1. INTRODUCCIÓN

La biometría se basa en la premisa 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 validarla.

Los dispositivos capaces de realizar el proceso de identificación o validación son el tema de este estudio.

Desde sus primeras apariciones en el mercado, este tipo de dispositivos han tenido que sortear tres dificultades fundamentales:

- Su elevado coste que impedía su despliegue masivo, de cientos o incluso de miles de unidades en las grandes corporaciones donde, cada empleado, debería poseer sus propios dispositivos de seguridad.
- Su tamaño, demasiado grande para poder instalarlo normalmente en ordenadores de sobremesa, portátiles o en los pequeños dispositivos de mano tan de moda en la actualidad como teléfonos móviles, PDA´s,... etc
- Y por último, la poca sensibilidad mostrada por los grandes suministradores de redes hacia el uso y la necesidad de integración de este tipo de productos biométricos en sus infraestructuras de red.

Este panorama está cambiando drásticamente en estos últimos meses como consecuencia del interés y de la necesidad creciente surgida en el mercado a la hora de exigir sistemas más seguros. (mercado internacional)

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

Las identificación por medio de las huellas dactilares es una de las forma más representativa de la utilización de la biometría. Existen sin embargo otros dispositivos biométricos que procesan otras características humanas.

2. OBJETIVOS

En el mundo interconectado del siglo XXI la identificación es insuficiente. Se necesitan sistemas aun más seguros. EL control de accesos e intrusión... sean una realidad segura para empresas y consumidores. Ese paso se realizará por medio de los sistemas biométricos los únicos que permiten una AUTENTICACIÓN inequívoca e individualizada. El presente trabajo tiene como objetivo dar a conocer que es un dispositivo biométrico, su origen, conocer los diferentes dispositivos biométricos que existen en el mercado y su funcionamiento. Otro enfoque importante del trabajo es saber cuando o porque se usarían tales dispositivos, tendencias, ventajas y desventajas de su uso. También se listaran algunas empresas con sus productos y algunos ejemplos prácticos de uso de estos dispositivos.

3. ¿QUE ES LA BIOMETRÍA?

La palabra biometría deriva de las palabras: bio (vida) y metría (medida).

La ciencia biométrica se define como el análisis estadístico de observaciones biológicas.

Así, un ***dispositivo biométrico*** es aquel que es capaz de capturar características biológicas de un individuo (rostro, huella dactilar, voz, etc), compararlas, electrónicamente, contra una población de una o más de tales características y actuar según el resultado de la comparación.

4. ORIGEN DE LA BIOMETRIA

No es verdad que la biometría sea una técnica de identificación futurista. Desde hace varios siglos los hombres se han identificado por medio de este sistema.

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 las 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. Ésta 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.

En el siglo diecinueve comienzan las investigaciones científicas acerca de la biometría con el fin de buscar un sistema de identificación de personas con fines judiciales. Con estas investigaciones se producen importantes avances y se comienzan a utilizar los rasgos morfológicos únicos en cada persona para la identificación.

De hecho, en cierta forma es una vuelta a los conceptos que durante la segunda mitad del siglo 19 manejó el francés Alphonse Bertillon. El funcionario de la Prefectura de Policía de París logró desarrollar, con las limitaciones de la época, una base de datos con las características fisiológicas de 1.500 procesados por delitos violentos en esa localidad.

Aunque Bertillon menospreciaba la utilidad de los rastros dactilares (para él eran simples “marcas distintivas”), su método se impuso en la Francia decimonónica, al punto que obtuvo el cargo de jefe nacional de identificación. El “bertillonage” incluía datos tales como la longitud de la mano izquierda, el largo y el ancho del cráneo, la

longitud de la oreja izquierda y otros. Sirvió, por ejemplo, para determinar la verdadera identidad de antisociales reincidentes.

A más cien años de la muerte de Bertillon, los métodos más aceptados de identificación se basan en la colección de rastros dactilares y, últimamente, de muestras de ácido desoxiribonucleico (ADN), cuyos grados de confiabilidad resultan casi infalibles.

Hoy en día, la mayoría de los países del mundo utiliza las huellas digitales como sistema práctico y seguro de identificación. Con el avance tecnológico nuevos instrumentos aparecen para la obtención y verificación de huellas digitales. Se comienza a utilizar otros rasgos morfológicos como variantes de identificación, por ejemplo el iris del ojo, el calor facial o la voz.

Actualmente la biometría se presenta en un sin número de aplicaciones, demostrando ser, posiblemente, el mejor método de identificación humana.

5. TÉCNICAS DE AUTENTICACIÓN

La autenticación, que establece una prueba de identidad de un usuario para una computadora, es una de las cuestiones más importantes de seguridad en las computadoras y redes. Por ejemplo, los cajeros automáticos, son ejemplos típicos de maquinas que necesitan de una prueba, normalmente una secuencia de números, que verifique si el dueño de una determinada cuenta bancaria es realmente la persona que esta accediendo. Es de esperarse, que una buena clave de acceso sea, además de secreta a extraños y de deducción complicada (fechas de nacimiento, números de teléfonos, o todavía números repetidos, nunca son buenas estrategias), fácil de recordar. El problema principal es que estos objetivos son incompatibles: una contraseña ***fácil*** de recordar por una persona es, típicamente, ***fácil*** de romper.

La autenticación de usuario es básicamente un proceso de prueba de su identidad. Existen tres técnicas básicas, basada en: “algo que el usuario sabe”, “algo que el usuario tiene” y “algo que el usuario es”.

Las señas de acceso corresponden a la categoría “algo que el usuario sabe” por ejemplo, PASSWORD. Las tarjetas de crédito y llaves comunes son ejemplos de técnicas “algo que el usuario tiene”. La huella digital, la voz, la retina, son ejemplos ”algo que el usuario es”.

La autenticación “algo que el usuario sabe”: asume que solo una persona conoce una determinada clase o seña de acceso. Este tipo de autenticación se usa ampliamente en redes, Internet y en las intranets. Una gran amenaza que trae esta técnica es que un impostor descubra la contraseña de alguien y se haga pasar por esta persona, violando la seguridad. Existen formas de disminuir la posibilidad de que alguien descubra la seña, por ejemplo aumentando la longitud de la contraseña. El problema de aumentar el tamaño de la clave radica en que los seres humanos no somos buenos para recordar

códigos largos, lo cual hace que, auque el sistema admita contraseñas largas, pocos las utilicen.

Existen infinidad de variantes de sistemas basados en "algo que el usuario sabe", pero todos tienen un punto débil, dependen de la buena memoria del usuario.

En conclusión con esta técnica, es difícil aumentar la seguridad manteniendo la comodidad para el usuario.

La técnica "algo que el usuario tiene": supone que el usuario legitimo es una persona que tiene un dispositivo determinado (tarjeta, llave, control remoto, etc) que lo autentica ante el sistema. Si alguien roba el dispositivo, o él legitima usuario lo pierde, el sistema no vale nada. Por ejemplo, un automóvil, quien tenga las llaves, es el *"dueño del auto"*.

La técnica "algo que el usuario es" intenta basarse en alguna característica biológica y física del usuario. Puede autenticar por ejemplo: las huellas dactilares, el iris, la palma de la mano, DNA, etc Sistemas de este tipo suelen ser más difíciles de burlar que los anteriores y mucho más cómoda para el usuario, pues no dependen de su buena memoria.
Sin embargo estas técnicas aun no se usan ampliamente, pues el reconocimiento biométrico exige dispositivos relativamente caros en comparación con otros no biométricos. Sin embargo las demandas actuales de seguridad y comodidad están haciendo posible la producción masiva, lo cual traerá un abaratamiento de los dispositivos.
Existe una variedad de dispositivos biométricos todos son bastante caros para usarse en todos los casos donde se requiera seguridad. Sin embargo existen situaciones en las cuales el valor de lo que se quiere resguardar justifica el costo del sistema.
Los dispositivos más usados actualmente están basados en el reconocimiento del iris, las huellas digitales, la caligrafía y de patrón de voz.
Sin embargo una desventaja de los dispositivos biométricos es el hecho de que están sujetos a un gran margen de error. Generalmente el margen de error esta relacionado con el costo de los dispositivos, cuanto más económico sea, mayor es el margen de error.

Combinando técnicas
A fin de aumentar la seguridad, muchos sistemas combinan las técnicas anteriores. Por ejemplo, los cajeros automáticos. Aquí el usuario debe, primero introducir su tarjeta, "algo que el usuario tiene", luego de que el sistema la reconoce como válida, debe ingresar su PIN "algo que el usuario sabe".

Es común, también, que al comprar con tarjeta de crédito, la vendedora solicite la cédula de identidad policial. Aquí el sistema combina las técnicas "algo que el usuario tiene" y "algo que el usuario es" usando de esta forma una técnica biométrica primitiva.

Se utiliza también un sistema en el cual un individuo debe primero ingresar un código alfanumérico, y luego presentar al sistema alguna característica biométrica, por ejemplo, la palma de la mano. En este sistema se combinan las técnicas, "algo que el usuario es" con "algo que el usuario sabe".

6. ¿POR QUÉ USAR BIOMETRÍA?

La biometría es fácil de usar, nada que recordar nada que cambiar nada que perder. Además proporciona un nivel más alto de seguridad, unívoca "firma" de una característica humana que no puede ser fácilmente adivinada o "hackeada". La Identificación y Autenticación biométrica (I&A) explota el hecho de que ciertas características biológicas son singulares e inalterables y son además, imposibles de perder, transferir u olvidar. Esto las hace más confiables, amigables y seguras que los passwords.

En el pasado el procesamiento de I&A biométrico era hecho manualmente por gente que física y mentalmente comparaba huellas dactilares contra tarjetas, rostros contra fotos de pasaportes y voces contra cintas grabadas. Hoy en día, dispositivos tales como escáneres, videocámaras, y micrófonos pueden, electrónicamente, capturar y entregar estas mismas características biométricas para automatizar procesos y comparaciones. Cada tecnología biométrica (huella dactilar, rostro, voz, etc) tiene sus propias características, variedades y certezas.

El proceso de captura, extracción de esas características y variedades, el almacenamiento y la comparación es universalmente similar para todos los dispositivos biométricos.

Pero no todo es perfecto en estos sistemas. Existe la posibilidad de que el sistema acepte o rechace indebidamente a un usuario. Existen algoritmos que permiten minimizar estos errores.

Los niveles de precisión biométricos pueden variar pero son siempre más confiables que el 100% de falsas aceptaciones experimentadas con las passwords prestadas o robadas.

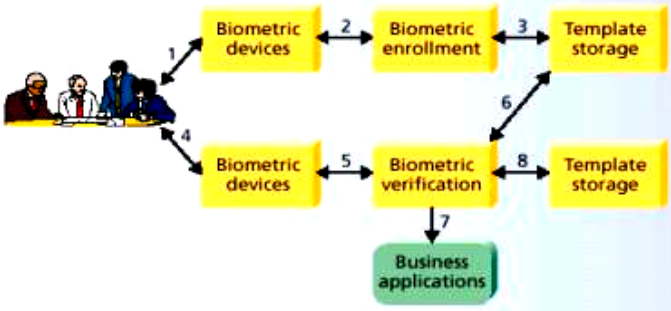
7. FUNCIONAMIENTO BÁSICO DE DISPOSITIVOS BIOMÉTRICOS

La figura siguiente, muestra el diagrama en bloques de un sistema biométrico general y describe brevemente su funcionamiento.

La mayoría de los sistemas biométricos funcionan de maneras muy similares y se puede resumir en dos pasos:

- El primer paso consiste en que la persona debe *registrarse* ("enroll" en inglés) en el sistema. 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 el segundo paso.

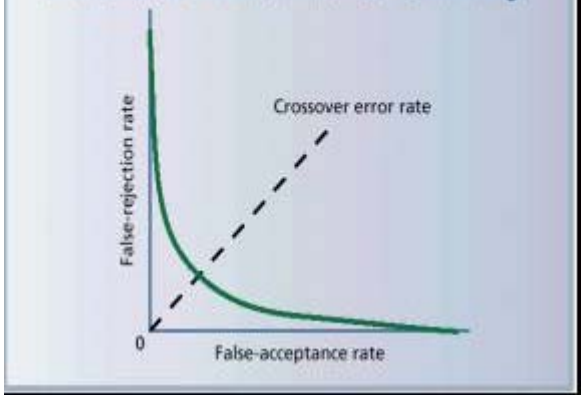
Figure 1. How a biometric system works.



(1) Capture the chosen biometric; (2) process the biometric and extract and enroll the biometric template; (3) store the template in a local repository, a central repository, or a portable token such as a smart card; (4) live-scan the chosen biometric; (5) process the biometric and extract the biometric template; (6) match the scanned biometric template against stored templates; (7) provide a matching score to business applications; (8) record a secure audit trail with respect to system use.

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. Cada proveedor de tecnología biométrica configura la/el falsa/o aceptación/rechazo de forma diferente. . *La figura* siguiente muestra esta relación de compromiso.

Figure 2. Crossover error rate attempts to combine two measures of biometric accuracy.



Las tasas de errores son medidas de dos maneras, una por la cantidad de personas con permiso que son rechazadas (tasa de falso rechazo) y otro por la cantidad de personas sin permiso que son aceptadas (tasa de aceptación indebida). En este caso, es claro, que la mayor preocupación se centra con el segundo tipo, pero en implementaciones practicas el primer problema genera mucho molestia.

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.

- De acuerdo a la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona.

  - En el caso de ***verificació*n**, la persona le informa al sistema cual es su identidad ya sea presentando una tarjeta de identificación o entrando alguna clave especial. El sistema captura el rasgo característico de la persona (la huella digital en nuestro ejemplo) y lo procesa para crear una representación electrónica llamada *modelo en vivo* ("live template" en inglés.) Por último, el sistema compara el modelo en vivo con el modelo de referencia de la persona. Si ambos modelos parean la verificación es exitosa. De no serlos, la verificación es fallida.

  - En caso de que la función del sistema biométrico sea ***identificació*n**, 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.

    Dependiendo de la función del sistema, este segundo paso puede ser:

    - *Identificación positiva*

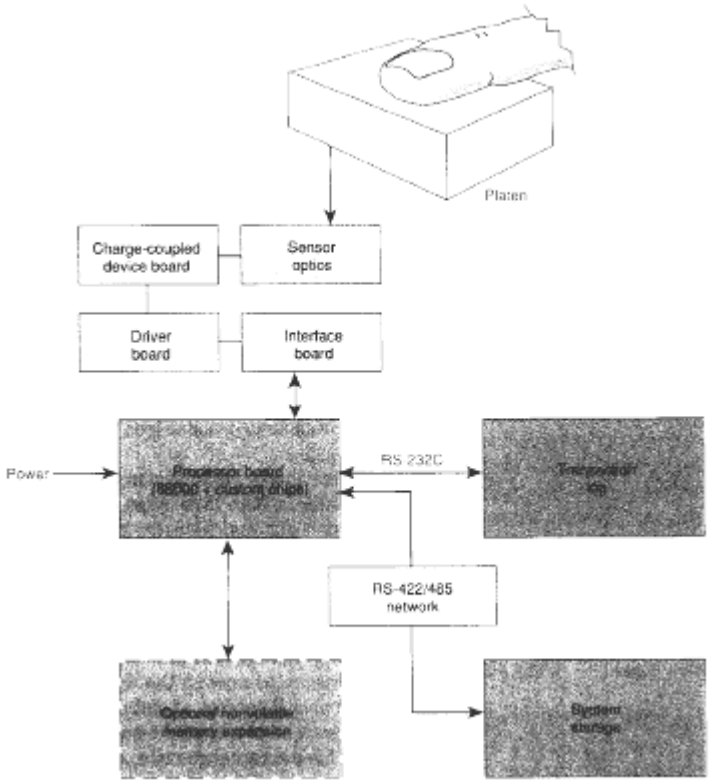
      La función de un sistema de *identificación positiva* consiste en probar que la identidad de la persona está registrada en el sistema. La persona hace una reclamación positiva de identidad al sistema biométrico, es decir, la persona alega que está registrada en el sistema. El sistema responde comparando automáticamente el modelo en vivo con uno o varios modelos de referencia. Si la persona es identificada, el sistema biométrico le concede a la persona ciertos privilegios, de lo contrario los privilegios son negados.

    - *Identificación negativa*

      La función de un sistema biométrico de *identificación negativa* consiste en probar que la identidad de la persona no está registrada en el sistema biométrico. Un ejemplo puede ser un sistema que verifique que las personas que entran a un banco no se encuentren en una lista de delincuentes. La persona le hace una reclamación negativa de identidad al sistema biométrico, el cual responde comparando automáticamente el modelo en vivo con uno o varios modelos de referencia. Si la identidad no está registrada, el sistema biométrico le concede ciertos privilegios a la persona como, por ejemplo, permitirle entrar al banco. Si el sistema reconoce a la persona, este le niega dichos privilegios y hasta quizás alerte si se debe tomar alguna acción más radical como intervenir la persona.

Tanto en verificación como en identificación, si la comparación es exitosa el sistema biométrico concede a la persona ciertos privilegios como, por ejemplo, acceso a un área restringida o acceso a su cuenta de banco. Cuando la comparación es fallida, los privilegios son negados.

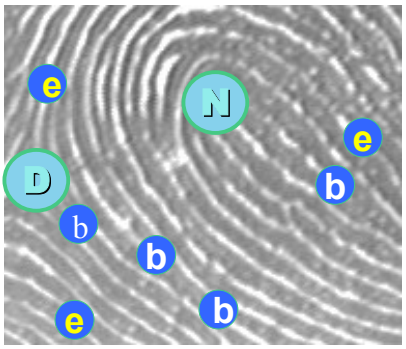
8. DISPOSITIVOS BIOMÉTRICOS DE USO FRECUENTE



Lector de Impresión Digital

Descripcion funcional:

- Diseño formado por las papilas de la piel del dedo.
- Única para cada persona.
- Cambia poco con la edad.



Claves:

- Papilas
- Puntos característicos (minúcias)
- e = extremidades
- b = bifurcaciones
- N = Núcleo
- D = Delta

La impresión digital es reconocida a través del sistema automaticamente.
El sistema mantiene un banco de datos con las impresiones registradas.
El sistema recibe una impresión y puede entonces efectuar su inclusión o consultar si ya existe por los procesos de validación (1:1) o identificación (1:N)

Identificación (1:N)
Proceso por el cual el sistema compara la hulla del usuario (una), con todas las huellas almacenadas (N) y extrae la que más se asemeja a la del usuario. Para esto se utiliza algoritmos de complejo desarrollo, técnicas de inteligencia artificial y características de las impresiones digitales (minúcias).

Validación (1:1)
El proceso (1:N) necesita hacer muchas comparaciones. Esto demanda muchos recursos y tiempo. Otra técnica, mucho más sencilla de implementar es la validación, consiste en usar algun otro sistema (contraseña, tarjeta, etc...) junto con la huella. Esto permite un ahorro de tiempo y recursos, pues el algoritmo utiliza la clave, por ejemplo, para reducir el conjunto de busqueda.

Fases del reconocimiento digital

1 – Capturar la impresion digital
A través de un scanner de impresiones, la imagen es capturada “en vivo” o podemos utilizar un scanner de papel para adquirir la imagen.

2 – El Tratamiento de la imagen y extraccion de minúcias
La imagen capturada es sometida a diversos algoritmos para el mejoramiento y extraccion de las minúcias.

3 – Busqueda en la base de datos.(modulo N)
A través de las minúcias extraídas efectuamos una busqueda en el banco de datos. Esta busca retorna una lista de candidatas.

4 – busqueda “Módulo K” en el banco de datos
Analisis minucioso del resultado de la busqueda anterior para identificar la impresion digital que está siendo buscada.

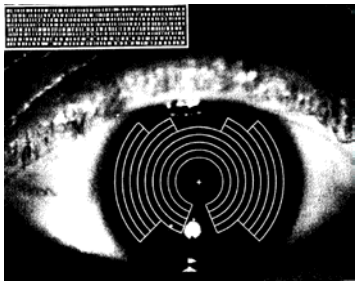
5 – Divulgación del resultado
El sistema informa si la impresion digital fue localizada en el banco de datos, informando el “puntaje” obtenido en la busqueda.

Los lectores de huella digital utilizan un escáner que hacen rebotar rayos de luz en el dedo, de donde una computadora procesa el patrón refractado. Esto permite al lector crear una *imagen* de su dedo, que es trasmitida al software biométrico.

El software tiene una base de datos de huellas digitales entradas previamente, contra las cuales es comparada la imagen tomada. Si se encuentra *semejanza* entre la imagen tomada y la almacenada en la base de datos, el software biométrico permitirá el acceso al sistema; de otro modo será rechazado y se generará una alarma o un registro si es necesario.

Scanner de la Iris

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal una estructura única por individuo que forma un sistema muy complejo - de hasta 266 grados de libertad - inalterable durante toda la vida de la persona. El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.



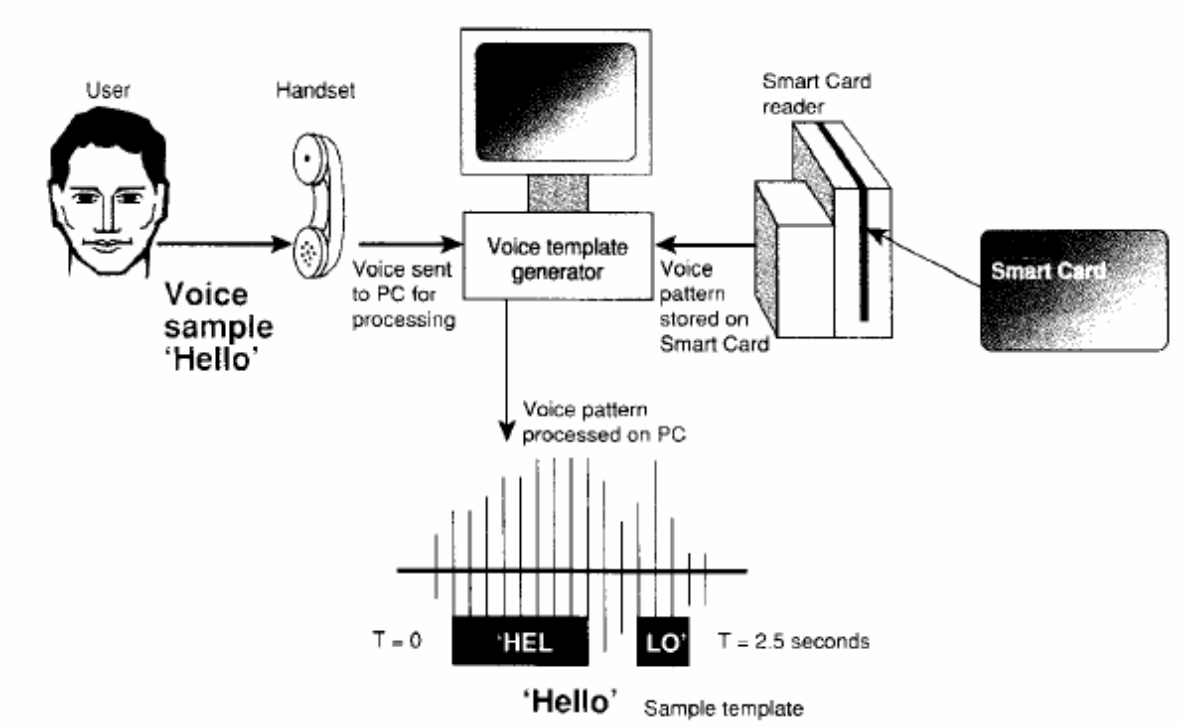
La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retinales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios. Para ello, se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado, usando una cámara de alta resolución. Generalmente esto se hace mirando a través del lente de una cámara fija, la persona simplemente se coloca frente a la cámara y el sistema automáticamente localiza los ojos, los enfoca y captura la imagen del iris, ésta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos (típicamente 256 KBytes) suficiente para los propósitos de autenticación. Esa muestra, denominada iriscode (en la figura se muestra una imagen de un iris humano con su iriscode asociado) es comparada con otra tomada con anterioridad y almacenada en la base de datos del sistema, de forma que si ambas coinciden el usuario se considera autenticado con éxito; la probabilidad de una falsa aceptación es la menor de todos los modelos biométricos.

El iris del ojo como un identificador es quizás uno de los métodos más ajenos para las personas, ya que entre nosotros no nos reconocemos por la apariencia del iris. Es este misterio lo que seguramente haya hecho de este método uno muy utilizado en las películas de espionaje

.

Este identificador es uno de los más precisos entre los sistemas biométricos. Algunos factores que han afectado su proliferación lo son la poca aceptación entre sus usuarios y el precio muy caro de la tecnología.

identificador de patrones 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. Tan solo basta recordar las veces en que reconocemos a alguien conocido por teléfono para comprender la riqueza de esta característica como método de reconocimiento.

Los sistemas de verificación mediante la voz "escuchan" mucho mas allá del modo de hablar y el tono de voz. Mediante el análisis de los sonidos que emitimos, los tonos bajos y agudos, vibración de la laringe, tonos nasales y de la garganta, también crean modelos de la anatomía de la traquea, cuerdas vocales y cavidades. Muchos de estos sistemas operan independientemente del idioma o el acento de la persona.

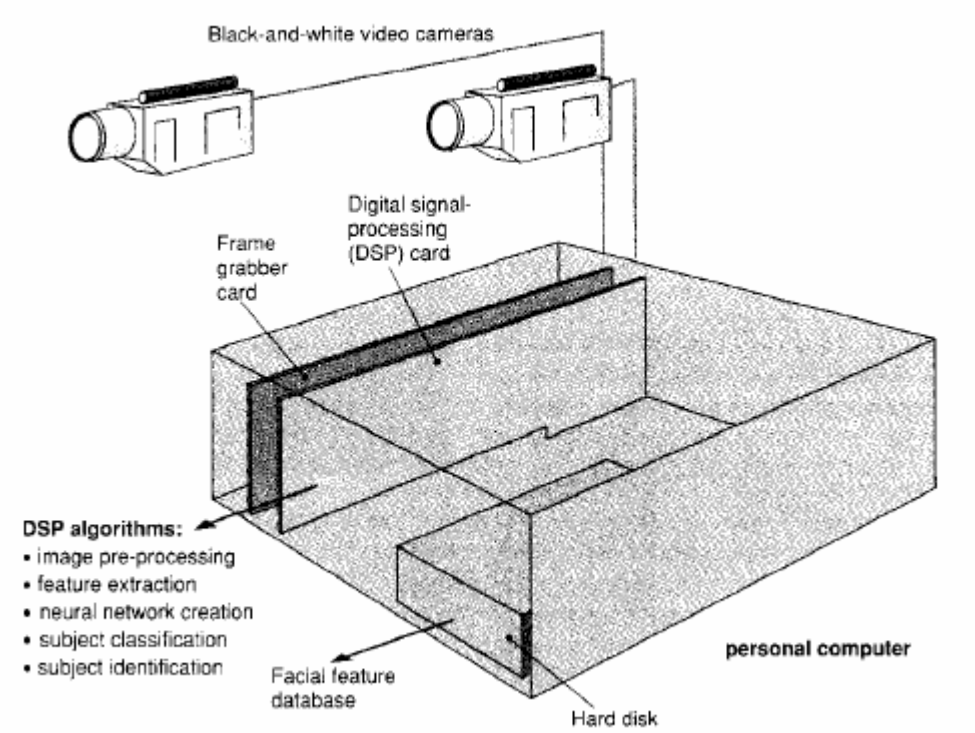
Esa tecnología ya fue utilizada, pero no fue bien recibida (a pesar de ser relativamente barata) pues es relativamente fácil de romper con grabaciones digitales y por la posibilidad de rechazar una autenticación de alguien que tenga los patrones levemente alterados por causa de la inestabilidad de la voz.

Firmas

La firma es un método de verificación de identidad de uso común. Diariamente las personas utilizan su firma para validar cheques y documentos importantes. Como la firma es una habilidad adquirida, se le considera un rasgo de comportamiento. Mas es muy complejo reproducir la habilidad humana de identificar si una firma es o no autentica.

En biometría, el uso de la firma para verificación de identidad se hace de una manera diferente a la tradicional. Dependiendo del sistema, tanto la superficie donde se firma como el bolígrafo utilizado pueden contener varios sensores. Estos sensores miden características mucho mas allá que simplemente la forma o apariencia de la firma: la presión que se aplica sobre la superficie, el ángulo al cual se sujeta el bolígrafo y hasta la velocidad y el ritmo de cómo la persona ejecuta su firma son características capturadas por el sistema.

Reconocimiento del rostro



Muy popular hoy en día, relativamente barato y con niveles razonables de acierto, este dispositivo captura patrones geométricos en el rostro a través de una cámara. Los sistemas de reconocimiento de rostro son tal vez los más fáciles de comprender ya que para nosotros la cara es la manera más directa de identificar a los familiares, amigos, conocidos o celebridades.

Los métodos utilizados en el reconocimiento de rostros van desde la correlación Estadística de la geometría y forma de la cara, hasta el uso de tecnología de redes neuronales que buscan imitar la manera en que funciona el cerebro humano. Muchos de estos sistemas pueden reconocer a una persona aun cuando esta se haya dejado crecer la barba o el bigote, se pinte o se cambie el estilo del cabello, tenga maquillaje o use anteojos.

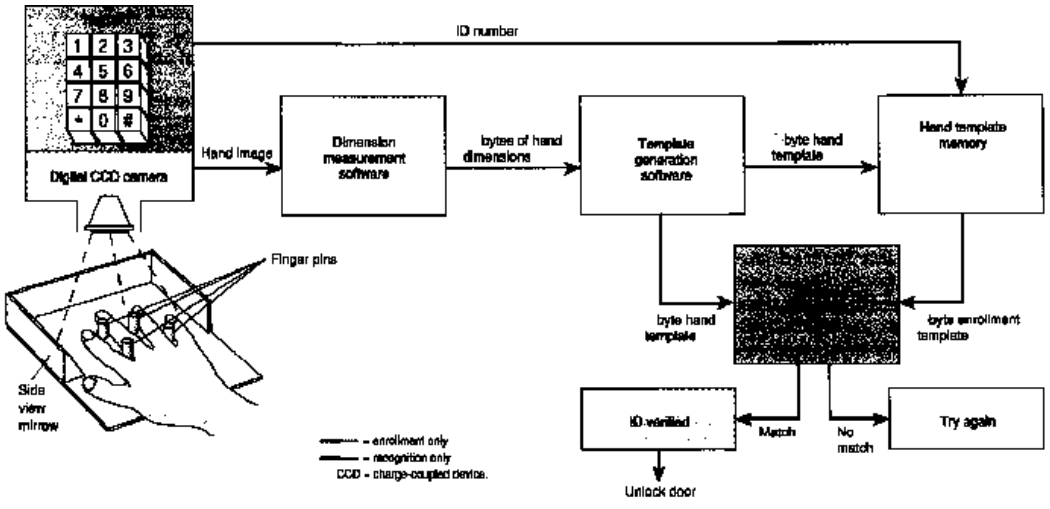
El uso de estas técnicas anteriores, combinadas con técnicas de encriptación, ha sido ampliamente usada en Internet, para resolver el problema de la autenticación de los usuarios, servidores, páginas y sitios. Existe toda una tecnología de certificación desarrollada, que resuelve específicamente la cuestión de la autenticación utilizando técnicas de criptografía.

Velocidad de digitación:

Algunos estudios comprueban que una manera en la que diferentes personas digitan esta bien distinguida y algunas experiencias se han hecho con esta idea. Existen problemas con las variaciones ocasionales debidas a dolencias. Para un estudio más detalla ver http://www.ii.uam.es/~abie/docs/biotest.htm que es un tesis de grado sobre este tema.

Lectores de la mano:

El reconocimiento de la mano se puede hacer en dos y tres dimensiones.
Los sistemas de dos dimensiones buscan en la palma de la mano patrones en las líneas, estos patrones son casi tan distintivos como las huellas digitales. El sistema toma entonces los puntos de minucia de la palma, los compara contra el modelo de referencia (reference template), y procede en consecuencia.
Los lectores de tres dimensiones, sin embargo funcionan de forma distinta. Estos no intentan identificar patrones en las líneas de la palma, ni huella. Estos miden las dimensiones de la mano (largo de los dedos, altura de la mano, etc)
Sin embargo, el esquema ambos sistemas (2Dy3D) son similares. En la figura se muestra un sistema con teclado. Existen también sistemas de este tipo que no usan teclado.



No son tan precisos como los de impresiones digitales, pero son más baratos de mantener.

Scanner de Retina:

La vasculatura retinal (forma de los vasos sanguíneos de la retina humana) es un elemento característico de cada individuo, tan distinto como una impresión digital y aparentemente más fácil de ser leído, por lo que numerosos estudios en el campo de la autenticación de usuarios se basan en el reconocimiento de esta vasculatura.

En los sistemas de autenticación basados en patrones retinales el usuario a identificar ha de mirar a través de unos binoculares, ajustar la distancia ínter ocular y el movimiento de la cabeza, mirar a un punto determinado y por último pulsar un botón para indicar al dispositivo que se encuentra listo para el análisis. En ese momento sé 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.

El sistema no es muy cómodo si el usuario tiene anteojos o si tiene contacto con el lector óptico. Por estas razones el escaneo de retina no es bien aceptado por los usuarios, a pesar de que la tecnología en sí trabaja muy bien. En tanto esos dispositivos todavía son bastante caros y usados solamente en instalaciones de altísima seguridad.

La compañía EyeDentify posee la patente mundial para analizadores de vasculatura retinal, por lo que es la principal desarrolladora de esta tecnología; su página *web* se puede encontrar en `http://www.eyedentify.com/`.

Para finalizar se muestra una tabla de comparaciones entre los dispositivos biométricos:

Table 1. Comparison of biometrics

Characteristic	Fingerprints	Hand geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error incidence	Dryness, dirt, age	Hand injury, age	Glasses	Poor lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds, weather
Accuracy	High	High	Very high	Very high	High	High	High
Cost	*	*	*	*	*	*	*
User acceptance	Medium	Medium	Medium	Medium	Medium	Very high	High
Required security level	High	Medium	High	Very high	Medium	Medium	Medium
Long-term stability	High	Medium	High	High	Medium	Medium	Medium

* The large number of factors involved makes a simple cost comparison impractical.

Tabla tomada de la revista IT Pro enero-febrero 2001

9. MERCADO BIOMÉTRICO: PRESENTE Y FUTURO

Algunas aplicaciones y beneficios de la tecnología biométrica en cuanto a control de acceso y algunos tópicos claves a considerar al invertir en un dispositivo biométrico. También mencionaremos los dispositivos disponibles actualmente en el mercado y daremos un vistazo a lo que el futuro le depara a esta industria.

Desempeño

En estos equipos, el desempeño es el tiempo total que le toma a una persona usar el equipo. Para los fabricantes es difícil especificar el desempeño, dado que depende relativamente del usuario. Algunos fabricantes hablan de un "tiempo de verificación" del lector, pero ello solo es el tiempo que le toma al lector verificar la identidad después que el usuario ha colocado la parte de su cuerpo en la unidad. Muchos lectores biométricos verifican la identidad en menos de dos segundos. El desempeño incluye el tiempo de verificación más el tiempo que toma digitar el número de identificación y colocar la parte del cuerpo a ser leída.

Tecnologías Disponibles

La industria está constantemente descubriendo nuevos atributos físicos y maneras para medir la individualidad de los humanos. Algunos de estos sistemas aún están desarrollándose. Mientras tanto, revisaremos los dispositivos y tecnologías biométricas que están disponibles comercialmente. A menos que se mencione lo contrario, toda la información ha sido provista por los fabricantes.

El Ojo

Actualmente dos compañías fabrican sistemas que leen partes del ojo para identificación. El sistema EyeDentify observa el patrón vascular de la retina del ojo. Iriscan, como su nombre implica, se basa en el iris (la parte colorida de su ojo) para identificación. Ninguna de estas tecnologías requieren digitar un número de identificación para usar el sistema.

EyeDentify

EyeDentify liberó su primer producto en 1982. La tecnología se fue refinando y una segunda generación de sistemas apareció en el mercado en 1989. El producto actual ha sido el resultado de constantes avances y reducciones de costos.

Producto: Icam 2001
Precio de lista: $2,650
Tasa de Falso Rechazo: 0.4%
Tasa de Falsa Aceptación: 0.001%
Tasa de Igual Error: no disponible
Tiempo de Verificación: 1.5 a 4 segundos (varía dependiendo del número de usuarios)
Autónomo (standalone): Sí
Red: Sí

Iriscan

Iriscan introdujo su tecnología al mercado comercial en 1994. La unidad captura una imagen del iris mediante video CCD estándar, similar al de las cámaras de video.

Producto: Sistema 2000EAC
Precio de lista: $5,950
Tasa de Falso Rechazo: 0.00066%
Tasa de Falsa Aceptación: 0.00078%
Tasa de Igual Error: 0.00076%
Tiempo de verificación: 2 segundos (10,000 usuarios)
Autónomo (standalone): Sí
Red: Sí

La Huella Digital

Actualmente, varios fabricantes tienen sistemas en el mercado diseñados especialmente para aplicaciones de control de acceso.

Identix / Fingerscan

Identix introdujo su sistema de huella digital para control de acceso en 1988. En 1994 formaron una alianza con Bio Recognition Systems (BRS). BRS integraba la unidad lectora de huellas de Identix y los algoritmos asociados de creación de plantillas de Identix con la terminal de control de acceso de BRS.

Producto: TouchLock II
Precio de lista: $2,950
Tasa de Falso Rechazo: <1.0%
Tasa de Falsa Aceptación: 0.0001%
Tasa de Igual Error: no disponible
Tiempo de verificación: 0.5 segundos
Autónomo (standalone): Sí
Red: Sí

Startek

Esta compañía taiwanesa introdujo un sistema al Mercado en 1993. La información a continuación proviene de fuentes de referencia.

Producto: FIC-2000I
Precio de lista: $5,500 por un sistema de 4 puertas
Tasa de Falso Rechazo: 1.0%
Tasa de Falsa Aceptación: 0.0001%
Tasa de Igual Error: no disponible
Tiempo de verificación: menos de 1 segundo
Autónomo:
Sí Red: Sí

La Mano

La geometría de la mano fue la primera tecnología utilizada en un dispositivo disponible comercialmente, el Identimat, el cual apareció en el Mercado en 1976. Hoy dos compañías ofrecen sistemas de geometría de la mano: Recognition Systems, Inc. y BioMet Partners.

BioMet Partners

El Digi-2, introducido en 1994, verifica la identidad mediante la forma y tamaño de dos dedos. BioMet Partners ofrece un módulo OEM consistente en una maquinaria óptica y los algoritmos asociados de creación de patrones. Otras compañías integran el módulo en un lector de control de acceso. La información a continuación proviene de fuentes de referencia.

Producto: Digi-2
Precio de lista: no disponible
Tasa de Falso Rechazo: 0.1%
Tasa de Falsa Aceptación 0.1%
Tasa de Igual Error: 0.1%
Tiempo de verificación: 1 segundo
Autónomo: Sí
Red: Sí

Recognition Systems, Inc.

Desde que introdujo su primer sistema en 1986, Recognition Systems (RSI) ha refinado y reducido el costo de la tecnología de reconocimiento de la mano. Actualmente RSI ofrece su cuarta generación de productos, los HandReaders HandPunch y HandKey para control de asistencia y control de acceso respectivamente. Los equipos evalúan una imagen tridimensional de los cuatro dedos y parte de la mano.

Producto: HandKey ID3D
Precio de lista: $2,150
Tasa de Falso Rechazo: 0.1%
Tasa de Falsa Aceptación 0.1%
Tasa de Igual Error: 0.1%
Tiempo de verificación: 1 segundo
Red: Sí

La Voz

Varias compañías han introducido sistemas de voz a través de los años, pero sólo una, Voice Strategies, está mercadeando un sistema activamente.

Voice Strategies

Introducido en 1991, el sistema de Voice Strategies utiliza tecnología desarrollada por Texas Instruments. Los teléfonos que se colocan en los puntos de acceso se enlazan con una computadora central donde la verificación toma lugar.

Producto: VACS (Voice *Access Control System* o Sistema de Control de Acceso por Voz)
Precio de lista: $21,000 por un sistema de 16 puertas
Tasa de Falso Rechazo: no disponible
Tasa de Falsa Aceptación: no disponible
Tasa de Igual Error: no disponible
Tiempo de verificación: 1.5 segundos
Autónomo: No
Red: Sí

El Futuro

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 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 que 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 biométricos hicieron su aparición en aplicaciones de alta seguridad, su consideración principal era mantener afuera a "los tipos malos". Se prestó poca atención a dejar entrar a "los buenos". Para esas aplicaciones, una tasa baja de Falsa Aceptación era el requerimiento más importante.

A medida que los biométricos 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.

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", si un sabueso puede distinguir personas por su olor, por qué no un biométrico!

Resumen

A medida que el mercado biométrico se expande, la necesidad de comprender todos estos tópicos se hace más crítica. La aceptación del usuario siempre será un factor esencial en la implementación exitosa de un dispositivo biométrico. Desafortunadamente, algunos fabricantes son incapaces de medir el grado de aceptación del equipo. Aplicaciones diferentes exigen niveles diferentes de desempeño para alcanzar una alta aceptación de los usuarios.

Por ejemplo, un laboratorio de defensa de alta seguridad puede requerir una baja Tasa de Falsa Aceptación, mientras que una guardería podría requerir una baja Tasa de Falso Rechazo. Por ello, es de suma importancia entender qué significan estos indicadores, cómo deben interactuar y cómo impactarán la aceptación del usuario.

Algo seguro es que el futuro es muy brillante para los biométricos en aplicaciones de control de acceso. Sólo los dispositivos biométricos ofrecen un control verdadero sobre quién puede entrar. La tecnología ya no es material de ciencia-ficción, ha sido usada con resultados dignos de alabanza por muchos años y por compañías grandes y pequeñas. Los sistemas biométricos de hoy cumplen con los requerimientos de seguridad y presupuestos de la gran mayoría de las aplicaciones comerciales de control

de acceso. Y a medida que los precios bajen, los biométricos se convertirán en artículos de uso diario en la vida de más y más personas.

10. APLICACIONES

La biometría protege el aeropuerto de Tel Aviv (Publicación diaria de Prime Media Press ® - Derechos reservados © Copyright internacional 1997-2002 (30.01.2002):

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.

Pedro Diestre, analista senior de EDS Seguridad en España, Italia y Portugal, explicaba que 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.

Siguen una lista de lugares donde se utilizan dispositivos biométricos

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

Iris

Sun SparcStation para análisis

11. TÉCNICAS PARA BURLAR DISPOSITIVOS BIOMETRICOS

Como es de esperarse no existe ninguna técnica de autenticación que sea cien por ciento segura. Los dispositivos biométricos no son la excepción. Como lo demuestra el siguiente artículo publicado por el diario PLANTÃO INFO de SÃO PAULO en edición del 20 de mayo del 2002.

"Dedos de gelatina pueden burlar biometría

SÃO PAULO - Los sistemas biométricos de seguridad capaces de identificar personas con la lectura de sus huellas digitales pueden fácilmente ser engañados por un ingrediente bastante común en casas de todo o mundo: la gelatina.

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

Para obtener los moldes de dedos falsos, dice el articulo, 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, dice la BBC, esta imagen fue trasferida 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.

De a cuerdo con los especialistas en seguridad Bruce Schneier, que analizó el trabajo de los científicos, el hecho de que alguien consiga usar un ingrediente domestico para falsificar una huella digital es suficiente para que se deje de usar el sistema de biometría con fines de seguridad.

Por: Renata Mesquita, do Plantão INFO"

12. CONCLUSIÓN

Los presentados hasta aquí son los sistemas biométricos principales actualmente en uso y desarrollo, pero no son los únicos. Los investigadores examinan actualmente la viabilidad de sistemas basados en el análisis del ADN e incluso de los olores corporales.

La mayoría de las soluciones requieren asociar dispositivos de entrada de información externas a un software de soporte. Existen sistemas que utilizan un dispositivo de entrada de información externo que todos tienen: el teclado. En vez de sustituir el sistema de la conexión del usuario mediante nombre/password, esta tecnología (dinámica, llamada de golpe de teclado) trabaja conjuntamente con la información de la conexión. Cuando usted pulsa su nombre y password, el software mide su ritmo al pulsar y lo compara con su perfil.

No hay razón técnica por la que varios sistemas biométricos no podrían trabajar en conjunción para analizar muchas de nuestras características, pero cada sistema está asociado a un modelo que identifica al usuario.

Teniendo en cuenta las preocupaciones actuales por la seguridad, los sistemas biométricos parecieran ser inevitables. Pero de hecho sigue habiendo resistencia considerable a ellos.

Pero el factor de decisión, uniforme para los negocios, puede ser la cuestión de sí estos sistemas están percibidos según lo necesitado.

Los departamentos de administración de redes, por ejemplo, tienen que considerar la pérdida real que ocasiona el acceso desautorizado, así como el costo y las complicaciones de poner elementos de hardware en los escritorios de los usuarios y de mantener ese hardware. Para los usuarios caseros, el costo, la conveniencia, y la necesidad son consideraciones importantes. Los vendedores de accesorios biométricos tienen mucho que hacer antes de que sus sistemas lleguen a ser de uso común, pero seguramente en la primera década del milenio próximo se encontraran estos elementos en la mayoría de los sitios que requieran de acceso seguro.

Debe tenerse en cuenta sin embargo, que en los últimos tiempos han comenzado a surgir diversos grupos de protesta frente al avance del uso de los dispositivos biométricos.

La principal queja se basa en el hecho de que la organización puede utilizar los datos obtenidos no solo para la identificación de la persona, sino también para ser vendida o utilizada por otras corporaciones, gobiernos o centros médicos. Una lectura de la retina inofensiva para el usuario puede ser utilizada para indicar si la persona tiene SIDA o toma drogas, por ejemplo.

Precisamente, para evitar el peligro de la centralización o venta no autorizada de la información, una alternativa comenzó a ser utilizada por las empresas. El uso de una "tarjeta inteligente" en conjunto con un dispositivo como el de lectura dactilar, permite almacenar los datos obtenidos en el chip del usuario en vez de ser guardados en la base de datos del sistema. La información del usuario es comparada luego con la guardada en la tarjeta, ofreciendo así una seguridad extra a la persona.

13. BIBLIOGRAFÍA

http://www.visioningenieria.com/soluciones.html
http://www.trielo.com.br/ase_productos
http://www.ast_afis.com.com/es/es-id4.html
http://www.biometria.com.pe
http://www.pyratech.hpg.ig.com.br//prmcipal.html
http://www.ii.uam.es/~abie/docs/biotest.htm
http://www2.vol.com.br/info/aberto/infonews/052002/20052002-22.shl
http://www.homini.com/biometria.html
http://www.homini.com/origen.htm
http://www.ast_afis.com/biometria.html
http://homepage.ntlworld.com/avanti/
http://www.belt.com.es/noticias/02_abril/22_26/23_biometria.html
http://www.embratel.com.br/internet.wks05/tecnologia/tegnologia
http://www.iriscan.com/
www.neotec.com.pa/ComoPorque
www.neokoros.com
www.biometrics.org
www.ibia.org
www.insys.com.mx/biometria/biometria
http://www.nrtec.com.mx/biometria.htm
http://www.e-printing.com.ar/noticias/2002/ene2002/15195679.htm
http://www.ibia.org
http://www.biometrics.org
http://www.afb.org.uk
http://homepage.ntlworld.com/avanti/
http://stat.tamu.edu/Biometrics/