AVANCES EN TÉCNICAS BIOMÉTRICAS Y SUS APLICACIONES EN SEGURIDAD

LIC. LEÓN P, SUSAN K.
Universidad de Carabobo. Valencia. Edo Carabobo. Venezuela
Email: Sleo300379@gmail.com

RESUMEN

INTRODUCCIÓN

En la actualidad los sistemas basados en reconocimiento biométrico han cobrado gran relevancia en entornos que requieren la identificación de usuarios o accesos restringidos. En comparación con los métodos clásicos comúnmente utilizados, como llaves o claves, los rasgos biométricos no pueden, en general, ser prestados, robados o copiados. El usuario empleará su huella, retina, voz u otro rasgo biométrico para ser reconocido. Por otro lado, esta clase de sistemas suele ser fácil de mantener y en general no requiere la intervención de más agentes que el propio usuario para funcionar. Los rasgos biométricos pueden clasificarse según varias características [Maltoni *et al.*, 2003]. Entre ellas cabe mencionar su unicidad, su distintividad o individualidad, su universalidad, su facilidad de proceso y adquisición o su variabilidad con el tiempo. Son ejemplos de ello las PDAs, los ordenadores portátiles, los *Tablet* PC, y los teléfonos móviles 3G, entre otros.

FUNDAMENTACIÓN TEÓRICA

La biometría se refiere a la aplicación automatizada de técnicas biométricas a la certificación, autentificación e identificación de personas en sistemas de seguridad. Las técnicas biométricas se utilizan para medir características corporales o de comportamiento de las personas con el objeto de establecer una identidad. Para diferenciar estos conceptos, organizaciones y autores han dado un nombre compuesto al contexto tecnológico como biometría informática y autentificación biométrica.

FUNCIONAMIENTO DE LOS PRODUCTOS BIOMETRICOS

Para realizar la autentificación biométrica, primero se debe registrar a los individuos que van a hacer uso del sistema. Para el registro se utiliza un dispositivo biométrico para examinar el atributo físico o de comportamiento elegido. La autentificación posterior se realiza cuando el individuo presenta su rasgo corporal o muestra su comportamiento ante un dispositivo biométrico.

Para el caso de verificación, la persona le informa al sistema cual es su identidad ya sea presentando una tarjeta de identificación o entrando alguna clave especial.

Y en el caso de la identificación, la persona no le informa al sistema biométrico cual es su identidad. El sistema tan solo captura el rasgo característico de la persona y lo procesa para crear el modelo en vivo. Luego el sistema procede a comparar el modelo en vivo con un conjunto de modelos de referencia para determinar la identidad de la persona.

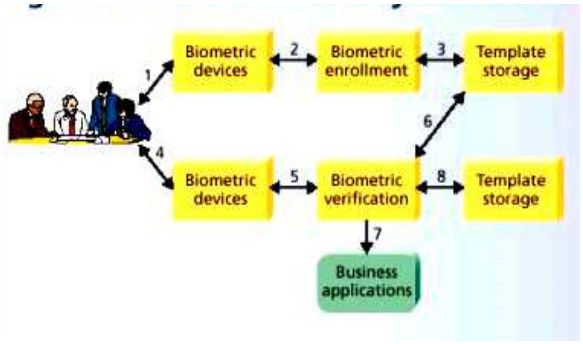

Fig 1. Funcionamiento de un sistema biométrico

TÉCNICAS BIOMÉTRICAS

ADN

El ADN es único para cada individuo, excepto para el caso de gemelos monocigóticos.

Es el método más común en aplicaciones forenses para reconocimiento. Además, la información que se puede extraer a partir del ADN de una persona, puede revelar discapacidades u otras características que el usuario no desee hacer públicas.

DINÁMICA DEL TECLEO

Este rasgo biométrico es de tipo conductual y por lo tanto muy variable en el tiempo.
Para su captura basta con emplear secuencias del tecleo del usuario, por lo que no es intrusivo. Es poco distintivo pero puede ser utilizado para identificación en casos sencillos.

Fig 2. Sistema de verificación de patrones de tipeo

ESCÁNER DE RETINA

La estructura vascular de la retina es supuestamente diferente para cada individuo y cada ojo. La captura de este rasgo biométrico es compleja ya que requiere cooperación por parte del usuario y contacto con el sensor, lo cual compromete seriamente su aceptabilidad.
Además, puede revelar ciertas afecciones, como hipertensión.

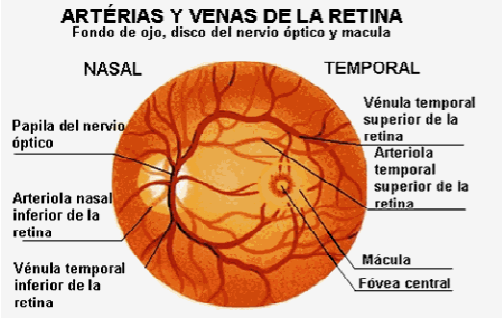

Fig 3. Reconocimiento de retina

FIRMA

A pesar de que la captura de la firma requiere contacto con una superficie, es un rasgo muy aceptado dada su frecuente utilización desde el pasado. La firma varía a lo largo del tiempo para un mismo sujeto e incluso existen sujetos cuya firma varía muy significativamente en cada realización, por lo que su identificación es compleja.

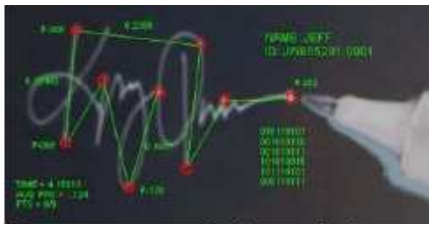

Fig 4. Reconocimiento dinámico de la Firma

FORMA DE CAMINAR

La forma de caminar de cada individuo es un rasgo biométrico complejo a nivel espacio-temporal. No es un rasgo muy distintivo, pero puede ser suficiente en aplicaciones que requieran un nivel bajo de seguridad. Para su

captura es necesario el uso de cámaras de vídeo y es, en consecuencia, no invasivo.

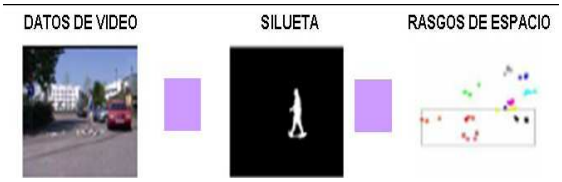

Fig 5. sistema de reconocimiento de forma de caminar por analisis de silueta

GEOMETRÍA DE LA MANO

La geometría de la mano es otro rasgo de baja distintividad de cada individuo. Para adquirir la imagen de la mano es necesario que el usuario sitúe la palma de su mano en un escáner u otro dispositivo capturador. Se han propuesto plantillas de almacenamiento de nueve *bytes*, por lo que supone una alternativa útil en sistemas de memoria o ancho de banda limitado.

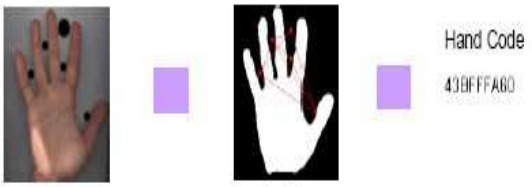

Fig 6 . Sistema de reconocimiento de la palma de la mano

IRIS

Se ha demostrado [Daugman, 1999] que el iris es altamente distintivo para cada uno de los dos ojos de cada individuo. La captura del iris requiere participación por parte del usuario ya que debe situarse a una distancia predeterminada del sensor (generalmente un capturador de fotografías de iris). El reconocimiento por iris suele ser extremadamente preciso y rápido, aunque hoy en día continúa siendo una tecnología cara.

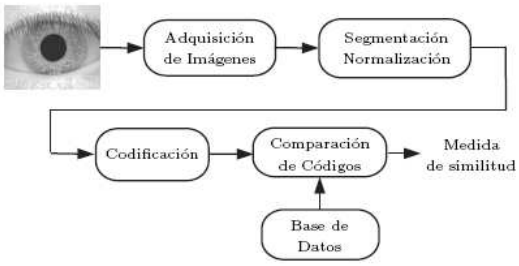

Fig 7. Sistema de reconocimiento de patrón de Iris

OLOR

El olor es característico de cada sustancia química y puede ser capturado por sensores químicos, cada uno sensible a una sustancia diferente. Una parte del olor emitido por los seres humanos es distintiva para cada individuo, pero resulta complicado descartarla de sustancias artificiales como perfumes o desodorantes.

OREJA

Para el reconocimiento basado en la oreja se emplea la forma del borde de la oreja y de las estructuras cartilaginosas. Los sistemas que se han propuesto en la actualidad suelen emplear la distancia de los salientes del borde de la oreja con respecto a una referencia común del interior de la oreja.

ROSTRO

El rostro es uno de los rasgos biométricos más aceptados ya que es el comúnmente empleado en el reconocimiento humano entre individuos. Además, para adquirir este rasgo basta con una fotografía, lo cual es no invasivo. Los mayores inconvenientes que presenta es la posibilidad de emplear máscaras, no detectables en sistemas sin vigilancia.

Además, el sistema debe poder adaptarse a los cambios con la edad del usuario, la iluminación, las expresiones y la posición relativa con respecto a la cámara.

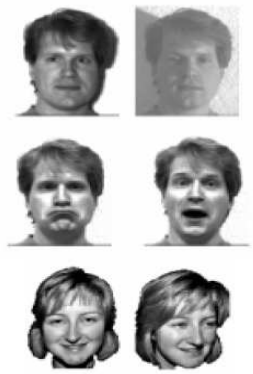

Fig 8. Técnica de reconocimiento de rostro

TERMOGRAMAS

El calor radiado por el cuerpo humano es característico de cada individuo. Puede ser capturado mediante una cámara de infrarrojos de forma no intrusiva o incluso oculta. La mayor desventaja de esta clase de sistemas es el coste de los sensores y su vulnerabilidad ante otras fuentes de calor no controlables. Los termogramas pueden ser también empleados para captar la estructura de las venas de la mano.

VOZ

La voz es un rasgo biométrico muy aceptado y fácil de obtener. Las principales desventajas que posee son su baja distintividad y la facilidad de ser imitada. Además, afecciones comunes como resfriados o incluso el estado de ánimo hacen que sea un rasgo muy variable.

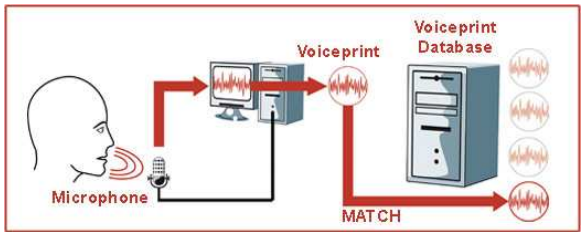

Fig 9. Reconocimiento de Voz

RECONOCIMIENTO DE LA HUELLA DACTILAR

Esta técnica biométrica consiste en comparar una huella digital con los modelos almacenados en una base de datos, tanto para identificar como para autentificar a un usuario. Hay una gran variedad de métodos de verificación de huellas. Algunos de ellos pueden incluso detectar cuando el dedo presentado corresponde a una persona viva o no. En esta clase biométrica existe un mayor número de dispositivos que en otras clases de biometrías. Debido al descenso de los precios de estos dispositivos, esta técnica está ganando aceptación. Una aplicación muy típica consiste en el control de accesos, debido al pequeño tamaño, facilidad de integración y bajo coste de los dispositivos de autentificación en relación con otros métodos biométricos.

Fig 10. Reconocimiento de huella digital

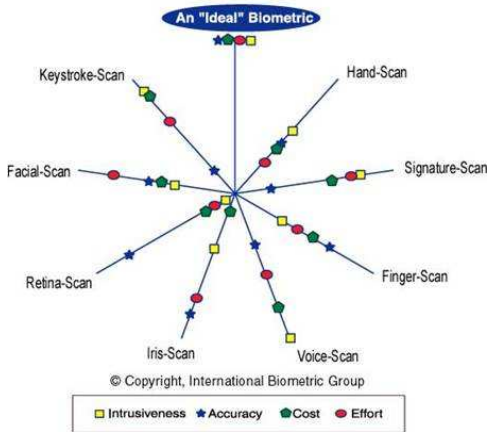

Fig 11. Características principales de tecnologías biométricas

ESPECTROSCOPÍA DE LA PIEL

La calidad óptica de la piel humana esta determinada por sus propiedades químicas y estructurales, que varían de una persona a otra. Estas propiedades pueden ser medidas

usando espectroscopia óptica de reflexión difusa. Esta tecnología biométrica usa un sensor biométrico basado en un diodo emisor de luz (LED) y foto detectores de silicio que fueron desarrollados para mejorar las medidas biométricas basadas en las propiedades ópticas de la piel en los dedos, manos u otros sitos de la piel.

RASGOS COMUNES EN LAS TÉCNICAS BIOMÉTRICAS

- **Universalidad**: todo el mundo debe poseer esa característica.

- **Distintividad**: dos personas deberán ser suficientemente diferentes en términos de ese rasgo.
- **Estabilidad**: el rasgo debe permanecer invariable en el tiempo a lo largo de un periodo de tiempo aceptable.
- **Evaluabilidad**: la característica debe poder ser medida cuantitativamente.
- **Rendimiento**: los recursos empleados para el reconocimiento deben ser razonables y no deben depender de características del entorno.
- **Aceptabilidad**: los usuarios deben estar dispuestos a emplear ese rasgo.
- **Fraude**: los sistemas basados en ese rasgo deben ser suficientemente seguros para que resulte complicado engañarlos.

En la Tabla 1 clasifica los rasgos biométricos expuestos en función de las características explicadas anteriormente.

Identificador biométrico	Universalidad	Distintividad	Estabilidad	Evaluabilidad	Rendimiento	Aceptabilidad	Fraude
ADN	A	A	A	B	A	B	B
Dinámica del tecleo	B	B	B	M	B	M	M
Escáner de retina	A	A	M	B	A	B	B
Firma	B	B	B	A	B	A	A
Forma de caminar	M	B	B	A	B	A	M
Geometría de la mano	M	M	M	A	M	M	M
Huella dactilar	M	A	A	M	A	M	M
Iris	A	A	A	M	A	B	B
Olor	A	A	A	B	B	M	B
Oreja	M	M	A	M	M	A	M
Rostro	A	B	M	A	B	A	A
Termograma facial	A	A	B	A	M	A	B
Venas de la mano	M	M	M	M	M	M	B
Voz	M	B	B	M	B	A	A

Tabla # 1. Comparación de tecnologías biométricas A, M y B denotan niveles (Alto, Medio y Bajo)

APLICACIONES DE SEGURIDAD DE LAS TÉCNICAS BIOMÉTRICAS

-Seguridad en la movilidad y accesos
Aeropuertos, fronteras, centrales electricas, centros de control de suministro, instalaciones industriales, instituciones públicas, control hospitalario de neonatos

-Seguridad en las transacciones:(comercio electrónico y banca)

- Cajeros automáticos, verificación de uso de tarjetas de credito en comercios, pago por Internet

-Seguridad en el acceso y firma de documentos electrónicos

- Sector sanitario, industrial, administración pública, comercio, actas notariales.
- Validación de firma digital, sistemas de voto electrónico y voto por internet

-Seguridad en el acceso a equipos industriales

- Maquinaria que sólo deba ser utilizada por personal específicamente formado.

-Aplicaciones comerciales

- Las tecnologías tradicionales de las que disponemos utilizan sistemas basados en el conocimiento y en muestras.

-Reforzar la seguridad de las infraestructuras PKI

- De esta manera puede ofrecerse una protección más eficaz a los certificados y

firmas digitales que se utilizan en este tipo de estructuras.

-Aplicaciones gubernamentales y forenses
Conseguir la misma autenticidad en un sistema de identificación que un sistema de verificación es mucho más difícil debido al gran número de comparaciones que han de realizarse. Las herramientas tradicionales de reconocimiento del personal como pueden ser las contraseñas o los PINs no son útiles para el reconocimiento negativo de las aplicaciones.

VENTAJAS Y DESVENTAJAS DE LAS TÉCNICAS BIOMÉTRICAS

Las técnicas biométricas presentan procesos de verificación de la identidad basados en características físicas (cara, huellas digitales) o de comportamiento (registro vocal, firma a mano alzada). Primero estas características (como ser el registro vocal) son capturadas e ingresadas al sistema, asociadas a cada usuario respectivo. Luego, en el momento de la verificación, la autenticación se produce por la comparación del patrón almacenado y el registro realizado por el usuario que requiere el acceso.
Esta técnica ha evolucionado mucho, llegando a ser muy exactas, y a precios razonables.

TÉCNICA	VENTAJAS	DESVENTAJAS
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de réplicas, cortes o lastimaduras pueden alterar la autenticación
Lectura de iris/retina	Muy seguro	Intrusivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puede ser alterado por el estado emocional de la persona
Reconocimiento de la voz	Barato, útil para accesos remotos	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible

Tabla # 2. Tabla de ventajas y desventajas de las técnicas biométricas

AVANCES DE TÉCNICAS BIOMÉTRICAS

Sistema de video vigilancia que reconoce 100.000 rostros en 1,4 segundos

Mitsubishi Electric ha desarrollado un sistema de reconocimiento facial que compara una imagen capturada con una base de datos a una velocidad de ejecución 1.000 veces más rápida que los sistemas actuales. El nuevo sistema permite efectuar una búsqueda entre 100.000 individuos en sólo 1,4 segundos, frente a la velocidad de docenas de rostros por segundo que pueden analizar las tecnologías actuales.

La tecnología permite capturar los rostros desde diferentes ángulos, tanto de frente como de perfil, y compararlos con idénticos parámetros de la base de datos, lo que aumenta la fiabilidad de los resultados.

El metro se queda con tu cara

La Comunidad planea instalar un sistema que, con la ayuda de más de 6.000 cámaras de vigilancia, registrará el rostro de todos los pasajeros y los cotejará con una base de datos de «fichados» por la Policía. También controlará los equipajes.

Capaces de captar los parámetros que hacen que cada una de las caras sean únicas, al igual que las huellas dactilares.

Seguridad virtual.

Este software de reconocimiento tendría la capacidad de crear zonas de seguridad virtual. Sin necesidad de colocar elementos físicos emitiría una alarma si un usuario atravesase el perímetro que previamente se ha diseñado.

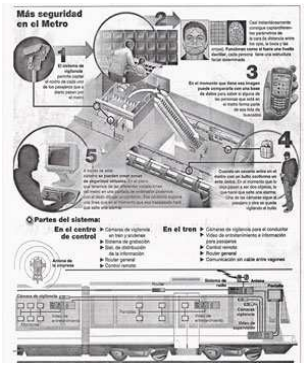

Fig 12. Forma de trabajo de la seguridad virtual

Investigadores españoles diseñan un sistema para transmisiones de voz

Investigadores de la Escuela Universitaria Politécnica de Mataró (EUPMT) han desarrollado un sistema digital que funciona como una "marca de agua" insertada en las grabaciones de voz y que permite garantizar la autenticidad del sonido.

Entre las aplicaciones de esta nueva tecnología, que aún está en las fases de desarrollo más incipientes, destaca su aplicación en el terreno civil para garantizar que las transmisiones entre aviones y la torre de control las efectúe quien corresponda y que las frases no han sido manipuladas.

La marca de agua en los sistema de voz tendría, además de en la aviación, aplicaciones en el sector bancario, pues permitiría dar instrucciones de voz a través de Internet de manera segura y fiable, mientras que el ámbito judicial, y concretamente los forenses, también se pueden ver beneficiados por este tipo de investigaciones.

El desarrollo de esta tecnología se enmarca en el campo de la biometría, una ciencia que estudia el reconocimiento de las personas a través de sus parámetros biológicos y de comportamiento.

Azertia desarrolla para BBVA un sistema de autenticación por voz para sus empleados

Se trata de una solución biométrica de reconocimiento del locutor a través de la línea telefónica

Azertia ha desarrollado para BBVA un sistema de Autenticación por voz, que permite a los empleados la reactivación automática de su clave de acceso al sistema informático de la entidad bancaria.

El proyecto se basa en la integración de los módulos de síntesis de voz y reconocimiento del locutor (desarrollado por la Universidad Politécnica de Madrid) con los sistemas de seguridad de BBVA. Con Azertia ha colaborado Agnitio, empresa surgida como Spin-Off de la Universidad para llevar sus desarrollos al mundo empresarial, que los comercializa como producto Batphone.

El objetivo de este proyecto ha sido desarrollar un sistema de autenticación por voz, que permita a los empleados la reactivación automática de su clave de acceso. La solución, que en el caso de tener éxito tras una fase de prueba exhaustiva, se integraría en los sistemas de BBVA, incluye un proceso de registro de los usuarios que pueden acceder al sistema, y la generación de los modelos de voz para diferentes dicciones.

Finalmente, el sistema hace una autenticación de voz con desafío dinámico, a fin de evitar suplantaciones basadas en la grabación previa de la voz del interlocutor. El sistema, así, se basa en la confluencia de dos tecnologías de carácter emergente, la biometría, y la tecnología de la voz.

DNI (Documento Nacional de Identidad) en España.

A final de año ya habrá 2,5 millones DNI electrónicos, con lo que España se sitúa en la vanguardia tecnológica mundial.
La Policía Nacional ha alcanzado en una semana la expedición del DNI electrónico

número 700.000, cifra que se enmarca dentro del objetivo de que los ciudadanos puedan acceder al nuevo Documento Nacional de Identidad en todas las provincias españolas antes de finalizar 2007

Fig 13. DNI de España

Nuevo celular con identificación dactilar

Porsche se ha aliado a Sagem para lanzar un teléfono de diseño que incorpora un lector de huellas dactilares, el exclusivo celular P'9521

Fig 14. Celular P5'9521

Identificación dactilar móvil

Los Angeles Police Department (LAPD), a través del Programa Homeland Security Grant para la promoción de cooperación inter-agencias, ha solicitado 500 dispositivos portátiles de identificación dactilar BlueCheck de la empresa Cogent Systems, los que serán utilizados para ser operados por oficiales de LAPD así como por otras fuerzas locales que operen bajo el sistema LACRIS (Los Angeles County Regional Identification System.

Los dispositivos BlueCheck utilizan comunicación wireless y pueden operar con las computadoras de portátiles ubicadas en las patrullas, las que proveen la comunicación contra el LAFIS, permitiendo en segundos obtener una respuesta contra los 9 millones de registros criminales existentes.

Fig 15. Dispositivo portátil para identificación dactilar

Nueva gama de terminales biométricos de control de acceso

Sagem Défense Sécurité (grupo de SAFRAN) está lanzando dos nuevos productos biométricos del control de acceso en ocasión de una de las principales exposiciones de seguridad en Europa - IFSEC 2007

Son el MorphoAccess™ 500, un terminal de control de acceso físico, y MorphoSmart™ 1350, un lector para control de acceso lógico. El MorphoAccess™ 500 tiene una nueva plataforma electrónica y un nuevo sensor biométrico (reconocimiento de huella dactilar), y puede identificar hasta 50.000 personas

De acuerdo con especificación PIV IQS del FBI (1), la serie MA500 ofrece mayor seguridad y rendimiento. Es también compatible con la mayoría de los sistemas de control de acceso y tiempo y asistencia disponibles en el mercado.

El MorphoSmart™ 1350 es un nuevo lector USB de huella dactilar para control de acceso lógico. Resuelve las necesidades de las compañías que buscan utilizar tarjetas inteligentes (smartcards) con biometría.

Fig 16. MorphoAccess™ 500

Fig 17. MorphoSmart(TM) Optic 1350

Cardtech/Securtech

TARJETA-BIOMETRIA en Estados Unidos específicamente en San Francisco, a través de exposiciones de casos como “Austria ID Card Implementation”, “Biometrics in Advanced Card and ID Security”, “REAL ID Technology Benefits and Challenges”, entre otras.

Fig 18. Tarjetas Biométricas en Estados Unidos para la seguridad de acceso y manejo de transacciones en Francia

Biometría en las escuelas y en el proceso de votación en Brasil

El gobierno brasileño está apostando en el uso de la tecnología del biometria en dos áeras esenciales para el país: educación y elección. El ministerio de los planes de la educación para introducir por la mitad de las escuelas públicas brasileñas hasta el final del año el control de la presencia de las pupilas para el sistema del biométrico. "Cada escuela tendrá su sistema, pero sugerimos que la pupila inserte el dedo en el sensor del biométrico para colocar su llegada pronto que él llega la universidad".

La votación electrónica con biometria tendrá que alcanzar, según los planes del TSE, toda la base electoral brasileña, estimación en 125 millones de votantes. Programado para comenzar en 2008, el sistema de la votación con biometria utilizará la huella digital del votante. Este método también es usado en Venezuela actualmente en su proceso electoral.

500 casos de doble identidad en Perú

El sistema que utiliza el Registro Nacional de Identificación y Estado Civil (Reniec), que permite la identificación por medio de las huellas dactilares, se logró detectar a más de 500 personas que tienen más de una identidad

Fig 19. RENIEC en Perú

Tecnología para el reconocimiento del rostro.

La tecnología que han desarrollado estos dos jóvenes escanea y hace un *mapa del rostro humano* como una superficie tridimensional, suministrando una referencia mucho más precisa para identificar a una persona que los sistemas actuales.
Los desarrolladores de este sistema fueron 2 gemelos israelíes idénticos de 22 años, casi imposible de diferenciar, los cuales con este sistema podrían revolucionar la seguridad internacional.

Pronósticos

El informe de la Comisión Europea indica que son los Estados miembros los que deben proporcionar las garantías necesarias en materia de respeto a la vida privada y de protección de datos**,** de forma que se controle el uso de los datos biométricos y se impida su uso ilegal.

Todas estas garantías son especialmente

importantes si se tiene en cuenta el aumento de la presencia de los identificadores biométricos en la vida cotidiana de los ciudadanos.

El futuro está muy cerca

En un plazo medio, como puede ser 2015, los alumnos tendrán que pasar un sistema de entrada biométrico en el colegio; los adultos encenderán los coches mediante un escáner que identificará su huella dactilar y los abuelos deberán identificarse a la puerta de las guarderías para poder recoger a sus nietos.

En el hogar, un instrumento que acumulará toda la información técnica sobre la casa se activará mediante un escáner del iris, que podrá también utilizarse para permitir o impedir la entrada de visitantes**.**

Los sistemas de **reconocimiento de caras** podrán usarse en los transportes públicos para detectar a los viajeros que no han pagado su billete; los pagos a través de Internet serán más seguros y se evitarán problemas tan sensibles como el intercambio de bebés al nacer en los hospitales.

Tecnologías en desarrollo con técnicas biométricas

Reconocimiento de uña, tecnología emergente, que no ha sido muy estudiada, existe una patente del 17 de febrero de 1998 en Estados Unidos asignada a Minnesota Mining and Manufacturing Company.

Dinámica del Mouse, desarrollado por Queen Mary, Universidad de Londres

Pulso de la sangre, pulso cardíaco, investigado en La escuela Klipsh de ingeniería eléctrica y computadores, Universidad del estado de New Mexico.

Crestas de las articulaciones de los nudillos, patentado en Estados Unidos por Charles Colbert el 14 de Enero de 1997 y asignada a Personnel Identification & Entry Access Control Inc.

Arrugas del dedo, Toshiba + TEC presentaron un sistema para medir las arrugas del dedo en 1998.

Perfil de presión de la mano, patentado el 21 de agosto de 2003 ante la Organización Mundial de propiedad intelectual, Estados Unidos, Canadá y Australia por parte de Robert D. Inkster, David M. Lokhorst y Ernest M. Reimer.

Reconocimiento dinámico de asimiento, patentado el 21 de noviembre de 2002 en Estados Unidos, Australia y Organización Mundial de propiedad intelectual por Michael Recce del Instituto de tecnología de New Jersey.

Transmisión de sonido de los Huesos, patentado el 19 de Junio de 2003 en Estados Unidos por parte de Yumi Kato, Tadashi Ezaki y Hideo Sato y asignado a Sony Corporation

Firma bio-dinámica, patentada por Daniel H. Lange, asignada a IDesia Ltd., la patente más antigua es del cinco de febrero de 2004, se ha patentado en la Organización Mundial de propiedad intelectual, Oficina Europea de patentes, Canadá, China, Australia, Estados Unidos y Corea del sur, todas las patentes tiene como título "método y aparato para el reconocimiento de la identidad electro-biométrica.

Biométricos Multimodales y otras fusiones multi-biométricas

Hay algunas aplicaciones biométricas requieren un nivel de calidad técnica que es difícil obtener con una simple medida biométrica. El uso de múltiples medidas biométricas con alta independencia de sensores biométricos, algoritmos o

modalidades normalmente da una actuación técnica mejorada y reduce los riesgos. Esto incluye una mejora en el nivel de calidad donde todas las medidas biométricas no están disponibles.

Conclusiones

Los sistemas biométricos y técnicas son las 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.

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.

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.

Últimamente los fabricantes han dedicado una gran energía a esta área del desarrollo y continuarán haciéndolo.

Nuevas Tecnologías: Las ventas no son la única parte de la industria biométrica que está creciendo. El número de tecnologías 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.

Fig 20. Sistemas biométricos

Referencias bibliográficas

http://www.accu-time.com/products.htm

http://www.ansi.org

http://www.atlas.schindler.com/

http://bibliotk.gdl.up.mx/ceup/huella.pdf

http://www.bioidentidad.com/

http://www.biometricgroup.com/
http://www.biometria.gov.ar/

http://www.biometco.com/

http://www.biometrics.org

http://www.biometricsandsecurity.com/
http://www.digitalpersona.com/

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

http://www.iti.upv.es/services/reviewtic/publi c/2005/06/pdf/2005-06.pdf/attach/2005-06.pdf

http://www.jeuazarru.com/docs/biometria.pdf

http://www.monografias.com/trabajos43/biometria/biometria3.shtml#mas

http://www.q20.com.ve/

http://www.robotiker.com/castellano/noticias/eventos_pdf/37/Biometria2.pdf