



TECNOLOGÍAS BIOMETRICAS

**POR NIBALDO MUÑOZ V.
NINALDOAMV@GMAIL.COM**

I) CONCEPTOS BASICOS SOBRE BIOMETRIA

1.1 INTRODUCCION A LA BIOMETRIA

1.1.1 ANTECEDENTES HISTORICOS

Los primeros antecedentes conocidos sobre la utilización de biometría en la identificación de personas, se remonta al siglo VIII en China, en donde fueron encontradas huellas dactilares tanto en documentos, como en arcilla y roca. Registros posteriores (siglo XIV) indican que comerciantes utilizarían impresiones en tinta de las huellas de las palmas de las manos en papel como medio de reconocimiento de niños y jóvenes.

En las culturas occidentales la biometría hace su aparición recién a finales del siglo XIX. En 1868 Marcelo Malpigo realizó el primer estudio sobre huellas dactilares.

En 1865 Sir William Herschel implanta la huella dactilar como medio de identificación en documentos para personas analfabetas.

En principio los sistemas desarrollados se encaminaron a la identificación de criminales. El primer sistema biométrico ampliamente utilizado científicamente en la detección de criminales fue desarrollado por Alphonse Bertillon, jefe del departamento fotográfico de París, denominado sistema antropométrico, convirtiendo así a la biometría en un campo de estudio.

En 1941, Murria Hill de Laboratorios Bell realiza el primer estudio de identificación por voz.

En 1986 Sir Alec Jeffreys utiliza el ADN para esclarecer un crimen en Inglaterra.

Actualmente la biometría se encuentra en una etapa de importantes aportes en investigación, desarrollo e implementación de sistemas, principalmente en la industria.

Organizaciones científicas de la entidad de IEEE (The Institute of Electrical and Electronics Engineers), realizan constantes esfuerzos en investigación, lo que se traduce en gran cantidad de publicaciones relacionadas, enriqueciendo el conocimiento sobre las diversas tecnologías biométricas. En 1998 se formó el consorcio BioAPI con el fin de desarrollar un Standard API ampliamente aceptado y disponible para la aplicación de los diversos sistemas biométricos.

La conciencia sobre la necesidad de contar con herramientas más poderosas que favorezcan la seguridad, tanto en el acceso físico a instalaciones como en el acceso a sistemas informáticos, por parte de las naciones, producto de la gran cantidad de atentados, ocurridos durante los últimos años, impulsado de forma explosiva la investigación y desarrollo de los sistemas biométricos y sus múltiples aplicaciones.

1.1.2 ¿QUE ES LA BIOMETRIA?

El concepto biometría proviene de las palabras griegas “bios” de vida y “metron” de medida.

El termino biometría clásicamente se aplica de forma general a la ciencia que mediante el estudio estadístico y matemático, cuantifica características cuantitativas de los seres vivos.

Otras definiciones más recientes hacen referencia al estudio de métodos automáticos para el reconocimiento de humanos, basados en rasgos físicos o conductuales, con el fin de identificar y autenticar la identidad de las personas.

Según esta última definición la biometría también abarcaría los campos de la criptografía y la seguridad informática, estando inserta en uno de los tres puntos críticos en los que se suele cimentar un buen sistema de seguridad, estos son:

- Algo que la persona sabe (clave secreta)
- Algo que la persona tiene (tarjeta identificación)
- Algo que la persona es (dato biométrico)

En función de las características cuantificadas, es posible establecer dos grandes grupos. Las huellas dactilares, el iris, la retina, la geometría de la palma de la mano y el rostro, son ejemplos de características físicas o estáticas, las que formaran parte de la denominada biometría estática. Al conjunto de características, tales como la firma, la dinámica del tecleo y voz se les conoce como conductuales o de comportamiento y se encuentran insertas dentro de la biometría dinámica.

La figura 1.1 muestra los dos grandes grupos en los que puede ser subdividida la biometría, con ejemplos de algunas características estáticas y dinámicas.

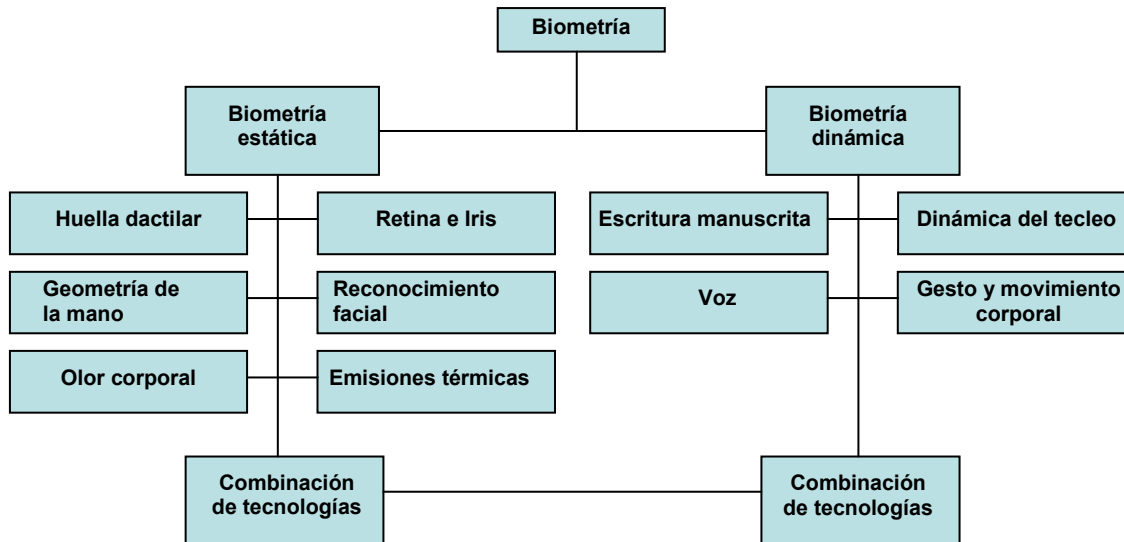


Fig.1.1

Como es posible apreciar la combinación de tecnologías representa una importante herramienta, ya que aumenta las probabilidades de aciertos en la identificación y autenticación de personas.

Para que las características físicas y conductuales puedan ser eficazmente utilizadas como medio de identificación y autenticaciones deben cumplir con los siguientes requisitos básicos:

- **Universalidad:** Todas las personas tienen que presentar la característica.
- **Singularidad:** La característica presentada en dos personas debe ser condición suficiente para su identificación.

- **Estabilidad:** La característica debe mantenerse estable a través del tiempo.
- **Cuantificable:** La característica debe ser mensurable de forma cuantitativa.
- **Aceptabilidad:** La característica debe tener un nivel de aceptación suficiente por parte de las personas.
- **Rendimiento:** La característica debe tener un nivel de exactitud elevado para que se considere como aceptable.
- **Usurpación:** Nivel de seguridad del sistema ante técnicas fraudulentas.
- **Fiabilidad:** La característica debe poseer una alta fiabilidad para se considerado como aceptable.
- **Factibilidad de uso:** Se debe garantizar la factibilidad de uso para que un sistema sea considerado aceptable.

A continuación la Tabla 1.1 muestra una tabla comparativa en la que se recogen algunas de las diferentes características y sus respectivos requisitos de aceptación:

	Iris	Retina	Huella	Mano	Escritura	Voz	Rostro
Fiabilidad	Muy alta	Muy alta	Alta	Alta	Media	Alta	Alta
Facilidad	Media	Baja	Alta	Alta	Alta	Alta	Alta
Usurpación	Muy alta	Muy alta	Alta	Alta	Media	Media	Media
Aceptación	Media	Media	Media	Alta	Muy alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Media	Baja	Media	Media

Tabla.1.1

En la figura 1.2 es posible ver una gráfica perteneciente al Grupo Biométrico Internacional en donde se muestran claramente algunas de las características de las principales tecnologías biométricas:

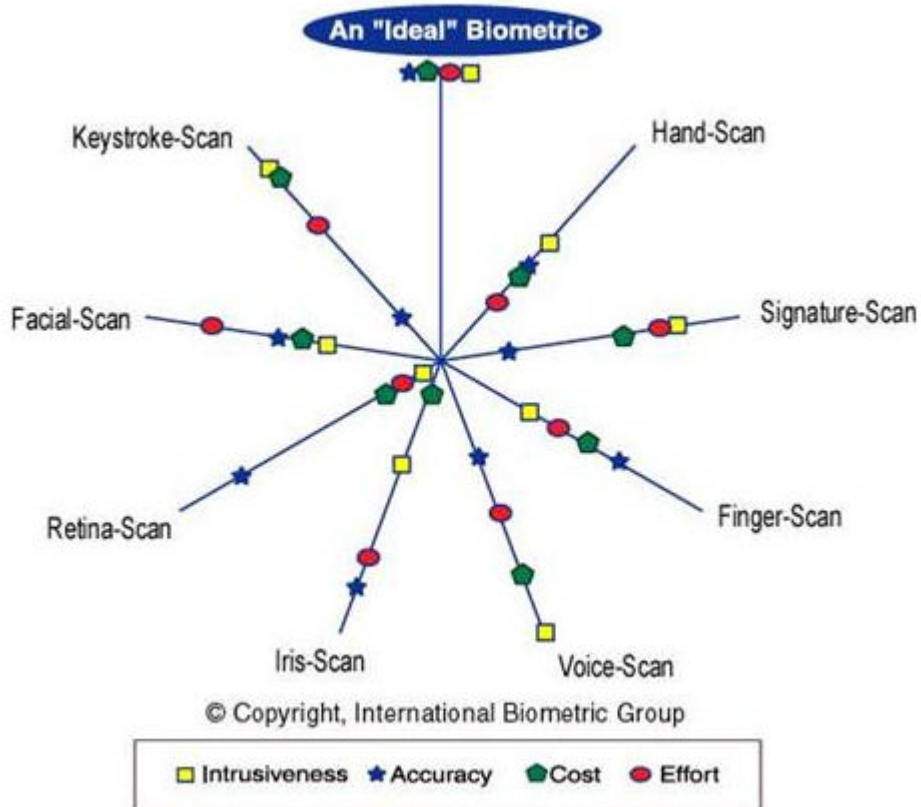


Fig.1.2

Todas las características antes mencionadas tienen como objetivo principal proveer un conjunto de herramientas que permitan identificar y autenticar personas, de la forma más eficaz y eficiente posible.

1.1.3 PROCESOS CLAVE EN LA IDENTIFICACION Y AUMENTACION BIOMETRICA

Durante el proceso de entrenamiento se extraen las muestras que posteriormente formaran el perfil o patrón del usuario, esto es, el proceso automático de codificación y almacenamiento de las características biométricas del individuo, todo esto con el fin de generar un registro o dar de alta al usuario dentro de un sistema.

El proceso de extracción puede requerir de varias muestras con diferentes grados, para así obtener datos precisos a la hora de generar un patrón.

Una de las características más importantes y valoradas dentro de un sistema biométrico es la capacidad de que estos sean automatizados. Como cualquier otro sistema, la automatización de sistemas biométricos puede ser organizada de acuerdo a una estructura definida. El modo de organizar la automatización de un sistema biométrico es la siguiente:

- La persona debe registrar una o más de sus características. Mediante la utilización de dispositivos es posible registrar dichas características, esto es, dar de alta a un usuario dentro del sistema.
- La calidad de los datos obtenidos durante el proceso de alta es un aspecto muy significativo. Las condiciones de la toma de las muestras y la cantidad de medidas definirán su calidad y, por lo tanto, la exactitud en la identificación.

El grado de similitud en la correspondencia biométrica se define como puntuación. Esta puntuación representa el éxito durante la extracción de las características de las muestras biométricas obtenidas.

Casi todos los sistemas biométricos entregan una puntuación durante el entrenamiento. Si la muestra es rica en información, existirá una alta puntuación en el intento de dar de alta al usuario.

A diferencia de otros sistemas tradicionales de autenticación (PIN, password, claves y tarjetas), en donde la respuesta binaria, es decir, si o no, prácticamente todos los sistemas biométricos se basan en algoritmos que generan una puntuación luego de un intento de reconocimiento.

El parámetro que define la exactitud de durante el proceso de dar de alta a un usuario se denomina FTER (Failure To Enroll Rate) y se calcula según la siguiente expresión.

$$\text{FTER} = \frac{\text{Numero insatisfactorio de altas en el sistema}}{\text{Numero total de intentos de alta}}$$

Este parámetro esta condicionado a factores externos producidos por diferentes circunstancias y que podrían generar errores en el proceso de identificación. Es por esto que se deben tomar en cuenta todas estas instancias y en casos eventuales proveer de soluciones a los problemas que pueden aparecer.

La siguiente tabla muestra algunos errores y soluciones:

Biometría	Factores causantes de error	Soluciones
Todas	Envejecimiento	Dar de alta periódicamente
Huella	Tipo de trabajo	Dar de alta varios dedos
Cara	Iluminación, fondo, contraste	Entornos controlados
Voz	Enfermedad, Interfases	Dar de alta periódicamente
Mano	Heridas	Dar de alta ambas manos
Iris	Posición del ojo, gafas	Facilitar posición adecuada

Tabla 1.2

- Los datos obtenidos son normalmente datos sin procesar. Reciben el nombre de muestras biométricas y no pueden ser utilizadas para el proceso de reconocimiento debido principalmente a su tamaño y complejidad. Estos datos deberán ser procesados con el fin de extraer las características que serán utilizadas en el proceso de autenticación.
- Es posible considerar dos plantillas principales, una generada cuando un usuario es ingresado en e sistema y otra cuando el mismo intenta acceder al sistema. En la etapa de acceso se comparan ambas plantillas con el fin de lograr la identificación del usuario.

- El patrón se crea a través de un proceso algorítmico que transforma las características del usuario, es decir, el patrón es una representación numérica de la muestra de la característica del usuario ingresado.

Una vez creado el patrón, el sistema podrá reconocer al individuo ingresado. Al intentar ingresar un usuario en el sistema, las características ingresadas deben ser comparadas con las ya almacenadas, para posteriormente verificar la similitud entre ambas y establecer el grado de coincidencias.

Luego de comparadas las plantillas, es preciso establecer si la similitud entre ambas sobrepasa un umbral preestablecido. El resultado de la comparación nos conducirá a diversas alternativas: correlación entre ambas, no correlación o bien sin conclusión.

La figura 1.3 muestra un ejemplo ilustrativo del proceso de autenticación en un sistema biométrico.

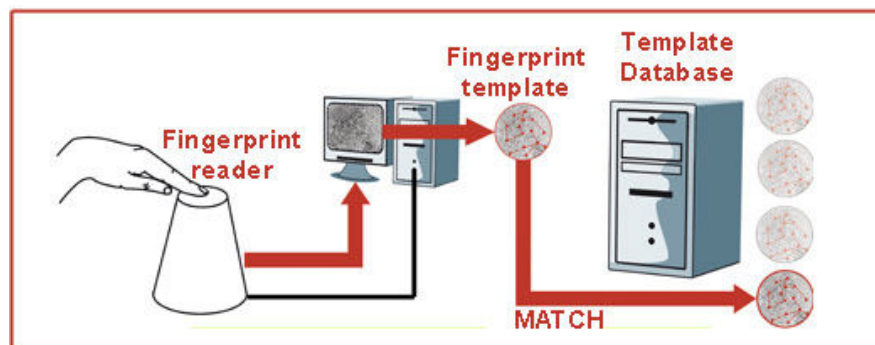


Fig.1.3

La calidad de un sistema biométrico también es posible determinarla por su tasa de error. La mayoría de los sistemas biométricos son capaces de realizar la autenticación con tasas de error menores a 1/100.000.

La tasa de error es posible expresarla en función de la tasa falsa de aceptación (FA), o número de usuarios ingresados de forma incorrecta y en la tasa de falso rechazo (FR), o número de número de usuarios rechazados en forma errónea. Es posible mejorar estas tasas variando el umbral. La intersección de las dos funciones se conoce como punto de igual error (EER, Equal Error Rate) y usualmente se utiliza como parámetro para determinar la calidad de un sistema biométrico.

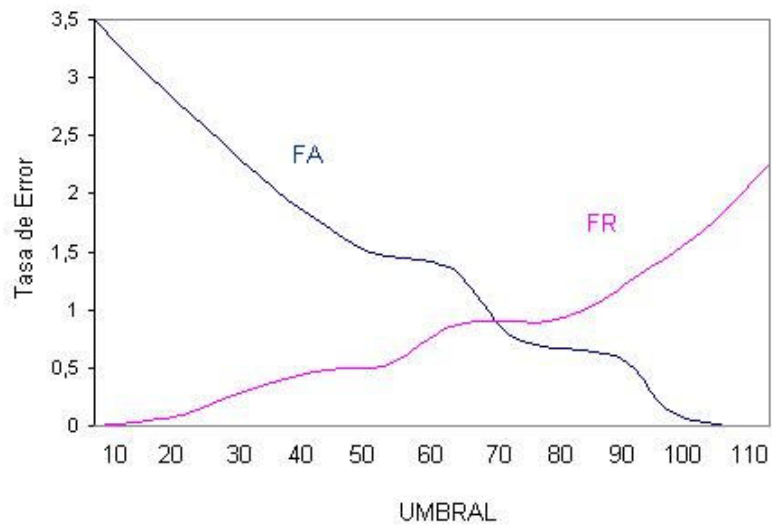


Fig. 1.4

Recopilación de datos

La recopilación de datos biométricos se cimienta en la premisa de que las características de cada individuo son suficientes para determinar a un usuario genuino de un impostor.

Durante el proceso de recopilación de datos, es en donde se presentan los primeros problemas. En primer lugar las muestras deben ser obtenidas mediante un sensor, por tanto, sujetas a la calidad y características técnicas del sensor utilizado. Así las características del sensor deberán ser estandarizadas, a fin de que garantizar que las muestras obtenidas de un usuario en diferentes sistemas sean compatibles.

La calidad de los sensores se encuentra en proceso de estandarización por parte de organismos encargados de definir las características que estos deben reunir para su posterior homologación. El FBI (Federal Bureau of Investigation) y NIST (National Institute of Standards and Technologies), han establecido parámetros de calidad para los sensores utilizados en la lectura de la huella dactilar.

Dado el carácter biológico de los datos obtenidos, estos presentan deterioros principalmente originados por el tiempo, desgaste, heridas, traumas, etc.

La manera en que las muestras son obtenidas presenta también diversas dificultades de medición. Iluminación, postura corporal en la toma de la muestra (reconocimiento facial), entre otros, son factores que podrían alterar la correcta lectura por parte de los sensores, así como también la posterior identificación y autenticación de usuarios.

Todos los factores antes mencionados, afectan la calidad y repetibilidad de la toma de muestras, por lo que se deben tener en consideración, a fin de minimizar las repercusiones de estos sobre los datos biométricos a utilizar.

Transmisión de datos

Generalmente el almacenamiento de los datos biométricos no ocurre en un solo lugar, o bien, estos se encuentran lejos de donde estos fueron extraídos. Además cuando se trata de una gran cantidad de datos, es posible que sea necesaria la compresión de estos antes de ser almacenados o transmitidos.

Luego la problemática radica en dos aspectos fundamentales:

- Restauración de datos biométricos
- Problemas de incorporación de ruidos

Si los datos biométricos se encuentran comprimidos, será necesaria su descompresión. Existen diversas técnicas de compresión digital que son de gran utilidad en el proceso de compresión y restauración de los datos recopilados. Dependiendo de los datos biométricos obtenidos, se utilizarán diferentes técnicas de compresión.

En el caso de toma muestras biométricas específicas, como es el caso de la huella dactilar, existen dispositivos especialmente diseñados para tomar dichas muestras y transformarlas mediante algoritmos específicos. Dada la naturaleza de estos algoritmos, es que estos presentan pérdidas de información originadas producto de la descompresión. Luego es de gran importancia lograr incorporar para determinadas técnicas biométricas, métodos de compresión con mínimas pérdidas.

Por otra parte la recopilación de muestras biométricas analógicas podría llegar a presentar inconvenientes, principalmente en su transmisión. Luego es de gran utilidad el uso de canales de transmisión que provean estabilidad en la toma de muestras, como es el caso de la obtención de datos mediante acceso telefónico.

En un sistema de transmisión de datos biométricos, es preciso que los protocolos sean estandarizados, de modo que varios usuarios puedan reconstruir la señal original, con las menores pérdidas posibles.

Actualmente existen diversas normas de compresión de datos biométricos, como por ejemplo, WSQ en el caso de la huella dactilar, JPEG para reconocimiento facial y CELP, para las muestras de voz y datos.

Procesamiento de datos

Luego que la señal ha sido recopilada y transmitida, esta pasa al subsistema de procesamiento, en donde se verificarán algunos parámetros de calidad de la señal obtenida, antes de que esta pase al subsistema de recopilación. La información recopilada es transformada mediante algoritmos, los cuales se encargan de extraer las características biométricas provenientes de la señal original. Para esto el subsistema de

procesamiento de la señal se divide en las siguientes tres áreas:

- Característica de la extracción
- Control de calidad
- Coincidencia de patrones

En primer lugar se verifica las características de la extracción, lo que incluye características del sensor utilizado, pérdidas de compresión, presencia de ruidos, etc.

La calidad de los datos biométricos es fundamental para su aceptación y posterior almacenamiento, por lo que se debe realizar un control exhaustivo de la señal, garantizando así, su preservación e invariabilidad.

La coincidencia de patrones es utilizada con el propósito de comparar ciertos patrones ya almacenados y realizar una superposición con datos de un usuario a identificar. En esta etapa se entregara una medida cuantitativa de las coincidencias entre ambas, la cual será enviada al siguiente subsistema.

El procesamiento de las señales mediante algoritmos precisa de la utilización de transformadas, como por ejemplo, la Transformada de Fourier, muy utilizada tanto en el procesamiento de señales de voz, como en el de imágenes.

Decisión

La toma de decisión bajo la búsqueda dentro de una base de datos, para la determinación de coincidencias y no coincidencias, mediante el uso de plantillas, se basa en la medida de la igualdad entre el dato biométrico de un usuario previamente ingresado, con uno a verificar, esto es, la autenticación de un usuario dado de alta previamente en el sistema.

Dependiendo del grado de coincidencias, y dado un umbral de aceptación, el cual puede ser fijo o variable, dependiendo de las características y cantidad de mediciones realizadas, se podrá establecer una decisión. El resultado de la comparación nos conducirá a diversas alternativas: correlación entre ambas, no correlación o bien sin conclusión.

El funcionamiento del sistema en la toma de decisión puede llegar a ser complejo, por lo que se debe tener en cuenta

particularmente la altura del umbral, la cual no debe ser demasiado tolerante, ya que esto podría llevar a la incorrecta decisión y, por tanto, la errónea verificación de la identidad de un individuo.

El rendimiento del sistema en la toma de decisión, es afectado también por los subsistemas anteriores, principalmente por el de procesamiento, lo que podría generar problemas en la toma de decisión. Idealmente el subsistema de decisión debe ser desvinculado del de procesamiento.

Almacenamiento de datos

Según el sistema de almacenamiento biométrico a utilizar, existen una o más formas de guardar los datos previamente recopilados y procesados.

Además de los datos biométricos del usuario ingresado, es útil que la plantilla de este contenga además datos personales que posteriormente servirán en la identificación y verificación de la identidad del individuo. La organización de la estructura de los datos debe ser flexible, permitiendo su reestructuración, si fuese necesario. De esta forma es posible definir algunos sistemas de almacenamiento, para diferentes tipos de medidas biométricas, dependiendo de sus características particulares.

Algunos sistemas de almacenamiento se muestran continuación:

- Sistema protegido dentro del dispositivo biométrico.
- Base de datos
- Tokens portátiles

BIBLIOGRAFIA

1. Biometrics Technologies. (2007). <http://www.biometco.com>
2. National Biometric Test Center. (2007). "San Jose State University". <http://www.engr.sjsu.edu>
3. Plataforma biométrica Homini (2004). <http://www.homini.com>
4. Tapiador, Marino y Sigüenza, Juan A. (2005). "Tecnologías biométricas aplicadas a la seguridad". Alfaomega. Madrid. España. 440 pp.
5. TecneSoft Net. Tecnología de avanzada. (2005, 2006, 2007). <http://www.tecnesoft.net>
6. Wikipedia. La enciclopedia libre (2008). <http://es.wikipedia.org>