UNIVERSIDAD CATOLICA DE SANTIAGO DE GUAYAQUIL

Facultad de Educación Técnica para el Desarrollo

Tesis de Grado

Previo a la obtención del título de

INGENIERO EN TELECOMUNICACIONES
Mención en Gestión Empresarial

Tema

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE INMÓTICA PARA EL EDIFICIO ADMINISTRATIVO DE LA FACULTAD TÉCNICA PARA EL DESARROLLO DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL"

Realizado por:

Byron Enrique Alvarado Zambrano

Carlos Jesús Landeta Rodríguez

José Luis Sánchez Jiménez

Roberto Andrés Castro Arreaga

Director

Ing. Luis Sánchez

Guayaquil – Ecuador
2010

TESIS DE GRADO
Título

"ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE INMÓTICA PARA EL EDIFICIO ADMINISTRATIVO DE LA FACULTAD TÉCNICA PARA EL DESARROLLO DE LA UNIVERSIDAD CATÓLICA DE SANTIAGO DE GUAYAQUIL"

Presentada a la Facultad de Educación Técnica para el Desarrollo, Carrera de Ingeniería en Telecomunicaciones de la Universidad Católica de Santiago de Guayaquil.

Por:

Byron Enrique Alvarado Zambrano
Carlos Jesús Landeta Rodríguez
José Luis Sánchez Jiménez
Roberto Andrés Castro Arreaga

Para dar cumplimiento con uno de los requisitos para optar por el Título de:

INGENIERO EN TELECOMUNICACIONES
Mención en Gestión Empresarial

Miembros del Tribunal

Ing. Héctor Cedeño **A**.
Decano de la Facultad

Ing. Pedro Tutiven López
Director de Carrera

Ing. Luis Sánchez
Director de Tesis

Dr. Kléber López Parrales
Coordinador Administrativo

Ing. Víctor del Valle Ramos
Coordinador Académico

AGRADECIMIENTO

Al llevar a cabo ésta última labor investigativa, sentimos necesidad de agradecer:

A Dios por su protección y bendiciones en el desarrollo de nuestro proyecto de investigación.

A la Universidad Católica Santiago de Guayaquil (UCSG), por habernos dado la oportunidad de realizar un trabajo de investigación.

A nuestras familias y amistades por el aliento, comprensión, la ayuda invalorable y el apoyo incondicional que siempre nos han demostrado durante la ejecución del proyecto de investigación.

Al Decano Ing. Héctor Cedeño, al Director de Carrera, Ing. Pedro Tutiven y al Coordinador Académico Ing. Víctor del Valle, quienes siempre nos dieron su apoyo para desarrollar ejecutar nuestro proyecto de investigación.

A nuestro Director de Tesis, Ing. Luis Sánchez., por su colaboración y orientación durante la investigación.

Y a todas las personas que de una forma u otra, han hecho posible la realización de esta obra. A todos ellos nuestra gratitud.

DEDICATORIA

Dedicamos este trabajo a Dios y a nuestras respectivas familias quienes son nuestra fuerza inspiradora, quienes en todo momento supieron apoyarnos en nuestros estudios, teniendo tolerancia y paciencia para sacar a luz este trabajo investigativo y poderlos culminar con éxito.

A nuestro Director de Tesis, porque gracias a sus conocimientos brindados, nos ha ayudado a la finalización de este proyecto de investigación.

A los docentes de Telecomunicaciones.

Byron Enrique Alvarado Zambrano
Carlos Jesús Landeta Rodríguez
José Luis Sánchez Jiménez
Roberto Andrés Castro Arreaga

RESUMEN

La presente tesis contempla un estudio de la Inmótica que utiliza la más alta tecnología en edificaciones convirtiéndolas en inteligentes. Edificios pensante, que controlan básicamente el acceso a las oficinas administrativas, para aumentar el confort y la seguridad de los directivos hacia las mismas y en pocas palabras se dice que es la automatización centros educativos, hoteleros, empresariales y similares, ofreciendo servicios avanzados de la actividad y de las telecomunicaciones. Con control automatizado, gestión y mantenimiento de los distintos subsistemas o servicios del edificio, de forma óptima e integrada; diseñados con suficiente flexibilidad como para que sea sencilla y económicamente rentable la implantación de futuros sistemas.

Con esta información recopilada por parte de todos los integrantes del grupo de tesis, proporcionarán al alumno de Ingeniería en Telecomunicaciones un conocimiento práctico de la Inmótica aplicada al Control de Acceso a través de Cerraduras Biométricas, esto se lo explicará con detalles a medida que avancemos con los capítulos.

La información aquí presentada proviene de una amplia gama de fuentes, donde destacan principalmente los textos especializados en control de acceso a través de cerraduras biométricas, de los fabricantes de las mismas, obtenidos de Internet y de los manuales de equipos que se contemplan para el desarrollo de la implementación.

INDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

INTRODUCCIÓN

Por definición la INMOTICA utiliza la más alta tecnología en edificaciones convirtiéndolas en inteligentes. Edificios pensantes que a base de una central inteligente (generalmente una PC, Un sistema embebido), controla básicamente todos los sistemas instalados, para reducir el consumo de energía y aumentar el confort y en pocas palabras se dice que es la automatización de edificios corporativos, educativos, hoteleros, empresariales y similares.

Pero cuando se puede decir que un edificio es inteligente esta es la pregunta más difícil y se pueden dar respuestas para todos los gustos. Una sería que la inteligencia de un edificio empieza cuando, una vez automatizado, es dotado de un sistema que contiene aplicaciones de alto nivel que gestionan dicha automatización y proporcionan servicios más avanzados.

Una definición más técnica sería definir como edificio inteligente a aquel que incorpora sistemas de información en todo el edificio. Ofreciendo servicios avanzados de la actividad y de las telecomunicaciones. Con control automatizado, monitorización, gestión y mantenimiento de los distintos subsistemas o servicios del edificio, de forma óptima e integrada; local y remotamente, diseñados con suficiente flexibilidad como para que sea sencilla y económicamente rentable la implantación de futuros sistemas.

CAPITULO 1

ESTUDIO DEL SISTEMA DE INMÓTICA

1.1 PLANTEAMIENTO DEL PROBLEMA

Enfocándonos en el tema, notamos que en la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil, no existe ningún tipo sistema de Inmótica que esté aplicada al Control de Acceso a las oficinas administrativas que cumpla con los enunciados de la Inmótica, y lo que existen son sistemas aislados que funcionan en ciertos lugares estratégicos de manera independiente.

Entre las principales actividades que se pueden mejorar en el edificio administrativo tenemos las siguientes:

- **Falta de Control de Accesos:**

  Notamos que en las oficinas de los directivos no existe ningún tipo de control de acceso. Además en la puerta principal, el ingreso no ofrece ningún tipo de seguridad y por lo regular la puerta permanece abierta durante todo el día.

  Este es un gran problema, más que nada por asuntos de seguridad ya que se está dando facilidades en el ingreso, y no sólo a nivel docente y de estudiantes, sino que puede ingresar alguna tercera personal indeseable que puede inclusive poner en riesgo nuestras vidas, ya que se pueden presentar varios tipos de situaciones con las facilidades del ingreso.

1.2 JUSTIFICACIÓN

En la actualidad, la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil, se encuentra con algunos problemas de Gestión de varios recursos en las oficinas de las áreas administrativas.

Con esta investigación se pretende satisfacer, la problemática actual de control de acceso, llevando a cabo 2 etapas:

- Realizar un estudio acerca del problema y realizar una investigación profunda acerca de los diferentes medios que nos permitan desarrollar nuestro tema planteado.
- Desarrollar un prototipo de Hardware, que permita llevar a cabo tareas tales como:

Control de Acceso Mediante Biometría a las oficinas Administrativas.

En el desarrollo de este proyecto se aplicará gran parte de los conocimientos adquiridos a lo largo de la carrera de Ingeniería en Telecomunicaciones consiguiendo de esta forma un mejoramiento de la imagen institucional de la Facultad en la que se va a contar con tecnología de punta.

Los beneficios que obtendremos van a representar un sustancial adelanto para la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil.

En el control de accesos a las oficinas muchas veces se manejan a través de una persona que está en la puerta de ingreso y en otras ocasiones no existe nadie. Este proyecto permitirá automatizar y sistematizar el proceso de control de acceso a los

directivos a sus respectivas oficinas administrativas de la Facultad Técnica para el Desarrollo.

Con nuestro tema pretendemos realizar un Sistema de Inmótica, con un tiempo de vida aceptable, escalable, confiable y con interfaces amigables.

Este prototipo además de servir como base para el desarrollo de futuros proyectos de esta índole, es un valor agregado para el área de innovación tecnológica de Ingeniería en Telecomunicaciones, debido a lo innovador y complejidad que conlleva la implementación y desarrollo de nuestro tema propuesto. Llevando a cabalidad la realización de este proyecto se puede generar un valor adicional a los conocimientos adquiridos durante la carrera, establecer unas bases que permitan el desarrollo integral de un profesional que se desempeñe a nivel laboral en las diferentes áreas de la ingeniería.

1.3 HIPÓTESIS

El sistema de control de acceso a través de huella digital es lo que usaremos muy pronto a nivel de hogar y empresarial por la seguridad que nos brinda con la tecnología de la huella biométrica, a la vez serán cada día más accesibles y muy económicos, el bajísimo consumo de corriente hacen que sea una tecnología ganadora, dentro de la implementación, diseño y construcción en un proyecto inmótico. Estos equipos van a funcionar con distintos métodos de apertura, los cuales los iremos conociendo más adelante.

1.4 OBJETIVO GENERAL

- Implementar un Sistema de Inmótica aplicado al Control de Acceso a las oficinas del edificio administrativo de la Facultad de Educación Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil, utilizando tecnología de reconocimiento biométrico de huellas dactilares.

1.5 OBJETIVOS ESPECIFICOS

- Mejorar la seguridad del acceso a las oficinas administrativas.
- Mejorar el ámbito y confort de trabajo.
- Implementar un sistema de reconocimiento biométrico que permita restringir el acceso a personas no autorizadas a las oficinas asignadas a los funcionarios administrativos de la Facultad de Educación Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil.
- Registrar en el sistema la información de reconocimiento de las huellas dactilares de los usuarios.

CAPITULO 2

SISTEMA DE INMÓTICA – CONTROL DE ACCESO

2.1 DEFINICIÓN DE INMÓTICA

Por inmótica entendemos la incorporación al equipamiento de edificios de uso terciario o industrial (oficinas, edificios corporativos, hoteleros, empresariales y similares), de sistemas de gestión técnica automatizada de las instalaciones, con el objetivo de reducir el consumo de energía, aumentar el confort y la seguridad de los mismos.

Entenderemos que un edificio es "inteligente" si incorpora sistemas de información en todo el edificio, ofreciendo servicios avanzados de la actividad y de las telecomunicaciones. Con control automatizado, monitorización, gestión y mantenimiento de los distintos subsistemas o servicios del edificio, de forma óptima e integrada, local y remotamente. Diseñados con suficiente flexibilidad como para que sea sencilla y económicamente rentable la implantación de futuros sistemas.

Bajo este nuevo concepto se define la automatización integral de inmuebles con alta tecnología. La centralización de los datos del edificio o complejo, posibilita supervisar y controlar confortablemente desde una PC, los estados de funcionamiento o alarmas de los sistemas que componen la instalación, así como los principales parámetros de medida. La Inmótica integra la domótica interna dentro de una estructura en red.

En la actualidad, la mayor parte de los sistemas eléctricos o electrónicos instalados en edificios terciarios adolecen un problema fundamental: su ineficacia. El primer y

más evidente resultado de esta ineficiencia es el gasto innecesario y excesivo de todo tipo de recursos-energéticos, hídricos, etc., incidiendo no sólo de forma económica sino también medioambiental. Esta falta de control y gestión genera también problemas de otra índole como incomodidades, incapacidades para atender desviaciones energéticas, derroche de energía y posiblemente falta de condiciones óptimas para atender situaciones de emergencia.

La gestión técnica de las instalaciones cobra aún más sentido ya que eventos detectados en diferentes zonas pueden requerir de la toma de medidas y/o acciones sobre la propia instalación al instante para permanecer funcionando correctamente de forma transparente al usuario.

Por ello la gestión técnica de este tipo de instalaciones cobra una máxima relevancia tanto en la optimización de los recursos del centro como en el bienestar y la comodidad de los usuarios y sus trabajadores.

Las ventajas de un sistema de control en edificios y grandes instalaciones son muy numerosas. Las más destacables son:

- Ahorro energético de hasta un 40%.
- Ahorro en servicios de mantenimiento
- Gestión del personal del edificio
- Supervisión en tiempo real de eventos
- Gestión de históricos y tiempos de funcionamiento
- Aviso de averías
- Avisos de mantenimiento preventivo
- Alarmas técnicas

- Telegestión remota
- Mejora de la eficiencia del trabajador o del edificio.
- Aumento del confort de los usuarios y estética.
- Detección y gestión eficaz de la seguridad en el complejo

2.2 CONTROL DE ACCESO A TRAVÉS DE HUELLAS BIOMÉTRICAS

Los sistemas inmóticos se van introduciendo poco a poco en la vida cotidiana de las personas facilitando las tareas domésticas y de oficina, pero además combinan la comodidad con la seguridad biométrica.

Así, además de dotar a un edificio de un control de acceso biométrico seguro y fiable, se evita la pérdida de llaves y sus consecuencias.

Esta aplicación ha sido llevada a cabo con equipos biométricos.

El control de acceso biométrico a una oficina o vivienda particular se realiza mediante la instalación de un terminal de control de acceso biométrico. El sensor de huella dactilar se integra en la pared o en el marco de la puerta de acceso a la oficina y la electrónica de control de acceso se coloca en un falso techo o se empotra en la pared dentro de una caja eléctrica, de modo que queda oculta y a resguardo de posibles manipulaciones.

A través de un software integrado en la cerradura donde nos permite la gestión de usuarios se dan de alta a las personas a las que se permite el acceso a la oficina. Este sistema puede ser combinable con otro tipo de tecnologías, como el control de acceso por radiofrecuencia (RFID), pero también puede combinarse con el acceso clásico mediante una cerradura mecánica.

De esta manera, ante un posible fallo en la conexión o que el suministro eléctrico cese, queda cubierto con la posibilidad de utilizar la cerradura mecánica. Así, el sistema de lectores biométricos para oficinas siempre se instala con un sistema mecánico paralelo de alta seguridad y con puertas de alta calidad, para que el valor de seguridad que aporta el sistema biométrico quede cubierto a través de la puerta de seguridad y su cerradura altamente fiable.

Esta aplicación se ha llevado a cabo en las oficinas administrativas de la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil.

Se trata de un producto altamente adaptable a diferentes entornos y necesidades del cliente, en este caso a las necesidades ejecutivas de control de acceso a las oficinas de un edificio administrativo.

2.3 INFORMACIÓN DE LAS CERRADURAS BIOMÉTRICAS

Chapa de acero inoxidable, cuenta con tres formas de abrirse: Huella digital, clave numérica o llave de seguridad.

Su diseño con cerrojo tubular estándar (70mm o 60 mm) permite una fácil instalación y el funcionamiento con una contra-chapa electrónica si se desea.

Utiliza 4 baterías AA con duración promedio de 12 meses. Tiene una función que avisa que la batería esta baja, a partir de ese momento tiene una duración de entre 20 y 30 aperturas para cambiarlas.

Es adaptable de derecha o izquierda.

Figura 2-1 Cerradura biométrica

2.3.1 CARACTERÍSTICAS DE LAS CERRADURAS BIOMÉTRICAS

- Modos de apertura: Número de identificación personal, huella digital y llave mecánica convencional.
- Pestillo de fácil instalación.
- Las huellas digitales pueden ser registradas o borradas directamente en la cerradura.
- Hasta 99 usuarios. 3 usuarios MASTER con capacidad de dar de alta o borrar usuarios.
- Añadir un nuevo usuario en el segundo.
- 4 pilas alcalinas AA incluidas.
- Cada usuario puede elegir un código de número personalizado.
- Pitidos de advertencia y luz indicadora de color rojo cuando la batería está baja.
- Entrada de alimentación externa de 9V si la batería es plana.

Figura 2-2 Panel de la cerradura biométrica

2.3.2 FUNCIONES DEL TABLERO DE LAS CERRADURAS BIOMÉTRICAS

- Activación de la chapa al acercar el dedo al lector.
- Activación por medio de clave numérica.
- Modificación del NIP.
- Borrado de huellas individuales..
- Única apertura normal para reconocimiento de usuarios

2.3.3 TIPOS DE CERRADURAS

Según su forma y método de instalación, las cerraduras pueden clasificarse en 3 grandes grupos: cilíndricas (o tubulares), de sobreponer (o de parche) y de embutir (o de caja). Dentro de cada grupo hay variados modelos que combinan distintas funciones y líneas de diseño.

2.3.3.1 Cerraduras cilíndricas:

Están compuestas por una caja cilíndrica con un eje de rotación perpendicular a la hoja de la puerta. El mecanismo central de la cerradura se encuentra al interior de la puerta. Pueden o no tener llave. Las que no utilizan llave reciben el nombre de

cerraduras de simple paso. También pueden combinar llave por fuera y seguro por dentro, o utilizar llave por ambos lados. Son muy fáciles de instalar y de una presentación limpia y agradable. Se utilizan principalmente en puertas de interior.

Figura 2-3 Tipos de cerraduras - cilíndricas

2.3.3.2 Cerraduras de sobreponer:

Son aquellas que van instaladas sobre la puerta, dejando visible el cuerpo de la cerradura. El cilindro se embute en éste, adosado por la cara opuesta de la puerta. La caja que aloja el picaporte y el pestillo va colocada en el marco. Por ser una cerradura que queda a la vista, al momento de la elección resulta importante tener en cuenta características tales como tamaño, forma y materialidad. Se colocan habitualmente en puertas metálicas, rejas y también en puertas delgadas cuyo espesor no permite la instalación de una cerradura embutida en su interior.

Figura 2-4 Tipos de cerraduras – De sobreponer

2.3.3.3 Cerraduras de embutir: La caja de la cerradura es de menor espesor exterior y es más alargada en sentido vertical ya que tiene que ir completamente embutida en el interior de la puerta. Pueden llevar como tirador una perilla o una manilla. Suelen utilizarse en puertas interiores y combinar, al igual que en el caso de las cerraduras cilíndricas, mecanismos con o sin pestillo y llave.

Figura 2-5 Tipos de cerraduras – De embutir

Las cerraduras se fabrican para un cierto rango de espesor de puerta y una determinada distancia desde el canto de la puerta hasta el centro del mecanismo de las manillas o de los pomos (es lo que se llama "Backset"). Además, algunas se pueden instalar indistintamente al lado derecho o izquierdo de la puerta (se saca el tornillo de retención, se rota la manilla en 180º y se vuelve a poner el tornillo). Pero hay otras, cuyo diseño permite su uso sobre un solo lado de la puerta.

La variedad de diseños y estilos de cerraduras es inmensa. No sólo en cuanto a sus formas sino también a los materiales con que se fabrican. El material del pomo es clave en la duración y el buen aspecto de la cerradura a través del tiempo. Las hay de acero inoxidable, bronce pulido, envejecido o satinado; también tipo madera, pintadas y doradas; con o sin lacas de protección. En zonas húmedas, como baños o

regiones costeras, por ejemplo, se recomienda utilizar acero inoxidable en vez de los cromados o dorados típicos, que pueden verse afectados por la salinidad y humedad ambientales.

2.3.3.4 Cerraduras para puertas de casa

En casas, generalmente se utilizan cerraduras de tipo cilíndricas (tubulares). Algunas de las características requeridas son: protección **anti-taladro**; llave de punto; tener más de un par de puntos de cierre y varios pasadores (mientras más mejor). Muchas cerraduras cuentan con pitones **anti corte**, los que poseen un refuerzo adicional al centro del pitón. Algunas también incluyen un **pestillo nocturno,** un botón que se acciona desde el interior que impide que la cerradura pueda ser abierta desde afuera, incluso si se cuenta con la propia llave.

Un buen complemento son los cerrojos, simples o dobles. Los simples tienen un cilindro exterior que se abre y cierra con llave y una mariposa por el interior, que abre y cierra el cerrojo. Los dobles tienen cilindro exterior e interior, que abren y cierran sólo con llave.

Figura 2-6 Tipos de cerraduras – Para puertas de casa

2.3.3.5 Cerradura para puertas interiores

En estos casos, se recomienda utilizar cerraduras del tipo cilíndricas (tubulares) o de embutir (de caja), ya que son de menor tamaño, decorativas, simples de instalar y no estarán sometidas a pruebas exigentes en materia de seguridad.

2.3.3.6 Cerraduras para baños:

Idealmente deben funcionar sin llave, pero con un pestillo que se acciona desde el interior. Es importante que cuente con una ranura de emergencia, la que permite desbloquear el pestillo desde fuera del baño (utilizando por ejemplo una moneda o simplemente el pulgar) en caso que una emergencia lo requiera. Se recomienda elegir cerraduras de acero inoxidable ya que son más resistentes al vapor y humedad.

2.3.3.7 Cerraduras para dormitorios infantiles:

Para evitar accidentes y permitir siempre el acceso al recinto es fundamental que las puertas nunca tengan pestillos o mecanismos que bloqueen el paso hacia el interior. Las cerraduras de libre paso, es decir aquellas que funcionan sin llave ni pestillo resultan las más adecuadas en estos casos, especialmente si cuentan con pomos o manillas redondeadas.

2.3.3.8 Cerraduras para dormitorios de adultos, escritorios y salida a patios:

En caso que requieran pestillo, se sugiere utilizar el mismo tipo de cerradura recomendada para baños, es decir, con pomo exterior con ranura para entrada de emergencia y pomo interior con botón giratorio que libere y bloquee la función.

2.3.3.9 Cerraduras para cocina y recintos comunitarios:

Se recomienda utilizar cerraduras de libre paso, con mecanismos similares a los especificadas para dormitorios infantiles.

2.3.3.10 Cerraduras para puertas de garajes, portones y entradas de autos

Las cerraduras eléctricas suelen utilizarse para este propósito. Muchos modelos incluyen un "led" o luz que se enciende cuando la puerta está en movimiento y por lo tanto advierte la entrada o salida de un auto. La apertura de esta cerradura puede realizarse mediante una llave (en el caso de venir desde el exterior), de un interruptor o cordel (que se acciona desde el interior), mediante un mando a distancia o control remoto, o mediante un tarjeta magnética. Cuentan con un transformador eléctrico con protección contra cortocircuitos o sobrecalentamientos.

Figura 2-7 Tipos de cerraduras – Garajes, portones

2.3.3.11 Cerraduras para puertas correderas

Especialmente para puertas correderas se fabrica la comúnmente llamada cerradura "picoloro".

En caso de requerir un nivel de seguridad adicional, se puede complementar con un método casero, pero muy eficiente, que consiste en sobreponer un trozo de madera o metal del ancho de la hoja fija dentro del riel de la puerta cerrada, para evitar que la quiten o abran con ganzúa.

2.3.3.12 Cerraduras para puertas de cristal

Existen distintos modelos: flotantes, para adherir, fijas, desmontables, eléctricas y mecánicas.

La mayoría de las cerraduras para este propósito tienen un sólo cilindro, que funciona desde el exterior con una llave y del interior con un pestillo de vuelta de mano. El problema con las cerraduras de este tipo es que no son muy seguras, pues se abren fácilmente al romper el cristal y dar vuelta el pestillo. Por seguridad, son más recomendables las que funcionan con llave por ambos lados.

2.3.3.13 Cerraduras para puertas con marco de aluminio

Existen cerraduras especiales para instalar en puertas con marco de aluminio. Suelen tener un espesor menor que las cerraduras convencionales y cierres de 2 o 3 puntos.

2.3.3.14 Cerraduras especiales

La electrónica y tecnologías actuales han permitido desarrollar una serie de productos especiales, para cumplir con determinados propósitos específicos.

2.3.3.15 Cerraduras "sin llaves" para hoteles, oficinas y empresas:

Responden a la necesidad de controlar los accesos de manera eficiente sin la utilización de llaves, que podrían ser copiadas fácilmente. Funcionan con un código o "password", que puede ser digitado manualmente o utilizando una tarjeta magnética, o también mediante una combinación de ambas (además de las llaves convencionales).

Figura 2-8 Tipos de cerraduras – Para hoteles, oficinas y empresas

2.3.3.16 Cerraduras biométricas:

Son cerraduras personalizadas, que se abren simplemente al tocarlas. Poseen un lector de huellas digitales (sensor óptico) que funciona de una manera muy sencilla: una luz roja ilumina el dedo. El reflejo de la luz en el dedo es diferente por la humedad distinta que hay en las zonas altas y bajas de la huella dactilar. La imagen refleja nítidamente la huella dactilar que es captada por una cámara CCD que digitaliza los datos recibidos. Estos son comparados con las huellas registradas y guardadas en forma de secuencia numérica. Sólo en caso de que se obtenga una correspondencia con estas, el usuario es autorizado y la cerradura se acciona. En Homecenter Sodimac de Parque Arauco puede encontrar un modelo que funciona

indistintamente con clave, con huellla o con llave, que es capaz de almacenar hasta 138 huellas dactilares diferentes y funciona con sólo 4 baterías alcalinas. Viene en opciones izquierda y derecha, en acero inoxidable o PVD dorado.

2.3.3.17 Cerraduras "inteligentes":

Utilizan llaves y cilindros "inteligentes", esto significa que sólo usted puede validar la copia de la llave mediante un circuito electrónico incorporado al cilindro de la cerradura.

2.3.3.18 Cerraduras para puertas de emergencia y de escape:

Resultan adecuadas para este propósito las llamadas "**Barras Antipánico**", que permiten la apertura instantánea de la puerta en caso de emergencia, mediante una simple presión en cualquier parte de la barra, independiente de la forma de cierre de la cerradura. Hay modelos para puertas de 1 y 2 hojas. La Barra Antipánico puede combinarse con la colocación de una manilla con llave por el exterior de la puerta, esto permite restringir el paso del exterior al interior sin interferir en el escape de emergencia.

2.3.3.19 Cerraduras para puertas blindadas: Son aún más resistentes que las cerraduras de seguridad. Cuentan con protección antibalas, antitaladro, antiganzúa y pitones verticales y horizontales. Utilizan llaves fabricadas a medida e imposibles de copiar.

2.4 PROCESO DE INSTALACIÓN

Las cerraduras se deben instalar sobre puertas terminadas y en la última etapa de la obra, una vez que estén secas las pinturas y completamente terminados los pisos. Para un funcionamiento más suave, se recomienda lubricar los mecanismos interiores de la cerradura al momento de su instalación.

En caso de repintar la puerta, es conveniente sacar la cerradura para evitar que se manche. No es recomendable instalar huinchas adhesivas sobre las cerraduras, podría afectar la laca protectora.

Para limpiar la cerradura usar sólo paño humedecido con agua. Nunca usar elementos abrasivos, alcohol, barnices, removedores de pintura, objetos filosos como cuchillos, llaves de puertas, colgadores de ropa, etc: pueden deteriorar la capa de laca protectora y empezar así un proceso de corrosión del metal.

Figura 2-9 Olvido de llaves

CAPITULO 3

ESTUDIO DE LA TECNOLOGÍA DE LA HUELLA BIOMÉTRICA

3.1 BIOMETRÍA

Figura 3-1 Estudio de la Biometría

La biometría es el estudio de métodos automáticos para el reconocimiento único de humanos basados en uno o más rasgos conductuales o físicos intrínsecos. El término se deriva de las palabras griegas "bios" de vida y "metron" de medida.

La "biometría informática" es la aplicación de técnicas matemáticas y estadísticas sobre los rasgos físicos o de conducta de un individuo, para “verificar” identidades o para “identificar” individuos.

En las tecnologías de la información (TI), la **autentificación biométrica** se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Figura 3-2 Aplicación para control de visitas.

En Disney World, se toman medidas biométricas de los visitantes con pase de varios días para asegurarse de que el pase es usado por la misma persona todos los días.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento.

3.2 HISTORIA

La biometría no se puso en práctica en las culturas occidentales hasta finales del siglo XIX, pero era utilizada en China desde al menos el siglo XIV. Un explorador y escritor que respondía al nombre de Joao de Barros escribió que los comerciantes chinos estampaban las impresiones y las huellas de la palma de las manos de los niños en papel con tinta. Los comerciantes hacían esto como método para distinguir entre los niños jóvenes.

En Occidente, la identificación confiaba simplemente en la "memoria fotográfica" hasta que Alphonse Bertillon, jefe del departamento fotográfico de la Policía de París, desarrolló el sistema antropométrico (también conocido más tarde como Bertillonage) en 1883. Éste era el primer sistema preciso, ampliamente utilizado científicamente para identificar a criminales y convirtió a la biométrica en un campo de estudio. Funcionaba midiendo de forma precisa ciertas longitudes y anchuras de la cabeza y del cuerpo, así como registrando marcas individuales como tatuajes y cicatrices. El sistema de Bertillon fue adoptado extensamente en occidente hasta que aparecieron defectos en el sistema - principalmente problemas con métodos distintos de medidas y cambios de medida. Después de esto, las fuerzas policiales occidentales comenzaron a usar la huella dactilar - esencialmente el mismo sistema visto en China cientos de años antes.

En estos últimos años la biométrica ha crecido desde usar simplemente la huella dactilar, a emplear muchos métodos distintos teniendo en cuenta varias medidas

físicas y de comportamiento. Las aplicaciones de la biometría también han aumentado - desde sólo identificación hasta sistemas de seguridad y más.

La idea para usar patrones de iris como método de identificación fue propuesto en 1936 por el oftalmólogo Frank Burch. Para los 1980's la idea ya había aparecido en películas de James Bond, pero permanecía siendo ciencia ficción.

En 1985 los Doctores Leonard Flom y Aran Safir retomaron la idea. Su investigación y documentación les concedió una patente en 1987. En 1989 Flom y Safir recurrieron a John Daugman para crear algoritmos para el reconocimiento de iris. Estos algoritmos, patentados por Daugman en 1994 y que son propiedad de Iridian Technologies, son la base para todos los productos de reconocimiento de iris.

En 1993 la Agencia Nuclear de Defensa empezó a trabajar con IriScan, Inc. para desarrollar y probar un prototipo. 18 meses después el primer prototipo se completó y esta disponible comercialmente.

3.3 FUNCIONAMIENTO Y RENDIMIENTO

En un sistema de Biometria típico, la persona se registra con el sistema cuando una o más de sus características físicas y de conducta es obtenida, procesada por un algoritmo numérico, e introducida en una base de datos. Idealmente, cuando entra, casi todas sus características concuerdan; entonces cuando alguna otra persona intenta identificarse, no empareja completamente, por lo que el sistema no le permite el acceso. Las tecnologías actuales tienen tasas de error que varían ampliamente (desde valores bajos como el 60%, hasta altos como el 99,9%).

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falso positivo (*False Acceptance Rate* o FAR), la tasa de falso negativo (*False NonMatch Rate* o FNMR, también *False Rejection Rate* o FRR), y el fallo de tasa de alistamiento (*Failure-to-enroll Rate*, FTR o FER).

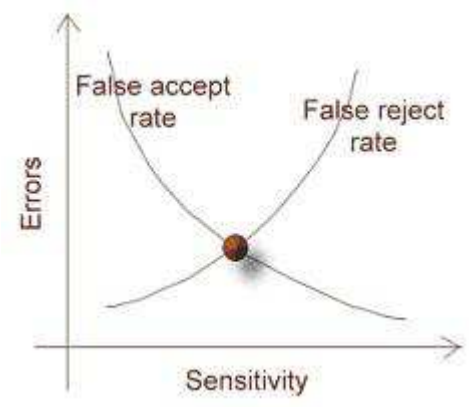


Figura 3-3 Rendimiento

En los sistemas biométricos reales el FAR y el FRR puede transformarse en los demás cambiando cierto parámetro. Una de las medidas más comunes de los sistemas biométricos reales es la tasa en la que el ajuste en el cual acepta y rechaza los errores es igual: la tasa de error igual (*Equal Error Rate* o EER), también conocida como la tasa de error de cruce (*Cross-over Error Rate* o CER). Cuanto más bajo es el EER o el CER, se considera que el sistema es más exacto.

Las tasas de error anunciadas implican a veces elementos idiosincrásicos o subjetivos. Por ejemplo, un fabricante de sistemas biométricos fijó el umbral de aceptación alto, para reducir al mínimo las falsas aceptaciones; en la práctica, se permitían tres intentos, por lo que un falso rechazo se contaba sólo si los tres intentos resultaban fallidos (por ejemplo escritura, habla, etc.), las opiniones pueden variar

sobre qué constituye un falso rechazo. Si entro a un sistema de verificación de firmas usando mi inicial y apellido, ¿puedo decir legítimamente que se trata de un falso rechazo cuando rechace mi nombre y apellido?

A pesar de estas dudas, los sistemas biométricos tienen un potencial para identificar a individuos con un grado de certeza muy alto. La prueba forense del ADN goza de un grado particularmente alto de confianza pública actualmente (ca. 2004) y la tecnología está orientándose al reconocimiento del iris, que tiene la capacidad de diferenciar entre dos individuos con un ADN idéntico.

3.4 TABLA COMPARATIVA DE SISTEMAS BIOMÉTRICOS

Lo que sigue a continuación es una tabla en la que recogen las diferentes características de los sistemas biométricos:

	Ojo (Iris)	Ojo (Retina)	Huellas dactilares	Vascular dedo	Vascular mano	Geometría de la mano	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Muy Alta	Muy Alta	Muy Alta	Muy Alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Baja	Alta	Muy Alta	Muy Alta	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Muy Alta	Alta	Muy Alta	Muy Alta	Alta	Media	Media	Media
Aceptación	Media	Baja	Alta	Alta	Alta	Alta	Muy Alta	Alta	Muy alta
Estabilidad	Alta	Alta	Alta	Alta	Alta	Media	Baja	Media	Media

Tabla 3-1: Tabla Comparativa de los Sistemas Biométricos.

3.5 PRINCIPALES PARTICIPANTES EN LA INDUSTRIA BIOMÉTRICA

La Industria de Biométrica ofrece varias tecnologías. Cada tecnología es considerada como un segmento de mercado diferente. Las más conocidas son las huellas dactilares, reconocimiento de cara y reconocimiento de iris (ojos). El cuadro abajo contiene las diferentes tecnologías, aplicaciones horizontales y los principales

mercados verticales (en el sector privado y público) que ofrece la industria biométrica (*):

Tecnología	Aplicación Horizontal	Principales mercados verticales
AFIS/Lifescan	Controles de Vigilancia	Servicios policiales y militares
Huellas Dactilares	identificación Civil	Gobiernos regionales y nacionales
Reconocimiento de cara	Identificación de Clientes	Instituciones Financieras
Geometría de Mano	Identificación Criminal	Hospitales y Sector Salud
Reconocimiento de iris (ojo)	Acceso a sistemas	Industria manufacturera
Reconocimiento de Voz	Acceso a instalaciones	Viajes y Turismo
Escritura y Firma	Vigilancia	

Tabla 3-2: Diferentes Tecnologías en la Industria Biométrica (*)

Figura 3-4 Reconocimiento de iris (ojo)

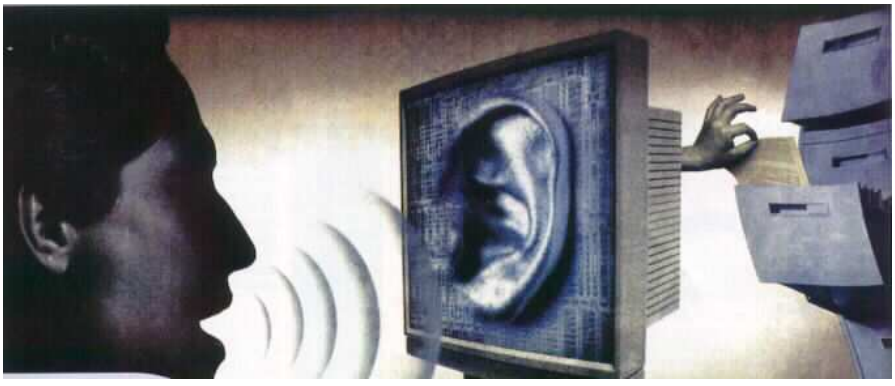


Figura. 3-5 Reconocimiento de voz

Hay muchos participantes en la industria biométrica. El mercado es muy complejo y el desarrollo de la tecnología a la medida se ofrece cada día más por muchas empresas. Las diferentes tecnologías se diferencian en términos de aplicación y segmentos de mercado. En términos generales, las empresas que mantienen participaciones de mercado significativas en segmentos específicos ni siquiera participan en otros. El cuadro abajo contiene los principales vendedores en la industria de la tecnología biométrica (*):

Tecnología	Vendedores
Huellas Dactilares	SAGEM Morpho Inc., Cogent System Inc., Identix Inc., SecuGen Corp., Sony Corp., Biometric Access Corp. Silicon scanner: Infineon Technologies AG, Siemens AG, Veridicom Inc., Authen Tec Inc., Bioscrypt Inc
Reconocimiento de cara	Identix Inc. (se fusiono con Visionics en Junio 2002) , Cognitec, ZN Vision (Alemania), Imagis (Canada)
Reconocimiento de Iris	Iridian Technologies Inc., including Argus Solutions, Eye Ticket Corp., IBM., Joh. Enschede Securiry Solutions, LG Elecetronics, NEC Singapore, Oki, Electric Industry Co., Panasonic, SAFLINK Corp., Siemens AG, Titan Corp., Unisys
Geometría de la mano	Recogntion Systems Inc. (RSI), Electronic Data Systems Corp. y ADT
Reconocimiento de voz	Gartner Group, Inc., Buytel, T-NETIX Inc., Veritel Corporation, Nuance y VeriVoice Inc
Reconocimiento de firma	Communication Intelligence Corporation (CIC), Cyber-SIGN Inc. ,Hesy, WonderNet, y ScanSoft

Tabla 3-3: Principales vendedores por aplicación de la Industria Biométrica(*)

3.6 ESTÁNDARES ASOCIADOS A TECNOLOGÍAS BIOMÉTRICAS

En los últimos años se ha notado una preocupación creciente por las organizaciones regulatorias respecto a elaborar estándares relativos al uso de técnicas biométricas en el ambiente informático. Esta preocupación es reflejo del creciente interés industrial por este ámbito tecnológico, y a los múltiples beneficios que su uso aporta. No obstante ello, aún la estandarización continua siendo deficiente y como resultado de ello, los proveedores de soluciones biométricas continúan suministrando interfaces de software propietarios para sus productos, lo que dificulta a las empresas el cambio de producto o vendedor.

A nivel mundial el principal organismo que coordina las actividades de estandarización biométrica es el Sub-Comité 17 (SC17) del Joint Technical Committee on Information Technology (ISO/IEC JTC1), del International Organization for Standardization (ISO) y el International Electrotechnical Commission (IEC).

En Estados Unidos desempeñan un papel similar el Comité Técnico M1 del INCITS (InterNational Committee for Information Technology Standards), el National Institute of Standards and Technology (NIST) y el American National Standards Institute (ANSI).

Existen además otros organismos no gubernamentales impulsando iniciativas en materias biométricas tales como: Biometrics Consortium, International Biometrics Groups y BioAPI. Este último se estableció en Estados Unidos en 1998 compuesto por las empresas Bioscrypt, Compaq, Iridiam, Infineon, NIST, Saflink y Unisis. El Consorcio BioAPI desarrolló conjuntamente con otros consorcios y asociaciones, un estándar que promoviera la conexión entre los dispositivos biométricos y los diferentes tipos de programas de aplicación, además de promover el crecimiento de los mercados biométricos.

Algunos de los estándares más importantes son:

Estándar ANSI X.9.84: creado en 2001, por la ANSI (American National Standards Institute) y actualizado en 2003, define las condiciones de los sistemas biométricos para la industria de servicios financieros haciendo referencia a la transmisión y

almacenamiento seguro de información biométrica, y a la seguridad del hardware asociado.

Estándar ANSI / INCITS 358: creado en 2002 por ANSI y BioApi Consortium, presenta una interfaz de programación de aplicación que garantiza que los productos y sistemas que cumplen este estándar son interoperables entre sí.

Estándar NISTIR 6529: también conocido como CBEFF (Common Biometric Exchange File Format) es un estándar creado en 1999 por NIST y Biometrics Consortium que propone un formato estandarizado (estructura lógica de archivos de datos) para el intercambio de información biométrica.

Estándar ANSI 378: creado en 2004 por la ANSI, establece criterios para representar e intercambiar la información de las huellas dactilares a través del uso de minucias. El propósito de esta norma es que un sistema biométrico dactilar pueda realizar procesos de verificación de identidad e identificación, empleando información biométrica proveniente de otros sistemas.

Estándar ISO 19794-2: creado en 2005 por la ISO/IEC con propósitos similares a la norma ANSI 378, respecto a la que guarda mucha similitud.

Estándar PIV-071006: creado en 2006 por el NIST y el FBI en el contexto de la norma FIPS 201 del gobierno de EE.UU, establece los criterios de calidad de imagen que deben cumplir los lectores de huellas dactilares para poder ser usados en procesos de verificación de identidad en agencias federales.

3.7 PROCESOS DE AUTENTIFICACIÓN E IDENTIFICACIÓN BIOMÉTRICA

En el proceso de autentificación (o verificación) los rasgos biométricos se comparan solamente con los de un patrón ya guardado, este proceso se conoce también como uno-para-uno (1:1). Este proceso implica conocer presuntamente la identidad del individuo a autentificar, por lo tanto, dicho individuo ha presentado algún tipo de credencial, que después del proceso de autentificación biométrica será validada o no.

En el proceso de identificación los rasgos biométricos se comparan con los de un conjunto de patrones ya guardados, este proceso se conoce también como uno-para-muchos (1:N). Este proceso implica no conocer la identidad presunta del individuo, la nueva muestra de datos biométricos es tomada del usuario y comparada una a una con los patrones ya existentes en el banco de datos registrados. El resultado de este proceso es la identidad del individuo, mientras que en el proceso de autentificación es un valor verdadero o falso.

El proceso de autentificación o verificación biométrica es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios (N) es elevado. Esto es debido a que la necesidad de procesamiento y comparaciones es más reducido en el proceso de autentificación. Por esta razón, es habitual usar autentificación cuando se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o se quiere un proceso muy rápido.

3.8 RECONOCIMIENTO DE IRIS

El iris es una membrana pigmentada suspendida en el interior del ojo, entre la córnea y el cristalino. Regula el tamaño de la pupila para controlar la cantidad de luz que ingresa al ojo. Adquiere su pigmentación de la melatonina.

Antes de que ocurra el reconocimiento de iris, se localiza el iris usando características del punto de referencia. Estas características del punto de referencia y la forma distinta del iris permiten digitalización de la imagen, el aislamiento de la característica, y la extracción. La localización del iris es un paso importante en el reconocimiento del iris porque, si está hecho incorrectamente, el ruido resultante (e.g., pestañas, reflexiones, pupilas, y párpados) en la imagen puede conducir al bajo rendimiento.

Debido a que el infrarrojo tiene energía insuficiente para causar efectos fotoquímicos, la modalidad potencial principal de daños es termal. Cuando se produce NIR usando los diodos electroluminosos, la luz que resulta es incoherente. Cualquier riesgo para la seguridad del ojo es remoto con una sola fuente de LED usando tecnología de LED de hoy. Los iluminadores múltiples de LED pueden, sin embargo, producir daño en el ojo si no es diseñado y usado cuidadosamente.

3.9 RECONOCIMIENTO VASCULAR

En la biometría vascular se extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo. A diferencia de la huella dactilar el patrón biométrico es

interno, por esta razón no deja rastro y solo se puede conseguir en presencia de la persona. Es por tanto muy dificil el robo de identidad.

Debido a estas características es especialmente indicado para entornos de alta seguridad, así como en entornos duros, en que la superficie del dedo (y por consiguiente la huella superficial) pueden estar en mal estado, erosionados o poco limpios.

3.9.1 ROBO DE IDENTIDAD

Las preocupaciones acerca del robo de identidad por el uso de la Biometria aún no han sido resueltas. Si el número de tarjeta de crédito de una persona es robado, por ejemplo, puede causarle a esa persona grandes dificultades. Si sus patrones de escaneado de iris son robados, sin embargo, y eso permite a otra persona acceder a información personal o a cuentas financieras, el daño podría ser irreversible. Frecuentemente, las tecnologías biométricas han sido puestas en uso sin medidas adecuadas de seguridad para la información personal que es resguardada a través de las mismas.

3.9.2 PRIVACIDAD

Aunque la biometría es frecuentemente utilizada como un medio para combatir la criminalidad, existe la preocupación de que la biometría pueda ser utilizada para disminuir las libertades personales de los ciudadanos.

Los desarrollos en tecnología video digital, infrarrojos, rayos X, inalámbricas, sistemas de posicionamiento global, biometría, escaneado de imágenes, reconocimiento de voz, ADN, e identificación de ondas cerebrales le proveen al gobierno con nuevos métodos para "buscar e investigar" vastas bases de datos individuales y colectivas de información sobre la población en general.

Los Padres de la Constitución de los Estados Unidos nunca pensaron acerca de este tipo de "búsquedas e investigaciones" cuando diseñaron la Cuarta Enmienda, pero como uno de los avances tecnológicos de nuestro tiempo, nosotros tenemos que pensar en ese contexto.

3.10 SISTEMAS BIOMÉTRICOS

Entenderemos por *sistema biométrico* a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada. En esta sección son descritas algunas de las características más importantes de estos sistemas.

3.10.1 Modelo del proceso de identificación personal

Cualquier proceso de identificación personal puede ser comprendido mediante un modelo simplificado. Este postula la existencia de tres indicadores de identidad que definen el proceso de identificación:

1. *Conocimiento:* la persona tiene conocimiento (por ejemplo: un código),
2. *Posesión:* la persona posee un objeto (por ejemplo: una tarjeta), y

3. *Característica:* la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares).

Cada uno de los indicadores anteriores genera una estrategia básica para el proceso de identificación personal. Además pueden ser combinados con el objeto de alcanzar grados de seguridad más elevados y brindar, de esta forma, diferentes niveles de protección. Distintas situaciones requerirán diferentes soluciones para la labor de identificación personal. Por ejemplo, con relación al *grado de seguridad*, se debe considerar el valor que está siendo protegido así como los diversos tipos de amenazas. También es importante considerar la reacción de los usuarios y el costo del proceso.

3.10.2 Características de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar biometría. Cualquiera sea el indicador, debe cumplir los siguientes requerimientos [4]:

1. *Universalidad:* cualquier persona posee esa característica;
2. *Unicidad:* la existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña;
3. *Permanencia:* la característica no cambia en el tiempo; y
4. *Cuantificación:* la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como *indicador biométrico*. Luego de seleccionar algún indicador que

satisfaga los requerimientos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores. En la siguiente sección se presentan estas restricciones.

3.10.3 Características de un sistema biométrico para identificación personal

Las características básicas que un sistema biométrico para identificación personal debe cumplir pueden expresarse mediante las restricciones que deben ser satisfechas. Ellas apuntan, básicamente, a la obtención de un sistema biométrico con utilidad práctica. Las restricciones antes señaladas apuntan a que el sistema considere:

1. *El desempeño*, que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.
2. *La aceptabilidad*, que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento de una retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al hecho de tener su ojo sin protección frente a un "aparato". Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones el efecto

psicológico de utilizar un sistema basado en el reconocimiento de características oculares será positivo, debido a que este método es eficaz implicando mayor seguridad.

3. *La fiabilidad*, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para chequear las venas de la mano detecta flujos de sangre caliente y lectores de ultrasonido para huellas dactilares revisan estructuras subcutáneas de los dedos.

3.10.4 Arquitectura de un sistema biométrico para identificación personal

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una huella dactilar mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento y comparación de los datos adquiridos (en el ejemplo una imagen) con los datos almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas

en el mismo u otro sistema. La arquitectura típica de un sistema biométrico se presenta en la figura 1. Esta puede entenderse conceptualmente como dos módulos:

1. *Módulo de inscripción (enrollment module) y*
2. *Módulo de identificación (identification module).*

El módulo de inscripción se encarga de adquirir y almacenar la información proveniente del indicador biométrico con el objeto de poder contrastar a ésta con la proporcionada en ingresos posteriores al sistema. Las labores ejecutadas por el módulo de inscripción son posibles gracias a la acción del lector biométrico y del extractor de características.

El primero se encarga de adquirir datos relativos al indicador biométrico elegido y entregar una representación en formato digital de éste. El segundo extrae, a partir de la salida del lector, características representativas del indicador. El conjunto de características anterior, que será almacenado en una base de datos central u otro medio como una tarjeta magnética, recibirá el nombre de template. En otras palabras un template es la información representativa del indicador biométrico que se encuentra almacenada y que será utilizada en las labores de identificación al ser comparada con la información proveniente del indicador biométrico en el punto de acceso.

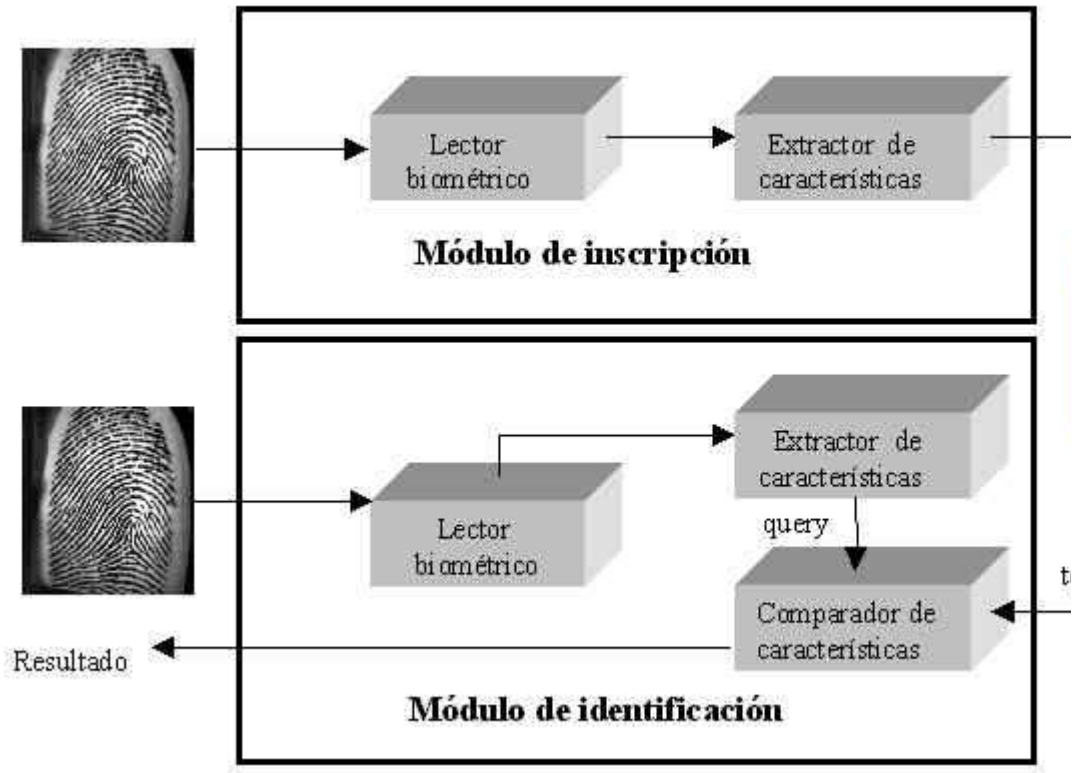


Figura 3-6: Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con huellas dactilares.

El módulo de identificación es el responsable del reconocimiento de individuos, por ejemplo en una aplicación de control de acceso. El proceso de identificación comienza cuando el lector biométrico captura la característica del individuo a ser identificado y la convierte a formato digital, para que a continuación el extractor de características produzca una representación compacta con el mismo formato de los *templates*. La representación resultante se denomina query y es enviada al comparador de *características* que confronta a éste con uno o varios *templates* para establecer la identidad.

El conjunto de procesos realizados por el módulo de inscripción recibe el nombre de *fase de inscripción*, mientras que los procesos realizados por el módulo de

identificación reciben la denominación de *fase operacional*. A continuación se entregan detalles de esta última.

3.10.5 Fase operacional de un sistema de identificación personal.

Un sistema biométrico en su fase operacional puede operar en dos modos:

1. *Modo de verificación, o*
2. *Modo de identificación*

Un sistema biométrico operando en el modo de verificación comprueba la identidad de algún individuo comparando la característica sólo con los templates del individuo. Por ejemplo, si una persona ingresa su nombre de usuario entonces no será necesario revisar toda la base de datos buscando el template que más se asemeje al de él, sino que bastará con comparar la información de entrada sólo con el template que está asociado al usuario. Esto conduce a una comparación uno-a-uno para determinar si la identidad reclamada por el individuo es verdadera o no. De manera más sencilla el modo de verificación responde a la pregunta: ¿eres tú quién dices ser?.

Un sistema biométrico operando en el modo de identificación descubre a un individuo mediante una búsqueda *exhaustiva* en la base de base de datos con los templates. Esto conduce a una comparación del tipo *uno-a-muchos* para establecer la identidad del individuo.

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema

de identificación necesita explorar toda la base de datos donde se almacenan los templates, a diferencia de un sistema verificador. De la discusión anterior resulta obvio notar que la exigencia sobre el extractor y el comparador de características es mucho mayor en el primer caso.

3.10.6 Exactitud en la identificación: medidas de desempeño

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos. Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como *variaciones intraclase*. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

1. Una persona autorizada es aceptada,
2. Una persona autorizada es rechazada,
3. Un impostor es rechazado,
4. Un impostor es aceptado.

Las salidas números 1 y 3 son correctas, mientras que las números 2 y 4 no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por

la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores [9]:

1. Tasa de falsa aceptación (*FAR*: False Acceptance Rate), que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado,
2. Tasa de falso rechazo (*FRR*: False Rejection Rate), definida como la frecuencia relativa con que un individuo autorizado es rechazado como un impostor.

La *FAR* y la *FRR* son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos. Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la figura 2. El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente

al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

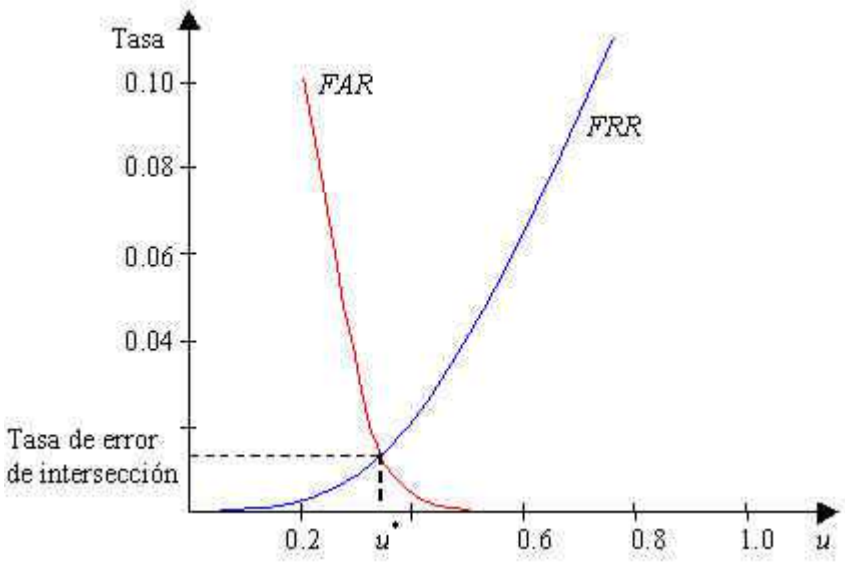


Figura 3-7. Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación u para un sistema biométrico.

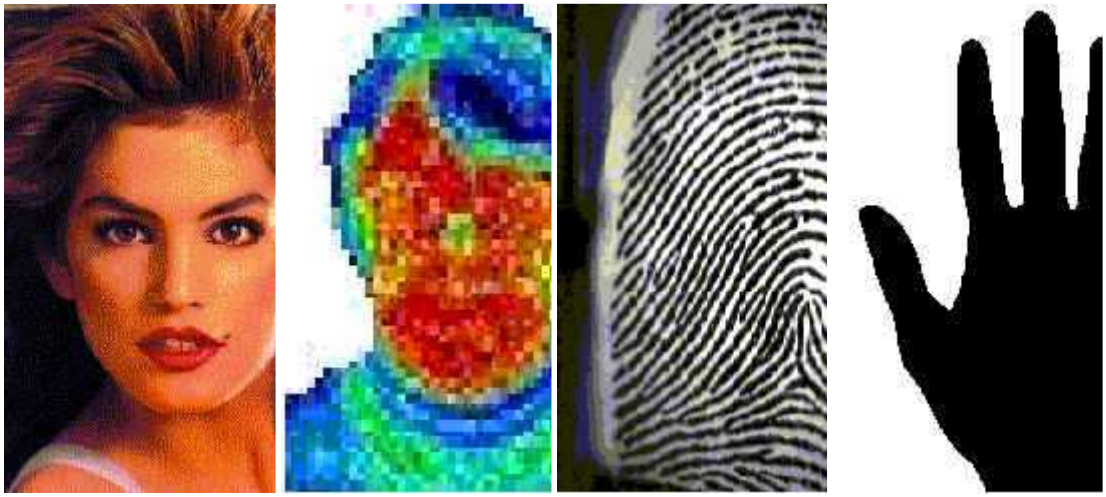
La FRR es una función estrictamente creciente y la FAR una estrictamente decreciente en u [9]. La FAR y la FRR al ser modeladas como función del umbral de aceptación tienen por dominio al intervalo real [0,1], que es además su recorrido, puesto que representan frecuencias relativas. La figura 2 muestra una gráfica típica de la FRR y la FAR como funciones de u. En esta figura puede apreciarse un umbral de aceptación particular, denotado por u*, donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de *error de intersección (cross-over error rate)* y puede ser utilizado como medida única para caracterizar el *grado de seguridad* de un sistema biométrico. En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para

identificación, mediante la FAR. Usualmente se elige un umbral de aceptación por debajo de u* con el objeto de reducir la FAR, en desmedro del aumento de la FRR.

3.10.7 Sistemas biométricos actuales.

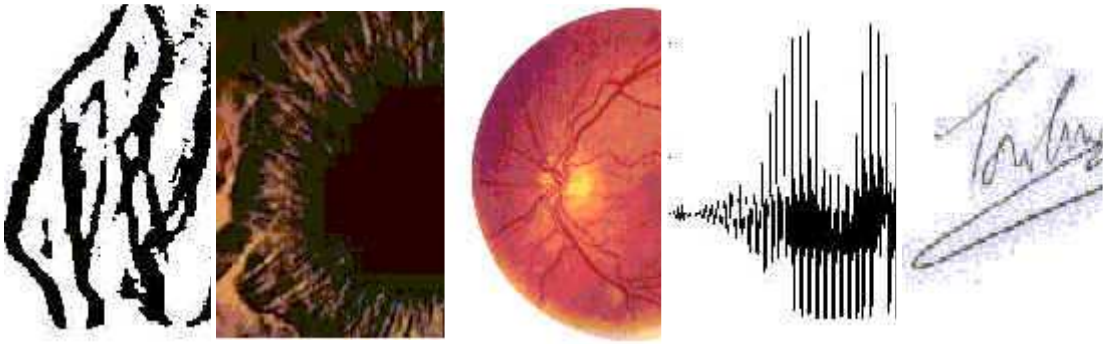
En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la figura 3. Las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

1. Rostro,
2. Termograma del rostro,
3. Huellas dactilares,
4. Geometría de la mano,
5. Venas de las manos,
6. Iris,
7. Patrones de la retina,
8. Voz,
9. Firma.



(a) (b) (c) (d)

Figura 3-8 Sistemas biométricos actuales



(e) (f) (g) (h) (i)

Figura 3-9 Técnicas biométricas actuales: (a) Rostro, (b) Termograma Facial, (c) Huella dactilar, (d) Geometría de la mano, (e) Venas de la mano, (f) Iris, (g) Patrones de la retina, (h) Voz e (i) Firma.

Cada una de las técnicas anteriores posee ventajas y desventajas comparativas, las cuales deben tenerse en consideración al momento de decidir que técnica utilizar para una aplicación específica. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento. Una huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser influenciada tanto por factores controlables como por psicológicos no intencionales. También las máquinas que miden características físicas tienden a ser más grandes y costosas que

las que detectan comportamientos. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades. Una compañía puede incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación. Por ejemplo en [4], se integran el reconocimiento de rostros y huellas dactilares. La razón es que el reconocimiento de rostros es rápido pero no extremadamente confiable, mientras que la identificación mediante huellas dactilares es confiable pero no eficiente en consultas a bases de datos. Lo anterior sugiere el utilizar el reconocimiento de rostros para particionar la base de datos. Luego de esto comienza la identificación de la huella. Los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por sus partes por separado. En efecto, las limitaciones de las alternativas por separado son soslayadas, logrando además respuestas exactas con un tiempo de proceso adecuado. En la figura 4 se presenta un esquema de división de las características biométricas.

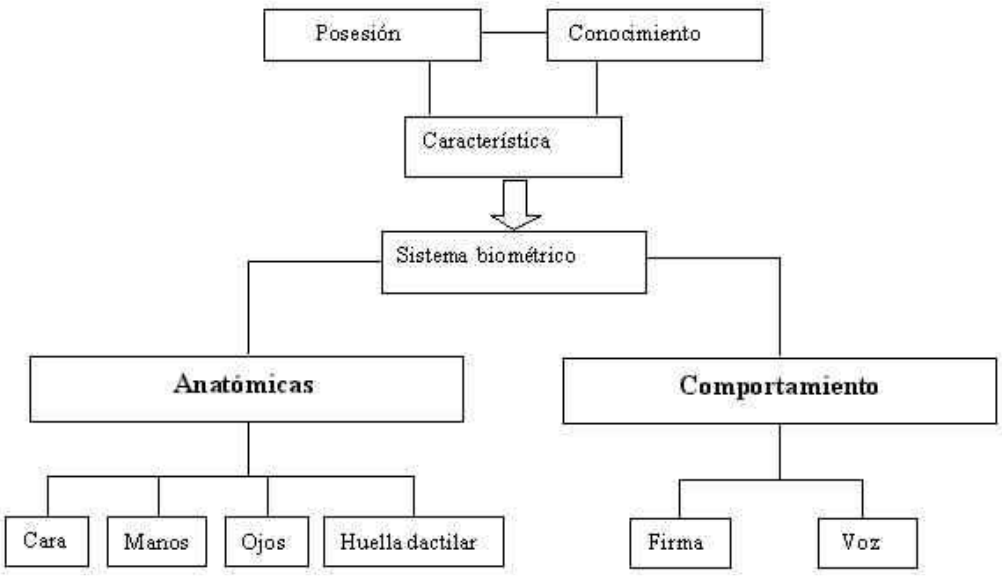


Figura 3-10. División de las características biométricas.

CAPITULO 4

IMPLEMENTACION DEL SISTEMA INMÓTICO APLICADO AL CONTROL DE ACCESO A TRAVÉS CERRADURAS BIOMÉTRICAS

4.1 COMPONENTES FÍSICOS

En este capitulo se detallan los componentes electrónicos que previo análisis de los objetivos y el alcance del proyecto cumplen con los requerimientos técnicos tanto de software como de hardware.

4.1.1 MICROCONTROLADOR PIC 18F2550

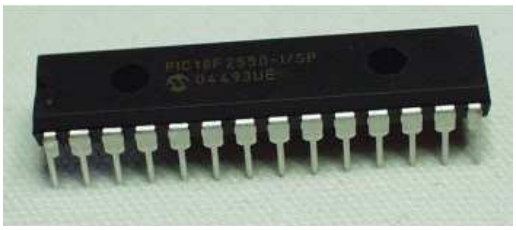


Figura 4-1 Microcontrolador PIC 18F2550

El 18F2550 es un microcontrolador para aplicaciones más exigentes de los lotes que tengan la memoria del programa (16k) y RAM (2k) y una completa interfaz Rs 232.

Viene en un paquete de 28 pines y también está optimizado para la programación C (75 estándar + 8 instrucciones extra) y utiliza la tecnología de nano vatios. Una vez más, el dispositivo utiliza ICSP para la programación y usted puede programar en el circuito si el diseño de la interfaz es correcto.

Como ocurre con todas las de la serie 18F es un 8x8 construido en hardware multiplicador para que los cálculos se ejecuten mucho más rápido.

4.1.2 CARACTERÍSTICAS DEL PIC 18F2550

- Arquitectura de 8 bits
- Memoria flash de 32 Kbytes
- Con capacidad de escribir su propia memoria de programa
- Memoria EEPROM de 256 Bytes
- Memoria RAM de 2048 Bytes
- 28 pines
- 24 Entradas / salidas
- Velocidad máxima del CPU de hasta 48 MHz
- Velocidad máxima del CPU de hasta 12 MIPS (millones de instrucciones por segundo).
- Oscilador interno de 8 MHz/32 KHz
- Convertidor A/D de 10 canales
- Resolución del A/D de 10 bits
- Comunicación digital disponible mediante USART, SPI o I2C
- 1 timer de 8 bits
- 3 timers de 16 bits
- 2 canal de PWM para control de motores
- Resolución de PWM de 10 bits
- Rango de operación de 2V a 5.5V
- Cuenta con tranceiver USB 2.0

4.1.3 INDICADOR LED

Un diodo emisor de luz, también conocido como LED es un dispositivo semiconductor que emite luz incoherente de espectro reducido cuando se polariza de forma directa la unión PN del mismo y circula por él una corriente eléctrica. Este fenómeno es una forma de electroluminiscencia. El color, depende del material semiconductor empleado en la construcción del diodo y puede variar desde el ultravioleta, pasando por el visible, hasta el infrarrojo. Los diodos emisores de luz que emiten luz ultravioleta también reciben el nombre de UV LED (*ultraviolet light-emitting diode*) y los que emiten luz infrarroja se llaman IRED (*infrared emitting diode*).

El funcionamiento físico consiste en que, en los materiales semiconductores, un electrón al pasar de la banda de conducción a la de valencia, pierde energía; esta energía perdida se puede manifestar en forma de un fotón desprendido, con una amplitud, una dirección y una fase aleatoria. El que esa energía perdida cuando pasa un electrón de la banda de conducción a la de valencia se manifieste como un fotón desprendido o como otra forma de energía (calor por ejemplo) va a depender principalmente del tipo de material semiconductor. Cuando un diodo semiconductor se polariza directamente, los huecos de la zona p se mueven hacia la zona n y los electrones de la zona n hacia la zona p; ambos desplazamientos de cargas constituyen la corriente que circula por el diodo.

Si los electrones y huecos están en la misma región, pueden recombinarse, es decir, los electrones pueden pasar a "ocupar" los huecos, "cayendo" desde un nivel

energético superior a otro inferior más estable. Este proceso emite con frecuencia un fotón en semiconductores de banda prohibida directa o "direct bandgap" con la energía correspondiente a su banda prohibida (véase semiconductor). Esto no quiere decir que en los demás semiconductores (semiconductores de banda prohibida indirecta o "indirect bandgap") no se produzcan emisiones en forma de fotones; sin embargo, estas emisiones son mucho más probables en los semiconductores de banda prohibida directa (como el Nitruro de Galio) que en los semiconductores de banda prohibida indirecta (como el Silicio).

La emisión espontánea, por tanto, no se produce de forma notable en todos los diodos y sólo es visible en diodos como los LEDs de luz visible, que tienen una disposición constructiva especial con el propósito de evitar que la radiación sea reabsorbida por el material circundante, y una energía de la banda prohibida coincidente con la correspondiente al espectro visible. En otros diodos, la energía se libera principalmente en forma de calor, radiación infrarroja o radiación ultravioleta. En el caso de que el diodo libere la energía en forma de radiación ultravioleta, se puede conseguir aprovechar esta radiación para producir radiación visible, mediante sustancias fluorescentes o fosforescentes que absorban la radiación ultravioleta emitida por el diodo y posteriormente emitan luz visible.

Figura 4-2 Representación simbólica del diodo LED.

El dispositivo semiconductor está comúnmente encapsulado en una cubierta de plástico de mayor resistencia que las de vidrio que usualmente se emplean en las lámparas incandescentes. Aunque el plástico puede estar coloreado, es sólo por razones estéticas, ya que ello no influye en el color de la luz emitida. Usualmente un LED es una fuente de luz compuesta con diferentes partes, razón por la cual el patrón de intensidad de la luz emitida puede ser bastante complejo.

Para obtener buena intensidad luminosa debe escogerse bien la corriente que atraviesa el LED; para ello, hay que tener en cuenta que el voltaje de operación va desde 1,8 hasta 3,8 voltios aproximadamente (lo que está relacionado con el material de fabricación y el color de la luz que emite) y la gama de intensidades que debe circular por él varía según su aplicación. Valores típicos de corriente directa de polarización de un LED corriente están comprendidos entre los 10 y los 40 mA. En general, los LEDs suelen tener mejor eficiencia cuanto menor es la corriente que circula por ellos, con lo cual, en su operación de forma optimizada, se suele buscar un compromiso entre la intensidad luminosa que producen (mayor cuanto más grande es la intensidad que circula por ellos) y la eficiencia (mayor cuanto menor es la intensidad que circula por ellos). El primer LED que emitía en el espectro visible fue desarrollado por el ingeniero de General Electric Nick Holonyak en 1962.

4.1.4 RECONOCIMIENTO DE HUELLAS DACTILARES.

Entre todas las técnicas biométricas, la identificación basada en las huellas dactilares es el método más viejo, el cual ha sido usado en numerosas aplicaciones. Una huella esta formada por una serie de crestas y surcos localizados en la superficie del dedo.

La singularidad de una huella puede ser determinada por dos tipos de patrones: el patrón de crestas y surcos, así como el de detalles.

Existen dos técnicas para realizar la verificación de las huellas:

1. Basada en Detalles: Esta técnica elabora un mapa con la ubicación relativa de "detalles" sobre la huella, los cuales permiten ubicar con certeza a un individuo. Sin embargo, existen algunas dificultades cuando se utiliza está aproximación. Es muy difícil ubicar los detalles con precisión cuando la huella suministrada es de baja calidad. También este método no toma en cuenta el patrón global de las crestas y los surcos. Entre algunos detalles que podemos encontrar en una huella, tenemos:

Figura 4-3 Detalles de las huellas

2. Cada individuo posee uno y solo uno, arreglo de detalles.

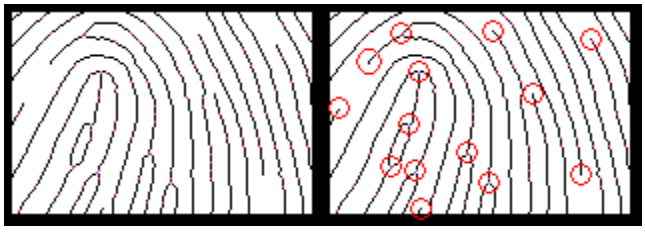


Figura 4-4 Trazado del patrón de detalles.

El mismo puede ser descrito por un modelo de probabilidad: P(C)=P(N).P(M).P(A)

Donde: P(C) = f(Ley de Poisson)

P(M)= f(frecuencia de aparición del detalle)

P(A) = f(número de permutaciones posibles de detalles)

3. Basadas en correlación: Este método viene a mejorar algunas dificultades presentadas por la aproximación creada por los el patrón de detalles, pero inclusive él mismo presenta sus propias fallas, está técnica requiere de la localización precisa de un punto de registro el cual se ve afectado por la rotación y traslación de la imagen.

Una vez obtenida la huella digital es necesario clasificarla. Este proceso consiste en ubicar dicha huella dentro de los varios tipos existentes, los cuales proveen un mecanismo de indexado; esto con la finalidad de reducir el tiempo de búsqueda. Los algoritmos existentes permiten clasificar la huella en cinco clases:

- Anillo de Crestas.
- Lazo Derecho.
- Lazo Izquierdo.
- Arco.
- Arco de Carpa.

Estos algoritmos separan el número de crestas presentes en cuatro direcciones (0°, 45°, 90° y 135°) mediante un proceso de filtrado de la parte central de la huella

Dentro del proceso de reconocimiento es necesario emplear técnicas muy robustas que no se vean afectadas por algún ruido obtenido en la imagen además de incrementar la precisión en tiempo real. Un sistema comercial empleado para la identificación de huellas dactilares requiere de un muy bajo promedio de rechazos falsos (FRR)[1] para un promedio de aceptación falso (FAR)[2]. Como por ejemplo:

- Un dedo (FRR y FAR): 1:1000
- Dos Dedos (FRR y FAR): 1:1000000

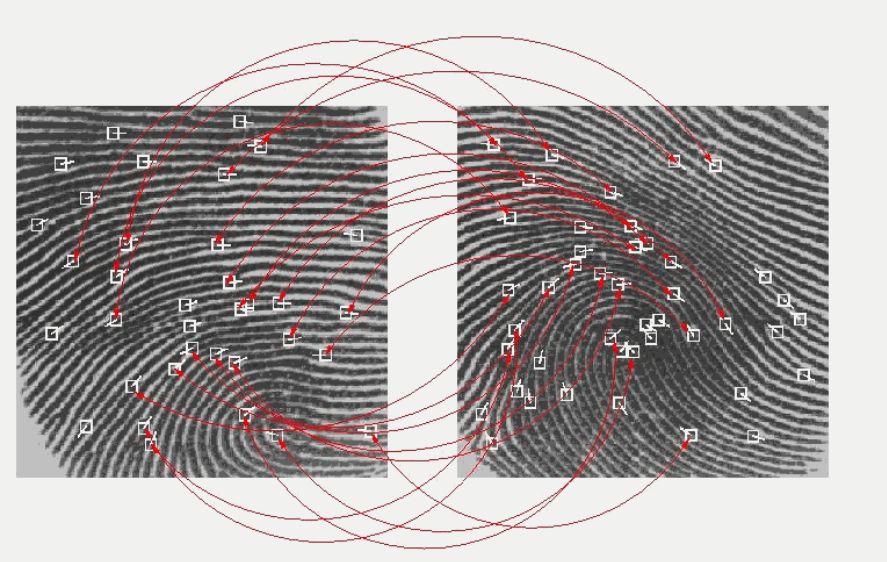


Figura 4-5 Proceso de comparación.

El siguiente es un diagrama de bloques de un sistema utilizado para la verificación de huellas dactilares. En el mismo se describen en forma general las operaciones lógicas necesarias para llevar a cabo la identificación:

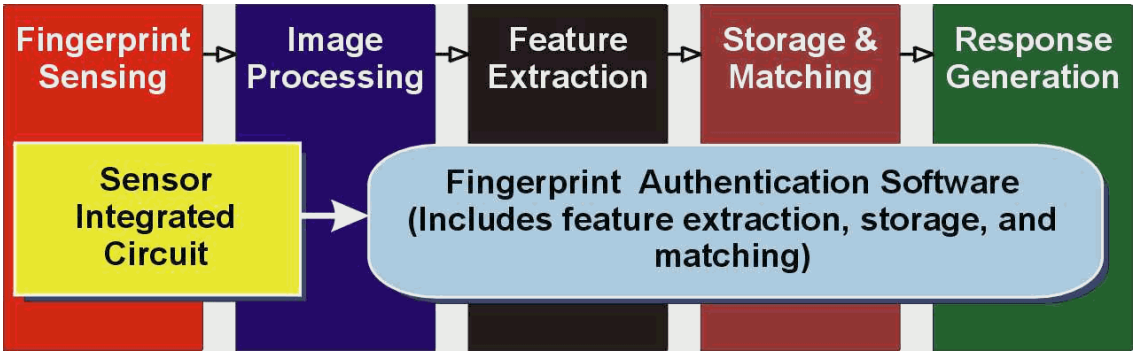


Figura 4-6 Diagrama de bloques de un sistema reconocimiento de huellas dactilares.

Tal vez el bloque más critico dentro del sistema propuesto arriba es el de adquisición de muestra. El mismo será detallado a continuación.

4.1.5 SENSORES PARA HUELLAS DACTILARES

Existen dos arreglos típicos:

4.1.5.1 SENSOR DE MATRIZ CAPACITIVO:

En la superficie de un circuito integrado de silicona se dispone un arreglo de platos sensores capacitivos (ver figura 4.). La capacitancia en cada plato (pixel) sensor es medida individualmente depositando una carga fija sobre ese pixel. El voltaje estático generado por esa carga es proporcional a la capacitancia del pixel y sus alrededores. Por la geometría del dedo, las líneas de flujo generadas desde el plato sensor energizado se inducen en la porción de piel inmediatamente adyacente a este plato, terminando en platos sensores inactivos o en el sustrato.

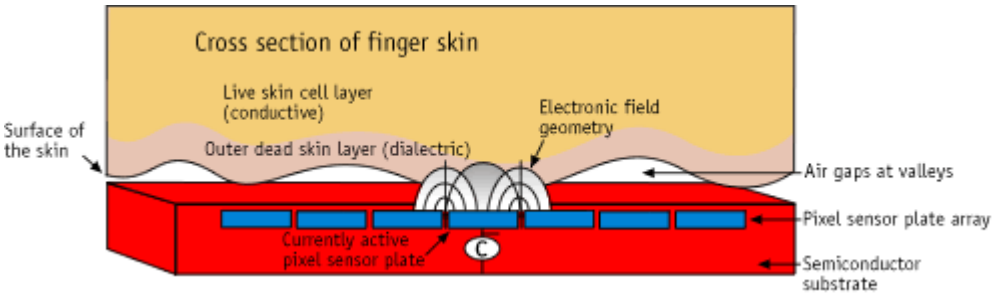


Figura 4-7 Sensor Capacitivo clásico.

Una ventaja de este diseño es su simplicidad. Una desventaja es que debido a la geometría esférica del campo eléctrico generado por el plato sensor, tendremos un efecto de solapamiento sobre platos (pixel) vecinos, los que producirá que el área sensora aumente en tamaño, trayendo como consecuencia un efecto de información cruzada entre los sensores adyacentes, reduciendo considerablemente la resolución de la imagen.

Para dedos jóvenes, saludables y limpios, este sistema trabaja adecuadamente. Los problemas comienzan a presentarse cuando se tienen condiciones menos optimas en la piel. Cuando el dedo esta sucio, con frecuencia no existirá aberturas de aire en los valles. Cuando la superficie del dedo es muy seca, la diferencia de la constante dieléctrica entre la piel y las aberturas de aire se reduce considerablemente. En personas de avanzada edad, la piel comienza a soltarse trayendo como consecuencia que al aplicar una presión normal sobre el sensor los valles y crestas se aplasten considerablemente haciendo difícil el proceso de reconocimiento.

4.1.5.2 SENSOR DE MATRIZ DE ANTENA:

Un pequeño campo RF es aplicado entre dos capas conductoras, una oculta dentro de un chip de silicon (llamado plano de referencia de la señal de excitación) y la otra localizada por debajo de la piel del dedo. (Ver figura 5.) El campo formado entre estas capas reproduce la forma de la capa conductora de la piel en la amplitud del campo AC. Diminutos sensores insertados por debajo de la superficie del semiconductor y sobre la capa conductora, miden el contorno del campo. Amplificadores conectados directamente a cada plato sensor convierten estos potenciales a voltajes, representando el patrón de la huella. Estas señales son acondicionadas en una etapa siguiente para luego ser multiplexadas fuera del sensor.

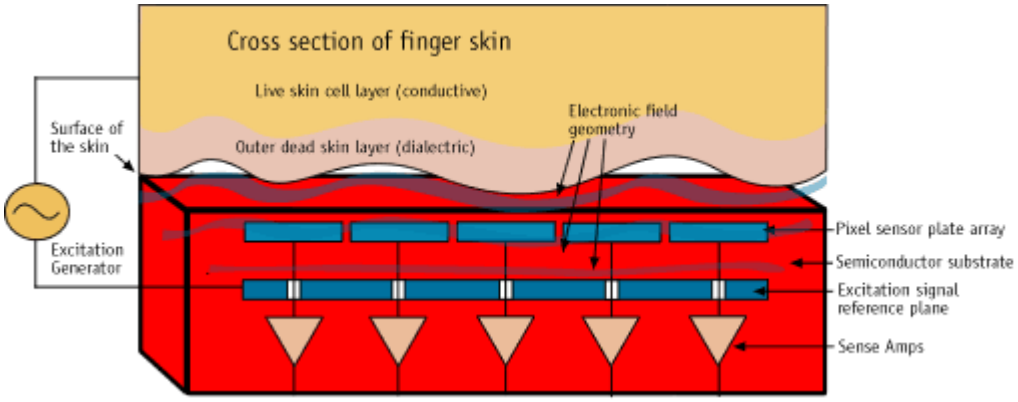


Figura 4-8 Sensor de Matriz de Antena.

Estos dispositivos no dependen de las características de la superficie, tales como las aberturas de aire entre el sensor y el valle, empleado para detectar ese valle.

En la figura 6 se puede observar la forma típica de un sensor aplicado a sistemas de reconocimiento de huellas dactilares.

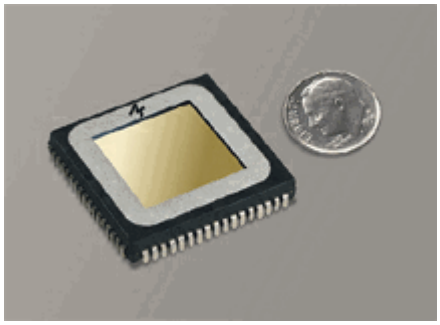


Figura 4-9 Disposición comercial.

4.1.6 PULSADORES

Elemento que permite el paso o interrupción de la corriente mientras es accionado. Cuando ya no se actúa sobre él vuelve a su posición de reposo.

Puede ser el contacto normalmente cerrado en reposo NC, o con el contacto normalmente abierto Na.

Consta del botón pulsador; una lámina conductora que establece contacto con los dos terminales al oprimir el botón y un muelle que hace recobrar a la lámina su posición primitiva al cesar la presión sobre el botón pulsador.

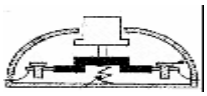


Figura 4-10 Botón pulsador

Diferentes tipos de pulsadores: (a) Basculante. (b) Pulsador timbre. (c) Con señalizador. (d) Circular. (e) Extraplano.

Figura 4-11 Diferentes tipos de pulsadores

4.1.7 MEMORIA EPROM 24LC1024

Los microcontroladores que disponen de memoria EPROM (Erasable Programmable Read OnIy Memory) pueden borrarse y grabarse muchas veces. La grabación se realiza, como en el caso de los OTP, con un grabador gobernado desde un PC. Si, posteriormente, se desea borrar el contenido, disponen de una ventana de cristal en su superficie por la que se somete a la EPROM a rayos ultravioleta durante varios minutos. Las cápsulas son de material cerámico y son más caros que los microcontroladores con memoria OTP que están hechos con material plástico.

Sus principales características son:

- Interfaz serial a dos cables, compatible con 12C
- Voltaje de operación de 2,5 V a 5,5V
- Máxima frecuencia del reloj: 400 Khz
- Tecnología CMOS de bajo consumo de potencia típicamente 1mA
- Entradas Schmitt trigger para supresión de ruido
- Memoria EEPROM de 128Kx8 (1024K- 1Mb serial)
- Conexión en cascada 4 memorias
- Más de un millón de ciclos de borrado / escritura
- Fácil interfaz a microcontrolador
- Gran capacidad de almacenamiento
- Encapsulado especial en montaje de 8 pines, especial para aplicaciones portátiles.

4.1.8 FUENTES DE PODER REGULADAS

Los reguladores de voltaje son un grupo popular de C.I. lineales. Un regulador de voltaje en C.I. recibe una entrada de voltaje de C.C. relativamente constante y suministra como salida un valor relativamente mas bajo de voltaje C.C. que el regulador mantiene fijo o regulado sobre un amplio rango de control para la corriente de carga y de voltaje de filtrado. Partiendo de un voltaje de suministro de C.A., se

puede desarrollar un voltaje en C.C. de estado estacionario rectificando el V_{CA}, posteriormente filtrándolo a un nivel de C.C. y finalmente regulándolo con un circuito regulador de voltaje en C.I.

4.2 COMPONENTES LÓGICOS

En este apartado se detalla lo relacionado con el software de control que se programará en el Microcontrolador y que permitirá interactuar al usuario con los periféricos del sistema.

4.2.1 LENGUAJE DE PROGRAMACIÓN C18

El lenguaje C fue creado en los años 70 para escribir el código del sistema operativo UNIX. Tanto por su origen como por sus características, es un lenguaje muy adecuado para la programación de sistemas, ya que combina la abstracción de los lenguajes de alto nivel con la eficiencia del lenguaje máquina.

La amplia utilización de C para distintos tipos de computadores ocasionó muchas variantes. Éstas eran similares, pero a menudo incompatibles, lo que se volvió un problema serio para los desarrolladores que necesitaban escribir programas que se ejecutaran en distintas plataformas. Entonces, se hizo evidente la necesidad de una versión estándar de C. En 1983, se creó el comité técnico X3J11 bajo la supervisión de American National Standards Comitte on Computer and Information Processing (X3), para “proporcionar una definición del lenguaje clara e independiente de la computadora”. En 1989, el estándar fue aprobado. ANSI cooperó con la International Organization for Standardization (ISO) para estandarizar C a nivel mundial; el documento conjunto del estándar se publicó en 1990 y se conoce como ANSI/ISO9899:1990 o ANSI C.

Entre las características de este lenguaje cabe citar que es altamente portable, es muy flexible, genera código muy eficiente y permite escribir código muy compacto (se pueden realizar muchas funciones escribiendo pocas líneas de código). El C18 es una versión del C creada específicamente para los microcontroladores PIC18, que

por sus características resulta demasiado complicado la programación en su lenguaje de bajo nivel, el Assambler.

4.2.2 COMPILADOR MPLAB C18

El compilador MPLAB C18 es un compilador que optimiza el estándar ANSI C en los microcontroladores PIC18. El compilador modifica el estándar ANSI X3.159-1989 sólo en los puntos en los que se puedan crear conflictos con el soporte del microcontrolador.

El MPLAB C18 tiene las siguientes características:

- Compatibilidad ANSI ’89.
- Integración con el MLAB IDE para una mayor facilidad de realización y debut de proyectos.
- Admite ensamblador empotrado.
- Gran variedad de librerías.
- Optimización multinivel.
- Acceso transparente en la lectura/escritura de la memoria.
- Versión estudiante gratuita.

4.2.3 LIBRERÍAS DEL C18

Una librería es una colección de funciones agrupadas por referencia y facilidad de llamada. En este apartado aparecen las librerías utilizadas en el proyecto. Las librerías relacionadas con el USB no se instalan con el compilador, teniendo que descargarse de la página del fabricante; el resto se encuentran en la carpeta lib dentro de la carpeta de instalación del MPLAB C18.

4.3 IMPLEMENTACIÓN

Por las últimas implementaciones tecnológicas, tales como cámaras de video vigilancia vía IP (protocolo de internet), internet banda ancha y ahora la instalación de un sistema inmótico aplicado a cerraduras biométricas, tenemos:

- Instalación interna en las oficinas administrativas de la Facultad Técnica.
- Restricción a manejo de equipos por personas no autorizadas.
- Facilidad para mantenimiento preventivo y correctivo necesarios.

Figura 4-12 Puerta con cerradura instalada

4.3.1 MATERIALES

- Llaves (2 piezas.)
- 4 baterías AA.
- Placa delantera y placa trasera.
- Empaque interno y externo.
- Plantillas de instalación.
- Tornillos y cilindro de pestillo.
- Manual de usuario.
- Taladro

Figura 4-13 Materiales

Fig. 4-14 Materiales ferreteros

4.3.2 REQUERIMIENTOS DE INSTALACIÓN

- Material de puerta: metal, madera, fibra de vidrio, cristal, acero (cualquier puerta con un corte estándar).
- Grosor de puerta apto de 1-3/8 " - 2.0"
- Pestillo ajustable: 2 3/8 o 2 pulgada 3/4 backset.
- Encaje estándar 2-1/8 " para el diámetro del agujero de ajuste.

4.3.3 ASPECTOS TÉCNICOS

- Sensor de huella digital: Sensor Óptico.
- Resolución de sensor: 500 DPI (Dots Per Inch - Puntos por pulgada)
- Velocidad de lectura de autenticación: <1 seg.

- Métodos de autenticación: 1:N o 1:1.
- FRR: < 0.0001%
- Angulo de lectura del dedo: + 45°
- Escaneo de Huella: Una vez para conseguir la plantilla de la huella.
- Plantilla de huella digital: Todas las huellas se quedan guardadas al cambiarle las
- baterías.
- Sensor de luz: Resistente a la luz solar.
- Superficie de sensor: Cristal óptico con capa de PVD.
- Voltaje de operación: 4 pilas AA alcalinas. Corriente continua 4.5~6.0v.
- Vida útil de baterías: Aproximadamente 12 meses.
- Temperatura para almacenaje: -25°c-85°c.
- Corriente estática: 10uA.
- Corriente dinámica: 110mA~180mA.

Fig. 4-15 Pilas de uso

4.3.4 DISEÑO DE LA CERRADURA

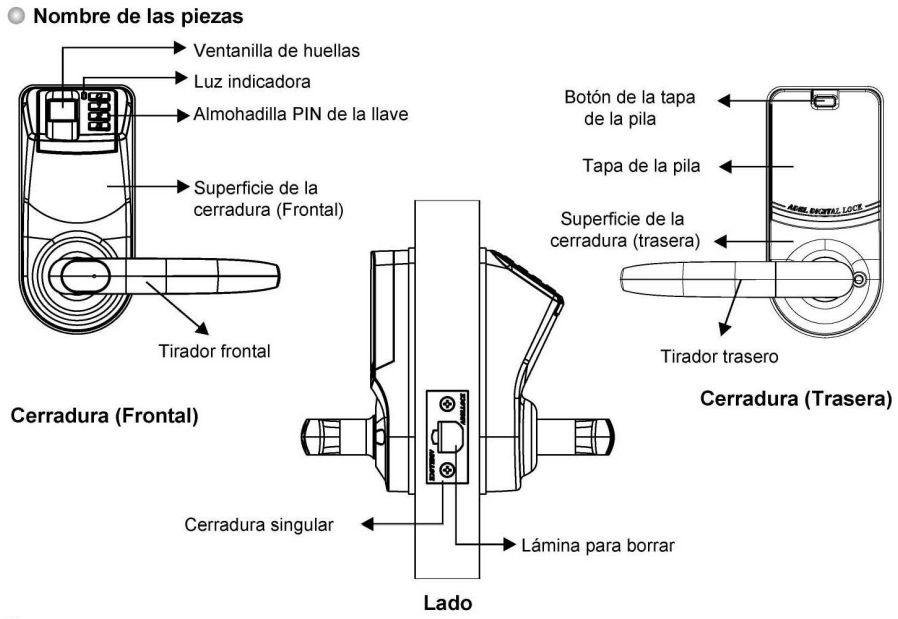


Figura 4-16 Diseño de la cerradura

4.3.5 INSTALACIÓN GENERAL

Como notarán en las imágenes, se procedieron a instalar las cerraduras biométricas en las puertas existentes en las oficinas de la Facultad Técnica para el Desarrollo de la Universidad Católica de Santiago de Guayaquil.

La obra civil tuvo que realizar el cambio de las cerraduras, es decir, la que regularmente se utilizaban por las nuevas cerraduras biométricas.

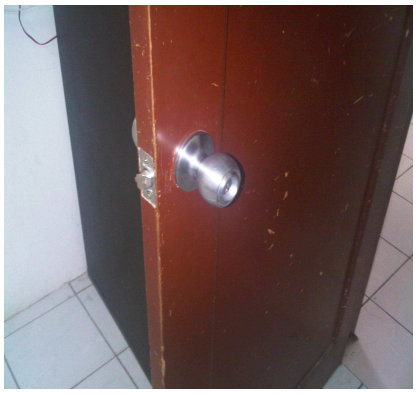


Fig. 4-17 Cerradura utilizada anteriormente

Figura 4-18 Nueva cerradura biométrica instalada

4.4 FUNCIONAMIENTO

Instrucciones de los botones para cerrar

Buttones	Function in setup state	Other functions
Buttone "0"	Activando la llave de la cerradura	
Buttone "1"	Entrando la programación	Principal del usuario del grupo
Buttone "2"	Entrando el modo de borrar	General de los usuarios del grupo
Buttone "3"	Entrando la posición del PIN (Identificación del Número Personal)	Provisional de los usuarios del grupo

Indicación del modo cerrado

1.Operación con éxito: la luz verde encendida, con dos bips largos.
2.Operación fallada: la luz roja encendida, con dos bips cortos.
3.La puerta abierta: por primera vez el motor eléctrico hace ruido rodante, esto indica que la puerta está abierta;
4.La puerta cerrada: por segunda vez el motor eléctrico hace ruido rodante, esto indica que la puerta está cerrada.
5.Entre el modo de pasar: la cerradura hace un bip después de instalar el programa; la luz verde se enciende y se apaga cada 5 segundos.

I.Asignación de la huella dactilary el PIN

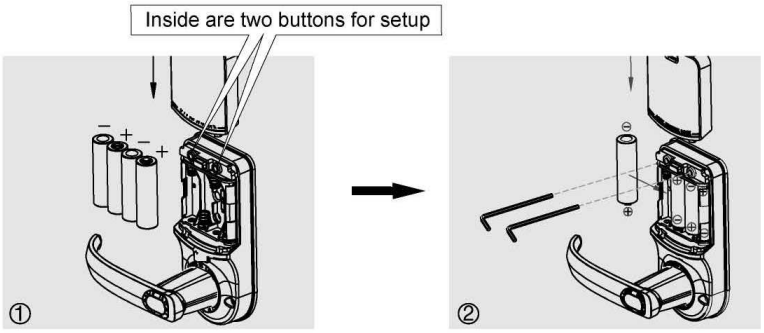
Tipo	Cantidad	Privilegio	
Huella principal	10	Añadir/Borrar huellas Programar PIN, y acceso general	Programando el modo de pasar
Huella secundaria	90	Acceso general	
Huella provisional	20	Acceso general	
PIN	1	Acceso general	

II.Unidad por defecto de fábrica:

Unidad por defecto de fábrica PIN: 1 2 3 1 2 3 1 2 3 1 2

Con la programación de fábrica cualquier huella puede abrir la puerta

III.Iniciación de la cerradura



1.Presione el botón de la tapa de la pila. Mueva la tapa de la pila hacia arriba y quítela, se puede ver un agujerito a cada lado, dentro de cada agujerito hay un botón para programar;

2.Quite cualquiera de las cuatro pilas, presionando los botones del lado frontal para confirmar que no hay eléctricidad, simultaneamente inserte dos objetos finos (ej. alambre) en los dos agujeritos para presionar los botones, sujete bien (no lo suelte) y vuelva a poner la pila. La cerradura ahora está en función. Si después de 5 segundos oye un sonido como "tut" la operación está completa y puede quitar los dos alambres.

Note: Después de empezar con la cerradura, todas las huellas y PINS programadas quedan anuladas; la cerradura vuelve al modo de fábrica. Cualquier dedo puede brir la puerta, huellas y PINS tienen que programarse otra vez.

IV.Programando las huellas principales, secundarias y provisionales

Programando la huella principal

Procedimineto de operación	Indicación de la cerradura
Presione el botón "0" para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier dedo en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete "1" para entrar el modo programador	La luz verde se enciendey se oye un bip
Presione "1" para entrar la huella principal	La luz verde se enciende y se oye un bip, la luz roja en la ventana está encendida
Ponga el dedo que se vaya a programar en la ventana de collección de huellas y presione dos veces	Cuando la luz roja está encendida, presione con el dedo; después de oir un bip quite el dedo y presione una vez más. Sonarán dos bips largos, la huella queda programada
La huella principal queda programada	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Note: 1.Cuando el producto es nuevo con defecto de fábrica, cualquier huella puede abrir la cerradura.
2.Después de haber programado la primera huella principal, la cerradura aceptará solo la huella principal.

Programando las huellas secundarias

Procedimineto de operación	Indicación de la cerradura
Presione el botón “0” para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete “1” para entrar el modo programador	La luz verde se enciende y se oye un bip
Presione “2” para entrar la huella secundarias	La luz verde se enciende y se oye un bip, la luz roja en la ventana está encendida
Ponga el dedo que se vaya a programar en la ventana de collección de huellas y presione dos veces	Cuando la luz roja está encendida, presione con el dedo; después de oir un bip quite el dedo y presione una vez más. Sonarán dos bips largos, la huella queda programada
La huella secundarias queda programada	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Programando las huellas provisionales

Huellas provisionales: Para estos que tengar acceso provisional (ej. Criada, Trabajadores, Amigos) Cuando desee puede borrar esta huellas.

Procedimineto de operación	Indicación de la cerradura
Presione el botón “0” para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete “1” para entrar el modo programador	La luz verde se enciende y se oye un bip
Presione “3” para entrar la huella provisionales	La luz verde se enciende y se oye un bip, la luz roja en la ventana está encendida
Ponga el dedo que se vaya a programar en la ventana de collección de huellas y presione dos veces	Cuando la luz roja está encendida, presione con el dedo; después de oir un bip quite el dedo y presione una vez más. Sonarán dos bips largos, la huella queda programada
La huella provisionales queda programada	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Programando el PIN

Procedimineto de operación	Indicación de la cerradura
Presione el botón “0” para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete “3” para entrar el modo PIN	La luz verde se enciende y se oye un bip
Entre 11 dígitos que quiera para el PIN (El PIN no puede empezar con “0”)	Después de entrar el PIN, la luz verde está encendida con dos bips largos, la programación del PIN queda completa
PIN queda puesto	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Notes:

1.El PIN tiene que tener 11 dígitos y no puede empezar con “0”.

2.Cuando se programa el PIN, si un PIN empieza con “0”, el PIN es inválido y no puede abrir la puerta.

V.Borrando huellas

Borrando la huella principal del usuario del grupo

Procedimineto de operación	Indicación de la cerradura
Presione el botón “0” para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete “2” para entrar el modo de borrar	La luz verde se enciende y se oye un bip
Presione “1” para confirmar que principal del usuario del grupo queda borrada	La luz verde está encendida , se oye un ruido fuerte, la luz roja se enciende y se oye un bip
La principal del usuario del grupo queda borrada y la operación queda completa	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Notes: 1. Una vez que la huella queda borrada, la cerradura volverá al estado de fábrica, todas las huellas quedarán borradas y el PIN volverá al modo de fábrica

2. Otro método para establecer el bloqueo de vuelta a ajuste de fábrica (Iniciación de la cerradura):
Presione el botón de la tapa de la pila. Mueva la tapa de la pila hacia arriba y quítela, se puede ver un agujerito a cada lado, dentro de cada agujerito hay un botón para programar;
Quite cualquiera de las cuatro pilas, presionando los botones del lado frontal para confirmar que no hay eléctricidad, simultaneamente inserte dos objetos finos (ej. alambre) en los dos agujeritos para presionar los botones, sujete bien (no lo suelte) y vuelva a poner la pila. La cerradura ahora está en función. Si después de 5 segundos oye un sonido como "tut" la operación está completa y puede quitar los dos alambres.

Borrando la huella secundarias del usuario del grupo

Procedimineto de operación	Indicación de la cerradura
Presione el botón "0" para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete "2" para entrar el modo de borrar	La luz verde se enciende y se oye un bip
Presione "2" para confirmar que secundarias del usuario del grupo queda borrada	La luz verde está encendida , se oye un ruido fuerte, la luz roja se enciende y se oye un bip
La secundarias del usuario del grupo queda borraday la operación queda completa	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

Borrando la huella provisionales del usuario del grupo

Procedimineto de operación	Indicación de la cerradura
Presione el botón "0" para activar la cerradura	Cuando la luz verde en la vetana de huellas está encendida, se oye un bip, la luz roja se enciende
Ponga cualquier huella principal en la ventana para entrar el modo de abrir	Cuando la luz verde está encendida, se oye un bip con un ruido rodante
Presione y sujete "2" para entrar el modo de borrar	La luz verde se enciende y se oye un bip
Presione "3" para confirmar que provisionales del usuario del grupo queda borrada	La luz verde está encendida , se oye un ruido fuerte, la luz roja se enciende y se oye un bip
La provisionales del usuario del grupo queda borraday la operación queda completa	Se oye un ruido rodante, la cerradura vuelve al estado cerrado

VI. Acceso con la huella y el PIN

Acceso con la huella

Procedimineto de operación	Indicación de la cerradura
Presione el botón “0” para activar la cerradura	La luz verde está encendida, se oye un bip y la luz roja en la ventana de huellas se enciende
Ponga cualquier huella en la ventana para reconocer	La luz verde está encendida, se oye un bip con un ruido rodante
Dé la vuelta el tirador para abrir la puerta	Si no, se cerrará automáticamente 5 segundos después

Access by PIN

Procedimineto de operación	Indicación de la cerradura
Directamente entre los 11 dígitos del PIN	La luz verde está encendida, se oye un bip con un ruido rodante
Dé la vuelta el tirador para abrir la puerta	Si no, se cerrará automáticamente 5 segundos después

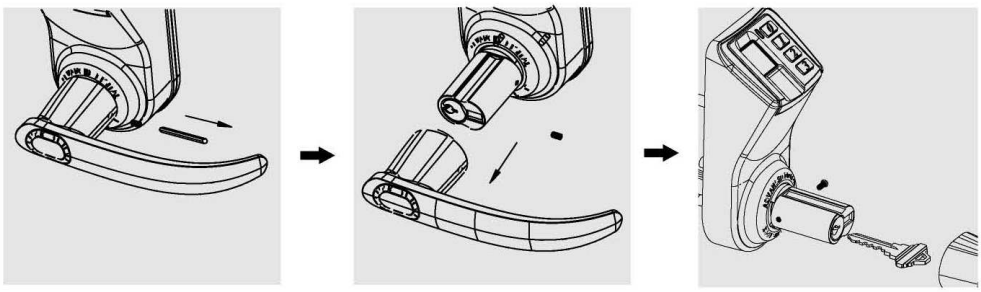
VII.Programando el modo de pasar

Presione y sujete el botón “0” 5 segundos después que la puerta se abre, el modo de pasar queda programado.

VIII. Cancelando el modo de pasar

Cuando la cerradura está en el modo de pasar, ponga una huella programada o entre una clave válida para cancelar el modo de pasar.

IX.Uso de la llave de urgencia



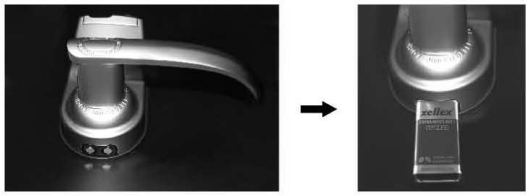
Quite el tornillo con un destornillador

Quite el tirador y podrá ver el ojo de la cerradura

Meta la llave y abra la puerta

X. Uso de electricidad externa

En caso de urgencia si la cerradura falla debido a insuficiente voltage, use una pila de 9V (tenga en cuenta los dos polos positivo y negativo) entre la huella o una de las claves restantes para abrir la puerta.



XI.Para cambiar las pilas

Procedimiento	Quite la tapa	Quite las pilas gastada	Ponga las pilas nuevas	La instalación de pilas está completa

Notes:

1.Cuando se ponen las pilas, tenga cuidado con el signo de los dos polos positivo y negativo.

2.Núnca mezcle las pilas nuevas con las viejas.

3.Cuide de el medio ambiente deshaciendose de las pilas gastadas en sitios designados para ello.

4.5 CULMINACIÓN DE LA INSTALACIÓN

La obra civil se realizó según lo planificado, se instalaron las cerraduras biométricas, se registraron las huellas de los usuarios correspondientes, se entregaron las llaves a cada uno de los usuarios y se dio una inducción para el uso de las cerraduras.

Luego se procedió a pintar las paredes de la Sala de Conferencias.

Figura 4-19 Culminación de Instalación.

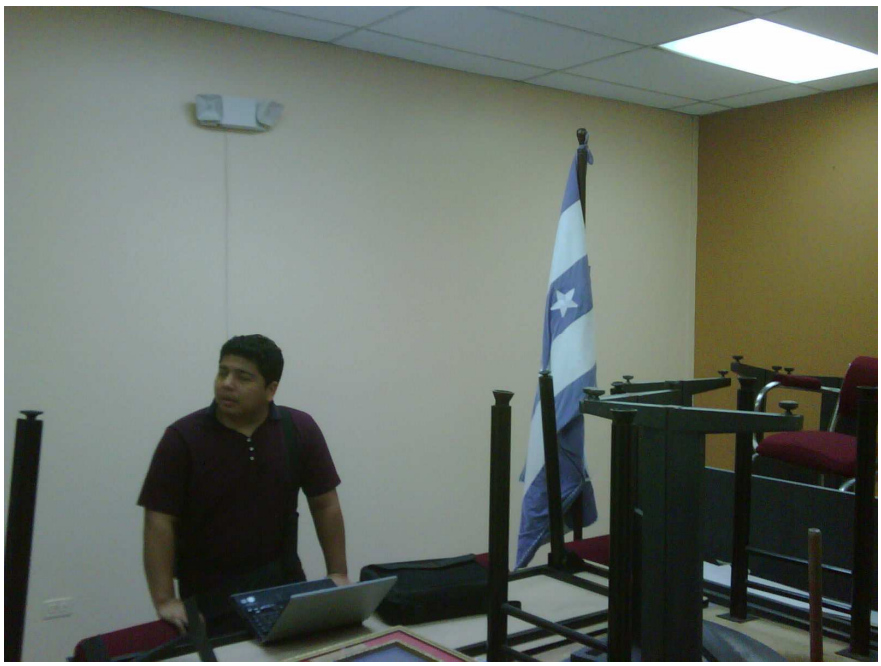


Figura 4-20 Pintado de la sala de profesores.

4.6 MÉTODO CORRECTO DE PONER LA HUELLA

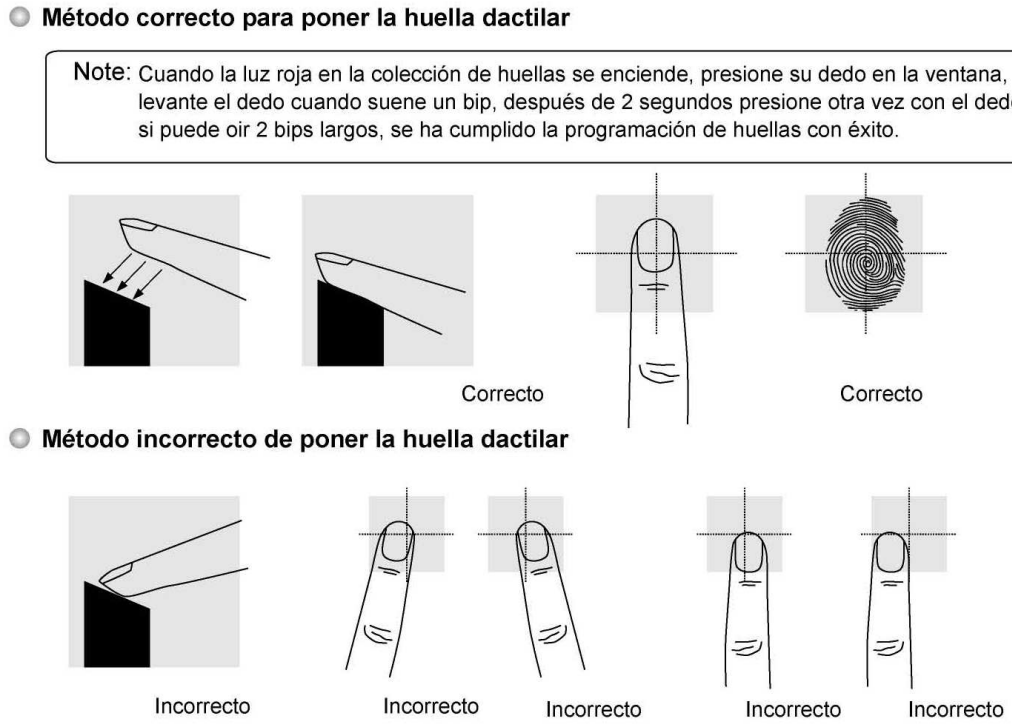


Figura 4-21 Método correcto de poner la huella.

CAPITULO 5

PRUEBAS Y AJUSTES DEL SISTEMA INMÓTICO APLICADO A SISTEMAS BIOMÉTRICOS

5.1 EQUIPOS BIOMÉTRICOS

Son 10 cerraduras portátiles, con sus respectivas baterías. Son de origen americano y están operativos y con una fácil configuración para el usuario administrador.

Figura 5-1 Cerradura biométrica

5.2 PRUEBAS CON LOS USUARIOS

Una vez ingresadas las huellas de los usuarios correspondientes, se procedió a realizar las pruebas necesarias para la satisfacción de los mismos.

También, se procedió a la enseñanza práctica de cómo poder agregar una nueva huella, ya que recordemos que en una oficina puede ser que trabajen más de una persona.

También se explicó cómo eliminar la huella de alguna persona que deje de tener acceso a la oficina.

Los usuarios se mostraron contentos y complacidos con esta instalación y realizaron preguntas, las cuales fueron respondidas a cabalidad dando a mostrar el conocimiento de esta nueva herramienta de trabajo.

5.3 INQUIETUDES

El Director de Carrera, nos hizo varias preguntas acerca de las cerraduras y su funcionamiento, para esto fuimos al lugar donde se encontraba una cerradura X y procedimos con una capacitación profunda para que tenga en cuenta en el día a día.

5.4 ENTREGA DE MANUALES DE USO

Con respecto a los manuales de usuario, se encuentran detallado en el capítulo , sin embargo procedimos con la entrega de manuales físicos al Director de Carrera, esto servirá de gran ayuda a las personas que tengan privilegios de Administrador, ya que son los únicos que podrán ingresar o eliminar huellas.

5.5 SATISFACCIÓN Y COMENTARIOS

Los usuarios se encuentran sumamente conformes con la instalación de este Sistema Biométrico, ya que representa avances en la tecnología de la Facultad de Educación Técnica de la Universidad Católica de Santiago de Guayaquil.

CONCLUSIONES Y RECOMENDACIONES

El diseño de este sistema inmótico aplicado a sistemas biométricos ha proporcionado conocimiento sobre tecnologías de automatización de edificios, dando un especial interés en la inmótica, tema elegido para el proyecto debido a factores como interoperabilidad, robustez, costos y el hecho de ser una tecnología del futuro en el Ecuador.

El interés por la inmótica se ha venido incrementando con rapidez. Muchas empresas y gobiernos están buscando aumentar la eficiencia de sus operaciones y reducir costos a través de esta tecnología. La oferta de este tipo de soluciones cada vez es mayor, en el mercado existen diversos fabricantes del hardware implementado, y están empezando a desarrollarse empresas dedicadas a la Inmótica, con aplicaciones empaquetadas o con desarrollos a la medida.

Se espera que en aproximadamente 5 años la tecnología de la Inmótica sea ubicua, ya que el costo de los componentes a utilizar, han venido bajando en los últimos años, lo cual permitirá el empleo masivo de esta tecnología y el surgimiento de muchas aplicaciones que aprovechen sus bondades.

El Sistema de Control de acceso implementado, intentó abarcar todos los elementos involucrados en el desarrollo de la Inmótica. El resultado fue un sistema funcional que permite controlar el acceso en determinados puntos y una fácil configuración del sistema para: agregar, quitar o modificar permisos a los usuarios.

Se seleccionó el sistema biométrico por sus ventajas en cuanto a seguridad. Diversos analistas, establecen que poco a poco las empresas que han instalado sistemas de

control de acceso en otras tecnologías, migrarán al sistema biométrico debido a la seguridad que se tiene con la huella biométrica ya que es única e irremplazable.

Aquí es donde la arquitectura orientada a la biometría toma importancia y apoyada con la Inmótica, da un gran poder de generación de procesos de negocio. El resultado de este tipo de herramientas son arquitecturas estándares, flexibles y fáciles de mantener.

Los beneficios son muchos, entre ellos está el mejoramiento del confort en el trabajo, seguridad para precautelar tanto los bienes materiales como inmateriales y lo más importante la seguridad de las personas.

Al contar con dispositivos de control automático que actuarán sobre los sistemas de control de acceso a oficinas para que operen únicamente cuando sea requerido, se logrará un retorno de la inversión en un corto plazo.

En nuestro país, dado el avance tecnológico y la implementación de nuevos sistemas multimedia y de telecomunicaciones acorde a las necesidades de desarrollo en la ejecución rápida y precisa de procesos, es menester, investigar y difundir el alcance que los sistemas domóticos en inmóticos ofrecen en la solución de automatización de viviendas y edificios. Para ello es recomendable, profundizar el tema de la seguridad como parámetro a controlar, teniendo en cuenta que el área de confort resulta ser secundaria, para así lograr satisfacer las necesidades económicas y sociales de nuestra nación.

.

BIBLIOGRAFIA

Errepar S.A. Santiago de chile.2007

Wayne Tomasi, Sistemas de Comunicaciones Electrónicas, Prentice Hall, Segunda Edición, 2006.

Angel Cardama A., Antenas, 3º. Ed. Alfaomega, 2004.

G. Drets & H. Liljenström, "Fingerprint Sub-Classification and Singular Point Detection", International Journal of Pattern recognition and Artificial Intelligence, vol. 12, no. 4, 407-422, 1998.

M. Eleccion, "Automatic Fingerprint Identification", IEEE Spectrum, vol. 10, 36-45, 1973.

R. González y R. Woods, Digital Image Processing, Addison-Wesley Publishing Company, Inc., 1992. Chap. 7.2.2.

L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998.

A. Hrechack and J. McHugh, "Automated Fingerprint Recognition Using Structural Matching", Pattern Recognition, vol. 23, no. 8, pp. 893-904, 1990.

Paginas webs:

http://es.wikipedia.org/wiki/Biometr%C3%ADa

http://www2.ing.puc.cl/~iing/ed429/sistemas_biometricos.htm

www.tecnoedu.com/

http://personales.com/colombia/bucaramanga/inmotica_domotica/inmotica.html

es.wikipedia.org/wiki/Inmótica

www.softwaredelhogar.net/hogar.../inmotica.php

http://es.wikipedia.org/wiki/Diodo_emisor_de_luz

ANEXO 1

PRESUPUESTO DE LA IMPLEMENTACIÓN DE CERRADURAS DE RECONOCIMIENTO BIOMETRICO

GRUPO FORTALEZA

ANEXO FACTURA No: 0265

COMPRADOR: UCSG

RUC:

DIRECCIÓN:

ATENCIÓN:

FECHA: 1 de Julio del 2010

DESCRIPCIÓN	VALOR	CANT.	SUBTOTAL
Cerradura			
Cerraduras biométricas:			
Sensor biométrico	125,00	10	1250,00
Microncontrolador PIC 18F2550	20,00	10	200,00
Memoria serial 24F1024	20,00	10	200,00
Componentes electrónicos varios por cerradura	100,00	10	1000,00
Placas de circuito impreso	80,00	10	800,00
Estructura metálica	150,00	10	1500,00
Baterías 2A	$1,50	40	60,00
Adecuación e Instalación de las cerraduras	$30,00	10	300
biométricas			
SUBTOTAL			5.310,00
.			
IVA 12%			637,20
		TOTAL	5.947,00