IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO AL LABORATORIO DE MÁQUINAS UNO EN EL TECNOLÓGICO PASCUAL BRAVO INSTITUCIÓN UNIVERSITARIA

HERNÁN DANILO AGUDELO ESPINOSA

CESAR AUGUSTO SUÁREZ CLAVIJO

WILFRED FERNEY SANTA VÉLEZ

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

FACULTAD DE INGENIERIA

TECNOLOGÍA EN ELECTROMECÁNICA

MEDELLÍN

2013

IMPLEMENTACIÓN DE UN SISTEMA DE SEGURIDAD PARA EL ACCESO AL LABORATORIO DE MÁQUINAS UNO EN EL TECNOLÓGICO PASCUAL BRAVO INSTITUCIÓN UNIVERSITARIA

HERNÁN DANILO AGUDELO ESPINOSA

CESAR AUGUSTO SUÁREZ CLAVIJO

WILFRED FERNEY SANTA VÉLEZ

TRABAJO DE GRADO PARA OPTAR POR ELTITULO DE TECNOLOGO EN ELECTROMECÁNICA

Asesor

ARLEY SALAZAR HÍNCAPIE

INSTITUCIÓN UNIVERSITARIA PASCUAL BRAVO

TECNOLOGÍA EN ELECTROMECÁNICA

FACULTAD DE INGENIERIA

MEDELLÍN

2013

NOTAS DE ACEPTACIÓN

_____

_____

_____

_____

_____

_____

_____

_____

Presidente del Jurado

_____

Firma del jurado

_____

Firma del jurado

Medellín, Mayo 2013

AGRADECIMIENTOS

A Dios por cada día y los favores recibidos, a mi madre como siempre por su entrega.

Dedicado a mi hija Valentina Agudelo “estudia, trabaja y se gente primero allí está la salvación”

A mis compañeros de proyecto Cesar y Wilfred mil gracias.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

ACEPTABILIDAD: Que tanta aprobación tiene la tecnología entre el público.

ANTROPOMETRÍA: es la sub rama de la antropología biológica o física que estudia las medidas del hombre. Se refiere al estudio de las dimensiones y medidas humanas con el propósito de comprender los cambios físicos del hombre y las diferencias entre sus razas y sub-razas. En el presente, la antropometría cumple una función importante en el diseño industrial, en la industria de diseños de vestuario, en la ergonomía, la biomecánica y en la arquitectura, donde se emplean datos estadísticos sobre la distribución de medidas corporales de la población para optimizar los productos

AUTOMATIZACIÓN: El término automatización se refiere a una amplia variedad de sistemas y procesos que operan con mínima o sin intervención del ser humano. El alcance va más allá que la simple mecanización de los procesos ya que ésta provee a operadores humanos mecanismos para asistirlos en los esfuerzos físicos del trabajo, la automatización reduce ampliamente la necesidad sensorial y mental del humano.

BIFURCACION: característica de una huella dactilar, que consiste en la separación de varias de sus líneas

BASE DE DATOS: Una **base de datos** o **banco de datos** (en ocasiones abreviada con la sigla *BD* o con la abreviatura *b. d.*) es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

BIOMETRÍA: Estudio mensurativo o estadístico de los fenómenos o procesos biológicos, es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas, teniendo así un registro.

CALIDAD: que tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica.

CARACTERISTICA BIOMETRICA: es un rasgo que posee cada persona para ser identificado; que posee en una parte del cuerpo.

CRESTA: Es la parte sobresaliente en las huellas, relieve.

DIGITALIZAR: Acción de convertir en digital información analógica. En otras palabras, es convertir cualquier señal de entrada continua (analógica) en una serie de valores numéricos.

ESTANDAR: Dentro de los parámetros establecidos

EXTRACCION: Forma de tomar la muestra biométrica para la base de datos.

Por ejemplo, una fotografía en papel puede digitalizarse para que pueda ser procesada en una computadora (u otro dispositivo digital similar).

FIABILIDAD: Que tan fácil es engañar al sistema de autenticación.

HISTERESIS: Tendencia de un material por conservar una de sus propiedades.

IRIS: El **iris**, en anatomía, es la membrana coloreada y circular del ojo que separa la cámara anterior de la cámara posterior. Posee una apertura central de tamaño variable que comunica las dos cámaras: la pupila.

LED: Pequeño diodo luminoso que se instala en los ordenadores y que se ilumina para indicar que el sistema está encendido.

PARÁMETRO: Dato o factor que se toma como necesario para analizar o valorar una situación.

PATRON BIOMETRICO: Componente que sirve para cotejar una extracción biométrica, con la base de datos, para verificar la identificación de una persona.

PDA: Un PDA (Personal Digital Assistant o Ayudante personal digital) es un dispositivo de pequeño tamaño que combina un ordenador, teléfono/fax, Internet y conexiones de red.

A los PDAs también se les llama palmtops**,** hand held computers (ordenadores de mano) y pocket computers (ordenadores de bolsillo).

Un PDA típico puede funcionar como teléfono móvil, fax, explorador de internet, organizador personal, GPS, etc.

PERÍMETRO: La palabra perímetro proviene del latín perímetros, que a su vez deriva de un concepto griego. Se refiere al contorno de una superficie o de una figura y a la medida de ese contorno. Conocer el perímetro de un campo, por ejemplo, permite definir qué cantidad de material se necesita para alambrarlo. De igual forma, el perímetro es un dato esencial para diseñar la seguridad de una casa o de un barrio cerrado.

PERMANENCIA: que tanto perdura la huella biométrica en el tiempo de manera inalterable.

PLUG DACTILAR: El Plug Dactilar es un dispositivo de control de accesos por biometría dactilar de fácil instalación y robusto.

PLUG VASCULAR: La tecnología biométrica vascular de dedo tiene muchas ventajas sobre otros tipos de biometría (como la biometría facial, de palma de la mano, de iris, o de huella dactilar): Alta precisión en la identificación; la tolerancia a la erosión del dedo. El patrón biométrico es interno, no deja rastro por lo tanto es mucho más seguro Y la falsificación es prácticamente imposible

RECOLECTABLE: Que tan fácil es la adquisición, medición y almacenamiento de la huella biométrica.

SINGULARIDAD: que tan único o diferenciable es la huella biométrica entre uno y otro individuo.

TERMINACION: Finalización de una huella

UNIVERSALIDAD: que tan común es encontrar este biométrico en los individuos.

VALLE: Parte plana de la huella dactilar, sin relieve

RESUMEN

Los sistemas han facilitado la implementación de algunas aplicaciones para optimizar los procesos industriales; es así como los medios en los cuales se almacena una información de un proceso, aplicación u otra variable que se puede controlar han tenido una evolución a través de los años y de la mano de la investigación han surgido nuevas técnicas para la identificación de las personas.

El reconocimiento de patrones exclusivos de cada ser humano, que se hacen irrepetibles e inmodificable con el tiempo, arrojan una cantidad de señales que hacen parte de lo que se llama biometría y que tiene aplicación en la identificación de una persona por medio de la comparación de un rasgo físico obtenido de manera anticipada y almacenado en una base de datos, la cual es la encargada de la comparación de este rasgo con otro tomado de manera momentánea.

La respuesta del sistema es emitir un porcentaje de coincidencia de los rasgos físicos comparados para determinar si esa persona que se coteja frente a la base de datos si es quien dice ser.

Estas características físicas pueden ser las huellas dactilares, las características de la retina o del iris, la geografía de la mano, entre otros; estos rasgos se llevan a los sistemas para controlar el acceso a ciertos recintos, manejar cuentas bancarias o cualquier aplicación que requiera un mínimo de tecnología aplicada a la seguridad.

La seguridad en los sistemas se puede realizar también por medio de tarjetas o combinando los sistemas de lectura de tarjeta y lectura de biometría, esto para facilitar los accesos y para tener un alto nivel de seguridad.

Este trabajo es una investigación de los sistemas de identificación de personas por medios tecnológicos y biométricos, aplicados a dispositivos que facilitan los accesos a los recintos donde se implementen. Es una guía para la aplicación y comprensión de los diferentes medios de identificación de las personas.

La implementación de un sistema de control de acceso a un recinto; hace que un sin número de disciplinas correlacionen para lograr el desarrollo de un producto; que permite la innovación tecnológica de un sistema. Mejorando de manera notoria las condiciones primarias de los controles de acceso aun recinto, beneficiando un público objetivo, pero con facilidad de expansión del mercado.

ABSTRACT

The systems have facilitated the implementation of some applications to optimize industrial processes is and means in which information is stored in a process, application or other variable that can be controlled have evolved through the years and hand research new techniques have emerged to identify people.

Pattern recognition unique to each human, which are unrepeatable and unchanging over time, show a number of signs that are part of what is called biometrics and has application in the identification of a person by comparing a physical trait obtained in advance and stored in a database, which is responsible for the comparison of this characteristic with other taken momentarily.

The system's response is to issue a percentage matching physical features compared to determine if that person is checked against the database if you are who you say.

These physical characteristics can be fingerprints, the characteristics of the retina or iris, hand geography, among others, these traits are carried systems to control access to certain precincts, manage bank accounts or any application requiring a minimum of technology applied to security.

Security systems may also be performed by combining the card or card reader systems and biometric reading this to facilitate access and to have a high level of security.

This work is an investigation of the person identification systems through technological and biometric devices applied to facilitate the access to the sites where they are implemented. It is a guide for the application and understanding of the different means of identifying individuals.

The implementation of an access control system to an enclosure; makes countless of disciplines correlate to achieve product development, technological innovation that allows a system. Markedly improving the primary conditions of access controls even grounds, benefiting one target audience, but with ease of market expansion.

INTRODUCCIÓN

La automatización en los procesos, la digitalización de los elementos y la información, los teléfonos personales, las transacciones en línea, en otra época era una idea futurista y algo alocada. En la actualidad es una realidad donde cada elemento diseñado tiene un gran porcentaje de tecnología al servicio del hombre, permitiéndole manejar su casa, sus asuntos laborales, sus cuentas personales con la misma seguridad y efectividad como si lo hiciera desde, su casa, su trabajo o su banco. Todo esto hoy es posible gracias a los sistemas de seguridad, que permiten identificar los usuarios por dispositivos láser, biométricos y base de datos.

El Tecnológico Pascual Bravo Institución Universitaria, es reconocido a nivel local y nacional por la formación de profesionales idóneos en todas sus áreas, este reconocimiento en gran parte se debe a la formación de personas capaces de desarrollar sus habilidades en el campo práctico; gracias a la educación impartida en los laboratorios de la institución.

Sin embargo se analizó que los laboratorios de la institución aunque cuentan con la seguridad requerida para almacenar herramientas como voltímetros, board, pinzas, multímetros, osciloscopios, motores, silletería y todos los elementos de un aula de clase, no cumplen con una base de datos o un registro mínimo de información de quien utiliza los laboratorios y cuando; para poder llevar un control de los elementos del laboratorio y del personal que ingrese a este .

Para resolver el problema de la falta de información o de registro en el laboratorio, para dejar un legado tecnológico a los futuros estudiantes y se piensa que es pertinente retribuir a la institución, por las bases y conocimientos brindados en la etapa formativa de los estudiantes de electromecánica, se realiza un trabajo de investigación, el cual proporcione la seguridad necesaria al laboratorio de máquinas, por medio de la utilización de dispositivos de seguridad láser, biométricos y bases de datos, que se instala en la entrada del laboratorio para el control de acceso de los usuarios

Es así como la institución inicia el proceso de automatización y modernización para brindar a la comunidad universitaria y en general un ambiente tecnológico, que incremente la calidad de los servicios prestados por esta y permita conservar el buen nombre y prestigio del cual se goza a nivel nacional

1. DESCRIPCION DEL PROBLEMA

El Tecnológico Pascual Bravo Institución Universitaria, es reconocido a nivel nacional y local por la calidad de sus carreras, enfocadas a satisfacer las necesidades de la industria.

Uno de los factores determinantes en la formación y el reconocimiento de los profesionales del Pascual Bravo es la capacidad de desarrollar sus habilidades en el campo practico, el cual se fortalece en la institución durante las prácticas de laboratorio, donde se utiliza un sin número de elementos y accesorios aplicables a cada disciplina como lo son los multímetros, calibradores, motores, voltímetros, silletería en general y la planta física .Estos espacios están abiertos a los docentes y a los estudiantes, pero no tiene un control que sea capaz de identificar a los usuarios que ingresan al laboratorio.

Se observa que el laboratorio de máquinas uno no tiene un dispositivo de seguridad que regule el ingreso a este, generando inseguridad que se ve representada en la perdida de los elementos del laboratorio, que a su vez genera retrasos en el aprendizaje de los alumnos, que se puede ver reflejada a futuro en la pérdida del reconocimiento de calidad del que goza la institución.

Este problema puede generar deserción en los alumnos existentes y apatía en los futuros estudiantes del Tecnológico, se realiza un trabajo de campo en el cual se efectúa una observación, esta ratifica que el laboratorio de maquinas uno no cuenta con un sistema de control para el acceso.

Por tal motivo es necesario implementar un sistema de seguridad para el laboratorio que permita la identificación de los usuarios en el momento del ingreso a este, es así como la institución da el primer paso hacia la modernización y tecnificación de sus servicios, por medio de dispositivos biométricos, láser y bases de datos, en pro del bien común.

2. JUSTIFICACIÓN

El Tecnológico Pascual Bravo Institución Universitaria, goza de gran prestigio a nivel nacional y local por la calidad de sus carreras, que satisfacen las necesidades de la industria por obtener profesionales idóneos para sus cargos.

El prestigio de los egresados y alumnos de la institución se fundamenta en las habilidades adquiridas en las prácticas de laboratorio, por tal motivo es pertinente conservar los laboratorios en condiciones optimas, al igual que los elementos que en el se encuentran. Es allí donde la institución marca la diferencia con otras de su misma naturaleza y es un deber de todos conservar el reconocimiento de calidad.

Es así, como para conservar todas estas condiciones planteadas se define un proyecto para el laboratorio de maquinas uno dentro de la institución, que consta de establecer unos parámetros biométricos, de almacenamiento de datos, por reconocimiento dactilar por láser que permita el acceso de los estudiantes y docentes de la institución al laboratorio, se pretende que una persona sea identificada en el momento del ingreso al laboratorio, haciéndose responsable de este y de sus elementos, de esta forma el Tecnológico aplica los conceptos de electrónica, electromecánica y automatización siendo pionera en innovación en su planta física y accesos a esta.

Se pretende dejar a través de este trabajo de investigación un legado tecnológico para los futuros estudiantes, además se realiza este para dar solución a un problema localizado en el cual se aplique los conceptos obtenidos a lo largo de la carrera, dando así una retribución por parte de los estudiantes a la institución.

El trabajo tendrá como público objetivo a los usuarios del laboratorio, ya sean estudiantes o docentes, los cuales trabajan en un ambiente de tecnología y seguridad, que garantiza el buen desempeño de todos, además se rompe el esquema de lo convencional de chapas y cerraduras para la seguridad del laboratorio.

De esta forma la institución da el primer paso para la modernización de seguridad en la planta física, porque al tener un laboratorio sistematizado, es más fácil aplicar los resultados de este a los otros laboratorios, convirtiendo a la universidad en potencia a nivel de dispositivos de innovación tecnológica en el ámbito local

3. OBJETIVOS DEL PROYECTO

3.1 OBJETIVO GENERAL

Implementar un sistema de seguridad para el acceso al laboratorio de máquinas uno en el Tecnológico Pascual Bravo Institución Universitaria. Mediante la utilización de dispositivos de seguridad láser, medios biométricos y base de datos que permitan la identificación de los usuarios al ingresar al laboratorio.

3.2 OBJETIVOS ESPECÍFICOS

- Recopilar, la información de dispositivos de seguridad láser, biométricos y bases de datos existentes en el mercado, teniendo como premisa el estado del arte (antecedentes y evolución).
- Clasificar la información encontrada, sobre dispositivos de seguridad.
- Estudiar la normatividad acerca de los sistemas y dispositivos de seguridad.
- Elegir un dispositivo de seguridad, para ser adaptado en el laboratorio de máquinas uno.
- Sugerir la implementación de un dispositivo de seguridad en el laboratorio.

4. MARCO DE REFERENCIA

4.1 MARCO TEÓRICO.

Desde que las sociedades se asentaron, en tiempos pasados, el hombre a buscado mecanismos, sistemas o elementos para proteger sus bienes y a sus familias. A medida que la humanidad evolucionaba las causas de la inseguridad se tornaron más complejas y es allí donde los entornos cambiaron para delimitar, espacios, bienes, territorios u otros elementos que requieran de la seguridad.

Es así como se inicia la era de la propiedad privada y con esta las puertas, cercas, candados, llaves, cadenas que permitieron proteger los bienes, pero como la evolución se da en todos los aspectos la parte de hurtos y maniobras evasivas para ingresar a espacios privados también lo hizo, dándole a los sistemas y la tecnología la oportunidad de intervenir para solucionar la necesidad de brindar seguridad de la mano de la modernización y automatización, para mantener los bienes fuera del alcance de los amigos de lo ajeno.

Cuando hacemos referencia a un sistema de seguridad no estamos hablando únicamente de sensores, cámaras y alarmas, sino también de puertas blindadas, persianas protegidas y rejas de seguridad. Podemos decir que la elección de un tipo de sistema u otro dependerá de las necesidades de cada familia o individuo, esta necesidad varía de acuerdo a la cultura del entorno, el estándar de vida y los factores psicológicos directos.

Entendiendo el concepto de sistemas de seguridad como el conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar las presencia, irrupción, o invasión de un desconocido o de un individuo que no posea un acceso permitido. Actualmente el mercado ofrece una gran gama de dispositivos que permiten proteger los bienes de una sociedad, de una empresa o de un usuario.

Los sistemas de seguridad se remontan mucho tiempo atrás y quizás los primeros registros de almacenamiento de datos y de biometría, teniendo como objetivo la identificación de cada persona, data del siglo XIV en china donde plasmaban la palma de la mano y de los pies de los niños, mas adelante los hombres fueron analizando y estudiando la antropometría de las personas para concluir que las huellas dactilares eran diferentes, es así como estos registros se hicieron de gran utilidad para la sociedad, porque con estos se podía reconocer a un criminal o a cualquier persona del cual se tuviera datos dactilares.

De las marcas borrosas del siglo XIV se pasa a la era tecnológica donde se almacenan datos a gran escala para permitir la identificación de los individuos en cualquier parte y en un instante y esta identificación se llama biometría.

La biometría se dedica al estudio estadístico de las características cuantitativas de los seres vivos: peso, longitud, etc. Sin embargo en épocas más recientes la biometría también se utiliza para referirse a los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas.

El termino biometría viene del griego "bio" que significa vida y "metría" que significa medida de acuerdo al significado otorgado por la real academia de la lengua española biometría es el estudio mensurativo o estadístico de los fenómenos o procesos biológicos, sin embargo más recientemente y para el tema que nos concierne el significado de biometría es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas.

Se establecen 2 tipos dependiendo de los aspectos físicos o aspectos vinculados a la conducta, hablamos de Biometría Estática y Biometría Dinámica.

Biometría Estática contiene las siguientes características:

Huella dactilar, características del ojo: Retina e Iris, rayas de la mano, geometría de la mano, poros de la piel, emisiones térmicas.

Biometría Dinámica contiene las siguientes características:

Escritura manuscrita, voz, tecleo, gesto y Movimiento corporal

El objetivo final de la utilización de las características enunciadas anteriormente es poseer un conjunto de herramientas que permitan conseguir bien la identificación y la verificación de la identidad de una persona.

4.1.1 Historia de la Biometría: la primera referencia acerca del uso de una característica biométrica con fines identificativos se remonta al siglo VIII, fecha en la que se encuentran en China huellas dactilares tanto en documentos como en esculturas de arcilla.

En 1856, sir William Herschel fue el primero en implementar la huella del pulgar como método de identificación en documentos para personas analfabetas.

En 1880 Henry Faulds, un medico escocés que trabajaba en Tokio, publicó un artículo en la revista Nature en el que sugería que las huellas dactilares encontradas en la escena de un crimen podían identificar al culpable.

En 1941. Murray Hill de los laboratorios Bell inició el estudio de la identificación por voz, sus trabajos fueron redefinidos por L.G. Kersta. En 1986 sir Alec Jeffreys utilizó por primera vez el ADN para identificar al autor de unos asesinatos en Inglaterra.

A partir de mediados y finales de los 90 el interés ha ido creciendo y en paralelo han aumentado los presupuestos de financiación para la investigación y desarrollo vinculados a la Biometría.

La biometría se soporta en siete pilares o conceptos básicos que son:

- **Universalidad:** que tan común es encontrar este biométrico en los individuos.
- **Singularidad:** que tan único o diferenciable es la huella biométrica entre uno y otro individuo.
- **Permanencia:** que tanto perdura la huella biométrica en el tiempo de manera inalterable.
- **Recolectable:** Que tan fácil es la adquisición, medición y almacenamiento de la huella biométrica.
- **Calidad:** que tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica.
- **Aceptabilidad:** Que tanta aprobación tiene la tecnología entre el público.
- **Fiabilidad:** Que tan fácil es engañar al sistema de autenticación.

En la biometría se distinguen dos grupos de registros biométricos los fisiológicos o morfológicos y los conductuales.

Los biométricos morfológicos o fisiológicos son aquellos que se soportan sobre características físicas inalterables y presentes en la mayoría de los seres humanos tales como: huella dactilar, geometría de la mano, características del iris, patrones vasculares de la retina, mano, etc.

Los biométricos conductuales son aquellos que se soportan sobre características de la conducta del ser humano tales como: pulsaciones del teclado, discurso, dinámica de la firma, entre otros.

4.1.2 El cuerpo humano y la biometría: El sujeto fundamental de la Biometría es el cuerpo humano. El estudio de la Biología nos enseña que las características externas que observamos en los individuos y que son estudiados por la Biometría, corresponden con las características genéticas heredadas que hacen a cada individuo singular.

A pesar de esta gran variedad, la biometría ve limitado su nivel de actuación a un subconjunto de características, sobre todo sin nos centramos en aspectos relacionados con el control de acceso por ejemplo a un recinto o a un sistema informático.

De todas las características biológicas presentes en los seres humanos con capacidad de ser medidas y por tanto susceptibles de ser utilizadas por la biometría podemos considerar 2 grupos, las que se centran en características estructurales y las que se centran en características de tipo funcional.

- **Características estructurarles:** Los sistemas óseo y muscular en el caso de la cara y la mano, el ojo en el caso de la retina y el iris, la piel en el caso de las huellas dactilares.
- **Características funcionales:** Sistema óseo y muscular en el caso del movimiento corporal, incluye la escritura y la dinámica del tecleo, labios, lengua, faringe, laringe, etc., en el caso del habla.

4.1.3 Ventajas de la biometría frente a los métodos tradicionales de autenticación: La biometría permite soslayar la mayor parte de estas dificultades y problemas y por otra parte permite facilitar el acceso de los sistemas informáticos a usuarios no expertos sin necesidad de recordar complejas contraseñas y permitiendo incrementar el nivel de privilegios de los usuarios sin arriesgar en perdida de seguridad. Si no se utiliza una técnica de identificación biométrica, no se puede asegurar que sea la misma persona la que accede a un mismo sitio cuando utiliza un sistema de identificación de contraseña o mediante un token. Solamente la identificación biométrica nos lo puede asegurar.

4.1.4 Términos y procesos biométricos claves: Una de las características más valoradas de los sistemas biométricos es su capacidad de que sean automatizados.

El modo de organizar la automatización en un sistema biométrico es la siguiente:

Deben existir dispositivos que permitan la captura de los datos biométricos (escáner para leer huellas dactilares, sistema de registro de voz, etc.) La obtención de estos datos no es tan sencilla como aparenta ser. Por una parte los dispositivos para la captura de la información deben presentar unos márgenes de tolerancia adecuados para permitir la reproductibilidad de la información capturada en momentos distintos.

Un aspecto significativo es la calidad de los datos adquiridos durante el proceso de darse de alta. La calidad de los mismos va a depender entre otros aspectos del número de muestras que se tomen de cada usuario. Esto es debido a que las condiciones de toma de las mismas pueden variar con el tiempo, adicionalmente la toma de varias muestras permite utilizar datos promedio.

Los datos biométricos capturados son normalmente información sin procesar: imágenes, registros de voz, tiempos de pulsación de teclas, etc. Reciben el nombre de muestras biométricas y no pueden ser utilizadas para el proceso de reconocimiento, debido, entre otras cosas, a su complejidad y tamaño. Por ello es preciso que esta información sea procesada con el fin de extraer las características que vayan a ser utilizadas durante el proceso de identificación o verificación.

4.1.5 Tecnologías biométricas

- **Recopilación de datos:** El subsistema abarca todos los aspectos relacionados tanto con la fase de darse de alta en el sistema como con los procedimientos de identificación y verificación que se lleva a cabo cuando un usuario pretende acceder a un sistema controlado mediante técnicas biométricas.

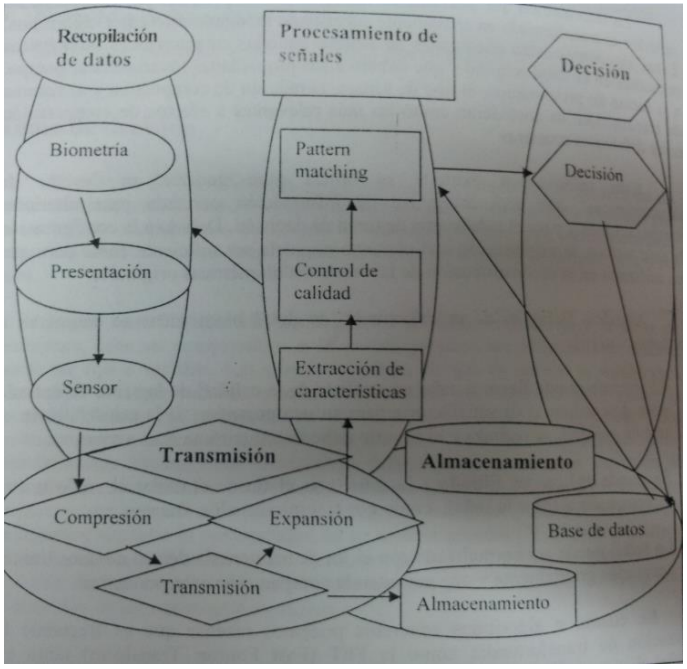
- **Transmisión de datos:** Utilizar técnicas de compresión digital de la información. La transmisión de información puede presentar problemas de incorporación de ruido, sobre todo si se utilizan señales analógicas. En este caso es especialmente significativa la utilización del canal telefónico para reconocimiento mediante voz del interlocutor.

- **Procesamiento de señales:** El sistema puede llevar a cabo un análisis de la calidad de la señal de entrada para determinar si es satisfactoria para su uso posterior. Si la señal falla en el test de calidad, se rechaza y el usuario debe introducir una nueva muestra. La señal puede ser normalizada con el fin de mantenerla dentro de unos límites aceptados previamente y que permitan la comparación entre muestras.

- **Almacenamiento de datos:** La información registrada durante la fase de inscripción o procedimiento de darse de alta debe almacenarse en forma estructurada para facilitar el procedimiento de identificación y verificación.

- **Proceso de decisión:** El proceso de identificación y verificación se culmina con la medida de un índice de comparación entre las plantillas almacenadas y los datos introducidos por un usuario en un momento cualquiera de acceso al sistema. Este índice permitirá tomar una decisión acerca de si la información / verificación es satisfactoria o no lo es.

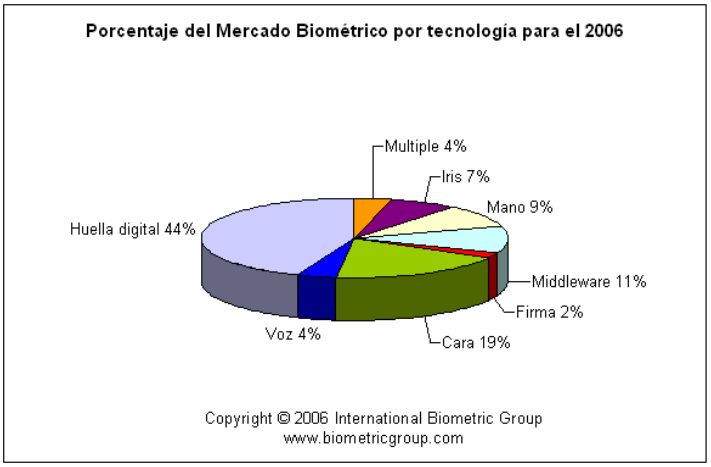
Figura 1: Proceso de decisión.



Tomado marzo 28 de 2013libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

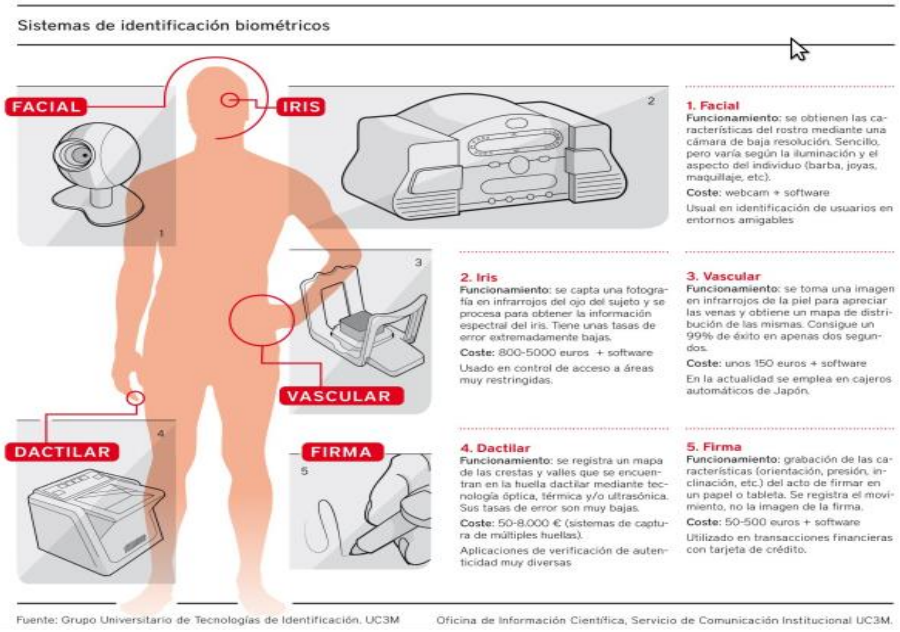
4.1.6 Modalidades biométricas: Las tecnologías biométricas de mayor uso hoy y con más apoyo por las industrias comerciales son: la huella digital, el reconocimiento facial, la geometría de la mano, el iris, la voz, la firma.

Figura 2: Porcentaje mercado biométrico por tecnología para el 2006.



Tomada Internet marzo de 2013, www.biometricgroup.com

Figura 3: Sistemas de identificación biométricos.



Tomado de Internet marzo 30 de 2013 www.biometricgroup.com

4.1.7 Evaluación y rendimiento

La realización de evaluaciones y medidas de rendimiento de los sistemas biométricos fiables es costosa, ya que es preciso realizar una recopilación de datos bastante exhaustiva, analizar dichos datos, extraer las conclusiones y elaborar la documentación pertinente. A sí mismo es preciso que quien realiza dichas pruebas cuente con la objetividad e independencia necesaria para asegurar unos criterios validos y que sean aceptados por todos los fabricantes implicados en el desarrollo de soluciones en el área de la biometría.

4.2 INTRODUCCION AL RECONOCIMIENTO DE PATRONES

El reconocimiento de patrones es la ciencia que se encarga de la descripción y clasificación (reconocimiento) de objetos, personas, señales, representaciones, entre otros.

Si bien el margen de aplicaciones es muy amplio, las más importantes están relacionadas con la visión y audición por parte de una maquina, de forma análoga a los seres humanos.

4.2.1 Dificultad intrínseca del reconocimiento de patrones: El conocimiento de los mecanismos llevados a cabo por los humanos para reconocer objetos dentro de una imagen o identificar personas, es de utilidad a la hora de implementar sistemas automáticos mediante el ordenador, puesto que este podrá emular los procesos llevados a cabo por las personas.

4.2.2 Aproximaciones al reconocimiento de patrones

Existen 3 aproximaciones principales al problema de reconocimiento de patrones:

- **Reconocimiento estadístico de patrones (o teoría de la decisión)**
- **Reconocimiento sintáctico de patrones (o estructura)**
- **Reconocimiento basado en redes neuronales:** Por otra parte, el reconocimiento de patrones está relacionado con otros campos, tales como:

Tratamiento de voz e imagen, visión artificial, entre otros. Inteligencia artificial, redes neuronales, gramáticas formales, teoría de la estimación y optimización.

4.2.3 Esquema general de un sistema de reconocimiento de patrones: Consta de varias etapas relacionadas entre sí (los resultados de una etapa pueden modificar los parámetros de etapas anteriores). El objetivo es ajustar el sistema para que sea capaz de clasificar señales u objetos de entrada, en una de las clases predefinidas, Para ello deberá analizar un cierto número de características. Por ejemplo peso, dimensiones, etc.

Por otra parte, existen algoritmos de aprendizaje no supervisado, en los cuales no resulta necesario conocer a que clase pertenece cada uno de los patrones de la secuencia de entrenamiento.

El sistema de reconocimiento de patrones deberá tener en cuenta las fuentes de variabilidad, ya sea incluyendo en la secuencia de entrenamiento patrones que hayan experimentado estas modificaciones, o realizando un pre proceso que compense la variabilidad. Por ejemplo, normalizando el tamaño de los objetos para deshacer el efecto del cambio de escala.

Figura 4: esquema general de un sistema de reconocimiento de patrones

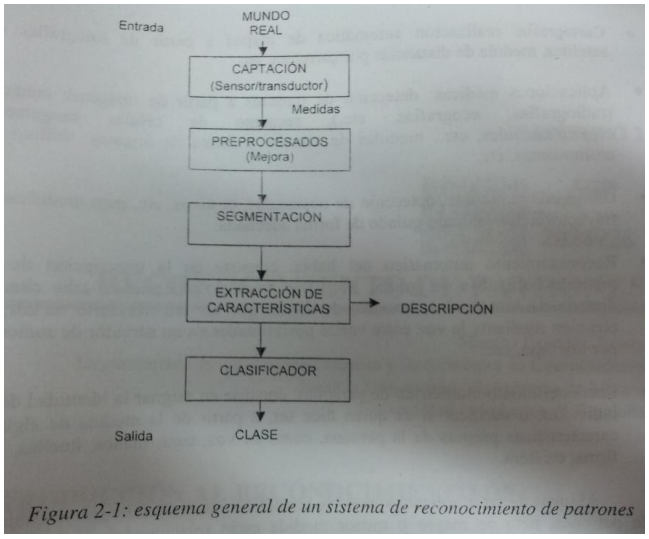


Figura 2-1: esquema general de un sistema de reconocimiento de patrones

Tomado marzo 28 de 2013 libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.2.4 Extracción de características: Uno de los aspectos más importantes a tener en cuenta en un reconocedor de patrones es el tipo de parametrizacion (o extracción de características) a realizar sobre la señal de entrada.

La parametrizacion proporciona innumerables ventajas, entre las que cabe destacar básicamente 2:

Una reducción del número de datos necesarios a procesar, tamaño de los modelos de los locutores, etc.

La transformación a un nuevo espacio de características en el cual más fácil discriminar entre locutores.

4.2.5 Selección secuencial hacia adelante: En la terminología inglesa se denomina Sequential Forward Selection. Consiste en evaluar cada una de las componentes por separado y elegir la que proporciona el mejor resultado.

Figura 5: Selección secuencial hacia adelante

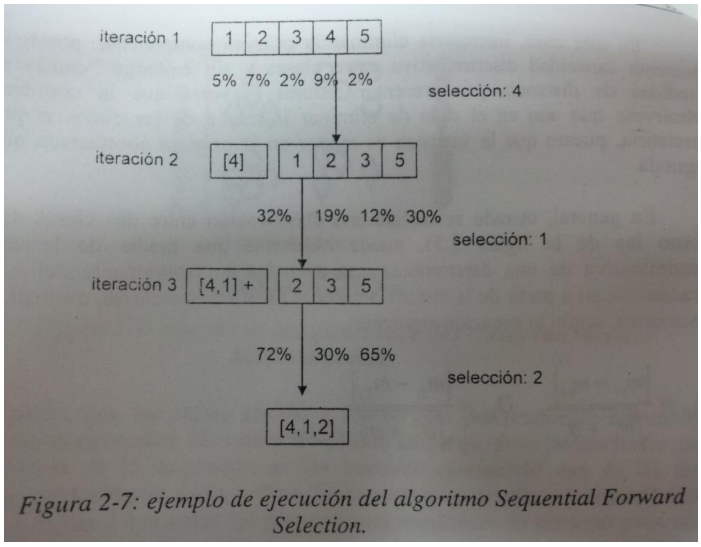


Figura 2-7: ejemplo de ejecución del algoritmo Sequential Forward Selection.

Tomado marzo 28 de 2013libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.2.6 Eliminación secuencial hacia atrás: En la terminología inglesa se denomina Sequential Backward Elimination. A diferencia del anterior se parte de todas las dimensiones y se va eliminado una en cada iteración, hasta llegar al número de componentes deseadas.

Figura 6: Eliminación secuencial hacia atrás

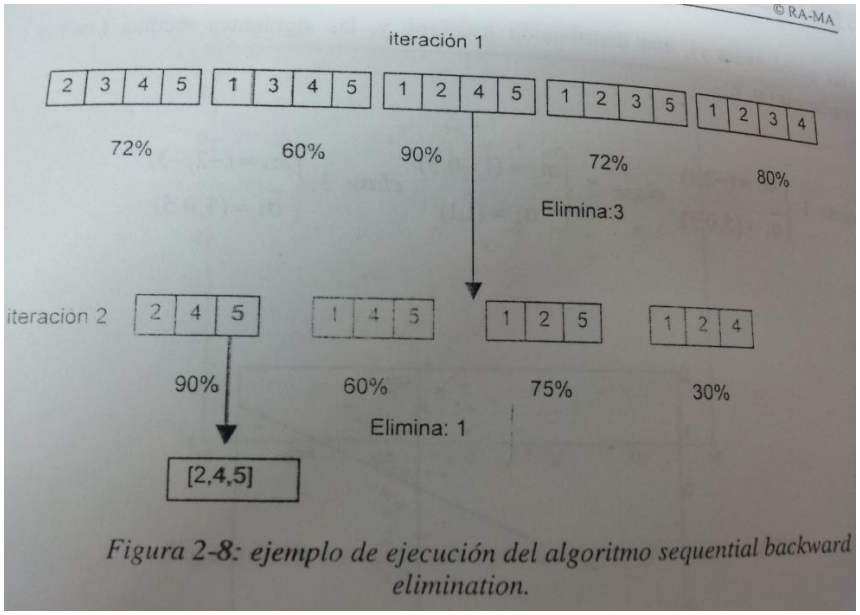


Figura 2-8: ejemplo de ejecución del algoritmo sequential backward elimination.

Tomado marzo 28 de 2013 libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.2.7 Análisis en componentes principales (PCA): Consiste en los siguientes pasos:

- Se calcula el número total de vectores
- Se calcula el vector media de todos los vectores
- Se calcula la matriz de covarianza
- Se diagonaliza la matriz de covarianza y se obtienen P autovectores
- Se ordenan los P auto vectores en función de su auto valor asociado (de mayor a menor). De esta forma el primero es el más importante, y depreciar los últimos suele suponer un error pequeño.
- Los auto vectores proporcionan los ejes de un nuevo sub espacio vectorial.

4.2.8 Detección de objetos por correlación: Mediante la correlación bidimensional de 2 imágenes, es posible detectar si una imagen está presente en

la otra y en qué posición. De esta forma, puede llevarse a cabo simultáneamente la segmentación del objeto dentro de la imagen y su reconocimiento.

4.2.9 Medida de distancia: Un aspecto clave a la hora de comparar modelos, es el criterio de semejanza o medida de distancia. Habitualmente, las señales de entrada no serán idénticas a las utilizadas en el proceso de modelado de cada una de las clases posibles. Por tanto, será necesario disponer de un criterio para decidir si 2 modelos son iguales o diferentes.

4.2.10 Métodos de clasificación: Clasificación basada en semejanza, clasificación basada en una medida probabilística y clasificación basada en crear fronteras de decisión.

- **Clasificación basada en semejanza:** Consiste en comparar el patrón a clasificar con los prototipos de cada una de las clases posibles obtenidos durante el proceso de entrenamiento.
- **Clasificación basada en medida probabilística:** La regla de decisión de Bayes óptima asigna un patrón de entrada a la clase con la máxima probabilidad a posteriori. Esta regla se puede modificar para asignar costes diferentes a distintos tipos de errores de forma que se mejore las prestaciones de uno de ellos a costa del otro.
- **Clasificación basada en crear fronteras de decisión:** Consiste en crear fronteras de decisión entre clases, a partir de la optimización de un determinado criterio de error. Algunos clasificadores que pertenecen a este método pueden aproximarse de forma asintótica al clasificador Bayesiano.

4.3 EVALUACION DE SISTEMAS BIOMETRICOS

Según la definición de la real Academia de la Lengua, evaluar es estimar aptitudes y rendimiento de los sistemas.

Tabla 1: Comparación de tecnologías

TÉCNICA	VENTAJAS	DESVENTAJAS
Reconocimiento de cara	Fácil, rápido y barato	La iluminación puede alterar la autenticación
Lectura de huella digital	Barato y muy seguro	Posibilidad de burla por medio de réplicas, cortes o lastimaduras pueden alterar la autenticación
Lectura de iris/retina	Muy seguro	Intrusivo (molesto para el usuario)
Lectura de la palma de la mano	Poca necesidad de memoria de almacenamiento de los patrones	Lento y no muy seguro
Reconocimiento de la firma	Barato	Puede ser alterado por el estado emocional de la persona
Reconocimiento de la voz	Barato, útil para accesos remotos	Lento, puede ser alterado por el estado emocional de la persona, fácilmente reproducible

Tomado de Internet marzo 30 www.biometricgroup.com

4.3.1 Planificando la evaluación:

- **Definiciones previas:**
  - **Muestra:** resultado de la captura por el sensor correspondiente de un determinado rasgo biométrico.
  - **Patrón:** medida de referencia almacenada del usuario, obtenida a partir de las muestras de entrenamiento proporcionadas por este. Dependiendo del sistema de clasificación usado, la referencia del usuario estará determinada directamente los vectores de características extraídos de las muestras de entrenamiento.

- **Inscripción:** proceso en el que se añade un nuevo usuario al sistema biométrico. Entre las operaciones a realizar se incluye la creación del patrón correspondiente.
- **Operación:** intento por parte de un usuario de validar o identificar su identidad, puede usar para ello una o más muestras, dependiendo de la política de decisión establecida en el sistema.

- **Clasificación de la muestra.**
- **Online:** cuando la inscripción o la clasificación se realiza en el momento en que es capturada la muestra.
- **Offline:** tanto la inscripción como las pruebas se realizan con muestras previamente grabadas.

4.3.2 Tipos de evaluación: Son tres tipos de evaluación:

- **Evaluación de la tecnología o tecnológica:** Es la más general, se realiza offline, por lo tanto es completamente repetible, y con ella se busca, fundamentalmente, medir el estado de la tecnología, determinar el progreso que ésta ha logrado e identificar los enfoques más prometedores. Las mas objetivas son las realizadas por laboratorios independientes, con bases de datos estándar y, preferiblemente, abiertas a cualquiera que desee participar.
- **Evaluación de escenario:** Se mide el rendimiento del sistema para un escenario prototipo que modela o simula un determinado campo de aplicación, con el objetivo de determinar si la tecnología está suficientemente madura como para cumplir los requisitos de funcionamiento para esa aplicación. A diferencia de la evaluación anterior, ésta no solo incluye los algoritmos de reconocimiento, sino que se extiende a todo el sistema, incluyendo la etapa de adquisición.
- **Evaluación operacional:** Es similar a la de escenario pero realizada para un sistema concreto, en un entorno de uso totalmente real y para una

población determinada. El objetivo es analizar si es sistema biométrico cumple los requisitos de una determinada aplicación.

4.3.3 Factores que afectan al rendimiento:

- Cuales son poco relevantes y, por tanto, su control no es trascendente
- Cuales pueden afectar a la medición del rendimiento, se procederá bien a fijar de antemano sus valores, o bien a diseñar las pruebas de tal manera que se pueda medir con la suficiente confianza su influencia en el sistema.
- Prever potenciales problemas que puedan surgir para anticipar los controles necesarios que minimicen su influencia
- Identificar casos excepcionales que puede ser interesante considerar en las pruebas.

Tabla 2: Factores ambientales relacionados con cada sistema.

	Iris	Caras	Huellas dactilares		Manos	Voz
			Sensor óptico	Sensor CMOS		
Luz ambiente	X	X	X		X	
Ruido ambiente						X
Temperatura			X	X	X	
Ruido eléctromagnético	X	X	X	X	X	X
Humedad ambiental			X	X		
Suciedad y contaminantes	X	X	X	X	X	
Variaciones de voltaje	X	X	X	X	X	X
Golpes y vibraciones	X	X	X	X	X	X

Tabla 3-1 Factores ambientales relacionados con cada tipo de sistema

Tomado marzo 28 de 2013libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.3.4 Los datos

- No es aconsejable el uso de muestras creadas artificialmente, tanto en lo que se refiere a la muestra en sí, como a las condiciones de adquisición; los resultados obtenidos no serán extrapolables a las condiciones reales de uso.
- Hay que tener cuidado con errores como dobles inscripciones, inconsistencias muestras-individuo, muestras incorrectas (dedo equivocado en huellas dactilares, imágenes en blanco).
- Una buena política es minimizar la intervención humana, pues puede añadir subjetividad (al decidir sobre la calidad de una muestra) y errores (el introducir una identificación incorrecta) en la adquisición. Cuanto más se automatice el proceso más objetivo, libres errores y cercanos a la situación real de uso serán los datos capturados.

4.3.5 Definiciones previas

- **Intento autentico:** la muestra a clasificar pertenece al propietario del patrón con el que se compara.
- **Intento impostor:** la muestra a clasificar no pertenece al propietario del patrón con el que se compara.
- **Cliente:** usuario inscrito en el sistema.
- **Impostor:** usuario que se hace pasar por un cliente sin serlo. Diremos que es activo si trata de parecerse o de imitar al cliente y pasivo en caso contrario.

4.3.6 Datos del cliente: Un problema a tener en cuenta a la hora de adquirir los datos del cliente es el del “envejecimiento del patrón”, esto es, cuanto mayor es el tiempo transcurrido entre la inscripción y la operación menor es el rendimiento del sistema.

4.3.7 Datos de impostores: Impostores genuinos: cuando para operaciones de impostores se usan muestras provenientes de usuarios totalmente diferentes a los clientes, y adquiridas ex profeso para este fin.

Impostores simulados: cuando se usan muestras de otros clientes.

4.3.8 Impostores genuinos: Adquirir datos de impostores completamente diferentes a los de los clientes es la forma más realista de evaluar el sistema, debido a la naturaleza no uniforme en el comportamiento de los distintos usuarios, es recomendable que el número de impostores sea suficientemente grande para poder elegir aleatoriamente para cada cliente un subconjunto de impostores distinto, con reemplazo.

4.3.9 Impostores simulados: Como antes, elegir de manera aleatoria un subconjunto diferente para cada cliente, se puede usar para ello solo las muestras de entrenamiento o incluir también las de prueba.

Realizar una comparación cruzada completa, donde cada muestra adquirida de cada cliente es comparada con todos los patrones ajenos, comparaciones para N clientes y 1 muestra por cliente.

4.3.10 Tamaño del conjunto de prueba: El tamaño del conjunto de prueba, definido por el número de voluntarios e intentos de cada uno, fija la precisión o la confianza de la estimación del error medio. Por lo tanto, un problema importante a resolver es encontrar el tamaño mínimo que asegure un determinado nivel prefijado de confianza sobre las medidas del rendimiento que se realicen con ese conjunto de prueba.

4.3.11 Medición del rendimiento del sistema: Las primeras etapas son las encargadas de adquirir, digitalizar y extraer los vectores de características del parámetro biométrico, y pueden, durante cualquiera de estos primeros pasos, aplicar un control de calidad de la adquisición realizada; la decisión a tomar si la muestra no tiene la calidad suficiente depende de la política establecida.

4.3.12 Validación de la muestra: Tasa de fallos en Inscripción (TFI). Es estimada como la proporción de voluntarios que han sido inscritos en el sistema de acuerdo con la política de inscripción establecida.

Tasa de fallos en Operación (TFO). Se estima mediante la proporción de operaciones (tanto del cliente, como de impostores) que no han podido ser completadas.

4.3.13 Errores en la etapa de clasificación: Tasa de falsos positivos (TFP). Es la probabilidad esperada de que una muestra de un usuario sea incorrectamente clasificada como coincidente con el patrón de otro usuario.

Tasa de falsos negativos (TFN). Es la probabilidad esperada de que una muestra de un usuario sea incorrectamente clasificada como no coincidente con el patrón de ese usuario.

Figura 7: Errores en la etapa de clasificación

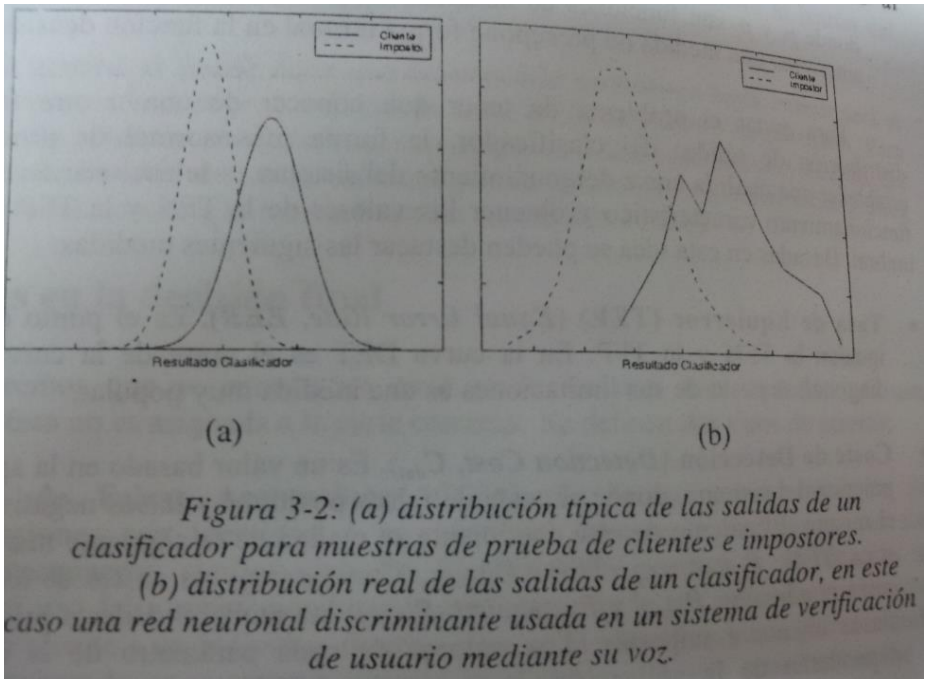


Figura 3-2: (a) distribución típica de las salidas de un clasificador para muestras de prueba de clientes e impostores. (b) distribución real de las salidas de un clasificador, en este caso una red neuronal discriminante usada en un sistema de verificación de usuario mediante su voz.

Tomado marzo 30 de 2013 libro, “Automatic Signature Verification and Wiriter Identification- the State of the Art”.

4.3.14 Errores en la decisión final: Tasa de falsas Aceptaciones (TFA). Es la proporción esperada de operaciones con identidad o no identidad falsamente reclamada que son incorrectamente confirmadas.

Tasa de falsos Rechazos (TFR). Es la proporción esperada de operaciones con identidad o no identidad correctamente reclamada que son incorrectamente rechazadas.

4.4 HUELLA DACTILAR

La identificación de personas a través del estudio analítico de las huellas dactilares denominada técnica de dactiloscopia, responde al método de identificación biométrico por excelencia, ya que aparte de ser un método aceptado popularmente y de fácil adquisición también cumple con las dos leyes básicas de regulación, las cuales son la invariabilidad temporal y la variedad infinita del autentificador.

4.4.1 Antecedentes históricos de la dactiloscopia: Desde los primeros siglos, los estudios realizados al cuerpo humano, arrojaron como resultado un sin número de dibujos y formas en las yemas de los dedos.

Transcurría el año 1665 cuando el italiano Marcelo Malpighi anatómico de profesión inicio los estudios sobre las crestas capilares, esto apoyado en el microscopio instrumento novedoso para la época. Pero solo fue hasta 1823 cuando el checo Johannes Purkinje tuvo la idea de utilizar la huella dactilar como posible autentificador biométrico.

El, en su tesis revelo que los dibujos papilares se manifiestan a partir del sexto mes de gestación y permanecen inalterables a lo largo de toda la vida, certificando de este modo la perennidad o invariabilidad de las mismas

Este es el punto de partida para la realización de otros estudios encaminados a demostrar las infinitas realizaciones de los dibujos papilares que posibilitara el uso de los mismos como eficientes autentificadores biométricos.

En 1886 el hoy llamado padre de la dactiloscopia Francis Galton se inquietó por los dibujos de las huellas y realizo un estudio de rigor acerca de estas, dando como resultado la demostración analítica de la no existencia de dos huellas digitales iguales y confirmo así otro requisito para que la huella fuese el autentificador por excelencia la exclusividad.

En 1890 el inspector de la policía de Bengala Edward Henry introdujo una clasificación sistemática la cual ordenaba la las muestras de las huellas de un modo lógico, por medio de este orden estableció las bases de la dactiloscopia moderna.

4.4.2 Caracterización y clasificación de las huellas dactilares: La huella dactilar obedece a un autentificador biométrica de tipo morfológico que presenta como característica principal la presencia de un conjunto de líneas genéricas denominadas crestas que corresponden a las partes donde la piel se eleva sobre zonas más bajas denominadas valles.

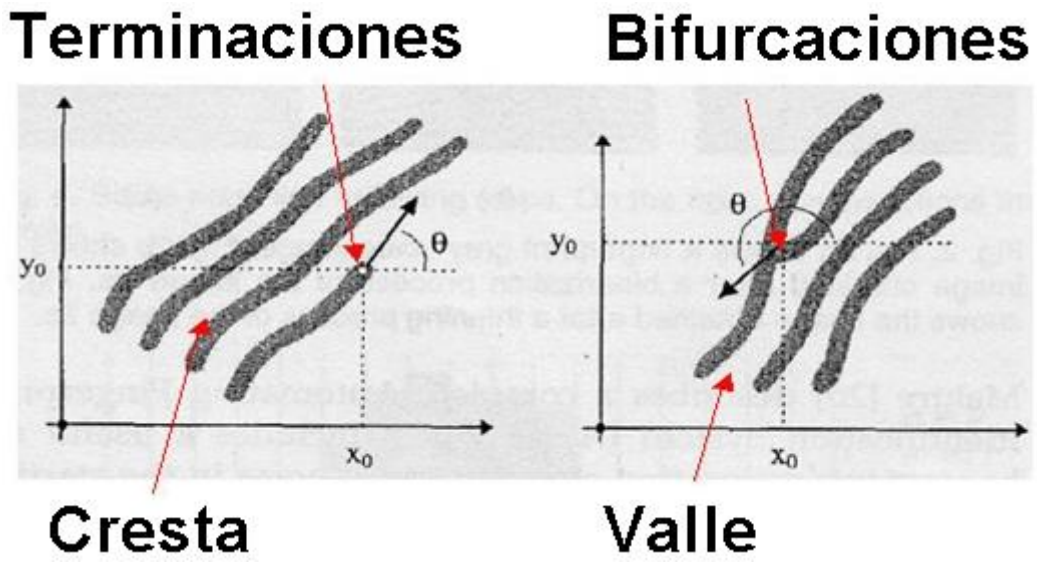
De esta forma un porcentaje de la población presenta dificultades para posibilitar una correcta adquisición y posterior identificación partiendo de sus huellas dactilares.

- **Colectivos étnicos:** los dedos de los asiáticos tienen las yemas muy pequeñas y este problema también se detecta en adultos de avanzada edad.
- **Colectivos profesionales:** gente que trabaja con sus manos (albañiles, carpinteros, agricultores) pueden presentar callosidades que dificultan la adquisición, así como profesionales que trabajan con químicos.

Existen dos características particulares de las crestas:

- **Final de cresta:** característica definida como el punto en el que la cresta se acaba de forma abrupta.
- **Bifurcación de la cresta:** Característica definida como el punto donde la cresta se bifurca en dos o más crestas.

Figura 8: terminaciones y bifurcaciones de la huella dactilar.



Tomada marzo 29 de 2013. Pds2006galeon.com

Figura 9: cresta y valle de la huella dactilar

Tomada marzo 29 de 2013. Pds2006galeon.com

4.4.3 Reconocimiento de huella dactilar: La comparación de la huella digital es una de las técnicas más antiguas y ampliamente utilizadas y aceptas a nivel global.

Los sistemas actuales de comparación de la huella digital tienen su base en los desarrollos realizados por Galton y Purkinje.

La huella digital aparece generalmente constituida por una serie de líneas oscuras que representan las crestas y una serie de espacios blancos que representan los valles. La identificación con huellas digitales esta basada principalmente en las minucias (la ubicación y dirección de las terminaciones de crestas, bifurcaciones, deltas, valles y crestas, aunque existen muchas otras características de huellas digitales.

Figura 10: características de huellas digitales

Tomado marzo 29 de 2013.Pds2006galeon.com

En las huellas dactilares se identifican dos partes principalmente .Las cuales son:

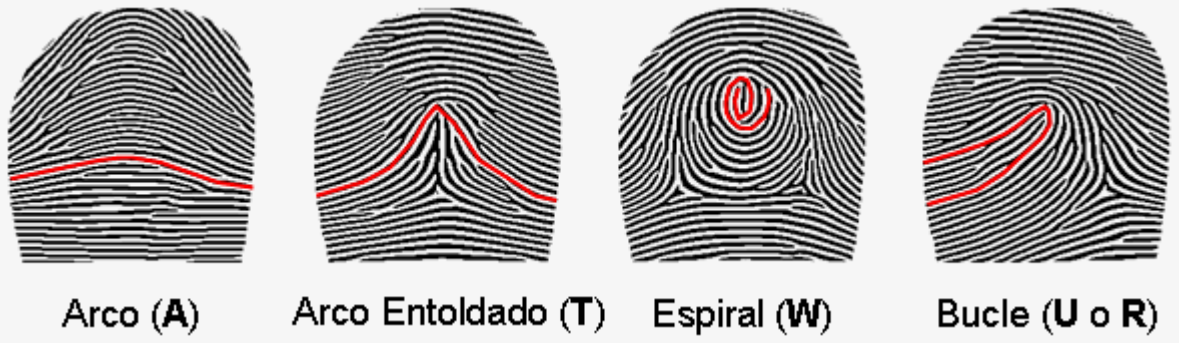
El core: que es el punto localizado en la zona nuclear de la huella donde una de las crestas cambia bruscamente su dirección y describe un ángulo de 180°. Este punto se utiliza como referencia para contar el número de crestas a considerar en un análisis dactiloscópico.

El delta: Punto característico del dibujo papilar de algunas huellas que pueden presentar forma de triángulo está formado por la aproximación de las crestas existentes en la zona frontera entre las zonas marginal, basilar y nuclear. Su importancia radica en que en estas zonas aparecen muchos puntos característicos.

4.4.4 Clasificación: Todos los dactilogramas coinciden en el hecho de que las crestas papilares no describen formas aleatorias, sino que se agrupan hasta llegar a constituir sistemas definidas por la uniformidad de su orientación y figura.

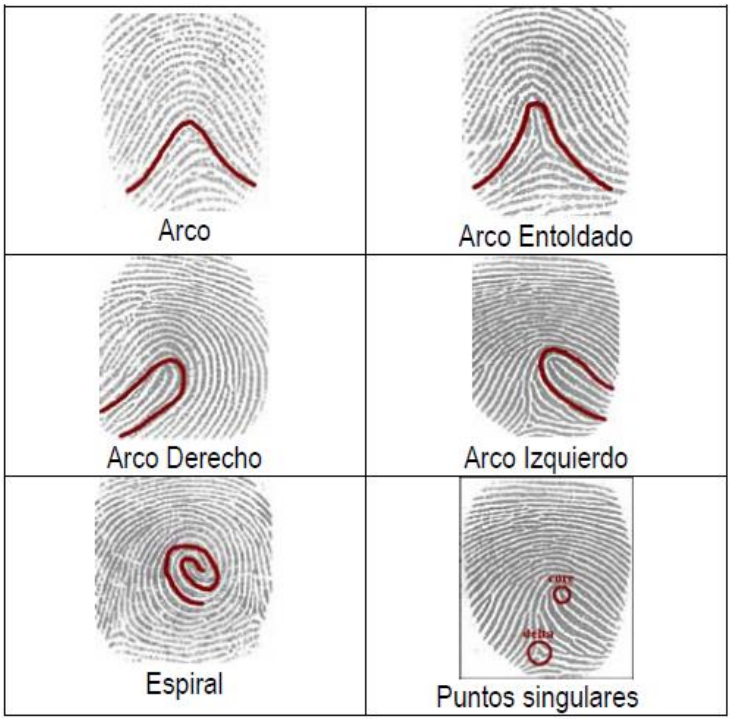
Según la clasificación Henry se pueden distinguir seis clases que son:

Figura 11: los cuatro patrones principales de la huella



Tomado marzo 30 http://nuestroblogsomosblogueros.blogspot.com

Figura 12: Seis patrones de las huellas



Tomado marzo 30 de 2013 www.mentesinquietas.net

4.4.5 Etapa de clasificación: Responden a un método de ayuda al reconocimiento, que utiliza la clasificación en una de las clases nombradas. Tiene utilidad en casos que demanden tiempo y dinero en su clasificación; por tener base de datos de considerables tamaños como los del FBI.

4.4.6 Algorítmica: Los algoritmos filtran la parte central de la huella a través de un banco de filtros de Gabor, dando como resultado la disminución de las crestas presentes en la huella, en función de su dirección (0°,45°,90°,135°).

4.4.7 Dispositivos de adquisición: En el mercado actual a pesar de la variedad de dispositivos de captura de la huella, la gran mayoría obedecen a escáner tipo inkless, estos elementos no requieren calcar los dibujos papilares por medio de tinta. Y según su forma y utilización se clasifican así:

- **Lectores OEM:** es una solución directa que se integra con facilidad a cualquier sistema electrónico.
- **Lectores integrados:** dispositivos periféricos que capturan la huella, con conexión fácil a ordenadores por medio de puertos USB y la información es almacenada en el disco duro, algunos tienen lector de tarjetas inteligentes (Smart card)
- **Terminales completos de identificación:** incorporan todo el Hardware y Software necesario para la captura y verificación de huellas dactilares.
- **PCMCIA**

La segunda clasificación estándar de estos tipos de escáneres se da según el tipo de sensor

- **Tecnología óptica:** utiliza un sensor tipo CCD(dispositivo de acoplamiento de carga) como elemento responsable de la captación de la imagen, después de recorrer el juego de lentes, este dispositivo electrónico tiene una matriz de foto sensores que se encargan de convertir la radiación luminosa en una tensión proporcional a la misma.

  La resolución o calidad del sensor la da los pixeles, otro sensor óptico es el CMOS que no tiene elementos ópticos reduciendo prestaciones a nivel de sensibilidad. Su principal ventaja es la elevada resolución de la imagen digital obtenida y la principal desventaja es la sensibilidad a la suciedad.

Figura 13: Tecnología óptica:

Tomado marzo 30 de 2013http://www.scssa.com.ar

- **Tecnología capacitiva:** utiliza un sensor de tipo electromagnético; el sistema detecta la diferencia de capacidades entre la huella y el sensor, las características eléctricas mas importantes de la piel humana son la impedancia y la capacitancia y el modelo equivalente es una matriz de resistores y capacitores en paralelo.

  La principal ventaja es el bajo consumo y el reducido tamaño del dispositivo sensor y su principal desventaja es la elevada sensibilidad a variaciones de los parámetros de humedad de la huella y de campo eléctrico.

Figura 14: Tecnología capacitiva

Tomado marzo 30 de 2013 http://www.google.com.co

- **Tecnología ultrasónica:** en este caso el sistema envía un barrido de ondas ultrasónicas que rebotan sobre la base de la huella, esta tecnología de ultima generación se basa en la diferencia de impedancia acústica existente entre la cresta y el valle de la huella

  La principal desventaja es el mercado, el alto costo del dispositivo sensor y la sensibilidad en la obtención de la huella.

  Esta tecnología requiere un Software de soporte para ayudar a la adquisición de la huella, este permite el control de acceso al ordenador mediante la verificación, la encriptación de datos y el bloqueo de salvapantallas.

Figura 15: Tecnología ultrasónica:

Tomado marzo 30 de 2013 http://spanish.alibaba.com

4.4.8 Reconocimiento de huellas dactilares digitales: Las técnicas de reconocimiento de huellas se dividen en dos categorías:

- **Técnicas locales o analíticas:** estas son basadas en las minucias de las huellas y su principal desventaja es la dificultad de extracción de las minucias en imágenes de baja calidad.

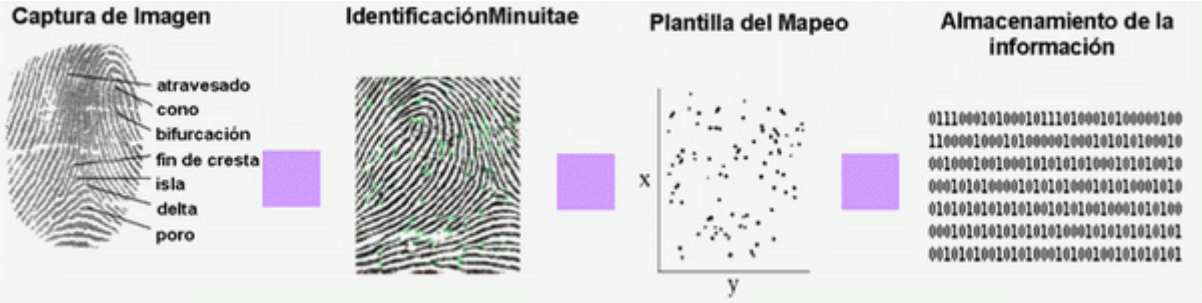
- **Técnicas globales u holísticas:** este sistema se trabaja por medio de algoritmos de alineación, por tal motivo es sensible a las translaciones y rotaciones de la huella durante el proceso de captura.

  El proceso básico para la identificación y verificación de personas a partir de la huella dactilar es:

- **Captura de la huella:** depende del dispositivo de captura y permite almacenar la huella para su análisis.
- **Creación del modelo:** se extraen las minucias o puntos característicos de la huella presentes en la imagen obtenida y se almacena en un fichero llamado patrón o modelo.
- **Comparación del modelo:** si es para verificación de la huella se compara la plantilla de referencia con la huella candidata una vez extraída las minucias de la misma. Y si es para identificación se compara la huella candidata parametrizada, con el total de las plantillas presentes.
- **Verificación/ identificación:** la verificación se lleva a cabo a partir del número obtenido en el proceso anterior (0,1) este número se compara con el umbral de seguridad establecido por el sistema. El proceso de identificación entrega el resultado, a la persona que presente una plantilla con mayor nivel de similitud con respecto a la entrada biométrica parametrizada.

De manera general la forma de procesar una huella digital es la siguiente:

Figura 16: reconocimiento de huella dactilar



Tomada de inetrnet marzo 29 de 2013. http://nuestroblogsomosblogueros.blogspot.com

4.4.9 Adquisición digital de la huella: Existen dos métodos de adquisición de la huella:

- El método off-line: donde se obtiene la huella digitalizada mediante el positivo impreso en papel obtenido con anterioridad, a partir de la operación de calcado del dedo tintado, esta aplicación es muy utilizada en criminalística.

- El método on-line: se realiza en tiempo real mediante el escaneo directo de la huella a través de escáneres de tipo inkless, esta metodología es muy utilizada en aplicaciones civiles

4.4.10 Preprocesado de la huella: El principal problema es discriminar de forma óptica si los pixeles evaluados, pertenecen a una cresta o no, esto se da por los defectos a la hora de la captura como los son las diferencias de brillos o el contraste de la imagen.

4.4.11 Extracción de las regiones de interés: Este proceso tiene como finalidad desestimar la información redundante relativa al fondo de la huella (blanco perfecto) de seta forma se obtiene una importante reducción del fichero final.

4.4.12 Binarizacion: El objetivo de esta etapa es decrementar el margen dinámico de niveles de gris entre las crestas y los valles de la imagen para facilitar el proceso de las etapas siguientes.

4.4.13 Adelgazamiento: Esta etapa realiza una reducción del grosor de las líneas mediante distintas técnicas hasta que todas presenten un grosor igual a 1 pixel, facilitando de esta manera el proceso de reconocimiento.

Una de las técnicas más utilizada es la llamada (MM), morfología matemática, esta es una técnica no lineal de la imagen basada en estructuras geométricas.

4.4.14 Depuración: En esta etapa se aplican los algoritmos de poda para poder eliminar las ramas parasitas residuales perpendiculares a las crestas de la huella, que han surgido durante el adelgazamiento, así como la unión de líneas rotas mediante el proceso de suavizado.

4.5 IRIS Y RETINA

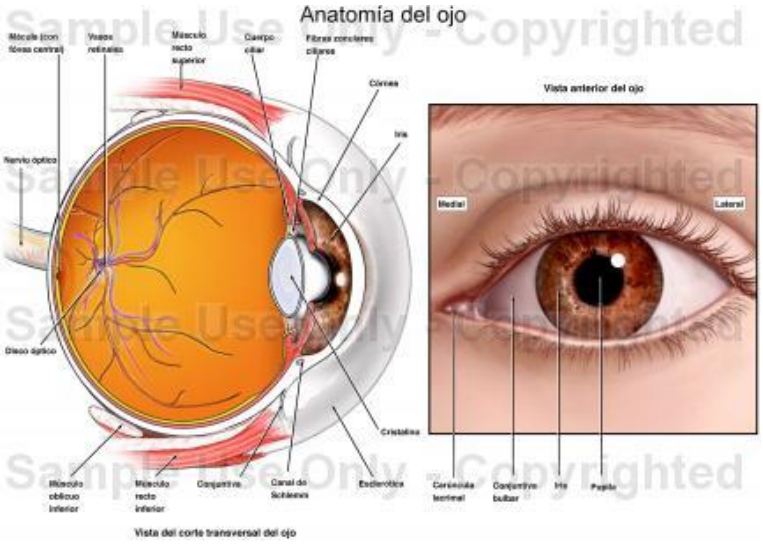
La utilización del ojo humano en la identificación de personas a arrojado dos técnicas biométricas, una basada en el iris y la otra basada en la retina, en la literatura anglosajona estas dos técnicas son confundidas y se cree que son una

sola, pero la verdad son diferentes desde el mismo momento de la captura de la imagen y las técnicas para la extracción de las características y comparación.

4.5.1 Anatomía del ojo: El ojo humano es el órgano encargado del sentido de la visión, el cuerpo humano esta dotado de dos ojos lo cual le garantiza una visión estereoscópica. Su formación se remonta al día 25 de gestación y finaliza en el octava semana cuando finaliza la génesis del esbozo ocular, que seguirá madurando hasta el noveno mes.

De una forma muy simple el ojo se puede considerar como una cavidad esférica recubierta de tres capas externa, media e interna.

Figura 17: Anatomía del ojo



Tomado marzo 30 de 2013http://legalpresentationgraphics.medicalillustration.com

4.5.2 Iris: Es uno de los componentes de la capa media y consta de un estroma con células pigmentadas y de un epitelio, el cual contiene los músculos esfínter y dilatador del iris; que actúan como diafragma. El iris forma la capa protectora entre la cámara anterior y posterior del glóbulo ocular, por eso se encuentra situado entre la cornea y el cristalino y presenta una abertura en su parte central llamada pupila.

4.5.3 Retina: Es la capa interna del glóbulo ocular, es l capa sensorial del ojo cuya función es transformar la luz en un impulso nervioso que será dirigido al cerebro, esta compuesta por diez capas, pero histológicamente puede dividirse en tres

tramos; la ora serrata que es la terminación anterior a la retina sensorial, la retina periférica con un predominio de bastones y la retina central situada en el polo posterior y en el centro se halla la macula.

4.5.4 Reconocimiento del iris ocular: El precursor tecnológico de esta técnica es John Daugman; la idea de utilizar el iris para identificar a las personas fue propuesto en 1936 Frank Burch, pero solo hasta 1987 influenciados por las películas de ciencia ficción, los oftalmólogos Leonard Flom Aran Safir, estos contactaron a Daugman para que desarrollara los algoritmos para poder realizar el reconocimiento biométrico a través del patrón del iris.

4.5.5 Captura de la imagen del iris: Para la captura se plantean dos posibilidades, el uso de cámara digital o el uso de cámara de video. También se puede plantear la posibilidad de en el rango infrarrojo, la cual no requiere una luz alta que moleste al usuario.

También se debe tener en cuenta que la cámara debe tener una resolución muy alta, que la imagen solo muestre el ojo de la persona, la imagen captura no debe tener deformaciones ocasionadas por las distancias, ni el ojo debe estar muy cerca de la cámara.

4.5.6 Preprocesado del iris: Esta etapa tiene una gran importancia ya la labor de adaptar la señal a los requisitos del bloque de extracción de características conlleva:

La localización del iris dentro de la imagen, la detección de los bordes del iris, eliminación de la imágenes no deseadas, compensación del tamaño del iris y y la adaptación de la imagen a la técnica de extracción.

4.5.7 Adaptación del iris detectado: Una vez aislado el iris de toda la imagen, se consideran las variaciones debidas al tamaño y a la dilatación de la pupila.

Se debe tener en cuenta que el tamaño de los datos sea el mismo sin importar el tamaño del iris y de la pupila y que estén suprimidos los conos superior e inferior.

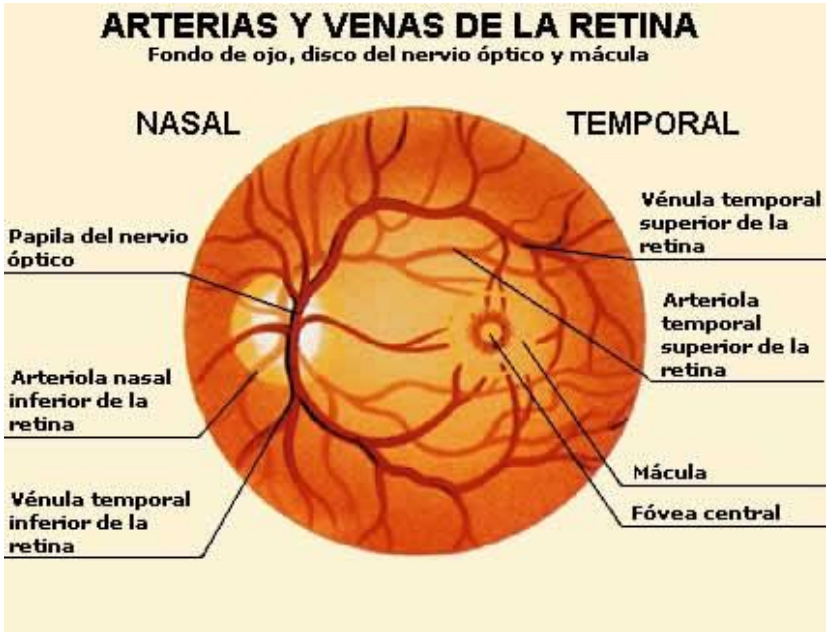
4.5.8 Base de datos: La no disponibilidad de una base de datos de iris para identificación de dominio público, forzó a realizar todo el trabajo de investigación sobre la captura de la imagen.

4.5.9 Identificación por escaneo de la retina: Se basa en la utilización del patrón de los vasos sanguíneos contenidos en la retina, que se obtienen a partir de l a imagen del fondo del ojo.

La distribución de los vasos sanguíneos que emanan del nervio óptico y aparecen dispersos en la retina es indudablemente una fuente de información biométrica y altamente distintiva.

Es una de las técnicas biométricas mas precisas, utiliza un rasgo fisiológico estable (la retina) y muy difícil de falsificar, la desventaja es que por medio de la retina se obtiene información innecesaria y de dificultad para usarse.

Figura 18: geografía del ojo



Tomado marzo 30 de 2013. http://usuarios.discapnet.es/

4.5.10 Soluciones comerciales: La tecnología de reconocimiento por iris de Iridian Technologies, basada en los algoritmos de Daugman es la base de la nueva iniciativa de seguridad de aeropuertos.

En el año 2002 se comercializo un dispositivo con soporte de software, el cual también controla el acceso.

4.6 GEOMETRIA DE LA MANO

El uso de la geometría de varias partes del cuerpo para la identificación de personas, según algunos estudios se remonta a los tiempos de los egipcios. Este proceso ha sido abandonado por tal razón este sistema no ha avanzado mucho en esta técnica biométrica, aunque diversos expertos sostiene la fiabilidad de la mano para identificar a una persona.

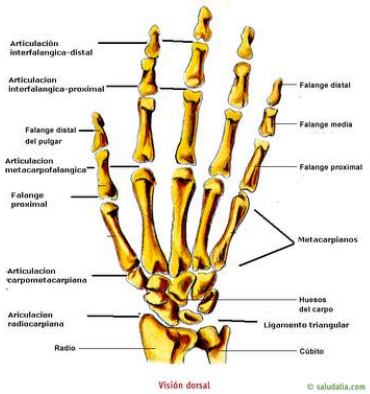
4.6.1 Estructura de la mano: La mano es un órgano del cuerpo humano, unido a la extremidad del brazo y esta comprendida desde la muñeca y hasta la punta de los dedos, es la que permite la mayor matización de la fina actividad mecánica del hombre.

Consta en esencia de un esqueleto óseo, provisto de veintisiete huesos articulados entre sí en los que se inserta un crecido número de tendones.

En la mano existen fundamentalmente tres grupos de huesos, los del carpo, metacarpo y dedos. El carpo es la parte mas próxima de la mano, cerca de la muñeca y consta de ocho huesos dispuestos en dos filas, cuatro en cada uno.

El segundo grupo esta formado por los cinco metacarpianos y forman la parte mas distante del esqueleto de la palma. El tercer grupo esta conformado por los huesos de los dedos, las falanges pequeñas y cortas.

Figura 19: Parte ósea de la mano

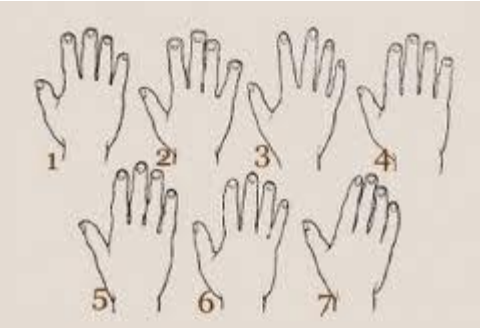


Tomado marzo 30 de 2013. www.google.com

Los músculos representados a menudo solo por la terminación tendinosa de una masa muscular del antebrazo, se divide fundamentalmente en dos grupos; los flexores que son los de cara palmar y los extensores que son los de la dorsal.

4.6.2 Clasificación de las manos: Se divide en 7 tipos

Figura 20: Clasificación de las manos



Tomado marzo 30 de 2013. http://tarot.lapipadelindio.com

- Manos de gran palma: también se le llama mano elemental, sus características esenciales son el grosor y el tamaño reducido de los dedos, su pulgar es corto, bastante ancho y muestra tendencia a curvarse hacia atrás.
- Mano espatulada: sus dedos suelen ser planos y las articulaciones poco o nada apreciables. Es considerado como el polo opuesto a la mano elemental.
- Mano cónica: también llamada mano artística, suele parecer larga, también huesuda.
- Mano cuadrada: es la que se toma como mano normal, sus proporciones son medias.
- Mano nudosa: se le llama también mano filosófica, su pulgar es ancho, las articulaciones de los dedos son notorias, nudosas y la palma es amplia.
- Mano puntiaguda: los dedos crecen de protuberancias en las articulaciones y cada uno parece dotado de una particular función, la palma es de dimensiones medias.

- Mano mixta: es la mano que normalmente se encuentra ya que se trata de una mezcla de varios de los otros seis tipos de manos.

4.6.3 Antecedentes históricos: Los orígenes de estos dispositivos data de los años 60 y 70, los cuales eran dispositivos netamente mecánica, pero solo hasta los años 80 se fabricaron de manera electrónica.

El creador de estos elementos fue David Sidlauskas, sin embargo la divulgación de estos trabajos se han mantenido en el anonimato ya que han sido poco comerciales y de poca divulgación.

4.6.4 Método de captura: Se hace por medio de la fotografía digital baja resolución, las fotos son tomadas desde la parte superior de la mano la cual esta ubicada sobre una plataforma diseñada al efecto.

Las fotos sacadas son almacenadas en archivos en formato JPEG, la foto extraída pasaría directamente a la etapa de preprocesado, sin almacenamiento intermedio. La cámara se encuentra situada a 42 cm de la palma de la mano y en la imagen también es capturado el dorso de la mano.

Por ultimo es importante la posición de la persona en relación con el sistema porque si la plataforma es demasiado baja, el usuario tendera a no posar completamente la mano. La altura recomendada para un sistema a ser usado por adultos es de 1.40 m.

Figura 21: Escáner de reconocimiento de la mano

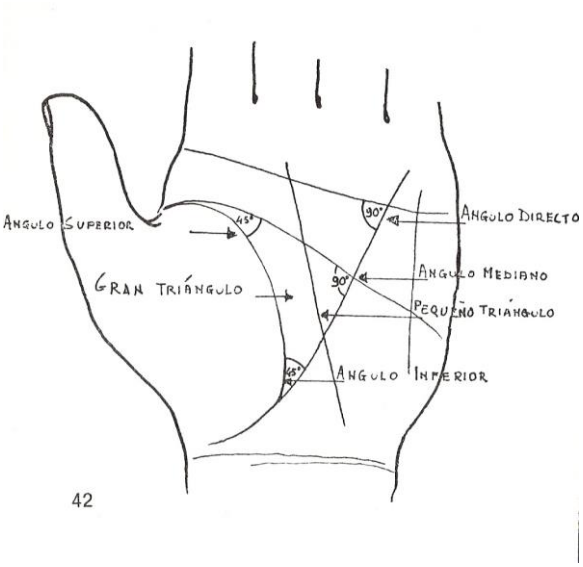
Tomado marzo 30 de 2013. http://blogyusos.blogspot.com

4.6.5 Preprocesado: Una vez capturada la foto de la mano, que contiene el dorso y la vista lateral, se inicia el preprocesado, en este se extraen los bordes de la imagen para su posterior entrada a la etapa de extracción de características, esta etapa se inicia traduciendo una imagen a color a blanco y negro con alto contraste entre la mano y el fondo.

4.6.6 Extracción de características: Una vez obtenidos los contornos del dorso de la mano y su perfil, se realizan una serie de medidas que darán como resultado el vector de características correspondientes. Las principales medidas son:

- Anchuras: de cada uno de los dedos, salvo el pulgar, en posiciones fijas evitando los puntos de los topes, debido a la presión ejercida por los dedos en estos puntos.
- Alturas: del dedo del corazón, del dedo meñique y de la palma de la mano.
- Desviaciones: de los dedos con respecto a la línea recta que debería formar las falanges.se mide como entre el punto medio entre del contorno del dedo y el punto medio de la recta
- Ángulos: entre la línea de unión de los puntos inter-dedo y la horizontal

Figura 22: Características de la mano



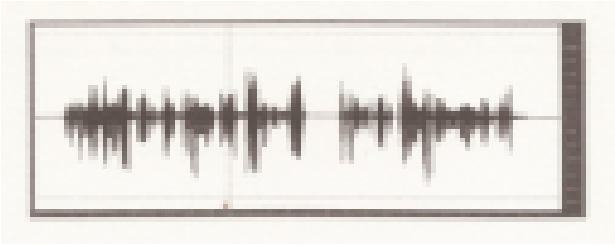
Tomado marzo 30 de 2013. http://www.metirta.com

4.7 RECONOCIMIENTO DE LOCUTOR

4.7.1 La señal de voz: Uno de los principales objetivos de este sistema es individualizar cada persona partiendo de las características particulares que tenemos cada uno de nosotros en nuestra voz. Hablando de las características de la voz en ella incluiríamos la acústica de las cavidades, la propagación de las ondas acústicas y la anatomía humana.

4.7.2 Características de la señal de voz: Una señal de voz se considera no estacionaria ya que con respecto al tiempo puede variar muchas veces. En la figura 23 podemos ver la onda que genera una voz por un lapso de 5 segundos.

Figura 23: Fragmento de voz de 5 segundos: amplitud respecto al tiempo



Tomado marzo 28 del libro Digital Image Processing, prentice-Hall, 2002.

Como podemos ver en la figura 23 no podemos sacar un patrón para individualizar a una persona, entonces para poder individualizar tenemos que enfocarnos no en segundos sino en cientos de milisegundos.

En la figura 24 de 80 milisegundos podemos observar que la señal se comporta como cuasi-estacionaria.

Figura 24: tramo de voz de 80 ms. Sonido sonoro (izquierda) y sordo (derecha).

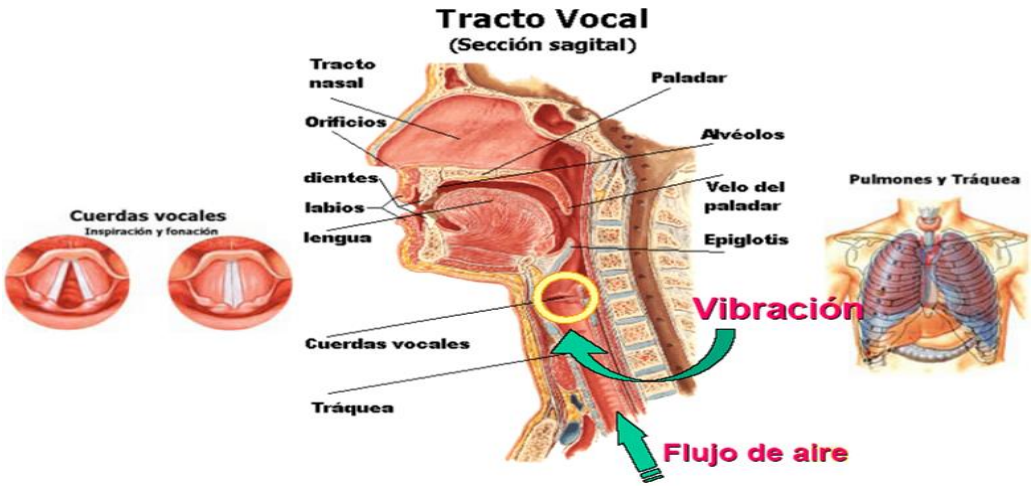
Tomado marzo 28 de 2013. (Extraído del libro de tecnologías biométricas aplicadas a la seguridad por Marino Tapiador y Juan Sigüenza)

En la figura 24 podemos observar una apariencia pseudo-periódica para el sonido sonoro pero también vemos que se pueden presentar sonidos con apariencia ruidosa. Este estudio nos clasifica de forma genérica los sonidos hablados en función de su naturaleza como:

- Sonoros, sonidos de carácter periódico.
- Sordos, sonidos de carácter ruidoso.

4.7.3 Naturaleza de la señal de la voz: Esta señal es producida por el aire que viene de los pulmones y atraviesa el tracto vocal, el cual está compuesto por: la tráquea, las cuerdas vocales, el velo del paladar, el tracto nasal, el tracto oral.

Figura 25: Partes del tracto vocal



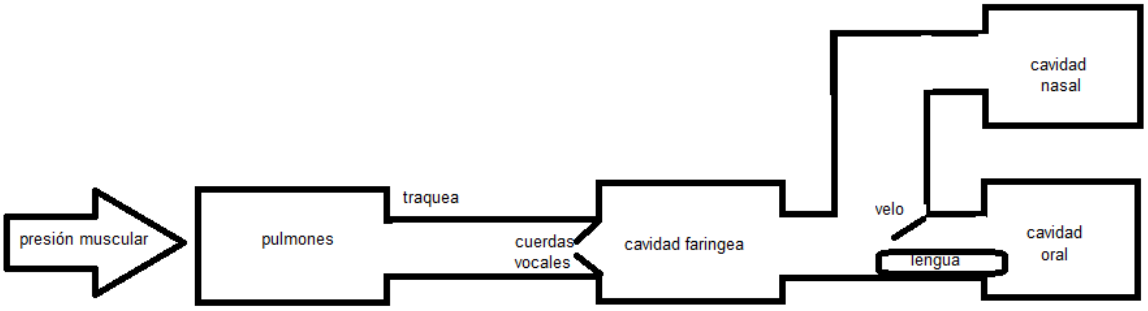
Tomado marzo 28 de 2013 (extraído de lectorbiometricodevoz.wordpress.com)

En la figura 25 vemos un flujo ascendente de aire que atraviesa la laringe pasando por las cuerdas vocales produciendo una onda acústica llamada voz, las cuales tienen unas características que dependerán de la velocidad de vibración de las cuerdas vocales, de la humedad entre otras características.

Las cuerdas vocales son las que producen ya sea los sonidos sordos o sonoros y dependen si las cuerdas están en relajación o en tensión porque si se encuentran

en tensión producirán un sonido sonoro, pero si se encuentran en relajación producirán un sonido sordo.

Figura 26: Modelo acústico de tracto vocal.



Tomado marzo 28 de 2013. Extraído del libro de tecnologías biométricas aplicadas a la seguridad por Marino Tapiador y Juan Sigüenza.

4.7.4 Niveles de información en la identidad del locutor: De acuerdo a nuestras características de la voz, nuestro sistema puede arrojar cierta información acerca de nosotros la cual se puede clasificar en:

Información de bajo nivel: aquí encontramos características como articulación de los sonidos, evolución del tono fundamental, transiciones peculiares entre sonidos, ritmo y velocidad de habla.

Información de alto nivel: aquí están asociadas las peculiaridades de tipo lingüístico, como la elección característica de palabras y estilos, hábitos sintácticos, léxicos, frases, dialecto, expresiones, jerga, velocidad de habla, cultural determinado o grupo social.

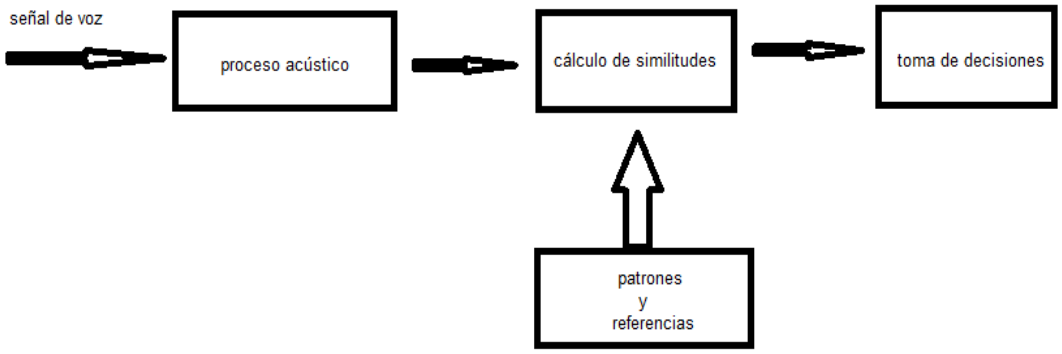
4.7.5 Sistemas de reconocimiento automático de locutores y principio de funcionamiento: Deben ser capaces de trabajar en tres formas distintas.

- Modo de entrenamiento: aquí se encuentran los patrones de referencia de cada usuario del sistema.

- Modo de funcionamiento o servicio: esta es la parte donde se pone en marcha el sistema y de acuerdo a unas señales de voz se toman decisiones a cerca de la identificación del hablante.

- Modo de actualización: se podrán incorporar o sacar nuevos locutores y actualizar o mejorar modelos.

Figura 27: Diagrama de bloques de un sistema de reconocimiento automático de locutores.



Tomado marzo 28 de 2013. Extraído del libro de tecnologías biométricas aplicadas a la seguridad por Marino Tapiador y Juan Sigüenza.

De acuerdo a la información recolectada por este sistema, él procederá a tomar las decisiones pertinentes en cuanto a la identificación del locutor.

4.7.6 Algoritmos de identificación automática del hablante

- **Alineamiento temporal dinámico (DTW):** Está técnica busca comparar entre locutores sonidos en lapsos de 15 a 40 m/seg. Lo más similares posibles. Fue pensada para reconocimiento de palabras aisladas, la desventaja de esta técnica es que tendríamos que usar sistemas dependientes de texto.

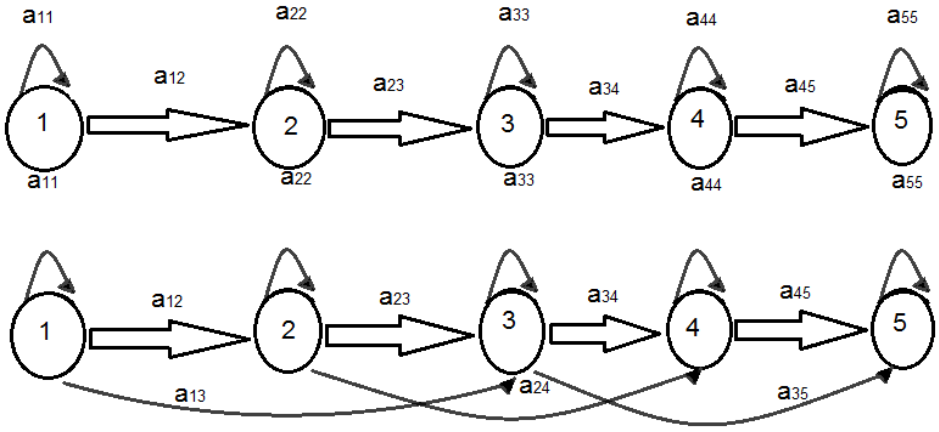
- **Cuantificación vectorial (VQ):** Cada vector N-dimensional de entrada es representado por un (codevector) de entre un conjunto pequeño de vectores (codebook). Estos pequeños codevectores son elegidos como los

mejores representantes de entre los codebook en que se pueden dividir los datos de entrada.

- **Redes neuronales (NN) :** Estas redes intentan emular el cerebro humano por medio de conexiones parecidas a las interconexiones nerviosas de nuestro sistema. Estas redes son capaces de modelar sistemas no-lineales y pueden ser utilizadas para clasificar, agrupación de datos, memoria asociativa y se han demostrado muy eficientes para aprender complejas asignaciones de entrada y salida.

- **Modelos ocultos de Markov (HMM):** Esta es la alternativa algorítmica que más aceptación tiene frente al resto ya que por su gran versatilidad que tiene en el reconocimiento del habla como en el reconocimiento de locutores. Modelo de Markov figura 1-6. Esta es una máquina de estados en la que ocurre un cambio de estado por unidad de tiempo discreto t. cada vez que entra a un estado, se genera un vector de parámetros ot. Cada uno de los estados j contiene una densidad de probabilidad bj (ot), por lo que cada vector de parámetros se forma con una misma densidad de probabilidad en cada estado. Además la probabilidad de transición de un estado i a un estado j es también probabilística, y está gobernada por las probabilidades de transición allí.

Figura 28: Modelos ocultos de Markov con estructura izquierda-derecha.



Tomado marzo 28 de 2013 Extraído del libro de tecnologías biométricas aplicadas a la seguridad por Marino Tapiador y Juan Sigüenza.

4.8 RECONOCIMIENTO DE FIRMA ESCRITA

Uno de los medios de identificación de los individuos es por medio de su escritura ya que gracias a esta nos comunicamos. En este capítulo se detallara la estructura típica de los sistemas automáticos de reconocimiento de firma, como su adquisición, clasificación de patrones, extracción de características y acondicionamiento de datos.

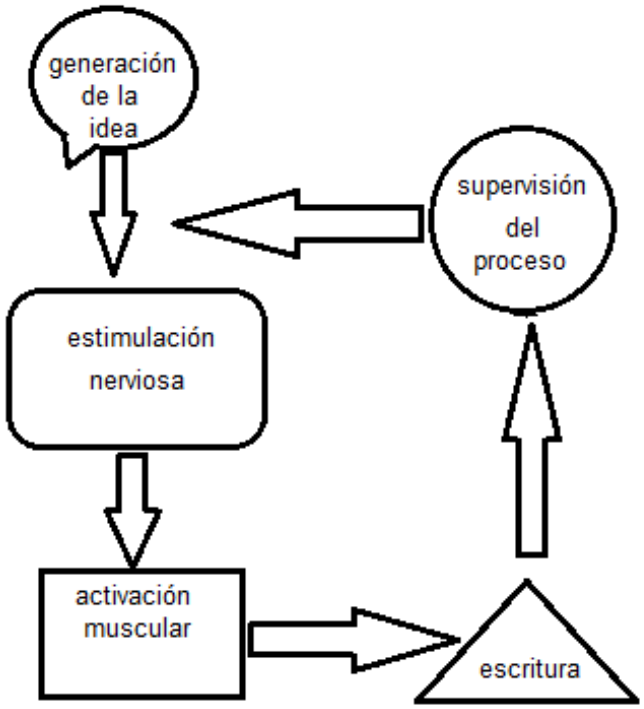
4.8.1 escritura, lenguaje, civilización y tecnología: La escritura es un modo gráfico de símbolos visuales con una determinada forma con el objetivo de registrar un mensaje y es típico de los humanos.

Todas las culturas que existieron han tenido este medio de comunicación por lo cual en esta época hemos sabido de ellos gracias a los manuscritos que han dejado incluidos dibujos y gráficos.

4.8.2 proceso de generación de escritura: Este proceso se puede simplificar en las siguientes fases:

- Generación de la idea: en esta etapa el individuo piensa o recibe la idea que quiere transmitir mediante la escritura.
- Estimulación Neuro-Muscular: como consecuencia de la idea el individuo por medio del sistema nervioso envía la señal a los músculos para la ejecución de los movimientos.
- Supervisión del movimiento: cuando los músculos se activan, la vista es la encargada de que los movimientos coincidan con la idea.

Figura 29: Proceso de generación de escritura.



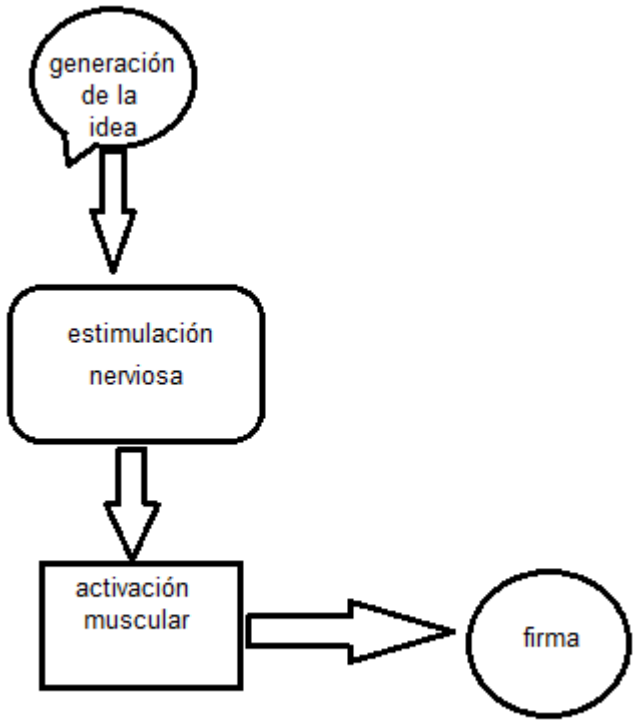
Tomado marzo 28 de 2013. Extraído del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.8.3 reconocimiento de firma manuscrita: Este es el medio más cotidiano de identificación de personas, lo podemos encontrar en el medio laboral, en cualquier tipo de transacciones ya sean bancarias o registraduría etc. Los principales factores por el cual la firma tenga una alta acogida en nuestro medio es:

- Facilidad de ejecución.
- Facilidad de verificación.

4.8.4 Proceso de generación de la firma manuscrita: Este proceso es un movimiento controlado que no necesita una realimentación de la posición de los miembros. La firma es un proceso de escritura rápida cuyo patrón de movimiento ha sido previamente aprendido por el individuo. Como esto es un aprendizaje previo hace innecesaria la supervisión del movimiento por el cerebro.

Figura 30: Proceso de generación de la firma manuscrita.



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.8.5 Adquisición de la firma: Estas se clasifican en 2 grandes grupos que son: off-line y on-line.

- **Adquisición off-line:** Estas muestras de firmas son realizadas en papel y para su captura consiste en una digitalización de dicha imagen.
- **Adquisición on-line:** En este sistema utilizamos dispositivos como tabletas digitalizadoras o acelerómetros acoplados a bolígrafos, el cual por medio de una trayectoria del bolígrafo se puede digitalizar la imagen. La ejecución de la firma y la digitalización ocurre simultáneamente.

4.8.6 acondicionamiento de la señal de firma: Este paso se hace básicamente para 3 objetivos:

- Eliminación de toda información irrelevante para el reconocimiento.
- Corrección de la información degradada durante la adquisición.
- Reducción de la variabilidad entre distintas realizaciones de la misma firma.

4.8.7 acondicionamiento para firma off-line: Este paso consiste básicamente en el procesado digital de la imagen.

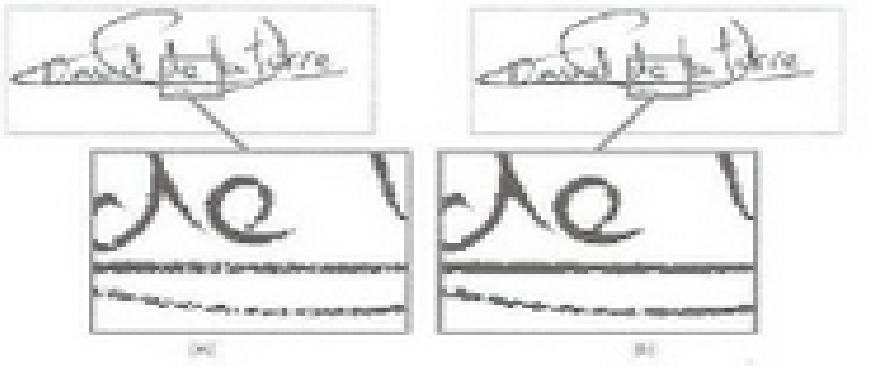
- **Binarización:** se realiza estableciendo un umbral fijo a partir del histograma de niveles de gris de la imagen.

Figura 31: Acondicionamiento para firma off- line.

Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

- **Eliminación de ruido:** Se hace después del paso de binarización y se trata de llenado de huecos, unión de trazos cortados.

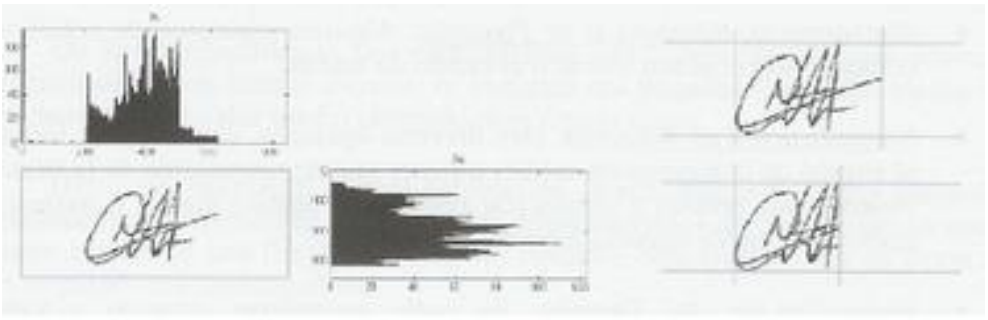
Figura 32: Eliminación de ruido.



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

- **Segmentación:** esta aísla trazos que contienen la información necesaria para caracterizar una firma.

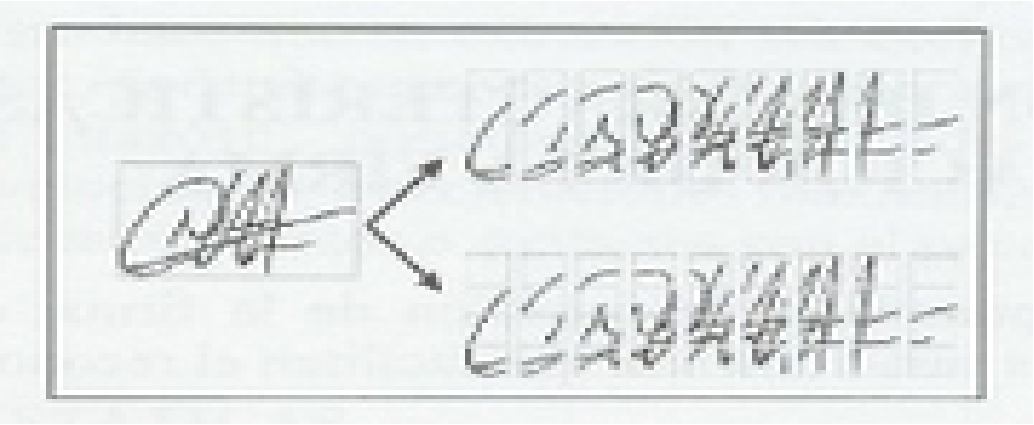
Figura 33: Segmentación



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

- **Normalización en posición y tamaño:** depende del algoritmo que se utilice en el programa puede ser necesaria la normalización en posición (respecto al punto inicial, respecto al centro de masas, etc.) y en tamaño.
- **División en celdas:** consiste en la división de la imagen de la firma en celdas de forma que cada una de ellas tenga una percepción local de la firma.

Figura 34: División de celdas.



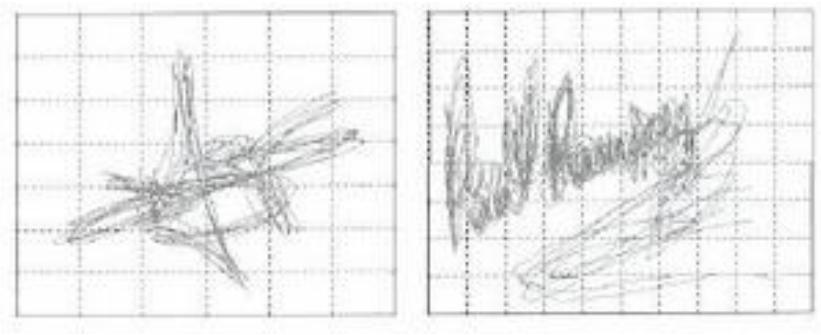
Tomado marzo 29 de 2013 extraído de http://www.slideshare.net/serweb/biometria-desarrollo-practica)

- **Otras operaciones morfológicas:** relleno de curvas cerradas, trazado de líneas horizontales, obtención del esqueleto de la firma.

4.8.8 acondicionamiento para firma on-line: Con este acondicionamiento lo que se busca es dar un aspecto más robusto a las 3 variaciones geométricas básicas, las cuales son traslación, escalado y rotación. Algunos ejemplos aplicados son:

- Alineamiento respecto a la posición: este es el eje neutro o el punto cero de partida, dependiendo de cómo se quiera tomar.
- Normalización en rotación: aquí existen diversas opciones como lo es alinear respecto al ángulo de trayectoria medio, normalizar respecto al eje mínimo momento de inercia.
- Normalización del tamaño: se normaliza respecto a rangos de variación o estadísticos de primer y segundo orden.

Figura 35: Acondicionamiento para firma on-line.



Tomado marzo 29 de 2013 extraído de http://www.slideshare.net/serweb/biometria-desarrollo-practica).

4.9 ESCRITURA MANUSCRITA

Esta parte de la ciencia ha sido muy estudiada por los profesionales forenses los cuales se enfrentan en la vida cotidiana al análisis de documentos manuscritos con el objetivo de identificar a la persona encargada de haber escrito dicho documento.

En la parte de la biometría tiene como objetivo la identificación de autor por medio de sistemas automáticos.

4.9.1 reconocimiento de escritura: Esta parte consiste en coger un documento escrito y de su forma gráfica se pasa a una computadora que por medio de una base de datos la procesa y la convierte en un texto digital, esta técnica lleva mucho tiempo en el mercado y una de las principales aplicaciones es la llamada OCR (Optical Character Recognition).

4.9.2 identificación de escritor: En esta parte de la biometría se mira el comportamiento, formas y relaciones de los trazos de la escritura, los cuales son utilizados como características para identificar el individuo. Este tema es bastante

estudiado por profesionales forenses que hacen un análisis grafístico para identificar criminales entre varios grupos sospechosos.

Uno de los estudios que se tiene documentación sobre identificación de escritor es el que se llevo a cabo por Srihari et al, en el cual participaron 1000 personas de diferente sexo, grupos de edades, etnias, etc. El cual consistió en que escribieran 3 veces con su puño y letra una carta, con lo cual crearon una base de datos y el objetivo de este experimento era consolidar la hipótesis de que cada individuo tenía una distinta escritura manuscrita.

Los examinadores forenses buscan diferentes características de estos escritos para individualizar la persona, estas características son de tipo cuantitativo y cualitativo, los cuales fueron seleccionados y clasificados en 4 grupos: elementos de ejecución, elementos de estilo, atributos de todos los hábitos de escritura y combinaciones de hábitos de escritura.

Las características computacionales utilizadas por Srihari et al (2001) fueron:

- **Nivel de documento**
    - Entropía de niveles de gris
    - Umbral de nivel de gris
    - Número de píxeles negros
    - Número de contornos interiores y exteriores
    - Número de componentes de curvatura de 4 direcciones
    - Altura media
    - Inclinación media

- **Nivel de párrafo**
    - Número de píxeles negros
    - Número de contornos interiores y exteriores
    - Número de componentes de curvatura de 4 direcciones
    - Altura media

- Inclinación media
- Ratio de aspecto
- Ancho de margen

- **Nivel de palabra**
  - Número de píxeles negros
  - Número de contornos interiores y exteriores
  - Número de componentes de curvatura de 4 direcciones
  - Altura media
  - Inclinación media
  - Longitud
  - Radio entre la zona inferior y la superior

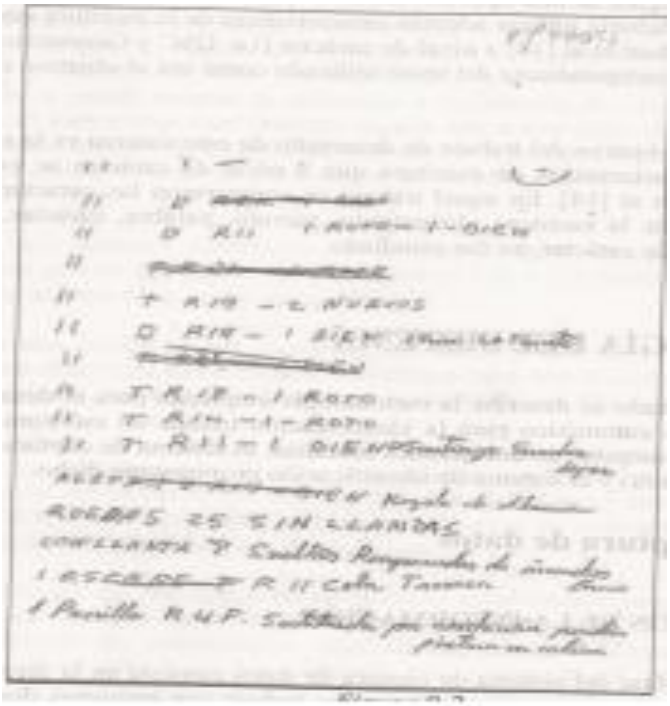
- **Nivel de carácter**
  - Número de pixeles negros
  - Radio de aspecto
  - Radio de altura y anchura del centroide
  - Características especiales
  - Características GSC (Gradient, Structural, Concavity).

4.9.3 Metodología del sistema: Consiste básicamente en la digitalización de la imagen y la forma en que vamos a ser la identificación.

4.9.4 Digitalización de la información: Después de la captura de las imágenes procedemos a digitalizarlas, las cuales pueden trabajar con fotocopias, escáner y

deben estar en tamaño A4. Estas imágenes son almacenadas en el disco duro del sistema.

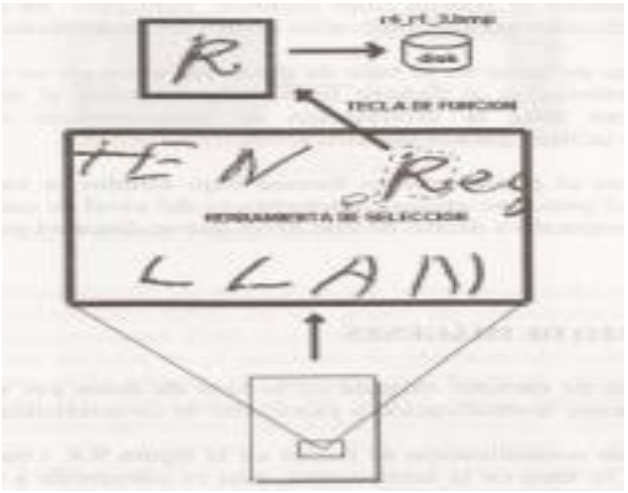
Figura 36: Digitalización de la información.



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.9.5 Segmentación de caracteres: Después que se disponga de la digitalización del documento el siguiente paso es la segmentación de caracteres, lo cual debemos contar con una herramienta de tratamiento de imágenes que será la encargada de señalar un carácter o una letra y transportarla al portapapeles del sistema el cual será el encargado de almacenar esta letra para mirar sus características y por ende la individualización de las personas.

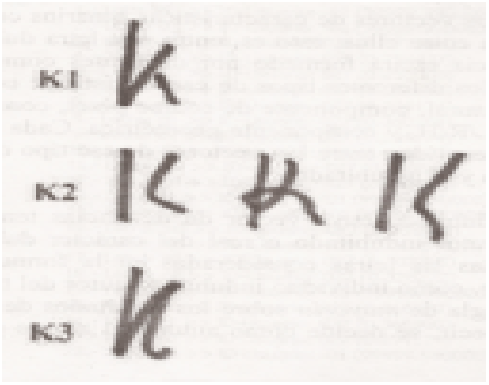
Figura 37: Segmentación de caracteres.



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.9.6 Sistema de identificación: Como podemos ver en la figura 3-3 la letra K tiene diferentes subclases, los diferentes examinadores forenses clasifican cada tipo de letra en cada una de estas subclases y luego la identificación se hace comparando estas formulaciones directamente.

Figura 38: Sistema de identificación.



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

El sistema de identificación que utilizan estos programas es el llamado el algoritmo de “vecino más próximo” que ha tenido una gran aceptación en este campo gracias a los altos porcentajes de confiabilidad que tiene.

4.9.7 Resultados: Primero se crea una base de datos que son obtenidos por medio de confiscados a delincuentes en casos reales, pero para nuestro caso tendremos una base de datos de alumnos y profesores del Pascual Bravo que tendrán acceso al laboratorio de máquinas 1. En la figura 3-4 se tiene una tabla de una base de datos.

Figura 39: Resultados.

Tomado marzo 29 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

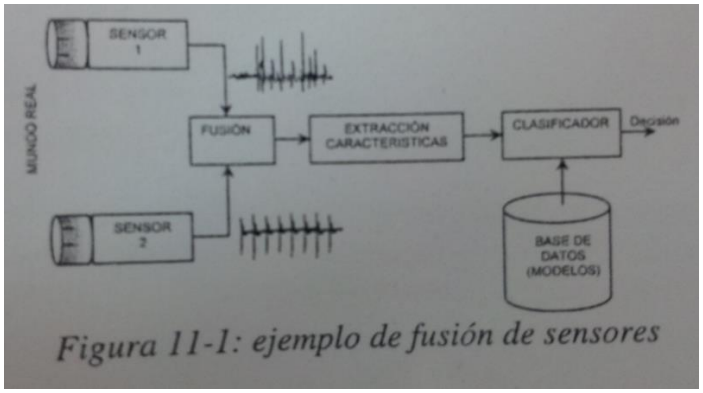
4.10 FUSION DE DATOS

El concepto fusión de información hace referencia a aquellas situaciones en las que se utiliza una combinación de informaciones provenientes de diferentes fuentes u orígenes.

Existen diversos tipos de fusiones, según la etapa en la cual se lleven a cabo, y el tipo de informaciones combinadas.

4.10.1 Fusión de sensores: En el caso de señales de voz la operación a realizar seria una combinación ponderada de las salidas de cada uno de los sensores. En cambio, si se tratara de reconocimiento de caras, podría utilizarse imágenes tomadas desde varios ángulos, para crear una imagen mosaico.

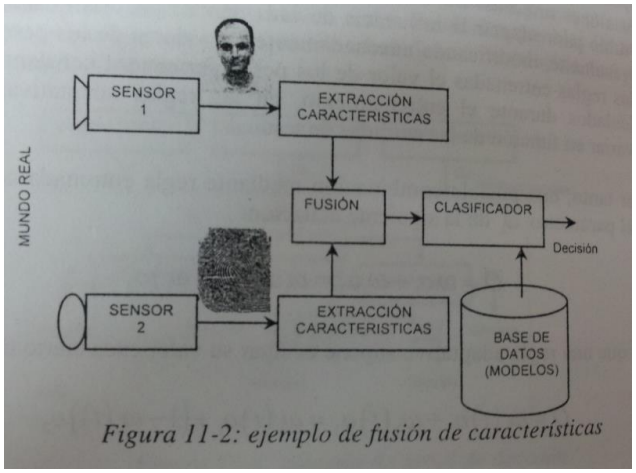
Figura 40: Ejemplo de fusión de sensores



Tomado marzo 30 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.10.2 Fusión de características: Un ejemplo de fusión multimodal biométrica que consiste en combinar las informaciones de cara y huella dactilar de una misma persona.

Figura 41: Ejemplo de fusión de características



Tomado marzo 28 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.10.3 Fusión de opiniones: También denominada de niveles de confidencia, consiste en combinar las puntuaciones (scores) proporcionadas por cada uno de los clasificadores. Típicamente las puntuaciones estarán basadas en una medida de distancia (cuanto menor sea, mayor adecuación habrá con un modelo determinado) o en una media de probabilidad (cuanto mayor sea, mayor adecuación habrá con un modelo determinado).

4.10.4 Suma ponderada: La combinación mediante suma ponderada de puntaciones consiste en asignar un peso a cada uno de los clasificadores y realizar la suma del producto de puntuaciones por los pesos respectivos.

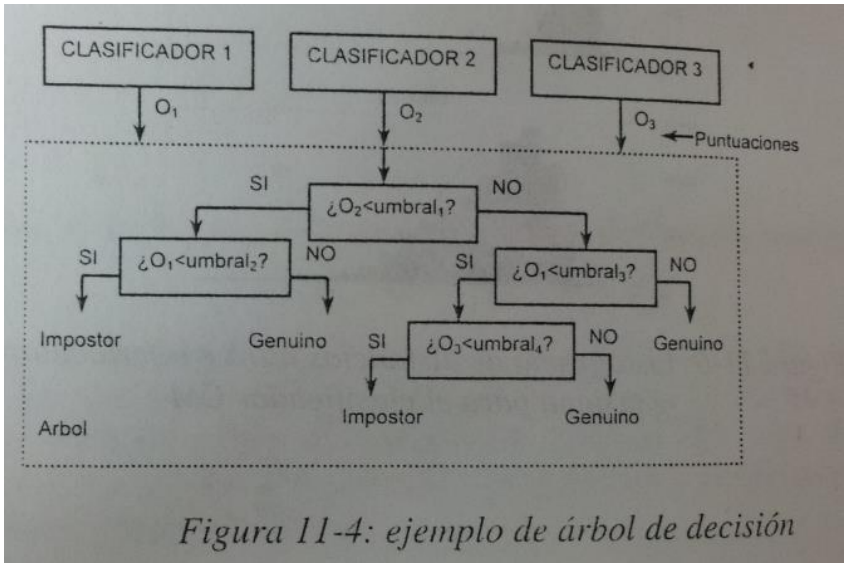
4.10.5 Reglas fijas y adaptadas: La media aritmética corresponde a una regla fijada, puesto que los factores de ponderación no se calculan a partir de lo datos. En cambio, la suma ponderada pertenece al tipo de combinadores denominados entrenados, puesto que requiere calcular los pesos a partir de una secuencia de datos de entrenamiento.

4.10.6 reglas fijas y adaptivas: Si el valor de las ponderaciones permanece constante, se trata de una aproximación no adaptativa o fija. Por otra parte, son posibles planteamientos en los que los valores de los pesos asignados a los distintos clasificadores, o por lo menos a uno de ellos, varían en función de la fiabilidad y capacidad discriminativa frente a su entrada.

4.10.7 Producto ponderado: Es una alternativa a la suma ponderada, consistente en realizar la media del producto de las opiniones (puntuaciones) asignadas por cada uno de los clasificadores.

4.10.8 Árboles de decisión: A partir de las puntaciones otorgadas por cada uno de los clasificadores y el conjunto de entrenamiento, es posible construir un árbol de decisión encadenando secuencias (si-entonces-sino). Por simplicidad en las decisiones tomadas en cada nodo, se usa en aplicaciones de verificación, puesto que en dicho caso cada una de las decisiones conduce a 2 resultados posibles (impostor o genuino).

Figura 42: Ejemplo de árbol de decisión



Tomado marzo 29 de 2013, del libro de tecnologías biométricas aplicadas a la seguridad de Marino Tapiador y Juan S. Pizarro.

4.10.9 Combinación de listas ordenadas: En esta alternativa cada clasificador proporciona como salida una lista ordenada, por orden de preferencia, de la clase pertenencia de la señal de entrada analizada. La fusión consistirá en combinar estas listas, a ser posible teniendo en cuenta la fiabilidad y capacidad discriminativa de cada uno de los clasificadores, para proporcionar una única lista.

4.11 TARJETAS DE IDENTIFICACION

Desde tiempos antiguos el hombre ha utilizado elementos que lo identifiquen a el y a su vez sus propiedades, frente a los demás.

Al principio se utilizaban tarjetas llamadas de visitas, las cuales eran construidas de cartón y las portaban personas de clase alta; con el paso del tiempo estas dejaron de ser exclusivas de esta clase y se divulgaron en todo el mundo y a lo largo del siglo XX han ido apareciendo otras alternativas en otros materiales y con mas tecnología como son las tarjetas electrónicas, evitando el fraude y mejorando la seguridad de la información almacenada.

4.11.1 Tarjeta en sistemas biométricos: La tarjeta se puede utilizar de dos maneras:

La primera es como reconocimiento del usuario, esta aplicación se encarga de buscar a la persona que tiene el patrón biométrico mas parecido a una muestra dada, es decir lo clasifica y lo busca en una base de datos.

La segunda es como autenticador, donde se busca es descubrir si la muestra biométrica que se ha captado pertenece realmente al patrón de un determinado usuario, que en el proceso de identificación ha declarado su identidad, es decir se debe responder a la pregunta ¿es esta persona quien dice ser?

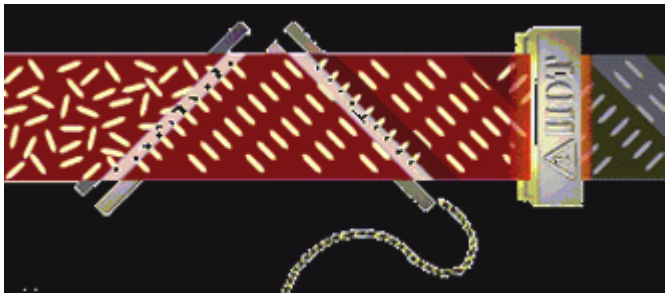
4.11.2 La tarjeta de banda magnética: Surgió en los años 50 con el boom del plástico, quien se encargo de reemplazar las tarjetas de cartón, una empresa tomo la decisión de fidelizar a sus clientes por medio de estas novedosas tarjetas, las cuales presentaban en diferentes servicios y luego los valores eran debitados de las cuentas bancarias, es así como surgen las actuales tarjetas de crédito.

Figura 43: tarjeta de banda magnética.

Tomado abril 02 de 2013. http://es.wikipedia.org

La implementación de la banda magnética en las tarjetas de plástico origino el desarrollo de los cajeros automáticos en los sistemas bancarios, donde se expandió decididamente al inicio de los años 80.

Figura 44: Banda magnética

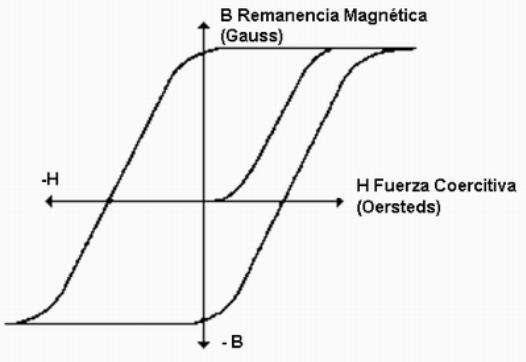


Tomado abril 02 de 2013. http://www.monografias.com

Desde el punto de vista técnico, el mecanismo de grabación y lectura de datos es idéntica al utilizado en la grabación de música en una cinta, o de una película en videos, salvo que aquí la grabación es digital.

El principio de funcionamiento radica en la curva de histéresis que presentan los materiales ferromagnéticos. Esta curva indica que un material de este tipo, al inducirle un campo electromagnético en un determinado sentido, se produce una polarización magnética de un determinado signo, siendo de signo contrario si el campo es de sentido contrario. Este tipo de materiales tiene la propiedad de mantener la polarización aunque se retire el campo inducido.

Figura 45: Curva de histéresis



Tomado abril 02 de 2013. http://www.monografias.com

El mecanismo se basa en hacer pasar a cierta velocidad la banda magnética frente a una grabadora, esta cabeza grabadora tiene una bobina enrollada a su alrededor por la que pasa una corriente lata, la cual trabaja en el sistema binario de 1 y 0; para obtener un uno o un cero se hace circular la corriente en sentidos contrarios.

- **Ventajas**
    - **Precio:** el costo es muy bajo y es su principal ventaja
    - **Utilización:** son las de mayor uso, son las más familiares entre los usuarios.
- **Desventajas**
    - **Baja capacidad de almacenamiento:** solo alcanza para almacenar un código, pero no para almacenar patrones biométricos.
    - **Facilidad de borrado de la información:** los materiales ferromagnéticos sufren desgastes, rayaduras y con el tiempo se va perdiendo el campo magnético.
    - **Grabación superficial de los datos:** los datos se encuentran grabados en el material ferromagnético y es accesible a cualquier persona y su contenido queda expuesto.

4.11.3 La tarjeta óptica o laser: Este nuevo diseño de tarjetas trabaja parecido a los discos compactos (CD) y consigue mejorar la capacidad llegando a las 4 MB, el mayor logro de estas tarjetas el aumento de memoria con un incremento leve en el precio comercial, estando por debajo de las otras tarjetas ene le mercado, inclusive por debajo que las tarjetas con chip.

Figura 46: Tarjeta óptica.

Tomado abril 02 de 2013. http://design.webtoolhub.com

Para evitar que los terminales de las tarjetas incrementaran el precio, se han desarrollado lectores que leen por infrarrojos, técnica que resulta más barata.

- **Las tecnologías de las tarjetas ópticas:** Una tarjera óptica consta de varias capas, la más exterior es una capa protectora que aísla el resto de la tarjeta, por debajo se encuentra otra capa también de protección y transparente pero más gruesa. A continuación encontramos la capa donde se almacenan los datos y se llama capa óptica de grabación.

  En el proceso de grabación se hace incidir un haz de luz láser de lata potencia para obtener un uno y si quiere obtener un cero se hace una codificación negativa, este haz crea un hoyo en la capa óptica que modifica las capas de reflexión de la capa en ese punto. El hoyo de diámetro de 5 micras se sitúa entre unas guías de 1.4 micras las cuales delimitan la tarjeta en pistas de unas 12 micras cada una.

La lectura se realiza haciendo incidir sobre la lectora un haz de menor potencia y detectando la existencia o no de flexión. El detector dará una lectura en el sistema binario de unos o cero y estos a su vez mostraran la información contenida en la tarjeta.

- **Ventajas**

    - Alta capacidad de almacenamiento: puede almacenar hasta 4 MB, lo cual hace susceptible el guardar patrones biométricos de gran tamaño.

    - Mayor robustez del soporte: comparada con la banda magnética, la banda óptica no se deteriora por campos electromagnéticos, no se raya fácil. De esta forma se considera que la información es más estable.

- **Desventajas**

    - Grabación superficial de los datos: igual que la banda magnética los datos se encuentran almacenados superficialmente.

    - Alto costo: esto se da por la no expansión del mercado, deberían ser tan baratas como las de banda magnética.

    - Desconocidas al gran publico: desconocimiento de los usuarios, genera rechazo y difícil adaptación.

4.11.4 La tarjeta chip: Tiene alrededor de tres décadas de existencia, la primera idea de una tarjeta con un chip empotrado en su interior se dio en los años 70, también por esta década se dieron avances en las tarjetas chip como el de la tarjeta de plástico con un chip programable, posteriormente en Japón a finales de la década se implemento las tarjetas sin contactos.

Los esfuerzos de las compañías materializaron diversos prototipos, estos supusieron un efecto innovador en la industria de la microelectrónica.

Es así como industrias como Phillips y Bull incursionaron en la fabricación de microprocesadores, mientras que estas compañías se afianzaban en el desarrollo de los microprocesadores, Schlumberger analizaba la viabilidad de tarjetas con circuitos integrados, con cierta inteligencia que pudiera competir en la relación costo/beneficio comparadas con las tarjetas de banda magnética.

Los desarrollos de Phillips desembocaron en la creación de una arquitectura distribuida, en la que el microprocesador y las memorias se encuentran en microchips independientes., los cuales necesitaban un bus de comunicación entre los microchips.

- **Tarjetas inteligentes:** Son aquellas que están basadas en un microprocesador y una memoria, lo cual se conoce como un micro controlador.

- **Tarjetas de memoria:** Son tarjetas de circuito integrado, en las que este no contiene un microprocesador, estas pueden ser:

- **De acceso libre:** no disponen de mecanismo alguno de protección de los datos. Son tarjetas que sirven únicamente como soporte portátil de información.

- **De acceso protegido:** protegen determinadas zonas de la memoria, ya sea mediante un fusible (que al quemarse inhabilita la escritura en la zona seleccionada) o mediante lógica cableada (que permite la introducción de un pin para facilitar el acceso a otra zona.

- **Tarjeta con contacto:** La comunicación se hace desde la conexión física de cada uno de los contactos metálicos de la tarjeta con los correspondientes de la lectora.

- **Tarjeta sin contacto:** La comunicación se realiza de forma aérea mediante radio frecuencia, por tanto no es necesario un contacto físico entre la tarjeta y la lectora. A estas tarjetas se les llama Tags y sirven especialmente para la identificación de animales o personas para sistemas de control de acceso.

- **Tarjeta hibrida con / sin contacto**: Son una mezcla de los dos tipos anteriores en donde se mezclan las ventajas de seguridad de una tarjeta con contactos, con la velocidad de las tarjetas sin contactos, esta variedad se aplica para tarjetas inteligentes es decir con microprocesador.

- **Ventajas**

    - **Capacidad de almacenamiento:** mayor que la tarjeta de banda magnética, pero inferior que la tarjeta óptica. Posee 8KB, pero solo por estrategias comerciales su capacidad podría ser mayor

    - **Robustez del soporte:** este tipo de tecnología es muy robusta frente a agentes climáticos o del medio, no sufre alteraciones su contenido salvo por mal uso.

- **Desventajas**

    - **Grabación de datos superficiales:** si el acceso a los datos no se encuentra protegido por ningún mecanismo adicional, su acceso es libre

y por lo tanto los datos pueden ser leídos sin ningún problema, lo que conlleva de nuevo a los problemas de facilidad de copia y de posibilidad de descifrado de los datos.

- **Desconfianza del gran público:** estas tarjetas son conocidas por los usuarios, ya que son típicas en los sistemas de telefonía pública. Sin embargo, la aparición de mafias dedicadas a clonar, hace que el usuario desconfíe de que realmente su información se encuentre segura.

4.11.5 La tarjeta inteligente: Es una tarjeta de plástico de medidas normalizadas, que contiene un circuito integrado donde guardar la información. El aspecto diferenciador de estas tarjetas con respecto a las demás tarjetas de chip es que el circuito integrado es un microprocesador.

- **Bloques de una tarjeta inteligente:**
  - **Unidad central de procesos:** Controla todo el funcionamiento de la tarjeta y ejecuta el sistema operativo, suele ser un microprocesador de 8 bits, aunque se puede encontrar de 16 y 32 bits.
- **Memorias**
  - ROM: donde se encuentra almacenado el sistema operativo
  - RAM: para los cálculos temporales que necesite el sistema operativo.
  - EEPROM: es la memoria propiamente dicha que puede utilizar el usuario para guardar su información. Es de tecnología no volátil, lo que le permite mantener la información grabada después de retirar la tarjeta.

- **Bloque de entrada y salida:** es el medio de comunicación de la tarjeta con el exterior, comunicación que se realiza a través de una única línea serie bidireccional.
- **Sistema de control de la alimentación:** para poder asegurar una alimentación de la tarjeta correcta y evitar fallos eléctricos en su interior.
- **Circuitería de arranque:** para que el terminal le indique a la tarjeta el momento en el que empieza la comunicación.
- **Sistema de supervisión de reloj:** para asegurarse de que la señal de reloj que se le suministra a la tarjeta sea estable y limpia.

- **Sistema operativo de la tarjeta inteligente (SOTI):**El sistema operativo proporciona una interfaz de comandos de alto nivel que facilitan el uso de la tarjeta inteligente. El SOTI no permite en ningún momento la ejecución de ninguna instrucción de bajo nivel, ni puede contener ninguna instrucción que pueda poner en entredicho la seguridad de la tarjeta, de esta manera se facilitan funciones como impedir la ejecución de instrucciones hasta que no se haya realizado un reset, después de recibir el reset, inicializa los parámetros de la tarjeta, da una respuesta y espera la recepción de una instrucción externa.

  La tarjeta inteligente puede prestar servicios como:

  Controlará el intercambio con el mundo exterior, si las verificaciones son positivas, ejecuta las instrucciones y da una respuesta y si la verificación es negativa, la respuesta emitida es un error al exterior.

  Gestionar el manejo de la memoria y de los datos, el SOTI alcanza el mismo rendimiento que un ordenador personal, en el que a los datos en el disco duro, no se hace referencia por su situación física, sino que gracias al sistema, se realiza por el identificador del fichero que los contiene y su posición relativa.

  Gestionar los mecanismos y servicios de seguridad**,** la tarjeta inteligente se va a comportar como un sistema portátil de extremada seguridad., incorporando a los ficheros unas determinadas reglas de acceso conforme unas claves.

  Controlar las fases del ciclo de vida de la tarjeta, puesto que no se puede permitir que el robo de un número de tarjetas en un proceso de transporte, implique la ruptura de la seguridad de un sistema basado en tarjetas inteligentes. Este control se realiza mediante unas claves de transporte.

- **Sistemas de ficheros:** El SOTI integra todo un sistema de ficheros para acceder a los datos que tiene grabados el usuario en la tarjeta, los cuales están estructurados de la misma forma que lo están en un ordenador, con una estructura jerárquica que se encuentra definida en la norma IS7816/4. En esta norma se definen los tipos de ficheros, los cuales se relacionan a continuación.

  - **Fichero maestro (MF):** es el directorio raíz de la tarjeta inteligente y su identificador es el 3F00.

  - **Fichero dedicado (DF):** es la nomenclatura para referirse a los directorios, es decir, son ficheros que, en lugar de contener datos, contiene ficheros.

- **Fichero elemental (EF):** es un fichero propiamente dicho, es decir, aquel que contiene datos se pueden clasificar según la utilización o según la estructura que tengan los datos.

- Según la utilización se clasifican en:

  - **Internos:** son aquellos que son interpretados por la tarjeta para operaciones internas, un ejemplo puede ser un fichero de claves, ya que estos no pueden ser leídos.

  - **De trabajo:** son los que utiliza el usuario libremente según las condiciones de acceso que se han establecido en la aplicación.

- Según la estructura de los datos se clasifican así:

  - **Transparentes:** son aquellos que no tienen estructura, es decir, todo el tamaño del fichero es un único bloque donde se puede almacenar datos. Para acceder a algún dato hay que especificar la ubicación del registro.

  - **De registros de longitud fija:** están estructurados en registros y todos estos tienen una longitud definida. La referencia a los datos se hace mediante al número de registro.

  - **De registros de longitud variable:** es el mismo caso que el anterior, pero aquí no se tiene la restricción de la longitud para todos los registros. Y la referencia es idéntica al caso anterior

  - **Cíclicos:** son ficheros de longitud fija en los que no existe una referencia absoluta de los registros, es decir, no tiene ni principio ni final, sino que se tiene un puntero al último registro al que se ha accedido.

- **Tipos de tarjetas inteligentes:** Atendiendo a dos parámetros diferentes como es la forma de comunicación y la funcionalidad ofrecida, las tarjetas inteligentes se pueden clasificar en varios tipos como son:

- **Tarjetas de contactos:** Son las más extendidas y reconocidas, ya que tienen los contactos del chip en la superficie del plástico. Su comunicación es mediante señales electrónicas que van por cables hasta los contactos a través de un zócalo, las señales son de niveles TTL (3v a 5v) y mediante los contactos se a la tarjeta: la alimentación (Vcc), la masa (GND), el reloj (CLK), el reset (RST) y la señal de entrada y salida de datos (I/0).

- **Tarjetas de acoplo:** La comunicación no se realiza con contactos electrónicos, sino por acoplos capacitivos e inductivos. Hay que ubicar la tarjeta tocando el lector, su función principal es mas de tarjeta de memoria que como tarjetas inteligentes.

- **Tarjetas de proximidad:** Se comunican por radiofrecuencia a una distancia entre 0 a 10 cm. En esta tarjeta, como en todas las que no tienen contactos, no se aprecia superficialmente la existencia del microcontrolador, aunque se encuentra al interior del plástico. La tarjeta tiene una antena por medio de la cual recibe la alimentación (por inducción de campo eléctrico)

- **Tarjetas de vecindad:** Se trata de una versión de las tarjetas de proximidad; pero donde la comunicación se puede realizar a distancias más elevadas (a partir de 10 cm).

- **Tarjetas de sistema operativo:** Son las tarjetas inteligentes clásicas. El inconveniente es que el desarrollador de la aplicación se encuentra restringido por las limitaciones que le ofrece el sistema operativo.

- **Tarjetas criptográficas:** Son idénticas a las anteriores, pero en este caso, además de hacer operaciones de criptografía secreta, también pueden hacer cifrado o firma con algoritmos de criptografía publica, su gran inconveniente además de estar restringido por el sistema operativo. Es el alto costo que tienen.

- **Tarjetas de sistema operativo abierto:** Son tarjetas en las que el diseñador de la aplicación puede crear su propio juego de comandos y estructura de datos. Incluso hasta estructura de seguridad, el caso más conocido es el de las tarjetas Javacard, las cuales se programan en lenguaje Java, con este tipo de solución, se gana en versatilidad, pero se pierde en potencia de cálculo.

- **Tarjetas de sistema abierto criptográficas:** Es la unión de las dos anteriores. Pero su mayor inconveniente es su alto precio en el mercado.

- **Sistemas biométricos match on card:** Esta idea se deriva de las tarjetas inteligentes, las cuales son sistemas microinformáticos, con capacidad de procesamiento de información, además las tarjetas inteligentes pueden contener información del usuario la cual es pertinente proteger, por tal motivo una identificación biométrica, comparada con un patrón de esta, determina una nueva aplicación en la tecnología de los controles de acceso biométricos.

- **Ventajas**

    - Mayor comodidad para el usuario, ya que no tendrá que recordar números, abriendo así las puertas a la aplicación a gran escala en otros usuarios

- Mayor seguridad porque el usuario no aplica técnicas como poner el mismo número a todas sus tarjetas.

- Se identifica realmente a la persona, no al portador de un número.

- El patrón biométrico no saldrá de la tarjeta, por lo que fallos de seguridad en el sistema, virus, entre otros no comprometerían el patrón biométrico.

- **Desventajas**

  - En algunas técnicas biométricas el patrón es tan grande que dificulta el almacenamiento en una tarjeta inteligente.

  - En otros casos el vector de caracterización también puede ser demasiado grande y requiere mucho tiempo y recursos para ser transmitido a la tarjeta inteligente.

  - También puede ocurrir que el algoritmo de verificación es demasiado complejo, para que pueda realizarse la verificación en un microcontrolador de una tarjeta.

4.11.6 Estándares biométricos: Los estándares biométricos son las reglas que tienen los productos y que tienen que cumplir cada una de ellas. Son procedimientos o investigaciones que afirmen ser compatible con el mismo producto. Estos estándares ofrecen muchos beneficios como es la compatibilidad entre productos, generación de madurez y estabilidad para los consumidores.

- **El papel de los estándares biométricos:** Hoy en día los software y el hardware que se utilizan en la industria biométrica son de tecnología propietaria y que puede variar debido a la inmadurez que se tiene todavía con respecto a este tema.

  A esto es a lo que se enfrentan las empresas que laboran en este campo, que en cualquier momento llegue otra tecnología y tengan que reorganizarse apuntando a estos nuevos métodos de sistemas y sensores biométricos.

  Por más que adoptemos estándares biométricos se debe aclarar que esto no asegura una total compatibilidad entre dispositivos y tecnologías.

- **Estándares internacionales**

  - **Bio api:** Nace en abril de 1998 y su idea es de estandarizar el modo en que las aplicaciones se comunican con los dispositivos biométricos y la forma en la que los datos son almacenados y utilizados. Las funciones de Bio api cubren aspectos como el entrenamiento, la verificación e identificación de usuarios, la captura de datos, el proceso de los mismos, la comparación de patrones y el almacenamiento de la información biométrica.

  - **Bapi:** Fue desarrollado y planeado por un vendedor de soluciones biométricas llamado I/O software. Microsoft fue uno de los primeros apostadores por Bio api, pero también le aposto a BAPI.

    Esto nos conduce a una situación indeseada ya que lo que queremos es lograr un único estándar en la parte de biometría.

  - **Ambi:** La Ambi Asociación Mexicana de Biometría e Identidad fue creada por el Ingeniero Mexicano Humberto López Gallegos en el año de 2007 con el objetivo de promover nuevas técnicas para una mayor eficiencia en el campo de la biometría para aplicarlo principalmente en Estados Unidos, Europa y Latinoamérica.

4.12 SEGURIDAD INFORMÁTICA Y PKI

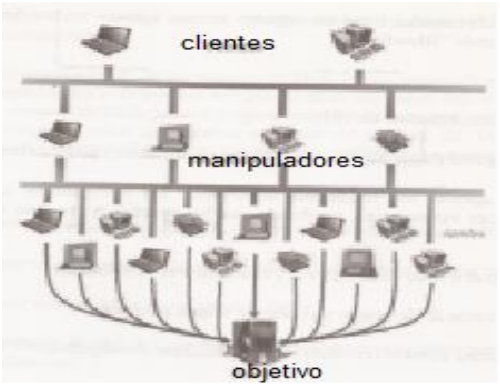
Hoy en día la mayoría de las empresas quieren incursionar en el campo on-line para garantizar una serie de ventajas como sería la comunicación constante entre sus proveedores, clientes y socios, incluso realizar negocios electrónicos. Pero claro que existe vulnerabilidad y todo tipo de ataques por parte de un sin número de agresores. Surge como una contra respuesta unas nuevas herramientas de seguridad o simplemente evolucionan las ya existentes en este momento.

A parte de que tiene que afrontar a los agresores también tiene que lidiar con problemas en su diseño, instalación, programación, gestión, errores en su funcionamiento, en su utilización, también se enfrenta a amenazas externas como virus, gusanos y caballos de Troya.

4.12.1 Amenazas comunes: Aquí se analiza principalmente las amenazas externas consideradas intencionales.

- **Denegación del servicio:** Este ataque tiene el objetivo de impedir el acceso de la victima a un recurso determinado como por ejemplo almacenamiento, conectividad o capacidad de computo, los daños ocasionados por este ataque DOS siempre serán económicos y moral a la víctima. Económico porque no puede ingresar a internet a ser sus negocios correspondiente y moral porque deja en evidencia para todas las faltas de seguridad y de que no está preparada para afrontar un ataque de esta magnitud.

Figura 47: arquitectura de denegación del servicio



Tomado marzo 30 de 2013, libro de tecnologías biométricas aplicadas a la seguridad por Marino Tapiador y Juan Sigüenza.

- **Man-in-the-middle (mitm):** Este ataque consiste en la capacidad que tiene el atacante para establecerse como intermediario entre la victima a atacar y otra máquina o recurso a la que la víctima acceda. Dentro de los ejemplos encontramos suplantación de identidad, de dirección IP, comunicaciones y de la sesión ya iniciada.

  Estos ataques son los más peligrosos ya que alguien que pueda ingresar en nuestras comunicaciones puede llegar a violar varios mecanismos de seguridad.

- **Sniffing:** Estos sirven para profundizar una infiltración ya iniciada ya que son considerados totalmente pasivos lo que hace casi imposible detectar su presencia. Técnicas que se han estudiado para detectar la presencia de los sniffers:

    - Envío de paquetes TCP/IP que de no ser descartados generarán respuesta.

    - Test ARP, consiste en enviar una petición ARP con todos los datos correctos excepto la dirección MAC destino.

    - Test DNS (para ver si el sniffer intenta resolver los nombres DNS de las IP numéricas).
    - Test de latencia (para detectar si el tiempo de respuesta medio de una máquina depende de la carga de la red).

- **Fraude:** En internet también existe el fraude y este consiste prácticamente en falsificar alguna información para nuestro beneficio, frecuentemente económico. Para realizar un ataque seguro lo primero que debe hacer el agresor es no dejarse ubicar lo que conlleva a que este tipo de gente utilice equipos que no sean de su pertenencia o sea que puede lanzar estos ataques de sitios públicos como bibliotecas o cibercafés.

  Dentro de estos encontramos (votaciones fraudulentas, fraudes con tarjetas de crédito, creación de cuentas gratuitas de correo electrónico).

4.12.2 Técnicas de defensa: Nuestro mundo también ha evolucionado con respecto a defensa se trata, dentro de estas técnicas encontramos (división de redes por niveles de seguridad, cortafuegos, proxys de aplicación, filtrado de entrada y salida, sistemas de detección de intrusos IDS, hosts y redes trampa.

4.13 MARCO CONCEPTUAL

El trabajo de investigación contiene vocabulario técnico el cual es pertinente aclarar para un mayor entendimiento, es así como todo este gira en torno a implementar un sistema de seguridad para el control de acceso, del cual se

entiende como el conjunto de dispositivos colocados estratégicamente en el perímetro de un sitio específico para detectar las presencia, irrupción, o invasión de un desconocido o de un individuo que no posea un acceso permitido, estos sistemas de seguridad tienen varios dispositivos de identificación como lo es la biometría que es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas, teniendo así un registro de los usuarios del laboratorio.

Este registro es almacenado en una base de datos el cual es el conjunto de rasgos o parámetros de identificación personal de los usuarios, almacenados en una memoria. Por medio de los dispositivos mencionados se llega a la automatización en la institución, automatizar es el proceso por el cual se agiliza una labor o tarea con la intervención directa de la tecnología.

Los dispositivos de identificación son elementos que reconocen y almacenan datos de los usuarios del sistema de seguridad, para facilitar el acceso a ciertas áreas en este caso el laboratorio de maquinas.

Los primeros estudios de identificación para las personas se hicieron basados en la antropometría que es la ciencia que estudia las medidas del cuerpo humano, para individualizar a las personas también existen técnicas como el reconocimiento del iris en el ojo que también es un parámetro biométrico.

Otra manera de identificación de las personas data de la revolución comercial con las tarjetas plásticas, que empezaron a reemplazar el dinero y con el transcurrir del tiempo se implementaron en otras áreas como la de identificación con la creación de tarjetas de proximidad.

4.14 MARCO HISTÓRICO

Actualmente la seguridad de los laboratorios del bloque 1 y 2 es buena si la comparamos con la seguridad de hace algunos años, hoy en día todos los laboratorios del Instituto Tecnológico Pascual Bravo, cuentan con un sistema de seguridad muy simple y poca tecnología, algunos de estos laboratorios tienen sensores de movimiento y los demás cuentan con chapas y sus respectivas llaves o candados con cadenas; mientras los laboratorios no estén siendo utilizados permanecerán cerrados. El personal asignado para la custodia y administración de los laboratorios realizan una tarea bastante ardua para mantener estos recintos al día, durante el transcurso del día realizan caminatas por todos los laboratorios revisando el personal que allí se encuentra, de observar movimientos sospechosos, que si estén utilizando los laboratorios de la mejor manera, entre otros aspectos, estas funciones están delegadas en monitores y personal

vinculado con la institución quienes refuerzan el proceso del día a día. Para los docentes que van hacer uso de estos laboratorios deben ubicar a las personas encargadas (monitores) para solicitar permiso de su ocupación, ellos le brindaran toda la información que concierne a estos recintos, inclusive la solicitud de equipos didácticos como un Videobeam para complementar la clase se puede realizar con ellos, todos los docentes al terminar la clase deben entregar al monitor en el mismo estado que se le hizo entrega del aula, sin ningún daño, esto incluye los equipos que haya solicitado como adición a la clase, si dentro de los recursos solicitados por el docente, alguno de ellos sufre una avería por mal uso, esta persona debe asumir el costo de este recurso.

Hay “tranquilidad” que todo el inventario que existe en los laboratorios del Instituto Tecnológico Pascual Bravo es verificable en su totalidad, no obstante, hay conciencia que el mundo es de cambios y la tecnología lo lleva de la mano en ese sentido, el Instituto Tecnológico Pascual Bravo sabe que debe estar a la vanguardia de las mejores instituciones del país como ejemplo a seguir para otras Universidades.

La gran política para que hoy en día estos inventarios sean confiables, verificables, reales y que el manejo de ellos sea óptimo, es por la implementación de la cultura y el amor por el servicio

Que pasaba con el sistema anterior?

La metodología aplicada al uso de los laboratorios hace algunos años, era muy rígida sin ninguna flexibilidad, siguiendo unos lineamientos entregados por la Institución que estaban llevando al personal y a los estudiantes a enfrentamientos verbales y físicos, es decir, si la persona no llenaba la planilla correctamente y no firmaba como prueba de entregado o recibido, no podía hacer uso de él, de igual forma para solicitar algún instrumento, entonces allí ya se incitaba a una discusión que en muchas ocasiones terminaron en bochornosos espectáculos, por eso mencionábamos en el párrafo anterior que la política tomada por el nuevo personal fue fomentar la cultura estudiantil, de crear conciencia que todos los equipos al interior de estos laboratorios como la parte física es de todos los estudiantes para su beneficio actual y para las futuras generaciones, que si debían existir unas reglas o normas como en toda institución, pero el frente de esta problemática era culturizar a todo el personal docente y estudiantil, mostrar los daños y los beneficios que se pueden tener al comparar un comportamiento negativo con otro positivo. El trato a la persona debe ser muy educada para que desde un comienzo haya un vinculo de seguridad y respeto, no solo por la persona como tal sino por el servicio prestado.

Que se perdía o dañaba?

Dentro del Instituto Tecnológico Pascual Bravo cualquier recurso didáctico, era o es tentativo para el personal docente y estudiantil y que en el momento de la pérdida o daño el resultado era el mismo, un perjuicio para la institución y obviamente al personal docente y estudiantil; para hacer una pequeña reseña de los recursos que más se perdían, son los siguientes:

Alambre (Cables por su cobre), escobillas de los motores, los motores propiamente, los transformadores, prensas, multímetros.

Los laboratorios no deben depender y tampoco deben descargar o delegar todo el proceso en una máquina que beneficiará la seguridad del laboratorio y que la carga laboral en el personal designado para ello será menor, pues finalmente el servicio y la cultura deben seguir acompañando esta tecnología, pues esa es la esencia de un buen funcionamiento.

Para la investigación, estudio y posterior socialización del proyecto se cuanta con los sistemas de seguridad implementados en bancos, universidades y hoteles, recopilando la información actual para ser vanguardistas, pero también los antecedentes históricos de estos sistemas que brindan un valioso aporte a la proyecto.

Con base en estos modelos se toma como punto de partida la implementación de los sistemas de seguridad de la universidad de Antioquia y de Bancolombia.

Para determinar la funcionalidad de los sistemas y que se observe en detalle la magnitud del proyecto.

Para el acceso a los laboratorios o a otra dependencia dentro de la institución no se tiene documentación sobre antecedentes históricos del proyecto o similares.

En la actualidad se implementa un sistema de control de acceso para el ingreso a la universidad en la portería peatonal del sector del volador, el cual consta de tres molinetes o torniquetes con lector de tarjeta con chip para a la identificación de cada estudiante y posterior ingreso.

5. METODOLOGIA

5.1. TIPO DE ESTUDIO

Este proyecto es del tipo Teórico-Práctico. La parte teórica está establecida en las actividades referentes a la investigación, selección, compra del dispositivo biométrico para el control de acceso al laboratorio. La estructuración teórica tiene como finalidad minimizar el margen de error a la hora de la compra del dispositivo, así como fundamentar la parte práctica que se debe dar en una segunda parte de este proyecto.

La parte práctica consiste en la tarea de montaje y ensamble de los componentes del sistema de seguridad para controlar el acceso

.

5.2. MÉTODO

Investigativo porque atreves del análisis y selección de la información recopilada, se determina y caracteriza el tipo de producto a adquirir e implementar.

5.3. POBLACIÓN

El proyecto va dirigido a todos los estudiantes, docentes y laboratoristas del Tecnológico que intervengan o interactúen directa o indirectamente con el laboratorio.

5.3.1 Fuentes primarias

La información necesaria para el desarrollo de este proyecto se obtuvo mediante el análisis de los diferentes dispositivos utilizados por parte del personal de la empresa Homini, en la implementación y puesta en funcionamiento de dispositivos de control de acceso y seguridad.

5.3.2 Fuentes secundarias

Manuales, libros, internet, donde se extrajo la información necesaria para el desarrollo de este proyecto.

5.4. PROCEDIMIENTO

Recopilación de la información, asesorías técnicas, informes de avance, reuniones de equipo, elaboración del informe final y entrega del anteproyecto y posteriormente el proyecto de grado.

6. RESULTADOS DEL PROYECTO

El proyecto es un sistema de seguridad que permite a los usuarios ser identificados cuando acercan un dedo sobre el lector de huellas digital.

Con base en la investigación realizada se determinó que la opción más acertada para la implementación de un sistema de seguridad para el control de acceso al laboratorio; es por medio de un dispositivo biométrico que reconoce las características de las huellas dactilares. La información que se recibe en el lector de huella en el momento del acceso al laboratorio, permite identificar o no a una persona.

Esto gracias a cotejar las características físicas de esa persona; en ese momento con los parámetros almacenados en la base de datos; quienes son los responsables de la identificación de los rasgos de la huellas dactilares.

La base de datos del dispositivo tiene capacidad para almacenar 2000 huellas, que son suficientes para identificar a los responsables de los laboratorios o a quienes ingresen a estos en cualquier momento.

La primera es almacenando con anterioridad los rasgos de las huellas en la base de datos, la cual es cotejada con la huella que se introduce en el dispositivo esta dará o no la autorización a una persona para que ingrese al laboratorio. La segunda la base datos lleva un registro de quienes, cuando, cuanto tiempo ingresaron al laboratorio, por medio de este se controla el uso de los laboratorios en las asignaturas.

El dispositivo puede ser anclado a la pared y luego de que el usuario se ha acercado, para ser identificado; la puerta del recinto se abre si está autorizado, si el dispositivo solo se va a usar como registro, todos los estudiantes que pretendan ingresar al laboratorio deben identificarse en el dispositivo.

Por motivos de presupuesto en este trabajo de solo se lleva a cabo la investigación y la compra para la implementación del dispositivo más acorde a las

necesidades de la institución, los detalles del montaje y los accesorios del control de acceso se darán en el capítulo de recomendaciones.

El control de acceso tiene las siguientes especificaciones generales

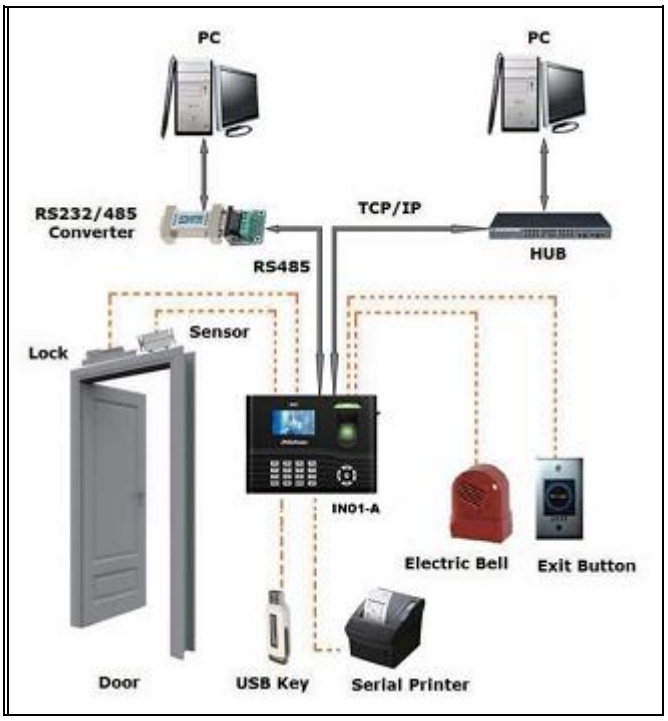
- Batería de respaldo que brinda autonomía de 8 horas sin suministro de energía.
- Carcasa elegante para adaptación a espacios exclusivos.
- Fácil instalación, seguro y confiable.
- Sencillo modo de operación.
- Avisos de confirmación audiovisual.
- Función webserver para administración remota de los registros de acceso.
- Sencilla administración desde un solo PC de hasta 255 equipos.
- Pantalla de 2,5 pulgadas.

Óptimo para medianas y pequeñas empresas que necesiten hacer control de asistencia a sus empleados, genera reportes de entradas, salidas, horas extras, ausencias, retardos, salidas temprano, permisos etc.

Figura 48. Control de acceso EP300

Tomado mayo 2013. www.services.com

Figura 49.Diagrama de conexión



Tomado mayo 2013. www.services.com

Tabla 3. Características del control de acceso

Ítem	**Descripción**
Capacidad de Huellas:	2.000 huellas
Capacidad de transacciones:	50.000 registros
Plataforma de Hardware:	Procesador USA TI 300 Mhz
Batería:	Batería incluida que brinda autonomía de 8 horas sin suministro de energía
Sensor:	Anviz Óptico
Algoritmo:	Bio Nano de alta velocidad
Comunicación:	TCP/IP y USB
Pantalla:	2,5 pulgadas
Alimentación de Energía:	12 VDC 0,5A (amigable con el medio ambiente, por bajo consumo de corriente)
Tamaño:	185X130X35 (mm)

Software:	Software incluido en español
Reportes:	Reportes de asistencia, días festivos ausencias, retardos, horas extras, etc.

Figura. 50. Aplicaciones del control de acceso

Tomado mayo 2013. www.services.com

figura 51. control de acceso real EP300

Fotografía tomada mayo 28 de 2013.

7. CONCLUSIONES

- Los sistemas biométricos, requieren de un a base de datos para cotejar o comparar las características de ciertos rasgos de las persona. Es decir requieren un patrón de comparación, para poder ser efectivo.

- La biometría es una rama de la biología, encargada de analizar y diferenciar los rasgos de las personas, para identificarla y personalizar las bases de datos.

- La biometría surgió para identificar a los criminales, posteriormente se tomaron estas bases de datos para individualizar las personas.

- Las huellas dactilares de una persona son irrepetibles en otra y son invariables en el tiempo.

- Las huellas dactilares son vulnerables a factores químicos y pueden deteriorarse impidiendo la correcta identificación de las personas.

- Los sistemas biométricos se diferencia uno de otro por la extracción del patrón biométrico y el tipo de patrón que se emplea para la identificación.

- Los sistemas biométricos se pueden combinar para obtener una alta seguridad en el sistema; es decir una aplicación entre tarjetas, huellas, geografía de la mano, reconocimiento del iris, entre otros.

- La aplicación de los sistemas biométricos en la institución fomenta el estudio de los sistemas de control y seguridad para la identificación de las personas y posterior aplicaciones a nivel industrial.

8. RECOMENDACIONES

Por motivos de presupuesto este proyecto solo llega a la fase de recopilación de información, selección y compra del dispositivo biométrico con soporte técnico o software.

El proyecto queda a la expectativa por la parte del montaje del dispositivo biométrico y todos sus componentes, tales como los electroimanes para abrir y cerrar la puerta, el cableado, la cantonera, el gato hidráulico o neumático para cerrar la puerta o un torniquete. Esta segunda fase puede ser por medio de otro trabajo de grado.

Para la implementación de este sistema se debe tener en cuenta que si se va a cambiar el sistema biométrico por uno de tarjeta, para enrolarlo a la red del Tecnológico, que viene desde la entrada peatonal del cerro el volador, se puede hacer siempre y cuando el lector de tarjeta tenga el sistema wigan y las tarjetas sean HID.

A continuación se relaciona los elementos y los precios al día de hoy para facilitar el proceso del montaje partiendo de una investigación sólida y veraz.

Tabla 4. Elementos para controlar puertas

Elementos para controlar puertas ITEM	**Cantidad**	**Descripción**	**Valor Unitario**	**Valor Total**
1	1	Suministro e instalación Electroimán	$400.000	$400.000
2	1	Soporte en U o Z-L	$140.000	$140.000
3	1	Suministro e instalación Fuente para electro imán de 5 AMP	$210.000	$210.000
4	1	Metro Instalado UTP	$2.420	$2.420
5	1	Metro	$1.750	$1.750

		instalado Cable dúplex 2 x 18		
6	1	Botón de salida tipo hongo (instalado)	$80.000	$80.000

Tomado de Internet. Mayo de 2013. www.homoni.com

9. BIBLIOGRAFIA

ESPINOSA DURÓ, Virginia. Evaluación de Sistemas de Reconocimiento Biométrico. Barcelona: Escuela Universitaria Politécnica de Mataro, 2004.

VILLALBA, Alejandro, ARTACHO, Juan Manuel, SANCHEZ, Diego, BERNUÉS, Emiliano. Autenticuz: Sistema de reconocimiento para control de acceso automático. Zaragoza: Universidad de Zaragoza, 2004.

TAPIADOR, Marino, PIZARRO Juan S. Tecnologías biométricas aplicadas a la seguridad pág. 201-219.

10. CIBERGRAFIA

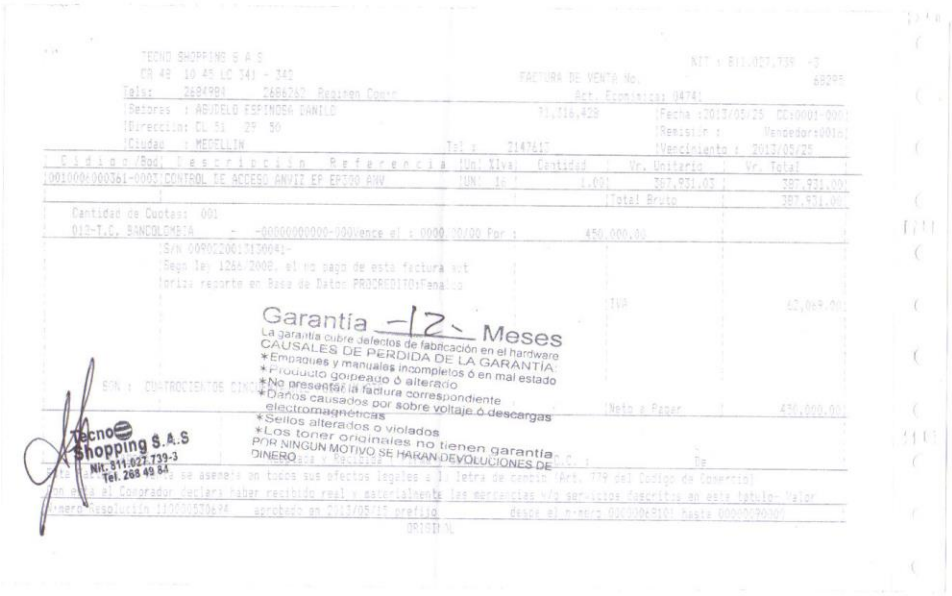
SISTEMAS DIGITALES DE SEGURIDAD. http// www.sistemasdeseguridad.com.mx (citado en 7 de abril de 2013)

SAB. Controles de acceso (en línea). http// www.sabiometria.net (citado en 6 de abril de 2013)

ICONTEC. Normas técnicas para trabajos escritos (en línea). http// www.icontec.com (citado en febrero 22 de 2013).

ANEXOS

Anexo 1. Factura


TECNO SHOPPING S.A.S

CR 43 10 45 LC 141 - 142

Tels: 2684994 2686742 Regimen Comun

FACTURA DE VENTA No.

Act. Economicas: 0474

NIT : 811.027.739 -3

Señores : ASUDELO FERNANDEZ DANILO

71.316.429

Fecha :2017/05/25 CC:0001-0001

Direccion: CL 51 29 50

Remision : Vendedor:001

Ciudad : MEDELLIN

Tel : 2147617

Vencimiento : 2017/05/25

Clasif/Bod	Descripcion	Referencia	Und	Niva	Cantidad	Vr. Unitario	Vr. Total
1001000:000361-0001	CONTROL DE ACCESO ANVIZ EP EP700 AW		UNI	16	1.00	387.931,03	387.931,00
						Total Bruto	387.931,00

Cantidad de Cuotas: 001

012-T.C. BANCOLOMBIA - -00000000000-000Vence el : 0000/00/00 Por : 450.000,00

S/N:0090C2001713004|-

Segu la: 1266/2000, el no pago de esta factura ant

toriza reporte en Base de Datos PROCREDITOsFana

IVA 62.069,00

Garantia 12 Meses

La garantia cubre defectos de fabricación en el hardware

CAUSALES DE PERDIDA DE LA GARANTIA:

*Empaques y manuales incompletos ó en mal estado

*Producto golpeado ó alterado

*No presentar la factura correspondiente

*Daños causados por sobre voltaje ó descargas electromagneticas

*Sellos alterados o violados

*Los toner originales no tienen garantia

POR NINGUN MOTIVO SE HARAN DEVOLUCIONES DE DINERO

S/N : CONTROCIENTOS CINC

Neto a Pagar 450.000,00

Tecno Shopping S.A.S

Nit: 811.027.739-3

Tel. 268 49 84

Numero Resolucion 18000570498 aprobado en 2013/05/17 prefijo desde el numero 00000e910| hasta 00000990000

0915D %