

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro

Este documento examina 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.

Los Beneficios de los Biométricos para Control de Acceso

El objetivo de cualquier sistema de control de acceso es permitir la entrada del personal autorizado a sitios específicos. Los sistemas de acceso basados en carnets pueden autorizar pedazos de plástico, pero no pueden distinguir quién porta el carnet.

Los sistemas que usan números de identificación personal (PINes) sólo requieren que un individuo se sepa un número específico para otorgarle acceso. Los dispositivos biométricos verifican la identidad de una persona mediante características físicas únicas e inalterables como las dimensiones de la mano, peculiaridades o medidas de los ojos, huellas digitales o voz.

Los biométricos pueden eliminar el uso de carnets. Aunque el costo inicial de las tarjetas plásticas ha bajado drásticamente, el beneficio real de eliminar carnets se obtiene al reducir costos administrativos. Los carnets perdidos deben reponerse, pero las manos o los ojos no se pierden, no se roban ni se olvidan. No pueden compartirse ni prestarse a otros y nunca se gastan o necesitan ser reemplazados.

Integración

Los controles de acceso no sólo deben identificar a una persona, sino abrir puertas, conceder o negar el acceso basándose en restricciones de tiempo y supervisar las alarmas de las puertas. Los biométricos pueden realizar estas tareas de varias maneras.

Sistemas Aislados

Los dispositivos aislados o autónomos (standalone) consisten en un lector biométrico y un controlador de puertas completo para una sola puerta. Los usuarios se "enrolan" en la unidad dejando que el lector mida las dimensiones de sus manos, ojos o huellas digitales y guarde esas características personales únicas como una plantilla. En un sistema autónomo la plantilla biométrica se almacena localmente.

Cuando los empleados necesitan entrar a un sitio, generalmente marcan un código corto de acceso en el teclado incorporado en la unidad y luego colocan la mano o el ojo para que el lector realice una comparación con la plantilla almacenada. Una vez verificada, la cerradura recibe una señal y se concede el acceso.

Muchos sistemas autónomos incluyen puntos de monitoreo que vigilan el interruptor de la puerta por condiciones de "puerta abierta demasiado tiempo" y "puerta abierta forzada". También incluyen señales de salida para sonar una campana o enviar señales a un panel de alarmas cuando se detectan las condiciones mencionadas. Se puede registrar una bitácora conectando la unidad a una impresora. También es posible programar restricciones de tiempo para usuarios individuales por medio del teclado incorporado. El número de usuarios que soportan estas unidades generalmente está limitado por la memoria disponible y varía de modelo en modelo.

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 2

Sistemas en Red

Las empresas pueden requerir controlar el acceso en más de una puerta. Si bien esto se puede solucionar con múltiples unidades aisladas, una red de dispositivos biométricos tiene muchas ventajas, siendo la más obvia la supervisión centralizada. Las actividades de rutina y las condiciones de alarma se reportan a la PC central, donde se pueden organizar y presentar en manera de reportes.

Los sistemas en red también permiten el "manejo de plantillas", donde todos los usuarios se enrolan en un mismo lector, el cual automáticamente transfiere todas las plantillas a las otras unidades en la red. Luego las plantillas se pueden eliminar o editar en la PC central.

Algunos sistemas biométricos (como aquellos que ofrece Voice Strategies) almacenan toda la información en la PC, que es también donde se realiza la comparación contra la plantilla. Otros sistemas operan sin una PC central, distribuyendo todos los datos de las plantillas a cada lector. En ambos casos el efecto del manejo de plantillas es el mismo. La conexión entre unidades se lleva a cabo generalmente via RS-485, o sobre una línea telefónica y modems.

Integración con Otros Sistemas

Los fabricantes de biométricos ofrecen varios métodos para integrar sus lectores con sistemas convencionales basados en carnets o PINes. La más común es la "emulación de lector de tarjetas": en este modo el "puerto de salida de lector de tarjetas" del biométrico se conecta al puerto de lector de tarjetas del panel existente.

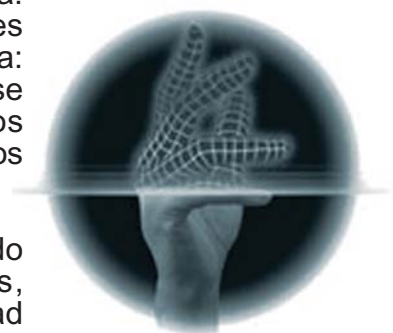
Cuando una persona usa un dispositivo biométrico en modalidad de emulación de lector de tarjetas, el biométrico envía el número de identificación del usuario al sistema sólo si la persona se verifica y resulta ser una persona autorizada. En ese caso los datos se envían en un formato consistente con el del sistema existente de control de acceso por tarjetas. Cuando el número de identificación llega al panel, se trata como si proviniese de un lector de tarjetas. El control y monitoreo de las puertas es manejado por el panel de control de acceso, no por el biométrico.

Algunos equipos biométricos tienen la capacidad de leer carnets como una alternativa a que el empleado marque su código de acceso en un teclado. El biométrico envía el código del carnet al panel central sólo después de verificar la característica física del usuario.

Los fabricantes de biométricos soportan varios estándares de emulación de tarjetas, como Wie-gand, tarjeta inteligente, banda magnética y código de barras. Los formatos de emulación más comunes son el Wiegand de 26 bits con un código de facilidad de 8 bits y el Track 2 de ANSI para banda magnética. Las tarjetas de proximidd también se usan, puesto que generalmente envían los datos en formato Wiegand.

Ninguno de los sistemas con emulación de tarjetas puede transferir los datos de plantillas al sistema existente bajo el concepto de "mane-jo de plantillas" mencionado arriba. Si el sistema existente basado en carnets tiene múltiples unidades biométricas, cada usuario debe enrolarse en cada unidad biométrica: un proceso tedioso. Algunos equipos biométricos permiten enlazarse fuera del sistema basado en carnets, permitiendo a los usuarios enrolarse en una sola terminal y luego distribuir sus plantillas a los otros lectores biométricos.

Algunos fabricantes de sistemas de control de acceso han integrado unidades biométricas a sus productos. Monitor Dynamics, Sensormatic/SoftwareHouse y Westinghouse han integrado la unidad



Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 3

HandKey ID3D de Recognition Systems a sus sistemas. En este tipo de integración, el software de control de acceso puede administrar las plantillas y comunicarse con los dispositivos biométricos.

Asuntos a considerar

1. Aceptación del Usuario

Para que los empleados acepten una unidad biométrica en lugar de un dispositivo "convencional" de marcar asistencia o control de acceso, la unidad no debe causar ningún tipo de inconveniente, incomodidad física, "ansiedad por alta tecnología", ni generar dudas acerca de la salud de los individuos. Estos podrían parecer asuntos subjetivos, pero son lo suficientemente importantes para requerir sesiones informativas del equipo y las ventajas que representa para todos.

La gente prefiere usar dispositivos mecánicos que sean fáciles e intuitivos. Alguna vez ha pasado una tarjeta de crédito por la maquinilla verificadora con la banda magnética del lado incorrecto? Muchos dispositivos biométricos son tan fáciles de usar que hacen de ésta una experiencia muy rara. Demostrar el uso adecuado de la nueva tecnología solo toma unos cuantos minutos.

El equipo biométrico debe trabajar correctamente. Cuando una unidad trabaja correctamente, mantiene a "los malos" afuera y deja entrar a "los buenos". La probabilidad de que esto no suceda se conoce como tasas de error de "falsa aceptación" y "falso rechazo" (las cuales se explican en el documento titulado "Conveniencia versus Seguridad"). Basta decir que los equipos biométricos han probado ser extremadamente seguros, confiables y libres de frustraciones del usuario en pruebas de laboratorio así como en aplicaciones de la vida real.

2. 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.

Si se deben digitar números de empleado, estos deben ser lo más cortos possible. Si se debe usar un número largo, algunos biométricos lo pueden obtener leyendo una tarjeta o carnet. La rapidez que se obtiene de usar tarjetas se debe medir contra los costos e inconvenientes de manejar tarjetas. El tiempo total que se requiere para usar un lector variará dependiendo de la facilidad de uso de la unidad y del tiempo de verificación.

Un sistema de control de acceso basado en tarjetas inicialmente parecerá más rápido, pero como un usuario de biométricos menciona, "la diferencia en velocidad entre un lector de carnets y un lector de manos es aproximadamente dos segundos, pero esto se compensa con el hecho de que la mano está justo enfrente suyo, mientras que generalmente usted debe halar, desenganchar o buscar su carnet en los bolsillos".

3. Tecnologías Disponibles

Los dispositivos biométricos utilizan una amplia variedad de características humanas para confirmar la identidad. La industria está constantemente descubriendo nuevos atributos físicos y maneras para medir la individualidad de los humanos. Algunos de estos sistemas aún están desarrollándose. Discutiremos estas tecnologías luego. Mientras tanto, revisaremos los dispositivos y tecnologías biométricas que están disponibles comercialmente. A menos que se mencione

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

Emulación de lector de tarjetas: Sí

Iriscan

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

Emulación de lector de tarjetas: Sí



identix

La Huella Digital

Las agencias de policía y de aplicación de justicia han usado por décadas las huellas dactilares con propósitos de identificación. El FBI inició sus esfuerzos por automatizar los procesos desde 1960. 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. Identix compró recientemente a BRS.

Producto: TouchLock II

Precio de lista: \$2,950

Tasa de Falso Rechazo: <1.0%

Tasa de Falsa Aceptación: 0.0001%

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 5

Tasa de Igual Error: no disponible
 Tiempo de verificación: 0.5 segundos
 Autónomo (standalone): Sí
 Red: Sí
 Emulación de lector de tarjetas: Sí

Startek

Esta compañía taiwanesa introdujo un sistema al Mercado en 1993. La información a continuación proviene de fuentes de referencia. Startek no respondió a las solicitudes de información.

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
 Emulación de lector de tarjetas: no disponible

La Mano

Los sistemas de geometría de la mano utilizan el tamaño y forma de la mano y los dedos para verificar la identidad. 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
 Emulación de lector de tarjetas: 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. Hasta la fecha, los equipos de RSI son los dispositivos biométricos de mayor uso para control de acceso.

Producto: HandKey ID3D
 Precio de lista: \$2,150

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 6

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
 Emulación de lector de tarjetas: Sí

La Voz

La verificación de voz utiliza los tonos bajos y agudos, vibración de la laringe y tonos nasals y de la garganta para verificar la identidad. 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

Emulación de lector de tarjetas: No



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.

El uso de tarjetas inteligentes también está creciendo, así como la cantidad de información que se puede almacenar en una tarjeta. Mientras más datos se almacenen, mayor será el peligro potencial de una falla de seguridad. Los biométricos son una solución obvia a estos asuntos.

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

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 7

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!

Como mencionamos, también se están aplicando nuevas tecnologías a los sistemas existentes. Por ejemplo, se está desarrollando un sensor para capturar huellas digitales utilizando tecnología de ultrasonido para adquirir la imagen. Este enfoque permitirá minimizar problemas de polvo y brascas que pueden confundir a los lectores ópticos actuales. También se está experimentando con hologramas para almacenar las imágenes de las huellas digitales, lo que permite un almacenamiento más compacto y comparaciones ópticas más rápidas.

Aunque estas tecnologías se ven muy prometedoras, su utilidad la determinará lo hábil que sea cada una para ofrecer soluciones de buen desempeño y bajo costo que cumplan con las necesidades del mercado.

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.

Equipos Biométricos HandReader y el Control de Acceso: Presente y Futuro Pág. 8

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.