UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

SISTEMA DE CONTROL DE ACCESO MEDIANTE RECONOCIMIENTO BIOMÉTRICO.

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO ELECTRÓNICO

PRESENTADO POR:

JOHN NEIL SEVILLANO COLINA

PROMOCIÓN
2001- II

LIMA – PERÚ
2008

SISTEMA DE CONTROL DE ACCESO MEDIANTE RECONOCIMIENTO BIOMÉTRICO

Dedico este trabajo a:

A Adriana y Camila las razones de mi vida,

A mis padres, Zoila y Juan por el amor y apoyo que siempre me dan

A mi esposa Anita por su amor, apoyo y comprensión,

Y a mis Maestros por los concejos y conocimientos impartidos.

SUMARIO

Hoy en día las instituciones y empresas incorporan como parte de las medidas de seguridad, personal que cumple las funciones de monitoreo y control del acceso hacia sus instalaciones, la motivación principal para esto es por la necesidad de reducir los riesgos relativos a la sustracción de información o valores (centros de cómputo, maquinarias, almacenes de suministros, bases de datos de información restringida, etc.) que posee la empresa, protegiéndolos tanto del personal interno como externo evitando el ingreso no autorizado a estas.

Sin embargo, estas medidas si bien permiten aliviar el problema no permiten optimizar y dinamizar los procedimientos de control. Los sistemas de control de acceso electrónico, son una respuesta a esta necesidad ya que se presentan como una herramienta que el personal de seguridad y monitoreo puede utilizar para automatizar y optimizar su funciones y establecer reglas y procedimientos que permitan incrementar la seguridad y control del acceso a los ambientes y la protección de los recursos de la empresa.

El presente estudio realiza el análisis de los principales componentes de un sistema de control de acceso y de las configuraciones y arquitecturas que existen actualmente en el mercado. Así mismo se ha realizado un estudio profundo sobre la tecnología biométrica de reconocimiento de huellas, finalmente en base al análisis realizado se plantea la solución de control de acceso biométrico, que incluye la arquitectura de control de acceso, con sus respectivos componentes.

CONTENIDO

PRÓLOGO

Actualmente la protección de los recursos de las empresas e instituciones ha llevado a que estas busquen formas de controlar y restringir el acceso a los mismos por parte de su personal como de usuarios externos. Esto es motivado por la necesidad de reducir los riesgos relativos a la sustracción de estos recursos. Generalmente estos recursos corresponde a información y/o valores cuya perdida o robo puede comprometer el desempeño y normal funcionamiento de la empresa.

El presente informe tiene como objetivo realizar un estudio de un Sistema de Control de Acceso Electrónico mediante Reconocimiento Biométrico, comparando y evaluando las principales tecnologías biométricas, para determinar las consideraciones necesarias para su implementación, las cuales permitirán una toma de decisión para la implementación de control de acceso biométrico que mejor se adapte a las necesidades de la empresa o institución donde se implemente.

El informe abarca el análisis de las principales tecnologías biométricas de mayor uso y aplicación práctica en la actualidad (huellas dactilares, iris, rostro, geometría de la mano).

El informe de suficiencia se divide en los siguientes capítulos:

En el primer capitulo, se describe el planteamiento del problema donde se indica la razón para la implementación de un sistema de control de acceso, así como los objetivos y limitaciones del estudio. En el segundo capitulo se realiza una descripción de la teoría relacionada a los sistemas de control de acceso electrónico, sus principales componentes y arquitecturas. En el tercer capitulo se describen las estructura y características de los sistemas biométricos actuales, los principios en los cuales se basan. El cuarto capitulo describe en detalle el sistema de reconocimiento de huellas. El quinto capitulo detalla la propuesta de solución donde se identifica a los usuarios del sistema, describe los requerimientos del sistema, analiza las alternativas de solución, y plantea la solución la cual incluye el equipamiento necesario y los costos involucrados. En el sexto capitulo se incluyen las conclusiones y recomendaciones del presente informe.

CAPITULO I
PLANTEAMIENTO DEL PROBLEMA

1.1. descripción del problema

Con la creciente demanda por controlar el acceso y realizar el seguimiento de los individuos, hacia adentro, hacia afuera o dentro de las áreas restringidas y oficinas en los locales de las empresas e instituciones, se hace cada vez más necesario el contar con sistemas electrónicos que respondan de manera optima a las necesidades de aseguramiento y control físico que se requiere. Los accesos no autorizados a las áreas restringidas pueden provocar pérdidas o daños significativos, ya que generalmente estas áreas restringidas contienen los activos de la empresa (información, centros de cómputo, maquinarias, almacenes de suministros, valores monetarios, etc.).

Un sistema de control de acceso electrónico por biometría permite satisfacer la demanda de seguridad y control que las empresas e instituciones requieren hoy en día. La naturaleza biométrica del control de acceso permite aprovechar una característica única de cada individuo existente en todos los seres humanos, para que en base a su tratamiento restrinja o conceda el acceso hacia las instalaciones criticas.

Los ambientes que se indican a continuación, corresponden a la sede administrativa en donde se maneja información o valores, cuyo daño, adulteración o uso indebido, puede afectar el normal desempeño de sus funciones o desvirtuar la confianza depositada en la Institución por parte de los usuarios a quienes se brinda un servicio:

- Archivo Central del 1º piso,
- Centro de Cómputo y oficinas de Informática, en el 2º piso,
- Ambientes del 3º piso, donde funcionan oficinas de Tesorería, Caja, y ambientes de archivo de documentos concernientes a procesos de adquisición, contratos y transacciones comerciales, realizados por la Institución,
- Oficinas de la Alta Dirección, en el 4º piso.

Actualmente, la circulación de personas hacia los ambientes descritos, denominados críticos, es supervisada por personal de vigilancia, que se encuentran ubicados en la sala recepción de cada piso. Las puertas de los ascensores y escalera permiten a las personas que transitan acceder a estas salas, pues es paso obligado para llegar a los ambientes.

Los ingresos del personal o de visitantes hacia los ambientes críticos, se realiza a través de puertas de madera, que los conectan con el hall del piso referido, excepto el caso de la Alta Dirección, cuyas puertas de ingreso la conectan con otros ambientes reservados. Durante el horario de labores, las puertas de ingreso son de apertura libre, sin cerrojos ni llaves, y los ingresos o salidas son registrados por personal de vigilancia ubicados en los pisos 2º, 3º y 4º; en el 1º piso no existe tal registro. Lo descrito se desarrolla hasta que se todo el personal que labora se haya retirado de las oficinas del piso correspondiente, luego de lo cual estas son cerradas con cerrojo, hasta el día siguiente en que son abiertas por el personal de limpieza, antes del inicio del horario de labores. El personal de limpieza posee duplicado de las llaves.

El Centro de Cómputo ubicado en el 2º piso funciona las 24 horas del día, con un operador por turno. Además, el personal de vigilancia ubicada en la sala de recepción del piso 1º, 2º y 3º, también cumple con un servicio de 24 horas. En el caso de la sala de recepción del piso 4º, el servicio de vigilancia, se retira a las 8 p.m., y se reinicia al día siguiente, a las 7 a.m.

Después del cierre de las puertas, al término de las labores, sólo se permite ingreso al personal que ha sido previamente autorizado por la unidad orgánica correspondiente. Para ello es necesario coordinar la apertura de puertas con el personal de monitoreo de Seguridad ubicado en el piso 11º. Este personal labora las 24 horas del día, y es el depositario de las llaves de todos los ambientes del local.

De la situación descrita permite encontrar las posibles fuentes de intrusión o vulneración a la información reservada:

- Personal que labora en los ambientes críticos, durante su acceso autorizado.
- Personal que laborando en otras áreas accede eventualmente a las áreas críticas.
- Personal de vigilancia estacionado en sala de recepción de piso, durante horas de la noche o madrugada, cuando todo el personal se ha retirado.
- Personal de limpieza, durante sus horas de trabajo previas al inicio de labores de oficina.
- Personal monitoreador de Seguridad que labora en piso 11º, durante horas de la noche o madrugada, cuando todo el personal se ha retirado.
- Personas visitantes, durante el tiempo que permanecen en el local.

Las principales condiciones que propician el accionar de personas con fines no autorizados o de intrusión, son:

- La ausencia de barrera física al tránsito de las personas hacia los ambientes críticos.
- La baja confiabilidad del registro manual de tránsito de personas, que representa poca efectividad en el establecimiento de procedimientos de mantenimiento de la seguridad.
- La ausencia de medios para establecer controles a las acciones del personal que accede de forma rutinaria a los ambientes críticos.

El control y asignación de la hora de inicio y término del permiso para permanecer en los ambientes, es una de las funcionalidades necesarias, lo cual no es posible de realizar con el grupo de trabajos de limpieza, que posee llaves de las puertas de ingreso.

Como procedimiento de seguridad se realiza el registro de las personas visitantes en el sistema de Control de Visitas. Esta aplicación alimenta la Base de Datos de información de visitantes. El sistema registra el ingreso al local, no registra eventos relativos al visitante durante su presencia en el local, salvo al momento de retirarse, en que el encargado de recepción registra la hora. Tampoco provee facilidades para la toma de acción por parte del personal de las diversas unidades orgánicas, respecto al mantenimiento de la seguridad.

1.2. objetivos del trabajo

- Realizar la descripción de los Sistemas de control de acceso electrónico así como de las tecnologías biométricas utilizadas para su implementación.
- Determinar las consideraciones a tomar en cuenta para realizar el diseño y la implementación de un sistema de control de acceso físico basado en biometría.
- Descripción de los Sistemas de control de acceso y descripción y comparación de las tecnologías biométricas.
- Determinar las consideraciones a tomar en cuenta para realizar el diseño y la implementación de un sistema de control de acceso físico basado en biometría.

1.3. limitaciones del trabajo

El presente Informe solo abarca el análisis de las principales tecnologías biométricas (huellas dactilares, geometría de la mano, rostro e iris) de mayor uso y aplicación práctica en la actualidad.

CAPITULO II
SISTEMA DE CONTROL DE ACCESO

2.1. definición

El control de Acceso es mecanismo que permite que solo las personas autorizadas puedan acceder a los locales o áreas restringidas.

Un Sistema de Control de Acceso es un sistema electrónico-electromecánico que permite controlar el acceso de las personas, identificándolos, y en base a los permisos asociados a estos, les concede o niega el acceso hacia una instalación u oficina. Este sistema registra las entradas, salidas y realiza el monitoreo de las personas que transitan por las instalaciones controladas, de esta forma permite conocer a donde ingresan, quienes ingresan, a que hora lo hacen, por cuanto tiempo, así como los intentos de acceso de cada individuo que interactúa con el sistema. Esto permite a la unidad encargada de la seguridad tomar respuesta cuando fuera necesario.

Para ello es necesario establecer una supervisión o monitoreo centralizado del funcionamiento del sistema de Control de Acceso instalado.

El acceso a cualquier recinto puede ser una función del nivel de autorización que posee, de la fecha y rango de hora, o una combinación de ambos criterios.

Los sistemas de control de acceso requieren de esquemas de reconocimiento personal para determinar o confirmar la identidad de un individuo [34]. El propósito de tales esquemas es asegurar que en base a la identidad verificada, el sistema conceda a este individuo los permisos de acceso y no a cualquier otro

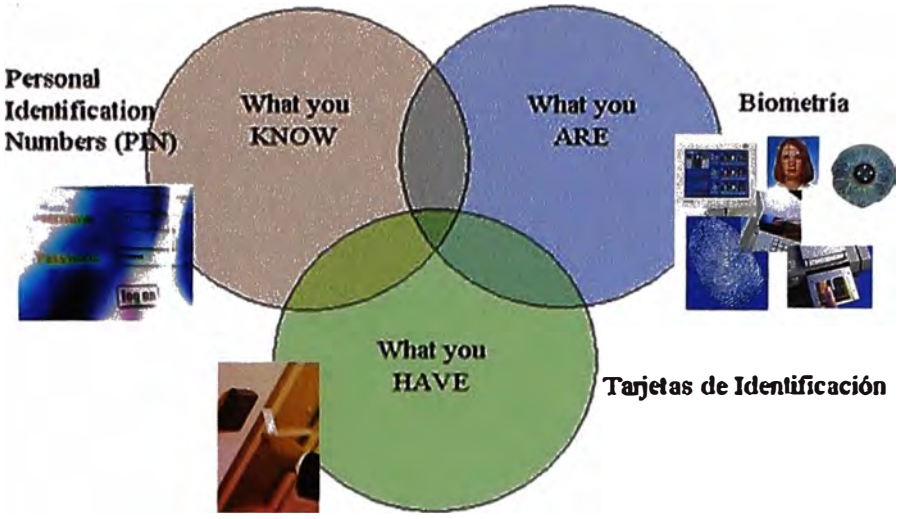


Fig.2.1 Tecnologías. de Identificación[43]

En general hay 3 métodos para verificar la identidad de un individuo. Indicadas en orden del más seguro y conveniente al menos seguro tenemos [16]:

- Algo que tú eres – una biometría.
- Algo que conoces - PIN, password, códigos.
- Algo que tienes – llave, token, tarjeta.

La identificación de los usuarios que acceden a los recintos controlados puede basarse en cualquiera de los métodos mencionados anteriormente o una combinación de tales técnicas.

Los ambientes de alta seguridad son supervisados por un centro de Monitoreo, con el propósito de propiciar rápida respuesta del personal de seguridad, en caso de violación de los procedimientos establecidos. Las áreas menos seguras pueden ser también monitoreadas, o en su defecto los eventos relacionados con la operación de las puertas pueden ser simplemente almacenados para su revisión posterior y auditoria, por parte del personal responsable.

La violación de procedimientos, no necesariamente indica la producción de actos que causan pérdida a la Institución, pero sí la existencia de situaciones en que la ocurrencia de tal pérdida es altamente probable.

El Sistema de Control de Acceso puede entenderse como una herramienta que ayuda a corregir prácticas inseguras, mediante la detección inmediata de ellas, y su reporte al área de supervisión.

Para un uso efectivo del control de acceso, es necesario que tanto el personal de monitoreo, como los equipos o componentes del Sistema electrónico-electromecánico funcionen de manera optima, para prevenir la intrusión de personas que pudieran hacer

uso de las facilidades, documentos o valores disponibles, causando perjuicio a la Institución. Cualquiera de ellos, por sí solo, no lograría resultados efectivos.

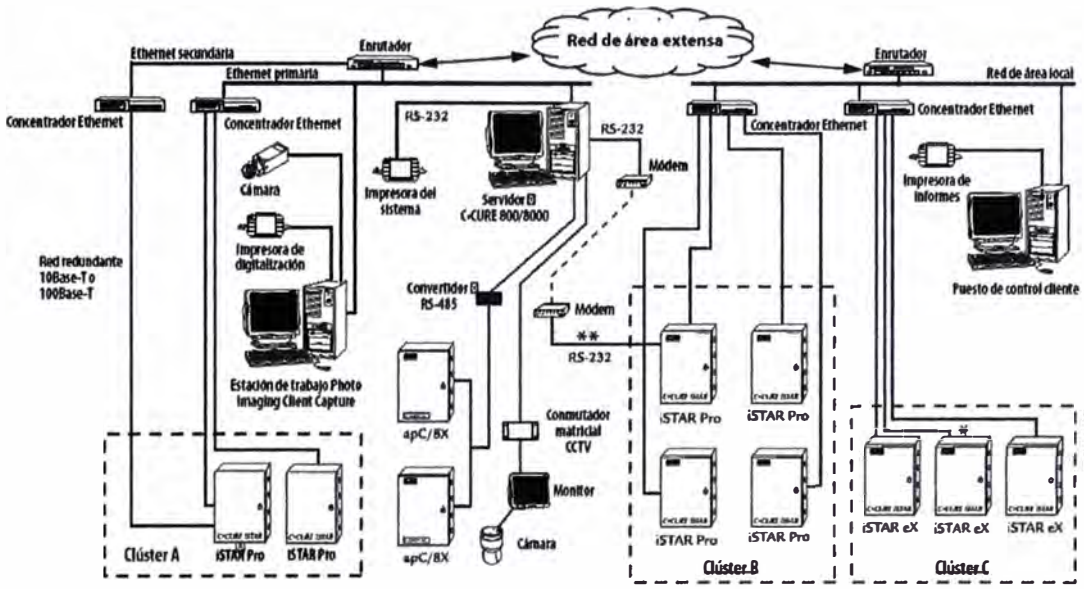


Fig.2.2 Sistema de Control de Acceso. De la figura se puede apreciar las configuraciones y formas de conexión de los distintos componentes del Sistema: con control redundante, conexión por modem o red Lan comunicados por enlace Wan para control de oficinas en sitios remotos [71].

2.2. descripción de un sistema de control de acceso

El sistema de Control de Acceso, se basa en la operación de hardware controlador, instalado cercanamente a las puertas protegidas. En ellos se almacenan datos relativos a los permisos para apertura de puertas. El sistema se basa además en la programación de códigos de identificación a las tarjetas portadas por los usuarios o permisos establecidos, para un individuo en base a la comparación de su muestra biométrica. Cuando el usuario presenta su tarjeta al lector de una puerta o cuando se identifica a través de su biometría, el sistema detecta el código programado que porta y lo transmite al hardware controlador cercano, donde se determina si procede o no la apertura, conforme a la información de permisos, previamente configurada. Luego el controlador emite los comandos respectivos a los dispositivos de cierre de la puerta, y detecta las señales generadas por otros dispositivos indicadores de status de posición de la puerta.

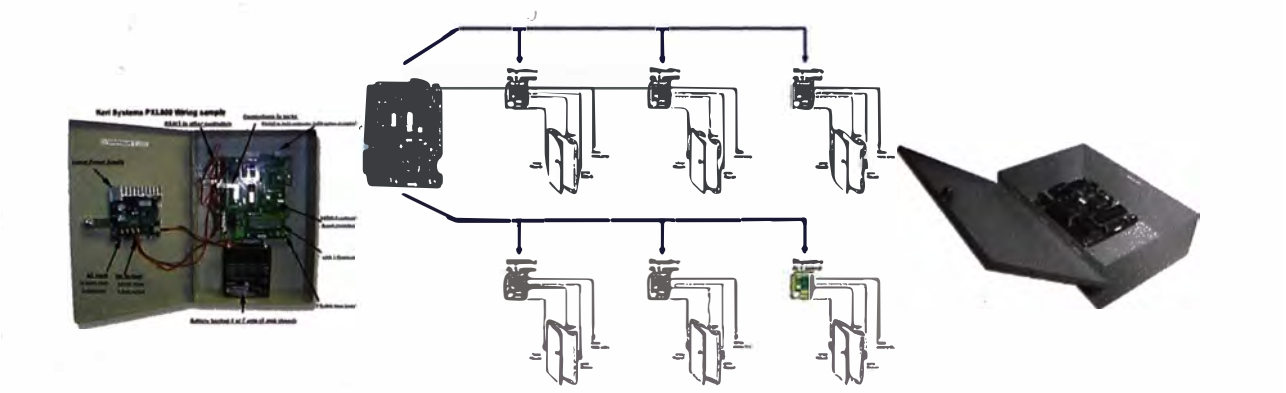


Fig.2.3 Sistema de Control de Acceso. Controlador principal y paneles controladores distribuidos [75,71]

A continuación se describen los principales componentes de un Sistema de Control de Acceso.

2.3. módulos controladores

La operación de un Sistema de Control de Acceso se basa fundamentalmente en una conformación de dispositivos de hardware llamados Módulos Controladores o Paneles Controladores. Estos se distribuyen en sitios del local, algunos de ellos cercanos a las puertas que están bajo su control, otros cercanos al ambiente donde funciona el servidor de Administración del sistema, y otros pueden estar en posición intermedia. A continuación se describen las funciones genéricas realizadas por estos dispositivos:

- Almacenar en memoria local los permisos de acceso vigentes para cada código de usuario,
- Recibir el código de usuario capturado por el lector de tarjetas bajo su control, cada vez que un usuario se registra para acceso en la puerta asociada.
- Acceder a memoria local y determinar si para el código recibido procede aceptación o denegación de acceso en la puerta correspondiente,
- Producir respuesta de datos al lector de tarjeta y de ser procedente emitir las señales eléctricas hacia los dispositivos que intervienen en la apertura de puerta.
- Recibir señales de status de funcionamiento y emitir señales eléctricas para la actuación, de diversos dispositivos auxiliares como detector de puerta abierta/cerrada, inhibidor de apertura, pulsador de apertura de emergencia, luz de advertencia, zumbador, etc.

La capacidad de los Módulos controladores está relacionada principalmente con la cantidad de dispositivos periféricos que pueden controlar (lectores, cerraduras, detectores de presencia - REX). Su capacidad de procesamiento está referido a la cantidad de

usuarios con o sin permiso de acceso, la cantidad de eventos que puede almacenar en memoria, el soporte a funcionalidad "anti passback", es decir que pueda rechazar el ingreso mediante tarjeta que fuera presentada previamente, sin haber registrado salida.

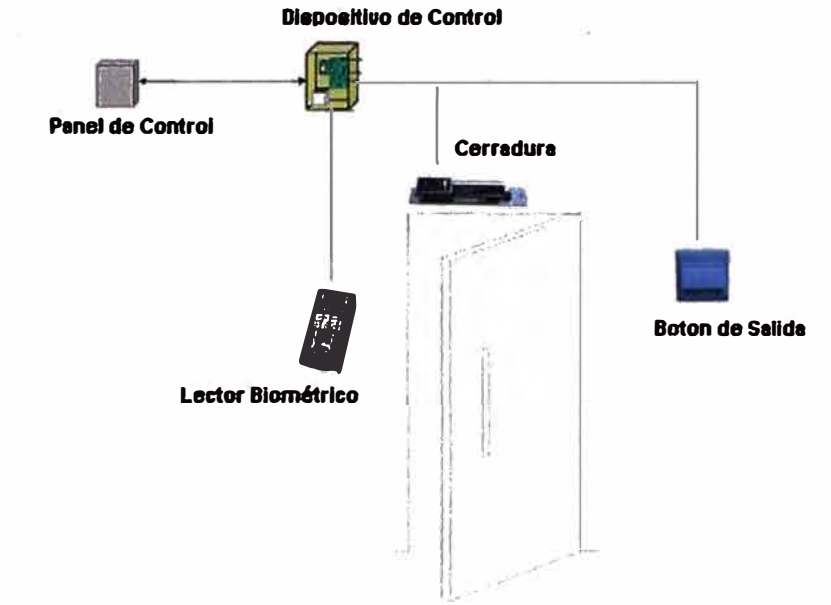


Fig.2.4 Sistema de Control de Acceso. Dispositivo controlador distribuido y elementos a controlar [75].

Según el nivel de procesamiento de información se puede identificar tres tipos de módulos controladores, presentes en cualquier Sistema de Control de Acceso, Un módulo que podemos denominar de primer nivel, se encarga de la definición de estados de operación de las puertas, relacionados con las señales de supervisión generadas por dispositivos detectores y con la emisión de comandos para la actuación de los dispositivos que intervienen en la apertura de puertas. Los módulos de primer nivel constituyen hardware de tres tipos: Módulo de entradas (IM), Módulo de Salidas (OM) y Módulo de Interfaz para Lector de Tarjetas (RI).

Estos módulos pueden estar integrados en un solo gabinete asociado al control de una puerta, o de varias puertas correspondientes a un área o piso del local.

Un tipo de módulo Controlador, denominado de Segundo nivel, más elevado en complejidad de procesamiento, que el primero, se encarga del almacenamiento en memoria no volátil, de información relativa a los códigos de identificación de usuarios y sus permisos asignados para cada puerta del Sistema. Los módulos IM, OM y RI, del primer nivel anterior, transfieren hacia este módulo de segundo nivel, los datos que definen los estados de operación de las puertas, así como los códigos detectados por los lectores de tarjetas. En este nivel, se procesa la información recibida, y se emiten los comandos correspondientes hacia los módulos de primer nivel, para permitir o denegar la

apertura de puertas, y se almacenan los datos relativos a los eventos de apertura relacionados a los códigos de identificación detectados en los lectores de tarjetas. A este módulo se le denomina Controlador Inteligente de Sistema (ISC), y tiene también la función de establecer comunicación con el servidor Administrador del Sistema, para que éste actualice su base de datos.

El módulo Controlador de tercer nivel, consiste en el servidor de cómputo donde se ejecuta Software Administrador del Sistema de Control de Acceso. Este realiza transferencias de información hacia y de el nivel ISC anterior descrito, y posee todos los atributos de una aplicación cliente servidor que funciona asociada a una Base de datos, que es también parte de este tercer nivel. Esta aplicación toma en cuenta todos los aspectos de procedimientos de seguridad, que pueden ser influenciados por los eventos y parámetros detectados o comandados por los dos niveles inferiores descritos. Mediante este software, se configuran las modalidades de actuación de los dispositivos controladores, se asignan los permisos a los portadores de tarjetas, permite al administrador realizar cambios inmediatos en la operación de las puertas, se producen reportes de administración relativos al flujo o permanencia de personas, seguimiento de ruta de personas, análisis de eventos, de acuerdo a diversas criterios de búsqueda: por fecha, hora, puerta, persona, etc. Este módulo de tercer nivel, esta más relacionado a la implementación de un Sistema Informático de la Seguridad. Adicionalmente, para el acceso al Sistema de Administración, se usan estaciones de trabajo que pueden acceder mediante aplicaciones cliente-servidor, desde cualquier punto de la red Ethernet del local.

2.4. lector de tarjeta

Es el dispositivo hardware que detecta el código de usuario (identidad del portador), que está almacenado en la tarjeta de identificación aplicada en el Sistema. El código detectado es transmitido como requerimiento de acceso hacia los Módulos Controladores

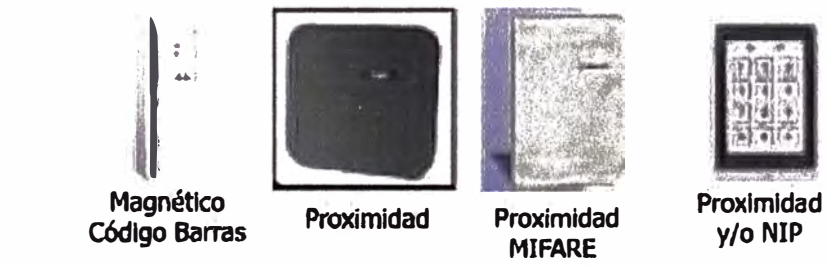


Fig.2.5 Sistema de Control de Acceso. Dispositivo lector de tarjeta [75].

En el caso de la identificación por tarjeta, la propiedad física aplicada en la grabación y detección del código, define el tipo de lector de tarjeta, la que puede ser: óptica, magnética, por transmisión radioeléctrica, por contacto eléctrico a un circuito integrado (chip). El método mayormente aplicado, por su seguridad contra duplicación, simplicidad en el manipuleo y rapidez de lectura, es el de transmisión radioeléctrica. A las tarjetas y lectores que usan este método se les refiere con el adjetivo "de proximidad", pues basta presentar la tarjeta a distancia del orden de 10 cm. del lector, para efectivizar la lectura.
El lector de proximidad emite señal de radiofrecuencia, que induce corriente en un conductor en forma de bucle, que está incorporado en el material plástico de la tarjeta. De esa manera la tarjeta refleja la señal, modulada con el código de usuario que se encuentra almacenado en un circuito también embutido en la tarjeta. La señal reflejada es a su vez captada por el lector, para su decodificación, y transmisión al módulo Controlador asociado.
Los datos concernientes a la tarjeta, son transmitidos por el lector hacia los módulos Controladores, codificados en un formato seleccionado entre varios posibles, siendo el denominado "Wiegand" el mayormente aceptado por los fabricantes de lectores o de sistemas de control de Acceso.

2.5. lector biométrico

Es el dispositivo hardware que determina el código de usuario correspondiente a la huella dactilar presentada, en base a la disposición de características esenciales de la huella dactilar del usuario (minucias). El código determinado es transmitido como requerimiento de acceso hacia los Módulos Controladores

Fig.2.6 Sistema de Control de Acceso. Dispositivo lector de huella, Iris y Mano, Rostro [78,79,80,81].

En el caso de la identificación por huella dactilar, el lector realiza escaneo de la conformación de líneas en la huella del usuario, para obtener una caracterización resumida de su geometría, en base a su contenido de "minucias". Tal contenido se

representa en un código binario, llamado "plantilla", cuyo tamaño es del orden de 300 bytes o mayor. La plantilla no es información procesable por el Sistema de Control de Acceso, por lo que debe traducirse el código de plantilla detectado en el lector, al código de usuario manejado por los módulos Controladores. Una manera de lograrlo, es estableciendo conexión entre el lector de huella y un computador donde corre una aplicación que maneja tabla de equivalencia plantilla vs. Código de usuario, de donde se obtendrá este último, para seguidamente transmitirlo al módulo controlador asociado. En otra modalidad de operación, el lector de huella posee un teclado, en el cual el usuario debe introducir una contraseña, la cual previamente se ha almacenado en memoria, estableciendo su equivalencia, con la plantilla y el código de usuario. El lector en este caso, verifica si la plantilla obtenida de la huella corresponde a la contraseña introducida, y de ser así transmitirá el código de usuario hacia el módulo controlador asociado.

La identificación por huella dactilar es el método comúnmente aceptado como el de mayor seguridad, pues depende de una cualidad física que es única para cada usuario, y que no puede ser suplantada o usada sin la presencia de la persona en sí especto a falsificaciones. Sin embargo, la necesidad de soporte informático para funcionamiento del lector de huella dactilar, hace que su operación se vea afectada por fallas técnicas que pueden ocurrir tanto en la red LAN aplicada para su conexión, como en el propio computador externo donde se debe procesar la aplicación para obtención del código de usuario. Por otro lado, con la modalidad de introducción de código vía teclado, se introduce cierta complejidad y demora a la actuación del usuario, que provoca incomodidad, sobretodo cuando el personal debe realizar accesos muy frecuentes.

Las razones expuestas hacen que la aplicación de lectores de huella dactilar, se utilicen mayormente en operaciones de alta seguridad, y donde la circulación del personal es muy reservada y se realiza bajo estrictos procedimientos.

2.6. cerradura electromagnética

Consiste en electroimán cuyas piezas se instalan en el marco de la puerta, de modo de asegurarla mediante la atracción magnética, inducida por corriente eléctrica mantenida en su magneto, proveniente del módulo Controlador instalado cercanamente.

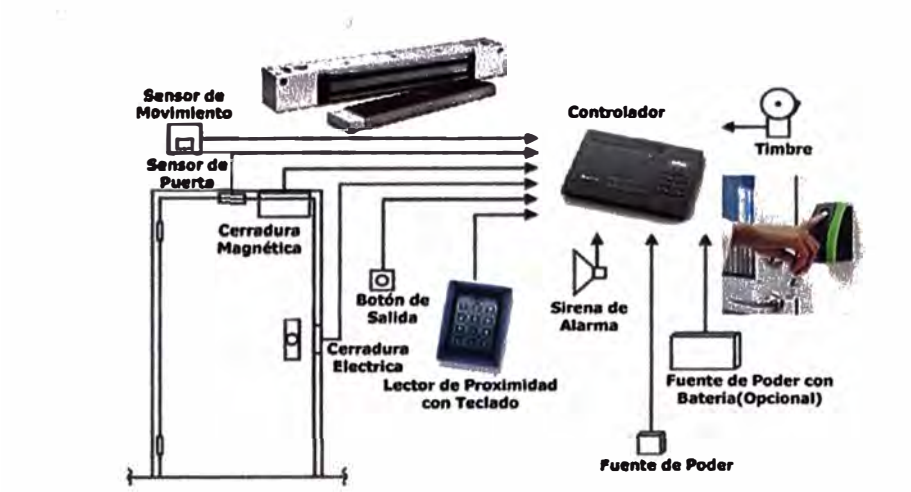


Fig.2.7 Cerradura Electromagnética, Instalación e interacción en el Sistema de Control de Acceso[75].

La cerradura electromagnética es un elemento de alta confiabilidad, que no usa piezas móviles, y por lo tanto no requiere de lubricación o mantenimiento. La cerradura se mantiene cerrada mientras se aplica alimentación de energía a su magneto, y se abre cuando se le retira, de manera que cumple con la norma de seguridad que exige la apertura de puertas en caso de corte de energía. Se fabrican para producir fuerza de retensión en amplio rango, siendo el valor de 600 libras el recomendado para puertas de oficinas. Por otro lado su reducido consumo de energía, del orden de 5watts, permite el mantenimiento de puerta cerrada, durante prolongado tiempo de alimentación por fuente de energía de respaldo, como batería electrolítica de baja capacidad.

2.7. accesorios de soporte a la apertura de puerta

Comprenden dispositivos que no intervienen en el proceso automático de apertura, pero que sirven para asegurar correcto funcionamiento de ella, o producen señales de supervisión hacia el módulo controlador, para que éste, de acuerdo a su programación produzca señalización o registro en el Sistema de Administración. Estos accesorios pueden comprender:

2.7.1 detección de presencia por luz infrarroja (rex):

Se instala en el lado de batimiento de la puerta, sobre su marco superior, y cumple la función de inhibir momentáneamente su apertura, desde el otro lado, cuando se detecta presencia de persona bajo su rango de detección óptico. Con ello se evitan posibles accidentes ocasionados por impacto de la puerta sobre personas posicionadas en su área de batimiento.

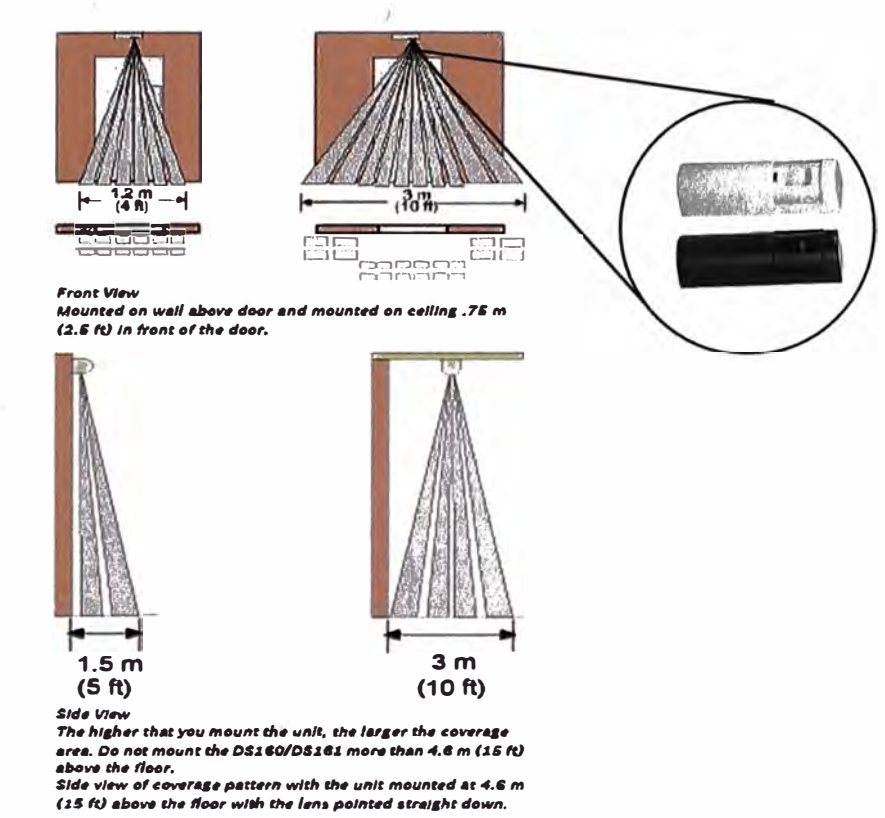


Fig.2.8 Detector de presencia por Luz Infrarroja (REX).[84]

2.7.2 pulsador de salida

Permite la salida de un ambiente protegido, mediante señalización hacia el controlador, para comandar la apertura de puerta, en caso no se disponga de tarjeta durante una emergencia.

Fig.2.9 Pulsador de salida[84]

2.7.3 sensor de puerta abierta

Detecta el estado de puerta abierta y lo señaliza hacia el módulo Controlador, para que éste finalice el proceso de apertura o reporte situación riesgosa hacia la administración del sistema, de acuerdo a su programación.

Fig.2.10 Sensor de puerta abierta[84]

2.7.4 cierrapuerta hidráulico

Mecanismo compuesto de resorte y amortiguador hidráulico, que se instala en el dintel de la puerta, cercano a su eje de giro. En condición de puerta abierta, el cierrapuerta ejerce fuerza sobre la hoja de la puerta, para retornarla a la posición de cerrada.

Fig.2.11 Cierra puerta hidráulico[88]

2.8. software de administración

Programa principal residente en hardware servidor, que se conecta vía red de computadoras LAN con los módulos Controladores de puertas. El software permite cargar en ellos los datos de configuración de permisos asignados a los portadores de tarjetas, por cada puerta y en rangos de horas o días. Asimismo, registra los eventos comunicados por los controladores, relativos a ingresos, salidas o intrusiones, asociados a las personas identificadas en los accesos.

El software mantiene una base de datos de toda la información ingresada al sistema, tanto la que define los parámetros de funcionamiento, como la que describe los accesos realizados. Provee además una interfaz gráfica de usuario para que el Administrador interactúe con él, a través de computadora personal conectada en red LAN, y presenta reportes de status del Sistema en respuesta a programas ejecutables invocados a elección por el Administrador.

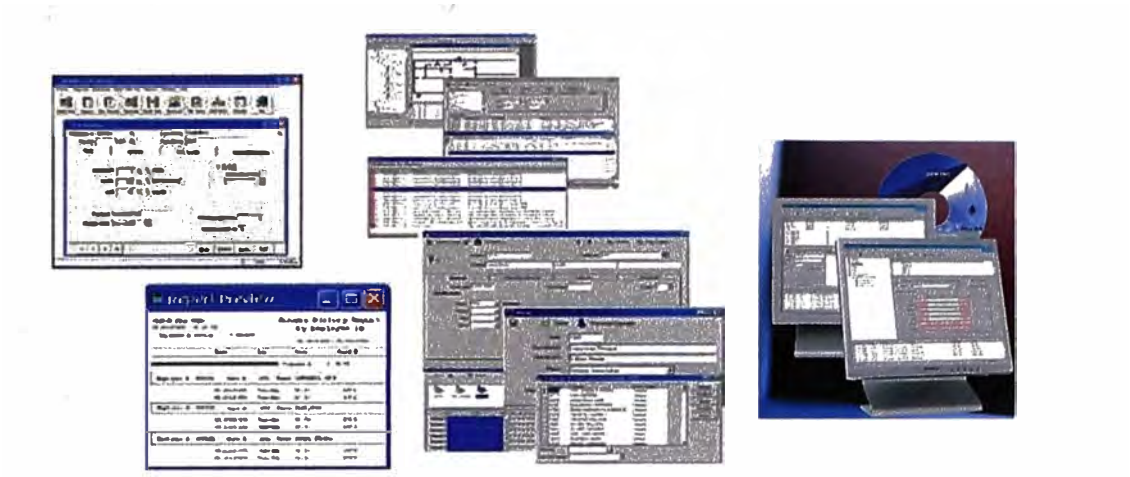


Fig.2.12 Software de Administración.[71,75]

2.9. arquitectura de un sistema de control de acceso

El concepto de arquitectura se aplica a la disposición espacial que tienen los tres módulos controladores descritos, que procesan información relativa a la apertura de puertas. Pueden distinguirse tres tipos de arquitectura que ofrece la tecnología actual de Sistemas de Control de Acceso: Aislada (*"stand alone"*), Distribuida y la arquitectura Integrada.

2.9.1 arquitectura aislada (stand alone)

En la arquitectura Aislada, los Módulos controladores de primer y segundo nivel están incorporados en un solo dispositivo, el cual por lo general, es el lector de tarjetas instalado adjunto á una puerta. El componente de tercer nivel, si es usado, lo constituye un computador conectado al lector mediante interfaz RS 232 o RS 485. Esta arquitectura se aplica para controlar una sola puerta, aunque puede expandirse para abarcar un número reducido de ellas, como las confinadas en un área o piso del local. Debido a la existencia de módulo de segundo nivel en cada una de las puertas, el costo del Sistema en arquitectura Aislada se torna excesivo cuando el número de puertas excede a 4.

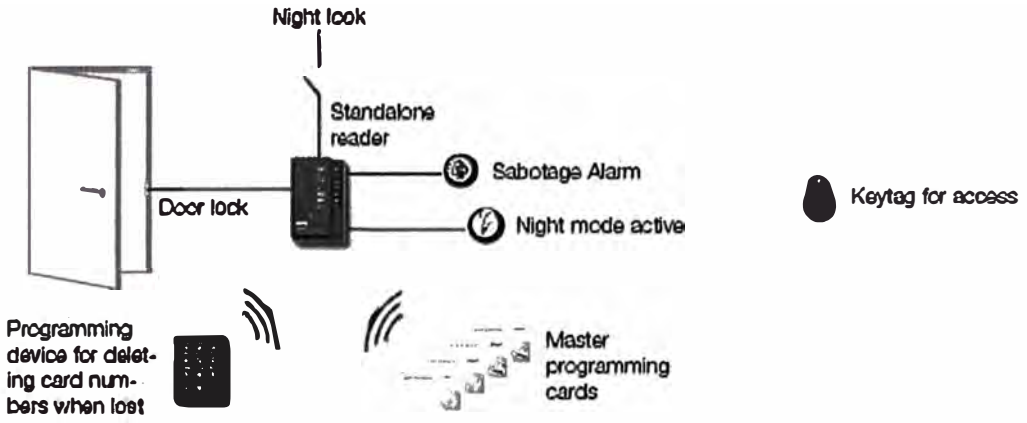


Fig.2.13 Diagrama de un Sistema de Control de Acceso Stand Alone.[36]

2.9.2 arquitectura distribuida

La arquitectura Distribuida, consiste de Paneles controladores que integran al Controlador Inteligente de Sistema ISC, y a los módulos de control de Entrada/Salida y de Interfaz para Lector de Tarjeta. Es decir que el Panel controlador contiene a los módulos de procesamiento de segundo y primer nivel descritos. Cada Panel está equipado para controlar un número limitado de puertas, que puede ser 1, 2, o 4; este número corresponde a la cantidad de puertas de un área o piso específico del local. La ubicación de cada Panel controlador de primer y segundo nivel, se elige en un punto del área o piso donde se encuentran las puertas a controlar. Varios de estos Paneles Controladores, instalados en áreas diferentes del local, se conectan en topología de bus a través de interfaz RS 422 o RS 485, hacia el módulo de tercer nivel, constituido por el servidor de Administración, el que se instala en ambiente reservado para cómputo. Alternativamente, la conexión de cada Panel con el servidor, puede realizarse por red LAN Ethernet. La cantidad de Paneles Controladores así conectados, puede ser considerable, siendo su máximo de 64.

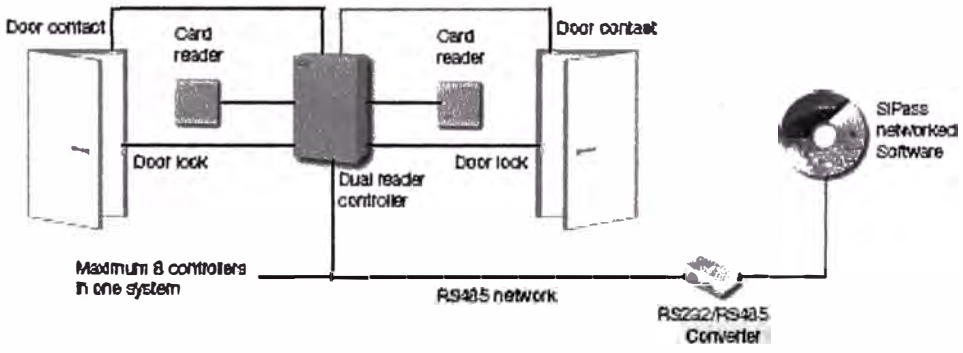


Fig.2.14 Diagrama de un Sistema de Control de Acceso de Arquitectura Distribuida.[36]

2.9.3 arquitectura integrada

En la arquitectura Integrada los módulos de primer nivel: ICM, OCM y CRIM, descritos, se instalan directamente en cada puerta a controlar, o en un punto desde donde se controla a varias puertas de un área o piso específico. Por lo general la concentración de estos módulos en un solo sitio de instalación, se limita a los necesarios para controlar 8 puertas como máximo. La cantidad de módulos de primer nivel, depende de la capacidad con que se fabrica cada módulo, la que puede ser para controlar una, dos cuatro u ocho puertas. Los módulos de primer nivel indicados, se conectan en topología de bus hacia un módulo de segundo nivel ISC, al que también se conectan otros módulos de primer nivel, instalados en sitios de concentración correspondientes a distintas áreas o pisos del local. La interfaz aplicada en el bus es generalmente RS 422 o RS 485. La ubicación del módulo de segundo nivel ISC, puede elegirse en un punto que sea aproximadamente equidistante con los módulos de primer nivel, que podría ser por ejemplo, un piso intermedio entre los varios pisos en que ellos estén instalados, de modo de limitar el recorrido de conductores aplicados en el bus, logrando con ello economía de materiales y simplicidad en la instalación y mantenimiento del sistema. La cantidad de módulos de primer nivel que se conectan a un solo módulo ISC, está determinado por la capacidad con que se fabrica este último, la que usualmente corresponde a la necesaria para controlar hasta 16 o hasta 32 puertas, (considerando lectores a la entrada y a la salida de cada puerta). Algunos productos ISC aplican varios buses en lugar de uno solo, cada uno de los cuales permite conectar proporcionalmente menor cantidad de módulos de primer nivel; implicando además, tendido de conductores independientes para cada bus. La comunicación entre el módulo de segundo nivel ISC, y el servidor de Administración del Sistema, usualmente se realiza por red LAN Ethernet, por interfaz RS 485, o por ambas.

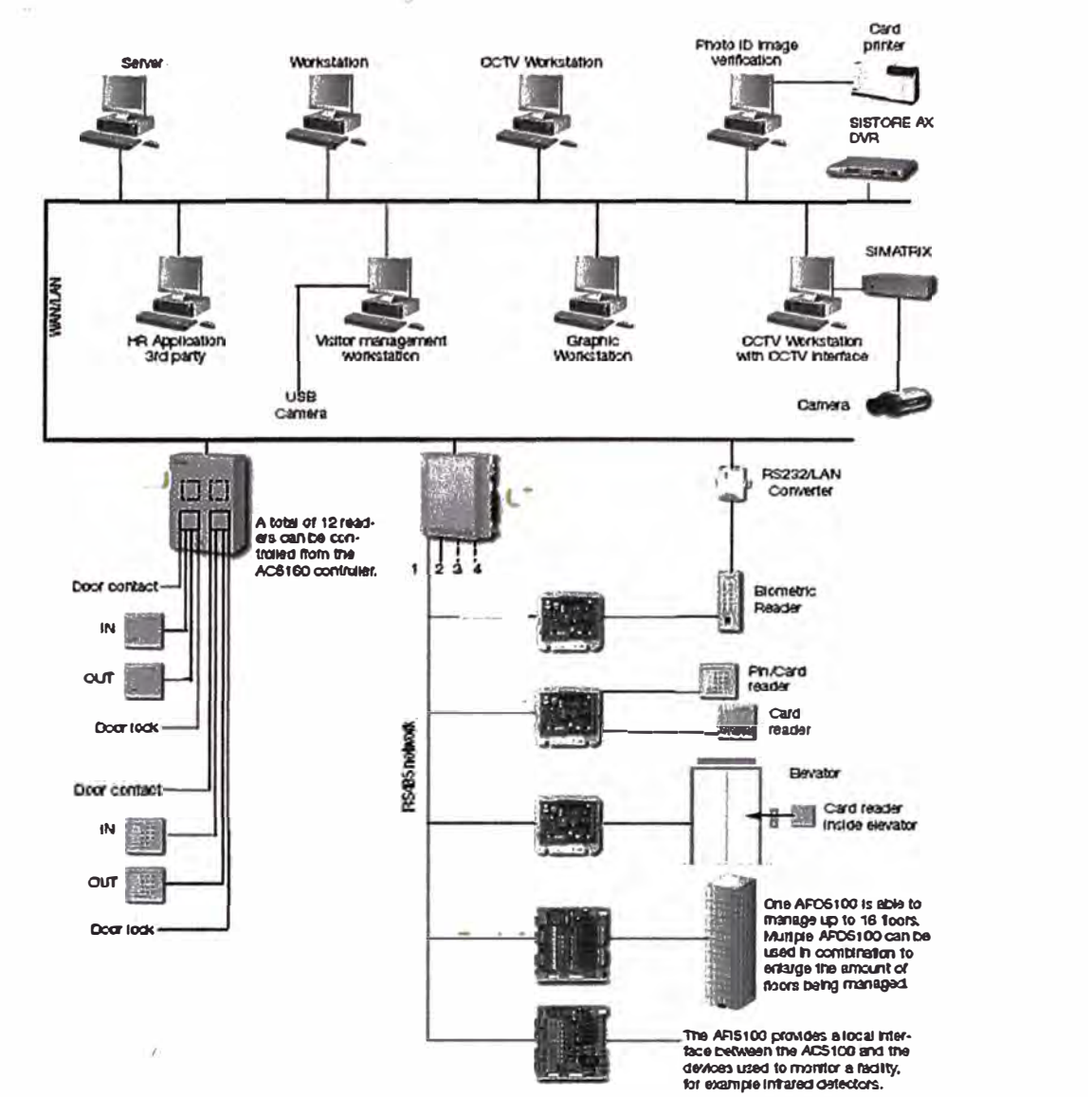


Fig.2.15 Diagrama de un Sistema de Control de Acceso de Arquitectura Integrada.[36]

CAPITULO III
TECNOLOGÍAS BIOMÉTRICAS

3.1 definición

Biometría es un término general usado alternativamente para describir una característica o un proceso.

Como característica: corresponde a un parámetro biológico o comportamental, que puede ser medido y utilizado para reconocimiento automatizado de individuos. Este parámetro o característica se entiende que es única para cada individuo, por lo que puede ser utilizado para verificar la identidad de una persona [73].

Como proceso: se refiere a los métodos automatizados de reconocimiento de individuos basados en características biológicas (anatómicas o fisiológicas) y comportamentales medibles.

Entendemos por sistema biométrico a un sistema automatizado que realiza labores de biometría. Es decir, un sistema que fundamenta sus decisiones de reconocimiento mediante una característica personal que puede ser reconocida o verificada de manera automatizada.

En la actualidad estos sistemas biométricos se utilizan dentro de diversas aplicaciones una de los cuales es el control de acceso.

Fig.3.1 Ilustración que muestra las Tecnologías Biométricas existentes. [64]

3.2 elementos claves en los sistemas biométricos

- **Enrolamiento:** es el proceso de colectar las muestras biométricas de un individuo, y la subsiguiente generación de su plantilla
- **Plantillas:** La data que representa la biometría del individuo enrolado en el sistema
- **Matching o Emparejamiento:** Es el proceso de comparación entre una muestra biométrica capturada en vivo contra una o mas plantillas en la base de datos del sistema.
- **Aplicaciones:** el objetivo es la identificación automática y confiable en modo desatendido y frecuentemente remoto.

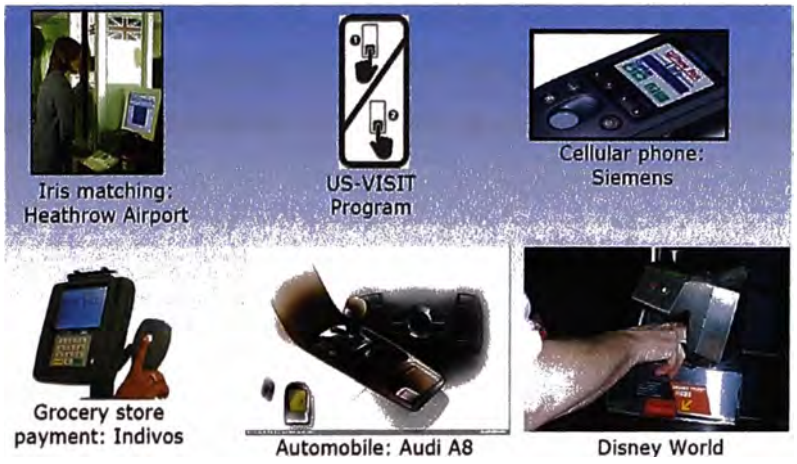


Fig.3.2 Ilustración que muestra los usos y aplicaciones de las tecnologías Biométricas.[64]

A continuación se describen algunas de las características más importantes de estos sistemas.

3.3 caracteristicas de un indicador biométrico

Un indicador biométrico es alguna característica con la cual se puede realizar la comparación biométrica y debe cumplir los siguientes requerimientos:

- **Universalidad:** el indicador o característica debe estar presente en cualquier persona.
- **Unicidad:** existe una probabilidad muy pequeña de que 2 personas posean la misma característica idénticamente.
- **Permanencia:** la característica no cambia en el tiempo.
- **Cuantificación:** la característica puede ser medida en forma cuantitativa.

Los requerimientos anteriores sirven como criterio para descartar o aprobar a alguna característica como indicador biométrico. Luego de seleccionar algún indicador que satisfaga los requerimientos antes señalados, es necesario imponer restricciones prácticas sobre el sistema que tendrá como misión recibir y procesar a estos indicadores. En el siguiente punto se presentan estas restricciones.

3.4 características de un sistema biométrico

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

- **El desempeño,** que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales. El objetivo de esta restricción es comprobar si el sistema posee una exactitud y rapidez aceptable con un requerimiento de recursos razonable.
- **La aceptabilidad,** que indica el grado en que la gente está dispuesta a aceptar un sistema biométrico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "confianza" a los mismos. Factores psicológicos pueden afectar esta última característica. Por ejemplo, el reconocimiento por escaneo de retina, que requiere un contacto cercano de la persona con el dispositivo de reconocimiento, puede desconcertar a ciertos individuos debido al exponer su ojo sin protección frente a un "aparato". Sin embargo, las características anteriores están subordinadas a la aplicación específica. En efecto, para algunas aplicaciones el efecto psicológico de utilizar un sistema basado en el reconocimiento de características oculares será positivo, debido a que este método es eficaz implicando mayor seguridad.
- **La fiabilidad,** que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, etc. Algunos sistemas incorporan métodos para determinar si la característica bajo estudio corresponde o no a la de una persona viva. Los métodos empleados son ingeniosos y usualmente más simples de lo que uno podría imaginar. Por ejemplo, un sistema basado en el reconocimiento del iris revisa patrones característicos en las manchas de éste, un sistema infrarrojo para chequear las venas de la mano

detecta flujos de sangre caliente y lectores de ultrasonido para impresiones dactilares revisan estructuras subcutáneas de los dedos.

3.5 arquitectura de un sistema biométrico

Los sistemas biométricos completos poseen cinco componentes, los que se encargan de capturar las características biométricas, transmitir las muestras biométricas, almacenarlas como imágenes y plantillas, procesarlas para generación de plantillas y emparejamiento, y un componente de toma de decisiones o motor biométrico. La arquitectura típica de un sistema biométrico se presenta en la siguiente figura.

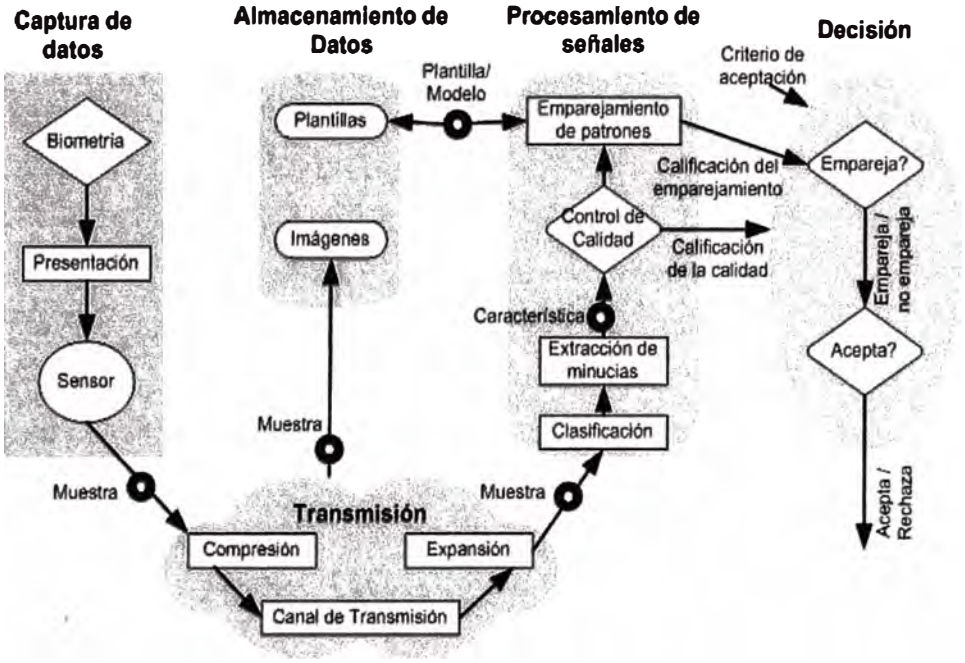


Fig.3.3 Arquitectura de un sistema biométrico para identificación personal, aquí ejemplificado con impresiones dactilares.[18]

- **Captura de Datos:** Es el proceso de adquisición análoga o digital de algún indicador biométrico de una persona, como por ejemplo, la adquisición de la imagen de una impresión dactilar mediante un escáner. La captura de datos consiste en convertir las características físicas en un formato electrónico capaz de ser transmitido electrónicamente y procesado.
- **Almacenamiento de datos:** Consiste en una base de datos donde se almacenarán las imágenes y plantillas biométricas. Debe ser segura, confiable y eficiente.
- **Procesamiento de Señales:** Este componente se encarga de procesar matemáticamente la muestra biométrica a través de algoritmos. Realiza tres funciones principales: Generar la plantilla biométrica usando un algoritmo de extracción de características biométricas, clasificar la muestra biométrica usando

un algoritmo de clasificación, y realizar el emparejamiento de plantillas biométricas entre una almacenada previamente y otra de referencia.

- **Decisión:** Este componente toma la decisión, o califica el resultado del procesamiento biométrico respecto al emparejamiento de patrones, de acuerdo a parámetros como umbral, calidad, etc. que son definidos por el usuario según el uso que se le quiera dar.

3.6 fase operacional de un sistema biométrico

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

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

Generalmente es más difícil diseñar un sistema de identificación que uno de verificación. En ambos casos es importante la exactitud de la respuesta. Sin embargo, para un sistema de identificación la rapidez también es un factor crítico. Un sistema de identificación necesita explorar toda la base de datos donde se almacenan los templates, a diferencia de un sistema verificador. De la discusión anterior resulta obvio notar que la exigencia sobre el extractor y el comparador de características es mucho mayor en el primer caso.

3.7 medidas de desempeño de un sistema biométrico

La información provista por los templates permite particionar su base de datos de acuerdo a la presencia o no de ciertos patrones particulares para cada indicador biométrico. Las "clases" así generadas permiten reducir el rango de búsqueda de algún template en la base de datos.

Sin embargo, los templates pertenecientes a una misma clase también presentarán diferencias conocidas como variaciones intraclase. Las variaciones intraclase implican que la identidad de una persona puede ser establecida sólo con un cierto nivel de confianza. Una decisión tomada por un sistema biométrico distingue "personal autorizado" o "impostor". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

- Una persona autorizada es aceptada,
- Una persona autorizada es rechazada,
- Un impostor es rechazado,
- Un impostor es aceptado.

Las salidas a y c son correctas, mientras que las b y d no lo son. El grado de confidencia asociado a las diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores:

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

La FAR y la FRR son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificación o verificación será un número real normalizado en el intervalo [0, 1], que indicará el "grado de parentesco" o correlación entre la característica biométrica proporcionada por el usuario y la(s) almacenada(s) en la base de datos.

Si, por ejemplo, para el ingreso a un recinto se exige un valor alto para el grado de parentesco (un valor cercano a 1), entonces pocos impostores serán aceptados como personal autorizado y muchas personas autorizadas serán rechazadas. Por otro lado, si el grado de parentesco requerido para permitir el acceso al recinto es pequeño, una fracción pequeña del personal autorizado será rechazada, mientras que un número mayor de impostores será aceptado. El ejemplo anterior muestra que la FAR y la FRR están íntimamente relacionadas, de hecho son duales una de la otra: una FRR pequeña usualmente entrega una FAR alta, y viceversa, como muestra la Fig.3.4. El grado de seguridad deseado se define mediante el umbral de aceptación u, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

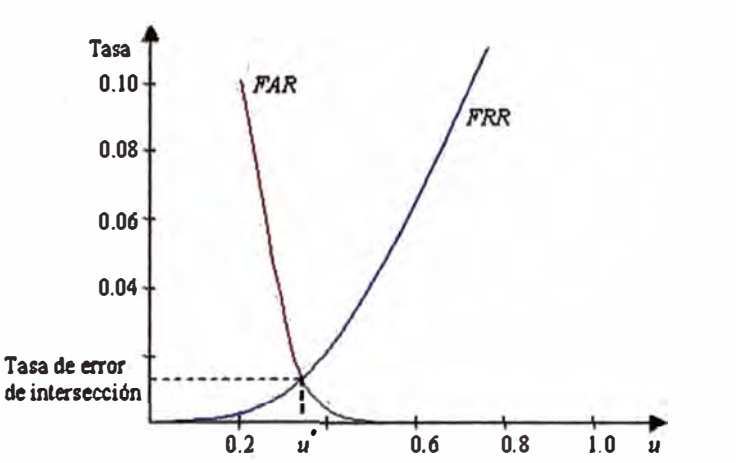


Fig.3.4 Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación u para un sistema biométrico. [15]

La FRR es una función estrictamente creciente y la FAR una estrictamente decreciente en u [9]. La FAR y la FRR al ser modeladas como función del umbral de aceptación tienen por dominio al intervalo real [0,1], que es además su recorrido, puesto que representan frecuencias relativas. La Fig.3.4 muestra una gráfica típica de la FRR y la FAR como funciones de u. En esta figura puede apreciarse un umbral de aceptación particular, denotado por u*, donde la FRR y la FAR toman el mismo valor. Este valor recibe el nombre de tasa de error de intersección (cross-over error rate) y puede ser utilizado como medida única para caracterizar el grado de seguridad de un sistema biométrico.

En la práctica, sin embargo, es usual expresar los requerimientos de desempeño del sistema, tanto para verificación como para identificación, mediante la FAR. Usualmente se elige un umbral de aceptación por debajo de u* con el objeto de reducir la FAR, en desmedro del aumento de la FRR.

La precisión de un sistema biométrico esta determinado a través de una serie de prueba, empezando con una evaluación de la precisión del algoritmo de comparación (evaluación tecnológica), luego evaluación de la performance en un entorno simulado (evaluación de escenario), seguido por pruebas en vivo in situ, antes de que todas las operaciones empiecen. Cada evaluación sirve a propósitos diferentes e involucra diferentes tipos de análisis.

3.8 sistemas biométricos actuales

Las biométricas más comúnmente implementadas o estudiadas incluyen a las huellas dactilares, rostro, iris, geometría de la mano, voz y firma manuscrita. Existen sin embargo otras modalidades que se encuentran en etapas de desarrollo y evaluación.

En la actualidad existen sistemas biométricos que basan su acción en el reconocimiento de diversas características, como puede apreciarse en la Fig.3.5 las técnicas biométricas más conocidas son nueve y están basadas en los siguientes indicadores biométricos:

- Impresiones dactilares,
- Rostro,
- Geometría de la mano,
- Iris,
- Voz,
- Firma
- Termograma del rostro,
- Venas de las manos,
- Patrones de la retina,

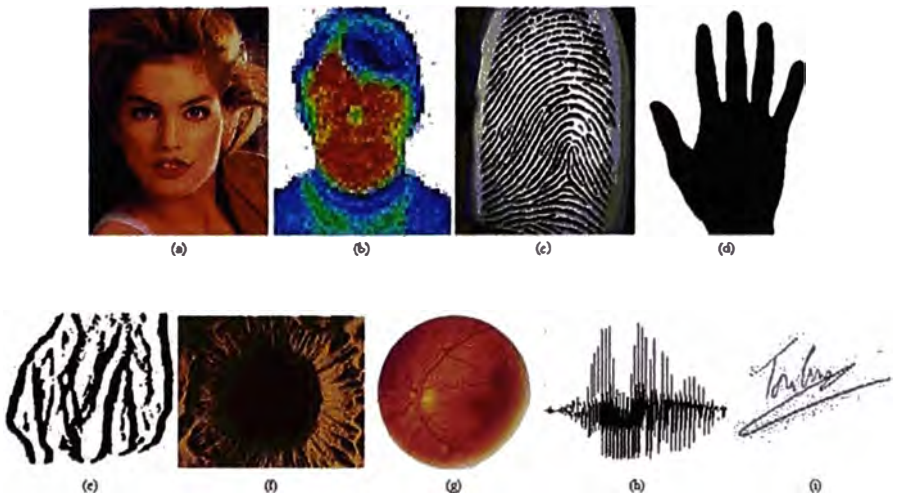


Fig.3.5 Técnicas biométricas actuales: (a) Rostro, (b) Termograma Facial, (c) Impresión dactilar, (d) Geometría de la mano, (e) Venas de la mano, (f) Iris, (g) Patrones de la retina, (h) Voz e (i) Firma.[15]

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

incluso decidir el uso de distintas técnicas en distintos ámbitos. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación. Por ejemplo, se integran el reconocimiento de rostros e impresiones dactilares. La razón es que el reconocimiento de rostros es rápido pero no extremadamente confiable, mientras que la identificación mediante impresiones dactilares es confiable pero no eficiente en consultas a bases de datos. Lo anterior sugiere el utilizar el reconocimiento de rostros para particionar la base de datos. Luego de esto comienza la identificación de la impresión dactilar. Los resultados alcanzados por el sistema conjunto son mejores que los obtenidos por sus partes por separado.

En efecto, las limitaciones de las alternativas por separado son soslayadas, logrando demás respuestas exactas con un tiempo de proceso adecuado. En la Fig.3.6 se presenta un esquema de división de las características biométricas.

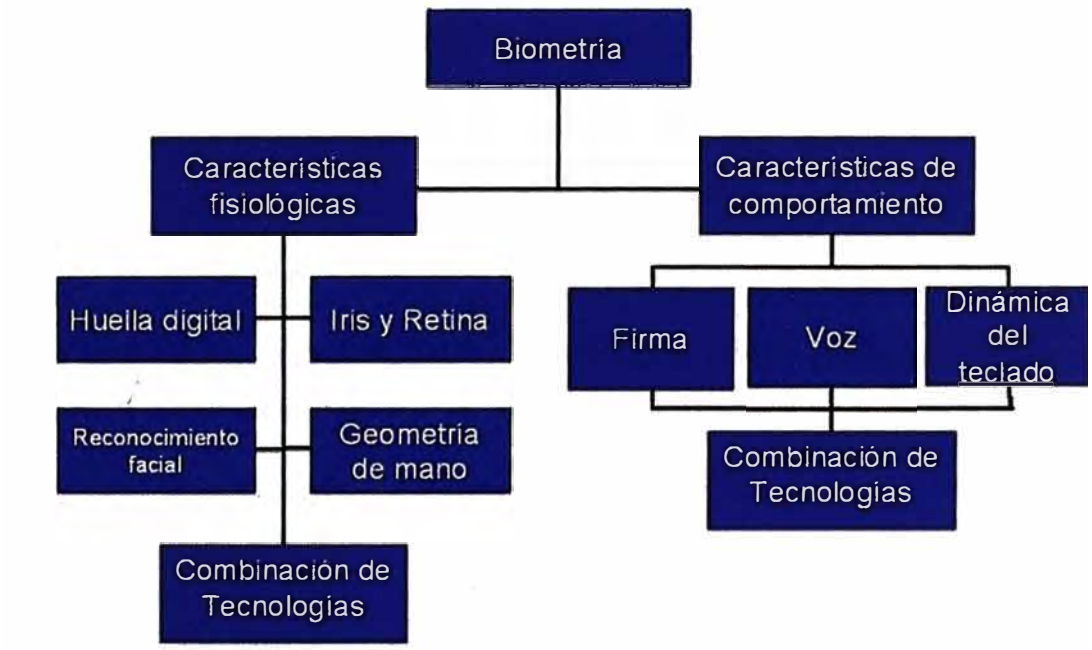


Fig.3.6 División de las características biométricas para identificación personal.[92]

CAPITULO IV
SISTEMA BIOMÈTRICO DE RECONOCIMIENTO DE HUELLAS DACTILARES

4.1. reconocimiento por huellas dactilares

La identificación biométrica es una de las más conocidas biometrías existentes. Debido a su unicidad y consistencia en el tiempo, las huellas han sido utilizadas para identificación por más de un siglo, y la identificación por medio de huellas ha llegado a ser automatizado debido al incremento en la potencia del cómputo, al desarrollo de teorías a la implementación de algoritmos eficientes. La identificación por huellas es popular debido a la inherente facilidad de su adquisición, las numerosas fuentes (10 dedos en ambas manos) disponibles para recolección.

Comparación manual de huellas para reconocimiento han sido utilizadas por muchos años, y ha llegado a ser una técnica identificación biométrica automatizada en las 2 últimas décadas.

Las huellas tienen una superficie irregular de crestas y valles que forman un único patrón para cada individuo. Para la mayoría de aplicaciones, el interés principal esta en los patrones de crestas de la primera falange del dedo.

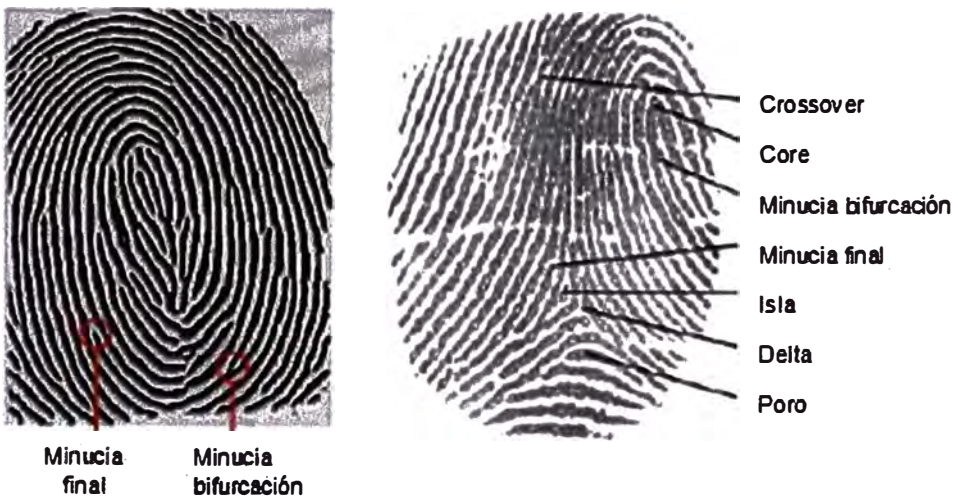


Fig.4.1 Reconocimiento de huellas, la figura muestra los diferentes puntos característicos o singulares utilizados para la identificación de individuos[60]

Una impresión dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela (crestas). Sin embargo estas líneas se interceptan y a veces terminan en forma abrupta.

Los puntos donde las crestas terminan o se bifurcan se conocen técnicamente como minucias. Otros puntos singulares de una impresión dactilar son aquellos donde la curvatura de las crestas es máxima. Esos puntos reciben el nombre de núcleos y deltas.

La característica más interesante que presentan tanto las minucias como los puntos singulares, núcleos y deltas es que son únicos para cada individuo y permanecen inalterados a través de su vida. A pesar de esta variedad de minucias (18 tipos distintos de minucias han sido enumerados) las más importantes son las terminaciones de las crestas y bifurcaciones de crestas. Esto último se debe a que las terminaciones de crestas representan aproximadamente el 60.6% de todas las minucias en una impresión dactilar y las bifurcaciones el 17.9%. Además varias de las minucias menos típicas pueden expresarse en función de las dos señaladas. Para poder identificar a una persona mediante las minucias de su impresión dactilar es necesario poder representar a estas últimas para poder compararlas. La representación estándar consiste en asignar a cada minucia su posición espacial (x, y) y su dirección que es tomada con respecto al eje x en el sentido contrario a los punteros del reloj. Esta representación se muestra en la Fig.4.2, para una minucia de término y una de bifurcación del surco (ridge).

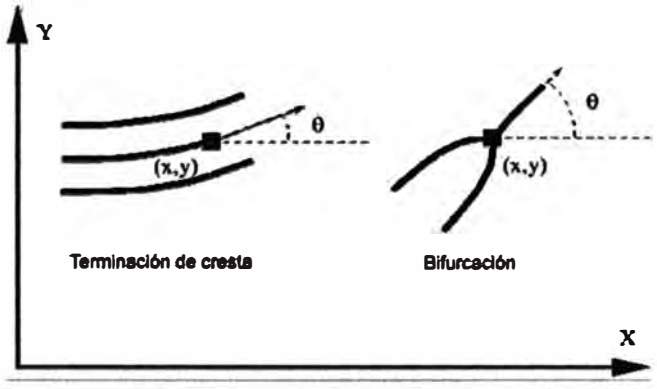


Fig.4.2 Representación de minucias en términos de su posición y dirección. [15,9]

El tipo de información que puede ser colectada de una impresión de las crestas de fricción del dedo, incluyen al flujo de las crestas de fricción (Detalle de Nivel 1), la presencia o ausencia de características a lo largo de las rutas de una cresta de fricción individual y su secuencia (Detalle de Nivel 2), y la intrincado detalle de una única cresta

(Detalle de Nivel 3). El reconocimiento usualmente se basa en el primer y segundo nivel de detalle o solo en el último.

4.2. diagrama de bloques del sistema de reconocimiento biométrico

Todo sistema de reconocimiento de huellas posee los siguientes bloques generales dentro de su estructura:

- Adquisición de la imagen
- Preprocesamiento de la Imagen
- Extracción de Características
- Comparación o Matching
- Decisión

A continuación se esquematizan por medio de un diagrama de bloques los principales bloques funcionales que componen un sistema de reconocimiento de huellas

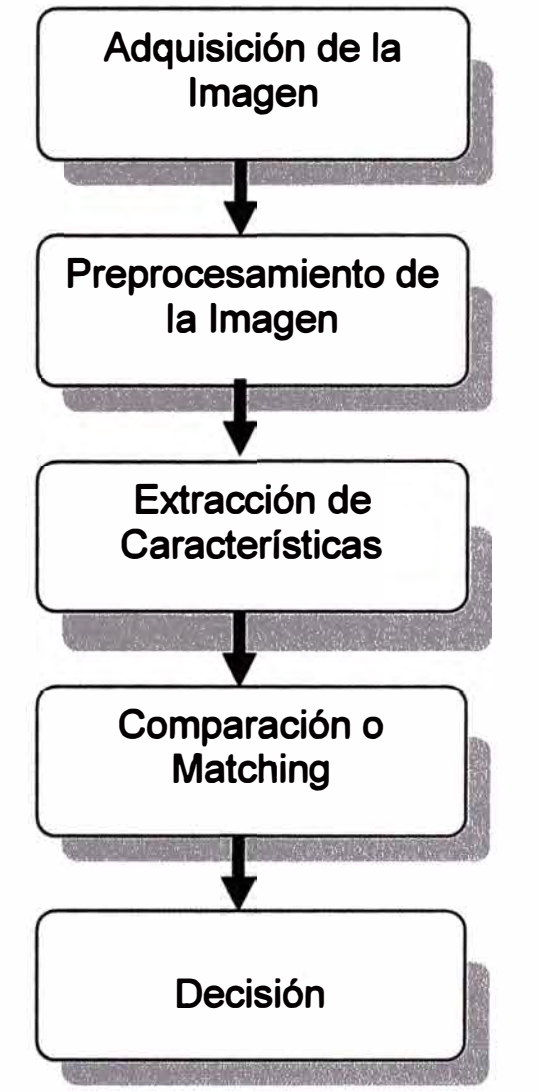


Fig.4.3 Principales Diagramas de Bloques típico de un sistema de reconocimiento de huellas. [14,34]

4.2.1 adquisición de la imagen

Durante esta etapa, la imagen de la huella dactilar del usuario del sistema es capturada por medio de un dispositivo o sensor electrónico, y convierte la señal capturada por el sensor en un mapa de bits. El dispositivo de captura puede ser de diferentes tecnologías. Ver 4.3.

Fig.4.4 Diferentes imágenes obtenidas al utilizar diferentes sensores biométrico[24]

4.2.2 preprocesamiento de la imagen

Esta etapa o modulo consiste de los procedimientos realizados a la imagen de la huella dactilar de preparación para el modulo de extracción de características, generalmente incluye los siguientes sub fases:

- verificación de la calidad: En esta etapa la huella adquirida es procesada para determinar si posee la calidad óptima que posibilite el reconocimiento. Debido a que la calidad de la huella afecta la performance de los algoritmos de comparación del sistema de reconocimiento de huellas (ver Ref. 30,48,49,57), es necesario que la huella se verifique previamente para verificar si es mayor al un mínimo umbral de calidad establecido en el sistema. Existen diversos algoritmos y técnicas para determinar la Calidad de la huella capturada, como se puede apreciar de la siguiente tabla.

TABLA Nº 4.1. Resumen de Métodos para Medir la Calidad de las imágenes de huellas dactilares[57]

Método	Algoritmos	Medida de Calidad
Modelo de Percepción Visual Humana para medir la calidad de la huella dactilar	Calculo de información de orientación de la región de interés.	0(pobre) -100(excelente) Puede ser configurado para retornar el nivel de calidad basado en umbrales
NIST Fingerprint Image Quality(NISTIR 7151)	Proceso de entrenamiento, Vector característico y Red Neuronal	1(Excelente) 5(Peor)
Otros	• Basado en Filtro de Gabor • Basada en Minucias • Basado Transformada Coseno	• Recuperable, No Recuperable. • Bueno, pobre, manchado, seco. • Bueno, Medio, pobre, fondo.

- estimación de la orientación: El campo de orientación de una imagen dactilar representa la direccionalidad de las crestas en la imagen dactilar. Este juego un papel importante en el análisis de imágenes. La imagen dactilar es dividida en un numero de bloques que no se traslapan (ej., 32 x 32 pixeles) y una orientación representativa de las crestas del bloque es asignado al bloque basado en un análisis del gradiente de escalas de grises en el bloque. A continuación se muestra el algoritmo utilizado para realizar la estimación de la orientación.

(a) Divide the input fingerprint image into blocks of size $W \times W$.

(b) Compute the gradients G_x and G_y at each pixel in each block [4].

(c) Estimate the local orientation at each pixel (i,j) using the following equations [28]:

$$V_x(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2G_x(u,v)G_y(u,v), \quad (1)$$

$$V_y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} (G_x^2(u,v) - G_y^2(u,v)), \quad (2)$$

$$\theta(i,j) = \frac{1}{2}tan^{-1}\left(\frac{V_x(i,j)}{V_y(i,j)}\right), \quad (3)$$

where W is the size of the local window; G_x and G_y are the gradient magnitudes in x and y directions, respectively.

(d) Compute the consistency level *of the orientation field in the local neighborhood of a block (i,j) with the following formula:*

$$C(i,j) = \frac{1}{N}\sqrt{\sum_{(i',j')\in D} |\theta(i',j') - \theta(i,j)|^2}, \quad (4)$$

$$|\theta' - \theta| = \begin{cases} d & if\,(d = (\theta' - \theta + 360)\ mod\ 360) < 180, \\ d - 180 & otherwise, \end{cases} \quad (5)$$

where D represents the local neighborhood around the block (i,j) (in our system, the size of D is 5×5); N is the number of blocks within D; $\theta(i',j')$ and $\theta(i,j)$ are local ridge orientations at blocks (i',j') and (i,j), respectively.

(e) If the consistency level *(Eq.(5)) is above a certain threshold T_c, then the local orientations around this region are re-estimated at a lower resolution level until $C(i,j)$ is below a certain level.*

Fig.4.5 Algoritmo de estimación del campo de una imagen dactilar. [94].

- mejoramiento o realce: Se realiza con la finalidad de obtener una imagen libre de errores, y permita determinar las características principales que requieren para el proceso de comparación. Podría llegar a obviarse en un sistema de captura que nos asegure unas condiciones de iluminación constantes (posiblemente, no seria necesario si se utiliza un sensor especifico). Existen diversos métodos propuestos para el realce de la imagen, en cada uno de ellos la imagen es subdividida en sub-bloques NxN y para evitar el efecto de traslape son superpuestas en cada dirección con las regiones vecinas, el resultado de la operación se aplica en la parte central (N/2xN/2). Mencionamos a continuación los métodos utilizados en el realce de la imagen:
    - basado en histograma: La operación se realiza en cada subimagen es una ecualización del histograma de escala de grises.

- basado en fft: A la sub imagen se le aplica un filtro de frecuencia igual a al potencia del modulo FFT, este método se basa en reforzar las frecuencias mas importantes y debilitar las sospechosas de contener ruido. La formula para la imagen de salida es:

$$Im = FFT^{-1}\{FFT(Im) \times |FFT(Im)|^{k}\} \tag{4.1}$$

Siendo Im (la sub imagen), FFT la transformada rápida de Fourier.

- basado en filtros de Gabor: Estos filtros tienen propiedades selectivas en orientación y frecuencia, además de poseer una resolución conjunta óptima en ambos dominios: espacial y frecuencia. La forma del filtro de Gabor es:

$$G(x, y; \theta, f) = \exp\left\{-\frac{1}{2}\left[\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right]\right\}\cos(2\pi f x_\theta), \tag{4.2}$$

$$x_\theta = x\cos\theta + y\sin\theta, \tag{4.3}$$

$$y_\theta = -x\sin\theta + y\cos\theta, \tag{4.4}$$

Donde O es la orientación del filtro de Gabor, f es la frecuencia de la onda coseno, σ_x σ_y son las desviaciones estándar de la envolvente gaussiana a lo largo de los ejes x, y. x_Θ e y_Θ definen los ejes x e y de la trama de coordenadas del filtro. El filtro de Gabor es aplicado a la imagen por convolución espacial. La convolución de un pixel (i,j) en la imagen requiere el correspondiente valor de orientación O(i,j) y el valor de frecuencia de crestas F(i,j) de cada pixel. La aplicación del Filtro Gabor G para obtener la imagen mejorada es la siguiente:

$$E(i,j) = \sum_{u=-\frac{w_x}{2}}^{\frac{w_x}{2}} \sum_{v=-\frac{w_y}{2}}^{\frac{w_y}{2}} G(u, v; O(i,j), F(i,j))N(i-u, j-v), \tag{4.5}$$

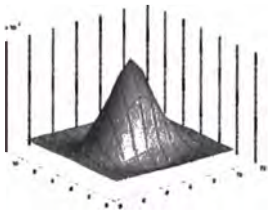
$$\sigma_x = k_x F(i,j), \tag{4.6}$$

$$\sigma_y = k_y F(i,j), \tag{4.7}$$

Donde O es la orientación de la imagen, F es la frecuencia de crestas de la imagen, N es la imagen normalizada, y w_x e w_y son el ancho y alto del filtro mascara de Gabor, respectivamente.

(a) Original image

(b) Enhanced image ($k_x = 0.2$, $k_y = 0.2$)



(c) Gabor filter ($k_x = 0.2$, $k_y = 0.2$)

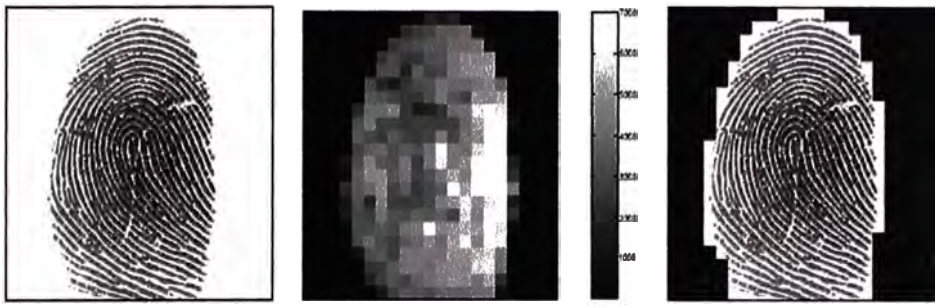
Fig.4.6 Imagen que ilustra el mejoramiento efectuado sobre la imagen original por el filtro Gabor [23].

- segmentación: En el procesamiento de las imágenes de huellas dactilares es usualmente necesario remover las partes que no llevan información válida. La segmentación es útil para este propósito. Uno de los métodos mas sencillos para la segmentación es el utilizar un umbral adaptivo, existen sin embargo otros que explotan el hecho de que hay una diferencia significante en las magnitudes de la varianza en la escala de gris a lo largo del flujo de las crestas de la huella. También existen métodos compuestos que combina la información de la dirección y varianza. Las formulas para determinar la varianza de los niveles de grises de un bloque, es calculada por:

$$V(k,l) = [1/XY]\sum^{Y}_{i=0}\sum^{X}_{j=0}[i(kY+i,lX+j)-\mu] \qquad (4.3)$$

X, Y dimensiones del bloque

μ media aritmética de los niveles de gris del bloque (k,l) e i es la imagen.



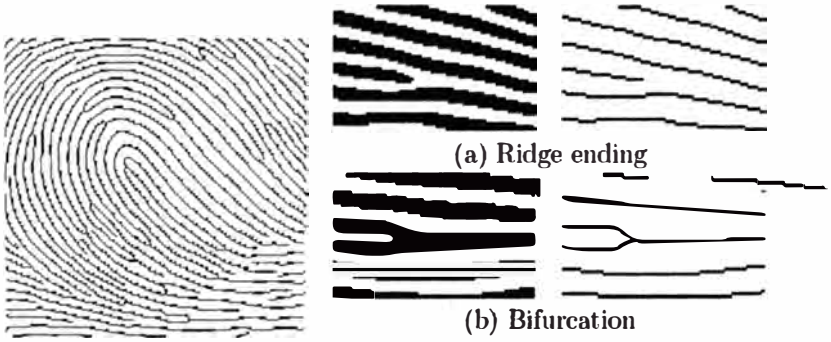
(a) Original image (b) Variance image (c) Segmented image

Fig.4.7 El resultado de la segmentación usando umbral de Huella Binarizada[14]

- binarización: Donde se procesa la imagen original convirtiendo los tonos de gris a blanco y negro, según estos sean mayor o un umbral global. El proceso de binarización mejora el contraste entre las crestas y valles en una imagen de huella dactilar.

Fig.4.8 Huella Binarizada[14]

- adelgazamiento: En este proceso las crestas de las líneas dactilares son procesadas de manera que todas tengan el mismo grosor (1 píxel), de esta forma la identificación de los puntos característicos e hace más fácil.



(a) Ridge ending

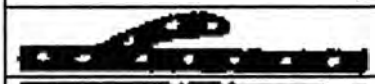
(b) Bifurcation

Fig.4.9 Izquierda, se ilustra el adelgazamiento efectuado sobre la imagen binarizada, Derecha, finalización de una cresta y un punto de bifurcación antes y después del adelgazamiento [23].

4.2.3 extracción de características

- Es la etapa primordial en el reconocimiento de huellas dactilares, por lo tanto mientras mas confiable sea el método o algoritmo utilizado se obtendrá un mejor rendimiento del sistema. Dentro de la imagen de una huella dactilar se pueden encontrar las minucias descritas en la TABLA Nº 4.2. Los dos tipos de minucias más importantes son las bifurcaciones y terminaciones, ya que los demás tipos de minucias se forman con una combinación de estas dos. Por esta razón, en la etapa de extracción de características se detectan estos dos tipos de minucias principalmente.

TABLA Nº 4.2. Tipos de Minucias.[14]

Características	
	Terminación
	Bifucarción
	Laguna
	Borde independiente
	Punto o isla
	Aguijón
	Cruce

- El método más comúnmente empleado para extraer minucias es el número de cruces (CN)[4]. Este método extrae las crestas terminales y bifurcaciones de la imagen adelgazada o esqueletizada examinando los vecinos locales de cada píxel de la cresta usando una ventana de 3x3 pixeles. El CN para un píxel de cresta P esta dado por [1]:

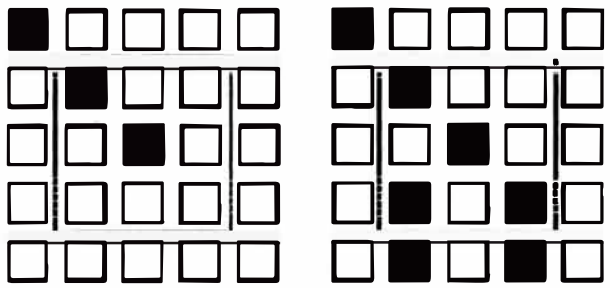
$$CN = 0.5\sum_{i=1}^{8}|P_i - P_{i+1}|, \qquad P_9 = P_1 \tag{4.4}$$

- Donde P_i es el valor del píxel en la vecindad de P. Para un píxel P, sus 8 pixeles vecinos son escaneados en una dirección contra el reloj como se ilustra por la siguiente figura:

P_4	P_3	P_2
P_5	P	P_1
P_6	P_7	P_8

Fig.4.10 Los pixeles vecinos del píxel P [23].

Después de que el CN para cada píxel de la cresta ha sido calculado, el píxel puede ser clasificado de acuerdo a la propiedad de su valor CN. As shown in Figure 3.2, a ridge pixel with a CN of one corresponds to a ridge ending, and a CN of three corresponds to a bifurcation. For each extracted minutiae point, the following information is recorded:



(a) CN = 1 (b) CN = 3

Fig.4.11 Ejemplos de un píxel final de cresta y bifurcación. (a) Un Número de Cruce de uno corresponde al píxel final de cresta. (b) Un Número de Cruce de 3 corresponde a un píxel de bifurcación. [23].

- Otro concepto relacionado a la extracción de los puntos característicos de las huellas, involucra la extracción del core o punto de referencia de la huella. A continuación se describe un algoritmo para la extracción de este punto característico.
  - Estimar y suavizar los campos direccionales de la imagen de la huella.
  - En cada bloque (8×8), calcula el índice de Poincare. El índice de Poincare es calculado como sigue:

$$Poincare(i,j)=\frac{1}{2\pi}\sum_{k=0}^{N-1}\Delta(k),$$

$$\Delta(k)=\begin{cases}\delta(k) & if\ |\delta(k)|<\frac{2}{\pi},\\ \pi+\delta(k) & if\ |\delta(k)|<-\frac{2}{\pi},\\ \pi-\delta(k) & otherwise.\end{cases}$$

$$\delta(k)=\theta(X(k'),Y(k'))-\theta(X(k),Y(k)).$$

$$k'=(k+1)\ \mathrm{mod}\ N. \qquad (4.5)$$

  - Donde θ (i, j) es el campo direccional de la huella. X (k), Y(k) son las coordenadas de los bloques que están dentro de la curva encerrada por N Bloques. Si el índice de Poincare es 1/2, este bloque es el bloque core. El

centro de este bloque es el punto core. Si mas de 2 puntos core son detectados se regresa al paso 1.

4.2.4 post procesamiento

- Las falsas minucias pueden ser introducidas dentro de la imagen debido a factores tales como imágenes ruidosas, e imágenes con defectos creados por el proceso de adelgazamiento. Por tanto después de extraída las minucias, es necesario emplear una etapa de post procesamiento para validar las minucias.

(a) Spur (b) Hole (c) Triangle (d) Spike

Fig.4.12 Ejemplos de estructuras de minucias falsas. [23].

4.2.5 clasificación

- A través de este modulo podemos determinar, la clasificación topológica que le corresponde a cada imagen de huella procesada. Podemos mencionar la aplicación de clasificación automática de huellas o Método PCASYS(Pattern-level Classification Automation System) que pertenece al NIST, y utiliza una red neuronal probabilística para realizar la clasificación

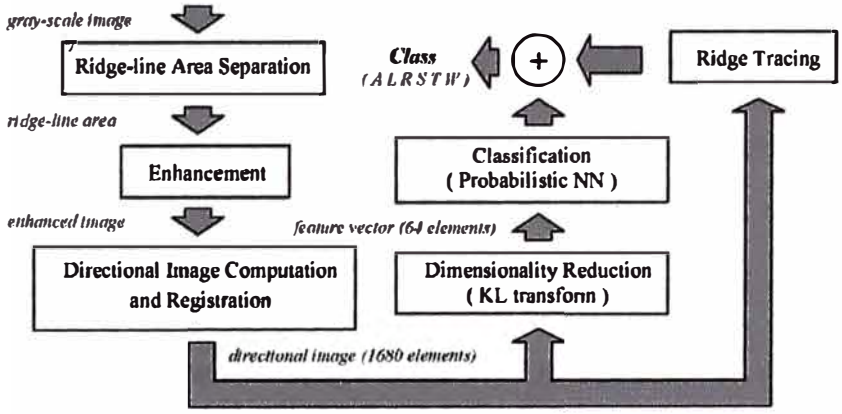


Fig.4.13 Esquema funcional del Método de Clasificación PCASYS.[5]

4.2.6 comparación o matching

- Una vez detectadas las bifurcaciones y terminaciones dentro de la imagen, se forma una plantilla, la cuál contiene el tipo de minucia detectada, posición, distancia a sus cinco vecinos más cercanos, y ángulo de orientación de la minucia. Con esta plantilla que se obtiene para cada minucia, se forma una base de conocimiento para cada individuo. Si la imagen pertenece a su clase de acuerdo

con la estructura global de la huella dactilar del individuo, ésta base de conocimiento se compara con la imagen del individuo a fin de poder decidir si pertenece o no al individuo.

4.3. dispositivos de captura

Existe una variedad de tipos de sensores, ópticos, capacitivos, ultrasónicos y térmicos que son usados para colectar la imagen de la huella.

Fig.4.14 Diversos tipos de lectores biométricos dactilares. Ópticos, Capacitivos, Ultrasónicos, térmicos, etc. [68].

4.3.1 sensores ópticos

Los sensores ópticos toman una imagen digital de la superficie del dedo, y son los más comunes hoy en día.

- frustrated total internal reflection (FTIR): Esta tecnología esta basada en el comportamiento de la luz en las fronteras de un material a otro. El dedo esta colocado en el lado superior de un prisma de vidrio. La luz que entra al prisma desde un LED en un lado del prisma es parcialmente reflejado en la superficie de contacto y luego es capturada vía lentes con un chip sensor de luz (por ejemplo un Charge Coupled Device (CCD) o sensor de imagen - Complementary Metal Oxide Semiconductor (CMOS)) en el otro lado del prisma. El contraste en la

imagen es causado por el hecho de que la luz es aleatoriamente dispersada o absorbida en los puntos donde las crestas de la piel y donde el prisma se contactan, y se refleja totalmente en los valles donde el contacto no se producen.

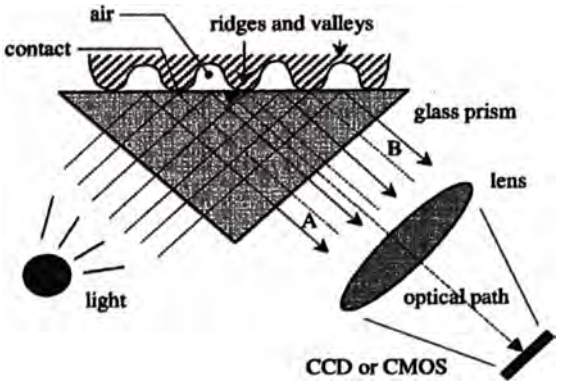


Fig.4.15 Un sensor de imagen basado en FTIR[24]

- surface enhanced irregular reflection (SEIR): Esta tecnología comparte algunas características con la tecnología FTIR. La luz incide perpendicularmente sobre la superficie de contacto, se dispersa en las crestas pero pasa completamente en los valles es decir ninguna dispersión se produce. La dispersión de la luz es colectada por el sensor de imagen, así se produce puntos de luz par las crestas y puntos oscuros para los valles. Los fabricantes de este sensor indican que esta tecnología da imágenes de un mayor contraste que la tecnología FTIR.

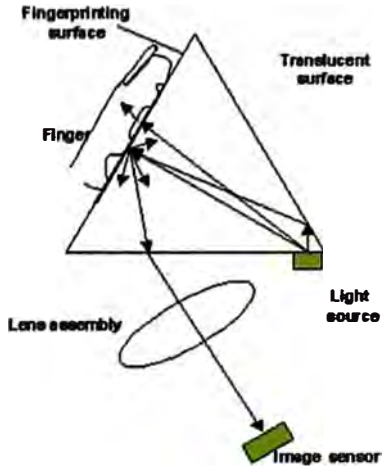


Fig.4.16 Un sensor de imagen basado en SEIR[24]

- electro-óptica: Este sensor usa una capa de un polímero emisor de luz, cuya emisión de luz varía según el potencial aplicado en un lado. Cuando un dedo se coloca sobre la superficie del polímero, las crestas tocan al polímero y los valles no, causando que el potencial varia a través de la superficie. Así, se genera una representación luminosa de la huella. Una segunda capa que consiste de un array de fotodiodos o un CMOS, convierte el patrón de luz en una imagen digital.

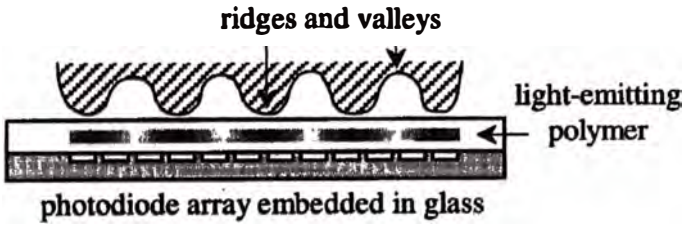


Fig.4.17 Un sensor de imagen electro óptico[24]

- touchless: En este caso una cámara de alta calidad es usada para enfocar la yema del dedo y directamente lee la huella. Usualmente alguna clase de soporte mecánico esta presente para facilitar la presentación del dedo a una distancia configurada.

4.3.2 sensores de estado sólido

- capacitivo: Un sensor capacitivo es un array bidimensional de platos microcapacitores embebidos en un chip. La superficie del dedo actúa como un segundo plato micro capacitor. Pequeña cargas eléctricas son creadas entre el array y el dedo, cuya magnitud depende de la distancia entre las superficies. De tal manera que el patrón de capacitancia resultante representa el patrón de crestas y valles de un dedo.

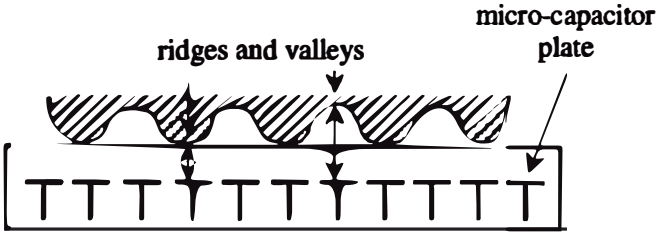


Fig.4.18 Un sensor de imagen capacitivo[24]

- campo eléctrico: Este tipo de sensor genera un pequeño campo de radio frecuencia, el cual es modulado por la alta conductividad de la capa inferior de la superficie de la piel (capa de células piel viva). Una matriz de antenas recibe la amplitud de la pequeña señal análoga modulada, la cual es posteriormente procesada y digitalizada para obtener una imagen que representa los contornos de la capa de piel viva.

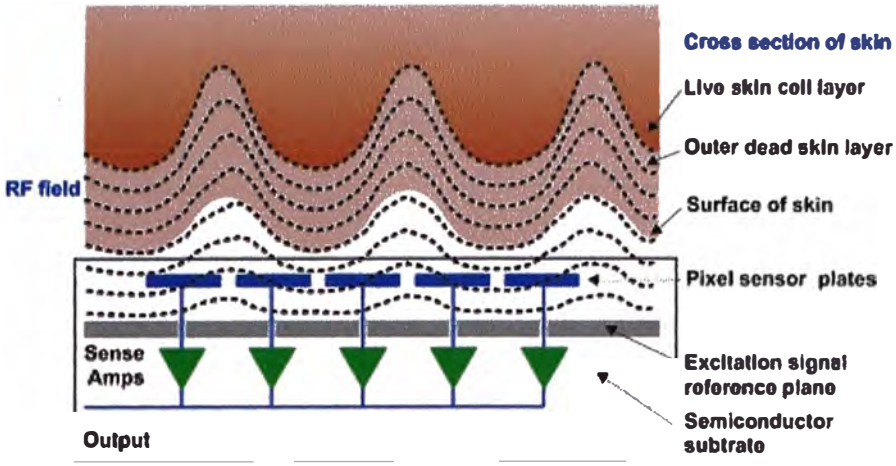


Fig.4.19 Un sensor de imagen de campo eléctrico[24]

- piezoeléctrico: Estos sensores usan el efecto piezoeléctrico. La superficie del sensor es hecha de un material dieléctrico no conductor el cual genera pequeñas cantidades de corriente cuando es presionado. La cantidad de corriente depende de la presión aplicada. Cuando la yema del dedo presiona el sensor, las crestas aplican una mayor presión que los valles que están mas cerca de la superficie del sensor. Típicamente, el material del sensor usa alguna clase de umbral para determinar si el sensor es o no presionado, así solamente permite la adquisición de imágenes binarias.
- térmico (sensor de barrido): Estos sensores son fabricados de un material piro eléctrico que genera corriente basado en diferencias de temperatura. Deslizar un dedo a través de un sensor calentado eléctricamente permite medir el flujo de calor de la piel, la cual es mayor en la dirección de contacto con el sensor, así permite la distinción entre las crestas y valles del dedo.

4.3.3 otros tipos de sensores

- Ultrasónico: Este tipo de sensado esta basado en el envió de señales acústicas hacia la yema del dedo y captura de la señal de eco. Como cada cambio de impedancia da un eco parcial, esta tecnología puede ser usada para capturar la imagen de la superficie debajo de la piel.

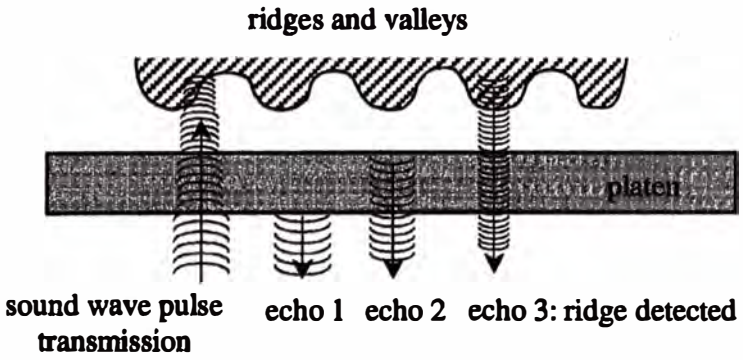


Fig.4.20 El principio del sensado ultrasónico de una huella dactilar[24]

4.4. estándares

El principal esfuerzo de estandarización de los sistemas biométricos ha partido como iniciativa de organizaciones norteamericanas como el FBI, el NIST y ANSI, entre otras.

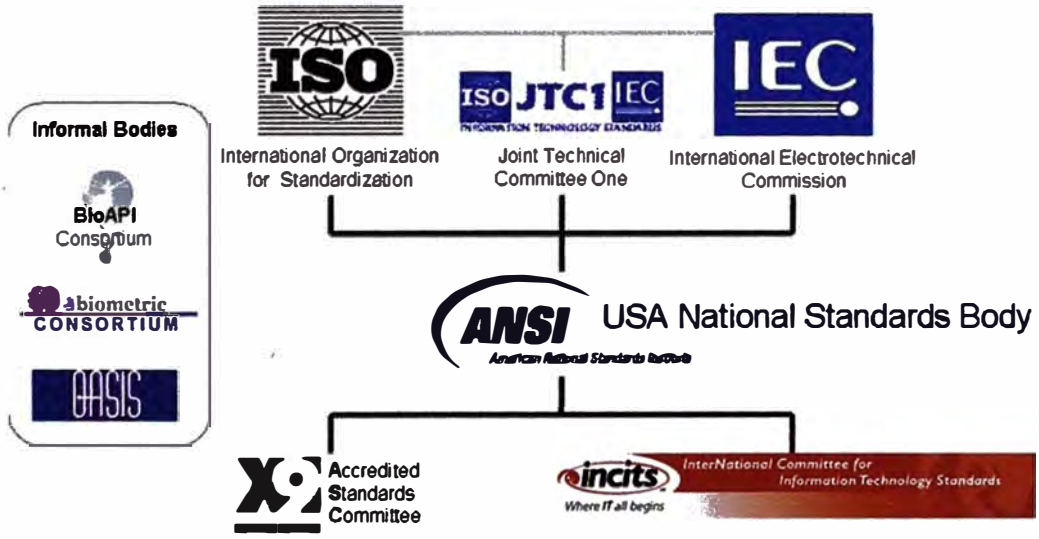


Fig.4.21 Cuerpo de Estándares Internacionales [90 ,91].

4.4.1 estándares existentes

Los mayores esfuerzos en los estándares desarrollados se enfocan en la estandarización del contenido, el significado y la representación de los formatos de datos de intercambio de huellas dactilares e incluyen las normas:

- ANSI/INCITS 381-2004 formato de intercambio de datos basado en imagines de dedos— Este estándar especifica un formato de intercambio para el intercambio de los datos basados en imágenes para el reconocimiento de huellas dactilares y de la palma. Define el contenido, el formato, y las unidades de medida para tal

información. Este estándar se piensa para esos usos de identificación y verificación que requieren el uso de los datos crudos o procesados de la imagen que contienen la información detallada del píxel. [89].

- ANSI/INCITS 377-2004 formato de intercambio de datos basado en patrones del dedo — Este estándar especifica un formato de intercambio para el intercambio de los datos para reconocimiento de huella dactilar basados en patrones. Describe la conversión de una imagen cruda de la huella dactilar a un patrón del dedo, recortado y muestreado seguido por la representación celular de la imagen del patrón del dedo para crear los datos del intercambio de los patrones del dedo.[89].
- ANSI/INCITS 378-2004 Formato de las minucias del dedo para el intercambio de datos – Este estándar define un método de representación de información de huellas dactilares usando el concepto de minucias. Define la ubicación de las minucias en una huella dactilar, un formato de grabación para contener los datos de las minucias, y extensiones opcionales para contar crestas información de núcleo/delta. [89].
- ANSI/NIST ITL 1-2000 Formato de datos para el intercambio información de huellas dactilares, Faciales, cicatrices, marcas & tatuajes (Scar Mark and Tatoo, SMT). Este estándar define el contenido, el formato, y las unidades de medida para el intercambio de la información de las imágenes de huellas dactilares, de la palma, faciales /ficha fotográfica, cicatriz, marca, y tatuaje (smt), que se puede utilizar en el proceso de la identificación de un sujeto. La información consiste en una variedad de ítems obligatorios y opcionales, incluyendo parámetros de escaneo, datos relacionados, descriptivos y de registro, información de huella dactilar digitalizada, e imágenes comprimidas o sin comprimir.[91]
- ISO/IEC 19794-2 formato de minucias del dedo para intercambio de dato — Este estándar describe cómo los puntos de las minucias serán determinados, define los formatos de datos para contener los datos para el uso general y de tarjeta inteligente, y detalla la información de la conformidad. Las pautas y los valores para los parámetros de combinación y decisión se proporcionan como anexo informativo. El estándar define tres tipos de minucias, incluyendo los finales de cresta y la bifurcación. La estrategia adoptada de la determinación de las minucias se basa en la imagen esqueletizada [91].

- ISO/IEC FCD 19794-3 Formato de intercambio basado en patrones del dedo — Este estándar de bosquejo especifica que una imagen de la huella dactilar está dividida en una grilla de células solapadas o no solapadas. En cada célula, el patrón del dedo será representado por una estructura de célula. Un método para obtener la estructura de la célula es descomponer cada uno de las células en una representación espectral de dos dimensiones tal como la Transformada Discreta de Fourier (Discrete Fourier Transform, DFT) de dos dimensiones. La descomposición produce los componentes espectrales, donde cada componente se puede caracterizar por una longitud de onda horizontales (x) y verticales (y), en dirección, amplitud, y fase. Para más información,[89].
- ISO/IEC 19794- 4 Formato de intercambio basado en imagines de dedos — Este estándar especifica que la imagen deberá parecer haber sido capturada en una posición vertical y deberá esta aproximadamente centrada. horizontalmente en el campo visual. La secuencia de la exploración y los datos registrados deberán parecer haber sido de izquierda a derecha, progresando de arriba a bajo de la huella dactilar. El origen de los ejes, ubicación del píxel (0.0), es en la esquina superior de la mano izquierda de cada imagen con la posición de la coordenada x (horizontal) aumentando positivamente del origen al lado derecho de la imagen mientras que la posición de la coordenada y (vertical) aumenta positivamente del origen a la parte inferior de la imagen. También especifica que el encabezado debe ser de acuerdo a CBEFF. [89].
- ISO/IEC 19794-8 Esquema Datos del Patrón del Dedo — Este estándar esta prensado para ser utilizado para alcanzar interoperabilidad entre los sistemas de reconocimiento de huellas dactilares basados en minucias y en patrones. Se basa en las características comunes compartidas entre el patrón espectral y las minucias por medio de la codificación de las crestas de una forma que el esquema de crestas proporcione las bases para detectar minucias [89].
- EFTS v7.1 Especificaciones de transmisión electrónica de huellas dactilares - Esta especificación cubre la transmisión electrónica de la información que implican las huellas dactilares al FBI del Sistema Automatizado Integrado de la Identificación de Huellas dactilares (IAFIS) basado en el estándar NIST ITL 1-2000 del ANSI. El propósito de este documento es especificar ciertos requisitos a los cuales las agencias deban adherir para comunicarse electrónicamente con el IAFIS.[]
- EBTS v1.0 Especificaciones de transmisión electrónica de biometría — esta especificación describe arreglos de las transacciones de las Especificaciones

transmisión electrónica de huellas dactilares (EFTS) del FBI, que son necesarias para utilizar el sistema de identificación biométrica automatizada (ABIS) del Departamento de Defensa (DoD).

- FBI- WSQ (Wavelet Scalar Quantization, WSQ) Compresión de imágenes de huellas dactilares por Cuantización de Wavelets Escalares — Es una compresión con perdida de información (Lossy) que es capaz de preservar los detalla de alta resolución de una imagen en escala de grises que son usualmente descartados por otros algoritmos de compresión del tipo Lossy. Alcanza un alto cociente de compresión, por medio 15:1 dependiendo de los parámetros. Para más información, ver el documento No. IAFIS-IC-0110 (V3), 19 de diciembre de 1997."Servicios de información de la justicia criminal (CJIS) Especificación de compresión de imágenes en escala de grises de huellas dactilares WSO" del FBI.
- JPEG2000 (Joint Photographic Experts Group 2000) la compresión de imágenes de huellas dactilares del Grupo de Expertos de la Asociación Fotográfica 2000 es un nuevo sistema de codificación de la imagen que utiliza técnicas avanzadas de compresión basadas en tecnología de Wavelets. Su arquitectura debe prestarse a una amplia gama de aplicaciones desde cámaras fotográficas digitales portables hasta avanzadas como la pre impresión (para las industrias de imprenta y publicación), diagnostico por imágenes en medicina y otro sectores clave.

4.5. mercado de mundial del reconocimiento de huellas

El mercado mundial Biométrico según IBG en su reporte del 2006-2007, ver Fig.4.22 muestra que la tecnología de reconocimiento de huellas abarca el mayor porcentaje de la distribución frente a otras tecnologías biométricas, esto nos permite deducir el afianzamiento de esta tecnología, lo cual también va de la mano con la cantidad de investigación relacionada a temas biométricos y en especial de la de reconocimiento por huellas. Este empuje ha fomentado entre otras cosas la aparición de estándares que permitan la interoperabilidad entre distintos productos biométricos.

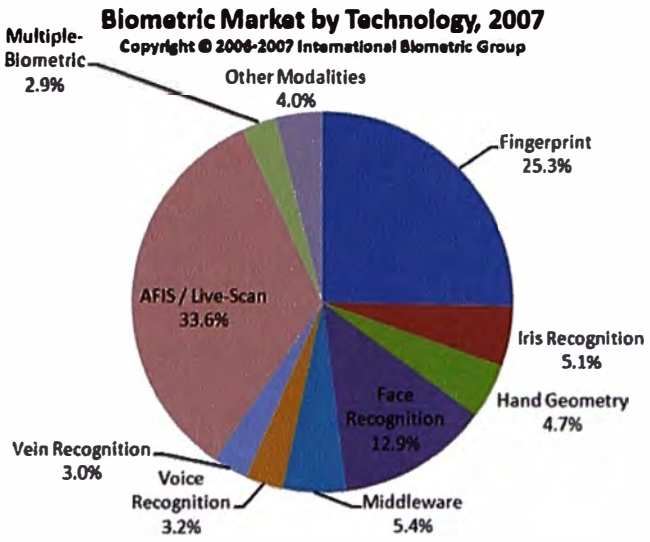


Fig.4.22 Distribución del mercado biométrico en función al tipo de biometría. [93].

Así mismo según el reporte "GLOBAL AFIS Market", elaborado por la empresa consultora Frost & Sullivan (2004), se indica que el mercado AFIS (Sistema Automático de Identificación por Huellas) de gran escala esta cubierto por 4 grandes compañías:

- Sagem
- NEC Technologies
- Printrak. A Motorola Company
- Cogent Systems

4.6. proyectos y programas relacionados al reconocimiento de huellas.

El gobierno de los EE.UU. Ha conducido a través de sus órganos técnicos especializados programas relacionados al reconocimiento de huellas, así podemos mencionar los siguientes programas más representativos:

- Evaluación para los proveedores de tecnología como el Fingerprint Vendor Technology Evaluation, (FVTE). Este programa fue diseñado para evaluar la capacidad de los sistemas de huellas dactilares para enfrentar los requerimientos de aplicación del mundo real tanto a gran escala como a pequeña escala. Durante estas pruebas se utilizaron diferentes combinaciones de huellas de diferentes tipos y calidades (captura en vivo o en papel). Se encontró que las variables que tenían más efecto en el acierto de los sistemas eran el número de dedos utilizados y la calidad de las huellas. Un numero elevado resultaba en un mayor acierto, el acierto de las búsquedas usando 4 o mas dedos era mayor que el acierto con 2 dedos.

- La captura rápida de huellas dactilares enroladas y de la palma de la mano, ha sido una iniciativa de las agencias de gobierno, para expandir la búsqueda de huellas dactilares de las palmas de las manos, desafiando a la industria a desarrollar y demostrar tecnología para capturar 10 huellas dactilares enroladas en menos de 15 segundos, mejorar significativamente la calidad de las huellas capturadas, reducir la tasa de error durante el enrolamiento y se portable, resistente, barato.
- Sistema automático integrado de huellas dactilares (IAFIS). El IAFIS contiene más de 47 millones de ternas de huellas. Este sistema integrado tiene capacidad de realizar búsquedas automatizadas de huellas decadactilares y huellas latentes, almacenamiento e intercambio de huellas.
- Personal identity verification standards for federal employees and contractors. El presidente de los EEUU emitió una directiva que indica el establecimiento de formas seguras y confiables para la identificación que emite el gobierno federal a sus empleados y contratistas que requieran acceso a las instalaciones y sistemas de información. Se establece que para el acceso seguro a las instalaciones y los sistemas de información se utilizara una tarjeta de identificación que incorpore características biométricas, tales como huellas.
- MINEX es un programa dedicado a la evaluación y desarrollo de las capacidades de los matcher's de huellas que ejecutan en una tarjeta inteligente ISO/IEC 7816. MINEX a programa del NIST que coordina el desarrollo de esfuerzos para mejorar la performance e interoperabilidad de las implementaciones de los estándares de plantillas de huellas biométricas INCITS 378 y ISO/IEC 19794-2.

En el Perú también se ha promovido los proyectos de gran envergadura, relacionados a la utilización de tecnología biométrica de reconocimiento de huellas, así podemos mencionar que:

- El RENIEC institución del Estado Peruano encargada del Registro e Identificación de los Peruanos, ha adquirido en el 2006 un Sistema AFIS, el cual es utilizado en sus procesos de validación para la emisión del documento de Identidad, que posibilita la detección de casos de dobles identidades, intentos de actos fraudulentos, y permite automatizar los procesos internos de la institución.
- Se ha firmado un convenio entre el Colegio de Notario de Lima y el RENIEC para la prestación del Servicio de Verificación Biométrica de la Identidad. Con este Servicio los notarios afiliados al convenio podrán validar la identidad de sus

clientes en línea, evitando así las suplantaciones y estafas. Este servicio es pionero en América Latina.

- El poder Judicial ha creado la base de datos biométrica de requisitoriados, con lo cual podrá controlar mediante la verificación e identificación biométrica dactilar a los ciudadanos peruanos que tengan restricciones de libertad y que están obligados a asistir a los centros judiciales.
- El nuevo documento de identidad electrónico que se emitirá en los próximos años, contara con una aplicación de verificación biométrica de la identidad embebida dentro del chip de la tarjeta inteligente que lo soporta, además de contar con los elemento de seguridad que lo hacen un documento mas robusto y con mejores prestaciones.

CAPITULO V
PROPUESTA DE SOLUCIÓN

5.1 instalaciones a controlar

Las instalaciones a ser controladas, así como la distribución del número de puertas por hall y al interior del hall (oficinas) se muestran en la siguiente tabla.

TABLA Nº 5.1. Distribución de los acceso a controlar por cada piso[65,66]

Piso	Puertas en hall	Puertas en oficinas al interior del hall	Total
11º	1	1	4
4º	–	3	4
3º	1	1	7
2º	4	2	5
1º	–	1	1
	34	14	48

Las puertas donde se requiere la instalación de controles de acceso corresponden a oficinas donde se realizan funciones relativas al archivo central de documentos, a procesos informáticos, a manejo de valores y efectivo, a la alta dirección, y al control de la Seguridad. Algunas de las puertas a controlar, sirven de pase general entre los halles de acceso a ascensores y escalera, en los pisos correspondientes, hacia ambientes donde labora el personal. Otras corresponden específicamente a oficinas donde se requiere un mayor nivel de seguridad.

5.2 requerimientos del sistema

5.2.1 respecto a los componentes hardware

- El Sistema de Control de Acceso debe permitir definir los permisos para los usuarios internos, de manera que se pueda registrar sus ingresos, salidas y eventos asociados al funcionamiento de las puertas, asimismo permitirá establecer su administración general, desde una estación de trabajo centralizada, que funcionará en el Centro de Monitoreo de Seguridad ubicado en el piso 11º.
- Los componentes del sistema deben poseer algún tipo de Certificación de manera que permita asegurar que cumplen y han sido elaborados bajo estándares de la industria.
- Debe registrarse tanto la entrada como salida del personal que accede a los pisos donde se instalaran las facilidades de control de acceso.
- Se instalarán lectores de tarjetas de proximidad, para registrar la entrada y salida, y comandar la apertura de puertas en los halles.
- En las puertas de entrada al centro de datos, a la oficina del archivo central, a la de manejo de valores y efectivo, así como a la del centro de monitoreo se instalaran facilidades de control de acceso biométrico, con la finalidad de brindar mayor seguridad, dado que estas zonas posee elementos o recursos críticos para la institución.
- En todas las puertas se instalarán cerraduras del tipo electromagnéticas, cuya activación o desactivación será comandada por los Módulos Controladores distribuidos en el edificio. Estas cerraduras permitirán que cuando la puerta este cerrada, y ante la denegación de acceso de un usuario por el sistema, la puerta se mantenga asegurada. En el caso que puerta abierta, no se establece aseguramiento.
- Cuando el usuario presente su tarjeta de proximidad, en el lector asociado a una puerta, el lector transferirá los datos de identificación del usuario, hacia el módulo de Interfaz para Lector que corresponda, el cual a su vez efectuara una transacción hacia el módulo Controlador Inteligente de Sistema ISC. En este módulo se efectuará el proceso de búsqueda en su memoria incorporada, donde se almacenan las configuraciones de acceso y permiso para todos los usuarios. El ISC ejecuta su programa de verificación de atributos (código, comparación de huella, etc.) correspondiente a la identificación, y produce el comando de concesión o denegación de apertura, hacia el módulo Controlador de Salidas (OM), el cual emitirá las señales eléctricas para que los dispositivos asociados

realicen la apertura o aseguramiento de la puerta: (lector de tarjeta de proximidad, lector biométrico, cerradura electromagnética). Asimismo el módulo ISC transferirá al hardware servidor de Administración los datos concernientes al evento procesado.

- La Infraestructura requerida esta basada en Módulos controladores ubicados en los mismos pisos en donde se ubican las puertas que se desean controlar. Se consideraran 4 tipos de módulos:
  - Controlador Inteligente del Sistema (ISC)
  - Controlador de Entradas (IM)
  - Controlador de Salidas (OM)
  - Interfase para lector(RI)
- El ISC, se encargará de comunicarse con otros controladores mediante comandos u ordenes, para que realicen la operación de apertura o aseguramiento de las puertas. También se encargará, del almacenamiento en memoria no volátil, de información relativa a los códigos de identificación de usuarios y permisos asignados para cada puerta del Sistema. Asimismo, realizará la correspondiente lectura y escritura en la memoria, de los eventos de apertura relacionados a los códigos de identificación detectados en los lectores de tarjetas, y la transferencia de información hacia el servidor de Administración.
- Los otros tipos de controladores, se encargarán de controlar los estados de operación de cierto número de puertas, relativos a las señales de supervisión generadas por dispositivos detectores instalados en las puertas, y a la emisión de señales eléctricas necesarias para la actuación de los dispositivos que intervienen en la apertura de puertas.
- La arquitectura del sistema debe estar basada en módulos controladores pudiendo ser del tipo Distribuida o Integrada, esta definición esta referida a los módulos controladores ISC.
- La Arquitectura Distribuida esta compuesta de Paneles de Control que incluyen dentro de un solo elemento las funcionalidades de controlador ISC, del Controlador de Entradas ICM, y de los módulos de Salida OM, y de la interfaz para lectoras (RI). Los paneles de control se instalarán en cada piso donde existan puertas a controlar, y se conectarán al hardware servidor de Administración del sistema, de manera redundante, mediante bus de interfaz RS 485 o RS 422, y por red LAN Ethernet.
- La arquitectura Integrada se componen de: Controlador de entradas (IM), Controlador de Salidas (OM) y de Interfaz para Lector de Tarjetas (RI), que se

instalarán en cada piso, con capacidad para controlar la cantidad de puertas requeridas en el piso correspondiente. Completa la arquitectura Integrada, un módulo Controlador Inteligente de Sistema ISC, al cual se conectarán los módulos mencionados en primer lugar, mediante bus de interfaz RS 485 o RS 422. El módulo ISC, se instalará en el segundo piso, y se conectará al hardware servidor de Administración del Sistema, de manera redundante, mediante bus de interfaz RS 485 o RS 422, y por red LAN Ethernet.

- El Software de administración centralizada, permitirá registrar los eventos de ingresos, salidas o intrusiones, y registros de personas identificadas en los accesos. Asimismo, el sistema permitirá o denegará el desbloqueamiento de una puerta bloqueada, basado en criterios establecidos a los usuarios de tarjetas de proximidad y lector biométrico.
- El sistema permitirá el desbloqueamiento programado de puertas individuales durante período de tiempo seleccionable, para cubrir casos que requieran acceso general.
- Sobre el marco superior de cada puerta de hall, por el lado de batimiento de la hoja, se instalará un detector de presencia por luz infrarroja, del tipo denominado "Request to Exit" REX. El funcionamiento de este dispositivo, será configurado para evitar que la puerta, al ser abierta desde el lado en que el marco la retiene, pueda impactar a una persona posicionada en el lado de batimiento. Mediante este recurso, se establecerá funcionamiento a puertas cerradas en todos los halles de pisos, permitiendo la salida de personas, en condiciones seguras, y manteniendo logrados los objetivos del control de acceso.
- El dispositivo REX, al detectar la presencia de una persona, accionará un contacto de relé, que inhibirá momentáneamente la apertura de puerta, si es que en ese momento alguien intenta salir, mediante presentación de tarjeta, desde el otro lado. Simultáneamente, se emitirá señal sonora de alerta a la persona, para que se retire del umbral de la puerta. La persona que presentó tarjeta, reconocerá por la inhibición del comando de apertura, que alguien se encuentra en el otro lado de la puerta, y esperará cantidad prefijada de segundos, al cabo de los cuales la inhibición cesará, y procederá a empujar la puerta con cuidado y observando por el ángulo de apertura, de modo de no causar daño a la otra persona.
- Cada puerta, por su lado interior, llevará instalado pulsador de apertura para caso de emergencia, en posición cercana al marco de la puerta, y protegido por cobertura de vidrio. Al ser presionado, este pulsador, enviará señal al controlador

local, el cual a su vez comandará la apertura de la cerradura electromagnética. Esta alternativa de apertura es necesaria para permitir la salida de personas en casos extraordinarios, como de evacuación por situación de emergencia, o de extravío de la tarjeta de proximidad.

- Se proveerá seguridad de operación a cada puerta, aun en evento de corte de la comunicación con el hardware servidor de Administración del Sistema, permitiendo que se continúe con el reconocimiento de tarjetas, concesión/denegación de accesos, y almacenamiento de la información de transacciones
- En el caso de aplicar arquitectura Integrada, se proveerá como repuestos, uno de cada tipo de los siguientes módulos instalados: Controlador de entradas (IM), Controlador de Salidas (OM) y de Interfaz para Lector de Tarjetas (RI). Además, el módulo ISC se proveerá en configuración redundante.
- En el caso de aplicar la Arquitectura Distribuida, se proveerá un Panel de Control equipado con la capacidad máxima instalada, para ser usado como repuesto.
- Los módulos controladores se instalarán en gabinetes metálicos cerrados con llave. Los módulos tendrán capacidad para señalizar hacia el sistema Administrador, eventos de apertura forzada del gabinete o de status anormal de los circuitos de conexión hacia los dispositivos asociados a la operación de las puertas.
- La alimentación de energía para los módulos Controladores, se proveerá mediante rectificador/cargador, para conversión del suministro comercial de 220VAC al valor de tensión continua con que operan los circuitos internos, y que posibilite el funcionamiento de batería electrolítica, para brindar autonomía de 12 horas de funcionamiento.
- Los equipos que se utilicen para brindar las facilidades de control de acceso deberán poder registrar los eventos de manera que se pueda realizar auditoria a través del software de control de accesos, esta auditoria debe permitir identificar a las personas, por hora de ingreso, hora de salida, etc.
- Las puertas deben estar aseguradas con cerraduras de tipo electromagnéticas, de manera que en condiciones de normal funcionamiento se mantenga cerrada la puerta si el acceso no fue validado. La operación en caso de siniestro debe ser de apertura.

5.2.2 respecto a los componentes software

- El software Administrador del Sistema de Control de Acceso permitirá la administración centralizada de los eventos de ingresos, salidas o intrusiones y el

registro de personas identificadas en los accesos. Permitirá configurar el acceso del personal autorizado:

- A una puerta o grupo de puertas especificas
- Por rango de horas o días de la semana.
- Detectar cuando un personal autorizado esta fuera del rango de horas de acceso a la instalación configuradas en su tarjeta, reportando de manera inmediata este evento (alarma en el software de administración remota).
- Debe contar con funcionalidad "Antipassback", es decir que pueda comandar a un controlador, para que sea rechazado el ingreso mediante tarjeta a alguna puerta, cuando tal tarjeta haya sido usada previamente, en el ingreso a una puerta, en la cual no se haya registrado salida asociada a esa misma tarjeta.

- Debe permitir el registro en línea de los accesos a través del controlador principal, los cuales deben almacenarse en la base de datos del servidor. Mediante consultas al(los) módulo(s) software de manejo de Base de datos, se podrá:
  - Conocer los accesos realizados en una área especificada en tiempo real (opcionalmente muestra la ubicación de la persona en un gráfico del edificio) a través de la interfase del software, y emitir alarmas para los diversos eventos (equipo malogrado, batería agotada, puerta abierta, etc.) que se generen en los accesos.
  - Realizar reportes: de Accesos y permanencias, de Accesos Denegados, Accesos por áreas, eventos anómalos, por tipo de usuario. Estos reportes deben ser personalizables de manera que se puedan realizar filtros a los datos que se deseen reportar.
- El sistema debe incluir un módulo de administración de visitas que permita:
  - Registrar como mínimo el Tipo de documento, el número de documento, los nombres (prenombres y apellidos), trabajador a quien visita, hora y fecha de visita, y motivo de visita.
  - Configurar las tarjetas con los respectivos permisos de acceso para ser asignados a un visitante de modo que el visitante tenga acceso únicamente al área autorizada.
  - Reportar todas las actividades de los visitantes.

5.2.3 respecto al soporte de recursos informáticos

- El software de administración del Sistema, se instalará en hardware servidor, existente en el centro de cómputo ubicado en el segundo piso del edificio. La

implementación del Sistema incluirá una estación de trabajo para las labores de administración del Sistema. Esta estación de trabajo se instalará en el centro de monitoreo de Seguridad, ubicado en el piso 11º. El esquema de funcionamiento cliente-servidor, que aplicará el software del Sistema, se soportará en la red Ethernet existente en el edificio.

- El sistema permitirá el acceso por una puerta de hall cualquiera, mediante la presentación de tarjeta, sólo a cantidad limitada de personas, las cuales estarán directamente involucradas en la realización de funciones específicas de la unidad orgánica correspondiente. El resto de personas no podrá realizar la apertura de la puerta con la presentación de tarjeta al lector de proximidad, por lo que deberá solicitar a alguna persona que labora en el ambiente protegido, que lo haga por ella. Para tal propósito utilizaran los aparatos telefónicos IP inalámbricos que se encuentran en cada piso a ser controlado.
- La utilización de la red LAN inalámbrica para soporte al funcionamiento de teléfonos IP inalámbricos, permitirá la actuación del personal de Seguridad, en permanente coordinación con el centro de administración del Sistema, que funcionará en el piso 11º. Ello será necesario para la solución de eventos relacionados con la operación de las puertas y en aplicación de procedimientos de seguridad que se establecerán. La coordinación telefónica, móvil, de carácter automático, selectivo, privado, con cobertura en los pisos bajo acceso controlado, y conectividad hacia anexos de oficinas, servirá de apoyo a la toma de acción en eventualidades tales como: atrapamiento de personas, intrusión detectada, vigilancia durante aperturas de duración programada, intervención de personas con recorrido sospechoso, supervisión de funcionamiento y corrección de problemas técnicos.

5.3 alternativas de solución

Como se ha indicado en los requerimientos anteriores, si bien se han definido aspectos tanto de hardware como software, que deberían componer la solución, sin embargo la selección de la tecnología biométrica elegida, aun no ha sido determinada, y es en este ítem que se realiza el análisis para determinar la tecnología mas conveniente para la presente propuesta:

TABLA Nº 5.2. Características de diferentes modalidades biométricas [22,65,66]

Descripción	**Comparación 1 a 1 / 1 a N**	**Variación A lo largo de la vida/ día a día**	**Máxima numero de muestras independientes por persona**	**Costo Relativo del Lector Biométrico**	**Tamaño del Lector**
Huella	SI/SI	Ninguna/poca	10	10-100	Muy pequeña
Rostro	SI/NO	Mucho/medio	1	100	pequeño
Iris	SI/SI	Ninguna/muy poca	2	100-1000	Medio
Mano	SI/NO	Mucho/muy poca	2	100	Medio

Según la TABLA Nº 5.2. Huella dactilar, iris y geometría de la mano representan 3 de los indicadores biométricos que presentan poca variación de sus características, representando muy favorables para ser utilizadas como medios de identificación.

TABLA Nº 5.3. Comparación de tecnologías biométricas según características. [22]

Biometría	Huella	Rostro	Iris	Mano
Universalidad	Medio	Alta	Alta	Medio
Unicidad	Alta	Bajo	Alta	Medio
Permanencia	Alta	Medio	Alta	Medio
Cuantificación	Alta	Alto	Medio	Alto
Performance	Alta	Bajo	Alta	Medio
Aceptabilidad	Medio	Alto	Bajo	Medio
Fiabilidad	Alta	Bajo	Alto	Medio

Según la TABLA Nº 5.3 se observa que la huella dactilar y el iris presentan los índices más altos de calificación. Esto nos indica que ambas biometrías potencialmente pueden ser utilizadas como medios de identificación. Sin embargo es necesario considerar que las soluciones de control de acceso usando el iris pueden representar un rechazo por parte de los usuarios que pueden considerar que estas pueden dañar su vista, así mismo la fase de captura de las muestras del iris puede llegar a tomar mas tiempo que su contraparte basada en huellas dactilares, ya que el sistema de captura necesita posicionar la imagen del iris de manera que se obtenga una muestra de buena calidad para efectuar la comparación biométrica. Otro factor a considerar consideración a tomar en cuenta es sobre la cuantificación de las muestras, dado que un ser humano posee 10 dedos, es muy fácil poder enrolar otro dedo en forma alternativa si esta ausente o incluso enrolar todos los dedos de las manos, de manera que se al presentarse mayor numero de muestras se incremente la identificación sea mas precisa.

Finalmente los equipos de captura de iris poseen un costo más elevado que el de captura dactilar. Por las consideraciones anteriores se ha seleccionado la alternativa dactilar como la más adecuada para la presente propuesta.

5.4 descripción de la solución

Dado los requerimientos definidos en el ítem 5.1, se ha determinado el número de componentes de la solución se detallan a continuación.

5.4.1 equipamiento requerido

Se detalla a continuación los componentes mínimos para la solución de control de acceso propuesta:

TABLA Nº 5.4. Descripción del equipamiento requerido para la solución de control de acceso. [65,66]

Descripción	Cantidad
Controlador Principal	02
Interfase de Control de Lectoras de Tarjeta	45
Lectores de Tarjeta / Lector Biométrico	90
Fuentes de Energía	45
Baterías	47
Cerraduras Electromagnéticas	45
Contactos Magnéticos	45
Servidor Principal	01
Software de Control y Administración	01
UPS	01
Computadora Personal	01
Impresora	01

5.4.2 análisis de costos

A continuación se presentan los costos promedio del equipamiento incluido en la solución de control de acceso.

TABLA Nº 5.5. Costo Unitario y Total del equipamiento que compone la solución. 65,66]

Descripción	Cantidad	Costo Unitario($)	Costo Total($)
Controlador Principal	01	2500	2500
Interfase para Lectores	14	500	7000
Lector Biométrico	10	1200	12000
Lectores de Tarjeta de proximidad	18	200	3600
Tarjeta de proximidad para usuarios	100	2.5	250
Cerraduras Electromagnéticas	14	350	4900
Software Administrador de Control de Acceso	01	3800	3800
Detector de presencia por luz infrarroja REX	06	200	1200
Pulsador de Salida	14	50	700
Sensor de puerta abierta	14	50	700
Cierra puerta hidráulico	14	100	1400
UPS	01	800	800
PC administración del Sistema e impresora	01	3800	3800
Fuente de Energía para Controlador Principal	01	25	25
Fuente de Energía para Interfase de Lector de Tarjetas y lectores Biométricos	15	25	375
Conversor RS232 a RS485	01	400	400
Gabinete	01	250	250
Baterías 7AH/12 VDC	15	25	725
Gabinete para fuentes	15	16	240
			44,665

A continuación se indican los costos relacionados al diseño y planos de la solución, y los trabajos de instalación y supervisión.

TABLA Nº 5.6. Costo Total por diseño, instalación y puesta en funcionamiento del sistema[65,66]

Descripción		Costo Unitario ($)	Costo Total($)
Ingeniería	Ingeniería de diseño y planos	3500	3500
Instalación y Supervisión	Instalación y mano de obra , incluye materiales, canaletas, uniones, herramientas, accesorios de montaje	12000	12000
	Supervisión del proyecto		
	Instalación del sistema de control de accesos		
	Programación de dispositivos, pruebas		
	Configuración del Software de Administración		
	Puesta en Servicio		
	Capacitación		
			15,500

TABLA Nº 5.7. Costo Total de la solución incluyendo diseño, puesta en funcionamiento del sistema, capacitación y componentes electrónicos y mecánicos y electromecánicos de la solución. 65,66]

Descripción	Costo Total($)
Componentes de la Solución de CA	46,665
Diseño, instalación y puesta en funcionamiento del sistema	15,500
	62,165.

CONCLUSIONES Y RECOMENDACIONES

A continuación se indican las conclusiones del Informe

- Los sistemas biométricos presentan mayor ventaja frente a otros sistemas de verificación de identidad como: usuario y password o utilización de tarjeta.
    - Ya que estos se pueden perder
    - Se pueden olvidar
    - O pueden ser robados para ser usados en accesos fraudulentos.
- La identificación personal biométrica no es transferible
- Al adoptar una solución de control de acceso biométrico los costos de administración asociados a las tarjetas son eliminados.
- Existe una alta aceptación por parte del usuario a estos medios de comprobación de su identidad, unos más que otros.
- La combinación de 2 o 3 de los métodos de identificación mencionados en el punto anterior permiten incrementar los niveles de seguridad y control, esto es lo que se denomina fusión de biometrías.
- La utilización de 2 o más muestras biométricas utilizadas para la validación de la identidad permite también incrementar el nivel de exactitud del sistema.
- Los sistemas de control de acceso electrónico permiten el monitoreo y registro de las actividades de los individuos cuando acceden a las instalaciones y es un herramienta eficaz para las tareas de seguridad y control.
- El éxito de una implementación de control de acceso esta influenciado por la adopción de la tecnología que presente los mayores beneficios en cuanto a aceptabilidad, universalidad, cuantificable, etc.
- La biometría de dactilar presenta mayores ventajas respecto de otras biometrías, respecto al número de muestras disponible de utilizar para la verificación de los usuarios.
- En la autenticación por reconocimiento de iris, la adquisición resulta a veces complicada ya que el usuario debe ser muy cooperativo y la iluminación muy específica.

- En el reconocimiento de rostros existe la problemática múltiple: tipo de iluminación, variabilidad del fondo de la imagen, posición/rotación del rostro, distorsión del objetivo/captador empleado, etc.
- Así mismo existe variabilidad del rostro: paso del tiempo, uso de gafas, uso de maquillaje, barba/bigote/patillas, piercing, peinado, tintes, lentillas estéticas, colgantes, pendientes y diademas, etc. que disminuyen la performance del sistema.
- En el reconocimiento por geometría de la mano que factores tales temperatura y condiciones medicas pueden afectar el tamaño de la mano con lo cual puede resultar en un incremento del numero de falsos rechazo.
- El reconocimiento por rostro puede presentar desventaja y aun puede perder efectividad si es que no se encuentra restringido por ciertos parámetros, edad, cambios en el color del cabello, cambios físicos en la apariencia del rostro, cabeza con recubrimientos (sombreros, capuchas, mascaras, etc.) los cuales pueden afectar los resultados.

A continuación se indican las recomendaciones del Informe

- Evaluar la posibilidad de Integrar el sistema propuesto con sistemas complementarios de CCTV.
- Realizar periódicamente evaluaciones a los registros de auditoria para determinar comportamientos anómalos o posibles amenazas a la seguridad de las instalaciones a controlar.
- Implementar sistemas redundantes de control de acceso.
- Realizar el mantenimiento preventivo de los equipos y dispositivos que componen la solución de manera que su operación no se vea interrumpida por desperfectos detectados durante su operación.
- Incrementar el numero de dedos o huellas utilizadas para la autenticación frente al sistema, esto permite tener una mayor certeza e incrementa el abanico de posibilidades para una autenticación por huella cuando no este presente una muestra o no pueda ser utilizada para la verificación (cortes profundos o heridas, amputaciones, etc.)
- Evaluar la incorporación dentro de lo lectores biométricos utilizados en la implementación de técnicas de verificación del dedo vivo, con la finalidad de disminuir la posibilidad de fraude o intentos de fraude al sistema.
- Evaluar la posibilidad de combinar 2 o mas tipos de biometrías con la finalidad de verificar si puede mejorar o incrementarse los niveles de seguridad.

BIBLIOGRAFÍA

1. Tamura, H. , "A comparison of line thinning algorithms from digital geometry viewpoint". Conf. on Pattern Recognition – USA, 1978.
2. M. Kawagoe and A. Tojo, "Fingerprint Pattern Classification, Pattern Recognition", 1984.
3. Ren Qun, Tian Jie, Zhang Xiaopeng, "Automatic Segmentation of Fingerprint Images", Chinese Academy of Sciences, P.R. China, 1995.
4. Amengual, J. C., Juan, A., Prez, J. C., Prat, F., Sez, S., and Vilar, J. M. "Real-time minutiae extraction in fingerprint images". 6th Conf. on Image Processing and its Applications-USA, 1997.
5. Raffaele Cappelli, Alessandra Lumini, Dario Maio,"Fingerprint Classification by Directional Image Partitioning", IEEE,1999.
6. Arun Ross, Anil Jain and Jian-Zhong Qian, "Information Fusion in Biometrics", Michigan State University, Siemens Corporate Research- USA, 2001.
7. Anil Jain, Arun Ross, Salil Prabhakar,"FINGERPRINT MATCHING USING MINUTIAE AND TEXTURE FEATURES", Conference on Image Processing, Thessaloniki, Greece, 2001.
8. Salil Prabhakar,"Fingerprint Classification and Matching Using a Filterbank"- Computer Science & Engineering, Michigan State University, USA, 2001.
9. Virginia Espinosa-Duró, "Minutiae Detection Algorithm for Fingerprint Recognition", Electronic and Automatic Department, Universidad Politecnica de Catalunya – España, 2001.
10. Shlomo Grecnberg, Mayer Aladjem, Daniel Kogam and Itshak Dimitriv, "Fingerprint Image Enhancement using Filtering Techniques", Electrical and Computer Engineering Department, Ben-Gurion University of the Negev, Beer-Sheva- Israel, 2001.
11. Yuan Yao, Paolo Frasconi, and Massimiliano Pontil, "Fingerprint Classification with Combinations of Support Vector Machines", University of Hong Kong, University of Firenze, University of Siena, Italy. 2001.

12. LinLin Shen, Alex Kot, WaiMun Koo, "Quality measures of fingerprint images", School of Electrical and Electronic Engineering Nanyang Technological University Singapore-2001.
13. Michael Yi-Sheng Yao, Sharath Pankanti, Norman Haas, Nalini Rataha, Rund M. Boile, "Quantifying Quality: A Case Study in Fingerprints". IBM T J Watson Research Center Yorktown Heights. USA, 2001.
14. García Ortega Víctor Hugo, "SISTEMA DE RECONOCIMIENTO DE HUELLAS DACTILARES PARA EL CONTROL DE ACCESO A RECINTOS", Instituto Politécnico Nacional – MEXICO, 2001.
15. Domingo Morales L. Javier Ruiz-del-Solar, "SISTEMAS BIOMÉTRICOS: MATCHING DE HUELLAS DACTILARES MEDIANTE TRANSFORMADA DE HOUGH GENERALIZADA", CHILE – 2001.
16. Elaine M. Newton, with John D. Woodward, "BIOMETRICS: A TECHNICAL PRIMER". USA, 2001.
17. Arun Ross, James Reisman, Anil Jai, "Fingerprint Matching Using Feature Space Correlation", Michigan State University and Siemens Corporate Research – USA, 2002.
18. A. J. Mansfield, National Physical Laboratory and J. L. Wayman,"Best Practices in Testing and Reporting Performance of Biometric Devices" Version 2.01 - , San Jose State University – USA, 2002.
19. Alfredo C. López, Ricardo R. López, Reinaldo Cruz Queeman,"Fingerprint Recognition", Electrical Engineering Department - Polytechnic University, Puerto Rico, 2002.
20. Neo TEC, "Comparación de Plantillas de Huella Digital Basadas en Minucias vs. Basadas en Patrones", http://www.neotec.com.pa/html/comoyporque.htm, Panamá, 2002.
21. Anil K. Jain, Arun Ross, "Learning user-specific parameters in a multibiometric system", Department of Computer Science and Engineering Michigan State University, East Lansing – USA, 2002.
22. Anil Jain, Ruud Bolle, Sharath Pankanti, "Biometrics, Personal Identification in Networked Society". Michigan State University - USA, 2002.
23. Raymond Thai, "Fingerprint Image Enhancement and Minutiae Extraction", School of Computer Science and Software Engineering, the University of Western Australia 2003.

24. D. Maltoni, D. Maio, A.K. Jain, S. Prabhakar, "Fingerprint Scanners and their Features", Handbook of Fingerprint Recognition - USA, 2003.
25. María Íñiguez Gómez, Emiliano Bernués del Río, Isabel Gil Lorente, "Aplicación para control de acceso mediante reconocimiento facial". Centro Politécnico Superior, Grupo de Tecnologías de las Comunicaciones. Departamento de Electrónica y Comunicaciones. Universidad de Zaragoza-ESPAÑA, 2003.
26. Elaine M. Newton, with John D. Woodward, "BIOMETRICS: A TECHNICAL PRIMER"- USA, 2003.
27. Peter Komarinski. Elvesier Academic Press. "Automated Fingerprint Identification Systems (AFIS)".
28. Ajay Kumar, David C. M. Wong, Helen C. Shen1, Anil K. Jain, "Personal Verification using Palmprint and Hand Geometry Biometric", Department of Computer Science, Hong Kong University of Science and Technology, Pattern Recognition and Image Processing Lab, Department of Computer Science and Engineering Michigan State University, East Lansing, 2003.
29. Jianwei Yang, Lifeng Liu, Young Fan, "A modified Gabor filter design method for fingerprint image enhancement". National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Science, Beijing, China, 2003.
30. Sanghoon Lee, Jaihie Kim. "Model-Based Quality Estimation of Fingerprint Images". Biometrics Engineering Research Center (BERC) Department of Electrical and Electronic Engineering. Yonsei University, Seoul Korea, 2003.
31. Sarat C. Dass, Anil K. Jain,"Fingerprint Classification Using Orientation Field Flow Curves", Michigan State University – USA, 2003.
32. SGIT, "INFORME TÉCNICO Nº 0009, Implementación de un Sistema Automático de Identificación de Impresiones dactilares de Gran Escala", (Large Scale AFIS), -Peru, 2003.
33. Sen Wang Wei Wei Zhang Yang Sheng Wang,"Fingerprint Classification by Directional Fields". National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, China, 2003.
34. Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition". IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY - USA, 2004.

35. Fernando Martín, Francisco Suárez, "IDENTIFICACION BASADA EN FILTROS DE GABOR", Departamento de Teoría de la Señal y Comunicaciones, Universidad del Vigo – España, 2004.
36. SIEMENS SWITZERLAND Ltd. Access Control SiPass Products & accessories, Catalogue 2004. 40pp. Mannendorf – Switzerland, 2004.
37. Arun Ross, Anil Jain, "Biometric Sensor Interoperability: A Case Study In Fingerprints", West Virginia University, Michigan State University-USA, 2004.
38. Muhammad Umer Munir and Muhammad Younas Javed, "Fingerprint Matching using Gabor Filters". College of Electrical and Mechanical Engineering, National University of Sciences and Technology, Rawalpindi, Pakistan, 2004.
39. Artzai Picón Ruiz, "El futuro de las tecnologías biométricas: Identificación colaborativa", ROBOTIKER-TECNALIA, Unidad INFOTECH – España, 2004.
40. Raffaele Cappelli, Dario Maio and Davide Maltoni, "Technology evaluations of fingerprint-based biometric systems". Biometric System Lab - DEIS, University of Bologna - Italia, 2004.
41. Elham Tabassi, Charles L. Wilson, Craig I. Watson, "Fingerprint Image Quality - NISTIR 7151"- USA, 2004.
42. Kaoru Uchida,"Detection and Recognition Technologies, Fingerprint Identification", NEC Secure Finger, USA, 2005.
43. Marios Savvides, "Introduction to Biometric Recognition Technologies and Applications". Carnegie Mellon CyLab & ECE – USA, 2005.
44. Anil K. Jain, Sarat C. Dass, "Fingerprint Classification Using Orientation Field Flow Curves", Michigan State University – USA, 2005.
45. Chris Roberts, "BIOMETRICS", Centre for Critical Infrastructure Protection, Nueva Zelandia, 2005.
46. BOSCH, Security Systems, Módulo de control de acceso de puerta (DACM), 2005.
47. Raffaele Cappelli, Dario Maio and Davide Maltoni. "TECHNOLOGY EVALUATIONS OF FINGERPRINT-BASED BIOMETRIC SYSTEMS", Biometric System Lab - DEIS, University of Bologna, Cesena – Italia, 2005.
48. Elham Tabassi, "NIST Fingerprint Image Quality", Biometric Consortium Conference - USA, 2005.

49. Yi Chen, Sarat Dass, and Anil Jain, "FINGERPRINT QUALITY INDICES FOR PREDICTING AUTHENTICATION PERFORMANCE". Department of Computer Science and Engineering Michigan State University, East Lansing 2005.
50. NORTH CAROLINA STATE UNIVERSITY. "ON LINE Access Control Specifications" – Washington D.C., USA, 2005.
51. Aparecido Nilceu Marana, Anil K. Jain, "Ridge-Based Fingerprint Matching Using Hough Transform", UNESP – Faculdade de Ciências – Departamento de Computação and Michigan State University – College of Engineering. - Brasil, 2005.
52. Yi Chen, Sarat Dass, and Anil Jain "Fingerprint Quality Indices for Predicting Authentication Performance", Michigan State University, 2005.
53. F. Javier Alvaro. "Sistemas de Control de Acceso, Informatización e Integración".Demes, S.L. España, 2006.
54. Alessandro L. Koerich, "Sistemas Biométricos", IEEE Computer Society Distinguished Visitors Program Lecture, 3er Congreso de Electrónica, Robótica y Mecánica Automotriz (CERMA) Cuernavaca, Morelos, México, 2006.
55. Chih-Jen Lee, Tai-Ning Yang, I-Horng Jeng, Chun-Jung Chen, and Keng-Li Lin, "Singular Points and Minutiae Detection in Fingerprint Images Using Principal Gabor Basis Functions", Department of Computer Science Chinese Culture University - Taiwan, 2006.
56. Jhon Archila, Diego Tibaduiza, Luz Jiménez, "IMPLEMENTACIÓN DE UN SISTEMA DE CONTROL DE ACCESO E ILUMINACIÓN". Facultad de Ingeniería Mecatrónica, Universidad Autónoma de Bucaramanga, Colombia, 2006.
57. NIST Biometric Quality Workshop. "HUMAN VISUAL PERCEPTION MODEL FOR MEASURING FINGERPRINT IMAGE QUALITY". Department of Defense, Biometrics Management Office-USA. 2006.
58. UNIVERSITY OF WINSCONSIN – MADISON POLICE DEPARTMENT. Access Control and Access Cards. 5pp. Board of Regents of the University of Winsconsin System. Madison, Winsconsin-USA, 2006. http://www.uwpd.wisc.edu/Access%20Cards%20and%20Control.html
59. BOSCH SECURITY SYSTEMS. LNL-500 Intelligent System Controller. Fairport, New York, USA, 2006.

60. National Science and Technology Council (NSTC), "Fingerprint Recognition", USA, 2006.
61. National Science and Technology Council (NSTC), "Iris Recognition", USA, 2006.
62. National Science and Technology Council (NSTC), "Speaker Recognition", USA, 2006.
63. Denis Speicher, "Vulnerability Analysis of Biometric Systems Using Attack Trees", Lane Department of Computer Science and Electrical Engineering Morgantown, West Virginia – USA, 2006.
64. Anil K. Jain, "Biometric System Security", Dept. of Computer Science and Engineering, Michigan State University - USA, 2006.
65. Subgerencia de Innovación Tecnológica, "SISTEMA DE CONTROL DE ACCESO ELECTRÓNICO", RENIEC – 2006.
66. Subgerencia de Innovación Tecnológica,"Especificaciones Técnicas del SISTEMA DE CONTROL DE ACCESO ELECTRONICO PARA LAS INSTALACIONES DE LA SEDE ADMINISTRATIVA DEL RENIEC", RENIEC – 2006.
67. Software House, "apC/8X Advanced Processing Controller, Manual"- USA, 2006.
68. WP6, "Forensic Implications of Identity Management Systems", FIDIS Consortium (Future of Identity in the Information Society), Europe, 2006.
69. Andover Continuum TM Product Catalogue"- USA, 2007.
70. TDSi TIME AND DATA SYSTEMS INTERNATIONAL, "Feature Lists for eXcel and eXpert Access Control Systems, and for eXguard PRO Administrator software".Doorset, Oregon, USA. http://www.tdsi.co.uk/es/about_access.htm
71. Hoja Técnica de los Controladores iSTAR, Software House, 2007.
72. Zeno Geradts (NFI, the Netherlands), Peter Sommer (LSE, UK). FIDIS consortium (Future of Identity in the Information Society). "Forensic Implications of Identity Management Systems".
73. Dr. Marios Savvides, "Introduction to Biometric Recognition Technologies and Applications", Carnegie Mellon CyLab & ECE, USA 2007.
74. Stephanie Schuckers, PhD Larry Hornak, PhD Tim Norman, PhD Reza Derakhshani Sujan Parthasaradhi, "Issues for Liveness Detection in Biometrics", Center for Identification Technology Research, West Virginia

University, Michigan State University, Marshall University, San Jose State University - USA, 2007.

75. SIASA, Sistemas Integrales de Automatización, Catalogo: "Sistemas de Control de Acceso", México, 2007.
76. TDSI, "Simplifying the Approach to Access Control", 2007.
77. Syscom,"Curso de Control de Acceso" http://www.syscom.com.mx/PPT/control_acceso.pdf , México, 2007.
78. Recognition Systems," Hand Punch Datasheet".
79. Bioscrypt, "VStation Datasheet".
80. A4 Vision, "VISION ACCESS - 3D FACE READER datasheet".
81. Iridian Technologic, "Biometric Comparison Guide".
82. Reco, "Electric Strikes Datasheet"
83. HID Corporation, "HID MFARE Reference Guide".
84. Kantech, "Request to Exit Detector, Data Sheet".
85. Rutherford Controls, "Hoja Técnica Condensada, Quick Systems".
86. INDALA, "FlexPass Datasheet".
87. Zebra Electrónica, "CERRADURA MAGNETICA DE ENTRABAMIENTO".
88. YALE, "Cierrapuertas Serie 2000, Datasheet".
89. INCITS, http://www.incits.org
90. ISO, http://www.iso.org
91. NIST, "American National Standard for Information Systems— Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information".
92. Plataforma Biométrica Homlni, http://www.homini.com/tecnologías.htm
93. Biometric Group, "Biometric Market Report", http://www.biometricgroup.com/reports/public/market_report.html
94. Anil Jain , Sharath Pankanti,"Fingerprint Classification and Matching", Michigan State University and IBM T. J. Watson Research Center