Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Automática y Sistemas Computacionales

TRABAJO DE DIPLOMA

Sistemas de autentificación biométricos.

Autor: Alexei Reyes Espino.

Tutor: Dr. Vitalio Alfonso Reguera

Santa Clara

2009

"Año del 50 aniversario del triunfo de la Revolución"

Universidad Central “Marta Abreu” de Las Villas

Facultad de Ingeniería Eléctrica

Departamento de Automática y Sistemas Computacionales

TRABAJO DE DIPLOMA

Sistemas de autentificación biométricos.

Autor: Alexei Reyes Espino.

Tutor: Dr. Vitalio Alfonso Reguera

E-mail: vitalio@uclv.edu.cu

Santa Clara

2009

"Año del 50 aniversario del triunfo de la Revolución"

Hago constar que el presente trabajo de diploma fue realizado en la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de estudios de la especialidad de Ingeniería en Automática, autorizando a que el mismo sea utilizado por la Institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos, ni publicados sin autorización de la Universidad.

_____

Firma del Autor

Los abajo firmantes certificamos que el presente trabajo ha sido realizado según acuerdo de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del Autor

Firma del Jefe de Departamento donde se defiende el trabajo

_____

Firma del Responsable de Información Científico-Técnica

PENSAMIENTO

"ser culto para ser libre"

José Martí

DEDICATORIA

A mis padres por su educación brindada desde la cuna.
A mis hermanos por sus consejos.
A mi esposa por su ayuda incondicional.
A mis amigos por su ayuda desinteresada.
A mis hijos que son mi vida.
A mi tutor por su dedicación.

AGRADECIMIENTOS

A todo el que de una forma u otra me ha ayudado, auque sea con un granito de arena y a la Revolución.

TAREA TÉCNICA

1. Recopilar información sobre los sistemas biométricos y su autentificación.
2. Realizar el estudio y descripción del escenario con vistas a identificar que dispositivos de autentificación biométrica pueden ser utilizados para mejorar la seguridad.
3. Proponer un sistema de autentificación basado en dispositivos biométricos para mejorar la seguridad de una planta industrial.

Firma del Autor

Firma del Tutor

RESUMEN

Este trabajo tiene como objetivo mejorar la seguridad en el acceso a instalaciones de de un combinado militar industrial. Para lo anterior se propone el cambio de tarjetas de identificación personal por lectores de huellas dactilares, lo cual tiene como ventaja principal la garantía de que solamente las personas autorizadas tendrán acceso a la entidad, por tratarse de una identificación biométrica y no una tarjeta que puede ser sustraída o presentada por otra persona no autorizada. Los lectores son de fácil instalación y de gran aceptación en el ámbito de las tecnologías de identificación biométricas, por lo que los convierte en los de mayor uso. También en nuestro trabajo se realiza un breve recuento de las principales técnicas de identificación biométrica que se utilizan en la actualidad y como estas técnicas biométricas cada día se utilizan en aplicaciones donde el hombre requiera de una seguridad de la información o de autentificación, ejemplo: en muchos países se han utilizado estas para la transparencia de los procesos electorales, en los eventos deportivos para detectar la presencia de intrusos y en problemas de seguridad en una gran cantidad de empresas.

TABLA DE CONTENIDOS

PENSAMIENTO i

AGRADECIMIENTOS iii

TAREA TÉCNICA iv

RESUMEN v

INTRODUCCIÓN 1

Organización del informe 2

CAPÍTULO 1. Generalidades de los sistemas de autentificación biométrica. 3

1.1 Tipos o patronas de identificación biométricos. 3

1.1.1 Huellas dactilares. 3

1.1.2 Geometría de la mano. 5

1.1.3 Reconocimiento de la voz. 6

1.1.4 Escritura o firma. 7

1.1.5 Oculares. 8

1.1.6 Reconocimiento de la retina. 9

1.1.7 Reconocimiento facial. 10

1.1.8 Venas. 11

1.1.9 ADN. 12

1.1.10 Otros en estudio. 12
1.2 Conclusiones del capitulo. 13
CAPÍTULO 2. Descripción del escenario. 14
2.1 Breve reseña. 14
2.1.1 Características del sistema. 16
2.2 Análisis del económico. 16
2.2.1 Concluciones del cápitulo. 19
CAPÍTULO 3. Propuesta de implementación. 20
3.1 Propuesta de implementación. 20
3.1.1 Principales caracteristicas de los lectores de huellas dactilares. 22
3.2 Análisis económico. 23
3.3 Consideraciones técnicas. 24
3.4 Conclusiones del capitulo 25
CONCLUSIONES Y RECOMENDACIONES 27
Conclusiones 27
Recomendaciones 28
REFERENCIAS BIBLIOGRÁFICAS 29

INTRODUCCIÓN

Las técnicas biométricas de identificación son las que se utilizan para la identificación y/o autenticación de las personas mediante el uso de una o varias características fisiológicas de los individuos, ya sea para el acceso a algún lugar restringido o para ser identificados y de esta forma permitir o no el acceso a un sistema. El desarrollo que han tenido en los últimos años las técnicas biométricas de identificación ha sido mayúsculo y a dependido del desarrollo de otras tecnologías como la compresión de datos, voz y video, lo que ha permitido que el almacenamiento de estos datos, así como su comparación con los provenientes de los usuarios que desean acceder a algún sistema restringido sea mucho mas sencillo. Desde la antigüedad, el hombre ha tratado de controlar el acceso a determinados lugares, o a determinada información. Los sobres lacrados con el sello real, el conocimiento de una contraseña, la utilización de un determinado uniforme, la posesión de una determinada llave, han permitido desde siempre el acceso a lugares restringidos. En la sociedad digital, se han sustituido los objetos anteriores por números PIN (Personal Identificación Number), certificados digitales, firmas digitales, etc.; Sin embargo estos objetos o datos pueden ser robados, falsificados, filtrados o deducidos. Es fácil conocer la contraseña de una persona o adivinar un numero PIN. Para permitir autenticar a una persona, ya sea para acceder a un lugar físico, para efectuar una transacción bancaria o para realizar una compra se deben buscar métodos que no dependan de una "llave" determinada, sino que la propia persona sea la llave que le permita autenticarse. Donde nuestro principal problema es controlar o restringir el acceso de personas que no estén autorizadas a acceder a este complejo militar, sin que no sea controlado por un patrón biométrico, ya que este no puede ser violado por sus características. Es por ello que se tiene como objetivo

fundamental la búsqueda de cual de todas las técnicas biométricas utilizadas en la actualidad es la que vamos a emplear y el porque de ello. [1]

Organización del informe

El informe está organizado de la siguiente forma: este consta de una tarea técnica, un resumen de lo fundamental del trabajo realizado, una tabla de contenido, una introducción del trabajo, la organización del informe y tres capítulos, el primero nos brinda una información de las principales técnicas de autentificación biométricas utilizadas en la actualidad, el segundo nos brinda una información sobre el estado del arte en nuestro propio escenario y el tercero nos propone la utilización de una de las técnicas biométricas a utilizar para garantizar la confiabilidad del sistema de protección de esta área.

.

CAPÍTULO 1. Generalidades de los sistemas de autentificación biométrica.

Introducción:

En el siguiente capitulo se realizará una breve introducción a las principales técnicas de identificación biométrica.

1.1 Tipos o patronas de identificación biométricos.

Dentro las principales técnicas de identificación biomédica se encuentran: Huellas dactilares, geometría de la mano, reconocimiento de la voz, escritura o firma, oculares, reconocimiento de la retina, reconocimiento facial, venas, ADN y otros en estudio

1.1.1 Huellas dactilares.

La identificación de Huellas Digitales es una de las técnicas más antiguas y ciertamente la mas difundida de los medios de identificación usados actualmente. La huella digital de un individuo es definida por una compleja combinación de patrones de líneas, arcos, lazos, y círculos. Un lector de huellas lee la huella mediante el uso de una luz intermitente a través de una lámina de vidrio, sobre el cual el usuario ha plasmado uno o varios de sus dedos, cuya reflexión se digitaliza, existen software de computadora que sirven para codificar los distintos patrones encontrados en la imagen digitalizada y las plantillas resultante puede ser encriptados de forma opcional y almacenada en una base de datos central, o sobre una tarjeta individual de cada usuario. Las Huellas Digitales pueden ser obtenidas de diferentes maneras. El procedimiento común envuelve la captura de la imagen de la impresión hecha

en algún papel lo cual no es muy práctico para la implementación de un sistema de identificación de civiles, para lo que se podría utilizar mejor un sistema de registro utilizando un escáner óptico. Un escáner registra y analiza una imagen del dedo que se coloca sobre una lámina de vidrio. A pesar que es mucho más conveniente que un sistema que utiliza tinta, el sistema óptico basado en un escaneo en vivo puede ser poco confiable dependiendo de los niveles de suciedad y otros agentes externos que podrían causar distorsión en la imagen. A continuación en la figura 1 se muestra un lector [2].

Figura 1 Lector de huellas dactilares.

El lector de huellas dactilares trabaja utilizando en sensor de silicón para tomar la foto de la huella y basado en minucia, busca cosas interesantes, usando patrones biométricos, los busca y los localiza para convertirlos en una representación numérica que crea un archivo plantilla de 256 bytes, en la Figura 2 se muestran otros tipos de lectores.

Figura 2 Otros lectores de huellas dactilares

A continuación alguna de sus principales ventajas la huellas digital es única de cada de cada persona, permanece inalterable por toda la vida, existen grandes base de datos en la actualidad, se ha invertido gran cantidad de dinero en el desarrollo de la misma, es una técnica no intrusita, es decir, el colocar el dedo en el lector no hace sentir al usuario que su cuerpo está siendo invadido y la tasa de error de los algoritmo es muy baja. Sus principales desventajas son: Al ejecutar la búsqueda pude ser lento, a menos que tenga varios sistemas identificadores repartiéndose el trabajo, la imagen escaneada puede ser borrosa o inexacta debido a heridas, suciedad en el dedo o en el escáner.

1.1.2 Geometría de la mano.

Para medir la geometría de la mano se utiliza un escáner de mano que no es más que un dispositivo bastante simple que mide la geometría de la mano para obtener una plantilla de la mano del usuario. El usuario coloca su mano en un pequeño dispositivo (que puede pesar aproximadamente 4.5 Kg.), posicionando sus dedos acordes al juego de pines señalizadotes marcados en el dispositivo por aproximadamente 1.2 segundos. Una cámara digital captura la forma de la mano y envía el dato a un microprocesador para su análisis. El dato es comprimido hasta tener aproximadamente 9 bytes de información fundamental que caracteriza la mano de cada persona y comparado con todos los perfiles almacenados en la base de datos. La información de los nuevos usuarios puede ser capturada fácilmente ya que este solo tiene que colocar la mano en el dispositivo tres veces para obtener el dato en forma inicial. El espacio de memoria requerido para almacenar las plantillas es bastante pequeño (alrededor de 9 bytes, lo cual cabe fácilmente en la cinta magnética de una tarjeta). El uso de señales en el dispositivo para colocar la mano facilita la recolección de los datos.

El bajo costo y alto rendimiento de este dispositivo lo hace una opción popular para pequeñas organizaciones. Más de 3500 escáneres de mano son usados actualmente; uno de los dispositivos más sobresaliente consiste en una cámara digital en Blanco y Negro que captura una imagen de la mano y, a través de un espejo, obtiene la forma de la mano de perfil. Un procesador mide las características más resultantes de la geometría de la mano como longitud y ancho de los dedos, área total, etc., obteniendo un dato total. El software que genera las plantillas reduce el dato hasta pesar 9 bytes, lo cual es comparado con el dato almacenado previamente de la persona. En la figura 3 se muestra uno de ellos, estos

trabajan capturando la imagen en tres dimensiones, son analizados 31000 puntos, y tomadas 90 medidas únicas, se mide longitud, anchura, grosor y el área de superficie. El (ID) se crea por el tamaño de la mano y se genera un archivo témplate de 9 bytes.

Figura 3 Escáner de mano.

Dentro de las principales ventajas se encuentran: la plantilla ocupa pequeñas cantidades de bytes, es un sistema no intrusivo y es de gran exactitud.

Sus desventajas: Los lectores son de gran tamaño y son muy costoso.

1.1.3 Reconocimiento de la voz.

La voz es uno de las características que identificamos como particulares de las personas, y en la vida diaria, nos permiten reconocerlas con facilidad. Es un medio natural de interacción con el entorno y por tanto resulta muy aceptable para los usuarios pronunciar una palabra o frase ante un micrófono para identificarse.

Las características específicas de la voz de cada persona se deben a diferencias en aspectos fisiológicos y de comportamiento del aparato fonador. La forma del tracto vocal (laringe, faringe, cavidad oral, cavidad nasal, etc.) goza del papel más importante porque modifica fuertemente el contenido espectral de la onda sonora generada. Son precisamente las características del espectrograma de la voz las que configura los parámetros biométricos usados habitualmente para distinguir un locutor de otro.

La gran variabilidad de la voz de un mismo individuo a lo largo de períodos relativamente cortos de tiempo, y la moderada especificidad de los parámetros que se extraen de ella hacen que el reconocimiento del locutor sea una técnica de verificación que se usa únicamente en combinación como identificación por tarjeta inteligente, por código

de acceso, sus principales ventajas son: Muy alta facilidad de medida ya que el costo del hardware necesario es mínimo y la adquisición muy sencilla y cómoda para el usuario, tiene muy alta universalidad ya que el sector de la población con problemas para el habla es relativamente bajo y tiene buenas prestaciones ya que la verificación es posible con recazos de cómputo muy bajo y el volumen de información es perfectamente aceptable.

Sus principales desventajas: Baja permanencia ya que los parámetros básico de la voz pueden variar fácilmente, debido a muchos factores en período de tiempo muy corto, baja unicidad ya que la capacidad de distinguir un usuario de otro es moderada, ya que un importante parecido del habla no es raro y baja resistencia a el engaño ya que con una simple grabación de alta calidad permitiría el acceso a no ser que la frase a pronunciar sea, por ejemplo, variable, o haya de ser respuesta a una pregunta realizada por el sistema de forma aleatoria. [3].

1.1.4 Escritura o firma.

El reconocimiento mediante el uso de la firma no es nuevo. Este método ha sido utilizado para validar todos nuestros documentos legales por años. Sin embargo, la validación absoluta de las firmas es un asunto dificultoso. Algunos sistemas usan bolígrafos que contienen dispositivos sensibles al movimiento y a la presión. Específicamente se utiliza un acelerómetro bi-axial que mide los cambios en las fuerzas en el eje de las x y las y. Otro censor de fuerzas mide las variaciones en el eje de la z, es decir, las fuerzas que suben o bajan. Los usuarios firman en el sistema que recolecta la información un número determinado de veces; la computadora lee y analiza los movimientos dinámicos que se producen cuando la persona firma. Luego, un software especial censa los movimientos del bolígrafo y genera una plantilla con los datos más resultantes, que puede incluir la velocidad con que la persona firma, curvas, lazos y cambios de presión. Estas plantillas forman un perfil que es comparado con otro almacenado en una tarjeta de identificación del usuario o en una base de datos centralizado. Otros sistemas biométricos de reconocimientos de firmas usan bolígrafos con una punta magnética en un tablero sensible. Estos sistemas analizan solo los cambios dinámicos en la dirección de las x y las y, y como resultado el hardware requerido es mucho más simple. Como la firma se ingresa siempre una gran

cantidad de veces, el sistema “aprende” la mayor cantidad de consistencias y verifica las partes de la firma. Los datos que contiene la plantilla del usuario son almacenados en una base de datos o en una tarjeta inteligente. El reconocimiento de firmas ha obtenido recientemente avances en exactitud y en la maduración del producto. Dentro de sus principales ventajas se encuentran: Cada persona firma de única manera, el hardware para implementar un sistema de firma es bastante sencillo y los costos de implementación es poco. Su principal desventaja es: La firma de una persona puede variar de una ocasión a otra, por lo que el dispositivo puede no siempre reconocerla en un solo intento. Sin embargo, los últimos desarrollos en reconocimiento de firma han mejorado está tecnología a continuación le mostramos uno de estos dispositivo en la Figura 4.

Figura 4 dispositivos de reconocimiento de firma

1.1.5 Oculares.

El ojo humano tiene una serie de características que son propios de cada persona.

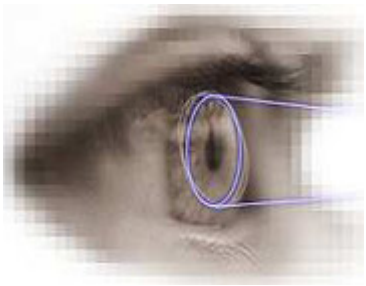

Figura 5 Ojo humano

El reconocimiento de iris es extremadamente eficiente. En términos de FAR, es más efectivo que el reconocimiento de huellas digitales. Los patrones de iris humanos son

estables en el tiempo, es protegido de daños por la cornea y tiene 6 veces mas características distinguibles que una huella digital. El iris no solo responde a la luz con una contracción automática, también responde de esta forma ante el estrés, drogas, etc. y sus principales ventajas son: El iris tiene más características únicas y es una técnica no intrusiva ya que el sujeto puede localizarse a una cómoda distancia del escáner y sus desventajas son: Los escáner del iris generan plantillas de 256 bytes lo que significa un costo dramático en dispositivo de memoria de la computadora y el escáner tiene un gran costo. A continuación la figura 5a. muestra el código del iris. [4].

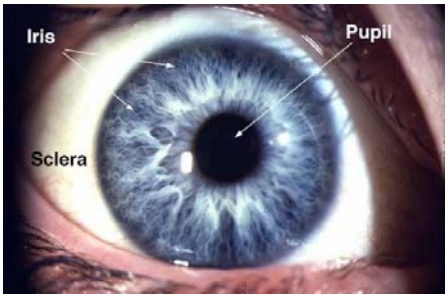

Figura 5a Código del iris

1.1.6 Reconocimiento de la retina.

La retina, se encuentra en la parte trasera del globo ocular, como se muestra en la Figura 6 y tiene patrones únicos de vasos sanguíneos. La recolección de los datos del usuario incluye el escaneo de la retina del usuario y el almacenamiento de las plantillas. Un dispositivo infrarrojo escanea la retina del usuario y la luz reflejada es colectada por una cámara especial. El escáner puede ser estacionario, en cuyo caso el usuario puede colocarse enfrente del mismo. Una vez que la retina es escaneada, un software especial crea un perfil digital del patrón del usuario el cual es único. Es tomado a partir de la disposición de los vasos sanguíneos en la retina. La imagen es procesada es reducida de 16 kbytes a 48 kbytes. El perfil es comparado con un perfil almacenado en una tarjeta de identificación del usuario o con la información en una base de datos central. La verificación puede tomar de 4 a 7 segundos.

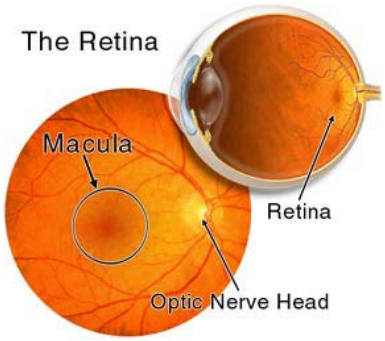

Figura 6 Patrones de la retina.

Sus principales ventajas: El tamaño de los perfiles es pequeño, el patrón de los vasos sanguíneos de una persona no cambian con el tiempo, excepto que la persona sufra de alguna enfermedad degenerativa y la verificación es rápida. Sus principales desventajas: Es una técnica intrusiva, ya que para obtener una medida es necesario que la persona coloque sus ojos a 2 o 3 pulgadas del escáner, donde esto representa un alto nivel de incomodidad para algunos, pocos proveedores poseen está tecnología y el sujeto debe cooperar con el lector.

1.1.7 Reconocimiento facial.

La variación en el enramado de vasos sanguíneos a través de la cara de un sujeto, crea una imagen termal única para cada quien, inclusive entre hermanos gemelos. Los termo gramas faciales no cambian durante la vida de una persona y no se ven afectados por cambios en la superficie de la cara, inclusive si se le practica una cirugía plástica, a menos que esta incluya el redireccionamiento del flujo sanguíneo. Las imágenes termográficas pueden ser obtenidas sin el contacto con el dispositivo que toma la imagen como se muestra en la Figura 7.

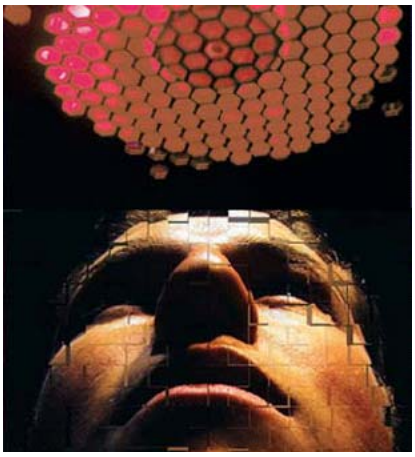

Figura 7 Reconocimiento facial.

Dentro de las principales ventajas se encuentran: No es un sistema intrusivo ya que el usuario no necesita introducir ni la mano ni sus dedos para ser escaneados, los datos son estables durante el tiempo de vida del usuario y un sujeto puede ser evaluado sin que este sepa que lo está siendo. Sus desventajas: Alto costo ya que los precio de una cámara infrarroja es muy alto y el tamaño de las plantillas es alto ya que puede oscilar entre 2000 y 3000 bytes, esto pude ser que haga que el sistema sea lento en el momento de realizar una búsqueda en grandes base de datos. Sin embargo con el desarrollo de las técnicas de compresión de video se resolverán estos problemas.

1.1.8 Venas.

Las venas del cuerpo humano presentan una distribución geométrica única para cada persona y que es invariable con el paso del tiempo. Su distribución aleatoria permite que un sensor similar al de una cámara de foto, capte mediante luz infrarroja las venas superficiales de la mano, como se observa en la figura 9, de manera que se obtiene un patrón exclusivo de cada individuo. Para medir la eficacia de este modelo biométrico, se ha probado el sistema en condiciones extremas, tanto de humedad con diferentes luces ambientales. De esta forma utilizando la información ofrecida por las venas de la mano, se a conseguido entre un 99,5 y un 99,8 por ciento de éxito, realizando la identificación de la

persona en solo dos segundos, donde se demuestra que no se produjeron resultados de "falsa aceptación", por lo que las probabilidades de que el sistema se equivoque frente a fraude es prácticamente nulas. En lo que respecta a la humedad, el sistema es más seguro que el de las huellas dactilares; mientras que en el caso de la luz ambiental, es necesario optimizar el escenario donde se ubicará el sensor, puesto que las imágenes se velan con altas concentraciones de luz solar. En general, las tasas de error son bajas y fluctúan entre el 0,5 y el 0,2 por ciento en la mayoría de los casos "el falso rechazo se produce fundamentalmente cuando las personas no colocan la mano correctamente en el sensor"

Figura 9 Lector de venas

1.1.9 ADN.

Es un campo de estudio actual. Este patrón, para que sea empleado masivamente, debe obtener un mayor desarrollo en los dispositivos usados en la captación y análisis de las muestras, lo que hoy no es posible aún. Limitada también por conceptos de aceptación popular, si el ADN se convierte en nuestra identidad entonces se estarán compartiendo, a nivel mundial. Resulta un método altamente complejo, caro e intrusivo.

1.1.10 Otros en estudio.

Actualmente en el mundo se continúa el estudio e investigación de novedosas técnicas de identificación biométrica como son:

- Actividad cerebral: es un sistema electrónico de seguridad que identifica las personas al monitorear el patrón único de la actividad del cerebro, este nuevo

sistema biométrico es difícil de falsificar, haciendo que sea adecuado para aplicaciones de máxima seguridad

- Radio frecuencia: Esta consiste en implantar un (chip) dentro del cuerpo humano que pueda contener un único número de identificación y otras informaciones sobre sus condiciones médicas esto solo se a utilizado en países muy desarrollados y se considera un dispositivo salva vidas.

- Temperatura corporal. Esta técnica se utiliza en la actualidad en los aeropuertos para controlar la entrada de personas que pueden estar infestada con virus, como el de la influenza A H1N1 colocando sensores que controlan la temperatura corporal.

- Olor. Los sensores de olor, aun en desarrollo, utilizan un proceso químico similar a el que se produce entre la nariz y el cerebro, sin que los perfumes sean capas de enmascarar el olor propio de cada individuo.

- Dinámica de pulsaciones del teclado. Esta técnica es utilizada solo en laboratorios donde se trabaja en computadoras por lo que no es de gran utilidad.

- Análisis del patrón de marcha**.** Esta técnica se utilizo en los juegos Olímpicos para detectar la presencia de intrusos en las áreas de competencia dando buenos resultados prácticos.

1.2 Conclusiones del capitulo.

En este capítulo se ha mostrado de una forma simple las principales técnicas biométricas mas utilizadas en la actualidad como están difundidas en cualquier rama de la ciencia; Medicina, protección de locales, seguridad de redes, protección de eventos deportivos, seguridad en los aeropuertos y para la transparencia de los comicios de algunos países.

.

CAPÍTULO 2. Descripción del escenario.

Introducción:

En el siguiente capitulo se realizará una descripción de cual es el método que se utiliza en nuestro escenario, sus principales característica y un resumen económico detallado de todos los materiales utilizados en el montaje del mismo.

2.1 Breve reseña.

El siguiente trabajo se desarrolla en una planta industrial militar donde existe un punto que acceden 60 usuarios aproximadamente en determinados horarios de la jornada de trabajo. Donde fue instalado un sistema de verificación y control del personal (lector de tarjetas de identificación personal) que tiene acceso a este recinto, por las características del trabajo que se realiza en esta área es necesario que estos se identifiquen de una forma segura, por lo que en la actualidad estos lo hacen mediante esta tarjeta personal. El lector se encuentra situado en la puerta de entrada de dicho taller esta tarjeta es introducida en el lector como se muestra en la Figura 10. La información que registra este es enviada a la PC del jefe de taller que es quien controla el personal que accede. Es responsable el personal de seguridad de que todo el que acceda a este lugar debe de ser registrado, tenga o no tarjeta de identificación personal. El personal de seguridad es cambiado constantemente, lo que hace que cualquier otra persona pueda acceder al taller si tiene la tarjeta de otro trabajador. Para la instalación de este sistema se utilizaron una serie de materiales: reloj 508 o controlador de acceso autónomo para puertas con función de control de asistencia y comunicación integrada (TCP-IP) y código de tarjetas, este reloj es el encargado de comunicarse con la PC a través de una dirección IP que es configurada por el usuario, transformador 110/ 16V 40VA este es utilizado para la alimentación del reloj, batería 12V 7A es utilizada para

emergencia, fuente auxiliar AI 624 de 6,12,24V 1.2A, cerradura tipo pulso eléctrico, un sensor magnético que es quien da la información que la puerta esta cerrada o abierta, UPS American Power BE 550 R 500VA,esta es utilizada para emergencia en la PC y para toda la alimentación del sistema de protección , lector de tarjeta de proximidad este es donde se introduce la tarjeta de identificación y un Switch Netgear de 5 puertos 10/100 Kbytes/seg. Por lo que se pueden emplear más sensores o lectores de tarjetas en alguna puerta de almacenes de materia prima o de producción terminada donde es mucho mas restringido el acceso de personas. [5]

Figura 10 lectores de tarjetas de identificación personal.

Figura 11 Tarjeta de identificación personal

Este tipo de identificación es muy difundida en todo el país pero tiene poca aceptación, por ejemplo: Es habitual la pérdida o sustracción de la misma, cualquier otra persona puede acceder a un recinto sin ser ella en realidad, pues no tiene ningún parámetro biométrico que identifique a el portador de está tarjeta, también es utilizada está identificación no solo para acceder, sino para el control del horario de trabajo que se realiza mediante una PC

donde todo es monitoreado para después ser procesado, esto tiene como limitante que cualquier personal que no tenga esta tarjeta y acceda a este lugar no es controlado, no existe evidencia de su entrada . [5]

2.1.1 Características del sistema.

Este tipo de identificación tiene como característica que cuando un trabajador comienza por primera vez, o algún visitante accede por este punto no puede ser procesado, dando lugar a no ser confiable el sistema, o sea que dicho control es solo para el personal que tenga este tipo de tarjeta y no para cualquier otro personal que acceda a este lugar.

Este servicio tiene un conjunto de accesorios para su funcionamiento que pueden ser utilizados por otros sistemas de identificación, que sea capas de controlar todo tipo de entrada de personas que accedan a este lugar que se base en un patrón biométrico [5]

2.2 Análisis del económico.

A continuación mostramos dos Tablas donde se muestra todos los materiales utilizados en el montaje de este sistema de acceso por medio de tarjetas. La Tabla 1 es la oferta que se realizo por primera ves en el control de acceso, pero no dio buenos resultados prácticos por lo que no se controlaba el horario de trabajo de los obreros, tan solo si accedió por el punto de control. Se hizo necesario que se implantara una tecnología que brindara más confiabilidad al sistema ya implantado. Donde en la tabla 2 se brindara una nueva oferta que controla el horario de trabajo y el acceso del personal que porta dicha tarjeta y se encuentre registrado como usuario. Es bueno resaltar que un mismo producto tiene diferentes precios por ser otros proveedores.

Partes y componentes	cant	Precio Unitario CUC	Importe CUC
Reloj C/Banda Mag C/adaptador	1	509.34	509.34
Trasformador 220/24Vac 40Va	1	10.62	10.62
Batería 12V 7A	2	19.21	38.43
Fuente Auxiliar 6,12,24 V 1.2A	1	14.21	14.21
Cerradura Electromagnética 24Vdc	1	93.15	93.15
UPS 500VA	1	117.00	117.00
Botón de Salida	1	57.98	57.98
Tarjeta Pvc de Proximidad P/Reloj Rta	60	1.57	93.98
		Total	934.70

Tabla 1 Listado de materiales utilizados en el montaje de las tarjetas personales sin el control del horario de trabajo.

Partes y componentes	cant	Precio Unitario CUC	Importe CUC
Clock 580 controlador de acceso autónomo con funciones de control de asistencia, comunicación integrada TCP/IP, con lector de huellas, códigos y tarjetas.	1	793.95	793.95
Trasformador 220/24Vac 40Va	1	10.21	10.21
Trasformador 110/16 V 40VA 1361	1	5.36	5.36
Batería 12V 7A	3	18.48	55.43
Fuente Auxiliar 6,12,24 V 1.2A	1	13.66	13.66
Cerradura tipo pulso eléctrico.	1	34.44	34.44
UPS 500VA	1	112.50	112.50
Botón de salida	1	52.35	52.35
Lector de tarjetas de proximidad.	2	257.50	515.00
Sensor magnético	1	3.93	3.93
Switch netgear 5 puertos 10/100	1	58.40	58.40
Tarjeta Pvc de Proximidad P/Reloj Rta	60	1.74	104.25
		Total	1759.07

Tabla 2 listados de materiales que incluyen una mejora al sistema.

En la realización de este análisis económico se tomo la segunda oferta que es la que esta instalada en dicha planta, el costo de materiales es de 1759.07 CUC, en este valor no se incluye el precio del software de gestión que oscila entre 800 y 1200 CUC ni el precio del montaje que fue de 243 CUC, para un monto que oscila entre 2802.07 y 3202.07 esta variación es debido a el software de gestión que no tiene un valor fijo. En todo este análisis no se tiene en cuenta el precio de la PC que ya se encontraba instalada en el local del jefe de taller es bueno resaltar que esta PC se encuentra instalada en red con todas las PC del complejo, por lo que cualquier funcionario puede también monitorear el acceso a dicha planta.

2.2.1 Concluciones del cápitulo.

En este capitulo se describe el método utilizado en esta área para el control de acceso del personal, está demostrado que la persona que no tenga o porte este tipo de tarjetas no es objeto de control por lo que no es seguro este sistema implantado, en el siguiente capitulo le proponemos otras técnicas de protección para acceder a lugares restringidos.

CAPÍTULO 3. Propuesta de implementación.

Introducción:

En el ámbito de las tecnologías de seguridad, uno de los problemas fundamentales a resolver es la necesidad de autentificarse de forma segura la identidad de una persona que pretende acceder a un determinado servicio o recinto físico, donde en nuestro caso se propone el cambio de las tarjetas por lectores de huellas digitales por su gran utilidad y aceptación.

3.1 Propuesta de implementación.

A continuación se propone el cambio de las tarjetas de identificación por lectores de huellas dactilares, por ser estas las de mayor uso en las técnicas de identificación biométrica en la actualidad y mayor aceptación, como se muestra en la Figura 11 y la Figura 11a, en estas Figuras se muestra como la huella dactilar es cada día mas aceptada en el ámbito de las tecnologías biométricas, se observa el aumento de el porcentaje de utilización de un 7 por ciento, con respecto a el año anterior. Es bueno resaltar que las huellas dactilares en nuestro país son tomadas a todas las personas mayores de edad para su carné de identificación personal, por lo que existe un registro, o base de datos para todas estas. Donde en caso de un intruso o una violación a está área puede aclararse por medio de los órganos del Ministerio del Interior. [6]

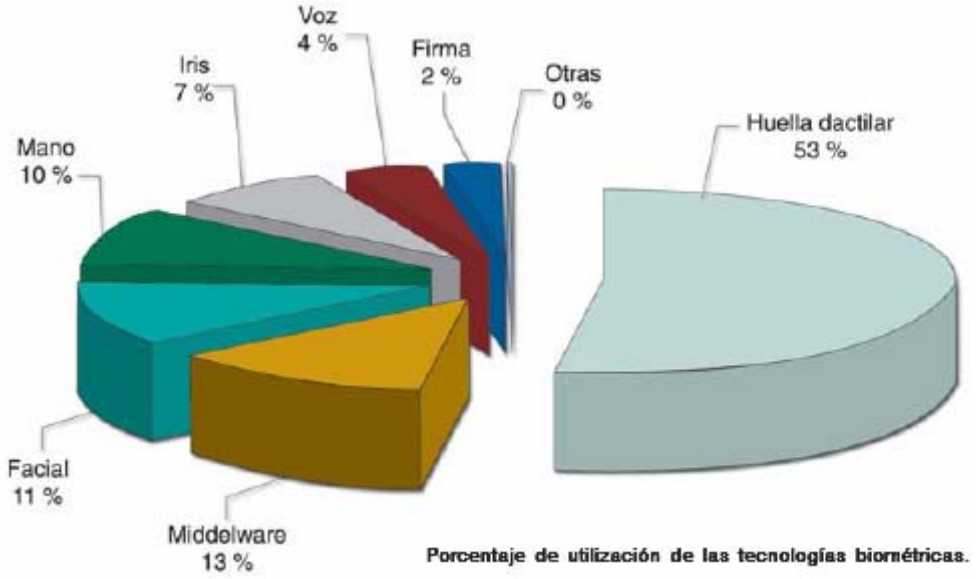

Figura 11 Porcentaje de utilización de las tecnologías biométricas (2008)

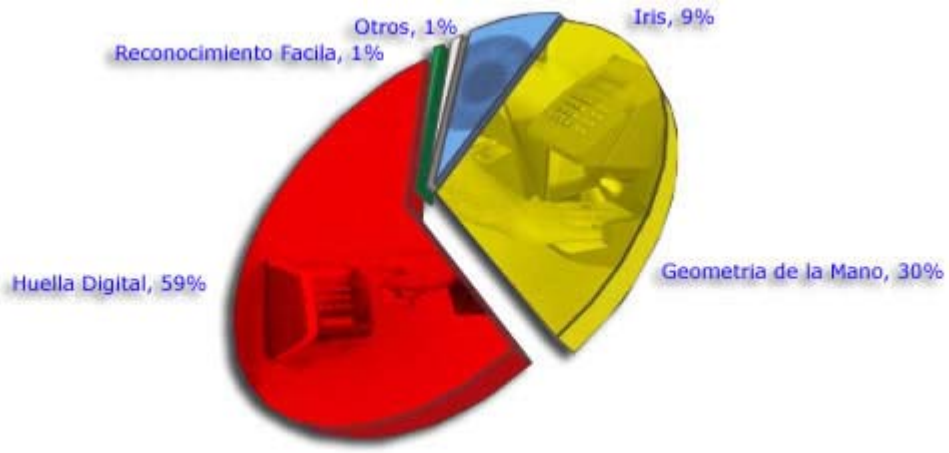

Figura 11a Porcentaje de utilización de las tecnologías biométrica.(2009)

En el caso de la huella dactilar se debe tener en cuenta que lo que es tomado por el lector no es la imagen de la huella sino una secuencia de números que la representan. Sus aplicaciones abarcan un gran número de sectores: desde el acceso seguro a computadora, redes, protección a ficheros electrónicos, el control de horario y el acceso a instalaciones de alto riesgo o alta seguridad como nuestro escenario. A continuación en la Figura 12 mostramos un ejemplo de una huella dactilar, esta formada por una serie de surcos. Sus terminaciones o bifurcaciones son llamados puntos de minucia, cada uno de estos puntos tiene una característica y una posición única que puede ser medida. Comparando esta distribución es posible obtener la identidad de una persona que intente acceder a un sistema en general. [7]

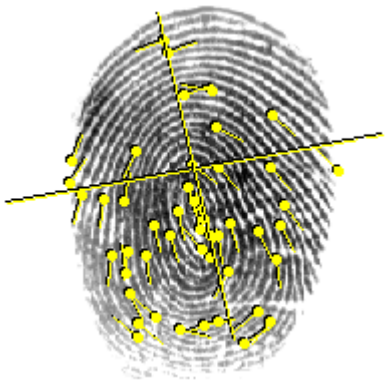

Figura 12 Huella dactilar

3.1.1 Principales caracteristicas de los lectores de huellas dactilares.

A continuación mostramos algunas características de los lectores para el acceso a una red o a una PC. [8]

1 Cambio rápido de usuario: Usando Windows XP usted puede cambiar de cuenta de usuario sin tener que cerrar una de las cuentas. Con solo apoyar su dedo, usted puede cambiar rápidamente sin cerrar documentos o programas y cada contenido personal.

2 Asistente de registración: cuando usted visita un sitio que requiere passwords por primera vez, el asistente se ejecuta. Usted tendrá que apoyar su dedo, teclear la información, y luego OK, esta será la última vez que necesitará hacerlo. Ahora usted podrá navegar por la Web y registrarse en sitios con sólo apoyar su dedo.

- Longitud del cable: 1.5 metros.
- Interfaz: USB.
- Windows XP horne, profesional, tablet PC, o media Center Edition con una Pentium 233MHz o procesador mayor, y 128 MB de RAM
- 45MB de espacio disponible para el disco duro.
- Un puerto USB (Universal Serial Bus) disponible.
- Drive para CD-ROM.

Figura 12 lectores de huellas dactilares

3.2 Análisis económico.

Si se realiza una comparación entre el precio de los lectores de huellas dactilares y el del lector de tarjetas de identificación, es obvio que el lector de huellas es mucho menos costoso que el de las tarjetas. Estas pueden perderse y deteriorarse con el paso del tiempo. En la Tabla 3 se hará referencia al precio de estos tipos de identificación.

Descripción	Cantidad	Precio unitario	Precio total
Lector de tarjetas de huellas dactilares SR20E	2	257.50	515.00
Tarjetas de identificación personal	60	1.74	104.25
Lector de huellas dactilares MA500	1	184.70	184.70
Lector de huellas dactilares MA520	1	235.60	235.60

Tabla 3 precio de los sistemas de identificación.

.

3.3 Consideraciones técnicas.

Para la implantación de los lectores de huellas dactilares es necesario tener en consideración algunos materiales que ya se encuentran instalados en el sistema de tarjetas personales como son: controlador de acceso para puertas con función de asistencia, comunicación integrada TCP/IP con lector de huellas, trasformador 110/16V para el reloj, cerradura tipo pulso eléctrico, tres UPS 500VA para garantizar la confiabilidad del sistema auque es bueno resaltar que esta planta presenta un grupo electrógeno de emergencia, switch 5 puertos 10/100, para garantizar la comunicación de la PC con todo el complejo industrial. La distancia que existe de la puerta de entrada del área es relativamente pequeña, por lo que la instalación de un lector de huellas dactilares por USB

si es posible en la Figura 13 y 13a se muestran otros lectores de huellas dactilares de la serie MA 500/520 que son de gran utilidad actualmente. [9]

Figura 13 Lector serie MA 500.

Figura 13a lector serie MA 520.

El lector MA 500 se puede instalar a el reloj 580 utilizado en la instalación de las tarjetas de identificación personal por tener conexión integrada TCP/IP y el puerto RS 232 y el swith netgear 5 puertos 10/10 el lector MA 520 presenta las mismas características de instalación solo se incluye un mando que puede estar fuera de la base para su manejo y esto es mas confortable que su compañero. [10].

.

3.4 Conclusiones del capitulo

Dada la importancia de autentificarse de una forma segura a estas áreas restringidas y la probabilidad de la perdida o sustracción de las tarjetas de identificación se propone la implantación de lectores de huellas dactilares (MA500 o el MA520) donde queda a consideración del cliente cual de estos modelos se empleará.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Dentro de las principales conclusiones de nuestro trabajo es que los lectores de huellas dactilares son de mayor utilización en el mundo de las tecnologías de seguridad, por ser un patrón biométrico que no tiene variación, tampoco es una técnica intrusiva y el usuario puede fácilmente acceder sin tener que portar ningún tipo de documento que pueda ser usado por otra persona, la empresa puede tener un control certero de sus trabajadores y de cualquier otro personal que acceda a el mismo. Es bueno resaltar que en la actualidad ya existen PC que traen lectores para acceder más fácilmente a las cuentas de usuarios que también pueden ser empleadas en el control de acceso a determinado recinto. Las técnicas biométricas tienen ventajas con relación a las empleadas tradicionalmente para acceder a lugares restringidos:

- Son muy amistosas con los usuarios, no es necesario portar ningún documento, solo vasta con su presencia.
- Estas técnicas se basan solo en las características propias de los usuarios.
- Alta confiabilidad.
- Tienen un tiempo relativamente corto para autentificar, bajo costo de fabricación.
- Con el paso destiempo se convertirán en la llave del futuro.

Recomendaciones

Por ser las técnicas de identificación biométricas las tecnologías de mayor seguridad para acceder a determinado lugar se recomienda:

1 Utilizar los lectores de huellas dactilares para el acceso y control del personar que acceda a nuestro escenario.

2 Tratar de que esta técnica sea empleada en todos los talleres que tengan un acceso limitado.

REFERENCIAS BIBLIOGRÁFICAS

- [1] www.biometriaplicada.com "Sistemas de Seguridad". {En Línea} Disponible en: http [visitado] abril 2009
- [2] www.xataka.com "Lectores por USB". {En Línea} disponible: Sistemas Biométricos. http [visitado] mayo 2009.
- [3] www.cubasi.cu "Huellas dactilares". {En Línea} Disponible en: Portal Cubasi ETECSA html [visitado] mayo 2009.
- [4] www.mercadopc.com "características técnicas". {En Línea} Disponible en: http Mercado PC [visitado] junio 2009.
- [5] www.todoar.com "Tarjetas da identificación". {En Línea} Disponible en: http [visitado] abril 2009
- [6] www.ibix.com.mx "Porcentaje de utilización". {En Línea} disponible: Sistemas Biométricos. http [visitado] marzo 2009.
- [7] www.homini.com "Huellas dactilares". {En Línea} disponible en :Plataforma Geométrica Homini http [visitado] abril 2009
- [8] www.biometricsolution.com "características". {En Línea} Disponible en: Technology html. [visitado] junio 2009.
- [9] www.biometricsolution.com "características". {En Línea} Disponible en: Technology html. [visitado] junio 2009.
- [10] www.biometricsolution.com "características". {En Línea} Disponible en: Technology html. [visitado] junio 2009.