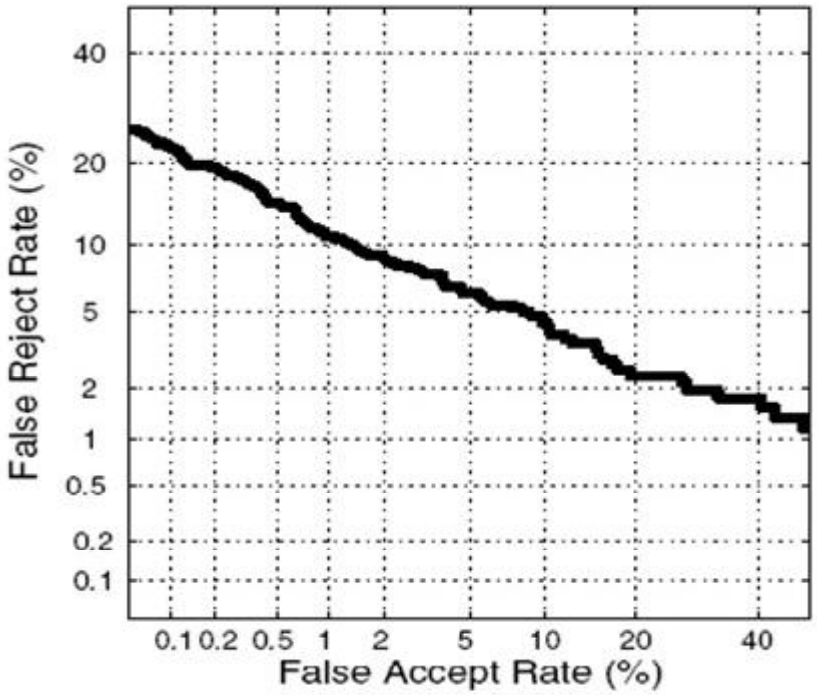


Figura 2. Rendimiento de un sistema biométrico resumido en un gráfico DET (La curva de rendimiento es calculadas usando los resultados de comparación de el Face-G de la base de datos de [16]), el cual muestra los valores de FRR contra FAR en escala de la desviación normal.

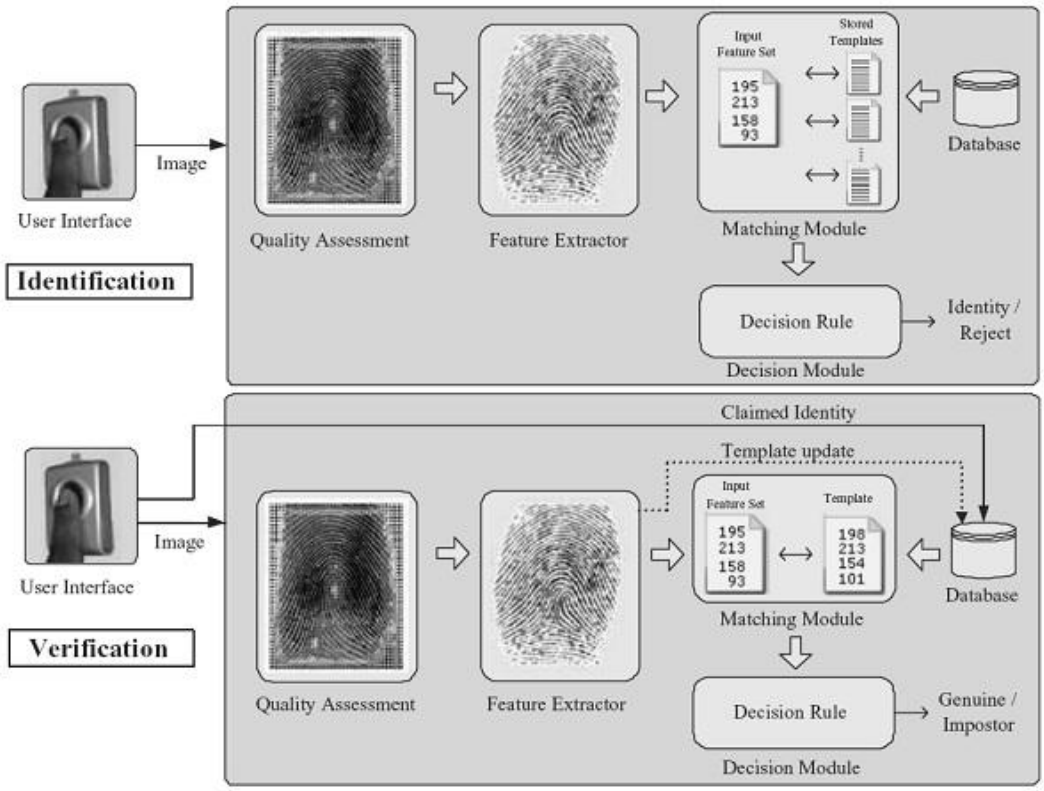


Figura 3: Reconocimiento (arriba) y Autenticación (abajo), diferencias entre las 2 fases **[8]**.

c. Reconocimiento / Autenticación: Hasta ahora se ha estado hablando siempre de Identificación Biométrica; sin embargo, la Identificación se puede realizar basándose en dos esquemas de funcionamiento del Sistema Biométrico: Reconocimiento y Autenticación, en la Figura 3 se puede ver claramente que la principal diferencia entre los esquemas se encuentra en el modulo de coincidencias o matching module ya que en este modulo se procesan las coincidencias entre las características.

• **Reconocimiento:** también llamado, en algunos textos, simplemente Identificación (lo cual llega a causar cierta confusión). Se basa en identificar a un usuario dentro de todos los usuarios que ya se encuentran en el sistema. Por lo tanto, se comparan las características extraídas con los patrones de todos los usuarios reclutados por el sistema. Este esquema de funcionamiento, necesario para muchas aplicaciones, tiene como inconvenientes la necesidad de una Base de Datos de patrones (con los requisitos oportunos de capacidad de almacenamiento y seguridad de los datos) y la existencia de una red de comunicaciones, siempre on-line, que comunique los puestos de identificación con la Base de Datos. El resultado de la comparación puede ser: siempre positivo (es decir, se identifica siempre con el usuario que ha dado una probabilidad más alta), o puede indicar rechazos (si el usuario con la mayor probabilidad no supera un determinado **umbral**).

• **Autenticación:** también llamado sencillamente Verificación. Trata de responder a la pregunta: ¿es este sujeto la persona que dice ser? En este esquema de funcionamiento, el usuario, al que se le toman sus características biométricas, también comunica su identidad. El sistema se encarga, entonces, de comparar las características extraídas, con el **patrón** del usuario indicado. Si la comparación supera un determinado **umbral** de similitud, se considera que el usuario es el indicado, rechazando la comparación en caso contrario. El patrón del usuario puede estar almacenado en una Base de Datos, tal y como se hace en los sistemas de Reconocimiento, o, si el patrón es suficientemente pequeño, en un sistema portátil de información como puede ser una tarjeta. En este último caso no son necesarias ni la Base de Datos ni la red de comunicaciones de los sistemas de Reconocimiento.

d. Medición del rendimiento: Uno de los aspectos más importantes para el funcionamiento de un sistema biométrico es su rendimiento, este se puede resumir utilizando medidas de un solo valor como la tasa de error igual (*Equal Error Rate, o EER*) y el valor d-prima (*D-prime value, o* d'). El primero se refiere a un punto en el DET (ver Figura 2) donde el FAR es igual al FRR, un valor bajo en el ERR indica un mejor rendimiento. El valor d-prima () mide la separación entre las medias de las distribuciones de probabilidad del genuino y el impostor en unidades de desviación estándar, este se define como:

$$d' = \frac{\sqrt{2}\left|\mu_{genuino} - \mu_{impostor}\right|}{\sqrt{\sigma^2_{genuino} + \sigma^2_{impostor}}}, \quad \textit{Ecuación 1}$$

Donde $\mu's$ y $\sigma's$ son las medias y las desviaciones estándar, respectivamente, de las distribuciones del genuino y del impostor. Un valor *d-prime* alto indica un mejor rendimiento del sistema biométrico.

III. TÉCNICAS BIOMÉTRICAS

Aunque las características de la huella dactilar son, sin lugar a duda, las más ampliamente utilizadas para realizar una identificación biométrica, cualquier otra característica biológica o del comportamiento de una persona puede ser usada para realizar la identificación, siempre que dichas características se demuestren propias y únicas de la persona a identificar. Las distintas técnicas que se están estudiando actualmente se pueden ver descritas en **[10]**, siendo:

• **Huella Dactilar:** tal y como ya se ha comentado, es, sin lugar a duda, la más estudiada y probada. Existen numerosos estudios científicos que avalan la unicidad de la huella de una persona y, lo que es más importante, la estabilidad con el tiempo, la edad, etc. En estos aspectos es una técnica que lleva mucha ventaja a las demás, debido a su siglo de existencia. Su captura recibe diversas formas, las cuales dependen de la innovación tecnológica. Actualmente los dispositivos de captura se pueden agrupar en 3 familias: Ópticos, de estado sólido, y ultrasonido. Para la extracción de características de esta técnica se tienen en cuenta características de las huellas como lo son: crestas (*rides*), valles (*valleys*) y algunas singularidades como: curvas (*loops*), bifurcaciones (*deltas*), espirales (whorls) Ver **Figura 4.** También es posible encontrar otro tipo de características denominadas minutas las cuales son discontinuidades o formas de terminación de los valles **[14]**

Entre las técnicas actuales más utilizadas para la extracción de características y de emparejamiento de coincidencias de imágenes de huellas dactilares encontramos según **[14]**:

• Orientación y Frecuencia Local de la Cresta: La orientación local de la cresta en el punto (x, y) es el ángulo θ_{xy} tal que las crestas de la huella dactilar, cruzan un pequeño vecindario arbitrario centrado en (x, y), formado con el eje horizontal. La frecuencia local de las crestas (o densidad) f_{xy} en el punto (x, y) es el número de de crestas por unidad de longitud a lo

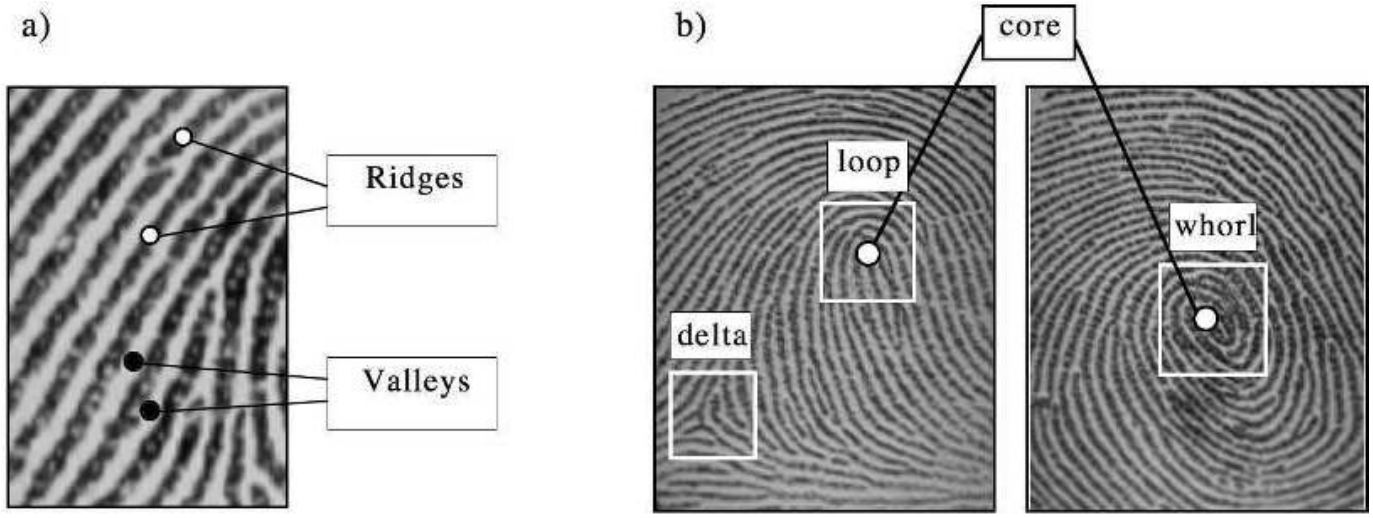


Figura 4. a) Crestas y Valles en una imagen de huella dactilar; b) Regiones Singulares (Cuadros blancos) y núcleos (Círculos) **[14]**

largo de un segmento hipotético centrado en (x, y) y ortogonal a la orientación local de las crestas θ_{xy}.

• Segmentación: La segmentación es una tarea de procesamiento de imágenes la cual consiste en separar el área de la huella dactilar del fondo, entre los métodos más utilizados para logra esto encontramos: segmentación por umbral local, segmentación por umbral adaptativo, entre otras.

• Mejoramiento y Binarización: El objetivo de esta técnica es mejorar la claridad de la estructura de las crestas en regiones recuperables y marca las regiones irrecuperables como ruido para un posterior procesamiento. En este ámbito, la técnica más empleada es la de *filtros contextuales*, en los cuales las características del filtro cambian de acuerdo al contexto local.

• Técnicas Basadas en Correlación: Digamos que $I(\Delta x, \Delta y, \theta)$ representa la rotación de una imagen de entrada I por un ángulo θ alrededor del origen y corrida por ΔX y Δy pixeles en dirección *x, y,* respectivamente. La similitud entre dos huellas dactilares T e I se define como:

$$s(T, I) = \max_{\Delta x, \Delta y, \theta} CC(T, I^{(\Delta x, \Delta y, \theta)}), \quad \text{Ecuación 2}$$

Donde $CC(T, I) = T^T I$ es la covarianza cruzada entre T e I.

• **Iris:** esta técnica fue impulsada por John G. Daugman en 1993, tal y como se muestra en [11]. Los resultados obtenidos son, sin lugar a dudas, unos de los mejores de la actualidad [7, 12], teniendo en cuenta que las características en las que está basada, el patrón de la textura del iris ocular, permanece inalterable durante la vida del sujeto debido a la protección que le proporciona la córnea.

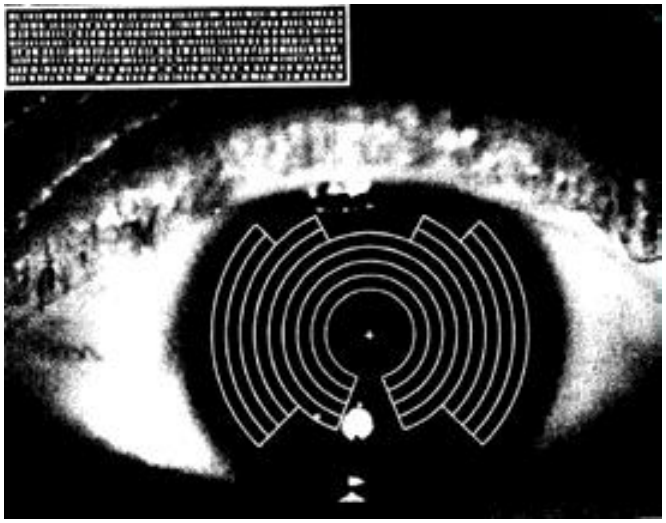


Figura 5: Reconocimiento del Iris [13]

• Oreja: desde un punto de vista forense, se ha demostrado que la oreja de un individuo posee muchas características propias del mismo. Es una técnica de estudio muy reciente y su gran inconveniente III inconveniente es la necesidad de que el usuario descubra su oreja frente a una cámara, lo cual puede ser incómodo en el caso de personas con el pelo largo, o de determinados condicionantes sociales, de educación, religiosos, etc.

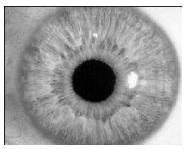
TECNICA	VENTAJAS	INCONVENIENTES
 VOZ	-Muy bajo costo -En algunas aplicaciones puede resultar inapropiables para el usuario(por ejemplo servicios telefónicos)	-Rendimiento bajo. -Se está estudiando el aumentar la unicidad y la estabilidad
 HUELLAS	-Muy estudiado/desarrollado -Unicidad, estabilidad y rendimientos 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 cornea. -FAR prácticamente nula. - Fácil detención de ojo vivo	-Alto coste. -Inicialmente incomodo 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

Tabla 1: Comparativa entre las técnicas más importantes [7]

• **Dinámica de Teclado:** se basa en reconocer a una persona por la forma en que escribe a máquina. Se mantiene la hipótesis de que el ritmo de teclado es característico de una persona, y prototipos existentes parecen reafirmar esa hipótesis. Sin embargo, además de ser una técnica basada en el comportamiento, y por tanto potencialmente emulable, tiene la limitación de no poder ser utilizada con usuarios que no tienen facilidad a la hora de escribir a máquina.

• **DNA:** sin lugar a dudas, la única técnica capaz de identificar unívocamente a una persona. Su potencia en el campo de la identificación choca con la dificultad en el desarrollo de sistemas automáticos de identificación en tiempo real y cómodo para el usuario. Los últimos intentos tratan de tomar la muestra mediante captación del sudor del sujeto. Sin embargo habría que estudiar la reacción de los usuarios frente a ese modo de captar la muestra.

• **Firma:** utilizada desde más antiguo que la huella dactilar, esta técnica siempre se ha visto entredicha por la posibilidad de falsificaciones, debido a que está basada en características del comportamiento. Las nuevas tecnologías facilitan realizar, no sólo el estudio de la firma ya realizada, sino también el estudio del acto de firmar, captando mediante un bolígrafo especial o una tableta gráfica, parámetros como velocidad, paradas, posición del bolígrafo, fuerzas, etc.

• **Olor:** técnica muy reciente, se basa en reconocer a una persona a través de su olor corporal. Las grandes incógnitas se encuentran en ver el rendimiento de este tipo de técnica frente a perfumes, colonias, olores ambientales, contactos con otras personas, etc.

• **Voz:** es una técnica con uno de los mayores potenciales comerciales: los servicios de atención telefónica personal, como la Banca Telefónica. Es una técnica que ha venido estudiando durante varias décadas, existiendo innumerables métodos para realizar, tanto la extracción de características, como la comparación [2] Ver Figura 6.

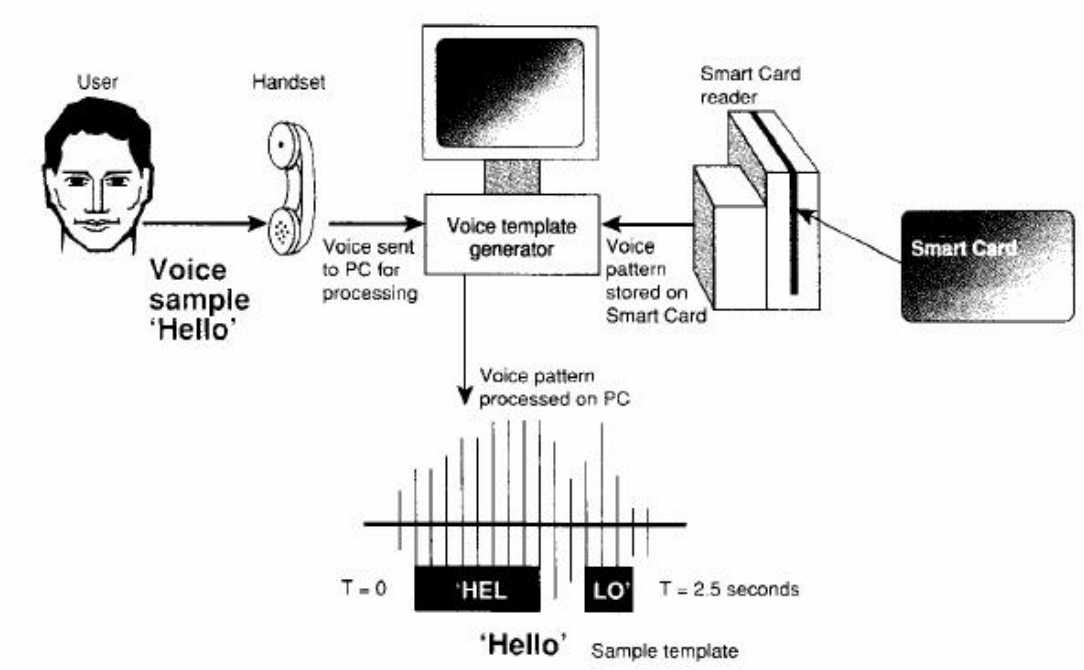


Figura 6: Identificador de Patrones de Voz **[13]**

• **Exploración de la Retina:** se ha demostrado que el patrón de los vasos sanguíneos de la retina presenta una mayor unicidad que el patrón del iris. Además, la casi imposible modificación de ese patrón, así como la facilidad para la detección de sujeto vivo, la hacen ser considerada la técnica más segura. Sin embargo, la forma de hacer la exploración, mediante láser, provoca un rechazo casi total por parte de los usuarios, estando sólo indicada para entornos de extrema seguridad, donde los usuarios son pocos y conscientes del grado de seguridad necesario.

• **Geometría del Contorno de la Mano y/o del Dedo:** se trata de una técnica en la que se estudian diversos parámetros morfológicos de la mano (o el dedo) del usuario, tales como anchuras, alturas, etc. [12]. La técnica basada en geometría del dedo se puede considerar como una simplificación de la basada en contorno de la Mano. El gran atractivo de esta técnica, debido a su simplicidad, bajo coste y mínimo tamaño del patrón, la han convertido en la técnica con mayor éxito comercial en el último par de años.

• **Rostro:** el método de identificación que nuestro cerebro usa más a menudo y de una forma más sencilla. En la actualidad existen muchos grupos de investigación trabajando en esta técnica con diversos métodos (estudios morfológicos, transformadas multiresolución, etc.). Los resultados que se están consiguiendo son bastante prometedores, aunque le falta todavía bastante hasta llegar al nivel de otras técnicas [6] Ver Figura 7

A la hora de juzgar una técnica biométrica, son muchos los parámetros que hay que considerar, de los que se pueden destacar los siguientes:

Universalidad: si las características se pueden extraer de cualquier usuario o no.

• Unicidad: la probabilidad de que no existan dos sujetos con las mismas características.

• Estabilidad: si las características que se extraen permanecen inalterables en relación con diversos parámetros (tiempo, edad, enfermedades, etc.).

• Facilidad de captura: si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto.

• Rendimiento: o tasas de acierto y error.

• Aceptación por los usuarios

• Robustez frente a la burla del sistema: si la técnica puede reconocer el falseamiento de los datos capturados (uso de fotos, dedos de látex, etc.).

• Coste: Por tanto, para cada situación y entorno, con un determinado requisito de seguridad, habría que seleccionar la técnica óptima para unos buenos resultados en el funcionamiento del sistema de identificación. Una comparativa sobre los sistemas más aceptados actualmente se puede encontrar en la Tabla 2.

Para Resumir a continuación de muestra una figura tomada de la revista IT Pro en enero de 2001, donde se comparan los distintos dispositivos biométricos.

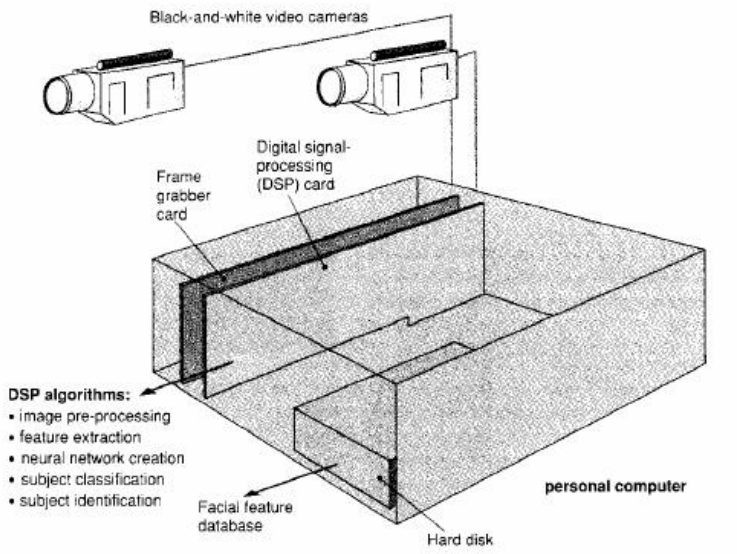


Figura 7: Reconocimiento del Rostro **[13]**

Tabla 2: Comparación de Dispositivos Biométricos [13]

RASTERISTIC	FINGERPRINTS	HAND GEOMETRY	RETINA	IRIS	FACE	SIGNATURE	VOICE
Ease to use	High	High	Low	Meduim	Meduim	High	High
rror incidense	Dryness, dirt, age	Hand injury, age	Glasses	Poor ligthing	Ligthing, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	-	-	-	-	-	-	-
ser acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
quired security level	High	Medium	High	Very high	Medium	Medium	Medium
ıg-term stability	High	Medium	High	High	Medium	Medium	Medium

IV. APLICACIONES PRÁCTICAS EN LA BIOMETRIA

[15] Algunos bancos como BanCafé de Colombia el tercero en importancia del país, Suruga de Japón el Bank of America y líneas aéreas como British Airways o Virgin, ya han impulsado experimentos piloto con cajeros automáticos y sistemas de embarque que emplean estos sistemas de reconocimiento, en lugar de las claves numéricas asociadas a bandas magnéticas a las que estamos acostumbrados.

En España, empresas como Visa, han confirmado que están haciendo un seguimiento de la tecnología, pero que no están implementando nada. Los bancos consultados (BBVA, la Confederación Española de Cajas de Ahorro y el Banco Santander Central Hispano no han sabido siquiera contestar.

En la actualidad hay bastantes empresas y equipos de investigación trabajando en temas biométricos tanto a nivel estatal como a nivel mundial, siendo sus principales objetivos:

- Proveer de recursos para apoyar a la comunidad biométrica en el avance de técnicas de reconocimiento.
- Organizar reuniones, forums y cursos para debatir las vías de investigación óptimas.
- Apoyar conferencias y ferias.
- Desarrollar y promocionar estándares tanto en los procedimientos de obtención de patrones como en el formato en que éstos se almacenan.
- Desarrollar y promocionar mejores prácticas de uso.
- Crear conciencia de las tecnologías de biometría y sus aplicaciones.
- Identificar oportunidades de investigación y promocionar colaboraciones de investigación.
- Mantener una relación activa con Agencias

gubernamentales tanto internacionales como nacionales.

En estas actividades están trabajando tanto desarrolladores, fabricantes e integradores, como universidades y centros de investigación.

Fruto de este común interés, diferentes consorcios han presentado proyectos de investigación en el marco del VI Programa de Investigación Europea, más concretamente en el área de las Tecnologías para la Sociedad de la Información y relacionados con la prioridad "Towards a global dependability and security framework".

V. CONCLUSIÓN

Se acerca el momento en el que nuestro cuerpo será nuestro DNI, en el que no habrá que memorizar contraseñas ni cargar con una docena de tarjetas electrónicas. Desde casi las primeras películas y series de ciencia ficción se ha visto cómo los humanos eran identificados, incluso a distancia, por sus huellas dactilares, su iris, su rostro, la palma de la mano o las venas del dorso o incluso su oreja. Es decir, por cualquier parte de su anatomía que se sepa única.

Pero lo que sí es seguro es que en el futuro los sistemas biométricos serán el medio de seguridad más utilizado en cuanto a control de acceso e identificación de personas se refiere, es por ello que las empresas se verán obligadas a utilizar este medio si quieren seguir en la competencia por sobre salir en su mercado especifico.

BIBLIOGRAFÍA

[1] A. Lervasi, C. Vázquez, D. Arcondo et al., Informe Central Identificación Biométrica. Revista RNDS, No 20 Septiembre 2005, pp. 48 - 68, http://www.rnds.com.ar/articulos/020/RNDS_048W.pdf

[2] J. S. Dunn, F. Podio., The Biometric Consortium, http://www.biometrics.org, 2009.

[3] C. Beavan., Fingerprints: The Origins of Crime Detection and the Murder Case that Launched Forensic Science. Hyperion, New York, 2001.

[4] S. Cole.,What counts for identity?: the historical origins of the methodology of latent fingerprint identification. Fingerprint Whorld, 27, 103, January 2001. Chapter 1 · An Introduction to Biometric Authentication Systems 17.

[5] S. Cole., Suspect Identities: A History of Fingerprinting and Criminal Identification. Harvard University Press, 2001.

[6] C. Reedman., Biometrics and law enforcement. Available from http://www.dss.state.ct.us/digital/biometrics%20and%20law%20enforcement.htm (accessed May 31, 2004).

[7] R. Sanchez-Reillo, C. Sanchez-Avila, J.A. Martin-Pereda., Minimal Template Size for Iris-Recognition. Proc. of the First Joint BMES/EMBS Conference. Atlanta (EE.UU.), 13-16 Octubre, 1999. p. 972

[8] J. L. Wayman., Digital Signal Processing in Biometric Identification: A Review. College of Engineering and office of research and graduate studies, San Jose State University, 2002

[9] R. O. Duda., P. E. Hart., Pattern Classification and Scene Analysis. John Wiley & Sons. 1973.

[10] A. K. Jain., R. Bolle., S. Pankanti., et al., Biometrics: Personal Identificacion in Networked Society. Kluwer Academic Publishers. EE.UU. 1999.

[11] J. G. Daugman., High Confidence Visual Recognition of Persons by a Test of Statistical Independence. IEEE Trans. on Pattern Analysis and Machine Intelligence, vol. 15, nº 11. Noviembre 1993. pp. 1148-1161.

[12] R. Sánchez-Reillo, C. Sánchez-Ávila, A. González-Marcos., Multiresolution Analysis and Geometric Measure for Biometric Identification. Secure Networking - CQRE [Secure]'99. Noviembre/Diciembre, 1999. Lecture Notes in Computer Science 1740, pp. 251-258. Springer-Verlag.

[13] http://www.jeuazarru.com/docs/biometria.pdf , 2003.

[14] A. K, Jain, P, Flynn, A. A, Ross., Handbook of Biometrics. Editorial Springer 2008.

[15] Grupo de Biometría, Departamento de Tecnologías de la Información, Robotiker http://revista.robotiker.com/articulos/articulo74/pagina1.jsp, visitada el 16 de octubre de 2006.

[16] National Institute of Standards and Technology. NIST Biometric Scores Set. Available at http://http://www.itl.nist.gov/iad/894.03/biometricscores.

[17] Cantú Rohlik, Cuitlahuac. Sistemas evolutivos para reconocimiento de imágenes. 2002. IPN-UPIICSA.

[18] Gargía Ortega V. H., Sistema de reconocimiento de huellas dactilares para el control de acceso a recintos. 2001. Centro de Investigación en Computación. Laboratorio de Sistemas Digitales.

[19] Sanchez Reíllo, R., Verificación Automática de Personas Mediante Huella Dactilar. Grupo Universitario de Tarjeta Inteligente Departamento de Tecnología Electrónica, Grupo de Microelectrónica, UNIIVERSIDAD CARLOS III DE MADRID, 2003.

[20] Urraza, J., Teoría y Aplicación de la Informática, Paraguay, 2004.

[21] ETESA, Licitación Pública N° 01 DE 2006, Bogotá, D.C., febrero de 2006.

[22] http://www.visioningenieria.com/soluciones.html Visitada el 4/06/2006 a las 10:35 AM

[23] http://www.trielo.com.br/ase_productos Visitada el 4/06/2006 a las 10:45 AM

[24] http://www.ast_afis.com.com/es/es-id4.html Visitada el 4/06/2006 a las 11:05 AM

[25] http://www.biometria.com.pe Visitada el 4/06/2006 a las 11:10 AM

[26] http://www.pyratech.hpg.ig.com.br//prmcipal.html Visitada el 4/06/2006 a las 11:15 AM

[27] http://www.ii.uam.es/~abie/docs/biotest.htm Visitada el 4/06/2006 a las 11:21 AM

[28] http://www2.vol.com.br/info/aberto/infonews/052002/20052002-22.shl Visitada el 4/06/2006 a las 11:30 AM

[29] http://www.homini.com/biometria.html Visitada el 4/06/2006 a las 11:33 AM

[30] http://www.homini.com/origen.htm Visitada el 4/06/2006 a las 11:36 AM

[31] http://www.ast_afis.com/biometria.html Visitada el 4/06/2006 a las 11:41 AM

[32] http://homepage.ntlworld.com/avanti/ Visitada el 4/06/2006 a las 11:45 AM

[33] http://www.belt.com.es/noticias/02_abril/22_26/23_biometria.html Visitada el 4/06/2006 a las 11:52 AM

[34] http://www.embratel.com.br/internet.wks05/tecnologia/tegnologia Visitada el 4/06/2006 a las 11:58 AM

[35] http://www.iriscan.com/ Visitada el 4/06/2006 a las 12:05 PM

[36] http://es.wikipedia.org/wiki/Red_neuronal_artificial Visitada el 8/06/2006 a la 01:53 PM

[37] http://www.laflecha.net/canales/empresas/noticias/200409091 Visitada el 10/06/2006 a las 09:17 PM