SOLUCIONES INTELIGENTES PARA EL CONTROL DE ACCESO FÍSICO MEDIANTE EL USO DE TECNOLOGÍA BIOMÉTRICA

JORGE EDUARDO VELASQUEZ VALENCIA

ALVARO ANDRES LINARES JARAMILLO

UNIVERSIDAD TECNOLOGICA DE PEREIRA

FACULTAD DE SISTEMAS

INGENIERIA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2013

SOLUCIONES INTELIGENTES PARA EL CONTROL DE ACCESO FÍSICO MEDIANTE EL USO DE TECNOLOGÍA BIOMÉTRICA

JORGE EDUARDO VELASQUEZ VALENCIA

ALVARO ANDRES LINARES JARAMILLO

CARLOS AUGUSTO MENESES

PROFESOR

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE SISTEMAS

INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA

2013

Contenido

1. TITULO

Soluciones inteligentes para el control de acceso físico mediante el uso de tecnología biométrica

2. RESUMEN

En este proyecto se realizó un estudio exhaustivo sobre la biometría, especialmente sobre los métodos de identificación existentes que utilizan diferentes características biométricas que los seres humanos poseemos y sobre las técnicas que cada método utiliza para la identificación de un usuario, adicionalmente se investigó sobre los dispositivos más comunes en el mercado, y sus características técnicas, como lo son la cantidad de usuarios que se pueden almacenar, la precisión, entre otras. También se investigó el estado actual del arte en este ámbito, así como algunos adelantos tecnológicos en dispositivos y técnicas de autenticación, verificación y reconocimiento de personas mediante esta tecnología.

El aporte principal está basado en el análisis de los diferentes dispositivos biométricos y la forma en que utilizando tecnologías como lo son los dispositivos programables (FPGA's, sistemas embebidos, entre otros) se puede obtener una solución óptima para controlar el acceso a una residencia. De igual manera a través de la recolección de información de los diferentes dispositivos se pudo realizar un cuadro comparativo demostrando las ventajas y desventajas de cada dispositivo en cuanto a desempeño, costo, velocidad y confiabilidad. Es así como finalmente se puede tener una recomendación óptima para este ambiente implementando este sistema de seguridad

3. FORMULACION DEL PROBLEMA

La seguridad ha sido una necesidad para el ser humano desde siempre, pero hoy en día, debido a situaciones como la pobreza, el aumento de la delincuencia común y otras, hace que las personas, hoy en día le presten más atención a sus seres queridos y a sus bienes materiales, buscando formas de solución como las cerraduras convencionales para evitar el ingreso de extraños a sus residencias y evitar así la posterior pérdida de sus artículos.

En la actualidad la evolución constante de la tecnología, hace que las personas adquieran dispositivos tecnológicos como televisores, dispositivos móviles y computadores de forma muy accesible, haciendo de sus hogares un sitio más cómodo y entretenido, convirtiéndolos en lugares atractivos por sus bienes contenidos donde si no existen las medidas necesarias para contrarrestar un ingreso no autorizado, se vuelven vulnerables para que ladrones puedan ingresar en el momento de ausencia de los dueños principalmente en horarios laborales.

Algunos factores que también pueden ayudar a que las residencias sean saqueadas son:

- Ubicación de la residencia lejana del perímetro urbano o con poca circulación de personas a su alrededor.
- Pocas medidas de seguridad para controlar el acceso a la vivienda.
- Falta de monitorización o ausencia de autoridad en la localidad.

Algunas de las modalidades que usan los delincuentes para entrar o irrumpir físicamente en los sitios y hurtar objetos de valor son las siguientes [1]:

- Modalidad De Violación de cerraduras: Los delincuentes fuerzan las cerraduras por medio de objetos contundentes o equipos especializados

para ingresar de forma ilícita al interior de los lugares y así extraer los elementos de valor que se encuentren.

- Modalidad de llaves maestras: Los delincuentes con buen entrenamiento en el funcionamiento de cerraduras (algunos casos cerrajeros que deciden delinquir) diseñan llaves especiales con el cual pueden acceder a los lugares a través de puertas y/o ventanas ofreciendo un acceso inmediato al interior del inmueble.

- Modalidad de hurto por ventosa: consiste en perforar, abrir o dañar puertas, ventanas o paredes, para acceder al interior del lugar.

- Modalidad de hurto por descuido: esta proporcionada básicamente por el descuido de las personas en la aplicación de las medidas básicas de seguridad, así los ladrones aprovechan al ver alguna entrada abierta y es en este instante donde aprovechan para hurtar los objetos de valor.

Una encuesta de convivencia y seguridad ciudadana realizada entre julio y agosto del año 2012 por el DANE revela las siguientes tasas de hurto a residencias por modalidad [2]:

- Violación por cerradura, Ventosa: 30.5%
- Otro: 29.3%
- Uso de fuerza, Amenaza: 25.5%
- Llamada millonaria, engaño: 7.8%
- No informa: 5%
- Uso de drogas para someter a los residentes: 1.8%.

El total de hogares encuestados en las 25 diferentes ciudades de Colombia, es de 5’983.000 de las cuales 212.000 hogares fueron robados o tuvieron algún percance con este tipo de delincuencia.

Con estas cifras se puede determinar que más de 200.000 hogares sufren anualmente las consecuencias del hurto, demostrando que existe una gran inseguridad o que los hogares son lo suficientemente vulnerables por carecer de medidas estrictas de seguridad para contrarrestar el robo

Lo anterior plantea el siguiente interrogante:

¿Será posible crear un documento que sirva de referencia a las personas para determinar o elegir adecuadamente las tecnologías o técnicas con las cuales se puedan controlar los diferentes accesos a una residencia?

4. JUSTIFICACION

Los dispositivos biométricos son equipos de cómputo desarrollados para reconocer rasgos corporales únicos de cada individuo, como los son las huellas dactilares, distribución las papilas gustativas, formas de manos, entre otras, ofreciendo una, por llamarla así llave genética, que permite la autenticación sin la necesidad de utilizar algún objeto o clave.

Los objetos más utilizados para el ingreso a residencias y a correos electrónicos en la actualidad son las llaves o un ***pin*** (por sus siglas en ingles Personal Identification Number), que no ofrecen la seguridad necesaria para el acceso. Este proyecto buscara ofrecer la información necesaria sobre estos dispositivos para su utilización en hogares o para aquellos que pretendan construir sistemas de seguridad contra el ingreso de personas y que a su vez permitirá conocer ventajas, desventajas, modo de utilización contra las diferentes formas de ingreso de personas no deseadas a la vivienda, además de informar sobre modelos de seguridad que utilizan varios dispositivos y sobre cómo utilizar estos modelos, y que valor agregado ofrece.

Al existir una gran cantidad de dispositivos electrónicos con los cuales se pueden realizar muchas aplicaciones, que permiten automatizar muchas de las actividades cotidianas que se presentan hoy en día, tales como las comunicaciones, monitorización de lugares a través de cámaras, llevar sistemas de información que facilitan el almacenamiento de datos, entre otros, y que combinando estas tecnologías se podría crear un sistema de seguridad el cual restringiría el acceso a un sitio determinado con mejores controles tales como el horario de ingreso de una forma más confiable.

Este proyecto se justifica socialmente pues el documento que se pretende obtener sirve de referencia para determinar o elegir adecuadamente las tecnologías que permitan controlar los diferentes accesos a una residencia, de igual manera se pretende que con el análisis obtenido se pueda usar o tomar una decisión en cuanto a la relación costo/beneficio, al qué y porqué usar determinado dispositivo para implementar un sistema de seguridad.

Para los usuarios de sistemas de seguridad, el hecho de tener mejores y nuevas alternativas, los beneficia por aumentar la garantía de tener un mejor nivel de protección tanto a su integridad como a sus bienes

5. OBJETIVOS

5.1. OBJETIVO GENERAL

Crear un documento que permita conocer posibles soluciones inteligentes para el control de acceso físico utilizando dispositivos de tecnología biométrica.

5.2. OBJETIVOS ESPECIFICOS

- Recopilar y levantar información pertinente acerca del estado del arte en cuanto a biometría y seguridad.
- Analizar diferentes dispositivos electrónicos programables.
- Analizar diferentes dispositivos biométricos.
- Analizar diferentes mecanismos de saqueo y hurto en las residencias.
- Crear un cuadro comparativo entre los dispositivos analizados.
- Estudiar las mejores combinaciones entre los dispositivos programables y biométricos.

CAPITULO II

6. ESTADO DEL ARTE

6.1 MARCO DE ANTECEDENTES

La tecnología biométrica consiste en el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o rasgos físicos intrínsecos del individuo, Y este es un desarrollo muy importante, el cual está siendo utilizado regularmente a nivel mundial. Cabe destacar que desde hace mucho tiempo la humanidad ha buscado los mecanismos para poder identificar a cada ser humano como alguien único, y tratar de hacerlo con la mayor exactitud posible y es en este instante donde utilizando las técnicas de biometría se ha podido llegar hasta un punto en el que es posible realizarlo.

La inclusión de estas técnicas biométricas para controlar el acceso físico a cualquier inmueble o utilización de un servicio es indispensable hoy en día, pues cotidianamente se presentan hurtos, ingresos no deseados o uso no autorizado de los recursos que se encuentran en un área designada o de confianza, la cual puede almacenar objetos o información valiosa para un individuo o empresa. Mediante estas técnicas biométricas es posible determinar la identificación de un individuo y asegurar que se trata de este, que no se están haciendo suplantaciones, es así como al implementar lectores de huellas digitales en cerraduras se puede restringir el acceso a cualquier persona diferente de los dueños del inmueble y la gran ventaja con esta tecnología es que no es necesario cargar llaves, tarjetas o algún otro mecanismo con el que se pueda abrir la cerradura, y que a su vez pueda ser extraviado y aprovechando esta situación extraer los objetos de valor del inmueble.

Estas tecnologías están siendo aplicadas en los bancos, los cuales desean incrementar la seguridad de sus cajeros y así poner en marcha un servicio mucho más óptimo para los clientes.
Los últimos datos del sector bancario a nivel mundial apuntan que un 70% de los bancos negocia proyectos para poner en marcha cajeros más seguros.[3]

Actualmente se utilizan otros medios de restringir accesos por medio de sistemas digitales tales como tarjetas electromagnéticas, que son manejadas en casas o edificios inteligentes, tal como el edificio de UNE en Pereira (Risaralda) sin embargo si algún empleado extravía dichas tarjetas existirían riesgos de seguridad que amenazarían la estabilidad del inmueble.

Con el surgimiento de la telefonía móvil, muchas personas empiezan a depender de este servicio, principalmente por motivos laborales y por la demanda que se está produciendo ya que cada vez es de más fácil acceso y económico obtener este servicio, es así como siempre estas tecnologías permanecen en constate evolución ya que demandan constantes esfuerzos investigativos que son necesitados para mejorar todos estas actividades y técnicas que deben satisfacer la creciente cantidad de usuarios que lo usan de forma cotidiana ya sea para facilitar sus labores o por simple comunicación.

La gran acogida de la tecnología móvil hace que surjan empresas las cuales se dedican a desarrollar y ofrecer servicios diferentes y de mejor calidad en sus dispositivos, aprovechando y renovando tecnologías ya existentes, ideando siempre nuevas estrategias de ventas para poder abrirse campo y/o mantenerse en este gran mercado tecnológico.

En la actualidad existen gran variedad de aplicaciones para suplir diferentes tipos de necesidades, entretenimiento, información, seguridad, comunicación, son algunos ejemplos de esto; las aplicaciones son cada vez más dinámicas, con

mejores gráficas y en donde su velocidad de procesamiento es mucho mayor, gracias a la utilización de dispositivos de alto desempeño.

Con los dispositivos móviles se están desarrollando cotidianamente aplicaciones que ayudan a los usuarios a tener acceso rápido a cuentas de correo, o datos confidenciales que pueden ser utilizados en las labores que día a día estos tengan, así es posible poder monitorizar en tiempo real cualquier sistema.

Actualmente se utilizan cámaras IP las cuales pueden ser empleadas para monitorizar a través de internet lo que sucede en un sitio así no se encuentre presencialmente o cerca, informando concretamente lo que ocurre en cualquier momento. [4]

6.2 MARCO TEORICO

6.2.1 Funcionamiento De Los Dispositivos Biométricos

La mayoría de los sistemas biométricos funcionan con arreglo a un modelo general que consiste en dos pasos. El primer paso es el registro de la persona en el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada modelo de referencia.
De acuerdo con la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona. En el caso de verificación, la persona le informa al sistema cuál es su identidad, ya sea presentando una tarjeta de identificación o introduciendo alguna clave especial. Se captura el rasgo biométrico y se compara con el modelo de referencia de la persona. Si ambos modelos coinciden, la verificación se realizó con éxito, si no es fallida.

En caso de que sea identificación, la persona no le informa al sistema biométrico cuál es su identidad. El sistema tan sólo captura el rasgo biométrico y lo compara con un conjunto de modelos de referencia para determinar la identidad de la persona. Los siguientes conceptos son tomados de [5]

6.2.2 Tecnologías biométricas

Existe una gran variedad de tecnologías biométricas, tantas como características biométricas. Muchas de ellas se están aplicando en la vida real y otras están en proceso de estudio. Algunas características biométricas que se utilizan actualmente son: voz, huellas dactilares, cara, iris, retina, venas de la mano, forma de la mano, forma de la oreja, forma de andar, forma de escribir en un teclado, firma, ADN y olor. Partiendo de estas características se han desarrollado dispositivos que han tenido mayor o menor éxito en el mercado. En la actualidad, los sistemas comerciales más usados son:

6.2.3 Reconocimiento facial

Estos sistemas extraen los rasgos faciales de los usuarios para su identificación. La fuente para realizar la identificación puede ser tanto imágenes fotográficas como de vídeo. La identificación se puede hacer en 2D, 3D o una combinación de ambas. El objetivo de un sistema de reconocimiento facial es, generalmente, el siguiente: dada una imagen de una cara «desconocida», o imagen de test, encontrar una imagen de la misma cara en un conjunto de imágenes «conocidas», o imágenes de entrenamiento. La gran dificultad añadida es la de conseguir que este proceso se pueda realizar en tiempo real.

6.2.4 Lector de impresión digital

Esta tecnología se basa en identificar al individuo por medio de su huella dactilar. Aunque puede utilizarse cualquier dedo de la mano, por una cuestión de dimensión y comodidad, los dedos más utilizados son el índice y el corazón. Su funcionamiento se basa en tomar una imagen de la huella y por medio de algoritmos reducir dicha imagen a una representación matemática de la huella ("plantilla"). Esta plantilla patrón se acumula en la memoria interna del equipo (junto con un número de identificación o PIN si se trata de un verificador, a fin de tener asociada la huella al individuo).

Luego, cada vez que la persona necesite identificarse, ya sea para registrar su horario de ingreso o regreso al trabajo o activar una puerta o barrera, debe digitar su PIN (en el caso que sea un verificador) y a continuación colocar su dedo (el mismo que registró originalmente) en el lector.

6.2.5 Reconocimiento de manos

El reconocimiento de la mano se puede hacer en dos y tres dimensiones. Los sistemas de dos dimensiones buscan en la palma de la mano patrones en las líneas, estos patrones son casi tan distintivos como las huellas digitales. El sistema toma entonces las características de la palma, los compara contra el modelo de referencia, y procede en consecuencia.

Los lectores de tres dimensiones, sin embargo funcionan de forma distinta. Estos miden las dimensiones de la mano (largo de los dedos, altura de la mano, etc.). Aunque no es la más segura de las técnicas biométricas, el uso de la palma de la mano como medida de autenticación ha resultado ser una solución ideal para aplicaciones de seguridad media y donde la conveniencia es considerada una opción mucho más importante que la seguridad o la precisión.

6.2.6 Sistema de autentificación biométrica de las venas

Es un sistema que captura la distribución de las venas de la palma de la mano o de los dedos. Está siendo muy utilizada en la actualidad debido a su fácil implementación y gran aceptabilidad por parte de los usuarios ya que muchos de ellos no requieren de contacto físico.

6.2.7 Sistema de identificación mediante el iris

La identificación basada en el reconocimiento de iris es más moderna que la basada en patrones retínales; desde hace unos años el iris humano se viene utilizando para la autenticación de usuarios.

Se captura una imagen del iris en blanco y negro, en un entorno correctamente iluminado, usando una cámara de alta resolución.

Generalmente esto se hace mirando a través de la lente de una cámara fija, la persona simplemente se coloca frente a la cámara y el sistema automáticamente localiza los ojos, los enfoca y captura la imagen del iris, ésta imagen se somete a deformaciones pupilares (el tamaño de la pupila varía enormemente en función de factores externos, como la luz) y de ella se extraen patrones, que a su vez son sometidos a transformaciones matemáticas hasta obtener una cantidad de datos suficiente para los propósitos de autenticación.

El iris humano (el anillo que rodea la pupila, que a simple vista diferencia el color de ojos de cada persona) es igual que la vasculatura retinal, una estructura única por individuo que forma un sistema muy complejo (de hasta 266 grados de libertad) e inalterable durante toda la vida de la persona.

El uso por parte de un atacante de órganos replicados o simulados para conseguir una falsa aceptación es casi imposible con análisis infrarrojo, capaz de detectar con una alta probabilidad si el iris es natural o no.

6.2.8 Sistema de reconocimiento mediante de la vasculatura retinal

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

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

En ese momento se escanea la retina con una radiación infrarroja de baja intensidad en forma de espiral, detectando los nodos y ramas del área retinal para compararlos con los almacenados en una base de datos; si la muestra coincide con la almacenada para el usuario que el individuo dice ser, se permite el acceso.

6.2.9 Sistema de reconocimiento de firmas

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

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

6.2.10 Sistema de Reconocimiento de voz

La voz es otra característica que las personas utilizan comúnmente para identificar a los demás.

Es posible detectar patrones en el espectro de la frecuencia de voz de una persona que son casi tan distintivos como las huellas dactilares. Tan solo basta recordar las veces en que se reconoce a alguien conocido por teléfono para comprender la riqueza de esta característica como método de reconocimiento.

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

6.3 MARCO REFERENCIAL

6.3.1 RECONOCIMIENTO BIOMÉTRICO

El reconocimiento biométrico responde a un sistema automático basado en la inteligencia artificial y el reconocimiento de patrones, que permite la identificación y/o verificación de la identidad de personas a partir de características morfológicas o de comportamiento, propias y únicas del individuo, conocidas como autentificadores. [6]

Asimismo, la naturaleza del tipo de característica, morfológica o de comportamiento, se encuentra directamente relacionada con el grado de variación de las mismas con el paso del tiempo, siendo mucho más inferior en el primer caso que en segundo, ya que como sabemos, el comportamiento está íntimamente relacionado con factores psicológicos y éstos sí que son función directa del tiempo.

Este tipo de reconocimiento se ha convertido en una herramienta habitual en las fuerzas de la policía durante los procesos de investigación criminal, posibilitando la detención de delincuentes a nivel mundial, aunque también se le reconocen otras aplicaciones específicas tales como el control de acceso a cualquier tipo de transacción o acceso a datos protegidos.

La biometría es una de las formas más eficaces para trabajar en seguridad, ya que un individuo cuenta con rasgos únicos que lo hacen diferente a cualquier otra persona, de esta manera se pueden utilizar dichas características para brindar el acceso a un recinto, donde solo esta persona pueda tener acceso, y que de igual manera, así se puede solucionar el problema de extraviar llaves o tarjetas las cuales son usadas para poder ingresar a un sitio o utilizar algún determinado servicio como transacciones financieras.

Los beneficios que trae consigo la tecnología biométrica es el incremento de la protección de identidad, la disminución de los riesgos de privacidad, la protección de derechos civiles y a la libertad civil, es por eso que en un mundo donde la tecnología avanza rápida y constantemente, la solución a esto requiere el desarrollo de sistemas complejos y robustos.

Cada día agencias gubernamentales, entidades, residencias y instituciones académicas confían más en la tecnología biométrica gracias a sus sistemas de seguridad que utilizan características morfológicas de cada individuo, contribuyendo así al no uso de dispositivos como lo son las tarjetas de crédito, que son uno de los blancos principales para criminales de todo tipo.

En la actualidad el reto más difícil de la tecnología biométrica es adaptarse a la rápida evolución del ambiente criminal, donde los investigadores prestan más atención al rango en donde los dispositivos biométricos pueden actuar y buscar soluciones para este espacio. [7]

6.3.2 GENERACION DE LLAVES BIOMETRICAS

La biometría moderna está definida como la ciencia que utiliza rasgos genéticos como las huellas dactilares, rostros, voz, entre otras, mejorando el nivel de seguridad de bienes y recintos residenciales, gubernamentales y públicos.

Para diseñar y desplegar un sistema de autenticación biométrico, se debe conocer las fallas, que pueden estimar una mayor debilidad de la seguridad y amenazas a la privacidad. Es por eso que surge la necesidad de crear una generación de llaves genéticas seguras ayudadas mediante un dispositivo biométrico.

Una generación de llave biométrica segura es un proceso el cual convierte un rasgo biométrico en cadena de bits (llave) utilizando además información auxiliar, esto se conoce como un ayudante biométrico. Un ayudante biométrico es una plantilla biométrica registrada y almacenada en un dispositivo local que puede ser eliminada cuando se requiera. Durante la autenticación se usa el ayudante biométrico junto con una petición de un dato biométrico para generar una llave. Por lo tanto, la llave biométrica es utilizada por ambos usuarios de la autenticación (usuario, sistema) y como una llave criptográfica, para aplicaciones de esta índole.

La generación de llaves biométricas debe cumplir a cabalidad los siguientes requerimientos:

Estabilidad de la llave: La llave deberá estar disponible para ser reproducida constantemente, respetando las variaciones entre clases.

Diversidad/Revocabilidad de la llave: La llave debe ser distinguida por diferentes aplicaciones y debe ser de fácil revocación sin afectar otras llaves.

Seguridad: El ayudante biométrico está comprometido, la entropía del dato biométrico y la llave asociada deben ser suficientemente altas. En otras palabras, el ayudante no revelará o mostrará mínima información solicitada del dato biométrico o llave. [8]

Una aplicación para identificación y generación de llaves se implementa en sistemas biométricos con plantillas protegidas. Al investigar dos terminales observando la inscripción y la identificación de secuencias de grupos de caracteres. El primer terminal crea una llave secreta con cada inscripción de caracteres y su posterior almacenamiento de su ayudante biométrico en una base de datos pública. Este ayudante permite a los datos facilitar una reconstrucción confiable de la llave secreta y por otro lado permite la determinación de las identidades de caracteres para la segunda terminal. Todos los ayudantes en la

base de datos se asumen públicos. Desde los secretos biométricos producidos por el primer terminal que han sido o están siendo usados, por ejemplo para el encrespamiento de datos, el ayudante debe proveer información en esas llaves secretas. Se determinó que la identificación y los rangos de las llaves secretas pueden ser realizadas conjuntamente por el sistema de identificación biométrico. [9]

Los datos biométricos usados en la identificación de sistemas, son principalmente usados en el control de acceso y aplicaciones de autenticación. Aparentemente es un comercio entre llaves secretas y rangos de identificación.

6.3.3 UN ESTUDIO EXHAUSTIVO DE VARIAS TÉCNICAS DE IDENTIFICACIÓN BIOMÉTRICA [10]

La sociedad electrónica de hoy ha hecho que cualquier individuo de algo mucho más grande globalmente, dando como resultado la necesidad de obtener sistemas de seguridad especializados y eficaces para el reconocimiento de personas.

La forma tradicional de usar tanto como password o alguna tarjeta no es ya lo suficientemente confiable para un sistema de seguridad. Esto lleva a la necesidad de desarrollar un sistema de identificación personal como solución a la problemática anterior usando información biométrica. Gracias a la información biométrica se puede tener acceso a un sistema de seguridad sin el riesgo de accesos a extraños ya que la identificación de los individuos es completamente segura pues dicha información no puede ser compartida o confundida.

Varios de los tipos de reconocimiento Biométrico son:

- **Reconocimiento Facial:** Donde gracias a una cámara es posible detectar la identidad de un individuo y autenticarlo ya sea por técnicas como la función de acercamiento, la cual consiste en reconocer puntos estratégicos de la locación de varias partes de la cara, como los ojos, nariz y boca, con dicha información se puede hacer un análisis de las relaciones geométricas en dichas áreas del individuo y así identificarlo.

  Un sistema de reconocimiento facial es una aplicación de cómputo para identificar o verificar automáticamente una persona desde una imagen digitalizada o de un marco de video desde una fuente proporcionada, tal como una cámara. [11]

  Un gran número de aplicaciones comerciales, de defensa o de seguridad demandan sistemas de reconocimiento facial en tiempo real, donde otras técnicas de biometría no son aplicables

- **Reconocimiento de Huellas digitales:** Esta técnica es el método más viejo en autenticación de identidad y ha sido usada desde 1896 y ha sido ampliamente usada en la identificación de criminales. Cada sujeto o individuo posee un patrón único de huellas y para el reconocimiento usualmente se analiza la información geométrica que se produce entre los patrones de la huella.
- **Geometría de la mano:** La imagen es obtenida a través de una cámara que se debe poner encima de la mano en una superficie específica, donde la mano puede ser alineada utilizando marcas de referencia para lograrlo. Normalmente se toman dos imágenes, una superior y una lateral, donde se analiza geométricamente la curvatura de los dedos o en ciertas áreas de la mano, sin embargo aunque esta técnica tiene una precisión aceptable no es lo suficientemente precisa para la identificación.
- **Reconocimiento de Iris:** La imagen del iris es captada usualmente por una cámara monocromática con una luz infrarroja, y lo que se hace es analizar

las imágenes a través de un filtro y esto es traducido a una información numérica a través de un algoritmo creado por el prof. John Daugman. Esta información es bastante precisa y difícil de replicar y puede ser usada tanto para verificación como para identificación de un individuo. Negativamente esta técnica necesita que el sujeto permanezca inmóvil mientras se hace la imagen, y no es recomendada para personas con cataratas y pequeños niños.

Recientemente, las técnicas de identificación que utilizan Biometría han atraído gran atención debido a la demanda de sistemas de seguridad cada vez más especializados y de mejor desempeño. [12]
Las técnicas de identificación biométrica proveen soluciones mucho más confiables y robustas comparadas con los modelos y técnicas convencionales para esta labor. Existen dos técnicas o métodos tradicionales de identificación. Una de ellas es el método de “token” (ficha, muestra, indicio, prenda, vale, llaves), el cual está basado en objetos que el usuario tenga para su identificación. El segundo método consiste en utilizar algo que el usuario deba saber, como ejemplo están los passwords. Sin embargo estos métodos no son muy confiables, pues si se usa el primero es muy probable que el usuario pueda extraviar el dispositivo el cual lo identifica, y en el segundo es muy probable que se pueda olvidar la contraseña.

Por esta razón se ha incursionado en la biometría ya que se puede utilizar información del cuerpo humano para identificación plena de un individuo, sin embargo aún no es completamente infalible, de esta manera se han ido utilizando otras técnicas llamadas tecnologías de identificación biométrica multimodal, la cual consiste en reunir información de varios patrones únicos del individuo para identificarlo con mayor confiabilidad.

El ojo humano es bastante complejo, pues es capaz de proporcionar bastante información única para identificar a una persona; desde la forma en que está compuesto, el iris, el movimiento, la forma muscular los cuales son únicos y que no son de fácil reconocimiento o adquisición como las huellas dactilares, que donde sea que se tenga un contacto directo se irán dejando huellas y así información importante que puede comprometer un sistema de seguridad.

La técnica de reconocimiento visual o del ojo trata de recopilar todos los factores que del ojo del individuo, y como este también está íntimamente ligado a la psicología, por medio de un visor se muestra un video clip y dependiendo de los gustos del individuo este prestará más atención en algunos sectores más que en otros, de esta forma se analiza este patrón de movimiento y se tiene información biométrica adicional.

Con esta técnica se pretende avanzar mucho al implementarla en sistemas de seguridad, ya que es posible por medio del ojo humano recolectar información biométrica de diferentes aspectos de este, así será cada vez más confiable utilizar sistemas de seguridad de este tipo, pues es muy difícil replicar u obtenerla, así la suplantación de identidad será evitada correctamente tal como el ingreso de extraños a cualquier recinto que requiera identificación plena de un individuo.

- **Reconocimiento de Voz:** Para la autenticación o reconocimiento de la voz es necesario un micrófono para captarla, la voz es digitalizada y luego usada para la autenticación. Los métodos de grabación de esta pueden ser al ir recitando un texto (dependientes de texto) o simplemente hablando (independientes de texto).

Gracias a estas técnicas es posible reconocer la identidad de un individuo, y que con los avances tecnológicos irán mejorando para convertir los sistemas de seguridad cada vez más eficaces contra amenazas e ingresos no permitidos.

6.3.4 SISTEMA DE AUTENTICACIÓN BIOMÉTRICO BASADO EN SERVICIOS MÓVILES DE USUARIO [13]

Los servicios móviles en la actualidad están mejorando rápidamente y están siendo destinados a proveer información de intercambio entre sistemas y la red. Muchos servicios son introducidos al usuario como servicios web; por lo tanto es requerido un sistema de seguridad para proteger la privacidad y la confidencialidad de la información de los usuarios. Se necesita un sistema robusto que incremente la seguridad en caso de servicios web móviles, como usuarios que están más expuestos a amenazas de este tipo. En este documento se introduce y se propone un sistema biométrico de encriptación para servicios móviles web para autenticación basado en el reconocimiento del iris. El iris del usuario será utilizado para regenerar una llave de encriptación de usuario para cada vez que el usuario necesite ser autenticado. Esta llave es más larga que una contraseña y menos que un dato biométrico, balanceándose entre seguridad y desempeño.

Los dispositivos móviles usualmente se conectan a redes inalámbricas para proveer a los usuarios muchos servicios web móviles como el comercio móvil y servicios web bancarios. Esta clase de servicios requieren intercambio de información segura, es por esto que las redes inalámbricas son más vulnerables a amenazas de seguridad que las redes cableadas, especialmente cuando los dispositivos móviles se conectan a través de internet, porque dependen de un tercero, lo que hace que la conexión no sea muy confiable.

En este artículo se propone un sistema de seguridad biométrico basado en la autenticación móvil para usuarios de servicios web. La principal debilidad del sistema, es la implementación de reconocimiento de iris. Usando este sistema de reconocimiento de iris se mejorará el desempeño. Otra de sus debilidades es la incompatibilidad entre el reconocimiento de iris y el sistema de error-conexión, tal incompatibilidad mejora el control del sistema sobre los errores corregidos.

El aporte de este documento es el sistema de autenticación remota, ya que es una alternativa al subsistema de reconocimiento de iris, sobre los dispositivos móviles existentes. Si pudiéramos reemplazar estos subsistemas con sistemas móviles específicos podríamos obtener mejores resultados.

6.3.5 SISTEMAS DE SEGURIDAD EMBEBIDOS

Los sistemas embebidos están siendo utilizados cada vez más de forma global, donde, la seguridad es un problema que los ha afectado influenciando su credibilidad. [14]

Este documento presenta una nueva solución para los sistemas embebidos, combinando una FPGA (Field – Programmable gate array) y un TPM (Trusted Platform Module) creando un nuevo módulo llamado TFSES (Security Embedded Systems base on TMP and FPGA).

Esta solución consiste en que la FPGA chequea la integridad de las instrucciones y de los datos antes que lo haga el procesador embebido, el resultado de este proceso es brindar mecanismos de protección de la integridad y privacidad de la aplicación de ataques físicos a la vez que de ataques de software. Sin embargo sistemas de seguridad física también pueden construirse utilizando TFSES.

Los TFSES pueden proveer una solución muy flexible para adaptar sistemas embebidos con la característica de la reconfiguración de las FPGAS, haciendo que estos dispositivos puedan correr mucho más rápido debido a la robustez de cómputo.

El costo de los TFSES es menor, ya que la arquitectura propuesta puede ser implementada con los dispositivos que se encuentran actualmente en uso. Las TFSES son dispositivos de bajo costo y de bajo consumo energético, sin embargo la ventaja de este no es tener un alto rendimiento, si no que esta creado para poder brindar soluciones creativas y seguras para un sistema embebido.

Las FPGAs se están volviendo más comunes y cada vez se usan a mayor escala tanto en sistemas de alto como de bajo rendimiento, sin embargo en muchas ocasiones se pretende hacer un traspaso de las funcionalidades de las FPGA a los ASIC. [15]

Es sorprendentemente difícil encontrar información acerca del paso de los programas o aplicaciones de las FPGA hacia los ASIC pero se puede encontrar documentación y guías más completas del caso contrario. Existen varios consejos de las FPGA y los ASIC y algunos de estos son:

- Los multiplexores son realmente caros en las FPGAs y baratos en las ASICs cuyo desempeño puede verse mejorado por una pequeña área de multiplexores estratégicamente situados, como barras cruzadas en lugar de buses.
- Si el diseño ha sido especialmente optimizado para los bloques DSP dentro de la FPGA, es muy probable que existan problemas de desempeño cuando se esté migrando el diseño hacia un ASIC.
- Es extremadamente importante que los generadores de memoria sean usados para memorias grandes en una ASIC. Ahorrar área de la tarjeta es

posible si algunas de las memorias pueden ser recreadas usando compiladores ROM.

- Pequeños archivos de registro con un solo puerto de escritura y varios de lectura son más eficientes en cuanto a ahorrar área en la mayoría de FPGAs.

Al existir varias técnicas de optimización para las FPGAs se pueden concluir que la mayoría de ellas son tanto benéficas como no dañinas para el desempeño y área en una migración hacia una ASIC. Las áreas más peligrosas son las de memoria y bloques DSP y se debe tener mucho cuidado para poder hacer una migración exitosa entre las dos plataformas de forma eficiente, especialmente si el diseño ha sido específicamente optimizado para los componentes de una FPGA.

Aplicaciones de estos dispositivos y sistemas son:

Una plataforma muy versátil, configurable y modular para procesamiento en tiempo real de video e imagen. Esta plataforma está basada en una tarjeta de desarrollo ***DE2*** la cual conectada a una cámara para la adquisición del video y una interfaz VGA (Video Graphics Adapter) para la restitución de la imagen. [14]

Utilizando una FPGA, se puede proveer el rastreo facial en tiempo real de alguna persona en específico y si los rasgos corresponden a ella es posible abrir el cerrojo de la puerta del automóvil. Todo el Sistema está desarrollado con una tarjeta DE2 usando lenguajes de descripción de hardware como VHDL o VERILOG para programarla.

Para la programación de la tarjeta no se usaron algoritmos básicos, por el contrario se desarrolló un algoritmo propio con el fin de optimizar el proceso de reconocimiento. Dentro de este proyecto se agrega un fondo oscuro y cuando los pixeles de fondo son distorsionados por alguna persona que se aproxima los pixeles correspondientes son almacenados en una memoria y luego son devueltos para el reconocimiento y detección del rostro, si los pixeles distorsionados son los mismos que los que se guardaron anteriormente en memoria, en este instante el seguro del automóvil se abre.

Utilizando estas herramientas es posible mejorar la seguridad en los automóviles para prevenir el hurto, haciendo que los vehículos sean mucho más seguros a la hora de dejarlos en algún lugar público mientras los dueños no se encuentran.

6.3.6 LAS FIRMAS DIGITALES

En la actualidad la firma manuscrita permite certificar el reconocimiento, la conformidad y/o el acuerdo de voluntades sobre un documento por las partes firmantes que forman parte de la transacción, lo que trae consecuencias legales claras y reconocimiento jurídico al instante. Ahora bien cuando nos encontramos con las transacciones que se realizan a través de las redes de información la situación varía en gran magnitud, porque en este tipo de contratos electrónicos la firma manuscrita no puede ser insertada en el documento. De esta forma es que en materia digital se ha suplantado la llamada firma manuscrita por la llamada firma digital. La firma manuscrita tiene un reconocimiento legal alto, a pesar de que pueda ser falsificada, pero la firma manuscrita tiene peculiaridades que la hacen fácil de realizar, de comprobar y vincular a quién la realiza, porque la verdadera firma manuscrita sólo puede ser realizada por una persona y puede ser comprobada por cualquiera con la ayuda de una muestra. [16]

La Secretaría General de la CNUDMI (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional) incluye ciertas técnicas basadas en la autenticación a través de un dispositivo biométrico basado en la firma manuscrita; con este dispositivo se firma en forma manual con un lápiz especial, en la pantalla del computador o ordenador, siendo analizada por éste y almacenada como un conjunto de valores numéricos que se podrían agregar a los datos de un mensaje y ser recuperados en la pantalla con la finalidad de que el receptor pueda tener como auténtica la firma. Esto quiere decir, que para el funcionamiento de este sistema se requiere el análisis previo de las firmas manuscritas y su almacenamiento utilizando un dispositivo biométrico.

De igual forma al almacenarse información confidencial y de identificación se deben desarrollar normas legales, que regulen la aplicación de la informática, para su desarrollo idóneo y con respeto a los derechos fundamentales del hombre, como el derecho a la privacidad, intimidad, sancionando leyes referidas al hábeas data, ya sea que se intente vía administrativa o jurisdiccional.

En Chile este sistema ofrece varias ventajas respecto de firma electrónica basada en certificados digitales personales. Una de ellas es la seguridad para evitar fraudes por suplantación, ya que permite capturar en un dispositivo (Ipad, smartphone o tablet) las características biométricas únicas de la firma de una persona en cuanto a desplazamiento, velocidad, presión y aceleración en el trazado de la firma, por lo que el sistema es invulnerable. [17]

Para [Santiago Uriel], otro de los beneficios es que mejora y hace más eficientes los procesos de negocios. "Nosotros analizamos en un banco tipo, de mil oficinas y de un activo de 80 millones de euros, cuál era el ahorro en horas y en papel con el uso de la firma manuscrita biométrica y el estimado es de 3.5 millones de euros al año. Si consideramos el total de nuestro sector esto implica un ahorro de 40 millones de euros en el mismo periodo", indica.

El abogado Rodolfo Herrera, experto en derecho informático y tecnología, explica que hoy en nuestro país se usan sistemas muy inseguros para la firma, como el pie de firma basado en imágenes JPG capturadas desde un documento escaneado, o el típico control de acceso a sistemas basado en "identificación de usuario y password". Buscando incrementar la seguridad y la confianza y a la vez reducir el uso del papel, ha llevado a usar firmas electrónicas o la huella para la firma de documentos electrónicos.

6.3.7 SEGURIDAD BASADA EN BIOMETRÍA PARA LA AUTENTICACIÓN EN WIRELESS BODY AREA NETWORK (WBAN) [18]

El avance en las tecnologías de comunicaciones inalámbricas ha desarrollado la WBAN, y en los últimos años varios científicos y especialistas se han concentrado en crear una arquitectura o sistema de monitorización enfocado hacia la salud, para mejorar así mismo los requerimientos técnicos específicamente diseñados para una WBAN.

WBAN al ser un medio de comunicaciones para transmitir información carece de seguridad, tales como perdida de información, autenticación y control de accesos. Al implementar un sistema con un alto grado de seguridad conlleva a tener inconsistencia en el desempeño computacional.

Anteriormente no se ha podido identificar una solución para el problema del desempeño computacional, sin embargo dentro de este estudio se establece que el uso de la biometría dentro de la comunicación utilizada por la WBAN reduce considerablemente la complejidad y el poder de computo.

Como conclusión se propone que un sistema de seguridad propuesto para la autenticación en una WBAN se utilice la biometría, específicamente donde la persona que envía la información deba ser autenticada con la información de un electrocardiograma como medio o mecanismo de autenticación para el sistema de la WBAN. De esta manera se cambia información de autenticación de formas criptográficas por información biométrica que es única para cada individuo.

6.3.8 "SOFT BIOMETRIC" Y SUS APLICACIONES EN LA SEGURIDAD Y NEGOCIOS [19]

La tecnología biométrica permite la identificación automática o la verificación de un individuo basada en la fisiología o por las características comportamentales. La Biometría es una investigación en la cual se ha fijado mucha atención recientemente.

La aplicación de la biometría dentro de la seguridad es muy prometedora ya que tiene muy fuertes medidas de seguridad y de igual manera mejora la calidad del servicio en esta rama. La biometría por software está definida por las características que proveen información acerca de un individuo, pero aún existe falta de altos distintivos y desempeño para diferenciar completamente dos individuos.

Algunas de las aplicaciones de "Soft Biometric": Es utilizada como una modalidad de biometría multimodal, es decir, que se pueden utilizar varias características del individuo como la voz y está puede ser soportada por el peso u otras características del mismo.

Esta tecnología también es utilizada como información descriptiva para reconocer personas, para sistemas de vigilancia o inclusive para negocios.

CAPITULO III

7. APORTES

La Biometría se puede entender como la medición de las características biológicas que hacen a un individuo único, ya sea por la anatomía que lo compone o por la forma en que este se comporta, sin embargo hoy en día este término se aplica más a las técnicas utilizadas para identificarlos a través de tecnología la cual recoge información que se pueda verificar, medir y retomar las veces que sean necesarias.

Las tecnologías que se han ido utilizando se han creado de acuerdo a las diferentes técnicas de identificación o de recolección de información biométrica tales como las huellas digitales, la voz, el rostro, los ojos y otras más que constantemente se desarrollan como evolución y mejoramiento de estas herramientas. Por lo tanto hoy en día se puede aprovechar completamente la funcionalidad de estas herramientas para la identificación plena de un individuo evitando así la suplantación de identidad y al utilizarlas adecuadamente dentro de un entorno donde sea necesario un sistema de seguridad para salvaguardar algo en específico se puede garantizar que solo las personas indicadas puedan tener acceso a este.

Entonces ¿cuál debe ser la mejor opción al implementar un sistema de seguridad utilizando tecnología biométrica? Realmente, esto debe ser analizado con calma y tranquilidad, pues para tener una implementación adecuada es necesario analizar todos los factores que interactúan con los dispositivos biométricos dentro del sistema y con los usuarios relacionados con este, tales como la ubicación física de los sensores o dispositivos que recolecten la información biométrica para ser medida y analizada determinando si corresponde al individuo adecuado, el proceso o labor en la que debe ser utilizado el dispositivo en el caso de identificación o verificación del sujeto, la cantidad de usuarios, la finalidad de la implementación del sistema de seguridad, ya que se debe integrar todo esto junto con los mecanismos de pestillos, cerrojos o candados del lugar que se debe

resguardar, teniendo en cuenta la confiabilidad, eficacia y/o robustez de los diferentes dispositivos existentes, pues habrá siempre mejor documentación o soporte debido a la investigación previa que han tenido unos con respecto a otros, tales como los dispositivos lectores de huellas dactilares los cuales llevan un campo de acción mucho más extenso en cuanto a tiempo se refiere que los lectores de iris que llevan mucho menos tiempo de aplicación.

Entonces como tal la eficiencia y el éxito a la hora de elegir que dispositivos depende exactamente de estos análisis, pues también se deben tener en cuenta los diferentes entornos y situaciones en las que se ven afectados los actores que interactúan con el sistema, y los limitantes que tiene cada dispositivo haciendo que estos factores sean esenciales a la hora de tomar una decisión adecuada, por ejemplo un sistema de reconocimiento de voz podría tener inconvenientes en ambientes muy ruidosos.

Para poder realizar un sistema de seguridad aplicando estas tecnologías simplemente es necesario realizar un proceso de verificación, donde gracias a los dispositivos o sensores es posible recolectar la información biométrica necesaria para determinar si una persona se encuentra registrada en la base de datos del sistema, es decir, si está es quien dice ser y el sistema la reconoce puede tener acceso físico a los lugares resguardados por el mismo sistema.

Inicialmente el análisis que se realizará es en un entorno específico y se determinará que tecnología puede ser la mejor a la hora de implementar un sistema de seguridad. Al enfocarse en una vivienda, donde el método de ingreso por defecto es la puerta principal, la cual consta de un cerrojo común utilizando llaves metálicas, donde es muy probable y común que estas se extravíen o que puedan ser hurtadas facilitando el acceso a desconocidos a la casa, de esta manera contando con un sistema biométrico se puede evitar con un alto grado de eficacia esta problemática, sin embargo se deben tener en cuenta varios factores los cuales afectarán el rendimiento, estabilidad del sistema y la recolección de la

información biométrica necesaria para hacer el proceso de verificación de usuario, tales como las condiciones ambientales del lugar y las condiciones fisiológicas de los usuarios.

Es esencial tener en cuenta algunas características propias de los diferentes dispositivos biométricos a la hora de realizar un análisis comparativo para tener de cierto modo el criterio de decidir con que tecnología es más recomendable irse. Tales factores son:

- Accesibilidad: La cual indica si cada persona puede poseerla
- Permanencia: El tiempo total que puede mantener activa.
- Desempeño: Sí el dispositivo es realmente bueno en la labor para la cual está siendo usado en cuanto a rapidez y eficacia.
- Unicidad: Determinando sí es único para cada individuo en cuanto al nivel de autenticación.

De acuerdo también a análisis técnicos previos que se han llevado a cabo en los dispositivos se puede tener un grado de decisión en cuanto a que dispositivo elegir, donde se mide la precisión de cada uno, la confiabilidad pues se deben tener en cuenta cuando existen fallos y qué los causa, y así mismo determinar si el dispositivo funciona adecuadamente sin dar o falsos positivos ó falsos negativos. La forma de uso y la accesibilidad son factores determinantes pues de acuerdo a estos, los usuarios pueden familiarizarse y usar adecuadamente el dispositivo con mayor rapidez, en cambio si fuera muy difícil de manejar posiblemente no se adaptarían al sistema y lo dejarían de usar. Finalmente los costos son esenciales a la hora de determinar que dispositivo utilizar, aunque está claro que la relación costo/rendimiento es proporcional, también se deben analizar los alcances del sistema y la economía de los usuarios.

Entonces, antes de realizar cualquier acción previa, lo correcto es tomar una lista de requerimientos con el fin de determinar lo que se necesita y espera del sistema,

dentro de estos requerimientos también existen especificaciones que se deben tener en cuenta, como el ambiente local, las localizaciones de las puertas de acceso, las fuentes de energía para conectar los dispositivos biométricos, el software, los periféricos y la red en el caso que sea necesaria.

En primera instancia los componentes para implementar un sistema de acceso vienen dado por un dispositivo de control de acceso, los cuales deben ser empotrados o puestos en el exterior de la vivienda;(en este caso el dispositivo biométrico), de esta forma se tomará la información biométrica del individuo. Estos dispositivos pueden trabajar enviando dos tipos de señales, la primera sería enviar un pulso eléctrico a un motor ubicado en los pestillos de la puerta, de esta forma está se abrirá, usualmente esto ocurre en los dispositivos que son embebidos, los cuales son más costosos por contar con un software propio capaz de realizar estas actividades y procesos de identificación y autenticación sin la necesidad de contar con algún otro dispositivo, como tarjetas FPGA o conexiones directas a ordenadores, haciéndolos un sistema autónomo y local pero a un costo mayor.

La segunda es una serie de números o información encriptada la cual es enviada a unidades de control de acceso, las cuales pueden ser tarjetas FPGA programadas exclusivamente para ello, y así estas determinaran si la autenticación o identificación de algún individuo es correcta. Usualmente estos dispositivos están localizados en un área diferente a la exterior donde se encuentran los sensores biométricos, ya que son bastante delicados y en consecuencia el pilar de decisión del sistema de control de acceso, sin embargo una ventaja de esta modalidad es la de contar con mayor memoria al poderse conectar directamente con bases de datos las cuales sirven considerablemente para llevar registros de todas las transacciones del sistema en cuanto al acceso y de igual manera se cuenta con un gran nivel de procesamiento lógico el cual puede ser reconfigurado o mejorado al poderse reprogramar dicho dispositivo.

7.1 ANÁLISIS DE DIFERENTES DISPOSITIVOS BIOMÉTRICOS SEGÚN SU TECNOLOGÍA

7.1.1 LOS DISPOSITIVOS LECTORES DE HUELLAS DACTILARES

7.1.1.1 Impresión de huella digital

Una impresión de huella es una impresión de las líneas de fricción de todo o de parte de un dedo. Una línea de fricción es una porción elevada de la palma de la piel de la mano o de los dedos, en la mano y en los dedos existen muchas de estas líneas conectadas entre sí formando figuras y patrones entre ellas, también son conocidas como líneas dérmicas o dermales. El método tradicional es utilizar tinta para empapar el dedo y hacer una impresión del dedo empapado en un papel, así la tinta marcará el papel dejando impreso en él las líneas de fricción, este pedazo de papel, es escaneado utilizando un escáner tradicional. Hoy en día, un enfoque moderno utilizado para la impresión de huellas es utilizar dispositivos tecnológicos lectores de huellas, estos están construidos basándose en técnicas ópticas, térmicas, ultrasónicas y de silicio entre los principales. Estos son las técnicas biométricas más antiguas y más utilizadas. El dispositivo lector de huellas es el más común y más utilizado en la actualidad. Y está basado en los cambios de refracción de los haces de luz provenientes del dispositivo hacia la piel de los dedos que tocan la superficie del lector.

Todos los dispositivos lectores de huellas comprometen recursos de luz, como sensores y superficies especiales de refracción. Algunos de estos dispositivos traen consigo chips de procesamiento y memorias.

El tamaño del área de lectura de estos dispositivos, es aproximadamente 10x10x15 mm.

El sensor de huellas de silicio, está basado en la capacitancia del dedo. La capacitancia de este sensor, consiste en arreglos rectangulares de capacitores sobre un chip de silicio. Una placa de capacitores es el dedo, otra placa contiene un área metalizada pequeña sobre el área del chip, ubicando la porción del dedo a la cual se le va a tomar la impresión contra la superficie del chip, y así cuando las líneas de fricción están cerca de píxeles cercanos, al tener una capacitancia alta, se cargan. Los valles que son la parte profunda entre dos líneas de fricción, al estar más lejanas, no influyen en la capacitancia.

Lo más nuevo y lo menos común en la actualidad, es el utilizar ultrasonido para la impresión de huellas digitales. Estos utilizan ultrasonido para monitorear las figuras en las superficies, el usuario ubica su dedo en un vidrio y el sensor se mueve y lee la superficie del dedo completa, este proceso toma alrededor de uno o dos segundos.

Las técnicas de impresión de huellas digitales, se pueden ubicar en dos categorías, una de ellas es la basada en los detalles minuciosos y la otra se basa en la correlación. Las técnicas basadas en los detalles minuciosos, ubican los puntos minuciosos primero y luego la relación de la ubicación entre ellos en el dedo. Las técnicas basadas en la correlación, requieren una ubicación precisa en un punto de registro y son afectadas por translación y rotación de imágenes.

Hoy en día existen empresas que se encargan de desarrollar dispositivos exclusivos para la identificación de individuos a través de impresiones dactilares, una de ellas es Secugen [11], y los dispositivos principales y sus respectivas características son:

7.1.1.2 HamsterTM Plus:

Esta es una versión simple y popular de un lector de huella dactilar producido por SecuGen, su diseño es cómodo y ergonómico, una de las características más fuertes y que llama más la atención, es su avanzado sensor óptico que utiliza tecnología biométrica basada en una superficie de reflexión irregular, otras de sus características son:

- Alto desempeño, sensor óptico sin necesidad de mantenimiento.
- Sensor resistente a rayones, impactos, vibraciones y descargas electroestáticas.
- Auto encendido, detección automática de dedos.
- Captura inteligente, ajusta el brillo de la captura de la huella dactilar.
- Conexión USB.
- Posición ajustable y removible.
- Compacto, ligero y fácil de llevar.
- Posibilidad de utilizar cualquier dedo.

7.1.1.3 HamsterTM IV:

Es otra versión versátil y popular de un lector de huellas, esta certificado en calidad y pruebas estándar, con un empaque cómodo y un diseño ergonómico, podemos encontrar en él, las siguientes características:

- Certificado por el FBI como dispositivo lector de huellas.
- Certificado en calidad y pruebas estándar.
- Alto desempeño, sensor libre de mantenimiento.
- Sensor resistente a rayones, golpes, vibraciones y descargas electroestáticas.
- Auto encendido, detección automática de movimiento de dedos.
- Captura inteligente, ajusta el brillo de la captura de la huella dactilar.

- Conexión USB.
- Posición ajustable y removible.
- Compacto, ligero y fácil de llevar.
- Guía integrada de dedo.
- Posibilidad de utilizar cualquier dedo.

7.1.1.4 OptiMouse Plus

Presentado como un modelo mejorado en la línea de ratones para computadores. Un innovador ratón óptico que puede operar sobre cualquier superficie sin ningún problema y con una respuesta excepcional, puede ser utilizado como dispositivo de autenticación, identificación y verificación gracias a su sensor de alto desempeño al lado derecho, para el dedo pulgar de la mano derecha; permite utilizar las huellas digitales como passwords que no se pueden perder, olvidar y/o robar, algunas de sus características son:

- Alto desempeño, sensor libre de mantenimiento.
- Sensor resistente a rayones, golpes, vibraciones y descargas electroestáticas.
- Captura inteligente, el dispositivo ajusta el brillo a la hora de la captura.
- Conexión USB.
- Seguimiento óptico del ratón.
- Rueda de desplazamiento y botones programables.
- Sensor ubicado en un costado de forma natural, para la consistente ubicación del dedo.

7.1.1.5 iD-USB SC

Es una combinación de un dispositivo lector de huellas y de un dispositivos lector de tarjetas, con un dispositivos USB listo para usar, adecuado para sus dos aplicaciones de autenticación, este dispositivo incorpora un módulo óptico de alta calidad de imagen junto con un lector inteligente de tarjetas.

Características:

- Alto desempeño, sensor libre de mantenimiento.
- Sensor resistente a rayones, golpes, vibraciones y descargas electroestáticas.
- Auto encendido, con tecnología de detección automática de dedos, que verifica la presencia de dedos, cuando sucede esto, el lector de huellas se enciende y escanea la huella tan pronto el dedo toque el sensor.
- Captura inteligente, el dispositivo ajusta automáticamente el brillo al momento de la captura, también permite capturar con una alta calidad una huella desde un rango de dificultades, como lo son los dedos sucios, húmedos, con heridas y condiciones de ambiente como puede ser la luz directa del sol.
- Integrado con una guía que permite leer la huella sin importar la dirección del dedo.
- 100% compatible con el dispositivo Hamster Plus.
- Lector de tarjetas sumiso a PS/SC, 100% compatible con HID Omnikey 3121.
- Distribución de energía eléctrica a través del puerto USB, no se requiere ningún otro tipo de fuente.
- Superficie montable, integrados tornillos.

7.1.1.6 iD-USB SC/PIV

Es una combinación de lector de huellas y lector de tarjetas, incorpora un sensor con una calidad de imagen alta y un lector inteligente de tarjetas con un módulo PC/SC.

Características:

- Certificado como dispositivo de captura por el FBI.
- Alto desempeño, sensor libre de mantenimiento.
- Sensor resistente a rayones, golpes, vibraciones y descargas electroestáticas.
- Auto encendido.
- Captura inteligente.

- Da acceso si verifica el dedo en cualquier orientación.
- 100% compatible con el dispositivo Hamster IV.
- Plug'n play, intercambiador en caliente.
- Distribución de energía eléctrica a través del puerto USB, no se requiere ningún otro tipo de fuente.
- Superficie montable, integrados tornillos.

7.1.1.7 iD-Serial

Es un sistema de autenticación de lectura de huellas dactilares diseñado para integrarse con aplicaciones como lo son puntos de venta, seguimiento del tiempo y de asistencia o cualquier otra aplicación donde sea preferible una interfaz serial. Este tipo de interfaces incorpora módulos autónomos, módulos de alta calidad de imagen tomada en una impresión dactilar, un procesador, un cable serial y una fuente de energía externa.

Algunas características

- Alto desempeño, sensor libre de mantenimiento.
- Sensor resistente a rayones, golpes, vibraciones y descargas electroestáticas.
- Auto encendido, con tecnología de detección automática de dedos, que verifica la presencia de dedos, cuando sucede esto, el lector de huellas se enciende y escanea la huella tan pronto el dedo toque el sensor.
- Captura inteligente, el dispositivo ajusta automáticamente el brillo al momento de la captura, también permite capturar con una alta calidad una huella desde un rango de dificultades, como lo son los dedos sucios, húmedos, con heridas y condiciones de ambiente como puede ser la luz directa del sol.
- Captura de huellas dactilares y la creación de plantillas con la opción de utilizar los formatos estándar 378-2004 propiedad o ANSI INCITS.
- Capacidad de transmitir plantillas a bases de datos/servidores separados para almacenamiento y clasificación.
- Capacidad de almacenamiento para 3.000 usuarios.

- Interfaz serial RS-232 con conector RJ-22 jack modular para máxima flexibilidad en configuraciones de cable.
- Superficie montable, integrados tornillos.
- Adaptador de poder.

7.1.1.8 Biometric Door[1]

Es un sistema de acceso a áreas restringidas, como pueden ser áreas restringidas, cuartos o bodegas, es utilizado como método de identificación la lectura de huella digital de usuarios. Este dispositivo permite administrar los horarios de acceso, perfiles de usuario, cada acceso es registrado, lo cual puede ser registrado de forma eficiente y amigable.

Cuenta con un módulo de control de visitantes, que permite llevar un registro detallado de todo el personal externo que ingresa al lugar que esta monitoreado por el dispositivo, incluyendo datos personales, imagen fotográfica y los objetos que ingresa.

Algunas de sus características son:

- Cada dispositivo puede almacenar alrededor de 9.000 usuarios e información sobre horarios, nivel de seguridad de huella, entre otros.
- Memoria de almacenamiento de eventos de acceso de hasta 12.800 registros.
- Modo identificación 1:1 y 1:N (solo huella y código más huella).
- Soporta hasta 64 horarios diferentes, cada uno de los cuales puede definirse hasta en cinco segmentos diferentes aplicables en un día.
- Almacena hasta 32 festivos.
- Permite la creación de hasta 16 privilegios de acceso de usuario.

[1] Control de Acceso. Biometric Door. Disponible en: http://www.stt-solutions.com/producto-detalle.php?idProduct=5

- Dispositivos con conectividad a Ethernet.
- Licencia gratuita de software de administración de control de accesos (el módulo de visitantes se licencia por separado).

7.1.2 TECNOLOGÍA PARA RECONOCIMIENTO DE ROSTRO

La técnica para reconocimiento de rostro es una aplicación de computador para la identificación y verificación automática de una persona tomando una imagen o un fragmento de video de un dispositivo de captura.

Esta tecnología viene siendo desarrollada en dos áreas, métrica facial y Eigen faces. (Rostros particulares)

7.1.2.1 Tecnología de métrica facial:

Está basada en la posición de zonas específicas del rostro, este sistema usualmente tiene en cuenta la posición de los ojos, nariz y boca, y también la distancia entre estas partes.

La región capturada es redimensionada a un tamaño predefinido, esta imagen nueva es llamada imagen canónica, después de que las métricas faciales son computadas, se almacenan en una plantilla. El tamaño de este archivo está aproximadamente entre 3 y 5 Kb, pero existen sistemas donde el tamaño de la plantilla es igual o menor a 96 bytes.

7.1.2.2 Método de Eigen Face

Está basado en categorizar el rostro de acuerdo al grado de este y un conjunto fijo de entre 100 y 150 eigen faces. Estas eigen faces son creadas cuando aparecen zonas luminosas y oscuras que son almacenados en un patrón específico. Este patrón muestra cómo diferentes características del rostro son señaladas, siendo evaluadas y puntuadas. Este será un patrón para evaluar la simetría. Este método evaluará por ejemplo la línea límite del cabello, el tamaño de la nariz o la boca. Otros eigen faces tienen patrones menos simples de identificar y el eigen face se verá muy poco como un rostro, esta técnica es similar al método utilizado por la policía para crear un retrato, pero el procesamiento de la imagen es automático y está basado en una imagen real. A cada rostro se le es asignado un grado de adaptación para cada uno de los 150 eigen faces, solo 40 plantillas con los grados más altos de adaptación son necesarios para reconstruir el rostro con una precisión de 99 porciento, lo siguiente es utilizar software de reconocimiento.

7.1.3 DISPOSITIVOS PARA RECONOCIMIENTO DE ROSTRO

7.1.3.1 SekuFace [2]

Este dispositivo desarrollado por Eurotech provee la mejor calidad y utiliza un sistema de reconocimiento de rostro, obediente con restricciones de seguridad y alineado con los niveles más altos de desempeño, está disponible en el mercado.

Características:

- Captura de imagen:

  Resolución 1296 x 966 pixeles.

[2] BIometric Face Recognition. SekuFace. Disponible en: http://www.eurotech.com/en/products/SekuFACE

Escaneo progresivo.

Lente de 8,5mm.

Control automático de ganancia.

Auto balance de blancos.

Compensación de contraluz.

- Incluido iluminador infrarrojo.
- Proceso de reconocimiento:

Captura una media de seis imágenes por segundo.

Creación de un perfil biométrico en tres segundos.

- Capacidad de almacenamiento de más de 600.000 archivos de imágenes jpeg de rostros (300 GB de almacenamiento; 500 KB por imagen incluido archivo de texto).
- Formato de transmisión de datos configurable.
- Parámetros RS232 configurables.
- Reconocimiento de rostro inequívoco.
- Vector biométrico de seguimiento de cumplimiento para restricciones de seguridad.
- Operación día y noche.
- Administración de listas “blancas” y listas “negras”.
- Interfaz web para la administración de las funcionalidades.

7.1.3.2 Tecnología de fusión multi-biométrica del dispositivo D-Station[3]

La tecnología de fusión multi biométrica por sus siglas en inglés MBFT, ofrece un alto desempeño y un alto grado de seguridad gracias a el uso de múltiples características biométricas y múltiples sensores para la autenticación de un usuario, gracias a esto, proporciona una increíble tasa de error del 0.001% al

[3] Tecnología de fusión multi-Biométrica. Disponible en: http://equiposyredes.es.tl/Reconocimiento-Facial-para-control-de-accesos-y-asistencias-.htm

utilizar el reconocimiento de huella dactilar y el reconocimiento de rostro, lo que lo convierte en uno de los dispositivos más confiables en el mercado.

7.1.3.3 Poderoso sistema de procesamiento paralelo Tri-CPU

Todas las sensacionales características de la D-Station son accionadas por su sistema único Tri-CPU. Este sistema Tri-CPU ofrece procesamiento paralelo que permite a la D-Station aumentar la velocidad de comparación de datos biométricos de gran escala. En procesamiento paralelo los poderosos CPUs de 667 MHz y dos de 400 MHz conforman 1.4 GHz de poder computacional, el cual permite a la D-Station proporcionar un desempeño excepcional en cómputo biométrico así como operación integral para sus sofisticadas funciones.

Principales Características

- Integra biometría de reconocimiento facial y de huella única y dual.
- Motor Tri-CPU que proporciona velocidad y exactitud de identificación.
- Pantalla táctil LCD a color ultra ancha Indicador LED, instrucciones sonoras y cámara para interacción directa con el usuario.
- Control de Accesos IP con PoE y WiFi (opcional).
- Cámara incorporada para interfaz de imagen y video.
- Acelerómetro integrado (sensor detector de movimiento de alta precisión) para detectar el impacto por violaciones o vandalismo.
- Lector de tarjetas interno para tarjetas Mifare ISO 14443 Tipos A y B.
- Soporte a memorias SD.
- Interfaz RS232 compatible con GPRS/GSM basadas en conexiones móviles y para impresoras seriales de registros de asistencia.

Ventajas

- Exactitud de comparación y velocidad increíbles.

- Sencillez de uso a través de su interfaz gráfica intuitiva: Simplifica considerablemente su uso para usuarios y administradores.
- Diversos modos de reconocimiento: Mayor exactitud a través de más entradas biométricas
- Índice de errores considerablemente reducido: En FAR=0.001%, la 'fusión dactilar dual' logra el 0.2%, la 'fusión dactilar y facial simple' logra el 0.1%, y la 'fusión dactilar y facial dual' logra el increíble porcentaje de 0.001% de FRR.
- Menores costos de instalación y mantenimiento así como aprovechamiento de la infraestructura existente mediante la comunicación IP, integración con PoE y conexión WiFi opcional.
- Puede registrar y comparar entradas biométricas y no biométricas de los usuarios mediante su cámara de reconocimiento facial, sensores dactilares, teclado en pantalla (PIN) y antena RFID.
- El dispositivo es tan fácil de usar que permite a los administradores y usuarios aprender fácilmente los controles y funciones con un entrenamiento y orientación mínimos.

Aplicaciones

- Control de asistencias y control de accesos para oficinas.
- Nómina integrada y administración de Recursos Humanos.
- Seguridad en red para edificios industriales, financieros y centros de investigación.
- Recolección de datos para administración de incentivos.

7.1.4 DISPOSITIVOS DE RECONOCIMIENTO DE VOZ

Naturalmente la voz es una característica del hombre que lo puede identificar, y aunque existan ciertas similitudes entre varios individuos, es muy difícil encontrar dos personas que la tengan exactamente igual. Gracias a esta capacidad el ser humano tiene un medio de comunicación que le ha permitido desenvolverse con la comunidad exitosamente. Con la introducción de tecnologías y sistemas digitales se ha ido viendo como es necesario interactuar con estos, y por ende se han ido evidenciando que se requiere con más frecuencia la comunicación con las maquinas a partir de la voz.

Gracias al reconocimiento de voz es posible que las computadoras puedan tener interacciones directas con los seres humanos, y esta acción se realiza cuando se digitaliza la voz a través de un micrófono, y de acuerdo a algoritmos únicos o patrones sistemáticos es posible adecuar la acústica, y almacenar dichos sonidos los cuales pueden ser comparados para tener un nivel de autenticación o identificación de un individuo de acuerdo a técnicas de reconocimiento como “dependiente del texto” donde se debe decir la misma palabra o frase almacenada para tener acceso a un lugar que posea control de acceso, la técnica llamada “independiente del texto” donde de acuerdo a las características intrínsecas de la voz del individuo, donde si son exactamente iguales se concede la autorización de acceso.

Para esta técnica de reconocimiento realmente aunque se toman en cuenta las características de sonido de la voz, realmente se considera que es un reconocimiento más a nivel comportamental, pues el individuo posee una forma de hablar única, o posee características vocales que cuando este emite un discurso puede tener acentuaciones que lo identifican adecuadamente, y que en combinación con el tono, dimensiones vocales o de la garganta, cavidades

nasales que determinan como tal el grado de individualidad físico y morfológico de este en cuanto a su voz, pueden ejercer una técnica multimodal que es bastante segura en cuanto a un control de acceso utilizando tecnología biométrica se refiere.

Estos dispositivos poseen también un margen de error, ya que para poder establecer e interpretar la voz del individuo se debe captar eficientemente la onda o voz, es por esta razón que el ambiente o entorno del micrófono debe ser lo más silencioso posible, para tener una buena captación y así digitalizar correctamente la onda sonora con el fin de comparar e identificar si el individuo es la persona correcta y así darle los permisos necesarios de acceso.

Por esta razón, se debe tener en cuenta al momento de implementar un sistema de seguridad de control de acceso la ubicación del mismo, pues al tener un análisis previo de la ubicación del hogar en cuanto al ruido del entorno, se puede determinar si es posible y elegir esta opción tecnológica. Suponiendo que el hogar se encuentre cerca de una autopista o a un bar donde los niveles acústicos de ruido son altos, preferiblemente no se debe utilizar esta herramienta pues podrían haber tanto falsos positivos o negativos, ya que la señal no se podría obtener claramente.

Una aplicación para implementar esta solución se encuentra fácilmente utilizando tecnologías de tarjetas programables, tales como las FPGAs o nuevas tecnologías como el Arduino, donde actualmente en el mercado se han introducido módulos de reconocimiento de voz los cuales son fácilmente integrables a un costo muy bajo, y permiten realizar funciones para un usuario especifico disponiendo y programando los recursos de dichos dispositivos adecuadamente mediante los lenguajes con los cuales ellos trabajen (verilog, VHDL, C++, etc.), o aplicaciones nativas con las cuales cuentan haciendo más fácil programarlos y utilizarlos para el fin deseado.

7.1.4.1 EasyVR

Este módulo puede ser utilizado con cualquier dispositivo o host el cual cuente con una interface UART, como un PIC, Arduino, o dispositivos programables tales como tarjetas de desarrollo que cuenten con FPGAs. Este módulo es ideal para aplicaciones que cuenten con automatización o añadir funciones de “escucha” a cualquier dispositivo que realice diferentes funciones.

Los lenguajes con que este módulo cuenta:

- Inglés.
- Italiano
- Alemán
- Francés
- Español
- Japonés

Este dispositivo puede asignar hasta 32 frases dependientes del texto del usuario las cuales se pueden hablar en cualquiera de los lenguajes o idiomas estipulados anteriormente, y de los cuales se puede disponer de alguna función en especial.

De igual manera este módulo cuenta con Passwords de voz, que al ser programado puede reconocerla y determinar un comando de una persona en específico, que en este caso sería permitir el ingreso a la casa.

Posee una interfaz gráfica de fácil interacción para poder programar los comandos de voz.

Posee código de muestra para múltiples plataformas tales como Robonova, Robozak y Arduino, con el fin de optimizar la instalación y creación de aplicaciones fácilmente con este módulo y las demás tecnologías.

Una de las ventajas de estas tecnologías es que es relativamente económico en cuanto a costos, pues es posible conseguirlo entre un rango de 50 a 60 dólares, sin embargo este costo se contrarresta en cuanto a la facilidad de uso, es decir, para utilizar correctamente estos dispositivos el ingeniero o persona encargada de implementar el sistema de seguridad con esta tecnología biométrica debe programar y conocer cómo funcionan las comunicaciones de ambos dispositivos para poder hacer uso de ellos adecuadamente sin que se presente ninguna falla más adelante, por lo tanto existe una relación entre el costo y la facilidad de implementación, a mayor costo mayor facilidad, pero sin embargo los dispositivos programables al contar con esta ventaja, se pueden desarrollar algoritmos que puedan ser adaptados a la medida, o simplemente crear funciones específicas las cuales al ser de carácter propio no se deben pagar costos adicionales por utilizar software de terceros.

7.1.5 DISPOSITIVOS DE RECONOCIMIENTO BIOMETRICO A TRAVES DEL OJO

Los dispositivos biométricos que se encuentran disponibles para poder reconocer un individuo a través de sus ojos están divididos en dos grupos conocidos hasta ahora, los cuales son a través del iris y de la retina.

Sin embargo se debe saber la diferencia principal entre el iris y la retina para poder hacer un análisis de ambas técnicas. El iris es la zona coloreada del ojo, mientras que la retina se encuentra detrás del ojo la cual no puede reconocerse o verse a simple vista.

De esta manera para poder tomar la información biométrica necesaria al momento de la identificación o autenticación de iris, se requiere de una cámara o un dispositivo que cuente con una, con el fin de analizar por vía imagen las características del ojo, el iris y su composición, este proceso puede llevarse a cabo en unos 2 segundos permitiendo identificar plenamente a una persona.

Sin embargo al momento de realizar el proceso de identificación a través de la retina, se debe tener un proceso mucho más invasivo, ya que la retina se encuentra detrás del ojo, por lo tanto se necesita un scanner con rayos IR para poder generar la imagen necesaria la cual puede ser analizada y de esta manera obtener la información biométrica del individuo. Este proceso es mucho más lento que el reconocimiento a través de iris pues puede tardar unos 20 segundos en realizarse, sin embargo es mucho más preciso ya que puede obtener hasta más de 400 puntos de referencia para el proceso de identificación.

7.1.6 DISPOSITIVOS PROGRAMABLES

Ciertamente hoy en día es más factible encontrar soluciones a cualquier tipo de necesidad con sistemas embebidos, es decir, sistemas que posean la capacidad de ser bastante miniaturizados y que están creados para realizar, brindar o prestar servicios o utilidades específicas.

En este caso Los dispositivos más utilizados para estas labores son las FPGA y los micro controladores. Sin embargo, ¿cuál se debe tener en cuenta a la hora de tomar una decisión en cuanto a crear un sistema de seguridad utilizando dispositivos biométricos?

Primero, analizando las características en cuanto a costo/rendimiento, las FPGA son más costosas que los micros controladores, sin embargo cada uno de ellos posee tanto ventajas como desventajas en ciertos aspectos.

A la hora del procesamiento de información las FPGA tienen una ventaja, pues estas son capaces de procesar grandes cantidades de información y de forma paralela, es decir que pueden tener varios procesos a la vez y almacenarlo en grandes velocidades haciéndolo un dispositivo bastante eficiente, sin embargo como se ha mencionado anteriormente un problema a la hora de adquirirlo y que se debe tener en cuenta a la hora de implementar cualquier proyecto son los precios de estos los cuales son mucho más elevados que otros dispositivos por contar con funciones de programación mucho más adecuada a la medida y en la utilización de periféricos o recursos de una manera más óptima, es decir si queda haciendo falta cualquier periférico es muy fácil agregarlo, sin embargo habría que reprogramar la unidad de control u otros componentes en algunos casos y esto no resulta fácil, pues la re acomodación de funciones o tareas a veces puede llevar más tiempo que puede ser esencial para la implementación del proyecto.

En cuanto a los micros controladores la característica o ventaja más evidente es el costo, aunque lamentablemente son mucho más lentos que las FPGA, también son mucho más flexibles en cuanto a su programación y poseen características que los definen concretamente para realizar y tomar decisiones y procesos lógicos dinámicos eficientemente, sin embargo la justificación de esta velocidad es porque los micro controladores son secuenciales en sus procesos, es decir llevan cabo un tarea a la vez, aunque a veces pareciera que pueden realizar varias al mismo tiempo, realmente no, a esto se le llaman interrupciones, ya que si está haciendo una tarea o proceso y otro requiere con mayor importancia ser atendido, pausa el primero y continua con el segundo hasta terminarlo, posteriormente toma el primer proceso y continua desde donde lo dejó.

Sin embargo los dos dispositivos van de la mano a la hora de hacer grandes implementaciones pues se puede usar la FPGA para el procesamiento y almacenamiento en paralelo de información, mientras los micro controladores pueden utilizarse para tomar decisiones de la misma.

Debe tenerse en cuenta también, que muchos de los dispositivos para control de acceso vienen y cuentan ya con sistemas embebidos para tomar decisiones, por ejemplo algunos dispositivos de identificación por huellas digitales cuentan con la capacidad de almacenar varios usuarios y posteriormente poder autenticar si cuando una persona se presente esta se encuentra en su lista de usuarios, y que por medio de análisis lógicos de permiso o conceda el acceso a un recinto por medio de señales eléctricas que den movilidad a un motor o cerradura electrónica abriendo la puerta. Obviamente estos dispositivos tienen un precio en el mercado mucho mayor que otros por contar con dichas funciones, además de estar completamente garantizados por los fabricantes, sin embargo, para cuando se desee tener todo en una base de datos de acuerdo a controles de acceso masivos, lo mejor si es poder contar con alguno de los dispositivos programables anteriormente mencionados, ya que podrán servir de puente y ayuda exclusiva para los servidores que cuenten con dichas tareas de almacenamiento.

Por lo tanto como conclusión en cuanto al uso de una FPGA o un micro controlador en combinación con dispositivos de autenticación biométrica para el control de acceso a una residencia, en cuanto a costo se pueden utilizar los micro controladores tal como el arduino, pues tienen una facilidad en cuanto al desarrollo, flexibilidad, herramientas y una amplia gama de librerías y aplicaciones.

De igual manera existen tarjetas de desarrollo muy económicas en las cuales se pueden utilizar FPGA pero siguen teniendo un costo mucho mayor, pero es una muy buena opción si se quiere tener un sistema con estos dispositivos.

Y finalmente para los dispositivos completamente embebidos ya que cuentan con estas funciones directamente, es posible conectarlos directamente a un servidor o pc para almacenar los logs de los accesos y transacciones sistemáticas que se presenten en cuanto al uso que se le dé a este.

7.1.7 TOMA DE DECISIONES

En este proceso de autenticación de muestras, existen cuatro pasos para determinar la autenticidad de dicha característica biométrica: • Búsqueda de coincidencias: En esta etapa se toma la muestra biométrica del usuario y se compara con muestras almacenadas para determinar el grado de similitud o la correlación entre las muestras. • Cálculo de una puntuación: Para este paso, se calcula un valor numérico, que es el que determina el grado de similitud o la correlación entre las muestras. Este valor es calculado por algoritmos encargados de búsquedas de coincidencias que al comparar las muestras, generan las puntuaciones que determinan la similitud o correlación. • Comparación con el umbral establecido: Un umbral es un valor predefinido, en los sistemas biométricos, lo más normal es que este número sea establecido por el desarrollador del algoritmo, si la puntuación de la muestra supera el umbral, se da por entendido que son similares, es posible que las muestras no sean idénticas, es por eso que se utiliza este valor, que permite la inclusión de posibles defectos en la toma de la muestra biométrica. • Decisión: Es el resultado de la comparación entre el umbral y la puntuación de la muestra. Y puede clasificarse en uno de tres grupos: coincide, no coincide o inconcluyente, este último refleja el estado del sistema de no poder concluir si coincide la muestra o no. La mayoría de los sistemas biométricos permiten el acceso si la muestra coincide, lo restringe si no, y pide otra muestra si es inconcluyente.

7.1.8 TABLA COMPARATIVA ENTRE LAS TECNOLOGÍAS BIOMETRICAS

Características	Huella Digital	Geometría de la mano	Retina	Iris	Rostro	Voz
Confiabilidad	Muy alta	Alta	Muy Alta	Alta	Alta	Media
Usabilidad	Alta	Alta	Baja	Media	Alta	Media
Precisión	Alta	Alta	Muy Alta	Muy Alta	Media	Media
Costo	Bajo	Bajo	Muy Alto	Muy Alto	Medio	Medio
Estabilidad a largo plazo	Muy Alta	Alta	Media	Media	Media	Medio
Aceptación	Alta	Alta	Media	Media	Baja	Media
Problemas de Adquisición de información	Resequedad, Edad, Suciedad	Heridas, Edad	Anteojos	Poca Luz, Problemas de salud de la visión (cataratas)	Luz, Edad, Anteojos, Cabello, Cabello facial.	Ruido Ambiental, Temperatura, Resfriados, Disfonía.
Velocidad	Muy Alta	Alta	Baja	Media	Media	Baja

Las características que se han tenido en cuenta para hacer el análisis correspondiente y en el cual fue basado el cuadro comparativo se describirán a continuación:

• Usabilidad: Algunos dispositivos biométricos no son muy amigables, un ejemplo claro de esto, es la dificultad de usuarios sin experiencia de alinear su cabeza con el dispositivo para la creación de plantillas faciales.

• Confiabilidad: Las dos causas principales que pueden afectar los datos biométricos son: el tiempo y las condiciones ambientales. Las características pueden cambiar dependiendo de la edad. Las condiciones ambientales pueden incidir directamente en el rasgo biométrico, por ejemplo, cuando un dedo tiene una herida o una cicatriz, otro ejemplo puede ser el ruido de fondo cuando utilizamos dispositivos de reconocimiento de voz.

• Precisión: Los proveedores de tecnologías usualmente miden la precisión de los dispositivos biométricos en dos métodos: falsa aceptación y falso rechazo. Ambos métodos se enfocan en la habilidad del sistema en permitir la entrada de usuarios determinados. Estas medidas pueden varias significantemente dependiendo de la forma en que se ajuste la sensibilidad del mecanismo que califica la muestra biométrica. Por ejemplo, se puede requerir que las medidas sean más estrictas entre las medidas de la geometría de la mano y la plantilla de usuario (se incremente la sensibilidad). Esto probablemente disminuya la tasa de falsa aceptación, pero al mismo tiempo puede incrementar la tasa de falso rechazo, por eso se debe tener cuidado para entender como los proveedores acotan los valores de las dos tasas.

• Costo: Este parámetro se refiere al costo monetario del dispositivo, se debe tener en cuenta que puede ser subjetivo, depende del país, como del distribuidor, y del tipo de dispositivo, de características como lo pueden ser: Dispositivo de captura. El desempeño de procesamiento para mantener la base de datos. Búsqueda y pruebas del sistema biométrico. Instalación, incluyendo valor de la implementación. Montaje, instalación, conexión y costos de sistemas de integración de usuarios. Mantenimiento del sistema.

• Estabilidad a largo plazo: Las organizaciones consideran la estabilidad de los dispositivos, incluye madurez de la tecnología, grado de estandarización, nivel de apoyo de proveedores y gobierno, cuota de mercado y otros factores de soporte. La madurez y la estandarización de las tecnologías usualmente son de estabilidad fuerte.

• Aceptación: generalmente es la aceptación de los usuarios conforme a la tecnología. Algunas culturas o sociedades no les gustan algunos de estos dispositivos porque arremeten contra su identidad, es por ello que depende de algunos sectores, estos dispositivos pueden ser de mejor aceptación que en otros.

• Problemas de adquisición de información: Los factores que pueden repercutir en la toma de información biométrica del individuo, por lo tanto aparecerán errores de lectura y no se podrá identificar a los usuarios que hagan uso del dispositivo. Estos problemas usualmente son generados por causas externas como condiciones climáticas o problemas fisiológicos que inhabiliten a los usuarios a identificarse plenamente.

• Velocidad: Es el tiempo que se demora el dispositivo en procesar la información, en dar acceso o negarlo, en la actualidad esta característica es una de las más importantes, las personas se aburren o no aceptan algo que sea lento, desean las cosas en ese mismo instante, un dispositivo que se demore más de un par de segundos, se vuelve un dispositivo poco aceptado e incómodo.

8. CONCLUSIONES

Para mejorar considerablemente la seguridad de una residencia, se puede aplicar y alcanzar este objetivo utilizando efectivamente un sistema de seguridad implementado sobre herramientas que utilicen tecnología biométrica, y que de acuerdo al análisis correspondiente que se le ha hecho a diferentes dispositivos que encierran las diferentes técnicas en estas modalidades se puede llegar a la conclusión que en cuanto a costo/beneficio se pueden elegir los lectores de huellas digitales, ya que es una tecnología bastante utilizada y que ha estado sufriendo mejorías constantes las cuales ayudan a solventar los diferentes problemas que presentaban a la hora de adquirir la información biométrica de los usuarios, como la suciedad, cicatrices en los dedos, etc. Y que en comparación con demás dispositivos posee un costo menor que los demás.

Si se desea crear un sistema apuntando hacia la economía, se pueden utilizar lectores de huellas digitales, que conectados en combinación con un microprocesador programado adecuadamente dentro de un módulo cercano la puerta de acceso de la vivienda puede conceder el acceso a los usuarios que estén registrados, sin embargo estos lectores al ser tan baratos no poseen las características contra los daños ocasionados por estar a la intemperie, sin embargo son una muy buena opción, en cuanto a los costos.

Por el contrario al utilizar los dispositivos que cuentan con características superiores en cuanto al acabado, durabilidad y que cuenten con tecnologías que mejoren la funcionalidad de reconocimiento evitando los problemas anteriormente mencionados, aunque al ser más costosos tienen la ventaja de tener durabilidad, eficiencia y usabilidad para cada usuario o individuo que requiera el sistema. De igual manera estos dispositivos pueden ir sujetos a microprocesadores, sin embargo algunos de ellos cuentan con sistemas embebidos de memoria y procesamiento con los cuales no se requieren combinar ni con FPGA o micro

procesadores, de esta manera el dispositivo en forma “Stand-Alone” puede proveer el servicio de autenticación y que instalado correctamente en la entrada de una casa puede dar el acceso a los individuos siempre y cuando estos se encuentren registrados en él.

De igual forma si se requiere llevar un log o transacciones de las entradas que se han llevado durante el día, o que el sistema tenga más servicios a nivel de domótica, sí es más indispensable contar con dichos dispositivos programables, pues con estos es más fácil poder integrar otros dispositivos si se tienen ideas de accesibilidad como dispositivos móviles, sin embargo estrictamente para hacer lo que se necesita en cuanto a restringir y contar con un control de acceso a un hogar o residencia utilizando tecnología biométrica, es la mejor elección por la fiabilidad, costo y los beneficios descritos.

9. BIBLIOGRAFIA

[1]. SEGURIDAD IMPERIO LTDA. Modalidades de Hurtos a Residencias. [En línea]<http://www.seguridadimperio.com/vigilancia/privada/seguridad_fija-modalidades_de_hurtos_a_residencias> [Citado el 19 de marzo de 2013]

[2]. Departamento encargado de las estadísticas en Colombia (DANE). Encuesta de convivencia y seguridad ciudadana. [En línea] <http://www.dane.gov.co/files/investigaciones/poblacion/convivencia/Pres_ecsc.pdf> [Citado el 19 de marzo de 2013]

[3]. VITERBO, Pedro. Los bancos incrementan la seguridad con biometría. En: Revista Dintel [en línea]. (septiembre 2009). Disponible en: <http://www.revistadintel.es/Revista/Numeros/Numero1/Seguridad/Publica/Viterbo.pdf>**[Citado el 19 de marzo de 2013]**

[4]. DOINTECH. Video Vigilancia IP: Sistemas de seguridad con cámaras IP. [En línea] <http://www.dointech.com.co/video-vigilancia-ip.html>**[Citado el 19 de marzo de 2013]**

[5]. TELEFONICA. Cuaderno de red de cátedras Telefónica. Sistemas Biométricos. [En línea] <http://www.rcysostenibilidad.telefonica.com/blogs/documentoscatedras/files/2012/07/Catedra_telefonica_Sistemas_Biometricos.pdf> [Citado el 19 de marzo de 2013]

[6]. Evaluación de Sistemas de Reconocimiento Biométrico, Virginia Espinosa Duró, [En línea]<http://www.jcee.upc.es/JCEE2001/PDFs%202000/13ESPINOSA.pdf**>[Citado 12 octubre de 2013]**

[7]. Biometría [En línea]. <http://www.biometrics.gov/**> [Citado 12 octubre de 2013]**

[8] Andrew Beng Jin Teoh; Kar-Ann Toh; IEEE Expore ; 2008; ISBN: 978-1-4244-17-18-6. Disponible en: <http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=4582898>

[9] Willems, Frans M.J; Ignatenko. Tanya; MM&Sec '10, Proceedings of the 12th ACM workshop on Multimedia and Security; páginas 63-66; ISBN: 978-1-4503-0286-9; 2010, Disponible en: http://delivery.acm.org.ezproxy.utp.edu.co/10.1145/1860000/1854243/p63-willems.pdf?ip=200.21.217.136&id=1854243&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF155474BF1484A332833151FA85FF6292E&CFID=252365920&CFTOKEN=21508316&__acm__=1381273879_a8998f27c24116709792765e9314060d

[10]. Khairwa, A.; Abhishek, K. ; Prakash, S. ; Pratap, T.A comprehensive study of various biometric identification techniques; páginas 1-6; ISBN: 13257576; 26-28 Julio 2012; Disponible en: http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=6396051

[11].Saifullah, S.; Khawaja, A. ; Hamza ; Arsalan ; Maryam ; Anum; Keyless car entry through face recognition using FPGA; Páginas 224-227; ISBN: 978-1-4244-9087-5; 9-10 Oct. 2010; Disponible en:

http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5654862

[12]. Zhen Liang; Fei Tan ; Zheru Chi. Video-based biometric identification using eye tracking technique; Páginas: 728-733; ISBN: 978-1-4673-2192-1; 12-15 Ago. 2012; Disponible en: http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=6335584

[13]. Al-Hussain, Arwa; Al-Rassab, Iehab. Procedings of the 8th International Conference on Advances in Mobile Computing and Multimedia, paginas 447-452, 2010, ISBN: 978-1-4503-0440-5, Disponible en: http://delivery.acm.org.ezproxy.utp.edu.co/10.1145/1980000/1971596/p447-al-hussain.pdf?ip=200.21.217.136&id=1971596&acc=ACTIVE%20SERVICE&key=C2716FEBFA981EF155474BF1484A332833151FA85FF6292E&CFID=252365920&CFTOKEN=21508316&__acm__=1381274715_80c44936c83f163bbcee1e984c28cd2c

[14]. Huaqiang Huang; Chen Hu ; Jianhua He; A security embedded system base on TCM and FPGA; Páginas 605 – 609; ISBN: 978-1-4244-4520-2; 8-11 Ago. 2009; Disponible en: http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5234634

[15]. Ehliar, A; Liu, D.An ASIC perspective on FPGA optimizations; Páginas 218 – 223; ISBN: 978-1-4244-3892-1; Ago. 31 2009-Sept. 2 2009; Disponible en:http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=5272311&tag=1

[16]. La firma electrónica digital en Venezuela, Quintero, Héctor R Peñaranda,2011,http://search.proquest.com.ezproxy.utp.edu.co/docview/922768241/140B329C6C6159EB542/4?accountid=45809

[17]. Llega a Chile el revolucionario sistema de firmas digitales a través de la tecnología biométrica: [Source: NoticiasFinancieras], Septiembre 15 del 2013,http://search.proquest.com.ezproxy.utp.edu.co/docview/1432362393/140BD6B256C6324B41D/4?accountid=45809

[18]. Título original: A biometric-based security for data authentication in Wireless Body Area Network (WBAN), Sofia Najwa Ramlil, Rabiah Ahmad, Mohd Faizal Abdollah, Eryk Dutkiewicz, Febrero 2013, http://ieeexplore.ieee.org.ezproxy.utp.edu.co/xpl/articleDetails.jsp?tp=&arnumber=6488348&sortType%3Ddesc_p_Publication_Year%26queryText%3Dbiometric+security

[19]. Título original: Soft Biometrics and Its Application to Security and Business, Masatsugu Ichino, Yasushi Yamazaki, 2013, http://ieeexplore.ieee.org.ezproxy.utp.edu.co/stamp/stamp.jsp?tp=&arnumber=6603525