Universidad Católica

"Nuestra Señora de la Asunción"

Facultad de Ciencias y Tecnología

D.E.I.

Teoría y Aplicación a la Informática 2

Sistemas de Identificación Biométricas Modernas y Biodinámicas

Ricardo Ariel Sosa Sartori

Mat. 048922

2do. Semestre - 2007

Identificación biométrica, la llave del futuro

Como salidas de una película de espías o de ciencia-ficción las nuevas tecnologías de identificación por medio de sistemas biométricos se perfilan como la futura llave que nos abrirá todas las puertas. El santo y seña del siglo XXI será nuestro propio cuerpo, nuestras características físicas, únicas y distintas de las de cualquier otro ser humano. Pronto la identificación por huellas dactilares, geografía de la mano, reconocimiento facial, del iris o de la voz se convertirán en los nuevos passwords de entrada a múltiples sistemas, desde el acceso a cuentas bancarias, vehículos, áreas laborales y archivos informáticos hasta, ¿por qué no?, a nuestra propia vivienda.

Identificación, vigilancia, control, no son conceptos del mundo moderno, sino que caminan de la mano de la historia del hombre. Ya en el antiguo Egipto se llevaban registros de población que facilitaban el control fiscal o militar y son bien conocidos también los Censos Israelitas, que datan del siglo XV A.C. y que permitían, entre otras cosas, la identificación de los componentes de las tribus nómadas para su posterior reagrupamiento. Desde entonces hasta hoy la identificación personal se ha basado tradicionalmente en la posesión de llaves, tarjetas, claves, de palabras o números, como el de la seguridad social, el carné de identidad, el de conducir, los códigos de barras, etc. Sin embargo, el ser humano posee características que lo hacen único: las huellas dactilares, la voz, el iris, el rostro o el ADN, constituyen la contraseña más segura que existe.

La verificación biométrica por medio de características físicas únicas comenzó al final del siglo XIX con las huellas dactilares y desde entonces su uso se ha visto generalizado sobre todo por los cuerpos de seguridad. Hoy, sistemas automáticos que escanean y digitalizan huellas han llevado esta técnica mucho más allá de las investigaciones policiales y se pueden encontrar todo tipo de dispositivos biométricos para controlar los accesos a sistemas informáticos, garantizar la seguridad en transacciones bancarias o simplemente acceder a nuestro dinero, como es el caso de los cajeros automáticos que reconocen el iris o la retina, de los que ya existen algunos prototipos instalados en las calles de Estados unidos y Gran Bretaña.

Ante la necesidad de sistemas cada vez más seguros los científicos han recurrido a la Biometría aplicada a la verificación de la identidad de un individuo de forma automática, empleando sus características biológicas, psicológicas y de conducta. Esta identificación, que es la única que permite una autenticación individual y exacta, utiliza

ciertos patrones fisiológicos, digitalizados y almacenados. Los rasgos comúnmente usados incluyen el modelo de huellas digitales, de vasos sanguíneos en la mano o retina, del rostro, el tamaño, forma y largo de los dedos e incluso el olor.

Cómo funcionan

Los sistemas biométricos se componen de un hardware y un software; el primero captura la característica concreta del individuo y el segundo interpreta la información y determina su aceptabilidad o rechazo, todo en función de los datos que han sido almacenados por medio de un registro inicial de la característica biométrica que mida el dispositivo en cuestión. Ese registro inicial o toma de muestra es lo que determina la eficacia del sistema. En el caso de las huellas dactilares, un usuario coloca el dedo en un sensor que hace la lectura digital de su huella, después, el programa guardará la información como un modelo; la próxima vez que ese usuario intente acceder al sistema deberá repetir la operación y el software verificará que los datos corresponden con el modelo. El mismo principio rige para la identificación por el iris/retina, con ayuda de videocámara, el rostro, la mano completa, etc. Las tasas de exactitud en la verificación dependen en gran medida de dos factores: el cambio que se puede producir en las personas, debido a accidentes o a envejecimiento, y las condiciones ambientales, como humedad en el aire, suciedad y sudor, en especial en la lectura que implique el uso de las manos.

En cuanto a qué partes del cuerpo son las más adecuadas para su utilización en identificación biométrica, aunque en principio cualquiera sería susceptible de ser usada, para su elección se atiende a criterios prácticos concretos. Lo ideal es que se trate de una característica física robusta, es decir, no sujeta a grandes cambios; que sea lo más distintiva posible en relación con el resto de la población, que sea una zona accesible, disponible y, por supuesto, aceptable por el usuario que, en ocasiones, puede llegar a percibir algunos dispositivos biométricos como excesivamente intrusivos.

Por último, hay que hacer una distinción entre aquellos dispositivos que miden el comportamiento y los que miden una característica fisiológica. Entre los primeros se encuentran el análisis de la dinámica de la firma y el del golpe en el teclado; los segundos incluyen la huella dactilar, la geometría de la mano y el dedo, la termografía facial y la exploración del iris o la retina. El reconocimiento de la voz es un parámetro biométrico basado en ambos análisis, el fisiológico que determina la zona vocal y el de comportamiento del lenguaje y las palabras usadas. Evidentemente aquellos dispositivos que se basen en el comportamiento requieren de la cooperación del usuario, mientras que se puede identificar fisiológicamente a cualquiera sin su

cooperación e incluso sin su conocimiento, como en el caso de la imagen captada por una videocámara.

Tipos de sistemas y sus aplicaciones

Cada sistema biométrico utiliza una cierta clase de interfaz, un sensor o mecanismo de captura determinado y un software específico. La identificación por geometría de la mano o huellas digitales, la más extendida, crea una imagen digital tridimensional, que es capturada, calibrada y guardada en un archivo. Para la identificación por el ojo existen dos sistemas: topografía del iris, identificando en pocos segundos más de 4.000 puntos, y topografía de la retina, midiendo con luz infrarroja de baja intensidad 320 puntos predefinidos en el diagrama de las venas. También se dispone de la Termografía, la dinámica del tecleo, la Cadencia del paso y el análisis gestual entre otros…

El reconocimiento facial compara las características faciales con una imagen previamente escaneada, lo mismo que la identificación por voz con un patrón pregrabado, que analiza la presión del aire y las vibraciones sobre la laringe. La identificación por firma mide el tiempo, la presión, la velocidad, el ángulo de colocación del lápiz y la velocidad de las curvas, todo a través de un lápiz óptico con el que la persona firma en un soporte específico o pad. Por último, los sensores de olor, aún en desarrollo, utilizan un proceso químico similar al que se produce entre la nariz y el cerebro, sin que los perfumes sean capaces de enmascarar el olor particular de cada uno.

La identificación biométrica experimenta una aceptación creciente debido a la reducción de los costos de los dispositivos y a su alta confiabilidad. Por ello, no se restringe su uso a aplicaciones de alta seguridad, como bancos e instalaciones gubernamentales, sino que también se extiende a las empresas, para el control de clientes y empleados y en el acceso a oficinas y plantas comerciales e industriales. Aunque la lista sería interminable, algunas de las aplicaciones de la identificación mediante sistemas biométricos serían los servicios públicos, servicios policiales, penitenciarios, instituciones de salud, permisos de conducir, inmigración, registro de armas, controles de acceso, tiempo y asistencia, seguridad de redes informáticas, comercio electrónico, educación, etc.

Autenticación de la Voz

Las nuevas tecnologías del habla permiten una interacción casi natural con sistemas que reconocen la identidad e intención de las voces humanas.

En esta entrevista Guillermo Brinkmann, responsable de estrategias en comunicación unificada y reconocimiento de voz de Avaya, cuenta los fascinantes pormenores de su funcionamiento.

La voz de una persona es única e inconfundible, incluso por teléfono. La expresión cotidiana "no te reconocí la voz", surge de lo usual que resulta identificar el interlocutor a partir de su **sonoridad única**. Los grandes cantantes crean su obra alrededor del "inconfundible estilo" de sus tonos, y el público reconoce a sus ídolos a partir de la sonoridad de sus palabras. La voz puede, en definitiva, ser una imagen indeleble grabada a fuego en la memoria de los demás. Este principio de identidad está en la base de lo que Guillermo Brinkmann denomina las **tecnologías del habla**, que permiten naturalizar la interacción con las máquinas, al **reconocer el estilo y la intención de una voz humana.**

¿Es cierto que la voz tiene la particularidad de ser como una huella digital?

Exactamente, es tan única o más que una huella digital, porque es un patrón, cuando se representa el sonido en el espectro aparece una figura con características únicas. Hay aplicaciones para acceso de usuarios que por lo general se asocian a recursos para seguridad, pero hay un montón de otras, relacionadas con servicios personalizados ¿Cómo se identifica al cliente que llama a un empresa? Por el número de teléfono, pero desde el mismo número pueden llamar distintas personas, o sea que no se trata de una persona sino de aquellas que tiene acceso a ese número. Lo mismo pasa con la clave de acceso de una página web, no se sabe quién entró sino aquellos que tienen conocimiento de la clave. Supongamos que la gente de Direct TV quiera sacar un perfil mío, la clave para alquilar películas es una sola, pero alquilo yo, mi mujer, mi suegro, algún amigo de la familia, entonces el perfil va a ser medio raro, infantiles, de acción, dramas. Ahí no se produce la identificación de la personal real sino de un código que se asocia a un nombre ingresado en la base. A través del reconocimiento de la voz sedefine un perfil de forma mucho más precisa.

¿Y estos desarrollos cuánto tiempo tienen?

En investigación unos 50 años, en aplicación real y efectiva no más de tres o cuatro, pero nosotros creemos que va a tener un crecimiento exponencial en los próximos años.

¿De qué factores depende?

Del dispositivo, hay lectores de iris, scaners de retina, lectores de huellas digitales, pero cuántos hay en una empresa, o en el estado, o en los hogares familiares, ninguno. Ahora, cuánto teléfonos hay, miles, millones. Lo poderoso es su capacidad remota y móvil. El dispositivo para la identificación biométrica por voz es el teléfono, que es universal. Además, la voz es infalsificable. Podrán decir que se puede grabar, y es cierto, pero si

se hacen preguntas ramdom nadie puede tener grabadas con anterioridad las miles que se pueden hacer, por ejemplo, un acceso que pide "diga el titular del diario Clarín de hoy". Nadie puede preverlo.

¿Qué utilidades se está dando a esta tecnología?

Por ejemplo para asistencia en identificación positiva, en las tarjetas de crédito, todas esas preguntas que te hacen para identificar tu identidad, dónde recibe su resumen de cuentas, cuándo cumple años su mujer, dónde vive, preguntas que son bastante intrusivas, muy personales; bueno, con esta tecnología es mucho menos intrusivo y más rápido, más efectivo, tiene una cantidad de beneficios importante. Mucha gente consulta sus movimientos bancarios con frecuencia pero no quiere que otras personas se enteren, o ni siquiera quieren tener contacto con otra persona por una cuestión meramente práctica ¿Por qué no dar ese servicio con una máquina que prácticamente habla?

¿Cómo funciona la verificación biométrica?

Se inicia con la elaboración del proyecto y con la concientización de la empresa que va a instalar la tecnología. Después, para el usuario lo primero es enrolar su voz para que el sistema tenga grabado el patrón biométrico vocal, así como si quiero tener tus huellas digitales, en algún momento la persona tiene que tocar el pianito. Una vez registrado, el patrón se guarda en una base de datos, y acá viene una aclaración importante, ese patrón no es audio sino datos, números, que resultan de una representación espectral del audio primitivo, características físicas, prosodia, entonación, ritmo. A nivel de espacio esto no ocupa casi nada. Cuando el usuario ingresa al servicio, por ejemplo, con las tarjetas de crédito. El sistema pide el número de tarjeta y el D.N.I, y luego se dispone a comprobar que esos datos corresponden a la persona, y le pregunta, "buenos días señor López, por favor, diga qué día es hoy".

Prácticamente se simula un diálogo humano

Estas tecnologías cambian el paradigma de la relación hombre máquina, es una interacción totalmente distinta a la que estás acostumbrado en un IVR convencional , que es muy rígido, niveles y opciones, no hay otra. Además, es posible complementar la verificación con el reconocimiento de voz, y hacer diálogos mucho más humanos, mucho más naturales. Visto desde acá el IVR es tremendamente limitativo, no tiene más de 9 opciones, sin tener en cuenta que está comprobado que una persona no registra más de 3 o 4 opciones. Lo dicen los estudios de usability. Cualquiera al que lo hagan llamar por primera vez a una empresa donde hay muchas opciones las va a escuchar todas porque, por más que aquella que necesita esté en el segundo lugar, le va a quedar la duda de si no queda una más precisa más adelante, y una vez que escuchó todo no va a recordar con precisión cuál era la correcta, y va a volver a empezar.

¿Sirve para cualquier circunstancia?

Te comunicás con una máquina en lo que se llama diálogo natural, lo que en inglés es NLSR, Nautal Language Speech Recognition; es natural, lo que no implica que sea libre, está todo sujeto a ciertas gramáticas, y éstas a su vez están atadas a un contexto. Al hablar con una aplicación de reserva de líneas aéreas el usuario va a poder decir quiero viajar mañana a Santiago en bussines class, quiero hacer una reserva, cosas así, pero cualquier frase tipo "qué tal soy Perez quiero que me reconozcan las millas", no, eso no. Eso es otra tecnología en la que tenés capacidad de procesar lenguajes totalmente abiertos, pero sólo para rutear, la máquina te pregunta ¿qué necesita? y sobre las probabilidades de respuestas el sistema interpreta, se llama Estatistical Language Processing, también es reconocimiento de voz pero distinto a la NLSR, se aplica a otra estrategia, para un principal ruteo. A partir del número único, el concepto del One Number, en lugar de dar un 0800 para cada cosa, con esta tecnología se puede dar uno solo que rutea al sistema a distintas áreas.

¿En qué lugares ya se incorporó esta tecnología?

En Estados Unidos y Europa se usa muchísimo el reconocimiento de voz, nosotros desde acá manejamos Cono Sur, tenemos aplicaciones en Brasil y en Bolivia instalamos una aplicación de reconocimiento para un Contact Center de códigos de áreas internacional para una Telco, en la que se ve las limitaciones que tiene el IVR tradicional que pone 1, 2, 3, 4 ....porque con la interfaz por tono hay cosas imposibles de automatizar y este es un claro ejemplo de eso. En los C.C. de operadores manuales cada vez que una persona quiere llamar a una ciudad extranjera tiene que hacer un contacto previo para averiguar el código ¿Cómo lo automatizas? Primero hay muchos países y dentro de cada país la cantidad de ciudades es enorme, es imposible. Nosotros automatizamos este C.C. donde la máquina le dice: Buenos días ¿necesita un código nacional o internacional? Diga a qué país quiere llamar, diga a qué ciudad, etc. Esto automatiza el 80% de las transacciones. A mí por ejemplo, me gusta ver películas y el Video Club me queda a 8 cuadras, a veces no sé si ir en auto o caminando. Cuando llego resulta que la película que quería no está y termino viendo lo que hay ¿por qué no poner este sistema? Llamás y te dice, buenos días ¿qué película quiere ver? El señor de los anillos uno, me quedan dos en stock ¿quiere que le reserve una?

¿Con voz sobre IP también funciona bien?

Si, funciona muy bien, tanto la verificación como el reconocimiento. Yo te haría una acotación, te diría Telefonía IP, con calidad de servicio, ancho de banda serio y medido, no vas a tener problemas. En esto es cuestión de tener imaginación, como con todas las tecnologías novedosas, cuando se entiende que funciona aparecen las miles de cosas que se pueden automatizar y mejorar.

Reconocimiento de la Firma

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

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se decrementa la seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando éstos desean acceder a él se le solicita tal firma, con un número limitado de intentos. La firma introducida es capturada por un lápiz óptico o por una lectora sensible, y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténticas.

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

Técnicas de reconocimiento Off-line

En este campo, el reconocimiento parte de firmas realizadas previamente, por lo que la única información de que se dispone es la imagen de la firma. Esto va a determinar tanto las características extraídas de la firma, como las técnicas de procesado de la información adquirida.

Técnicas de Reconocimiento On-line

A diferencia del reconocimiento off-line, ahora la información de la firma se adquiere durante la realización de la misma por el firmante. El proceso de adquisición requerirá por tanto el empleo de dispositivos especiales, como tabletas digitalizadoras, etc. Esto hace que los sistemas on-line dispongan de información temporal de la misma (duración total, duración de levantamientos respecto a la total, posiciones, velocidades y aceleraciones instantáneas, velocidades y aceleraciones de escritura máximas, mínimas y medias, posiciones relativas entre levantamientos y/o contactos con el papel). Además, puesto que la adquisición en estos sistemas suele consistir

en el muestreo periódico de características de la firma durante la ejecución de la misma, las técnicas de procesado aplicadas a la información adquirida, son típicas de señales unidimensionales.

En resumen, se podría decir que la principal diferencia entre ambas líneas de trabajo reside en la simultaneidad entre los procesos de realización de la firma y adquisición de la información para el reconocimiento. Como se puede imaginar, puesto que los sistemas on-line disponen de mayor información para realizar el reconocimiento, serán más eficientes en lo referente a verificación de firmantes. Además, como el firmante realiza su firma de forma automática la información dinámica no es fácilmente falsificable por un impostor, y menos aún si para entrenarse en la realización de la falsificación dispone de una imagen de la firma, donde no se conoce ni la dinámica del movimiento durante la ejecución original de la firma, ni la secuencia ordenada de trazos.

Tableta digitalizadora

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

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

- Alineación del punto inicial: El principal objetivo de esta tarea es extraer información independiente de la posición en la tableta donde se ha recogido la firma. Para conseguir esto se establece como origen de coordenadas el primer punto recogido en la firma, es decir, todas las firmas se alinearán con respecto al punto inicial. Esto permite un correcto proceso de matching.
- Segmentación de la firma: Esta tarea realiza automáticamente la decisión de si un punto determinado es o no información válida para el proceso.

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

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

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

Propiedades magnéticas

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

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

Un esquema en particular...

Conclusiones

Los presentados hasta aquí son los sistemas biométricos principales actualmente en uso y desarrollo, pero no son los únicos. Al igual que en muchos otros campos, la tecnología sigue avanzando tanto en la mejora de las técnicas utilizadas en los sistemas ya existentes como en el desarrollo

de nuevas técnicas. Esto es consecuencia de una demanda cada vez mayor de seguridad en un gran número de campos.

El futuro de los sistemas biométricos se ve 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 de precisión

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

A medida que estos sistemas se fueron moviendo a aplicaciones comerciales, la Tasa de Falso Rechazo fue tomando importancia. Algunos bancos lo dejaron claro al sugerir que un biométrico apropiado para verificación de tarjetas de crédito necesitaría una Tasa de Falso Rechazo de 1:100000 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 debe ser baja. 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 del 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 a 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.

Técnicas para burlar dispositivos biométricos

Como es de esperarse no existe ninguna técnica de autenticación que sea cien por ciento seguras. Los dispositivos biométricos no son la excepción. Así lo demuestra un artículo publicado por el diario PLANÂO INFO DE SÂO PAULO en edición del 20 de mayo del 2002.

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

Para obtener los moldes de dedos falsos, dice el artículo, inicialmente un equipo de investigadores usó la gelatina (no en estado líquido) 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 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 transferida a una lámina fotográfica revestida de cobre, que a su vez fue usada para crear el molde tridimensional de un dedo falso con huellas digitales. En este proceso una vez más los científicos japonenses consiguieron engañar los sistemas de seguridad biométricos en el 80% de las veces.

ANEXO – ACTUALES USOS DE LA IDENTIFICACIÓN BIOMÉTRICA

En Bretaña aumento el uso de la biométrica en los escolares. The British Educational Communications y Tecnología Agency (BECTA) publicó directrices para las escuelas del Reino Unido, "BECTA de Orientación sobre la Utilización de los Sistemas biométricos en las escuelas." BECTA explicó que la recopilación de las huellas dactilares de los escolares está cubierto en virtud de la Ley de protección de datos de 1998, hay que tener cuidado cuando esos datos son recogidos, y "las escuelas tienen el deber de garantizar que todos los datos personales que poseen se mantiene de forma segura." Al mismo tiempo, el Reino Unido Información de la Oficina del Comisionado también publicó directrices sobre la biometría de recogida de los escolares, que pueden tener tan sólo cinco años de edad. La Oficina convino en que esa era la recopilación de datos cubiertos por la Ley de Protección de Datos de 1998 y le dijo a las escuelas que "debería explicar las razones por las que presenta el sistema, cómo se utiliza la información personal y la forma en que se mantiene a salvo." No se sabe si los padres entienden perfectamente que, cuando la investigación de un delito, la policía británica se permite el acceso a las escuelas de las bases de datos biométricos sin permiso de sus padres.

U.S. Military Builds Biometric Database on Iraqis. Hoy en día los informes de que tropas de EE.UU. están usando escáneres móviles para capturar las huellas dactilares, ojos exploraciones, y la aportación de otros datos personales de cientos de miles de iraquíes. Aunque el General Patraeus ha indicado que el objetivo es la identidad insurgentes, tropas de EE.UU detienen a los iraquíes en los hogares, puestos de control, los lugares de trabajo, y "En varios vecindarios en Bagdad y sus alrededores, las tropas han ido puerta a puerta de recogida de datos." Un informe de marzo de la Defensa del Pentágono Ciencia Junta dijo militares uso de datos biométricos elevar sustancialmente la protección de la intimidad.

Federal Air Marshals to Surreptitiously Photograph Travelers. Los EE.UU. Departamento de Seguridad Nacional está invirtiendo en tecnología de reconocimiento de cara a fin de que puedan fotografiar a las personas en los aeropuertos, estaciones de trenes y autobuses, y en otros lugares para comprobar si se encuentran en bases de datos de terroristas. El departamento de policía de Los Ángeles ya está utilizando los dispositivos de mano de reconocimiento facial.

Biometrics at the Disney Gates. Cuando el visitante pasa por las puertas de los cuatro parques temáticos de Disney World, el Magic Kingdom, Epcot, Animal Kingdom, MGM Studios o la, se encontrará con algo inesperado y, en gran medida ajeno a ellos. Disney se ha embarcado en un programa para

utilizar una tecnología biométrica de geometría del dedo de la mano para garantizar su valiosa pase. Aparentemente, estos nuevos valores es para el beneficio del pase propietario. Sin embargo, también se está aplicando para garantizar Disney's estructura de precios y la estrategia de comercialización.

Nursery installs fingerprint ID system. Ahora escaneo de una huella digital se ha instalado en el sistema de control de entrada a los niños a una guardería. Sólo los padres y los cuidadores cuyo huellas digitales se guardan en una base de datos será capaz de tener acceso a Wansbeck Kids First Nursery en Ashington, Northumberland.
Allison Winship, su director, dijo: "Queríamos ofrecer la máxima seguridad para los niños y el personal. También quería llevar a la presión ejercida fuera de la personal como antes de que fueran siempre tener que responder a la puerta para permitir que los padres en"

Bibliografía

http://www.cienciadigital.es/hemeroteca/reportaje.php?id=83

http://www.disa.bi.ehu.es/spanish/asignaturas/17223/Sistemas_Biometricos.pdf

http://www.belt.es/noticias/2005/septiembre/07/voz.asp

http://isa.umh.es/arvc/documentos/articulos/Fernandez_JJAA07.pdf

http://www.eurekalert.org/staticrel.php?view=ef0717