Universidad Nacional Autónoma de México

Facultad de Ingeniería

“Automatización del proceso de control de asistencia del personal académico en tiempo real a través de reconocimiento biométrico”.

TESIS

QUE PARA OBTENER EL TÍTULO DE:

INGENIERO MECÁNICO Y ELECTRICISTA

PRESENTA:

ALEJANDRO OLIVARES MORALES

DIRECTOR DE TESIS:

M. EN I. JORGE VALERIANO ASSEM

CIUDAD UNIVERSITARIA MARZO 2010

INDICE

ANTECEDENTES

La Facultad de Ingeniería cuenta con varios puntos de control donde el personal académico debe registrar su ingreso y egreso para comprobar su asistencia a sus labores, para ello se utiliza un kardex que registra la hora de entrada y salida del mismo. Cada cierto periodo de tiempo esta información se recopila, se captura y se emite un reporte el cual permitirá emitir el pago correspondiente por concepto de prestación de servicios.

Esta actividad se realiza actualmente de manera manual lo cual implica que exista la posibilidad de tener diferentes tipos de errores u omisiones. Asimismo el registro manual de asistencia sin validación automática, permite que el registro de entrada o salida sea efectuado por una persona diferente a la persona que debe realizar el registro.

Mediante un registro de este tipo los responsables de área no tienen visibilidad de la asistencia o no del personal académico, no se pueden tomar decisiones de manera inmediata a fin de cubrir alguna ausencia y se corre el riesgo de realizar pagos de nómina de manera inadecuada.

CONTEXTO:

El control de asistencia del personal docente resulta una tarea indispensable que va mas allá del pago de la nomina, involucra la profesionalización de esta noble tarea ya que al cumplir cabalmente con nuestras obligaciones la misma repercute asimismo de manera intangible en el nivel académico que se trasmite a los alumnos derivado del cumplimiento en tiempo y forma al cumplir con nuestros horarios de trabajo.

Aunque actualmente el alcance se limita a controlar el registro de entrada y salida del personal la solución podría expandirse a cada aula, laboratorio, o recinto que se desee controlar.

ALCANCE:

El control de asistencia a través de reconocimiento biométrico supera muchas de las desventajas de identificación automática con dispositivos convencionales como son: tarjetas de registro haciendo uso de reloj de checado, números de identificación personal (NIP), tarjetas de identificación (código de barras, banda magnética, tarjetas inteligentes, RFID, etc.) ya que verifica la identidad de la persona autorizada de manera positiva y definitiva con virtualmente 0% de error.

El registro de control de asistencia se ha vuelto por sí mismo una tarea que requiere de precisión en su captura y en la emisión de reportes fidedignos que permitan automatizar el área de recursos humanos.

El presente proyecto mejorará de manera notable la rapidez con la que se realizan estas actividades, además de que la precisión de la información estará garantizada por tratarse de un sistema en la que la identificación del personal será totalmente automática.

RELEVANCIA:

La realización de un proyecto que involucre sistemas de identificación automática, implicará dar un paso importante en la utilización de nuevas tecnologías en la Facultad de Ingeniería. Esto se sumará a otros esfuerzos que en el mismo sentido son realizados en distintas áreas y coadyuvará con el propósito de mantener nuestra Institución a la vanguardia en el uso de nuevas tecnologías, tal el caso de sistemas de control de inventarios, sistema de control de activos fijos, credencialización, control de estacionamientos, control de bibliotecas, etc.

CAPITULO I. SISTEMAS DE IDENTIFICACIÓN AUTOMÁTICA

INTRODUCCIÓN

Existen diferentes técnicas de captura de datos, como son la captura manual, el reconocimiento óptico, reconocimiento óptico de caracteres (OCR), cinta magnética, código de barras, tarjetas inteligentes (Smart Cards), RFID y a través de reconocimiento de características biométricas. El uso de cada uno de ellos depende en gran medida del proceso en particular que se desee automatizar, el objetivo principal de este trabajo será documentar cada uno de ellos con la finalidad de entender claramente su definición, ventajas y desventajas así como las aplicaciones comunes en las cuales se utilizan. Finalmente nos enfocaremos a automatizar una problemática real seleccionando de entre todas las opciones actuales de Identificación Automática de Captura de Datos (AIDC) por sus siglas en inglés (*Automatic Identification Data Capture,* la captura de información a través de características Biométricas que para la parte de registro de asistencia se considera la forma ideal de captura por su precisión e imposibilidad de suplantación de identidad.

I.1. Sistemas de código de barras.

I.1.1. Historia.

El Código de Barras es un arreglo en paralelo de barras y espacios que contiene información codificada en las barras y espacios del símbolo. Esta información puede ser leída por dispositivos ópticos, los cuales envían la información leída hacia una computadora como si la información se hubiera tecleado.

El primer sistema de código de barras fue patentado en Octubre 20, **1949** por Norman Woodland y Bernard Silver. Se trataba de un "blanco" (bull's eye code) hecho mediante una serie de círculos concéntricos. Una faja transportaba los productos a ser leídos por un foto detector..

LOS SESENTAS

1961 es el año de aparición del primer escáner fijo de códigos de barras instalado por Sylvania General Telephone. Este aparato leía barras de colores rojo, azul, blanco y negro identificando vagones de ferrocarriles.

Para **1967** la Asociación de Ferrocarriles de Norteamérica (EEUU) aplica códigos de barras para control de tránsito de embarques. El proyecto no duró mucho por falta de adecuado mantenimiento de las etiquetas conteniendo los códigos.

En **1967** la sucursal de Cincinnati (Ohio, EEUU) instala el primer sistema de "Retail" (Supermercados) basado en códigos de barras. Al cliente que encontraba un código que no se podía escanear correctamente se le ofrecía cupones de compra gratis.

1969, el láser hace su aparición. Usando luz de gas de Helio-Neón, el primer escáner fijo es instalado. Su costo: $10 000 USD. Hoy por hoy el mismo tipo de escáner estaría costando menos de $ 2,000 USD.

A fines de los años **60** y comienzos de los **70** aparecieron las primeras aplicaciones industriales pero slo para manejo de información.

En **1969,** Rust-Oleum fue el primero en interactuar un lector de códigos con una computadora. El programa ejecutaba funciones de mantenimiento de inventarios e impresión de reportes de embarque.

LOS SETENTAS

En **1970** aparece el primer terminal portátil de datos fabricado por Norand. Este utilizaba un "Wand" o lápiz de contacto.

El código Plessey hace su aparición en Inglaterra (The Plessey Company, Dorset, Inglaterra), para control de archivos en organismos militares en **1971**. Su aplicación se difundió para control de documentos en bibliotecas.

Codabar aparece en **1971** y encuentra su mayor aplicación en los bancos de sangre, donde un medio de identificación y verificación automática eran indispensables.

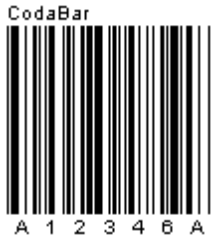

Figura I.1 Código Codabar

Buick (la fábrica de automóviles) utilizó identificación automática en las operaciones de ensamble de transmisiones, también por los años **70**. El sistema era utilizado para conteo de los diferentes tipos de transmisión ensamblados diariamente.

ITF marca su aparición en **1972**, creado por el Dr. David Allais, en ese entonces de Intermec (empresa dedicada a la fabricación y desarrollo de tecnología de captura de datos).

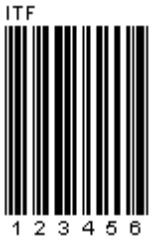

Figura I.2 Código ITF

En el año **1973** se anuncia el código U.P.C. (Universal Product Code) que se convertiría en el estándar de identificación de productos en Estados Unidos de Norteamérica. De esta forma la actualización automática de inventarios permitía una mejor y más oportuna compra y reabastecimiento de bienes.

En **1974**, Europa se hace presente con su propia versión de U.P.C., el código EAN (European Article Number), la asociación recibe el mismo nombre.

Figura I.3 Código UPC y EAN

En **1974**, nuevamente el Dr. Allais conjuntamente con Ray Stevens de Intermec inventa el código 39, el primero de tipo alfanumérico.

Figura I.4 Código 39

En **1977** por la internacionalización de la Asociación y derivado de la alta aceptación de utilizar este tipo de simbologías, el organismo cambia el nombre de EAN por EAN Internacional, ahora GS1. Actualmente existen 104 organizaciones miembro representadas en 145 países. Estas organizaciones proporcionan el apoyo total y la información a sus compañías locales. Más de un millón de compañías a nivel mundial se benefician de usar el Sistema GS1. AMECE es el organismo que representa a México. Al ingresar a esta asociación se conoce a detalle la forma de uso de los códigos de barras y las regulaciones pertinentes.

En **1978** Aparece el primer sistema patentado de verificación de códigos de barras por medio de láser.

LOS OCHENTAS

En **1980** El código PostNet, aparece como consecuencia de un requerimiento particular del Servicio Postal de los EEUU de automatizar los procesos de entrega y recolección de mensajeria.

Figura I.5 Código PostNet

En **1981** aparece la tecnología de lectura CCD (Charge Coupled Device) es aplicada en un escáner, En la actualidad este tipo de tecnología tiene bastante difusión en el mercado asiático, mientras que el láser domina en el mundo occidental. En ese año también aparece el código 128, de tipo alfanumérico.

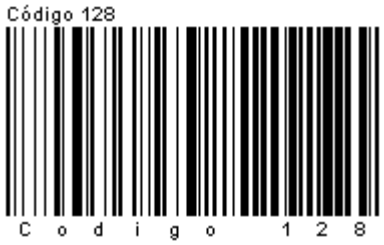

Figura I.6 Código 128

Aparece la norma ANSI MH10.8M que especifica las características técnicas de los códigos 39, Codabar, e ITF (Interleaved Two of Five).

El Dr. Allais es incansable. En **1987** desarrolla el primer código bidimensional, el código 49. Le sigue Ted Williams (Laser Light Systems) con el código 16K (**1988**).

LOS NOVENTAS

En **1990** se publica la especificación ANS X3.182, que regula la calidad de impresión de códigos de barras lineales. En ese mismo año, Symbol Technologies (empresa líder en la fabricación y desarrollo de tecnología de captura de datos y que fue adquirida por Motorola en el año de 2007) presenta el código bidimensional PDF417.

Figura I.7 Código Bidireccional PDF417

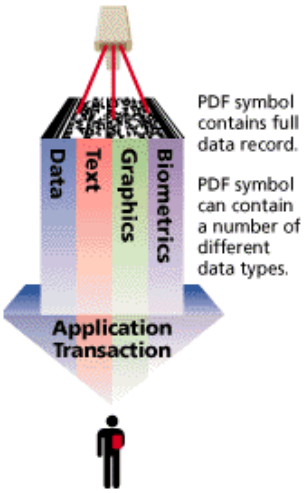

Figura I.8 Symbol Technologies presenta el Código PDF

I.1.2. Tipos de Código de Barras.

Características de un código de barras

Un símbolo de código de barras puede tiene varias características, entre las cuales podemos nombrar:

Densidad:
Es la anchura del elemento (barra o espacio) más angosto dentro del símbolo de código de barras. Está dado en mils (milésimas de pulgada). Un código de barras no se mide por su longitud física sino por su densidad.

WNR: (Wide to Narrow Ratio)

Es la razón del grosor del elemento más angosto contra el más ancho. Usualmente es 1:3 o 1:2.

Quiet Zone:

Es el área blanca al principio y al final de un símbolo de código de barras. Esta área es necesaria para una lectura conveniente del símbolo, recordemos que en realidad lo que lee un “scanner” es el reflejo de estos espacios blancos limitados por las barras negras, (representado en la figura I.2.1).

Figura I.2.1 Código de Barras

Código de barras Code128

El código de barras Code128 (figura I.2.2), es un código alfanumérico de alta densidad. Puede codificar 106 caracteres diferentes y se compone de tres subsets A, B y C, que no son otra cosa que diferentes formas de interpretar la información codificada. UCC / EAN 128 son variantes del subset C. Usando los subsets A o B puede codificar todos los caracteres ASCII, incluyendo los caracteres de control. El subset C permite codificar únicamente datos numéricos. Este código de barras contiene un *checksum*, antes del carácter de *stop*. La longitud de datos codificados es variable, con la restricción en el subset C cuya cantidad de dígitos debe ser par.

Figura I.2.2 Código 128

- **Permite codificar**: caracteres alfanuméricos
- **Longitud**: Variable
- ***Checksum***: Si

El código de barras Code128 es ampliamente usado en logística, paquetería, etiquetado de productos, billetes y aplicaciones postales.

Código de barras Code39

El código de barras Code39 figura I.2.3 (también conocido como 3/9, 3 de 9 o 3 entre 9) fue el primer código alfanumérico, de densidad media y es el código de barras más utilizado (uso no comercial). Este código es detector de errores, por lo que el uso de checksum no es obligatorio. Este código de barras debe comenzar y terminar con un asterisco (*) que hace las veces de un carácter de *start* y *stop*.

La versión estándar codifican 43 caracteres: A-Z, 0-9, espacio y "-", ".", " ", "$", "/", "+", "%". También es posible codificar todos los caracteres ASCII pero esta implementación influye negativamente en la densidad de impresión. El código puede ser de longitud variable y normalmente no lleva checksum (en algunos usos industriales se incluye un checksum de modulo 43, en este caso el código se denomina *Code39 Mod 43*).

Figura I.2.3 Código 39

- **Permite codificar**: 43 caracteres: A-Z, 0-9, espacio y -.$/+%.
- **Longitud**: Variable
- **Checksum:** Opcional

Código de barras Code93

El código de barras Code93 fue desarrollado en el año 1982 con la finalidad de complementar el estándar Code39. El Code93 es un código alfanumérico de alta densidad que soporta el juego de caracteres ASCII completo sin la ambigüedad de su antecesor, Code39. La versión estándar permite codificar 47 caracteres: A-Z, 0-9, espacio, "-", ".", " ", "$", "/", "+", "%" y cuatro caracteres especiales para soportar el código ASCII completo (figura 1.2.4). El código de barras puede ser de longitud variable y necesita dos caracteres de *checksum*.

Figura I.2.4 Código 93

- **Permite codificar**: 47 caracteres: A-Z, 0-9, espacio, -.$/+% y cuatro caracteres especiales.
- **Longitud**: Variable
- **Checksum**: Doble

Si bien la necesidad de un doble checksum parecería ser una molestia, ya que requiere mayor poder de cómputo para calcularlo, la posibilidad de codificar la tabla ASCII unívocamente es una clara ventaja del código de barras Code93 en comparación con su antecesor Code39.

Código de barras EAN

Virtualmente todos los productos vendidos en Europa utilizan el código de barras EAN-13. No puede simplemente crear códigos de barras EAN. *Article Numbering Association* es el encargado de asignar un código a cada producto, para asegurar de este modo que no haya dos productos con el mismo código.

Existen dos diferentes versiones de código de barras EAN, EAN 8 y EAN 13 (figura I.2.5), que permiten codificar 8 y 13 dígitos respectivamente. El código de barras EAN 13 es utilizado en la mayoría de los productos comerciales Europeos.

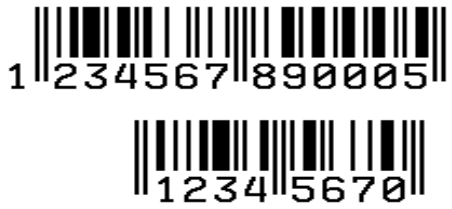

Figura I.2.5 Código EAN

- **Permite codificar**: Solo numérico
- **Longitud**: Fija, 8 o 13 dígitos
- **Checksum:** Si

Una variante del código de barras EAN de 13 dígitos, llamado Bookland, puede representar el numero ISBN de un libro. El código de barras adicional de 5 dígitos muestra el precio del libro y la moneda en la que se expresa el precio.

Código de barras UPC

Virtualmente todos los productos vendidos en los Estados Unidos utilizan el código de barras UPC-A (o el UPC-E, que es una modificación menor del UPC-A). No puede simplemente crear códigos de barras UPC-A. *Uniform Code Council* (UCC) es la encargada de asignar un código a cada producto, para asegurar de este modo que no haya dos productos con el mismo código.

UPC-A contiene 12 dígitos. Los primeros seis son asignados por la *Uniform Code Council*. Los cinco restantes se usan para identificar el producto. El último dígito es el checksum. El código de barras UPC-E es la versión recortada del UPC-A (figura I.2.6) para utilizar cuando no alcanza espacio para el código estándar UPC-A.

Figura I.2.6 Código UPC

- **Permite codificar**: Solo numérico
- **Longitud**: Fija, 12 o 7 dígitos
- ***Checksum***: Si

El código de barras UPC-A siempre debe ser de 1,5 pulgadas de ancho. El alto puede variar, pero no el ancho.

Código de barras Codabar

Codabar fue desarrollado en 1972 y es utilizado en biblioteca, bancos de sangre y encomiendas. Codabar es un código de barras numérico de alta densidad. El mismo incluye 16 caracteres: números 0-9, "-", ".", ":", "$", "/" y "+". Además, incluye cuatro caracteres especiales (A, B, C, D) que utilizan como caracteres de Start y Stop y no aparecen en la interpretación del código (figura I.2.7). Este código de barras es de longitud variable y no lleva checksum. En la versión mas usada del Codabar, la relación entre franjas anchas y angostas (*ratio*) es de 3.

Figura I.2.7 Código Codabar

- **Permite codificar**: 16 caractéres: 0-9, -.:$/+
- **Longitud**: Variable
- ***Checksum***: No

Código de barras Bookland

Es un código de barras especia que se utiliza para representar los números ISBN y precios en las tapas de los libros. Bookland utiliza el código de barras EAN de 13 dígitos para representar el numero ISBN y un código de barras suplementario de 5 dígitos que indica el precio del libro y la moneda en la que dicho precio esta expresado.

Figura I.2.8 Codigo Bookland

- **Permite codificar**: Solamente números
- **Longitud**: Fijo, 13 dígitos para ISBN mas 5 dígitos para el precio
- ***Checksum***: Si

Código de barras de 2 dimensiones PDF417

Su nombre viene de Portable Data File 417 (por sus siglas) Figura I.2.9 y es un conjunto de códigos de barra lineales, apilados, con un algoritmo interno que provee cierto nivel de redundancia y corrección de errores. Tiene también el inconveniente que requiere una área ciega antes y después del código además de zonas para delimitar el inicio y el final de los datos.

Figura I.2.9 Código PDF417

Data Matrix

El código Data Matrix es una simbología de dos dimensiones que consiste en bloques de información claros y oscuros. Tiene un patrón de identificación perimetral compuesto de dos líneas sólidas y dos líneas punteadas que indica la localización de los módulos de datos dentro del código de barras. Requiere una área ciega circundante y puede tener problemas de lectura en lugares poco iluminados o en etiquetas donde el código termina muy cerca de las orillas.

Figura I.2.10 Código Datamatrix

Código QR

Su nombre viene de “Quick Response” y es una simbología que provee lecturas muy rápidas, de forma omnidireccional y cuenta con buenos algoritmos de corrección de error. Sin embargo, al igual que la simbología anterior, los patrones de identificación se encuentran en las orillas, lo que puede traer problema de lectura cuando las condiciones del código no son óptimas. Debido a la ubicación del patrón de referencia, también se requieren áreas en blanco circundantes para que pueda ser correctamente decodificado.

Figura I.2.11 código QR

Código Azteca

Esta simbología de dos dimensiones y alta densidad está construida en una parrilla de forma cuadrangular que tiene un patrón de identificación de forma piramidal en el centro. Puede leerse en cualquier orientación y no requiere de espacios circundantes. Los datos van leyéndose del centro hacia fuera, por lo que la información crítica puede ubicarse cerca de la pirámide para una mejor y más rápida decodificación. Cuenta con sofisticados algoritmos de corrección de error y redundancia que permiten leer incluso en etiquetas dañadas o en mal estado. Este conjunto de características hacen de esta simbología su mejor opción para la recolección automática de datos.

Figura I.2.12 Código Azteca

Métodos de impresión de códigos de barras.

1) Impresión Directa:

El Código de Barras puede ser impreso como parte de la cara comercial del producto y se utiliza cualquier sistema de impresión convencional (offset, serigrafía, roto grabado, flexografía, litografía, etc.). Se necesita de una "película maestra" para que el impresor pueda hacer su trabajo.

2) Impresión a Solicitud

Si no es posible o no se desea que el Código de Barras sea impreso como parte del empaque, éste puede ser fijado en una etiqueta (auto adherible, colgante, cosida, etc.). Generalmente las etiquetas son impresas en transferencia térmica, térmicas o láser. Estos sistemas no requieren de una película maestra.

3) Impresión Térmica

Contraste Térmico Directo

Este proceso de impresión generalmente se usa en impresoras de etiquetas. Muchas impresoras de etiquetas pueden usar un medio de transferencia térmica directa o transferencia térmica. Básicamente, la impresión térmica directa tiene impresas barras de color negro intenso. El problema es que solamente el ojo humano puede ver el negro intenso. Para el lector, generalmente tienen una apariencia algo gris. Para mejorar esto, debe cambiarse el material ya que el valor de reflejo para las barras depende de los químicos sensibles al calor del papel.

También es posible que las características del papel térmico no sean adecuadas para la impresora. Se puede usar un papel con una sensibilidad térmica mayor o menor, o negro. Algunos papeles con una sensibilidad térmica muy alta tendrán un reflejo más alto de las barras con demasiada energía térmica. Los químicos sensibles al calor pueden tener el verde, azul o rojo como el color básico. El papel con químicos sensibles al calor verde o azul son más adecuados que el papel con químicos sensibles al calor de color rojo.

I.1.3. Aplicaciones.

Las aplicaciones del código de barras cubren prácticamente cualquier tipo de actividad humana, tanto en industria, comercio, instituciones educativas, instituciones médicas, gobierno, etc.

- Control de material en proceso
- Control de Inventario
- Punto de Venta (POS)
- Control de calidad
- Embarques y recibo de mercancía.
- Control de documentos
- Facturación
- Bibliotecas
- Bancos de sangre
- Hospitales
- Control de acceso y Control de tiempo y asistencia

Ventajas:

Algunas de sus ventajas sobre otros procedimientos de colección de datos son:

- Se imprime a bajos costos
- Porcentajes muy bajos de error
- Mayor velocidad de captura
- Los equipos de lectura e impresión de código de barras son flexibles y fáciles de conectar e instalar.

Beneficios

Es la mejor tecnología para implementar un sistema de colección de datos mediante identificación automática, y presenta muchos beneficios, entre otros.

- Virtualmente no hay retrasos desde que se lee la información hasta que puede ser usada
- Se mejora la exactitud de los datos
- Se tienen costos fijos de labor más bajos
- Se puede tener un mejor control de calidad, mejor servicio al cliente
- Se pueden contar con nuevas categorías de información.
- Se mejora la competitividad.

I.2. Sistemas de Reconocimiento Óptico de Caracteres (OCR).

I.2.1. Historia.

Abreviatura de OPTICAL CHARACTER RECOGNITION o Reconocimiento Óptico de caracteres. Software especial que permite leer, esto es, transformar en caracteres un texto escaneado y almacenado en forma de bits gráficos. Con la mayoría de los escáneres se acompaña un programa de OCR.

En 1959 en el inicio de la Banca Electrónica ERMA, Electronic Recording Method of Accounting, es creado por el Stanford Research Institute para Bank of America. ERMA es un sistema de ordenación robotizada de documentos y reconocimiento de caracteres (Optical Character Recognition, OCR) que permite la automatización de procesos en banca.

I.2.2. Tipos de OCR.

OCR para documentos

Día a día, la cantidad de información que alimenta a los negocios, institutos, escuelas, etc. va en aumento. Mientras que un creciente porcentaje es transmitido a través de la red mundial, una gran parte todavía corre por el método tradicional: el papel. Con el gran volumen de papel que muchas compañías deben procesar para operar exitosamente, la entrada manual de información puede convertirse en un entorpecedor e ineficiente proceso, algo que las empresas no pueden aceptar.

Para resolver esta problemática se requiere de un sistema de captura automática, OCR para documentos.

- ✓ Aumenta la precisión.
- ✓ Recupera rápidamente la inversión.
- ✓ Aumenta la eficiencia.
- ✓ Reduce costos de entrada de información.

OCR para documentos ha sido instalado en miles de negocios alrededor del mundo. Esta solución ha ayudado a compañías, grandes y pequeñas, a duplicar, e inclusive triplicar, su productividad y reducir dramáticamente sus costos.

Mejor aún, OCR para documentos fue diseñado para trabajar con cualquier tipo de forma en casi toda la industria. OCR para formas, rápida y fácilmente extrae la información que usted especifique de sus formas existentes.

Figura I.3.1 reconocimiento óptico de caracteres

OCR B fue diseñado en 1968 por Adrian Frutiger para cumplir los estándares de ”European Computer Manufacturer’s Association”. Fue desarrollado para usarse en productos y que a la vez podría ser leído por dispositivos de lectura y también por los humanos. OCR B fue reconocido como un estándar mundial en 1973, y es mas legible que los fonts OCR A.

La solución logra unos niveles envidiables de precisión extrayendo impresiones de máquina, impresiones manuales, "mark sense" (sensor de marca), y códigos de barra de una y dos dimensiones. Mientras se extrae la información, se puede aplicar reglas del negocio que validen la información. Una vez que la información es extraída y validada, cualquier carácter o región cuestionable se muestra para corregir o aceptar.

El paso final es crear un archivo ASCII de la información validada, corregida y verificada para procesamiento futuro. Todo esto es realizado con una mínima supervisión o intervención humana.

OCR A y OCR B son fonts (tipos de letra) estandarizados y diseñados para reconocimiento óptico de caracteres "Optical Character Recognition" a través de su lectura en dispositivos electrónicos diseñados para tal fin. OCR A fue desarrollado para cumplir con "American National Standards Institute" en 1966 para el procesamiento de documentos en los bancos, empresas emisoras de tarjetas de crédito y negocios similares. Este Font fue diseñado para ser leído por escáneres y no necesariamente por humanos.

HISTORIA DE LA TARJETA CON BANDA MAGNÉTICA

I.3. Sistemas de Banda Magnética.

Oberlin Smith publica en la revista Electrical World del 8 de septiembre de 1888 un artículo donde explicaba los principios básicos para grabar señales en un soporte magnético. El artículo fue publicado por La Lumier Electrique.

En 1898 cuando Valdemar Poulsen invento un grabador eléctrico sobre una tira de material flexible cubierta de polvo imantado, antecesor de la cinta magnetofónica actual y fue patentado en Estados Unidos (patente 661619.

Las primeras tarjetas con banda magnética fueron usadas desde principios de los sesentas en el transporte público, London Transit Authority instaló un sistema de tarjeta con banda magnética en el sistema de tren London Underground, en Londres.

A nivel de entidades financieras se empezaron a usar en 1951, a finales de los sesentas implementaron la tarjeta plástica con banda magnética.

Figura I.3.2. Primeras Tarjetas Plásticas de American Express y Diners

En 1970 cuando se establecieron los estándares internacionales (ISO 7811) el uso de la banda magnética se masificó y se extendió su uso a nivel mundial.

En 1971 The American Banking Association en Estados Unidos aprobó el uso de la banda magnética a nivel bancario.

El 16 de Enero de 1973 Robert E. Lawhend y William E. Steele patentaron una impresora para tarjetas con banda magnética, que fue asignada a Internacional Business Machines Corp. (IBM) con la patente No. 3711359 en Estados Unidos.

LA BANDA MAGNÉTICA

La banda magnética es una banda negra o marrón, esta banda esta hecha de finas partículas magnéticas en una resina. Las partículas pueden ser aplicadas directamente a la tarjeta o pueden ser hechas en forma de banda magnética y después ser adherida a la tarjeta.

La banda magnética puede ser de baja coercitividad Lo-CO (banda marrón), hecha de oxido de hierro, o de alta coercitividad Hi-CO (banda negra) hecha de ferrita de bario. Estos materiales se mezclan con una resina para formar una mezcla espesa que se cubre con un sustrato. Una vez cubierta con el sustrato las partículas en la mezcla son alineadas para dar una buena señal en proporción al ruido (esto es equivalente a eliminar los estallidos y golpes que se oyen en viejas grabaciones). La banda se pasa con la mezcla espesa aún húmeda a través de un campo magnético para encuadrar todas las partículas. La banda magnética en la tarjeta final puede ser codificada porque las partículas pueden ser magnetizadas en dirección sur o norte. Cambiando la dirección de codificación a lo largo de la banda permite escribir la información en la banda. Esta información puede ser leída y luego cambiada tan fácilmente como la primera codificación.

La densidad de partículas en la resina es uno de los factores de control de amplitud de señal. Entre más partículas haya, mas alta será la amplitud de la señal. La densidad combinada con el grosor da un método para controlar la amplitud. La importancia de la amplitud de la señal radica en la definición del diseño del lector de tarjetas. El estándar ISO/IEC 7811 define la amplitud de señal para las tarjetas que son usadas en un ambiente de intercambio (como las bancarias). La densidad de bits de información es seleccionada basada en los requerimientos del usuario. El estándar ISO/IEC 7811 establece los requerimientos de densidad de bits para las tarjetas en un ambiente de intercambio figura I.3.3.

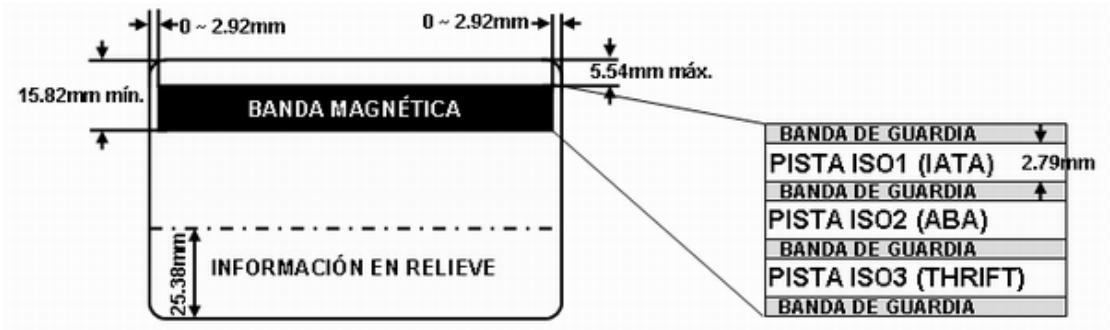

Figura I.3.3 Descripción de pistas en banda magnetica

I.4. Sistemas de Tarjetas Inteligentes.

Las *smart cards* son unas tarjetas de plástico con un tamaño definido normalmente por la razón aúrea que incluyen un microchip (Estándar ISO 7816). Mucha gente considera que las tarjetas inteligentes son un invento reciente, sin embargo llevan usándose desde los años 70.

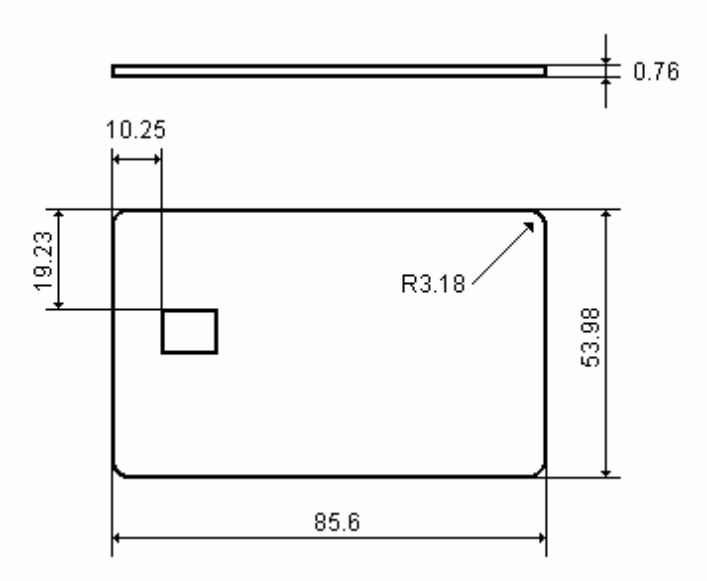

Figura I.4.1 Sistema de tarjetas inteligentes

Las smart cards las podemos clasificar según sus componentes como *memory cards* y *chip cards*.

- **Memory Cards:** Son las smart cards más comunes y baratas. Su objetivo es almacenar datos. El contenido de una Memory Card es:
    - EEPROM (Electrically erasable programmable read-only memory): Es un dispositivo que almacena datos dónde todas las aplicaciones pueden escribir. El tamaño de la EEPROM oscila entre 2KB y 8KB. El acceso a los datos de la EEPROM pueden ser bloqueados con un PIN. Por ejemplo, en una tarjeta de teléfono la EEPROM puede mantener el valor del saldo que nos queda.

- ROM (Read-only memory): Los datos que almacena no se pueden alterar nunca. Siguiendo el mismo ejemplo de la tarjeta de teléfono, en la ROM guardaría el número de la tarjeta, el nombre del titular,...

- **Chip Cards:** Estas tarjetas incoporan un microprocesador. Tal vez sean las únicas tarjetas que se merezcan llamarse inteligentes. Los principales componentes del chip de una tarjeta son:

  - ROM (Read-only memory): La ROM almacena el sistema operativo que se escribe solamente una vez (durante la fabricación de la tarjeta). Los tamaños de la ROM suelen estar comprendidos entre 8KB y 32KB, dependiendo del sistema operativo que se vaya a usar. Tal como su nombre indica, estas tarjetas son escritas una vez y ya no se puede cambiar su contenido almacenado.
  - EEPROM (Electrically erasable programmable read-only memory): En la EEPROM se almacenan las aplicaciones de la tarjeta y sus datos. En esta memoria se permite libre acceso (insercción, extracción y borrado). Los tamaños varían desde 2KB a 32KB.
  - RAM (Random access memory): Es la memoria volátil usada por el procesador para ejecutar las funciones pertinentes. La memoria es borrada cuando la alimentación se anula. El tamaño típico de la RAM ronda los 256 bytes, debido a que se le reserva un área muy pequeña, restringida a 25 mm^2.
  - CPU (Central processing unit): Es el corazón de la tarjeta. Normalmente se usan microprocesadores de 8 bits basados en la arquitectura CISC con una frecuencia de reloj de 5 Mhz. Aunque muchas ya implementan microprocesadores con arquitectura de 32 bits debido a las tarjetas Java.

Las Chip Cards son algo más caras que las Memory Cards. Sus costos oscilan entre 1 y 15 dólares dependiendo de las características de la tarjeta. El nivel de seguridad que ofrecen estas tarjetas es muy alto. Si dividimos el tipo de tarjeta según la interfaz obtenemos las *tarjetas de contacto* y las *tarjetas sin contacto*. Las tarjetas de contacto deben ser insertadas dentro del lector mientras que las tarjetas sin contacto son procesadas mediante una señal de radio y no requiere la inserción en un lector. También existen unas tarjetas que permiten ambos métodos de procesamiento.

I.4.1. Tarjetas de contacto.

Requieren la inserción en un lector de tarjetas para ser procesadas. El chip contiene de 6 a 8 contactos físicos. El contacto físico puede ser establecido por *deslizamiento* o por *presión*. La alimentación de la tarjeta la recibe del lector. Un ejemplo de chip que cumpla el formato estándar ISO 7816 es el siguiente:

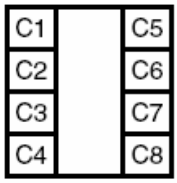

Figura I.4.2 Chip estándar ISO 7816

Los contactos están indicados por C_i. La función de cada contacto está definida como:

- **C1: Vcc** Suministra el voltaje
- **C2: RST** Reset
- **C3: CLK** Señal de Reloj
- **C4: RFU** Reservado para futuro uso
- **C5: GND** Tierra
- **C6: Vpp** Voltaje de Programación
- **C7: I/O** Entrada y salida de datos
- **C8: RFU** Reservado para futuro uso

Las tarjetas de contacto tienen ciertas limitaciones. Con el paso del tiempo estos contactos se desgastan. Las descargas electroestáticas debidas a contactos incorrectos pueden dañar los circuitos. También una causa común de daño es retirar la tarjeta del lector antes de que una transacción se complete.

I.4.2. Tarjetas libres de Contacto.

Tarjetas sin Contacto: Éstas tarjetas no requieren la inserción dentro de un lector. Solamente deben ser pasadas cerca de una antena para llevar a cabo la operación. La distancia de lectura oscila entre escasos centímetros a 50 cm. Las tarjetas sin contacto son más caras, aunque poseen una vida más larga.

Las tarjetas inteligentes también pueden ser clasificadas según su sistema operativo. En el mercado existen muchos sistemas operativos para tarjetas inteligentes. Algunos de los principales son:

- JavaCard
- MultOS
- Cyberflex
- StarCOS
- MFC

Los sistemas operativos de las tarjetas inteligentes se encuentran almacenados en la ROM.

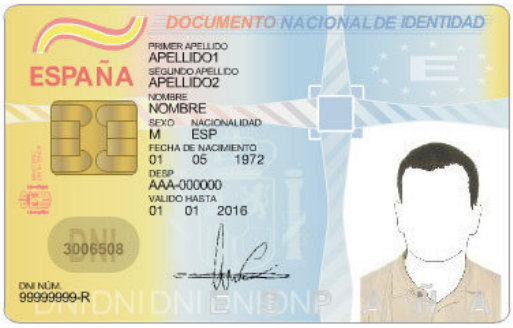

Figura I.4.3 Tarjeta inteligente

I.5. Sistemas RFID.

I.5.1. Historia

RFID con las siglas en inglés de Identificación por Radio Frecuencia, tecnología conocida desde hace más de cinco décadas y que unida al resto de elementos anteriormente descritos ha tomado un papel fundamental en el desarrollo de la Auto identificación electrónica de productos basada en el código electrónico del producto EPC (Electronic Product Code).

Un sistema de RFID está formado por dispositivos llamados "transponders" o "tags" que contiene el EPC, y lectores electrónicos o "reader" que se comunican con ellos. Estos sistemas se comunican vía señales de radio que transportan información de manera uni o bi direccional (distinguiendo así los tags de sólo lectura de los de escritura que permiten almacenar en el propio tag datos de interés).

"Cuando un tag entra a una zona de lectura, que puede ser radial (a diferencia de los lectores de código de barras), su información es capturada por el lector y puede ser utilizada."

Existen "tags" activos y pasivos. Los tags activos tienen batería propia por lo que de forma activa pueden informar de su presencia o activar cambios en otros dispositivos. Las distancias de lectura en estos casos son mayores. La vida útil de una batería puede fluctuar entre los 5 y 7 años, y puede ser renovada. Los "tags" pasivos no tienen batería propia, y sólo informan de su presencia cuando son preguntados por el lector. A través de una antena, el microchip recibe la energía emitida por el lector, con lo que puede enviar y recibir información.

Para organizaciones cada vez mas grandes y con una cantidad de productos mayor, la Identificación por Radio Frecuencia se vuelve necesaria. La tecnología RFID promete aumentar la eficacia así como la integridad de cada uno de los datos.

Figura I.5.1 Tarjeta RFID

I.5.2. Estándares de codificación

El código electrónico de producto o EPC por sus siglas en inglés es la evolución del código de barras ya que utiliza la tecnología RFID para identificar de manera única a los productos en sus distintas unidades de empaque, pieza, caja y tarima (item, case y pallet) agregando un número de serie a la información sobre su tipo y fabricante. Los códigos electrónicos de producto son administrados a nivel mundial por EPCglobal, filial de GS1.

Figura I.5.2 Código electrónico de identificación RFID

ePC" (Electronic Product Code) es una etiqueta electrónica con capacidad de comunicación (tag) por radiofrecuencia, capaz de identificar, mediante un código único, cualquier objeto fabricado o comercializado. El proyecto surge de las investigaciones del Auto-ID Center del MIT y está patrocinado por algunos grandes grupos de la distribución mundial, como Wal-Mart, Unilever, Procter & Gamble y Gillette. Forman parte del proyecto las tecnologías de red correspondientes, parecida a las de internet, capaces de garantizar la trazabilidad de estos productos a lo largo de toda la cadena del suministro.

Anunciado desde hace unos cuantos años como el objeto revolucionario capaz de reemplazar los cientos de miles de millones de etiquetas tradicionales con código de barras, la etiqueta EPC de bajo coste (objetivo: 5 céntimos, de euro o de dólar) ha disfrutado recientemente de un nuevo interés.

El anuncio que se dio a principios de año relativo a un pedido de Gillette para el suministro de 500 millones de tags ePC, no representa un hecho aislado en el mundo de la identificación automática y de la Gestión de la Cadena de Suministro. Por otro lado, todos los fabricantes de lectores e inlays (el circuito con su antena, ensamblados en un substrato cualquiera) ya se están preparando para incorporar circuitos ePC.

La razón principal del cambio obedece a una serie de limitaciones por parte del código de barras, que tiene respuesta con la utilización del EPC:

»El código de barras necesita visibilidad para funcionar, es decir debe ser visible ante el lector para que el producto puede ser identificado, es lo que en inglés se denomina line of sight (Línea de Vista).

El código de barras tradicionalmente identifica a un tipo de producto, no una unidad de dicho producto. Un código de barras puede identificar botellas de agua, pero no puede identificar una botella en concreto (por ejemplo con un número de serie).

Esta no es una limitación inherente de la tecnología, pero normalmente los sistemas de código de barras no se utilizan como identificadores únicos porque fue considerado inviable tecnológicamente en el momento de su concepción (no existían bases de datos relacionales de grandes prestaciones, no existía una forma cómoda y sencilla de colaboración de sistemas informáticos y no existía una red llamada internet)

La red EPC network

Al igual que un código de barras, el EPC de 96 bits utiliza una cadena de números para identificar al fabricante de un artículo y su categoría de producto. El EPC añade un tercer grupo de dígitos, que es un número de serie exclusivo para cada artículo. Este número es todo lo que se almacena en el microchip de la etiqueta RFID, pero el EPC se puede asociar con una gran cantidad de información en una base de datos, creando así unas posibilidades de explotación gigantescas. Por ejemplo, el lugar y la fecha de fabricación del producto, su fecha de caducidad, el lugar al que se debe enviar, etc. Además, la información se puede actualizar en tiempo real para seguir los movimientos o los cambios del artículo.

En un mundo en el que todos los artículos tuvieran un EPC, la suma de la información parcial almacenada por cada empresa reflejaría la fabricación, el envío, la venta de los productos, y todos aquellos eventos que puedan ser de interés en el proceso de ciclo de vida del producto. Esta información residiría en una gran red de bases de datos distribuidas. La transmisión y gestión de todos estos datos es la parte más importante (y difícil) de todo el proceso. El Auto-ID Center ha desarrollado una tecnología de software llamada Savant, que funciona como el sistema nervioso de la nueva red.

Cuando un Savant recibe de un lector de código electrónico de producto en un muelle de carga o en una estantería de almacenamiento, accede a un servicio de nombres de objetos (ONS) en la red local de una empresa o en Internet para buscar el producto asociado al EPC. El ONS es similar al servicio de nombres de dominio que dirige los ordenadores hacia puntos concretos de la World Wide Web.

El ONS dirige el Savant a una base de datos corporativa que contiene información sobre el producto. Parte de la información sobre cada producto (sus características básicas y su categoría general) quedará almacenada en un nuevo lenguaje de marcado físico (PML), que está basado en el lenguaje de marcado extensible (XML) estándar. El PML permite efectuar operaciones comerciales comunes, como buscar bebidas con gas en una base de datos de inventario o comparar los precios de láminas de acero laminado en caliente de una medida concreta.

Debido a los grandes beneficios de la tecnología RFID sobre otras tecnologías de identificación como el código de barras, múltiples cadenas de autoservicio están solicitando a sus proveedores que entreguen sus mercancías con etiquetas RFID en cajas y tarimas. La medida no solo beneficia a las cadenas, sino a todos aquellos proveedores que sepan obtener los beneficios del uso adecuado de la tecnología.

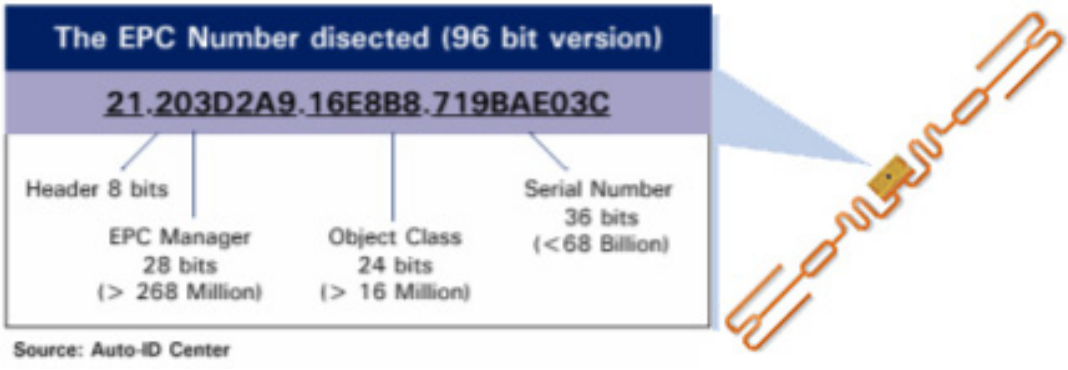

Figura I.5.3 Código EPC con tecnología RFID

I.5.3. Aplicaciones

Cadena de suministro (Supply Chain)

Identificación y autentificación de artículos individuales (items) con tecnología RFID

Los productos de consumo de alto valor son susceptibles a ser identificados con tecnología de identificación por radiofrecuencia para permitir una mayor visibilidad y control al mismo tiempo que evita falsificaciones.

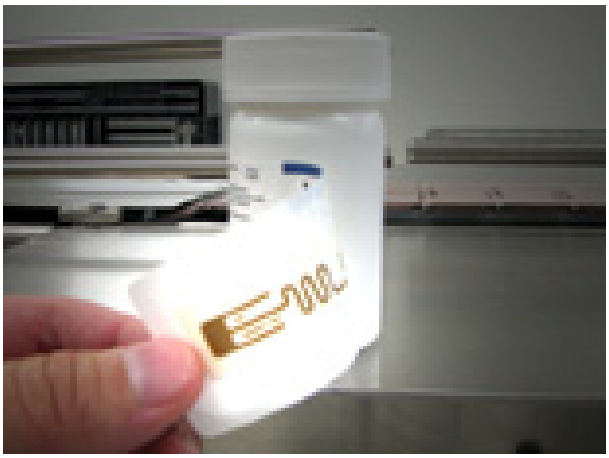

Figura I.5.4 Identificación de cajas (cases) con tecnología RFID

La tecnología RFID es también utilizada como elemento de automatización y visibilidad con baja tasa de error al utilizarse en túneles interrogadores sobre bandas transportadoras para identificar producto en sus niveles de empaque superiores.

Identificación de tarimas o estibas (pallets) con tecnología RFID

La identificación de contenedores logísticos en forma de pallet, representan una de las más valiosas aplicaciones de la tecnología RFID en términos de retorno sobre inversión.

De la mano de la tecnología de visión artificial, la tecnología RFID elimina robos y permite obtener control total de entradas y salidas de mercancía al almacén.

Figura I.5.5 Identificacion de palletes con tecnología RFID

Control de activos

Identifique y mantenga un control eficiente de los inventarios de computadoras, maquinaria y otras piezas de activo fijo como vehículos y equipo portátil mediante tecnología RFID.

Autentificación de medicamentos

EEUU y las dependencias del sector salud en América Latina requieren de mayores controles para asegurar el abasto y custodia de la cadena de suministro de medicamentos y combatir la falsificación. Con ello se requiere codificar el producto desde su fabricación a fin de insertar un tag de RFID que permita darle trazabilidad al mismo.

Atención a clientes

Utilizando dispositivos RFID (figura I.5.6), las empresas pueden llevar a cabo una mejor estrategia de marketing y distinción, mediante control de promociones, descuentos, acceso preferencial y servicios especiales a clientes frecuentes.

Figura I.5.6 Atención a clientes utilizando RFID

Control de acceso

Sistemas de alta seguridad con registro de actividades almacenado en un sistema de información local o en los mismos transponders. Ideal para instituciones como escuelas, instalaciones de seguridad o empresas en general.

Identificación vehicular

Sistemas de identificación automática de vehículos para casetas de cobro y control vehicular con tags pasivos y activos.

Manufactura y control de procesos

La tecnología RFID aplicada a procesos de manufactura, permite obtener trazabilidad y control de producción en proceso WIP (Work In Process) en distintos tipos de industria.

Industria del vestido

La mayor parte de las prendas de vestir están fabricadas con un alto porcentaje de materiales luminosos (transparentes) a la radio frecuencia como los son: tela, piel y los materiales plásticos. Esta cualidad permite a la industria del vestido, obtener grandes beneficios mediante el uso de la tecnología RFID.

I.6. Sistemas de reconocimiento biométrico.

I.6.1. Historia y tipos de biometría

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

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

La biometría, una de las diez tecnologías emergentes según un estudio (2001) del Massachussets Institute of Technology (MIT), es una ciencia que emplea métodos de identificación no tradicionales como la impresión de huella dactilar, la biometría dinámica de firma, la geometría del rostro o de la mano, el iris, la retina, así como el tipo de sangre y de ADN. En la actualidad debido a su sencilla implementación y bajo costo/beneficio, la biometría de huella dactilar es el método más utilizado y conocido; se emplean programas de lectura de huellas digitales, relojes checadores de control biométrico o programas de control de ausentismo por lectura biométrica, estos sistemas son aquellos que utilizando lectores de huellas digitales integrados a una red de computadoras o bien lectores autónomos de huellas dactilares permiten verificar el ingreso, salida, ausentismo y otras situaciones relacionadas con el control de personal.

Los principios en los que se basa están relacionados con la traducción de la información contenida en la huella digital (utilizan un mapa de puntos clave de una huella dactilar) a algoritmos únicos y personales que se emplean para identificar al usuario y relacionar esta información con sus datos personales. Estos sistemas de lectura de huellas digitales por biometría utilizan menos de un segundo para captar e identificar al poseedor de la impresión dactilar.

Existen diferentes métodos de identificación y autenticación de los seres humanos a través de características fisiológicas y de comportamiento los cuales pueden dividirse en:

Fisiológicos: Geometría de la mano, iris, retina, reconocimiento facial, huella digital
Comportamiento: Firma, voz, dinámica de teclado

I.6.2. Identificación por huellas dactilares

Son las formas caprichosas que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones.

Las salientes se denominan crestas papilares y las depresiones surcos inter papilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella.

Son únicas e irrepetibles aún en gemelos idénticos, debido a que su diseño no está determinado estrictamente por el código genético, sino por pequeñas variables en las concentraciones del factor del crecimiento y en las hormonas localizadas dentro de los tejidos. Cabe señalar que en un mismo individuo la huella de cada uno de sus dedos es diferente.

Clasificación

Los patrones de huellas digitales están divididos en 4 tipos principales, todos ellos matemáticamente detectables. Esta clasificación es útil al momento de la verificación en la identificación electrónica, ya que el sistema sólo busca en la base de datos del grupo correspondiente.

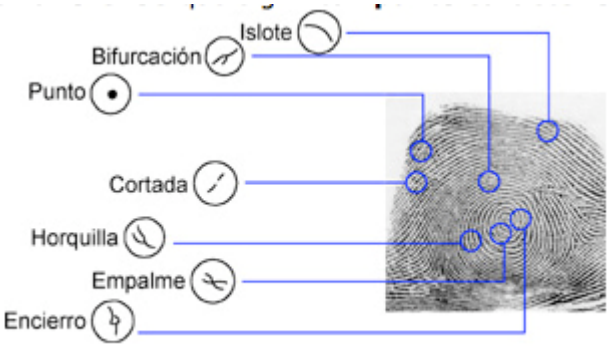

Figura I.6.1 Características de la Huella Digital

En la figura aparecen 8 puntos característicos que hay en un dedo, éstos se repiten indistintamente para formar entre 60 y 120 (por ejemplo 10 orquillas 12 empalmes 15 islotes, etc.). A estos puntos también se llaman minutae, o minucias, término utilizado en la medicina forense que significa “punto característico”.

Procedimiento

Con este conjunto de puntos, el software biométrico de huella digital genera un modelo en dos dimensiones, según se muestra en el ejemplo, mismo que se almacena en una base de datos, con la debida referencia de la persona que ha sido objeto del estudio.

Para ello, la ubicación de cada punto característico o minucia se representa mediante una combinación de números (x.y) dentro de un plano cartesiano, los cuales sirven como base para crear un conjunto de vectores que se obtienen al unir las minucias entre sí mediante rectas cuyo ángulo y dirección generan el trazo de un prisma de configuración única e irrepetible.

Para llevar a cabo el proceso inverso o verificación dactilar, se utilizan estos mismos vectores, no imágenes.

			
El dedo es leído por un lector de huellas.	El dedo es codificado.	Una plantilla matemática es generada.	El lector guarda y reconoce un conjunto de números que solo podrán ser reconocidos como una plantilla.

Figura I.6.2 Procedimiento del lectura de Huella digital

Dispositivo para identificación

El Sistema de Identificación Automatizada de Huellas Dactilares, tiene un índice de seguridad del 99.9% ya que verifica la identidad de una persona, basada en las características de sus huellas digitales.

Para tratar los datos de la huella se utiliza un algoritmo que permite asociar la huella que se desea identificar, con otras de similares características, almacenadas en la base de datos.

Existen dos maneras distintas usar los datos de una huella.

1. Verificación ¿Es la persona quien dice ser?

Se suele pedir un código, una lectura de tarjeta y comparar esa huella almacenada con la huella puesta en el lector, la verificación es un proceso un poco más molesto porque se le pide una información o una acción adicional al usuario, pero como ventaja tiene que es más rápido y más seguro.

2. Identificación. ¿Quién es la persona?

En este proceso directamente se compara una huella capturada contra todas las que están almacenadas en el ordenador, es un proceso algo más lento, pero la interacción con el usuario es mínima.

Es importante remarcar que la mayoría de los lectores dactilares , no guardan la imagen de la huella, solo almacenan los datos matemáticos explicados anteriormente.

Tipos de sensores

En el mercado actual existen muchos tipos de sensores biométricos, lectores capaces de convertir una huella en una imagen procesable por un algoritmo.

Existen muchos más tipos, la mayoría experimentales y nunca han llegado realmente al mercado, los que se puede encontrar se dividen en las siguientes categorías:

La mayoría de los dispositivos biométricos usan lectores ópticos, son los más versátiles y requieren de un lector óptico de alta precisión.

Lectores Ópticos

Ventajas: Bajo costo, rapidez de captura, resolución de la imagen, velocidad

Inconvenientes: Uso solo para interiores debido a la luz solar.

Lectores conductivos

Ventajas: Reducido tamaño ideal para dispositivo de uso personal, móviles, etc.
Inconvenientes: Muy sensibles a la humedad, poca calidad de imagen.

Lectores térmicos

Ventajas: Tamaño pequeño, uso en exteriores, dispositivos personales
Inconvenientes: sensibles a la temperatura, dificultad de uso, necesita un cierto aprendizaje.

Lectores ultrasonidos

Ventajas: No requiere de contacto, mucha seguridad
Inconvenientes: Precio alto, tamaño, requiere mantenimiento continuo.

I.6.3 Reconocimiento facial o biometría facial

El reconocimiento facial es una tecnología con mucho futuro, en la actualidad no está muy extendida, puesto que requiere de unas condiciones muy concretas, sobre todo de luz, además suele requerir cámaras de un coste bastante alto. La seguridad en este sistema es bastante bajo, es bastante fácil "engañar" al sistema, puede ser un buen complemento para otros sistemas biométricos.

I.6.4 Reconocimiento por voz

Similar al reconocimiento facial, no es suficientemente seguro como sistema biométrico, pero puede ayudar a otros sistemas.

El **Reconocimiento Automático del Habla** (RAH) o **Reconocimiento Automático de voz** es una parte de la Inteligencia Artificial que tiene como objetivo permitir la comunicación hablada entre seres humanos y computadoras electrónicas.

El problema que se plantea en un sistema de **RAH** es el de hacer cooperar un conjunto de informaciones que provienen de diversas fuentes de conocimiento (acústica, fonética, fonológica, léxica, sintáctica, semántica y pragmática), en presencia de ambigüedades, incertidumbres y errores inevitables para llegar a obtener una interpretación aceptable del mensaje acústico recibido.

Figura I.6.3 Reconocimiento de voz

Clasificación

Los sistemas de reconocimiento de voz pueden clasificarse según los siguientes criterios:

- **Entrenabilidad**: determina si el sistema necesita un entrenamiento previo antes de empezar a usarse.
- **Dependencia del hablante**: determina si el sistema debe entrenarse para cada usuario o es independiente del hablante.
- **Continuidad**: determina si el sistema puede reconocer habla continua o el usuario debe hacer pausas entre palabra y palabra.
- **Robustez**: determina si el sistema está diseñado para usarse con señales poco ruidosas o, por el contrario, puede funcionar aceptablemente en condiciones ruidosas, ya sea ruido de fondo, ruido procedente del canal o la presencia de voces de otras personas.
- **Tamaño del dominio**: determina si el sistema está diseñado para reconocer lenguaje de un dominio reducido (unos cientos de palabras p. e. reservas de vuelos o peticiones de información meteorológica) o extenso (miles de palabras).

Usos y aplicaciones

Aunque en teoría cualquier tarea en la que se interactúe con una computadora puede utilizar el reconocimiento de voz, actualmente las siguientes aplicaciones son las más comunes:

- **Dictado automático**: El dictado automático es, en el 2007, el uso más común de las tecnologías de reconocimiento de voz. En algunos casos, como en el dictado de recetas médicas y diagnósticos o el dictado de textos legales, se usan corpus especiales para incrementar la precisión del sistema.
- **Control por comandos**: Los sistemas de reconocimiento de habla diseñados para dar órdenes a un computador (p.e. "Abrir Firefox", "cerrar ventana") se llaman Control por comandos. Estos sistemas reconocen un vocabulario muy reducido, lo que incrementa su rendimiento.
- **Telefonía**: Algunos sistemas PBX permiten a los usuarios ejecutar comandos mediante el habla, en lugar de pulsar tonos. En muchos casos se pide al usuario que diga un número para navegar un menú.
- **Sistemas portátiles**: Los sistemas portátiles de pequeño tamaño, como los relojes o los teléfonos móviles, tienen unas restricciones muy concretas de tamaño y forma, así que el habla es una solución natural para introducir datos en estos dispositivos.
- **Sistemas diseñados para discapacitados**: Los sistemas de reconocimiento de voz pueden ser útiles para personas con discapacidades que les impidan teclear con fluidez, así como para personas con problemas auditivos, que pueden usarlos para obtener texto escrito a partir de habla. Esto permitiría, por ejemplo, que los aquejados de sordera pudieran recibir llamadas telefónicas.

I.6.5. Escáner de Iris o escáner de Ojos

Tecnología altamente segura, pero hoy en dia una tecnología bastante cara, solo para sitios de muy alta seguridad, los usuarios son reticentes a poner el ojo cerca de una cámara que es totalmente inocua, sin embargo algunas cámaras necesitan luz roja que puede ser visible o invisible (Infrarroja) en el caso de la luz visible el usuario siente que es una acción intrusiva y prefiere no exponerse.

Hay dos formas de escanear los ojos. Un escáner de retina mide el patrón de venas en el fondo del ojo, que se obtiene proyectando una luz infrarroja a través de la pupila. El escáner de iris se realiza utilizando una videocámara y examinando los patrones de color únicos de los surcos de la parte coloreada de nuestros ojos. Los escáneres de iris están empezando a utilizarse en la seguridad de los aeropuertos, control de asistencia, oficinas, etc. Los escáneres de retina son bastante invasivos y menos habituales, pero se siguen utilizando para restringir el acceso a instalaciones militares, laboratorios de investigación y otras áreas de alta seguridad.

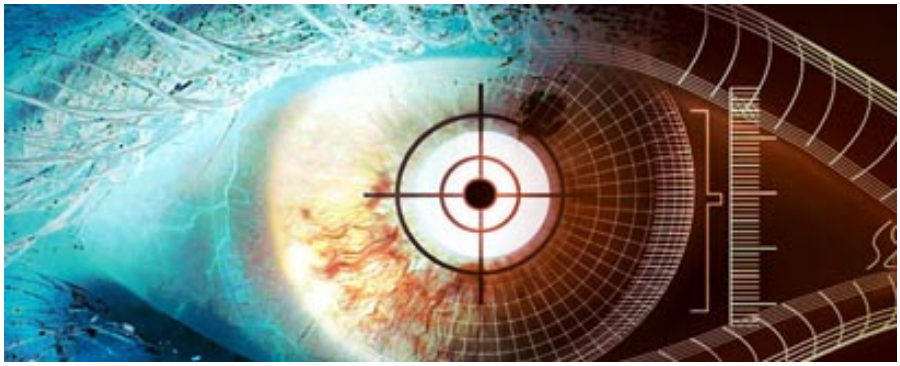

Figura I.6.4 Reconocimiento por medio del Iris

CAPITULO II. FUNDAMENTOS DE RECONOCIMIENTO BIOMETRICO.

II.1. Principio de Operación.

La alta fidelidad que entregan las tecnologías biométricas de mayor uso hoy y con más apoyo por las industrias comerciales son: la huella digital, el reconocimiento facial, la geometría de la mano, el iris, la voz, la firma. (Figura II.1)

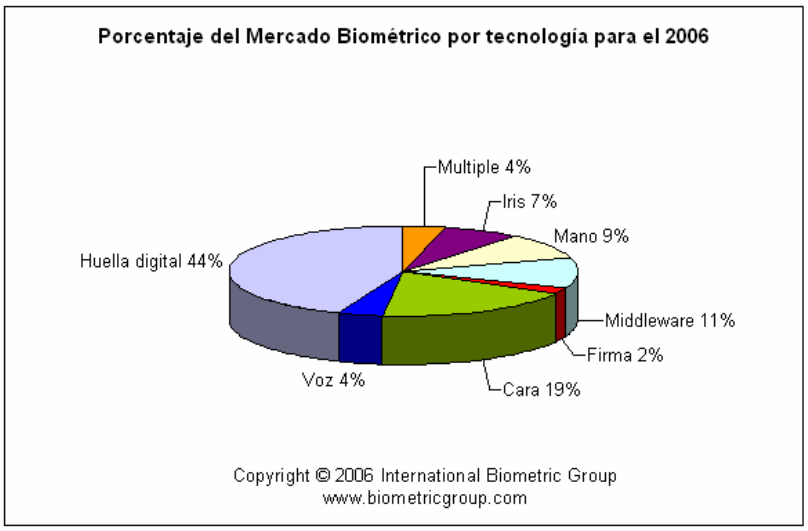

Figura II.1. Uso de Tecnología Biométrica

Ventajas de la Biometría

- ✓ Reduce la posibilidad de fraude
- ✓ Es imposible olvidar su huella
- ✓ Es imposible perder la huella
- ✓ La huella no se puede prestar a nadie
- ✓ Es prácticamente imposible de falsificar
- ✓ Ahorra tiempo al contabilizar
- ✓ Fácil de usar y aprender
- ✓ Bajo costo de inversión
- ✓ No requiere consumibles
- ✓ Rápido retorno de inversión

II.2. Tipos de reconocimiento biométrico.

II.2.1. Reconocimiento a través de él Iris

El reconocimiento del iris, como una técnica biométrica es uno de los modelos más efectivos para la identificación de una persona. Este método es estudiado por muchos investigadores. Uno de ellos es Daugman y propone una técnica que se basa en capturar la imagen del iris, y proceder a normalizarla a través de una conversión a coordenadas polares, y la aplicación contigua de ecuaciones diferenciales que permiten la obtención de un patrón denominado código del iris. Para la comparación de dos patrones, se utiliza la distancia de Hamming. Donde los resultados que se obtienen son muy eficientes y con mucha precisión, y cada vez se amplía su uso.

Es por esto, que el Reconocimiento del iris es uno de los avances más interesante y confiables dentro del reconocimiento de personas. Este método presenta las menores tasas de falla, y posee la cualidad que al analizar los patrones en personas distintas, la variabilidad es enorme. Además de todos estos beneficios, el iris permanece casi invariante por toda la vida ya que se encuentra protegido y a la vez la eliminación del ruido o los cambios de iluminación, son resueltos de manera muy simple.

DEFINICIONES IMPORTANTES

Iris

El iris es un órgano interno del ojo, localizado por detrás de la córnea (Figura II.2) y del humor acuoso, pero en frente de los lentes; diferencia el color de ojos de cada persona (Figura II.3), es igual que la vasculatura retinal.

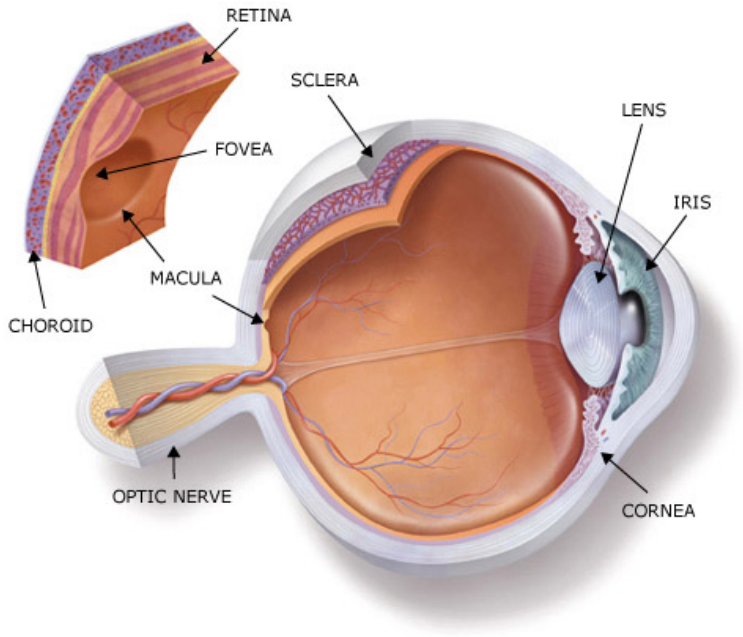

Figura II. 2

Figura II.3

Patrón del iris

Una propiedad que el iris comparte con las huellas dactilares es la morfología aleatoria de su estructura. No existe alteración genética en la expresión de este órgano más allá de su forma anatómica, fisiología, color y apariencia general. La textura del iris por sí misma es estocástica o posiblemente caótica. Pero el iris disfruta de ventajas prácticas adicionales sobre las huellas dactilares y otras variables biométricas, como son:

- ✓ La facilidad de registrar su imagen a cierta distancia, sin la necesidad de contacto físico o intrusivo y quizás discretamente.
- ✓ El alto nivel de aleatoriedad en su estructura que permite 266 grados de libertad que pueden ser codificados y una densidad de información de 3.4 bits por mm² de tejido.
- ✓ Estable y sin cambio durante el periodo de vida del sujeto, inalterable durante toda la vida de la persona.

El propósito del reconocimiento del iris es obtener en tiempo real, con alto grado de seguridad, la identidad de una persona; empleando análisis matemático del patrón aleatorio que es visible dentro del ojo a cierta distancia. Debido a que el iris es un órgano interno protegido (inmune a influencias ambientales) con textura aleatoria, estable (sin cambios), él puede ser usado como una clave viva que no necesita ser recordada pero que siempre estará ahí.

El iris se ve afectado por la pupila cuando ésta reacciona a la luz. Las deformaciones elásticas que ocurren con la dilatación y contracción son rápidamente corregidas empleando algoritmos matemáticos que se encargan de localizar los bordes interno y externo del iris.

Fundamentos del reconocimiento de iris

Dentro de este capítulo, se podrá observar el desarrollo del punto central, tomando como referencia principal, los estudios de John Daugman, quien ha realizado múltiples técnicas en el campo de la biometría. Los métodos que desarrolló son utilizados comercialmente por muchas compañías, como es el caso de LG, IBM, NBTC, Telecom, etc. Sin embargo se han tomado nociones de otros autores, con el fin de obtener un resultado más completo. Y vale mencionar también que existen diferentes técnicas aparte de la de Daugman, como la de Comparación de histogramas o la de Análisis de texturas, por mencionar algunas.

Para desarrollar algún tipo de proyecto o lograr obtener una aplicación de reconocimiento de iris, es necesario plantear un sistema ordenado. Un sistema de reconocimiento de iris típico se representa esquemáticamente en la Fig. II.4.

En la primer etapa, se adquiere la imagen del iris de la persona ha ser reconocida. Luego, la imagen digital es procesada para localizar el iris en la misma y normalizar su tamaño. En tercer lugar, la información contenida en el patrón de iris es extraída y un código asociado con el iris es generado. Finalmente, en la etapa de comparación, se decide, en base al porcentaje de similitud obtenido, si los códigos comparados fueron generados por el mismo iris, o sea, por la misma persona, o no.

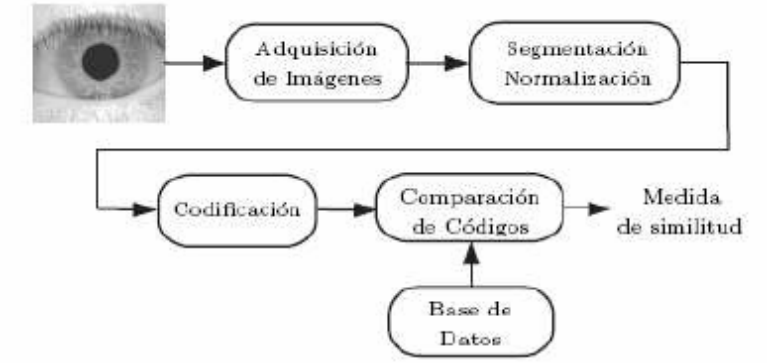

Fig. II. 4. Diagrama en bloques del sistema de reconocimiento del iris.

En general, los sistemas de reconocimiento de personas pueden ser utilizados en dos modos de funcionamiento diferentes, Autentificación e Identificación, Fig. II.5. En el primero, el código de iris se compara con el código asociado a la identidad proclamada por la persona, y se decide si estos códigos han sido generados por el mismo iris o no.

En el segundo, el código de iris a reconocer es comparado con una base de datos para comprobar la identidad de la persona.

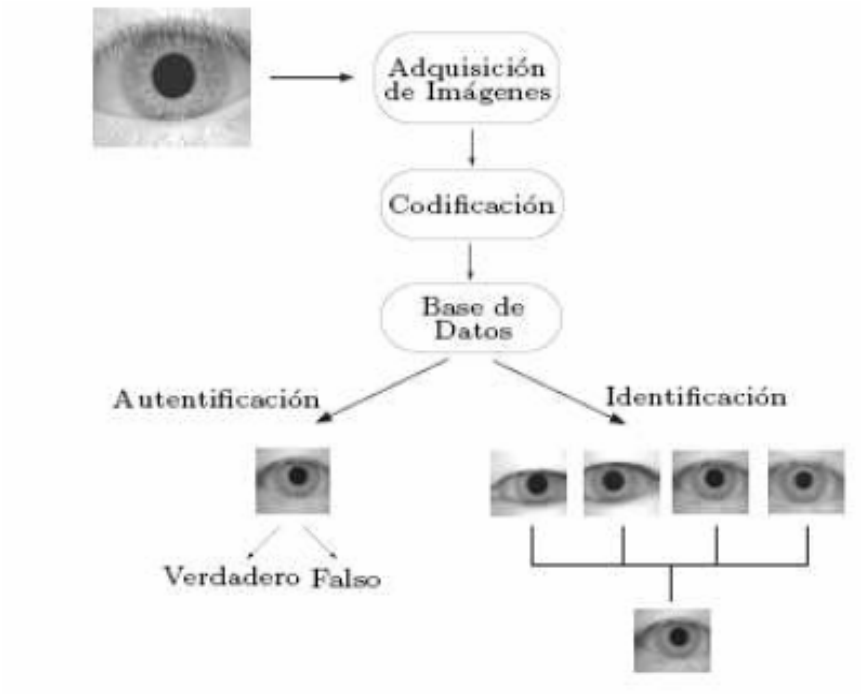

Figura. II.5. Sistema de reconocimiento. Autentificación e Identificación.

Adquisición de Imágenes

Uno de los desafíos mayores de reconocimiento del iris es capturar una imagen de calidad superior del iris. Dado que el iris es un relativamente pequeño y oscuro (típicamente de un centímetro de diámetro), esta se requiere ingeniería cuidadosa. Esta es una etapa muy importante ya que el rendimiento de todo el sistema es afectado directamente por la calidad de la imagen adquirida.

Primero, es deseable adquirir imágenes del iris con resolución suficiente y agudeza para obtener un buen el reconocimiento. Segundo, es importante tener un buen contraste en el modelo del iris interior sin acudir a un nivel de iluminación que incomoda al usuario. Tercero, estas imágenes deben idearse bien (por ejemplo, centradas), preferentemente sin exigirle al usuario que emplee el resto de la barbilla, u otro posicionamiento de contacto que sería intrusivo.

Para capturar la mayor cantidad e detalles en los patrones de iris, un sistema de adquisición de imágenes, debería poseer una revolución mínima de 70 píxeles en el radio del iris. Actualmente las resoluciones más comunes en el radio del iris van de 100 a 140 píxeles.

Existen distintos sistemas de adquisición de imágenes, la mayoría de ellos utilizan cámaras de video y sistemas de iluminación sofisticados. En la Fig.II.6 se representa un esquema del sistema de adquisición de imágenes. La lente plano-convexa ha sido agregada al sistema óptico de la cámara de manera de adquirir imágenes del ojo bien enfocadas y con la suficiente resolución a una distancia entre 10cm y 15cm.

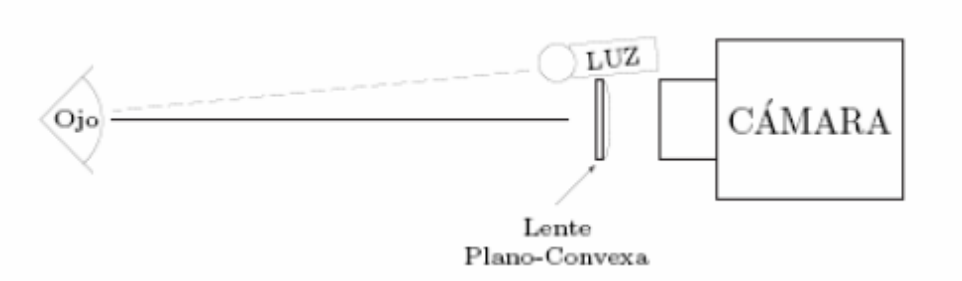

Figura II.6. Esquema del sistema de adquisición propuesto

Pre procesamiento

Ocurre que la imagen digital utilizada por el sistema de reconocimiento no sólo contiene el iris, sino también las regiones que lo rodean. Además, la imagen del iris suele estar obstruida por los párpados, pestañas y reflexiones producidos por el sistema de iluminación. Por otra parte, el tamaño del iris generalmente varia en diferentes imágenes debido a la contracción/dilatación del iris causada por diferentes niveles de iluminación, diferentes distancias ojo/cámara, rotación del ojo y otros factores. Por estos motivos es necesario aplicar un procesamiento a las imágenes antes de utilizarlas en la etapa decodificación, el cual puede ser dividido en dos etapas:

- ✓ Segmentación, donde se localiza la imagen del iris.
- ✓ Normalización, por la cual se obtiene una imagen del iris que es independiente del tamaño de la pupila y permite la comparación entre diferentes iris.

Segmentación

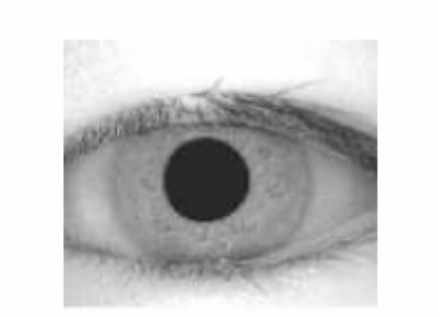

Figura II.7. Figura original desde donde se comienza el análisis

La etapa de segmentación es muy importante ya que si el iris no es correctamente localizado las etapas posteriores utilizaran datos erróneos, por lo tanto el código generado contendrá errores y el rendimiento del sistema será muy bajo.
El iris es la región anular comprendida entre la esclerótica y la pupila, la región del iris puede ser modelada como dos círculos no concéntricos, el exterior representa el borde iris/esclerótica, y el interior el borde iris/pupila; además los párpados, los cuales generalmente obstruyen el iris, pueden ser modelados como curvas segmento-lineales.

A pesar que los resultados de la búsqueda del iris restringen la búsqueda de la pupila, la concentricidad de estos bordes no puede ser asumida. Muchas veces el centro de la pupila es nasal, e inferior al centro del iris. Su radio puede tener un rango desde 0.1 hasta 0.8 del radio del iris. Un operador muy efectivo para determinar el centro del iris y la pupila es la siguiente expresión integro diferencial:

$$\max_{(r,x_0,y_0)} \left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{I(x,y)}{2\pi r} ds \right|$$

Donde I(x,y) es una imagen como el de la figura II.7. El operador busca sobre toda la imagen el dominio máximo (x,y) en la derivada parcial con respecto al radio r. El símbolo asterisco denota convolución. El operador de manera se comporta como un detector de bordes circular.

El operador sirve para encontrar dos bordes: el borde pupilar y el borde del iris, a través de un método iterativo denominado “De grueso a delgado”. Luego de una manera similar para detectar bordes curvilíneos es usada para localizar los bordes de los parpados. El resultado de todas estas operaciones de localización es el aislamiento del iris de otras regiones de la imagen como se muestra en la figura II.8.

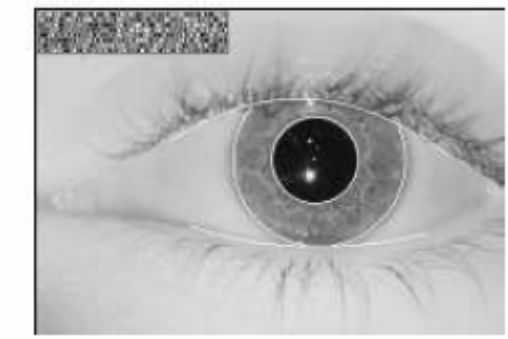

Figura II.8. Ejemplo de un patrón de iris a una distancia de 35 cm.
Las líneas indican los bordes de la pupila el iris y los párpados.

Normalización

Una vez localizado el iris en la imagen adquirida se genera una nueva imagen donde la región del iris es independiente del tamaño del mismo y permite la comparación con otros irises. La etapa de normalización producirá imágenes de iris que tienen las mismas dimensiones.

De esta manera dos imágenes del mismo iris, adquiridas bajo diferentes condiciones, tendrían las mismas características espaciales. Para llevar a cabo esta tarea, el algoritmo propuesto utiliza el método propuesto por Daugman, denominado modelo homogéneo “rubber - sheet”.

Este modelo asignan a cada punto en el iris un para de coordenadas reales (r,q), donde r esta en el intervalo cerrado [0,1] y q es un ángulo [0,2Π]. El redibujado de la imagen del iris I(x,y) de coordenadas cartesianas a coordenadas polares dimensionales no concéntricas puede ser representado como:

$$I(x(r,\theta), y(r,\theta)) \rightarrow I(r,\theta)$$

Donde x(r, q) y y(r, q) son definidos como combinaciones lineales del conjunto de puntos del borde de la pupila y el conjunto de puntos del limite del limbos a lo largo del perímetro exterior del iris. Los dos son hallados encontrando el máximo del operador anterior.

Dado que las coordenadas radiales a partir desde el borde interno del iris hacia el borde externo tienen un intervalo de una unidad, inherentemente corrige el patrón de deformación elástica cuando la pupila cambia de tamaño.

Este método transforma la región anular del iris en una región rectangular de dimensiones constantes. En la Fig. II.9.1 se representa esta transformación, donde I(x, y) es la imagen original e In(X, Y) es la imagen normalizada, denominada iris normalizado.

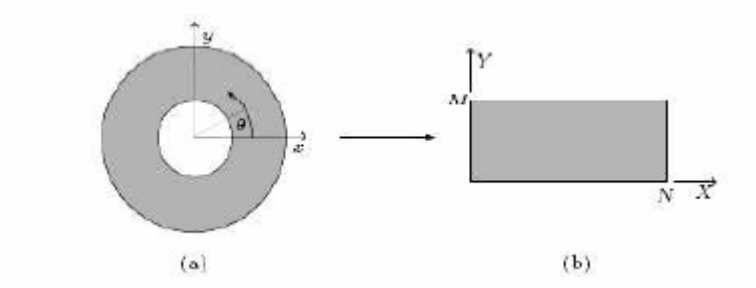

Figura. II.9.1 Normalización. (a) Imagen original I(x, y). (b) Imagen normalizada In(X, Y)

Además de generar la imagen normalizada del iris, en esta etapa se genera otra imagen denominada plantilla de ruido. La plantilla de ruido tiene las mismas dimensiones que el iris normalizado, y en esta se indican las regiones del iris normalizado donde el patrón de iris es obstruido por los parpados, ver Fig. II.9.2. La plantilla de ruido, Fig. II.9.2 (c), es utilizada como mascara en la etapa de comparación para evitar comparar regiones donde el iris es obstruido por los párpados.

Fig. II. 9.2. Normalización. (a) Imagen segmentada. (b) Iris normalizado.(c) Plantilla de ruido.

Codificación

Cada patrón aislado del iris es luego de modulado para extraer su información de fase usando al cuadratura 2D-Gabor-Wavelets. Este proceso se muestra en la figura 10, esto conduce a una fase de digitalización del patrón del iris, identificando en que cuadrante del plano complejo cada fasor resultante iría, cuando un área dada del iris es proyectada en el valor complejo de 2D-Gabor-Wavelets :

$$h_{\{Re,Im\}} = \mathrm{sgn}_{\{Re,Im\}} \int_{\rho}\int_{\phi} I(\rho,\phi) e^{-i\omega(\theta_0-\phi)} \cdot e^{-(r_0-\rho)^2/\alpha^2} e^{-(\theta_0-\phi)^2/\beta^2} \rho d\rho d\phi$$

Donde h{Re, Im}, puede ser visto el bit del valor complejo cuya parte real e imaginaria pueden ser 1 o 0 dependiendo del signo de la integral doble ;I(φ,D), es la imagen del iris en coordenadas polares que tiene el tamaño invariante y además corrige la dilatación de la pupila como hace en la sección anterior. α y β son parámetros de tamaño multiescala de dos dimensiones de wavelets, extendidos en 8 secciones de un rango de 0.15 mm a 1.2 mm en el iris.

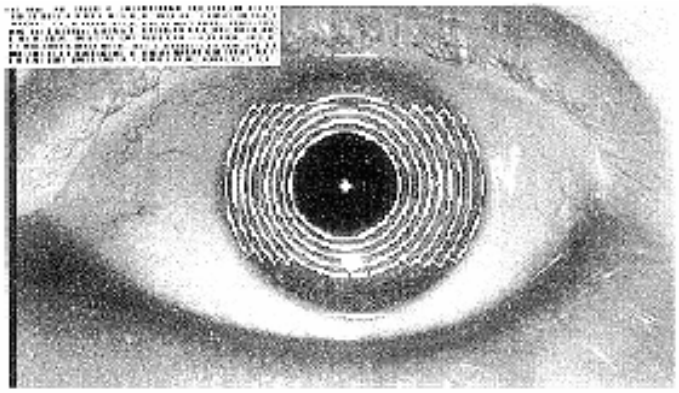

Figura II.10. (a) Mapa del Iris. En la parte superior se aprecia el código generado.

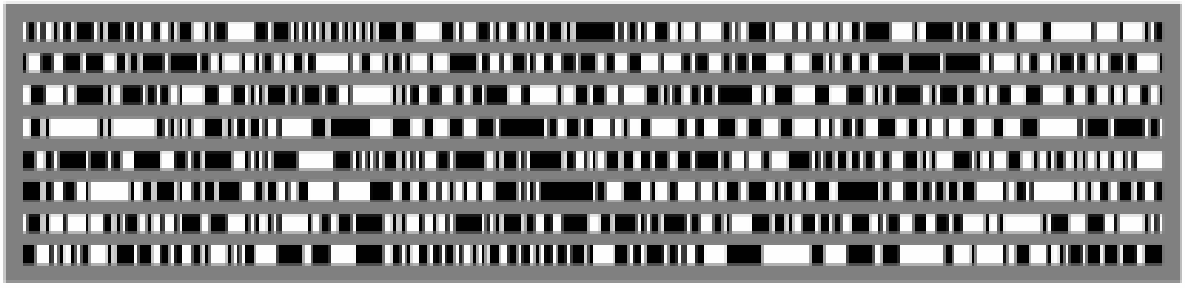

Figura II.10.1 (b) Representación pictórica del código de iris

El patrón detallado del iris es codificado en un código de 256 bytes, el cual representa todos los detalles de la textura empleando fasores en el plano complejo.

II.2.1 Reconocimiento a través del iris

La clave para el reconocimiento del iris es la falla de un test de independencia estadística, la cual involucra muchos grados de libertad, esto significa que el test es garantizado de finalizar con éxito cuando los códigos de fases de dos ojos diferentes son comparados, pero únicamente falla cuando un código de fase de un ojo es comparado con otra versión de si misma.

El test de independencia estadística es implementado por la expresión booleana XOR y es aplicada a los 2048 bits que codifican a cada uno de los dos patrones del iris. El operador XOR detecta falta de concordancia entre los correspondientes pares de bits, mientras la operación AND (intersección), asegura que los bits comparados no sean malinterpretados por puntos de los parpados, reflexiones especulares o ruido. Las normalizaciones del vector resultante y el vector mascara AND son luego calculados para determinar la distancia de Hamming como al medida de disimilitud entre dos irises, cuyos dos vectores de códigos son denotados por [codeA, codeB] y cuyas mascaras de vectores de bits son denotadas como [maskA, maskB]

$$\mathrm{HD} = \frac{\|(codeA \otimes codeB) \bigcap maskA \bigcap maskB\|}{\|maskA \bigcap maskB\|}$$

El valor de similitud absoluta es un 0, mientras que los valores mayores hasta el valor 1 representan la disimilitud.

El histograma de la figura II.11, muestra la distribución de las HDs (Hamming distance) obtenidas a partir de 9.1 millones de comparaciones entre diferentes pares de irises.

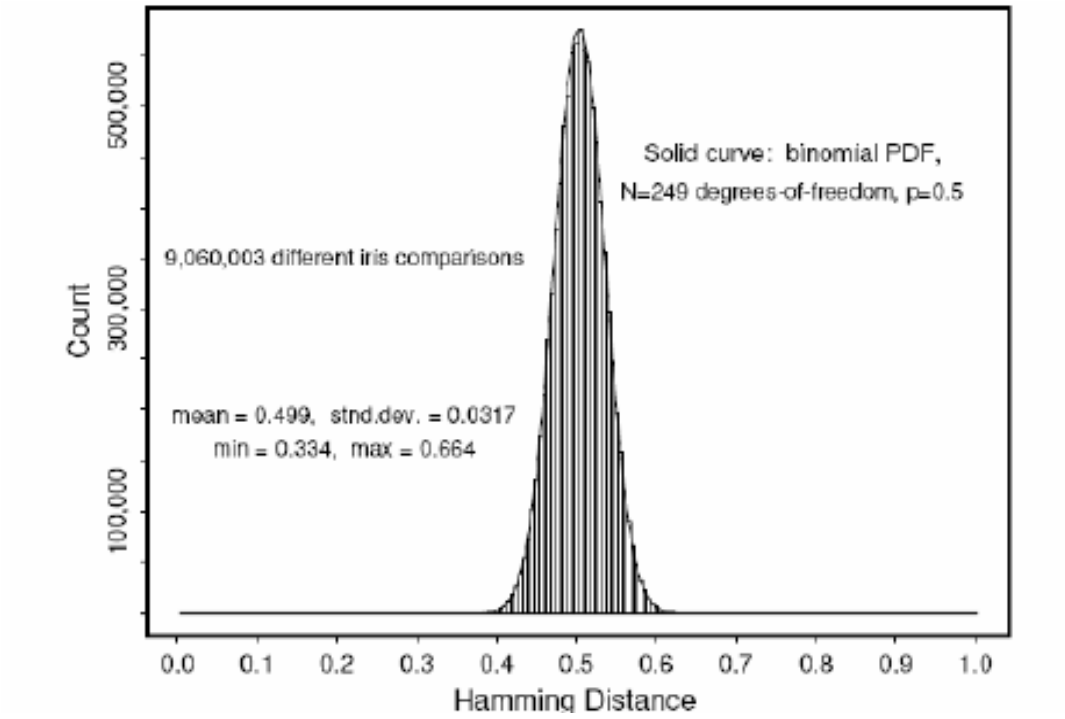

Figura II.11. Distribución de HDs a partir de 9.1 millones de comparaciones entre diferentes pares de irises de una base de datos

Cada una de las diferentes comparaciones hechas anteriormente fueron sometidas a ligeras variaciones. Se cambiaron ligeramente los iris de manera que se tuvieron 7 nuevos. Esto generó 63 millones de HDs. En el siguiente grafico se observa el histograma de solamente de los mejores valores obtenidos, es decir de los menores HDs. El HD promedio en este grafico es de 0.458 mientras que en la comparación anterior el valor promedio era de 0.499. Estos valores en teoría deberían ser iguales por lo tanto para poder identificar los patrones de iris con una alta confiabilidad necesitamos establecer un rango, este se da a través de la diferencia de estos dos últimos cálculos, lo que indicaría que para que dos irises sean iguales debe cumplirse que $HD \leq 0.32$.

II.2.2. Reconocimiento de huella dactilar

Huellas dactilares

Típicamente la huella dactilar de un individuo ha sido un patrón bastante bueno para determinar su identidad de forma inequívoca (figura II.12), ya que está aceptado que dos dedos nunca poseen huellas similares, ni siquiera entre gemelos o entre dedos de la misma persona. Por tanto, parece obvio que las huellas se convertirían antes o después en un modelo de autenticación biométrico: desde el siglo pasado hasta nuestros días se vienen realizando con éxito clasificaciones sistemáticas de huellas dactilares en entornos policiales, y el uso de estos patrones fue uno de los primeros en establecerse como modelo de autenticación biométrica. Cuando un usuario desea autenticarse ante el sistema sitúa su dedo en un área determinada, el área de lectura. Aquí se toma una imagen que posteriormente se normaliza mediante un sistema de finos espejos para corregir ángulos, y es de esta imagen normalizada de la que el sistema extrae las *minucias* (ciertos arcos, bifurcaciones y remolinos de la huella) que va a comparar contra las que se tiene en la base de datos. Es importante resaltar que el sistema no analiza la huella en sí sino las *minucias*, concretamente la posición relativa de cada una de ellas.

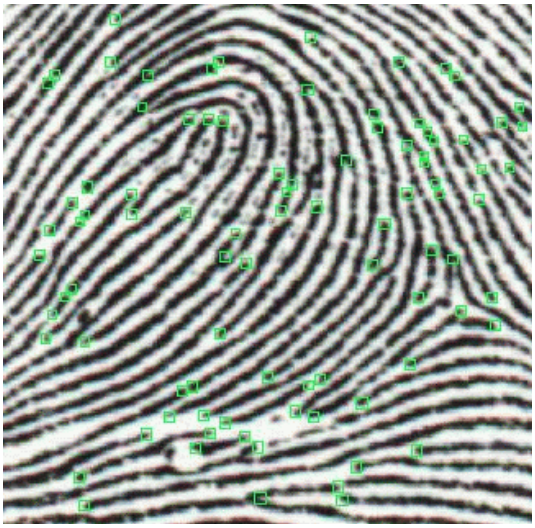

Figura II.12. Huella dactilar con minucias

Las huellas de los dedos presentan como característica principal, la presencia de un conjunto de crestas o partes donde la piel se eleva sobre las partes más bajas o valles existentes entre las crestas. Con respecto a estas crestas se definen dos características particulares que obedecen al término de *minucias*:

- Final de *cresta (ridge ending)*. Característica definida como el punto donde la cresta acaba de forma abrupta.
- Bifurcación de la *cresta (ridge bifurcation)*. Característica definida como el punto en el que la cresta se bifurca en dos o más crestas. Estas dos características quedan unívocamente definidas a partir de su localización (coordenadas x, y respecto al sistema de coordenadas central de la imagen) y de su orientación (ángulo q).

Está demostrado que dos dedos nunca pueden poseer más de ocho minucias comunes, y cada uno tiene al menos entre 30 y 40 de éstas. En la figura II.13 se muestra una imagen de una huella digitalizada con sus minucias. Si la comparación de las posiciones relativas de las minucias leídas con las almacenadas en la base de datos es correcta, se permite el acceso al usuario, denegándose obviamente en caso contrario.

Los sistemas basados en reconocimiento de huellas son relativamente baratos, en comparación con otros biométricos, como los basados en patrones de retinas. Sin embargo, tienen en su contra la incapacidad temporal de autenticar usuarios que se hayan podido herir en el dedo a reconocer. Un pequeño corte o una quemadura que afecte a varias minucias pueden hacer inútil al sistema. También elementos como la suciedad del dedo, la presión ejercida sobre el lector o el estado de la piel pueden ocasionar lecturas erróneas.

Algoritmos de huellas

Autenticación significa comprobar si un individuo es quien dice ser. El algoritmo de autenticación que se utiliza en el presente proyecto, está formado por dos bloques: en primer lugar se extraen las *minucias* características de la huella "actual" del usuario que se va a autenticar (*algoritmo de extracción de minucias*) y, en segundo lugar, se comparan esas *minucias* características de su huellas con las *minucias* almacenadas en la base de datos en forma de "plantilla" (*algoritmo de comparación de minucias*) (figura II.13).

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

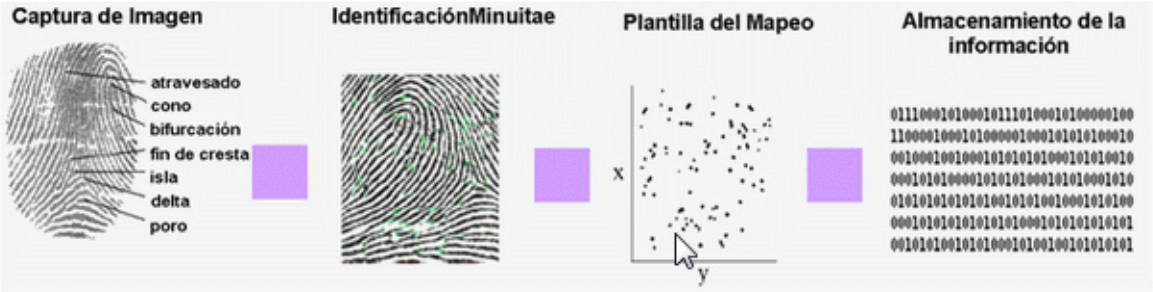

Figura II.13: Proceso común de escaneo de la huella digital

Cuando hablamos de huella "actual", se hace referencia a la huella situada sobre el lector de huellas dactilares (también huella "en vivo"), mientras que la "plantilla" se corresponde con las características extraídas de una huella anteriormente, normalmente para ser almacenada en una base de datos.

Se dice que un usuario ha sido autenticado si las características extraídas de la huella "actual" coinciden con las de la "plantilla" dentro de un límite de tolerancia para el algoritmo de comparación de *minucias*.

Algoritmo de extracción de minucias

Una de las tareas más importantes en un sistema de reconocimiento de huellas es la extracción de las *minucias* de una imagen capturada de una huella. Debido a las imperfecciones de la imagen adquirida, en algunos casos el algoritmo de extracción puede obviar algunas *minucias*, y en otros se pueden añadir *minucias* falsas. Las imperfecciones de la imagen pueden también generar errores al determinar las coordenadas de cada *minucia* y su orientación relativa en la imagen. Todos estos factores contribuyen a disminuir la fiabilidad del sistema de reconocimiento, puesto que el reconocimiento de huellas dactilares está basado en la comparación, dentro de unos límites de tolerancia, del patrón biométrico, o conjunto de *minucias* extraídas, adquirido "en vivo" y el almacenado.

A continuación describiremos en profundidad cada una de las fases de este algoritmo y lo que se consigue en estas.

Normalización de la imagen

El objetivo de esta fase es disminuir el rango de variación de grises entre los *valles* y las *crestas* de la imagen para facilitar el proceso en las siguientes etapas.

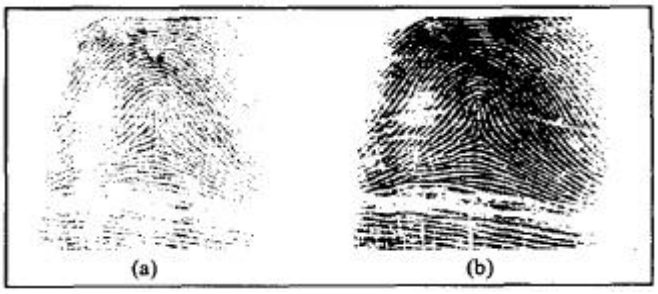

Figura II.14. (a)Huella original (b) Huella normalizada

Cálculo del campo orientación

El campo orientación representa la orientación local de las *crestas* que contiene la huella. Para estimarlo, la imagen se divide en bloques de 16x16 píxeles y se calcula la inclinación para cada píxel, en coordenadas x e y. Debido a la carga computacional del proceso de reconocimiento, es suficiente aplicar una máscara de 3x3 píxeles para el calculo de la inclinación en cada píxel.

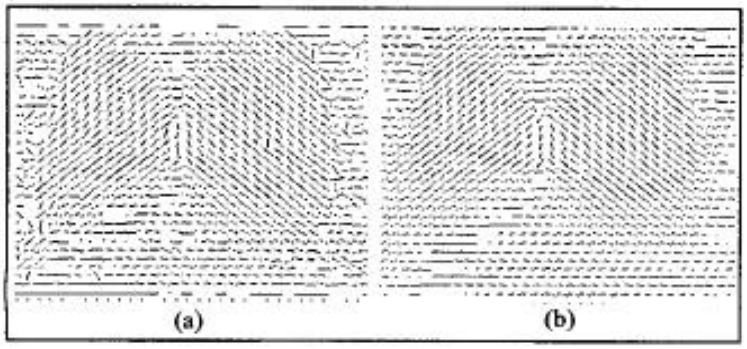

Figura II.15. (a) Huella orientada (b) Campos re alineados

El ángulo de orientación se calcula a partir de la información de la inclinación. Frecuentemente, en algunos bloques, el ángulo de orientación no se calcula correctamente debido a ruidos y daños en los *valles* y las *crestas* de la imagen capturada. Como no pueden existir variaciones significativas del ángulo entre bloques adyacentes, se aplica un nuevo filtro “espacial” de 5x5 píxeles al campo orientación estimado para reordenar correctamente todos los segmentos. La figura II.15 (a) muestra el campo orientación obtenido a partir del cálculo de la inclinación. La figura II.15 (b) muestra los campos re-alineados después de aplicar el filtro “espacial”.

Selección de la zona de interés

Debido a que la imagen contiene “ruido” de fondo, el algoritmo puede generar *minucias* fuera del área ocupada por la huella. Para evitar este problema, se selecciona el área de imagen, definida por todos los bloques de 16x16, en la que existe una alta variación del nivel de grises en la dirección normal de las *crestas* existentes (el campo orientación normal de las *crestas* se había calculado previamente). Después de esto el área de la imagen con ruido, que será excluido en las siguientes etapas, se define por bajas variaciones en todas las direcciones. En la figura II.16 se muestran las variaciones de una huella y la región de interés obtenida a partir de esta.

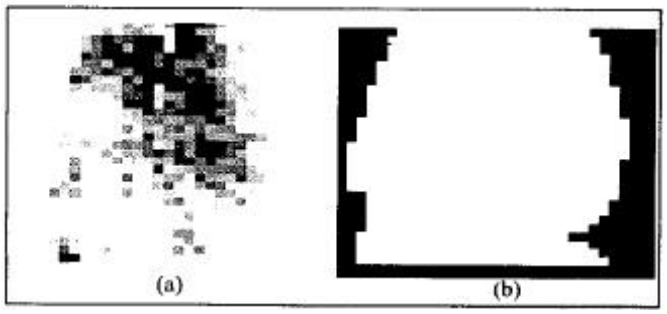

Figura II.16. (a) Variaciones de la huella (b) Región importante

Extracción de crestas

Para decidir si un píxel pertenece o no a una cresta dada, es necesario filtrar la imagen de la huella con dos máscaras adaptables, ambas capaces de incrementar el nivel de gris en la dirección normal de la cresta. La orientación de la máscara se adapta a cada bloque de 16x16 píxeles, dependiendo los ángulos obtenidos del campo orientación re alineados de la figura II.15 (b).

Si el nivel de gris de un píxel excede un umbral en las dos imágenes filtradas, se considera que el pixel pertenece a la *cresta;* de otra forma se asigna a un *valle,* produciendo una imagen binaria de la huella. Las dimensiones de la máscara son LxL y están definidas por las ecuaciones dadas en (1) y (2).

$$h_1(u,v) = \begin{cases} \dfrac{1}{\sqrt{2\Pi\delta}} \cdot e^{-\left(\frac{u-u_0}{\delta}\right)^2} & , \text{ si}: u_0 = E\left[(v_c - v)ctg(\theta) + u_c\right] \\ 0 & , \text{en otro caso} \end{cases}$$

$$h_2(u,v) = \begin{cases} \dfrac{1}{\sqrt{2\Pi\delta}} \cdot e^{-\left(\frac{v-v_0}{\delta}\right)^2} & , \text{ si}: v_0 = E\left[(u_c - u)tg(\theta) + v_c\right] \\ 0 & , \text{en otro caso} \end{cases}$$

$$\forall u, v \in [1, L]$$

Donde *u* y *v* son las coordenadas de un píxel en la máscara; (uc, vc) es el centro de la máscara; q, es el ángulo de orientación de la *cresta* en cada bloque de la imagen, y d, es un parámetro para ajustar la función máscara al ancho de la cresta. La figura II.17 (a) muestra la imagen filtrada con una de las máscaras “espaciales”. La figura II.17 (b) representa la imagen binaria obtenida después de aplicar un umbral, produciendo bordes de *crestas* lisos.

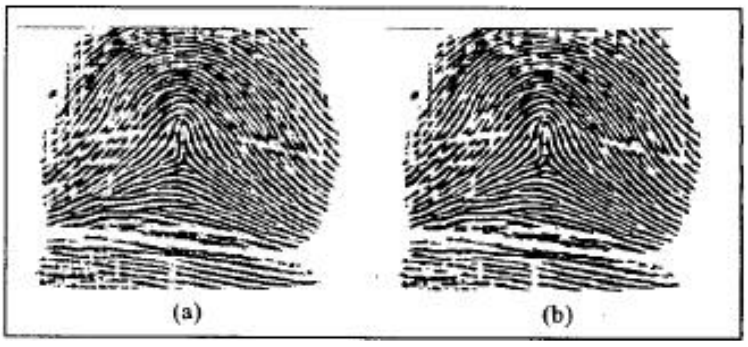

Figura II.17. (a) Imagen filtrada (b) Imagen binaria obtenida

Perfilar las crestas

Para simplificar el proceso en las siguientes etapas, se filtra la imagen para perfilar las *crestas* de la huella y eliminar las manchas de ciertas áreas. Para conseguir esto, se extraen primero los componentes de baja frecuencia y a continuación se eliminan a la imagen original, proporcionando los componentes de alta frecuencia necesarios para perfilar las crestas, como se deduce de:

$$p[u,v] = f[u,v] + \lambda \cdot f_H[u,v] = f[u,v] + \lambda \cdot (f[u,v] - f_L[u,v])$$

donde p[u,v], es el resultado de perfilar la imagen; f[u,v], es la imagen binaria; fH[u,v] y fL[u,v] son, respectivamente, las imágenes de alta y baja frecuencia; y l es un factor (l>0), que determina el grado de perfilación. En la figura II.18(a) se muestra el resultado de la huella después de aplicarle el primer filtro. Se puede aplicar un nuevo filtro para eliminar las *crestas* falsas debidas a manchas en la imagen. En este caso se utiliza una máscara "espacial" capaz de adaptar su orientación localmente a la orientación de la cresta.

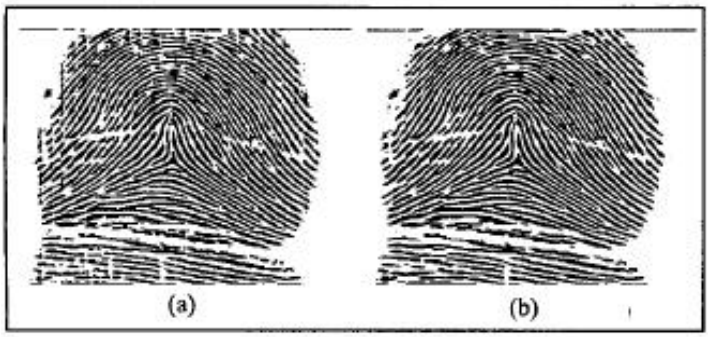

Figura II.18. (a) Imagen después del primer filtro perfilador
(b) Imagen después del segundo filtro perfilador con máscara espacial

Simplificación

En este paso se aplican dos algoritmos consecutivos paralelos de simplificación, para reducir a un único píxel el ancho de las *crestas* en la imagen binaria. Estas operaciones son necesarias para simplificar es siguiente análisis estructural de la imagen para la extracción de las *minucias* de la huella.

La simplificación se debe realizar sin modificar la estructura original de las *crestas* de la imagen. Durante este proceso, el algoritmo no puede calcular mal los comienzos, finales y, o bifurcaciones de las *crestas*, ni las *crestas* se pueden romper.

Eliminar imperfecciones

Después de la simplificación, dependiendo de la calidad de la imagen, las imperfecciones estructurales de la huella original permanecen en un cierto grado. Esto conlleva *crestas* rotas, *crestas* falsas y huecos; así que, es necesario aplicar un algoritmo para eliminar todo las líneas que no se corresponden a *crestas* y un algoritmo para enlazar *crestas* rotas. La figura II.19 (a) muestra la imagen adelgazada obtenida una vez aplicado el algoritmo de adelgazamiento y eliminación de imperfecciones.

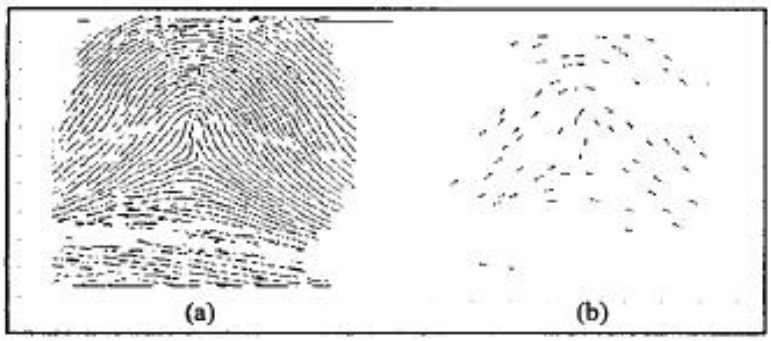

Figura II.19.
(a) Imagen después de la simplificación y eliminación de imperfecciones
(b) Patrón de minucias después del proceso de eliminación de conjuntos

Extracción de *minucias*

En la última etapa, se extraen las minucias de la imagen simplificada, obteniendo el patrón biométrico de la huella (*plantilla*). Este proceso conlleva la determinación de: (i) si un píxel pertenece o no a una *cresta* y, (ii) si es así, si es una bifurcación, comienzo o final de *cresta* obteniendo así un grupo de candidatos a *minucias*. A continuación, todos los puntos en el borde de la zona de interés se borran. Entonces, puesto que la densidad de *minucias* por unidad de área no puede exceder un cierto valor, todos los conjuntos de puntos candidatos cuya densidad excede este valor son sustituidos por una simple *minucia* localizada en el centro del conjunto. En la figura II.19 (b) se muestra el patrón de *minucias* resultante.

Una vez finalizado el proceso de extracción de minucias la *plantilla* contiene entre 70 y 80 minucias. En la figura II.20 se muestra el patrón de minucias obtenido superpuesto sobre la imagen de la huella normalizada:

Figura II.20. Patrón de minucias

Algoritmo de comparación de *minucias*

Con el emparejamiento se determina si dos huellas son del mismo dedo o no. Las dos características usadas en el emparejamiento de huellas son los finales y las bifurcaciones de las *crestas* (*minucias*).

A continuación se explica en detalle cada una de las etapas del algoritmo de comparación de minucia:

Para cada *minucia* detectada, se almacenan los siguientes parámetros:

- ✓ Coordenadas x e y de la *minucia.*
- ✓ Orientación definida como la orientación local de la *cresta* asociada.
- ✓ El tipo de *minucia*, que puede ser *final de cresta* o *bifurcació*n.
- ✓ La *cresta* asociada.

Para la comparación de las minucias se utilizarán las coordenadas polares de estas.

Alineación del conjunto de minucias

Si denotamos por P al conjunto M de *minucias* en la imagen *plantilla* tenemos que:

$$P = \left(\left(x_1^P, y_1^P, \theta_1^P \right)^T, \ldots, \left(x_M^P, y_M^P, \theta_M^P \right)^T \right)$$

y llamando Q al conjunto de N minucias en la imagen de “entrada” (la que se va a comparar con la imagen *plantilla*) tenemos:

$$Q = \left(\left(x_1^Q, y_1^Q, \theta_1^Q \right)^T, \ldots, \left(x_N^Q, y_N^Q, \theta_N^Q \right)^T \right)$$

Para cada *minucia* Pi) 1 (*M i* £ £ y Qj (1 £ *j* £ *N*) en el conjunto de *minucias* de la imagen de “entrada” y de la *plantilla*, denotamos *rotate[i][j]* como el ángulo de rotación entre la imagen de “entrada” y la *plantilla*, tomando Pi y Qj como el punto de referencia de la imagen.

Si podemos tomar Pi y Qj como un par de *minucias,* las *crestas* asociadas de Pi y Qj son iguales dentro de un cierto grado *rotate[i][j],* que asumiremos de un valor entre 0 y 360, en otro caso pondremos *rotate[i][j]* como 400 para representar el hecho de que Pi y Qj no se corresponden con un par de *minucias*.

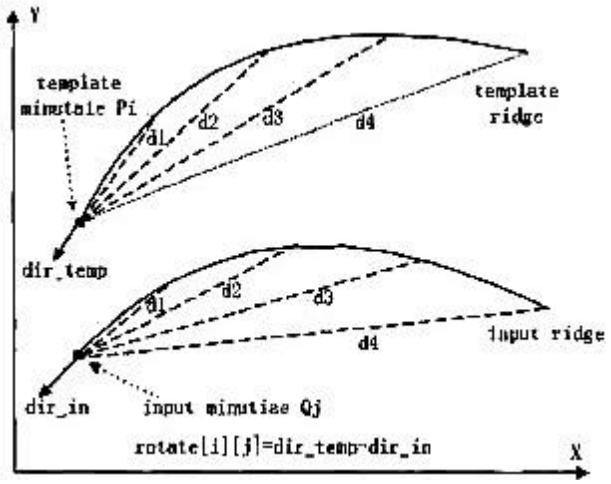

Figura II.21. Alineación de la cresta de entrada y la cresta plantilla

Si Pi y Qj no son del mismo tipo, se asigna 400 a *rotate[i][j]*. Por otra parte denotaremos por R y r a las *crestas* a las que pertenecen de las minucias Pi y Qj . Se compara R con r para obtener las diferencias de estas dos *crestas* de acuerdo a la ecuación siguiente:

$$Diff\_dist = \frac{1}{L}\sum_{i=0}^{L}\left|R(d_i) - r(d_i)\right|$$

$$Diff\_ang = \frac{1}{L}\sum_{i=0}^{L}\left|R(\alpha_i) - r(\alpha_i)\right|$$

Donde L es el número de puntos grabados. R(di) es la distancia desde el punto i en la *cresta* R a la minucia Pi . R(*a*i) es el ángulo entre la línea que conecta el punto i sobre la cresta R a la *minucia* Pi y la orientación de la minucia Pi ; r(di) y r(*a*i) tienen significados similares. Si *Diff_dist* es más grande que *Td* o *diff_ang* es mayor que *To*, se pone *rotate[i][j]* a 400. De otra forma calculamos *rotate[i][j]* como:

Rotate[i][j] = *dir_Temp* – *dir_in* Donde *dir_temp* es la orientación de Pi y *dir_in* es la orientación de Qj.

Para alinear el conjunto de *minucias* de entrada con el conjunto de minucias de la *plantilla* en la coordenada polar, lo que se necesita hacer es trasladar las *minucias* de la imagen de entrada y las de la *plantilla* a coordenadas polares con respecto a las *minucias* de referencia Pi y Qj, y a continuación añadir el ángulo *rotate[i][j]* al ángulo radial de la coordenada polar de cada minucia de “entrada”. Es decir, para una *minucia* (xi, yi, qi)T aplicamos la siguiente ecuación:

$$\begin{pmatrix} r_i \\ e_i \\ \theta_i \end{pmatrix} = \begin{pmatrix} \sqrt{\left(x_i - x^r\right)^2 + \left(x_i - y^r\right)^2} \\ \tan^{-1}\left(\frac{y_i - y^r}{x_i - x^r}\right) + rotate[i][j] \\ \theta_i - \theta^r \end{pmatrix}$$

Donde (xr, yr, qr) T es la coordenada de la *minucia* de referencia, y (ri, ei, qi) T es la representación de la *minucia* en el sistema de coordenadas polares (ri representa la distancia radial, ei representa el ángulo radial, y qi; representa la orientación de la *minucia* con respecto a la *minucia* de referencia).

Comparación de las minucias alineadas

Los pasos del algoritmo de comparación de *minucias* son los siguientes:

1) Para *i*(1£ *i* £ *M*) y *j*(1£ *j* £ *N*) , si *rotate[i][j]=400*, se repite este paso y se elige otro Pi y Qj , sino se va al paso 2. Si se ha hecho para todos los pares de *minucias*, se va al paso 5.

2) Poner Pi y Qj como *minucia* de referencia. Convertir cada *minucia* en el conjunto de *minucias* de la *plantilla* y conjunto de *minucias* de entrada al sistema de coordenadas polares con respecto a la correspondiente *minucia* de referencia a través del método descrito al final de la sección 2.1.

3) Representar las *minucias* de la *plantilla* y de la entrada en el sistema de coordenadas polares como cadenas simbólicas, concatenando cada *minucia* en orden creciente de ángulos radiales:

$$P_i^s = \left(\left(r_1^P, e_1^P, \theta_1^P \right)^T, \ldots, \left(r_M^P, e_M^P, \theta_M^P \right)^T \right)$$

$$Q_i^s = \left(\left(r_1^Q, e_1^Q, \theta_1^Q \right)^T, \ldots, \left(r_N^Q, e_N^Q, \theta_N^Q \right)^T \right)$$

4) Comparar las cadenas resultantes Pis y Qj s para encontrar el nivel de coincidencia de Pi s y Qj s. Asignar a *m_score[i][j]* el valor del resultado.
Continuar en el paso 1.

5) Encontrar el máximo valor de *m_score[i][j]* y usarlo como el nivel de coincidencia del conjunto de *minucias* de la entrada y la *plantilla*. Si el nivel de coincidencia es mayor que un umbral, se considera que la imagen de “entrada” se originó a partir de la misma huella que la *plantilla*, sino se considera que las dos imágenes provienen de dedos diferentes.

II.2.3. Reconocimiento de voz y firma

Voz

Otro elemento que puede ser analizado para su aplicación biométrica es la voz humana. Todas las personas tenemos un tono de voz que nos caracteriza, y una forma de hablar específica (pausada, lenta, rápida, etc.). Por lo tanto el análisis de la voz es un análisis físico y de conducta del individuo.

Un algoritmo utilizado para el reconocimiento de voz es el siguiente:

Figura II.22. Algoritmo de reconocimiento de voz.

Pre-procesamiento: convierte la entrada de voz a una forma que el sistema pueda procesar. Esto se logra aplicando reducciones de ruido y amplificación de la señal, de manera que se obtiene una señal de entrada óptima.

Reconocimiento: traduce la señal a texto, y ejecuta el análisis de la señal.

- ✓ Articulación: la forma en la que la persona *produce* los sonidos.
- ✓ Acústica: analiza la señal como una secuencia de sonidos.
- ✓ Percepción auditiva: analiza la forma en la que la persona *procesa* el habla.

Comunicación: envía los datos procesados al sistema de software o hardware que lo requiera. También envía el resultado de la validación en caso de que la voz se compare con la información de la base de datos.

II.2.4. Reconocimiento del rostro

Patrones faciales

Dentro del reconocimiento de patrones, existe una premisa importante: los objetos pueden ser correctamente clasificados si la variabilidad dentro de instancias de una clase dada, es menor que la variabilidad entre dos clases diferentes. Tomando como ejemplo el reconocimiento de rostros, en él se presentan grandes dificultades para ubicar los ojos, la nariz, boca, y demás. Y donde además, los gestos, las muecas y el paso del tiempo modifican el patrón de identificación.

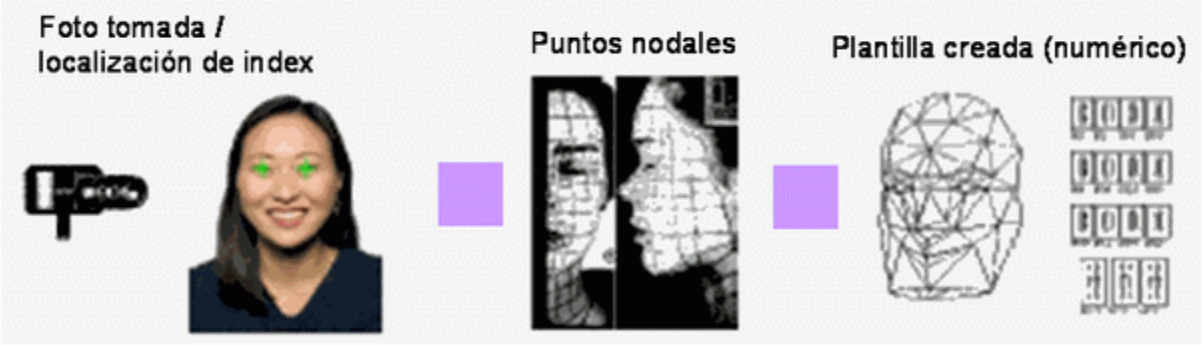

Figura II.23. Sistema de reconocimiento facial

El reconocimiento del rostro de una persona es uno de los métodos más aceptados por los usuarios, junto con la huella digital.

El método de patrones faciales es utilizado con frecuencia en robots, para detectar a las personas y poder diferenciarlas.

Sin embargo, es un método que es difícil de implementar, y tiene la desventaja de que no es una característica fija, sino que el rostro de una persona varía con la edad.

Análisis de componentes principales

Esta técnica consiste en obtener la imagen del rostro de la persona, y aplicar algoritmos de compresión para eliminar información que no es útil, como por ejemplo el cabello, el color y el maquillaje6. De esta manera se obtiene una imagen muy reducida que contiene toda la información necesaria para identificar a la persona. Esta imagen también se conoce como Eigenface. (Ver figura II.24)

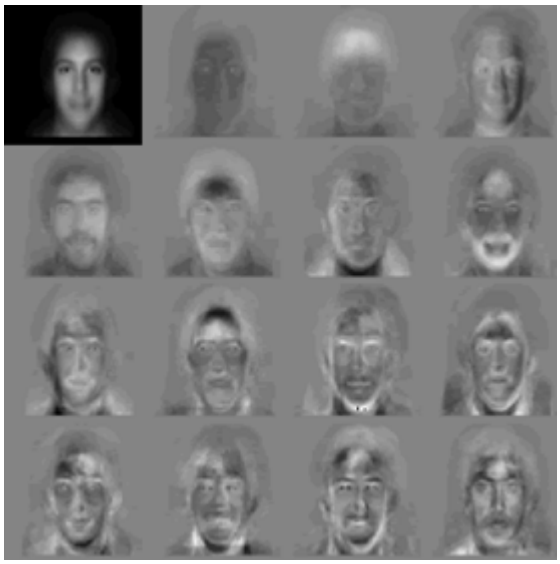

Figura II.24. Análisis de rostros utilizando la técnica de análisis de componentes principales (Eigenfaces)

El algoritmo de reconocimiento debe alinear los ojos y bocas de los sujetos, antes de comenzar la compresión de las imágenes. Luego se aplica la compresión para reducir la dimensión de los datos, de forma que se revela la estructura de los patrones faciales.

Análisis lineal discriminante

Este método de análisis presenta la ventaja de que puede validar a un usuario aunque su imagen no sea exactamente igual en todas las ocasiones. Por ejemplo, en la siguiente figura se observan cinco rostros para cada persona. Las caras no son exactamente iguales, pero el algoritmo permite decidir si la persona es la misma o es otra diferente. (Ver figura II.25)

Figura II.25. Seis usuarios diferentes presentan cinco rostros. Las imágenes de cada usuario presentan diferencias entre sí.

Agrupaciones de grafos elásticos EBGM

Este método toma en cuenta que una imagen real tiene muchas características que varían, como por ejemplo la iluminación, postura y la expresión facial. El algoritmo que se utiliza se denomina filtro de Gabor, que se utiliza para detectar formas y extraer características utilizando el procesamiento de la imagen. Este algoritmo localiza puntos importantes en el rostro, respecto a un punto de referencia. (Ver figura II.26)

Figura II.26. Imagen analizada utilizando EBGM.

II.3. Tabla comparativa de lectores biométricos.

Tecnología	Como Trabaja	Tamaño plantilla (bytes)	Fiabilidad	Facilidad De Uso	Posibles Incidencias	Costo	Aceptación Usuario
Huella digital	Captura y compara patrones de la huella digital	250-1000	Muy alta	Alta	Ausencia de miembro	Bajo	Alta
Geometría de la mano	Mide y compara dimensiones de la mano y dedos	9	Baja	Alta	Edad, Ausencia de miembro	Bajo	Alta
Retina	Captura y compara los patrones de la retina	96	Baja	Baja	Gafas	Alto	Baja
Iris	Captura y compara los patrones del iris	512	Baja	Baja	Luz	Muy alto	Baja
Geometría facial	Captura y compara patrones faciales	84 o 1300	Baja	Baja	Edad, Cabello, luz	Medio	Baja
Voz	Captura y compara cadencia, pitch, y tono de la voz	10000-20000	Alta	Media	Ruido, temperatura y meteorología	Alto	Media
Firma	Captura y compara ritmo, aceleración, y presión de la firma	1000 – 3000	Alta	Media	Edad, cambios, analfabetismo	Alto	Media

II.4. Procesos de Autentificación e Identificación biométrica

Procesos de Autentificación e Identificación biométrica

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

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

El proceso de autentificación o verificación biométrica es más rápido que el de identificación biométrica, sobre todo cuando el número de usuarios (N) es elevado.

Esto es debido a que la necesidad de procesamiento y comparaciones es más reducido en el proceso de autentificación. Por esta razón, es habitual usar autentificación cuando se quiere validar la identidad de un individuo desde un sistema con capacidad de procesamiento limitada o se quiere un proceso muy rápido (figura II.27).

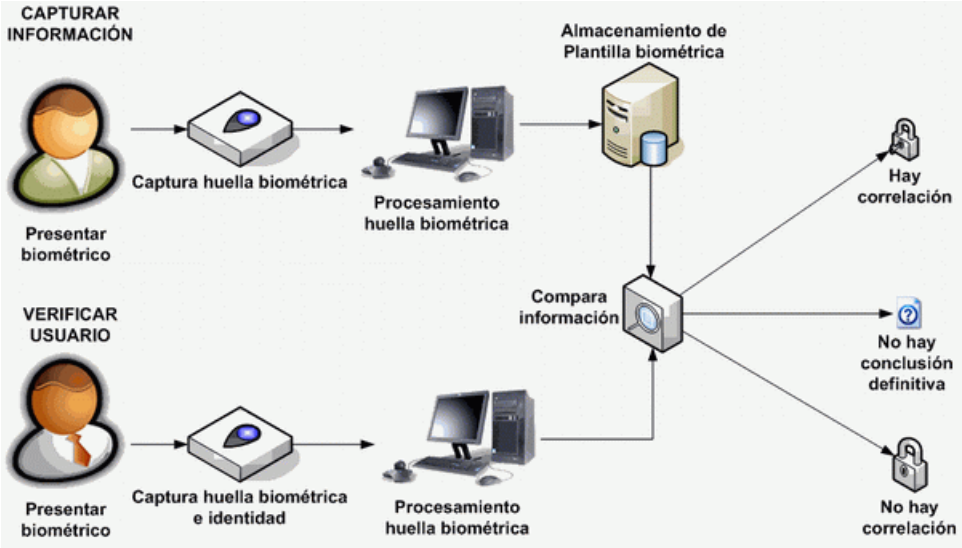

Figura II.27. Sistema de reconocimiento de huella dactilar

II.5. Funcionamiento y rendimiento

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

El rendimiento de una medida biométrica se define generalmente en términos de tasa de falsa aceptación (*False Acceptance Rate* o FAR) la probabilidad de que el sistema autentique correctamente a un usuario ilegítimo, la tasa de falso rechazo (*False NonMatch Rate* o FNMR, también *False Rejection Rate* o FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente ; evidentemente, una FRR alta provoca descontento entre los usuarios del sistema, pero una FAR elevada genera un grave problema de seguridad, proporcionando acceso a un recurso a personal no autorizado.

Para determinar las prestaciones de un sistema biométrico se suele utilizar la tasa de éxito (*Success Rate, SR*) que responde a una combinación de los dos factores anteriores:

$$SR= 1 – (FAR +FRR)$$

El *FAR* y el *FRR* responden a parámetros inversamente proporcionales, por tanto, variarán en función de las condiciones prefijadas por el programa de identificación biométrica. Así si por ejemplo se tiene que utilizar el programa en un entorno de máxima seguridad, se intentará que el *FAR* sea lo más pequeño posible, aunque esta acción signifique de forma explícita, el incremento drástico del factor *FRR*.

Por lo tanto se debe fijar un parámetro o umbral que permita igualar los dos factores, asegurando de esta manera el óptimo funcionamiento del sistema. Este umbral se denomina tasa de error igual (*Equal Error Rate*, ERR), y es el que determinará, finalmente, la capacidad de identificación del sistema. En la figura II.28 se muestra dicha relación.

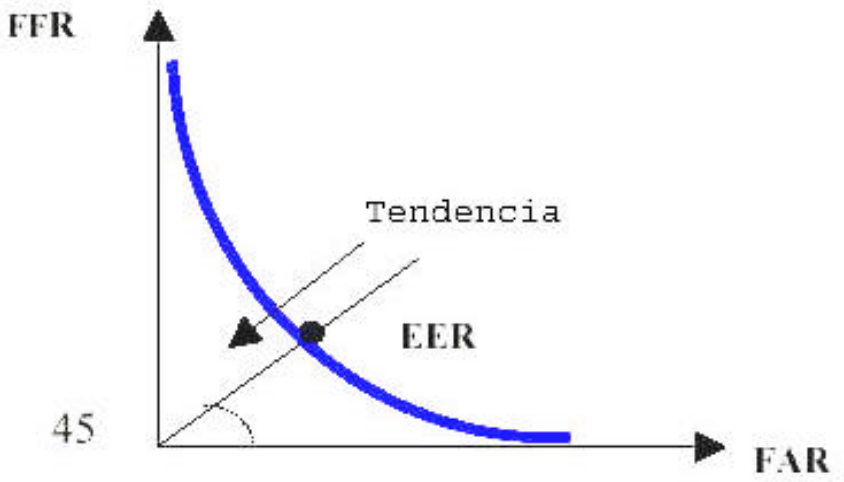

Figura II.28. Relación entre FAR, FRR y ERR

Tabla comparativa de sistemas biométricos

De acuerdo características de los sistemas biométricos:

	Ojo (Iris)	Huella	Escritura y firma	Voz	Cara
Fiabilidad	Muy alta	Alta	Media	Alta	Alta
Facilidad de uso	Media	Alta	Alta	Alta	Alta
Prevención de ataques	Muy alta	Alta	Media	Media	Media
Aceptación	Media	Alta	Muy alta	Alta	Media
Estabilidad	Alta	Alta	Baja	Media	Media

CAPITULO III. COMPONENTES DE UN SISTEMA BIOMETRICO.

III.1. Lector de huella dactilar.

El objetivo al utilizar un Sistema de Control de Asistencia utilizando un equipo que incluya un lector de huella dactilar (figura III.1) es realizar un software que permita llevar registro automático del tiempo laborado e incidencias del personal en base a los turnos y políticas definidas por la empresa u organización.

El programa Control de Asistencia confronta el registro de checadas contra el turno definido del trabajador realizando un cálculo preciso del tiempo laborado, tiempo extra, tiempo de labor en día de descanso y tiempo de labor en día festivo. Se obtendrán reportes en Formato Control de Asistencia de los empleados, Faltas, Retardos, Tiempo Extra y un reporte de Pre nómina si así se define.

Figura III.1

Justificación

La asistencia y control de personal docente requiere que los usuarios autentifiquen su identidad a través de un método que no permita la suplantación de identidad. El lector de huellas digitales nos permite registrar el ingreso del personal colocando el dedo sobre un sensor, en lugar de usar el teclado para ingresar sus datos. El lector de huellas digitales viene integrado en la carcasa del equipo y el mismo incluye un display que muestra la hora de registro y despliega la información del usuario al pasar su huella por el sensor. El dispositivo lector guarda un registro de los usuarios y puede realizar una autenticación 1:1 (validación de un usuario y una clave) o 1:N (Validación de un usuario contra la base de datos completa de todos los usuarios del sistema). Asimismo el lector podrá operar de manera “on-line” (validación inmediata del usuario contra una base de datos alojada en la PC) o en modo “off-line” (validación del usuario contra la información guardada en el dispositivo lector que cuenta con memoria propia).

Preguntas más frecuentes

¿Cómo funciona un lector de huellas digitales?

Probablemente ya conoce los lectores de códigos de barra que se usan en los supermercados. Cuando adquiere un artículo, el cajero pasa el lector sobre el código de barras del producto y el sistema identifica el artículo y su precio.
Un lector de huellas digitales funciona de una manera similar. Cuando pasa el dedo sobre el sensor de huellas digitales, la PC lo identifica y lo registra. Como su huella digital es única, ninguna otra persona podrá usar su nombre de usuario o contraseña.

Ventajas de usar el lector de huellas digitales para controlar el registro de asistencia

Los lectores de huellas digitales son un medio muy seguro de controlar el registro de asistencia porque no existe nadie que tenga su misma huella digital. Con un lector de huellas digitales, su nombre de usuario y contraseña se ingresan al pasar el dedo sobre el lector.

¿Cómo se utiliza el lector de huellas digitales?

Una vez que se haya configurado el lector de huellas digitales, basta pasar el dedo sobre el sensor para usarlo.
Si el lector de huellas digitales no reconoce su huella, lea los siguientes consejos para asegurar que el lector obtenga una buena imagen de su huella digital.

- Deje el dedo recto al pasarlo sobre el lector.
- Pase el dedo en línea recta, sin inclinarlo ni girarlo hacia los lados.
- Pase el dedo lentamente para darle tiempo al sensor para que reconozca su huella.

¿Cómo se configura el lector de huellas digitales?

La primera vez que vaya a usar el lector de huellas digitales, debe registrar sus huellas digitales con el Asistente de registro de huellas para que sirva de modelo de comparación (Figura III.2).

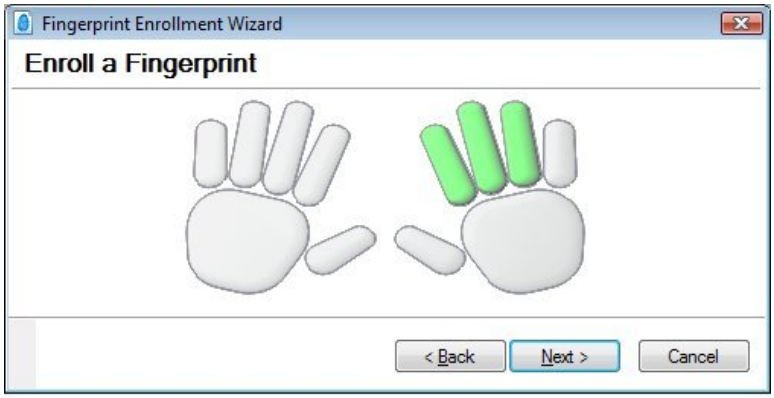

Figura III.2

Capacidad de registro

El dispositivo lector es capaz de almacenar las 10 huellas de cada persona para permitir su registro y acceso, no es una práctica muy común ya que al hacer esto se limita el número de usuarios que el sistema puede mantener en memoria o el número de registros en el mismo.

Luego de registrar sus huellas digitales, sólo necesita pasar su dedo por el sensor de huellas para la verificación (Figura III.3).

Figura III.3 Dispositivos de lectura de huella dactilar

Comparación de este sistema contra otros basados en PC

DESCRIPCIÓN	Equipo que Integra Lector de Huella	Solo lector	COMENTARIOS
Requiere de una PC atada al lector	No	Si	El equipo integrado trabaja y opera en forma independiente. Es un servidor independiente , desde un nodo de la red se pueden obtener reportes
Hay disco duro	No	Si	Los discos duros se dañan rápidamente. El equipo integrado usa memoria flash sin partes mecánicas, lo que asegura mayor tiempo de vida sin problemas
Problemas de virus	No	Si	El equipo integrado está basado en memoria flash y no necesita de licencias de antivirus.
Licencias de Windows	No	Si	El equipo integrado tiene su propio sistema operativo basado en un servidor de web , se evita el problema de parchar y licenciar nuevas versiones
Opción a trabajar con batería hasta por 24 horas	Si	No	Se puede conectar batería de respaldo que son mucho mas eficientes que los no break que solo duran pocos minutos
Las sucursales remotas requieren de PC	No	Si	Las sucursales remotas donde no hay personal técnico ni de mantenimiento operan fácilmente pues El equipo integrado es independiente, opera por si solo
Gastos ocultos del equipo	No	Si	El costo de una pc por reloj, su Windows, sus antivirus, su contrato de mantenimiento, actualizaciones constantes de software y hardware, visitas continuas de personal de soporte, gastos por administración de una PC adicional en sucursales remotas y locales.
Equipo voluminosos y difícil de instalar	No	Si	El El equipo integrado mide aproximadamente 10 x 15 x 4 cm. La PC, requiere cpu, gabinete, monitor y un escritorio, cablear los componentes

III.2. Bridge Ethernet-RF para conexión a sistema de información Central.

Ethernet es un estándar de redes de computadoras de área local con acceso al medio por contienda CSMA/CD. El nombre viene del concepto físico de *éter*. Ethernet define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI. La Ethernet se tomó como base para la redacción del estándar internacional IEEE 802.3. Usualmente se toman Ethernet e IEEE 802.3 como sinónimos. Ambas se diferencian en uno de los campos de la trama de datos. Las tramas Ethernet y IEEE 802.3 pueden coexistir en la misma red.

Tecnología y velocidad de Ethernet

Hace ya mucho tiempo que Ethernet consiguió situarse como el principal protocolo del nivel de enlace. Ethernet 10Base2 consiguió, ya en la década de los 90s, una gran aceptación en el sector. Hoy por hoy, 10Base2 se considera como una "tecnología de legado" respecto a 100BaseT.

Las tecnologías Ethernet que existen se diferencian en estos conceptos:

Velocidad de transmisión

- ✓ Velocidad a la que transmite la tecnología.

Tipo de cable

- ✓ Tecnología del nivel físico que usa la tecnología.

Longitud máxima

- ✓ Distancia máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).

Topología

- ✓ Determina la forma física de la red. Bus si se usan conectores T (hoy sólo usados con las tecnologías más antiguas) y estrella si se usan hubs estrella de difusión) o switches (estrella conmutada).

A continuación se especifican los anteriores conceptos en las tecnologías más importantes:

Tecnologías Ethernet

Tecnología	**Velocidad de transmisión**	**Tipo de cable**	**Distancia máxima**	**Topología**
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (Hub o Switch)
10BaseF	10 Mbps	Fibra óptica	2000 m	Estrella (Hub o Switch)
100BaseT4	100Mbps	Par Trenzado (categoría 3UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseTX	100Mbps	Par Trenzado (categoría 5UTP)	100 m	Estrella. Half Duplex(hub) y Full Duplex(switch)
100BaseFX	100Mbps	Fibra óptica	2000 m	No permite el uso de hubs
1000BaseT	1000Mbps	4 pares trenzado (categoría 5e ó 6UTP)	100 m	Estrella. Full Duplex (switch)
1000BaseSX	1000Mbps	Fibra óptica (multimodo)	550 m	Estrella. Full Duplex (switch)
1000BaseLX	1000Mbps	Fibra óptica (monomodo)	5000 m	Estrella. Full Duplex (switch)

Hardware comúnmente usado en una red Ethernet

Los elementos de una red Ethernet son: Tarjeta de Red, repetidores, concentradores, puentes, los conmutadores, los nodos de red y el medio de interconexión. Los nodos de red pueden clasificarse en dos grandes grupos: Equipo Terminal de Datos (**DTE** Data Terminal Enable) y Equipo de Comunicación de Datos (**DCE** Data Communication Enable). Los DTE son dispositivos de red que generan lo que son el destino de los datos: como los PCs, las estaciones de trabajo, los servidores de archivos, los servidores de impresión; todos son parte del grupo de las estaciones finales. Los **DCE** son los dispositivos de red intermediarios que reciben y retransmiten las tramas dentro de la red; pueden ser: ruteadores, conmutadores (switch), concentradores (hub), repetidores o interfaces de comunicación. P. ej.: un módem o una tarjeta de interface.

- ✓ NIC, o Tarjeta de Interfaz de Red - permite que una computadora acceda a una red local. Cada tarjeta tiene una *única* dirección MAC que la identifica en la red. Una computadora conectada a una red se denomina **nodo**.
- ✓ Repetidor o *repeater* - aumenta el alcance de una conexión física, recibiendo las señales y retransmitiéndolas, para evitar su degradación, a través del medio de transmisión, lográndose un alcance mayor. Usualmente se usa para unir dos áreas locales *de igual* tecnología y sólo tiene *dos* puertos. Opera en la capa física del modelo OSI.
- ✓ Concentrador o *hub* - funciona como un repetidor pero permite la interconexión de *múltiples* nodos. Su funcionamiento es relativamente simple pues recibe una trama de ethernet, por uno de sus puertos, y la repite por todos sus puertos restantes sin ejecutar ningún proceso sobre las mismas. Opera en la capa física del modelo OSI.
- ✓ Puente o *bridge* - interconecta segmentos de red haciendo el cambio de *frames* (tramas) entre las redes de acuerdo con una tabla de direcciones que le dice en qué segmento está ubicada una dirección MAC dada.

Conexiones en un Switch Ethernet

Conmutador o *Switch* - funciona como el *bridge*, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los *switches* pueden tener otras funcionalidades, como *Redes virtuales*, y permiten su configuración a través de la propia red. Funciona básicamente en la capa 2 del modelo OSI (enlace de datos). Por esto son capaces de procesar información de las tramas; su funcionalidad más importante es en las tablas de dirección. Por ej.: una computadora conectada al puerto 1 del conmutador envía una trama a otra computadora conectada al puerto 2; el *switch* recibe la trama y la transmite a todos sus puertos, excepto aquel por donde la recibió; la computadora 2 recibirá el mensaje y eventualmente lo responderá, generando tráfico en el sentido contrario; ahora el *switch* conocerá las direcciones **MAC** de las computadoras en el puerto 1 y 2; cuando reciba otra trama con dirección de destino de alguna de ellas, sólo transmitirá la trama a dicho puerto disminuyendo así el tráfico de la red y contribuyendo al buen funcionamiento de la misma.

El bridge inalámbrico convierte virtualmente cualquier dispositivo Ethernet (lector de huella dactilar, consola de videojuegos, impresora, portátil o, incluso una computadora de escritorio) en un dispositivo de red inalámbrica. Al incorporar el bridge inalámbrico a la red, el acceso al lector de huella dactilar y la transferencia de datos desde y hacia una computadora personal (PC) puede controlarse inalámbricamente, sin la molestia de tener que instalar cables Ethernet por las paredes y por los techos.

El bridge inalámbrico cuenta también con la encriptación WEP a 128-bit, que aumenta la protección de los datos en la red existente. Con el nivel de seguridad que proporciona, ninguna persona que no esté autorizada podrá acceder a la red si no cuenta con un permiso.

La mayoría de los bridges inalámbricos existentes en el mercado no requiere que se instale software ni que se configuren controladores, por tanto, es una auténtica muestra de un producto plug and play (instalar y utilizar), siempre y cuando el sistema operativo del ordenador personal esté basado en Ethernet. Este económico bridge inalámbrico 802.11b/g de alta velocidad ofrece un rendimiento de calidad al aumentar el número de dispositivos y de periféricos en la red inalámbrica.

Características Generales	
Tipo de dispositivo	Puente (Bridge)
Factor de forma	Externo
Anchura	Variable
Profundidad	Variable
Altura	Variable
Peso	

Conexión de redes	
Tecnología de conectividad	Inalámbrico, cableado
Velocidad de transferencia de datos	108 Mbps
Banda de frecuencia	2.4 GHz
Formato código de línea	CCK, BPSK, QPSK, PBCC, OFDM
Protocolo de interconexión de datos	Ethernet, Fast Ethernet, IEEE 802.11b, IEEE 802.11g
Método de espectro expandido	OFDM
Alcance máximo en interior	100 m
Alcance máximo al aire libre	400 m
Indicadores de estado	Actividad de enlace, alimentación
Características	Señal ascendente automática (MDI/MDI-X automático)
Cumplimiento de normas	IEEE 802.3, IEEE 802.3u, IEEE 802.11, IEEE 802.11b, IEEE 802.11g

Antena	
Antena	Externa desmontable
Cantidad de antenas	1
Expansión / Conectividad	
Interfaces	1 x red - Radio-Ethernet 1 x nodo de red - Ethernet 10Base-T/100Base-TX - RJ-45
Diverso	
Algoritmo de cifrado	RC4, WEP de 128 bits, encriptación de 64 bits WEP, TKIP, WPA
Cumplimiento de normas	UL, FCC
Alimentación	
Dispositivo de alimentación	Adaptador de corriente - externa
Parámetros de entorno	
Temperatura mínima de funcionamiento	0 °C
Temperatura máxima de funcionamiento	55 °C

III.3. Aplicación WEB para administración y control de asistencia.

Ventajas operativas: INFORMACION OPORTUNA

La oportunidad de la información es elemental para una mejor administración. El programa de control de asistencia le ayudará a conocer el estadístico de asistencias, puntualidades, incapacidades todo en un programa administrativo, donde se podrá visualizar una estadística general y de manera muy rápida la relación de los empleados que registran eventualidades, retardos, excepciones e incidencias

Instalación

Los manuales de instalación le llevarán paso a paso en el proceso de instalación y configuración de su sistema

Facilidad de Uso

El sistema seleccionado deberá operar en ambiente Windows. Las pantallas serán intuitivas y fáciles de utilizar. Cada pantalla del sistema de preferencia contará con ayuda en línea que le permitirá aprender fácilmente el uso correcto y operación del sistema

Manejo y administración de empleados

El sistema facilitará una completa administración de cada empleado, controlar su fecha de alta, número de seguro social, numero de materias asignadas, horarios, capturar la fotografía del empleado y muchos otros procedimientos. Podrá marcar a los empleados que tienen derecho a NO CHECAR y evitará listarlos en los reportes de incidencias

Conexión en red

El sistema de control de asistencia deberá trabajar con una base de datos ACESS o profesional Microsoft SQL Server 2000. Este tipo de servidor le permite almacenar una gran cantidad de información con altos niveles de eficiencia y seguridad. Las instalaciones locales o foráneas podrán conectarse al servidor fácilmente seleccionando el nombre del servidor o la dirección IP asignada al servidor. Si posteriormente se desarrolla una interface WEB se podrá accesar a la información desde cualquier lugar del mundo siempre y cuando se cumplan con las políticas de seguridad del sistema.

Restricción de acceso

El sistema permitirá configurar el acceso de cada usuario a cada una de las pantallas, además, se puede restringir la información que cada usuario puede consultar y limitar el acceso y consulta de información por, división, facultad, y departamento. Esta característica impedirá que un usuario consulte información que no sea de su competencia. De acuerdo al perfil podrán generarse reportes particulares derivados de los registros del sistema.

Administración de horarios

No hay un estándar en el manejo de los horarios. Sabemos que los horarios en una facultad o actividad docente nos obligan a manejar horarios nocturnos, vespertinos, diurnos, mixtos y especiales. El sistema de control de asistencia permitirá la configuración directamente sobre un calendario que le mostrará los días configurados, se realizara una interface que permita cargar los horarios del personal docente directamente de la hoja de control que se utiliza actualmente (Anexo I).

Flexibilidad de configuración

El sistema de control de asistencia contendrá un módulo de configuración de políticas del sistema, donde se podrá decidir cuestiones como:

- ✓ Si desea que el sistema inicie automáticamente con Windows
- ✓ Si desea que el reloj checador inicie automáticamente con Windows
- ✓ Si los retardos se cuentan como faltas
- ✓ Si la facultad paga tiempos extraordinarios o no
- ✓ Si los horarios son corridos o programados

Respaldos de base de datos

La utilería de respaldo de la base de datos le ayudará a mantener su información correctamente respaldada y resguardada con una solo instrucción. Los respaldos podrán restaurarse posteriormente con la misma utilería del sistema

Control de acceso

Los sistemas y equipos para control de asistencia permiten controlar dispositivos de apertura y cierre de puertas, o cualquier otro dispositivos para control de acceso peatonal y/o vehicular como torniquetes, exclusas, barreras vehiculares. Las aplicaciones de control de acceso y asistencia son ampliamente utilizadas en controles de edificios inteligentes y zonas de áreas restringidas, seguramente esta será un área de oportunidad a considerar en un proyecto futuro.

CAPITULO IV. ANÁLISIS DE LOS COMPONENTES DE HARDWARE UTILIZADOS EN EL SISTEMA.

IV.1. Comparativa y selección de lector de huella dactilar.

TERMINAL KIMALDI KBIO ALONE

DESCRIPCIÓN:

- ✓ Control de accesos con identificación biométrica por huella dactilar. Sistema seguro y fiable. Elimina la posibilidad de suplantación de identidad por transferencia y duplicación de tarjetas o códigos. Simplemente con poner el dedo sobre el lector el usuario es identificado, si se trata de un usuario registrado se produce la apertura automática del acceso (Figura IV.1.1)

Control de accesos con identificación biométrica off-line de huella dactilar y control de usuarios de la base de datos on-line.

MODO DE OPERACIÓN KBIO OFFLINE

- ✓ Identificación biométrica por huella dactilar
- ✓ Combina funcionamiento autónomo con funcionamiento a tiempo real.
- ✓ Posibilidad de almacenar hasta 4,000 huellas.
- ✓ Posible conexión a Bluetooth, WiFi y otras redes inalámbricas usando un bridge inalámbrico.

(Figura IV.1.1)

CARACTERÍSTICAS DEL SISTEMA:

• Combina el funcionamiento off-line o autónomo con el funcionamiento a tiempo real controlado desde una PC:

1.- *Operaciones Off-line:* funcionamiento autónomo no supeditado a las comunicaciones con la PC. Cuando el terminal detecta el dedo sobre el sensor óptico, éste captura la huella del dedo y realiza la identificación 1:N contra todas las huellas de la base de datos. Si el dedo está registrado, se activa la apertura de la puerta y se guarda un evento. Éste contiene información del momento de su generación y su resultado que podrá ser recuperado posteriormente.

2.- *Operaciones On-line*: carga de usuarios y gestión de la base de datos; pulsación de las teclas de función; monitorización de las entradas digitales; control del sistema en tiempo real; recuperación de eventos producidos, que contienen información del momento de su generación y su resultado. Además, después de
cada intento de identificación se envía a la PC información del resultado de ésta.

- ✓ Programación de la aplicación software a partir de OCX.
- ✓ Lector óptico de altas prestaciones y mantenimiento nulo.
- ✓ Señales ópticas y auditivas para los distintos mensajes.
- ✓ Número máximo de usuarios: 1.000 / 4.000 huellas.
- ✓ Conexiones RS-232, TCP-IP.
- ✓ Posible conexión a Bluetooth, WiFi y otras redes inalámbricas usando bridge inalámbrico.

APLICACIONES TÍPICAS:

Especialmente indicado para aplicaciones con uno o varios nodos (TCP-IP o RS-232) en la que se quiera manejar la base de datos de usuarios de manera remota y centralizada, y que una vez configurados los equipos, éstos tengan un comportamiento autónomo, bien completamente off-line sin necesidad de ningún host o reportando únicamente un evento después de cada acceso.

Una aplicación concreta podría ser el control de accesos a las habitaciones de un hotel. Desde recepción se darían de alta los huéspedes (usando un dispositivo de captura de huellas con conexión USB). Estas huellas se registrarían remotamente al terminal de la habitación. Los huéspedes tendrían simplemente que colocar el dedo sobre el sensor óptico para su identificación y acceso a la habitación.

ESPECIFICACIONES TÉCNICAS:

- ✓ Resolución escáner óptico 500 dpi
- ✓ Nº máximo de huellas 1.000 huellas (opcionalmente 4.000)
- ✓ Tiempo medio identificación 2-3 seg. para 1.000 huellas
- ✓ Eventos Hasta 8.000 eventos.
- ✓ Altas y bajas de forma remota centralizada desde el host.
- ✓ Teclas 2 teclas on-line 1 off-line.
- ✓ LED's 3
- ✓ Indicador acústico Buzzer (timbre) en tarjeta principal
- ✓ Opciones de puerta 1 relay
- ✓ Tiempo de apertura configurable
- ✓ Entradas digitales 3 con monitorización on-line.
- ✓ Conectividad Según modelo: RS-232 o TCP-IP.
- ✓ Programación A partir librerías OCX para VB.
- ✓ Rango de temperatura -10 ºC a 50 ºC
- ✓ Alimentación 12 VDC
- ✓ Dimensiones (mm) 112 x 170 x 56 mm.
- ✓ Peso (gr.) Aprox. 450 gr.
- ✓ Carcasa Poliestireno anti-impactos.

FAMILIA KBIO:

Familia de terminales para Control de Accesos con identificación biométrica de huella dactilar:

- ✓ Terminal con lector de huella robusto y de fácil manejo.
- ✓ Sistema de detección de presencia de dedo y activación automática de la identificación
- ✓ Funcionamiento autónomo o distinto conexionado en función del modelo: RS-232, TCPIP.
- ✓ Fácil integración tanto a nivel de software como de hardware, ofreciendo un sistema robusto y fiable con todas las facilidades y prestaciones de la tecnología biométrica.
- ✓ Opcionalmente el lector puede integrar la validación de usuarios va tarjetas Smart Cards, RFID, etc. (Figura IV.1.2)

Aplicaciones habituales:

- ✓ Control de accesos a habitaciones de hoteles, residencias, campamentos, control de presencia, acceso a sala de servidores, accesos museos, escuelas, aulas, control de accesos a centros de cómputo, etc.

Figura IV.1.2

Lectores Biométricos SAGEM Security

Sagem Defense Securite, parte del grupo SAFRAN es una compañía francesa que incursiona en el mercado de los biométricos desde 1980, convirtiéndose rápidamente en uno de los líderes del mercado. Las soluciones de Sagem han sido ampliamente probadas y con casos de éxito en todo el mundo y han sido siempre evaluados con calificaciones sobresalientes en todas las pruebas realizadas.

Sagem Sécurité
SAFRAN Group

Los sistemas de control de acceso y asistencia de Sagem comparten las mismas características de calidad y soporte que toda su línea de productos con una durabilidad extendida la cual es un requisito en este tipo de sistemas

MODELOS DISPONIBLES

MA100/110/120

El MA100 opera exclusivamente en modo de identificación con capacidad de 500 personas con 2 plantillas biométricas cada uno. Los MA110 y MA120 pueden operar ya sea en identificación o autenticación leyendo tarjeta sin contacto (Figura IV.1.3).
Software Incluido: Sistema MorphoAccess MEMS

Figura IV.1.3

MA 500

La serie MorphoAccess MA500 (Figura IV.1.4) opera exclusivamente en identificación y ofrecen una capacidad de 2 plantillas por persona de 3,000 hasta 50,000 personas.

Software Incluido: Sistema MorphoAccess MEMS

Figura IV.1.4

MorphoAccess

Fabricadas para uso externo tienen una calificación IP65, pueden hacer identificación o verificación y pueden almacenar hasta 48,000 personas, estos dispositivos se recomiendan para ambientes extremos (Figura IV.1.5)

Figura IV.1.5

Funciona con las terminales MorphoAccess, las cuales ofrecen interfases estándar de comunicación como son Wiegand, TCP/IP, DataClock, RS232 y RS422.

Software MorphoAccess MEMS

Sistema MorphoAccess de enrolamiento y administración MEMS (Figura IV.1.6) ofrece la posibilidad de integrar una solución biométrica a un sistema de control de acceso a un bajo costo y con muy pocas modificaciones, al ser un SW que generalmente se entrega sin costo en la compra del producto no permite la interacción con su base de datos.

Figura IV.1.6

Lectores Biométricos ZKSoftware

ZKSoftware Sociedad Anónima Limitada es una compañía de tecnología biométrica de identificación en China.

El grupo **ZKSoftware** goza de su propia cadena industrial de investigación, desarrollo, diseño, embalaje y venta. Desde 1985 cuando la sociedad se lanzó a la investigación del algoritmo de identificación de huella digital, el número de usuarios ha ascendido a más de 35 millones, mientras que están en operación más de 300.000 juegos de productos fabricados por esta sociedad. **ZKSoftware** está dedicando a popularizar, aplicar y desarrollar la industrialización de la tecnología biométrica de identificación en el mundo. Su algoritmo de identificación biométrica ***Biokey*** con la propiedad intelectual independiente es una de las tecnologías más abiertas en el mundo. Y El Grupo **ZKSoftware** ha construido su propia licencia y servicio del código original. Con más de 1200 exploradores de cooperación y el costo muy bajo del hardware de ***Biokey***, **ZKSoftware** ha quitado el umbral para entrar en esta industria y espera que ***Biokey*** pueda establecer un nuevo estándar del funcionamiento y del precio.

El equipo terminal de huella digital de ***Biokey*** es el más barato y más abierto entre los productos terminales de la huella digital en el mundo, y actualmente **ZKSoftware** es el más fuerte suministrador, productor y fabricante de OEM de la tecnología de identificación de huella digital aplicada a la industria civil, que ocupa más de 70% del mercado de la industria civil en China, y ha ocupado continuamente el primer lugar en cuanto al cuota en el mercado en cinco años.

En realidad la cartera de productos de ZKSoftware es extremadamente amplia, solo mostraremos aquí las características principales de algunos de ellos.

De acuerdo a la explicación anterior de bajo costo y excelentes prestaciones se selecciono el lector de huellas T6 para este proyecto.

Reloj checador con Huella Digital Modelo T6 / FP-60 (Figura IV.1.7)

- Reloj checador con huella digital, hasta 1,500 huellas dactilares
- Sensor óptico de huella digital
- Permite grabar de 1 a 10 huellas por usuario
- Almacena hasta 30,000 registros, sin descargar en la PC
- Resolución de 500 dpi
- Teclado numérico y de función con 16 teclas
- Pantalla LCD para 80 caracteres, 4 líneas y 20 columnas
- Reloj electrónico inteligente
- Conectividad por Ethernet (TCP/IP), RS232, 485.
- Puerto USB para la descarga de registros a unidad portátil (Memoria USB)
- Dimensiones: 180x125x55 mm
- Cambio automático de horario, verano-invierno
- Permite la respuesta de confirmación a través de voz.

Figura IV.1.7

Figura IV.1.8

Reloj Checador CA-8, Control de acceso con Huella digital (Figura IV.1.8)

El reloj CA-8 representa la nueva generación en tecnología de reconocimiento de huella digital. Ideal para empresas con más de 500 empleados, ideal para sucursales, puede usarse en Internet. NO REQUIERE PC para Operar. Agrega a las versiones predecesoras la capacidad de control de acceso a través de puertos I/O y relays para apertura de puertas.

El software de administración como reloj checador suministra:

- ✓ Administración de múltiples relojes.
- ✓ Administración de departamentos. Creación de múltiples horarios
- ✓ Creación de múltiples turnos
- ✓ Definición de minutos de tolerancia. Definición de días festivos
- ✓ Incidencias
- ✓ Permisos
- ✓ Horas extra
- ✓ Horas trabajadas
- ✓ Retrasos
- ✓ Exportación de reportes a Excel, Base de datos, archivo de texto.
- ✓ Apis de programación para controlar el reloj en aplicaciones del usuario
- ✓ Capacidad de mostrar mensajes personalizados por empleados (con los Apis)
- ✓ Fácil integración a otros sistemas de nómina

Reloj checador B4 Control de acceso con Huella digital (Figura IV.1.9)

El algoritmo de la versión 2005, permite una validación y registro de huellas más confiable y más exacta, la velocidad de la identificación es muy alta ya que sólo necesita 2 segundos para procesar 3000 platillas de huella digital.

Está construido con un gabinete metálico (ZEM100) lo cuál lo hace ideal para aplicaciones a la intemperie. Integre un procesador Intel 32 X-Scale CPU, permite una fácil para integrar a varios sistemas.

Apoya la identificación de la rotación de 360 grados de los dedos, fácil para utilizar. Sensor óptico de alta definición, mejora la calidad de la imagen capturada, funciona igual con dedos secos y mojados.

Ajusta la distorsión de la imagen,
Capacidad de huellas digitales：1500/2800
Comunicaciones： RS232, RS485, TCP/IP
Velocidad de identificación ： ＜=2S
Temperatura de funcionamiento **:** 0°C-45°C

Figura IV.1.9

IV.2 Bridge Ethernet a RF para conexión a red.

El DWL-G810 es un Bridge Ethernet-a-Wireless (E2W) que convierte virtualmente cualquier dispositivo Ethernet – Set Top Box, Consola de Juego, Impresora o Computador o en nuestro caso el lector de huella dactilar– en un dispositivo de red Inalámbrico. Ahora, impresoras habilitadas para conexiones Ethernet pueden ser compartidas en casa u oficina sin necesidad de pasar cables a través de los muros o techos. Y los jugadores de juegos de consola podrán unirse en juegos de video multi-jugadores, o hacia Internet utilizando conexiones de Banda Ancha.

Con su interface de configuración vía Web, la instalación del DWL-G810 es fácil, habilitando la conexión de los usuarios muy rápidamente. La configuración de parámetros avanzados también pueden ser aplicados de manera sencilla e intuitiva. El DWL-G810 (Figura IV.2.1) incluye encriptación WEP hasta 152 bits y soporte WPA, proporcionando un mayor nivel de protección para garantizar la confidencialidad de los datos y ayudar a prevenir el acceso a la red inalámbrica.

Principales Características:

- ✓ Rendimiento 15 x veces superior que el de un producto Wireless 11b
- ✓ Ancho de Banda de 54Mbps/108Mbps, en 2.4GHz
- ✓ Compatible con productos que operen bajo los estándares 802.11b y 802.11g, y todos los productos inalámbricos de D-Link.
- ✓ Seguridad Avanzada, WPA
- ✓ Antena desmontable con conector RSMA
- ✓ Alto Rendimiento
- ✓ Fácil integración en red

Figura IV.2.1

IV.3 Librerías de desarrollo SDK (Software Development Kit)

Permite implementar software con un interface de usuario de forma fácil y rápida
Ventajas:

- ✓ Aplicable a entornos cliente / servidor y también entornos web
- ✓ Soporta el entorno .net para el desarrollo de nuevas aplicaciones.
- ✓ Control de los dispositivos de hardware
- ✓ Lectura de huellas
- ✓ Extracción de la información parametrizada o minucia de las huellas
- ✓ Registro de huellas
- ✓ Autentificación de huellas (1:1, 1:N)
- ✓ Disponible en versión para entornos Windows y Linux
- ✓ FAR: 0.001% FRR: 0.1%

eNBSP SDK 4.0 (Figura IV.3.1) es un kit de desarrollo de software (ahora denominado **BSP - *Biometric Solution Provider***) y un algoritmo de reconocimiento de huellas 1:N, sirve no sólo para aplicaciones básicas, sino también para aplicaciones que utilizan las huellas de base de datos de gran capacidad y donde se requiere una velocidad de búsqueda de huellas muy elevada.

Este kit de desarrollo proporciona un interface de programación de alto nivel API (Application Programming Interface) que permite implementar un software con una interfaz de usuario de una forma fácil y rápida, ahorrando tiempo y esfuerzos en el desarrollo de la aplicación.

El kit de desarrollo permite operar en distintas plataformas puesto que soporta varios sistemas operativos y lenguajes de programación, así como distintos dispositivos de reconocimiento de huella.

IV.3.1 Principales características

1. Proporciona un interface de programación API óptimo para el desarrollo de software de reconocimiento de huella digital.
2. Proporciona una aplicación de software de ayuda y una interfaz de usuario de rápida y fácil utilización.
3. Permite un fácil desarrollo mediante funciones de registro y autentificación de huellas que operan de forma transparente para el desarrollador.
4. Funciones de identificación 1:N muy rápidas - *Algoritmo eNSearch:* para aplicaciones grandes o medianas, permite capturar hasta 10 huellas por persona.
5. Permite una fácil personalización del interface de usuario minimizando el costo y tiempo empleados en el desarrollo
6. Seguridad en la utilización de la información de la huella mediante un algoritmo de encriptación de 128 bits
7. Soporta la conversión de distintos formatos de imágenes de huella (BMP, JPG, WSQ, etc.)

IV.3.2 Funciones que soporta:

- ✓ Permite el control del dispositivo de lectura
- ✓ Captura y normaliza la imagen de la huella dactilar
- ✓ Realiza la extracción de la Minucia
- ✓ Registra la huella digital
- ✓ Permite la autenticación de la huella digital (1:1, 1:N)
- ✓ Provee librerías para Microsoft .NET
- ✓ El SDK proporciona ejemplos en varios ambientes de desarrollo.

IV.3.3 Ambiente de desarrollo:

- ✓ **Sistema Operativo** Windows 95/98/Me/NT4.0 /2000/XP
- ✓ **PC** Pentium o superior
- ✓ **Lenguaje de Desarrollo** VC++, VB, ASP, Delphi, .NET etc
- ✓ **Servidor Web** IIS 4.0
- ✓ **Web Browser** IIS 4.0

IV.3.4 Estructura de desarrollo

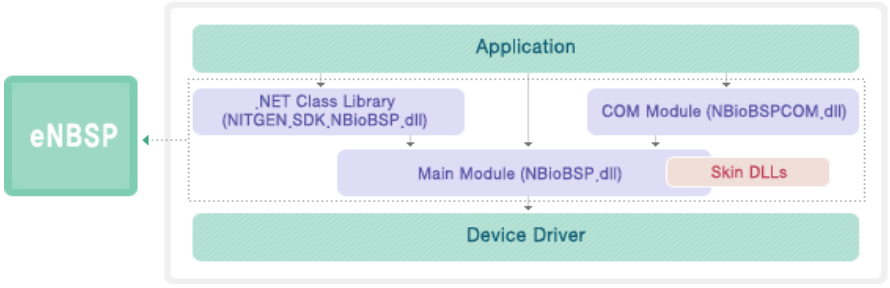

Figura IV.3.1

IV.4 Tabla comparativa de lectores de huella dactilar

CARACTERISTICAS	KIMALDI KBIO ALONE	SAGEM SECURITE MA100/110/120	SAGEM SECURITE MA 500	ZKSOFTWARE T6 / FP-60	ZKSOFTWARE CA-8	ZKSOFTWARE B1
Lector Biométrico de Huella Digital	✓	✓	✓	✓	✓	✓
Resolución (DPI´s)	500 DPI´s	500 DPI´s	500 DPI´s	500 DPI´s	500 DPI´s	500 DPI´s
Almacenamiento Máximo de Huellas Dactilares	4, 000 Huellas	500 Huellas	50,000 Huellas	1,500 Huellas	1,000 Huellas	2,800 Huellas
Máximo No. De Eventos	8, 000	✗	10,000	30,000	50,000	120,000
Conectividad	RS232, TCP-IP	RS485, Ethernet, TCP/IP, USB	Ethernet, WiFi	RS 232, TCP-IP, 485	RS 232, TCP-IP, 485	RS 232, TCP-IP, 485
Confirmación a través de voz	✗	✗	✗	✓	✗	✗
Tiempo de Verificación	2-3 seg.	1 segundo	1 segundo	2 segundos	2 segundos	2 segundos
Buzzer y LEDS	3 LED´s	LED´s MULTICOLOR	LED´S BICOLOR	LED´s BICOLOR	LED´s BICOLOR	LED´s BICOLOR
Temperatura de Operación	10º a 50º C	10º a 45º C	10º a 50º C	0º a 45º C	0º a 45º C	0º a 45º C
Software	✗	Morpho Access MEMS (No incluye)	Morpho Access MEMS (No Incluye)	Control de Asistencia 2008	Control de Asistencia 2008	Control de Asistencia 2008
Tipo de Teclado	✗	✗	12 TECLAS	16 TECLAS	16 TECLAS	16 TECLAS
Rango Falso de Aceptación	No especificado	No especificado	No especificado	< .0001%	< .0001%	< .0001%
Rango Falso de Rechazo	No especificado	No especificado	No especificado	< 1 %	< 1 %	< 1 %

IV.4.1 Selección y ventajas competitivas

De acuerdo a la tabla previa seleccionamos el lector T6/FP-60 por reunir las mejores ventajas competitivas ya que:

- Cuenta con una alta resolución en pantalla.
- Posibilidad de guardar hasta 10 huellas por usuario.
- Pantalla LCD para 80 caracteres, 4 líneas y 20 columnas
- Alta capacidad de almacenamiento de huellas.
- Tiene la capacidad de almacenar hasta 30,000 registros sin necesidad de descargar la información a la PC
- La descarga de registros se puede hacer a través de USB
- Cambio automático de horario, verano-invierno
- Permite trabajar en modo ON-LINE, OFF-LINE
- Cuenta con soporte técnico especializado
- Provee con librarías de desarrollo sin costo
- El Software Control de Asistencia 2008 viene incluido.
- Se considera el mayor fabricante de lectores biométricos en el mundo.
- Con estas características es el lector de menor costo del mercado
- Permite la fabricación de lectores bajo demanda (OEM)
- Permite la instalación sin restricciones del Software de Control de Asistencias

CAPITULO V. IMPLEMENTACIÓN Y PRUEBAS.

V.1. Configuración del dispositivo.

V.1.1 Configuración de lector de huella T6. (Figura V.1)

1.-Configure la dirección IP asignada y seleccione comunicación Ethernet.

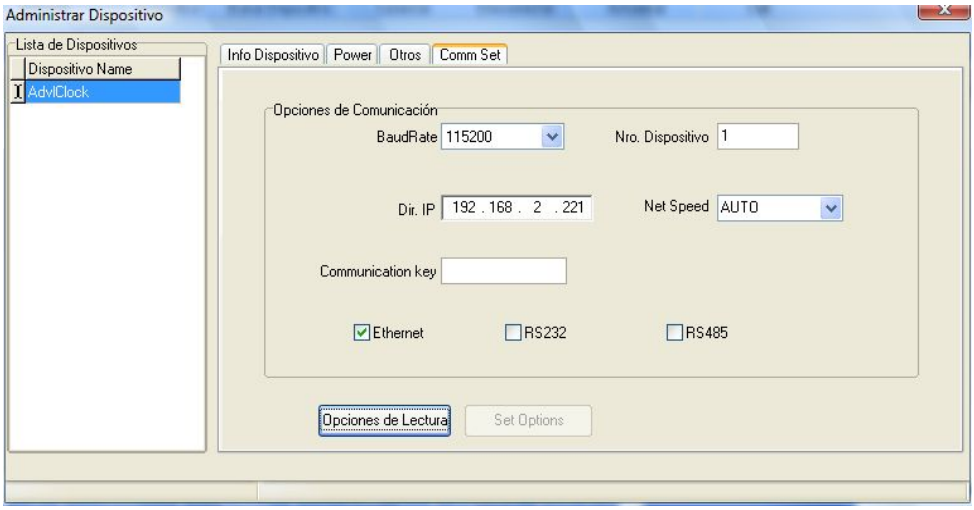

Figura V.1 asignación de dirección IP a lector de huella

V.2. Configuración del sistema.

V.2.1. Alta de usuarios. CATALOGOS

Los Catálogos son la información base para la operación del Sistema. A continuación los enumeramos y podemos darnos una idea del alcance del mismo.

- ✓ **Empresas:** Capacidad de manejar varias Empresas a la vez aun que se tenga duplicado el número de trabajador en diferentes empresas.
- ✓ **Departamentos:** Clasificación por Departamentos ó Centros de Costos. Útil para permitir que diferentes usuarios accedan a reportes limitándolos solo al departamento al que pertenecen.

- ✓ **Categorías:** Generalmente usada para diferenciar empleados sindicalizados ó de confianza para separar reportes semanales ó quincenales.

- ✓ **Grupos:** Campo de clasificación adicional para ser usado libremente cuando se requiera alguna clasificación especial dentro de la empresa. Ej. grupos ó equipos de trabajo con una misma rotación.

- ✓ **Trabajadores:** Información general de los trabajadores, fotografía, turnos, rotación, datos de credencial elector y datos de validación, registros de asistencia y acceso.

- ✓ **Supervisor de Asistencia:** Persona encargada de dar permisos de registro cuando una persona llega con retardo, sale temprano ó registra salida con tiempo extra.

- ✓ **Usuarios:** Personas que pueden operar el Sistema Control de Asistencia. Se manejan dos niveles de Usuario: Usuario Administrador y Usuario General. El Usuario Administrador tiene acceso a todas las opciones del sistema mientras que el Usuario General puede definirse como acceso de Lectura ó Escritura según convenga. También se puede limitar acceder solo a las opciones de menú seleccionadas y sólo a los departamentos seleccionados.

- ✓ **Conceptos:** Se pueden dar de alta conceptos justificantes de faltas como lo son incapacidades, vacaciones, permisos y en general todos los que apliquen dentro de la empresa.

- ✓ **Festivos:** Se dan de alta los días festivos de tal manera que no se genera falta en estos días para los trabajadores. El sistema marca en automático una falta cuando no existe registro por parte del trabajador en determinado día. Por el contrario, si un trabajador marca registro de asistencia en día festivo se le considera tiempo extra.

V.2.2 Turnos de trabajo.

La definición del turno (Figura V.2.1) es sumamente importante para el cálculo del tiempo normal, tiempo extra, faltas, retardos y demás incidencias. Los registros realizados por el trabajador son confrontados contra el turno y de ahí se derivan las incidencias.

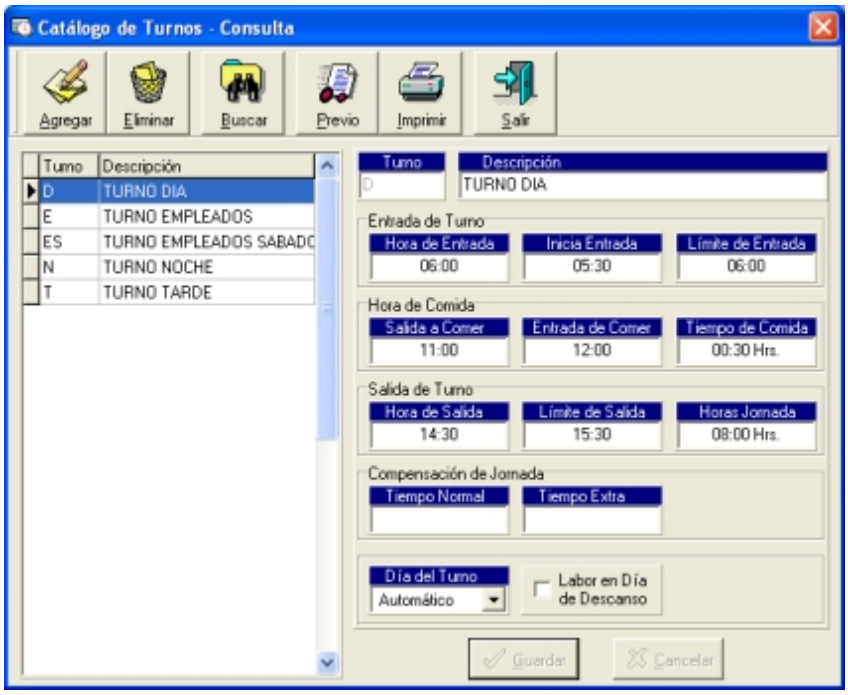

Figura V.2.1 Pantalla ejemplo del catálogo de turno

Se pueden definir cuantos turnos sean necesarios. Posterior a ello se define la rotación de turnos que se va actualizando automáticamente por el sistema. Para nuestro caso particular tomamos como base de registro de turnos la plantilla de registro de horarios y asignaturas por semestre de la Facultad de Ingeniería.

V.2.3 Creación de departamentos

Para dar de alta un departamento, se debe dar click en la pestaña que se encuentra de lado izquierdo de la pantalla (Figura V.2.2), en el texto que dice Lista de Departamentos. Siga las instrucciones de la ventana que se muestra a continuación si desea editar el nombre de un departamento.

FiguraV.2.2

V.2.4 Alta de empleados

Para dar de alta a cada uno de los empleados de la empresa, se debe seleccionar en la parte izquierda de la pantalla en la palabra empleados (Figura V.2.3). Al dar click se desplegará la ventana que aparece a continuación. Sólo se debe seleccionar el departamento al que pertenece el empleado y darlo de alta con los datos correspondientes, se tiene la opción de agregar una foto si así se desea.

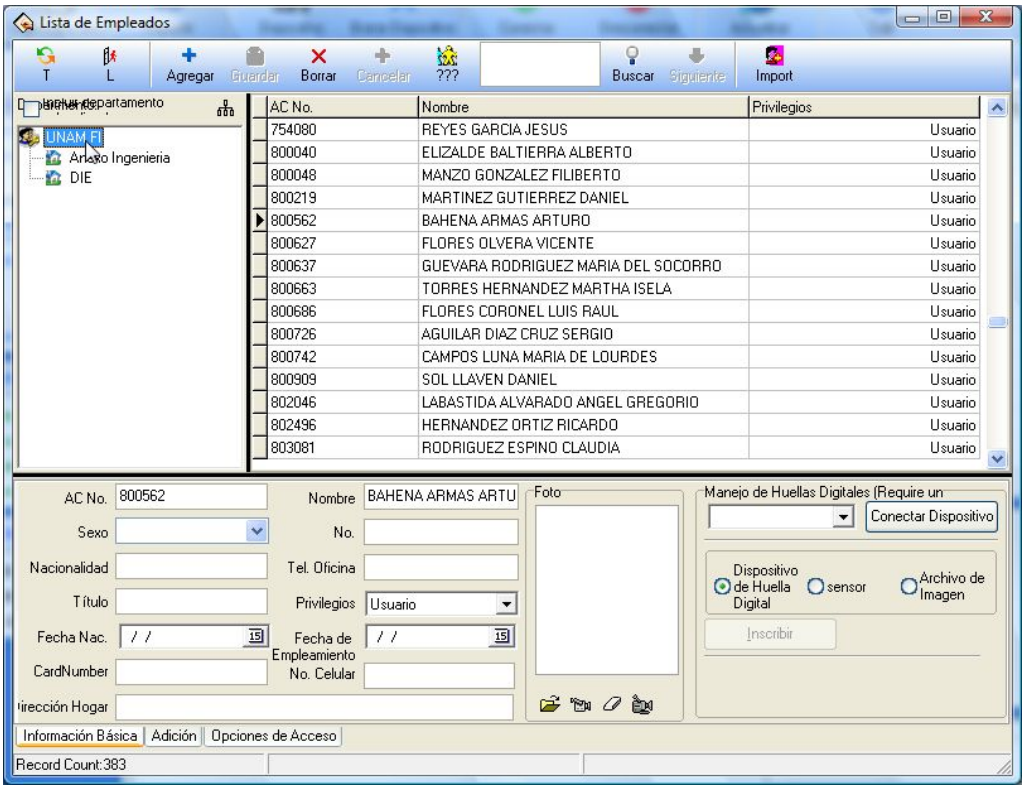

Figura V.2.3 Pantalla para alta de empleados

V.3. Registro de usuarios a través de huella dactilar

Toda vez que el empleado esta ya dado de alta se pedirá el registro de su huella dactilar haciendo uso de la pantalla siguiente (Figura V.3.1)

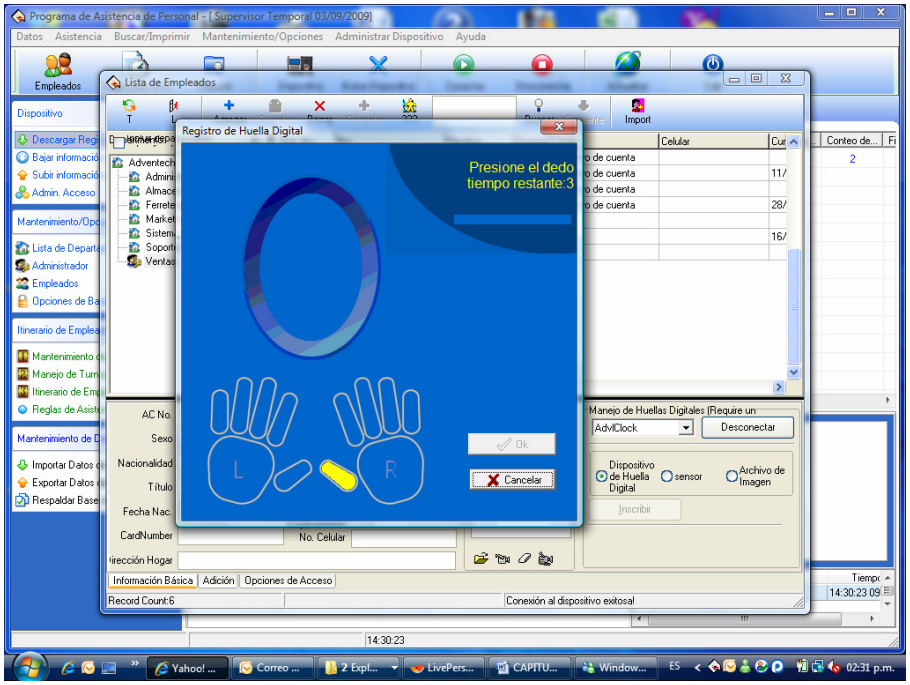

Figura V.3.1 Registro de huellas

Es importante mencionar que pueden registrarse de ser necesario hasta 10 huellas por usuario, generalmente se toman 4, dos de cada mano.

V.4. Asignación de horarios y turnos de empleados.

El sistema permite agregar cualquier número de empleados y a cada uno de ellos asignarles un horario especifico de acuerdo a la materia en cuestión. Mediante la realización de una interface de extracción de datos la generación de horarios se hace de manera automática, de cualquier modo esta imagen nos muestra como se visualiza la información para cada empleado (Figura V.4.1).

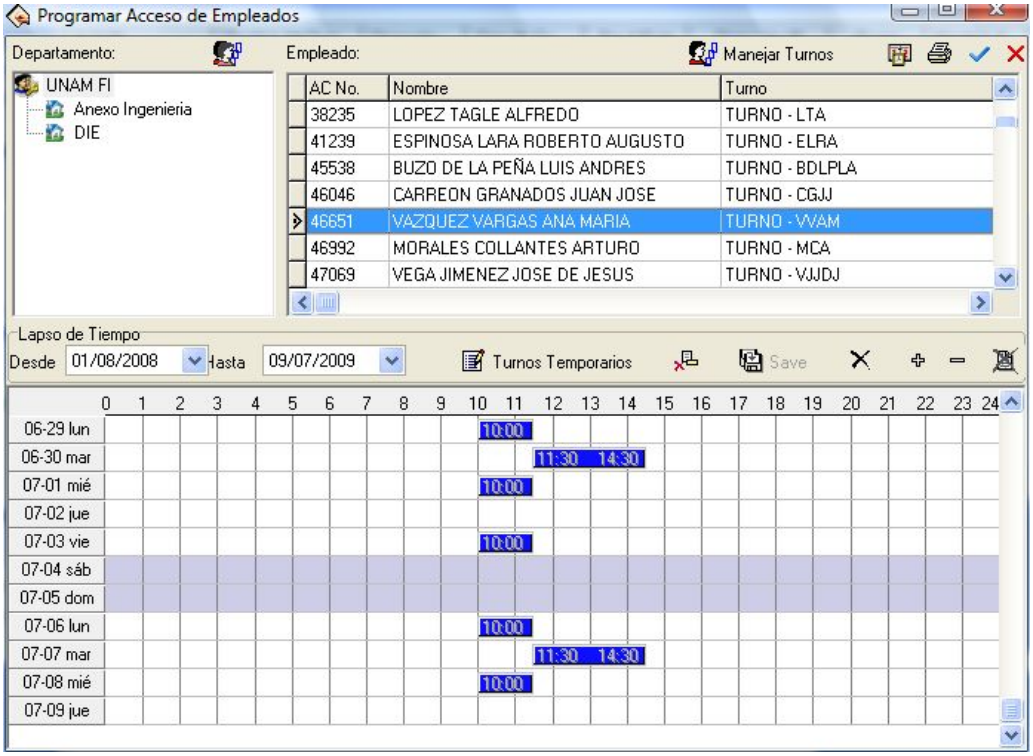

Figura V.4.1 Pantalla para visualización de turnos

Una vez definido el horario de los empleados se deben crear las reglas de acceso, es decir el tiempo de tolerancia que tienen para registrar su ingreso y egreso y si es obligatorio el registro (Figura V.4.2).

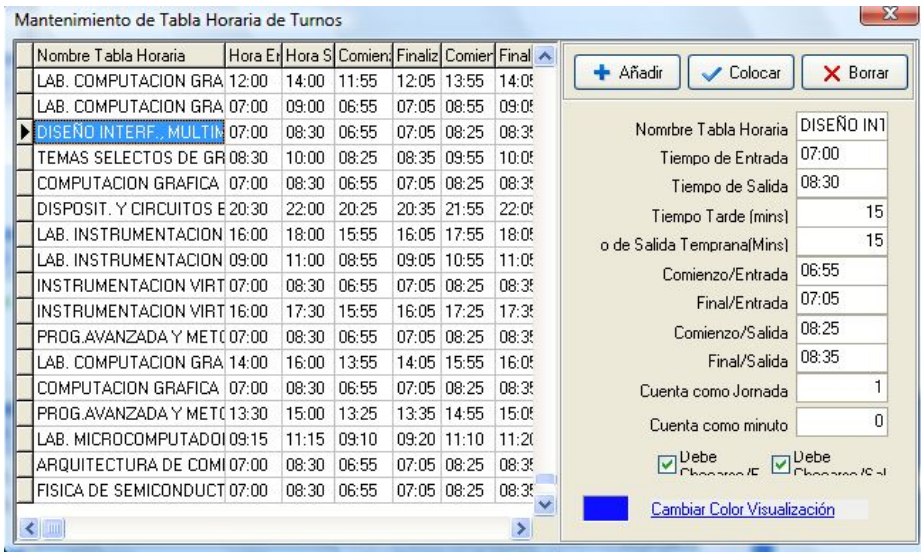

Figura V.4.2

V.5. Alta de usuarios y definición de perfiles.

Dentro de la lista de usuarios podemos agregar uno o varios administradores del sistema. Seleccionamos el usuario, seleccionamos las tareas a las cuales tiene permiso, así como los dispositivos a los que tiene acceso. Debe reiniciar el sistema para que la nueva información se actualice (Figura V.5.1).

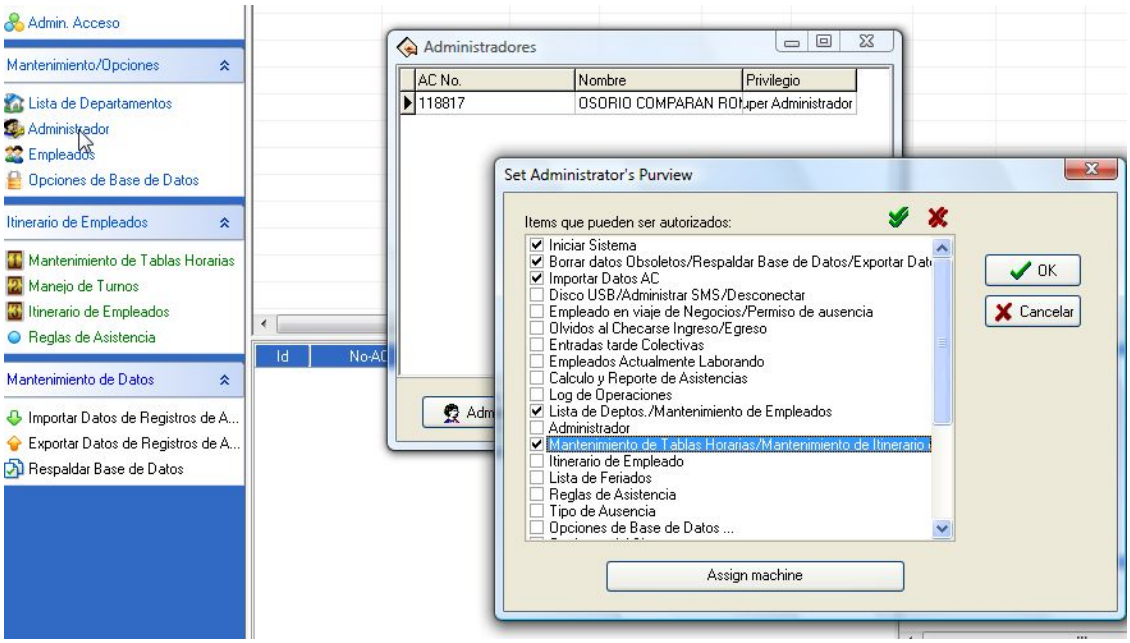

Figura V.5.1 Asignación de privilegios

Aquí debemos enfatizar que la aplicación puede instalarse libremente en todas las PCs que se desee de tal forma que puede crearse un administrador para cada departamento o facultad y asimismo pueden crearse perfiles para registro de usuarios y perfiles de usuarios comunes para consulta de listas de asistencia.

V.6. Carga de información de PC a Dispositivo

Para cargar la información a un dispositivo debemos seleccionar la información de los empleados, seleccionar el dispositivo y oprimir el botón cargar (Upload) (Figura V.6.1)

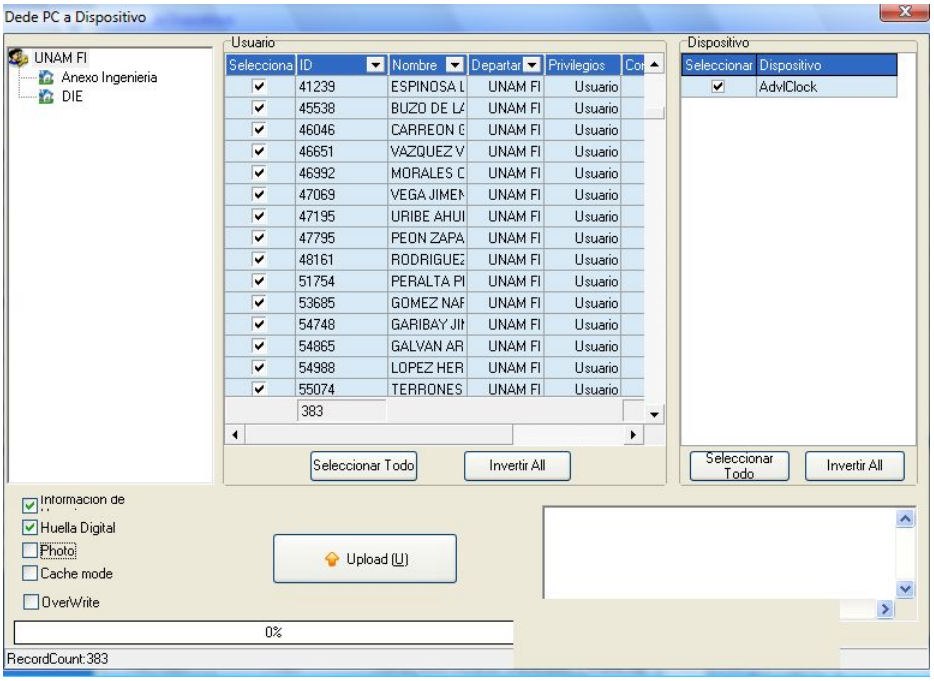

Figura V.6.1 Carga inicial de datos a dispositivo lector de huellas

V.7. Descarga de registros de asistencia.

a) Como primer paso debe seleccionar el lector del cual desea obtener los datos (Figura V.7.1).

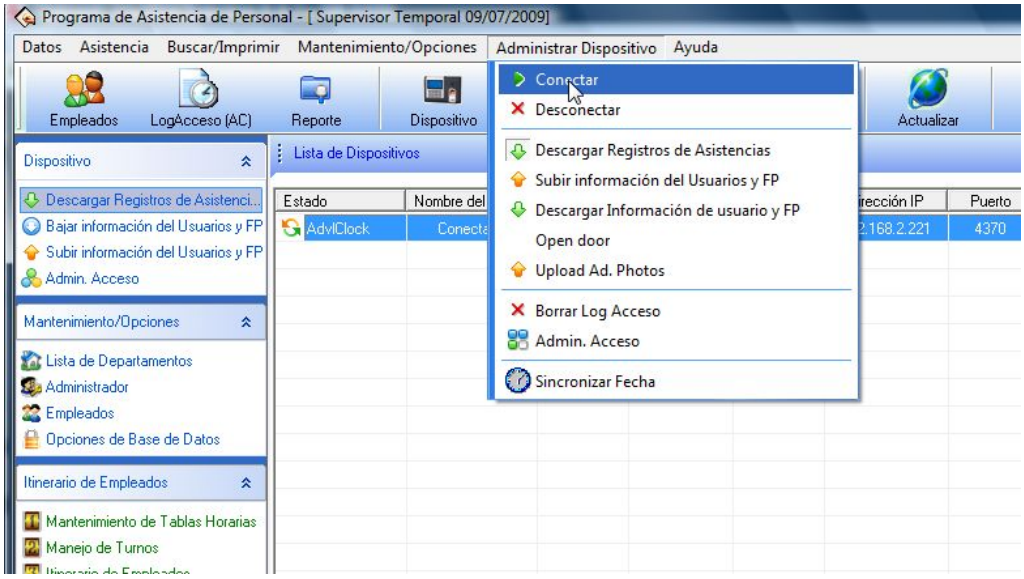

Figura V.7.1 Conexión a dispositivo

b) Una vez hecho esto, seleccione descargar registros de asistencia (Figura V.7.2)

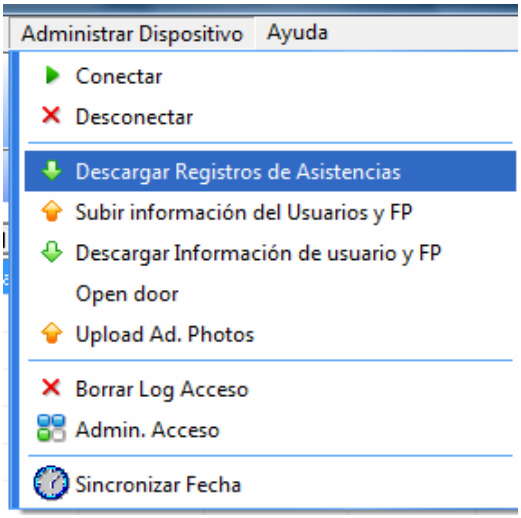

Figura V.7.2 Descarga de datos de dispositivo lector a PC

c) Hecho esto y una vez iniciada la comunicación se despliega la barra de extracción de información (Figura V.7.3)

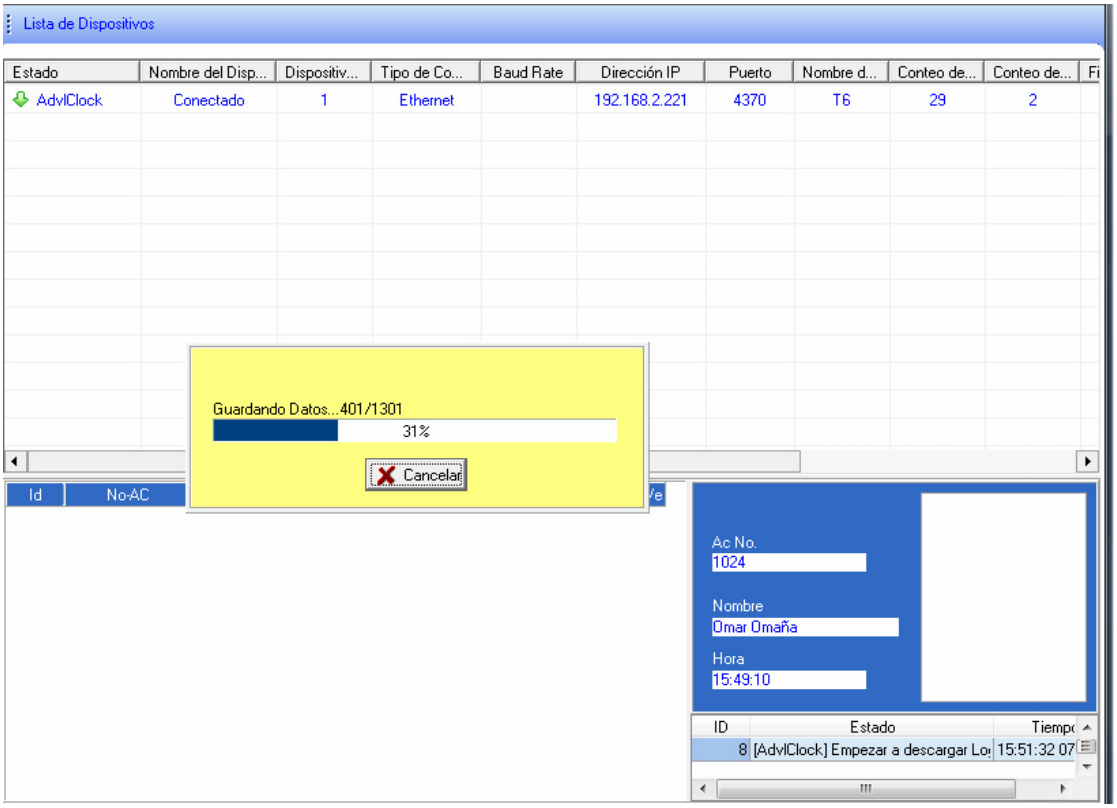

Figura V.7.3 Pantalla de transferencia de información

V.8. Tipo de reportes de asistencia

Los Reportes del Sistema de Control de Asistencia pueden ser filtrados por rango de fechas facilitando la selección del período y sin necesidad de realizar cierres del período. También se puede seleccionar por Trabajador, Departamento, Categoría, Grupo y Turno. Se pueden exportar los reportes a Archivo Texto ó Excel.

Reporte de registros de asistencias

Se puede obtener en dos formatos distintos: Resumen general y registros de asistencia a detalle. Se realiza la obtención de los registros realizadas por los trabajadores en el Reloj Checador con opciones de resumen, registros consecutivas ó agrupados por trabajador incluyendo conceptos de ausentismo y faltas. También se pueden seleccionar registros incompletos para validación de incidencias en el registro de los profesores.

Reporte de Ausentismo

Reporta el total de faltas de un período seleccionado y el detalle de fechas de dichas faltas. Las faltas son auto generadas por el sistema dada la ausencia de registro del trabajador cuando éste tiene definido un turno por atender de acuerdo a su rol de turnos u horarios asignados.

Reporte de Retardos

Reporta los trabajadores que registraron su entrada posterior al tiempo definido de entrada ó respecto a un límite de tolerancia. El tiempo de entrada y tolerancia se define en el turno y puede ser igual ó diferente para cada uno de los días comprendidos en el rol de turnos de cada trabajador. Se obtiene el número de retardos por trabajador de un período seleccionado así como el tiempo acumulado en dichos retardos y el detalle de registro de cada retardo.

Reporte de Tiempo Extra

Reporta el total del tiempo extra de cada trabajador calculado a partir del tiempo excedente de jornada definida en el turno. Se obtiene el detalle de su registro, el supervisor que autorizó la entrada y el tiempo extra laborado. Se tiene la opción de resumen por departamento con porcentaje de participación de cada departamento del total global de horas extras generadas.

Reporte Tipo Tarjeta Reloj

Reporte de período semanal con el resumen de checado día a día de cada trabajador. Opcionalmente se incluye texto de conformidad a ser firmado por el trabajador.

Reporte de Control de Accesos

Reporte detallado de los registros de asistencia realizados en unidades de control de acceso incluyendo el registro de fecha y hora de acceso, el tipo de registro de entrada ó salida, la identificación del dispositivo de acceso y supervisor en caso de haber requerido autorización (Figura V.8.1).

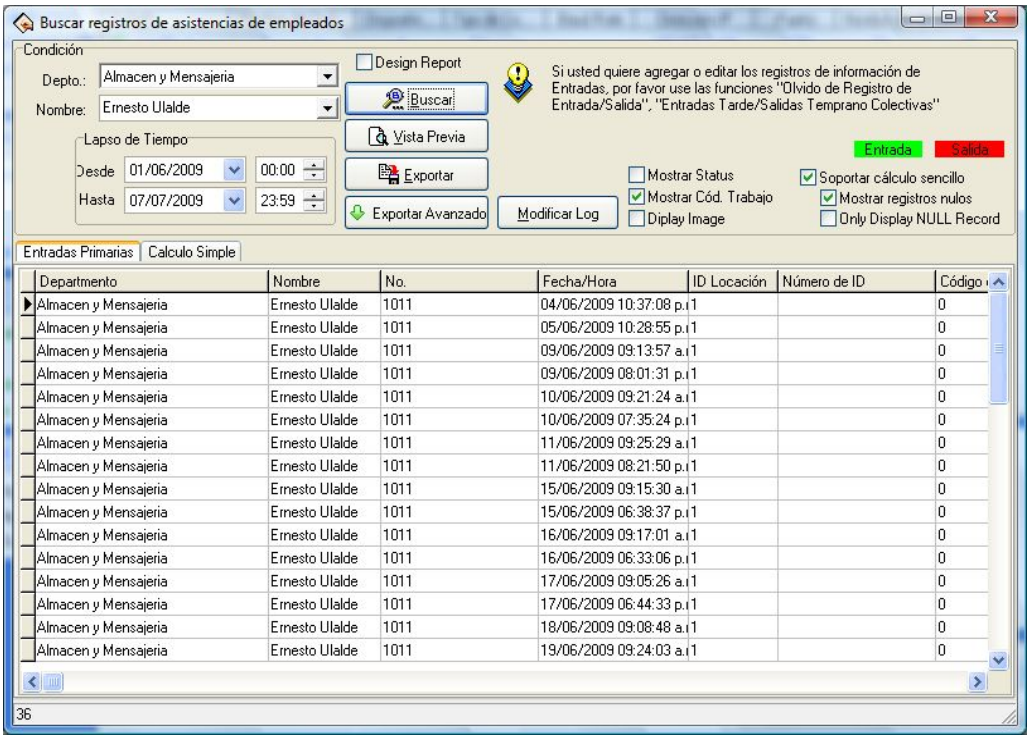

Figura V.8.1generación de reporte de asistencia.

Para emitir un reporte de Asistencia de un empleado en particular, solo debe seleccionar el empleado, seleccionar el lapso de tiempo que desea consultar. Podrá editar o agregar registros de información de Entradas en la opción “Olvido de registro de Entrada/Salida”.

En esta ventana se muestra el status de transferencia de datos (Figura V.8.2).

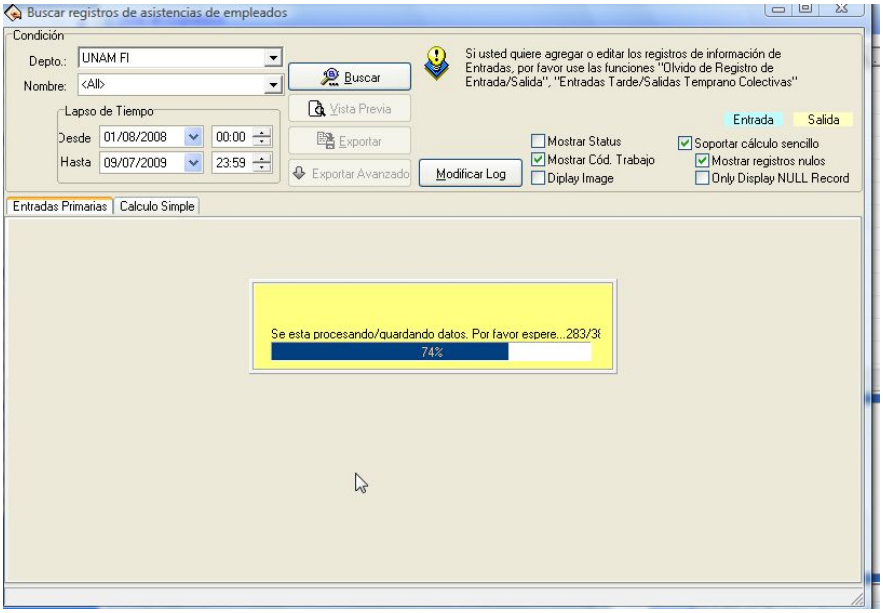

Figura V.8.2 Procesamiento de datos para emisión de reportes

V.9. Utilerías

a) Como se muestra en la siguiente ventana (Figura V.9.1), se puede reiniciar el dispositivo y capturar una imagen, entre otras opciones que se muestran a continuación.

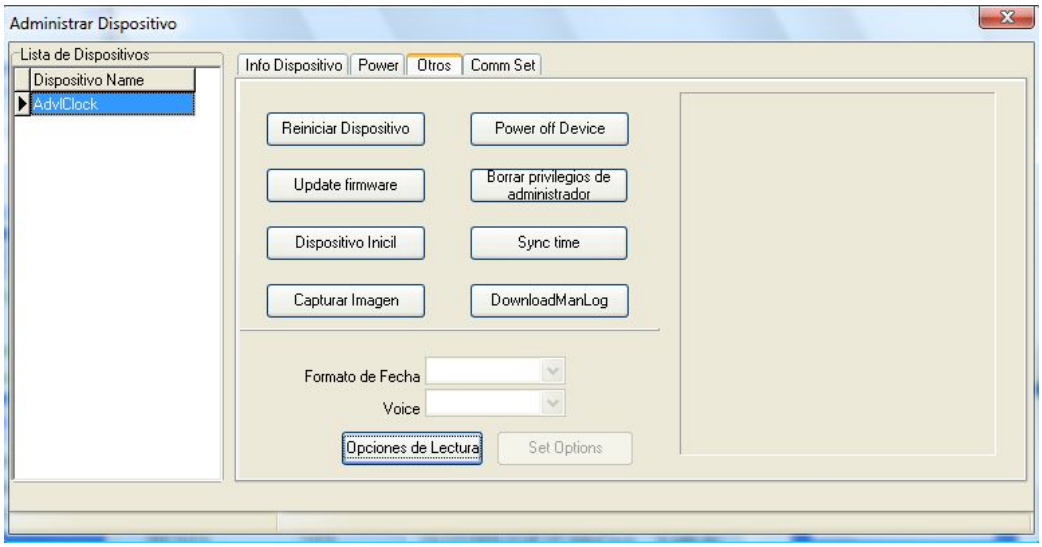

Figura V.9.1 Opciones del lector de huella

b) De igual forma puedes visualizar la información del dispositivo, como el conteo de usuarios, huellas digitales, y la capacidad del mismo (Figura V.9.2).

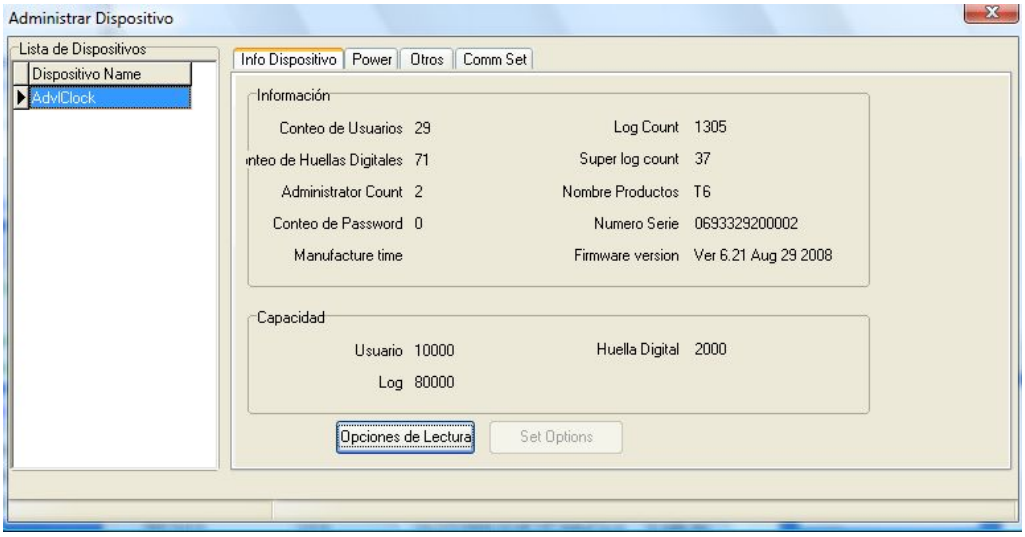

Figura V.9.2 Estadísticas del dispositivo lector

V.10. Importación de base de datos.

Con este Software tienes la posibilidad de importar la base de datos de la forma más sencilla. Sólo debes dar click en la parte izquierda de tu pantalla (Figura V.10.1), en la opción Importar datos de asistencia.

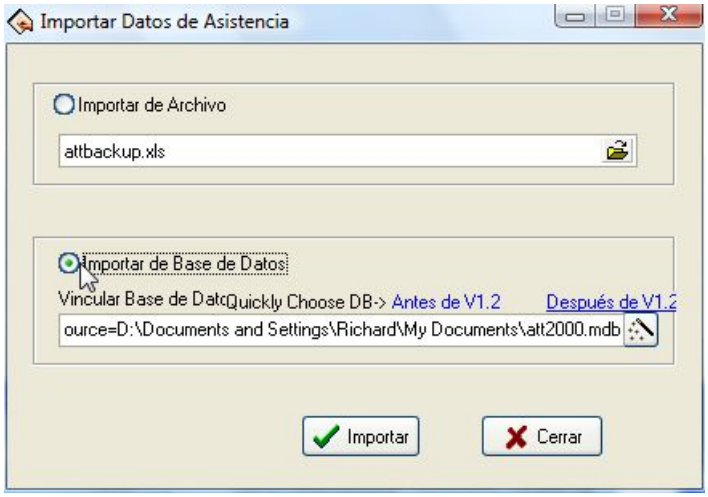

Figura V.10.1 Importación de datos

V.11. Respaldo de base de datos

De igual forma puedes respaldar tu base de datos con tan solo dar click en la parte izquierda de tu pantalla, en la opción respaldar base de datos, y podrás guardar la base de datos en cualquier lugar de tu PC (Figura V.11.1).

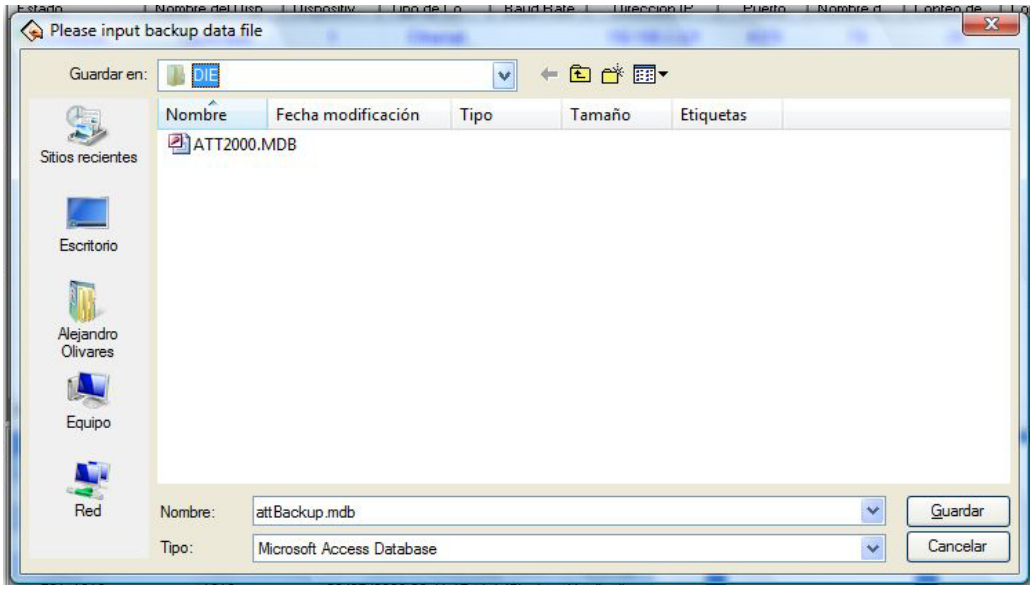

Figura V.11.1 Respaldo de Información

V.12. Integración del Sistema de Control de Asistencia

Toda vez que interactuamos con el sistema de control de asistencias que el fabricante provee, se realiza un análisis de la base de datos con que cuenta el mismo a fin de integrar los datos actuales de profesores, asignaturas y horarios (capturada en formato Excel *.XLS), (Anexo I) a la base de datos de la aplicación, desarrollando para ello una interface automática que lea el archivo de Excel y los integre de manera automática al sistema de control de asistencias.

V.12.1 Análisis de base de datos (Desarrollo de Interface)

Para efectos de desarrollar la interface a la base de datos del sistema de control de asistencia es importante conocer las tablas que componen la base de datos (Figura V.12.1).

Diagrama de Base de Datos

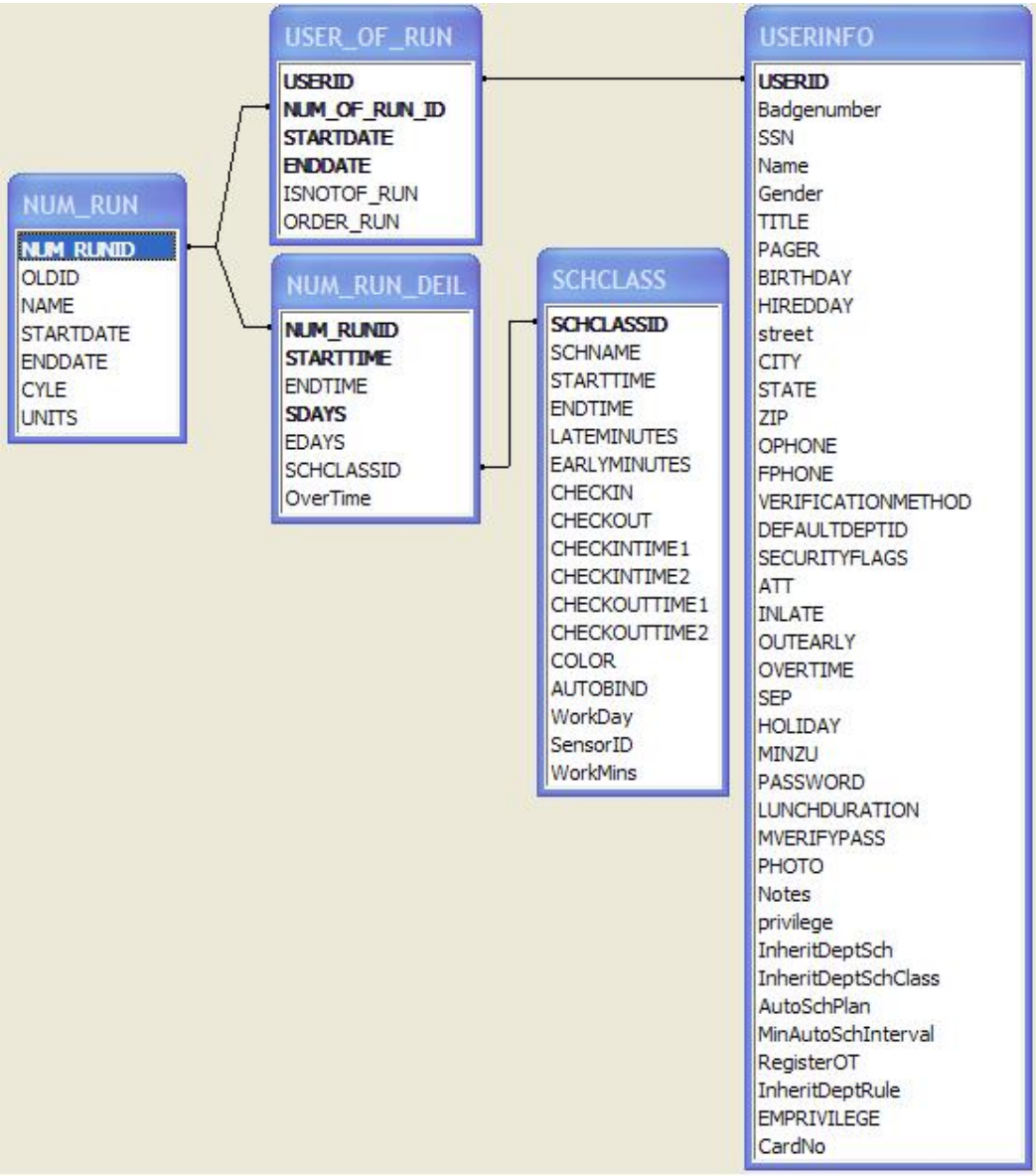

Figura V.12.1

V.12.2 Descripción de Tablas

Tabla: NUM_RUN

Descripción: En esta tabla se guardan los registros de “turnos”, es decir representa un turno de un empleado, es decir el horario de trabajo de ese empleado.

Campos de Interés:

- **Nombre de Campo: NUM_RUNID**
    - Descripción: Clave única(llave primaria) de la tabla
    - Tipo: Numérico Automático (auto numérico).
    - Longitud Máxima: N/A
    - Llave Primaria: Si
    - Llave Foránea: No

- **Nombre de Campo: NAME**
    - Descripción: Nombre del Horario, puede ser una descripción del horario, en el sistema cuando creo un registro lo nombre “TURNO - <iniciales del empleado>”
    - Tipo: Texto
    - Longitud Máxima: 60
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: STARTDATE**
    - Descripción: Fecha de inicio del turno, por ejemplo fecha a partir de la cual es válido el turno
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: ENDDATE**
    - Descripción: Fecha de término del turno, por ejemplo fecha hasta la cual es válido el turno
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

Tabla: NUM_RUN_DEIL

Descripción: Esta tabla es el detalle de NUM_RUN, es decir NUM_RUM representaba los turnos, esta tabla representa los horarios, es decir cada registro de esta tabla representa un día y un horario de ese Día donde el usuario tiene que trabajar, en un turno se pueden tener varios horarios, ya sean seguido o intercalados, como ejemplo en una empresa cada empleado tiene 1 turno pero 2 horarios, el horario de entrada de 9 a 3 y el de regreso de la comida de las 4 a 4:30

Campos de Interés:

- **Nombre de Campo: NUM_RUNID**
    - Descripción: Clave para referenciar a que turno pertenece
    - Tipo: Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: Si

- **Nombre de Campo: STARTTIME**
    - Descripción: Hora de inicio del horario
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: No

- **Nombre de Campo: ENDTIME**
    - Descripción: Hora de Final del horario
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: No

- **Nombre de Campo: SDAYS**
    - Descripción: Día de inicio que aplica el horario(Día de la semana lunes = 1, martes = 2, miércoles = 3, … , sábado = 6)
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: No

- **Nombre de Campo: EDAYS**
    - Descripción: Día de termino que aplica el horario(Día de la semana lunes = 1, martes = 2, miércoles = 3, … , sábado = 6)
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: SCHCLASSID**
    - Descripción: Referencia a la tabla SCHCLASS
    - Tipo: int
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: Si

Tabla: SCHCLASS

Descripción: Esta tabla es el detalle de NUM_RUN_DEIL, es decir NUM_RUN_DEIL representaba los horarios, esta tabla representa las materias donde aplica el horario, es decir cada registro de esta tabla representa una materia, tiene además otros datos de importancia. La manera más fácil de explicar es con un ejemplo, supongamos que tenemos un turno del 01/enero/2009 al 31/diciembre/2009; ahora de ese turno tenemos 2 horarios de 9:00 am a 12:00 pm y de 3:00 pm a 5:00 pm que aplica lunes miércoles y jueves; por ultimo digamos que tenemos 2 materias(o trabajos) que aplican con esos horarios Matemáticas e Historia, entonces nuestras tablas serian así:

NUM_RUN

NUM_RUNID	NAME	STARTDATE	ENDDATE
1	Turno-Ejemplo	01/01/2009	31/12/2009

NUM_RUN_DEIL

NUM_RUNID	STARTTIME	ENDTIME	SDAYS	EDAYS	SCHCLASSID
1	9:00 am	12:00 pm	1	1	1
1	3:00 pm	5:00 pm	1	1	2
1	9:00 am	12:00 pm	3	3	1
1	3:00 pm	5:00 pm	3	3	2
1	9:00 am	12:00 pm	4	4	1
1	3:00 pm	5:00 pm	4	4	2
1	9:00 am	12:00 pm	1	1	3
1	3:00 pm	5:00 pm	1	1	4
1	9:00 am	12:00 pm	3	3	3
1	3:00 pm	5:00 pm	3	3	4
1	9:00 am	12:00 pm	4	4	3
1	3:00 pm	5:00 pm	4	4	4

SCHCLASS

SCHCLASSID	SCHNAME	STARTIME	ENDTIME	LATE MINUTES	EARLY MINUTES	CHECKIN	CHECKOUT
1	Matemáticas	9:00 am	12:00 pm	15	15	1	1
2	Matemáticas	3:00 pm	5:00 pm	15	15	1	1
3	Historia	9:00 am	12:00 pm	15	15	1	1
4	Historia	3:00 pm	5:00 pm	15	15	1	1

Campos de Interés:

- **Nombre de Campo: SCHCLASSID**
    - Descripción: Clave única de la tabla
    - Tipo: Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: Si

- **Nombre de Campo: SCHNAME**
    - Descripción: Nombre/Descripción de la materia/Trabajo
    - Tipo: Texto
    - Longitud Máxima: 60
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: STARTIME**
    - Descripción: Hora de inicio de la materia/trabajo
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: ENDTIME**
    - Descripción: Hora de fin de la materia/trabajo
    - Tipo: Fecha/Hora
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: LATEMINUTES**
    - Descripción: Minutos de tolerancia para salida. Es decir hasta cuantos minutos después de la hora de salida pueden aun registrar su salida
    - Tipo: Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: EARLYMINUTES**
    - Descripción: Minutos de tolerancia para entrada. Es decir hasta cuantos minutos antes de la hora de entrada pueden registrar su entrada
    - Tipo: Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: CHECKIN**
    - Descripción: Si el valor del campo es 1, entonces significa que es obligatorio el registro de entrada a la materia, en caso contrario no es necesario el registro de entrada.
    - Tipo: Numérico
    - Longitud Máxima: N/A

- **Nombre de Campo: CHECKOUT**
    - Descripción: Si el valor del campo es 1, entonces significa que es obligatorio el registro de salida de la materia, en caso contrario no es necesario el registro de salida.
    - Tipo: Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: No
    - Llave Foránea: No

Tabla: USERINFO

Descripción: En esta tabla se guardan los datos de un empleado, nombre, clave, género, fecha de nacimiento, fecha de contratación, etc.

Campos de Interés:

- **Nombre de Campo: USERID**
    - Descripción: Clave única de la tabla
    - Tipo: : Numérico Automático(auto numérico)
    - Longitud Máxima: N/A
    - Llave Primaria: Si
    - Llave Foránea: No

- **Nombre de Campo: BADGENUMBER**
    - Descripción: Clave del empleado
    - Tipo: Texto
    - Longitud Máxima: 24
    - Llave Primaria: No
    - Llave Foránea: No

- **Nombre de Campo: NAME**
    - Descripción: Nombre completo del empleado
    - Tipo: Texto
    - Longitud Máxima: 60
    - Llave Primaria: No
    - Llave Foránea: No

Tabla: USER_OF_RUN

Descripción: En esta tabla se crean la liga para relacionar a un usuario con un turno, lo que indirectamente lo relaciona a horarios y materias.

Campos de Interés:

- **Nombre de Campo: USERID**
    - Descripción: Referencia a la tabla USERID
    - Tipo: : Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: Si
- **Nombre de Campo: NUM_OF_RUN_ID**
    - Descripción: Referencia a la tabla NUM_RUN
    - Tipo: : Numérico
    - Longitud Máxima: N/A
    - Llave Primaria: Si(Parcial)
    - Llave Foránea: Si

CAPITULO VI CONCLUSIONES

En este trabajo se incluyó un resumen general de los diferentes métodos de codificación y tecnologías de reconocimiento biométrico que actualmente se utilizan para el registro y control de acceso de usuarios o empleados a sus centros de trabajo. También se realizo una pequeña introducción a la biometría y dentro de esta al reconocimiento por iris, voz, reconocimiento facial y de la huella digital, todo ello al con el fin de validar cuál de ellos es el más seguro y aceptable para los usuarios.

Un sistema biométrico en un sistema de reconocimiento en el que la identidad de un individuo es determinada a partir de algunas de sus características fisiológicas o de comportamiento. Se añade así un nuevo paradigma a la identificación personal, ya que la autenticación se realiza por medio de ***algo que la persona es***, ya sea un rasgo fisiológico personal, como por ejemplo la huella dactilar (figura VI.1), el iris, etc.; o ***algo que la persona genera*** como un patrón de comportamiento, por ejemplo la voz, la firma escrita, entre otras.

Figura VI.1

Los métodos tradicionales de autenticación presentan el gran inconveniente de no poder discriminar de manera fiable entre los individuos legítimos y los individuos impostores, ya que la identidad que la persona tiene puede ser sustraída, pérdida, etc. En cambio, los métodos basados en la autenticación de la entidad por medio de los rasgos biométricos de un individuo proporcionan una mayor fiabilidad en la identificación personal.

Las características fisiológicas en las que se basan más frecuentemente los sistemas de reconocimiento biométrico son:

- Huella Dactilar
- Huella Palmar (Palma de la mano)
- Geometría de la mano/dedos
- Cara
- Iris
- Retina

Entre las características del comportamiento esta la voz, la escritura y la firma escrita. En el presente trabajo se menciona también las técnicas y sistemas de reconocimiento de huellas dactilares, el uso de algoritmos de procesado para la mejora de la calidad de imagen y para la extracción de características, el uso de algoritmos para el reconocimiento de patrones de minucias de huella dactilar y la implementación práctica de ellos en un sistema completo de verificación.

Es ya una realidad que la identificación automática a través de tarjetas de código de barras o Smart Cards conviven ya con sistemas biométricos los cuales en un futuro cercano desplazaran a los sistemas tradicionales de control toda vez que la biometría brinda mayor seguridad en el registro de las personas.

Es también ya una realidad que la biometría está implantada en tantos lugares que nos es ya familiar y cotidiano. Algunos de los usos actuales podemos verlos en el acceso a las computadoras, ingreso a aplicaciones con información muy crítica, control de acceso a empresas, bancos, escuelas, laboratorios, etc.

Para el desarrollo de este proyecto, se adquirió un lector de huellas digitales económico y con una tasa muy alta tasa de fiabilidad que permitirá el registro de los profesores en sus horarios de trabajo, con ello se tendrá un control exacto de las asistencias y por supuesto permitirá tomar decisiones de reemplazo o cobertura de algún profesor que por alguna razón falte a dar su clase.

En la actualidad debido a su sencilla implementación y bajo costo/beneficio, la biometría de huella dactilar es el método más utilizado y conocido; **se emplean programas de lectura de huellas digitales, relojes checadores de control biométrico o programas de control de ausentismo por lectura biométrica, estos sistemas son aquellos que utilizando lectores de huellas digitales integrados a una red de computadoras o bien lectores autónomos de huellas digitales permiten verificar el ingreso, salida, ausentismo y otras situaciones relacionadas con el control de personal.** Los principios en los que se basa están relacionados con la traducción de la información contenida en la huella digital (utilizan un mapa de puntos clave de una huella dactilar) a algoritmos únicos y personales que se emplean para identificar al usuario y relacionar esta información con sus datos personales. Estos sistemas de lectura de huellas digitales por biometría utilizan menos de un segundo para captar e identificar al poseedor de la impresión dactilar.

Se ha desarrollado una aplicación cliente-servidor que permite realizar una interface entre la base de datos de la aplicación de registro y control de asistencia del fabricante del hardware y la hoja de trabajo en Excel (Anexo I) que la Facultad de Ingeniería utiliza ahora para el registro y generación de horarios de los profesores.

La interface permite subir de forma inmediata todos los horarios establecidos para el ciclo laboral actual sin la necesidad de su captura en la aplicación de control de asistencia.

La aplicación de control de asistencia a la vez nos permite el registro exacto del ingreso y egreso de los profesores y emite reportes de asistencia en periodos definidos por el administrador del sistema.

La puesta a punto del programa (creación de horarios, alta de empleados, etc.) y su uso diario es sencilla, disponiendo por ejemplo de asistentes para la copia de horarios entre días de la semana; asimismo controla los permisos de accesos de

cada empleado o autónomos, se pueden restringir las entradas por lector o por horario. Se captura la huella desde el propio PC (con ayuda de un lector USB) y se envía a los terminales deseados. El software descarga automáticamente todos los eventos ocurridos en los terminales, y los presenta en forma de reportes para su mejor comprensión. Estos informes son exportables a Excel. Admite la creación y control de varias empresas y/o departamentos, lo que lo convierte en un sistema escalable.

Una vez implementado e instalado el sistema se espera una reducción del índice de ausentismo y mayor agilidad en el procesamiento de información para el pago de nómina. Se eliminarán por completo los registros de asistencia vía Kardex y se evitará también que personas ajenas al registro puedan registrar la entrada o salida en los turnos correspondientes.

TRABAJO A FUTURO

El propósito actual de este trabajo se ha limitado a conocer a detalle los mecanismos de identificación actual y la viabilidad de implementación del reconocimiento de huella dactilar en la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. Con esta premisa podemos acotar una serie de acciones a futuro que podrían desarrollarse los cuales se enumeran a continuación.

- Desarrollo de Interface WEB para análisis de información estadística de los registros de asistencia del personal.

- Generación de reportes de asistencia, por áreas, departamentos, facultades, etc. partiendo de que la base de datos actuales del sistema nos permite el acceso irrestricto a la misma, los cuales pueden ser consultados mediante la creación de la interface WEB sugerida.

- Integración del sistema de control de asistencias al sistema de nóminas de la Facultad de Ingeniera toda vez que la información colectada es de un muy alto índice de fiabilidad.
- Expansión del sistema de control de asistencias a todos y cada uno de los departamentos de la Facultad, el sistema es multiusuario, maneja múltiples empresas (facultades) y múltiples departamentos, adicional a ello y no menos importante es que cada dispositivo permite solo recibir y colectar la información que le corresponde.
- Creación de una RED de dispositivos de control de asistencia a través de una red Ethernet o Inalámbrica WIFI 802.11a, b, o g.
- Adición de control de mecanismos de apertura al dispositivo de control de asistencia para controlar la asistencia y control de apertura y cierre a laboratorios, aulas, etc.

VENTAJAS Y DESVENTAJAS

La autenticación de la gente a través del uso de equipos biométricos de rostro, palma, voz, huella dactilar, etc. Posee ventajas y desventajas operativas y comparativas, las cuales deben tenerse en consideración al momento de decidir si el utilizar este tipo de equipo cumple con los requerimientos solicitados. En particular deben considerarse las diferencias entre los métodos anatómicos y los de comportamiento, para fines prácticos se usan siempre métodos anatómicos para la autenticación de personal.

En el caso particular de la huella dactilar, salvo daño físico, es la misma día a día, a diferencia de una firma que puede ser diferente debido a por factores controlables como por psicológicos no intencionales. Debido a diferencias como las señaladas, no existe un único sistema biométrico que sea capaz de satisfacer todas las necesidades.

Dependiendo del nivel de seguridad que se requiera se puede incluso decidir el uso de distintas técnicas y diferentes tipos de equipos en diferentes áreas de control. Más aún, existen esquemas que utilizan de manera integrada más de una característica para la identificación, como vimos con anterioridad se puede utilizar un mismo equipo para identificar la huella y además requerir con números de identificación única para tener 2 elementos de validación, se puede incluir también la comparación del rostro o la identificación de la voz, por supuesto entre mas elementos de control necesitemos más costoso será el equipo a utilizar. Por ejemplo, se integran el reconocimiento de rostros y huellas dactilares.

Anexo I Registro actual de control de horarios y asignaturas

(División de Ingeniería Mecánica y Eléctrica DIE)

(Extracción de hoja de calculo Excel)

CURP	NO_TRAB	NOMBRE_LARGO	DIV	CVE.	ASIGNATURA	GPO	HORAS	INICIO	FIN	LUN	MAR	MIE	JUE	VIE	SAB	SALON	TIPO	INSC
BOBR280629HDFRRB00	10370	BROWN Y BROWN ROBERTO	3	627	PLANTAS GENERADORAS	2	4.00	1800	2000		*		*			109A	T	1
BOBR280629HDFRRB00	10370	BROWN Y BROWN ROBERTO	3	1890	PLANTAS GENERADORAS	2	3.0	1800	1930		*		*			109A	T	18
MACC370427HMCRLR02	16504	MARTINEZ CALDERON CARLOS	3	1834	MAQUINAS SINCRONAS Y D CORRI	3	4.00	915	1130		*		*			L-18	T	2
MACC370427HMCRLR02	16504	MARTINEZ CALDERON CARLOS	3	1889	MAQUINAS ELECTRICAS II	3	4.5	915	1130		*		*			L-18	T	4
MACC370427HMCRLR02	16504	MARTINEZ CALDERON CARLOS	3	4892	LAB. PROTECCION DE SISTS. ELECT	2	2.0	1800	2000	*						LAB.	L	6
VILJ211225HNEQNC03	16793	VIQUEIRA LANDA JACINTO	3	814	SISTEMAS ELECTRICOS DE POTENC	3	4.00	1130	1330		*		*			110	T	2
VILJ211225HNEQNC03	16793	VIQUEIRA LANDA JACINTO	3	1064	SISTEMAS ELECTRICOS DE POTENC	3	4.5	1130	1345		*		*			110	T	25
VILJ211225HNEQNC03	16793	VIQUEIRA LANDA JACINTO	3	1749	SISTEMAS ELECTRICOS DE POTENC	3	4.5	1130	1345	*		*				109	T	30
FEVP330206HVZRLL00	17729	FERNANDEZ VILLALOBOS PELAYO	3	129	DINAMICA DE SISTEMAS FISICOS	1	4.00	830	950	*		*		*		415	T	1
FEVP330206HVZRLL00	17729	FERNANDEZ VILLALOBOS PELAYO	3	1547	DINAMICA DE SISTEMAS FISICOS	1	4.5	830	1000	*		*		*		415	T	38
FEVP330206HVZRLL00	17729	FERNANDEZ VILLALOBOS PELAYO	3	1656	MAQUINAS ELECTRICAS I	1	4.5	1000	1130	*		*		*		211	T	29
ROCF341014HDFDYR06	22568	RODRIGUEZ Y CAYEROS FRANCISCO	3	558	MEDICION E INSTRUMENTACION	1	3.0	830	1000	*		*				109A	T	40
PABL380802HQTLNB12	26451	PALOMINO BENSON LEOBARDO LUIS	3	943	ADMON. DE CENTROS TECNOL. DE	2	4.0	700	900		*		*			L-10	T	4
VAOD420312HDFZRV01	27121	VAZQUEZ ORTIZ DAVID	3	1749	SISTEMAS ELECTRICOS DE POTENC	4	4.5	1800	2015	*		*				109	T	9
VAOD420312HDFZRV01	27121	VAZQUEZ ORTIZ DAVID	3	1749	SISTEMAS ELECTRICOS DE POTENC	5	4.5	915	1130		*		*			109A	T	22
VAOD420312HDFZRV01	27121	VAZQUEZ ORTIZ DAVID	3	4749	LAB. SISTS. ELECTRICOS POTENCIA	16	2.0	1100	1300					*		LAB.	L	7
ZEGA440520HDFPRD07	31971	ZEPEDA GOROSTIZA ADAN	3	962	TEMAS SELECTOS DE ING. DE SOFT	2	3.0	1600	1730			*				109A	T	6
ZEGA440520HDFPRD07	31971	ZEPEDA GOROSTIZA ADAN	3	962	TEMAS SELECTOS DE ING. DE SOFT	2	3.0	1600	1730	*						LAB.	T	6
ZEGA440520HDFPRD07	31971	ZEPEDA GOROSTIZA ADAN	3	1553	INGENIERIA DE SOFTWARE	2	4.5	1800	2015	*		*				LAB.	T	28

GLOSARIO

A

Accuracy – Precisión

Término general utilizado para describir cuál es el rendimiento de un sistema biométrico. La estadística real que determina dicho rendimiento varía según la tarea a realizar (verificación, identificación de grupo abierto (listas de vigilancia) e identificación de grupo cerrado).

Algorithm - Algoritmo

Secuencia limitada de instrucciones o pasos que indica a un sistema computarizado cómo resolver un problema en especial. Un sistema biométrico utiliza múltiples algoritmos; por ejemplo, para el procesamiento de imágenes, la generación de plantillas, comparaciones, etc.

ANSI – Instituto Americano de Estándares Nacionales

Organización privada y sin fines de lucro que administra y coordina el sistema de evaluación de conformidad y de estandarización voluntaria de los Estados Unidos.

API - Interfaz de programación de aplicaciones

Instrucciones o herramientas para formato utilizadas por programadores de aplicaciones para vincular y construir aplicaciones para hardware y software.

Arch – Arco (Figura G.1)

Patrón de huellas dactilares en el cual las crestas de fricción entran por un lado, se elevan en el centro y salen por el lado opuesto. Este patrón no presenta ningún delta verdadero.

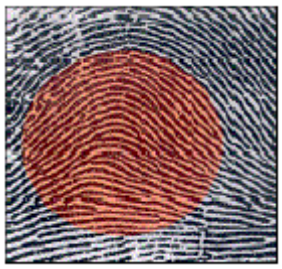

Figura G.1.

Aspecto Métrico

La medición métrica verifica si el ancho de la barra, los espacios o las combinaciones están dentro de la especificación.

Authentication - Autenticación

En Biometría, la palabra “autenticación” suele usarse como sinónimo genérico de “verificación”.

B

Behavioral Biometric Characteristic – Característica biométrica de comportamiento

Característica biométrica aprendida y adquirida con el tiempo, y no basada en la biología. De algún modo, todas las características biométricas dependen tanto de características de comportamiento como de características biológicas. Ejemplos de modalidades biométricas en las que pueden dominar las características de comportamiento son el reconocimiento de firmas y el dinamismo de pulsación de teclas.

Benchmarking – Evaluación comparativa

Proceso mediante el cual se compara el rendimiento medido con un valor de referencia estándar, disponible al público.

Bifurcation - Bifurcación (Figura G.2.)

Punto en una huella dactilar en el que una cresta de fricción se divide o bifurca para formar dos crestas.

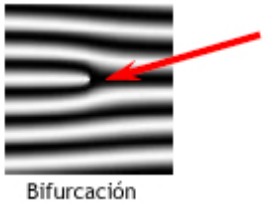

Figura G.2.

Binning - Binarización

Proceso de análisis (examen) o de clasificación de datos para acelerar o mejorar la coincidencia biométrica.

BioAPI – Interfaz de programación de aplicaciones de biometría

Define la interfaz de programación de aplicaciones y la interfaz del proveedor de servicios para una interfaz estándar de tecnología biométrica. La interfaz BioAPI permite que los dispositivos biométricos sean fáciles de instalar, incorporar o fáciles de cambiar dentro de la arquitectura global del sistema.

Biological Biometric Characteristic – Característica biométrica biológica

Característica biométrica basada principalmente en una característica anatómica o fisiológica, y no en un comportamiento aprendido. De algún modo, todas las características biométricas dependen tanto de características de comportamiento como de características biológicas. Ejemplos de modalidades biométricas en las que pueden dominar las características biológicas son la geometría de las huellas dactilares y la geometría de las manos.

Biometrics – Biometría

Término general utilizado para describir una característica o un proceso.
Como característica: Característica biológica (anatómica y fisiológica) y de comportamiento medible, que puede ser utilizada para el reconocimiento automatizado.
Como proceso: Métodos automatizados de reconocimiento de un individuo, basados en características biológicas (anatómicas y fisiológicas) y de comportamiento medibles.

Biometric Data – Datos biométricos

Término general para referirse a los datos computarizados, creados durante un proceso biométrico. Comprende las observaciones crudas del sensor, las muestras biométricas, los modelos, plantillas y resultados de semejanza. Los datos biométricos se utilizan para describir la información recopilada durante los procesos de inscripción, verificación o identificación, pero no se aplican a la información del usuario final; como nombre de usuario, información demográfica ni autorizaciones.

Biometric Sample – Muestra biométrica

Información o datos computarizados, obtenidos por medio de un dispositivo con sensor biométrico. Por ejemplo, imágenes de rostros o de huellas dactilares.

Biometric System – Sistema biométrico

Componentes individuales múltiples (tales como sensor, algoritmo de coincidencia y visualización de resultado) que se combinan para crear un sistema totalmente funcional. Un sistema biométrico es un sistema automatizado capaz de:
1. capturar una muestra biométrica del usuario final;
2. extraer y procesar los datos biométricos de dicha muestra;
3. almacenar la información extraída en una base de datos;

4. comparar los datos biométricos con los datos en una o más referencias de referencia; y
5. decidir el grado de coincidencia e indicar si se ha logrado una identificación o verificación de identidad o no.

C

Capture – Captura

Proceso de recopilación de una muestra biométrica de un individuo por medio de un sensor.

Cálculo de Dígito Verificador

Algoritmo del Sistema GS1 para el cálculo de un Dígito de Verificación para verificar la exactitud de los datos decodificados de un símbolo de Código de Barras.

Closed-set Identification – Identificación de grupo cerrado

Tarea biométrica durante la cual se sabe que un individuo no identificado es parte de la base de datos y el sistema intenta determinar su identidad. El rendimiento se mide según la frecuencia con la cual el individuo aparece en el rango principal del sistema (o en los primeros 5, en los primeros 10, etc.).

Comparison – Comparación

Proceso de comparación de una referencia biométrica con una referencia o referencias almacenadas con anterioridad, para tomar una decisión sobre identificación o verificación.

Contraste

Mide el reflejo de una barra y un espacio, es decir, el grado en que las barras y los fondos de los símbolos en Códigos de Barras reflectan la luz.

D

Database – Base de datos

Recopilación de uno o más archivos computarizados. En el caso de sistemas biométricos, estos archivos pueden ser lecturas del sensor biométrico, plantillas, resultados de coincidencias, información sobre el usuario final, etc.

Decision – Decisión

Acción a seguir (automática o manual) que resulta de la comparación de un resultado de semejanza (o medida similar) con la escala del sistema.

Decodificación

Como un parámetro de calificación, el resultado de la decodificación intentada de un perfil de reflectancia de lectura aplicando el algoritmo de decodificación de referencia de la simbología.

Decodificador

Componente del lector de Códigos de Barras que traduce a datos las señales eléctricas que representan el perfil de reflectancia de la lectura.

Delta Point – Delta (Figura G.3.)

Parte del patrón de una huella dactilar que se asemeja a la letra griega delta (x), como se observa a continuación. Técnicamente, es el punto en una cresta de fricción más cercano al punto de divergencia de los dos tipos de líneas, y está ubicado justo en frente del punto de divergencia.

Figura G.3.

Detection and Identification Rate – Tasa de detección e identificación

Tasa en la cual los individuos que son parte de la base de datos son correctamente identificados en una aplicación.

Detection Error Trade-off (DET) Curve – Curva de compensación por error de detección (Figura G.4.)

Trazo gráfico de las tasas de error medidas, como se observa a continuación. Por lo general, las curvas DET trazan las tasas de error de coincidencias (tasa de falsa no coincidencia vs. tasa de falsa coincidencia) o las tasas de error de decisión (tasa de falso rechazo vs. tasa de falsa aceptación).

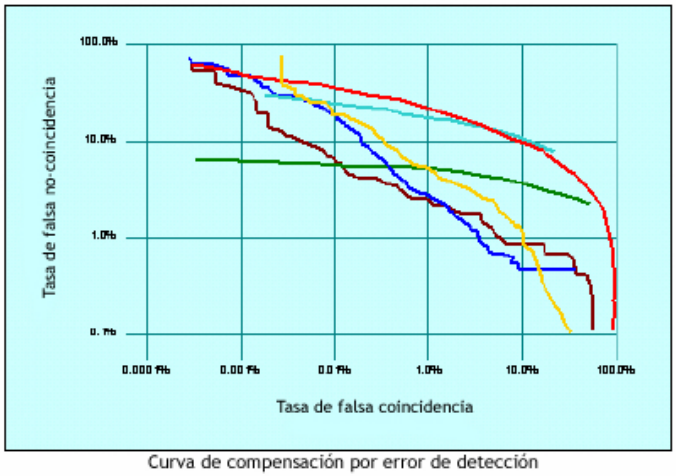

Figura G.4.

Difference Score – Resultado de diferencia

Valor obtenido a través de un algoritmo biométrico, que indica el grado de diferencia entre una muestra biométrica y una referencia.

Dígito Verificador

Un dígito calculado usando los demás dígitos de una Cadena de Elementos, usado para verificar que la composición de los datos es correcta.

Dimensión X

Ancho nominal de los elementos angostos de un símbolo de código de barras; la dimensión básica del símbolo del código de barras en las que normalmente se basan todas sus demás dimensiones.

E

Encryption – Codificación

Transformación de datos en forma incomprensible de modo que no puedan ser leídos por personas no autorizadas. Se utiliza una clave o contraseña para decodificar los datos codificados.

End User – Usuario final

Individuo que interacciona con el sistema para inscribirse, ser verificado o identificado.

Enrollment – Inscripción

Proceso de recopilación de muestra biométrica de un usuario final, conversión de la misma en referencia biométrica y almacenamiento de la referencia en la base de datos del sistema biométrico para posterior comparación.

Equal Error Rate (EER) – Tasa de igual error

Estadística utilizada para mostrar el rendimiento biométrico; por lo general, durante la tarea de verificación. La tasa EER es la ubicación en una curva ROC (Característica de funcionamiento del receptor) o DET (Compensación por error de detección) donde la tasa de falsa aceptación y la tasa de falso rechazo (o uno menos la tasa de verificación {1-VR}) son iguales. Por lo general, cuánto más bajo sea el valor de la tasa de igual error, mayor será la precisión del sistema biométrico.

Escaneo

Acción de pasar en lector óptico sobre un Código de Barras para su lectura. Ej. El escaneo de productos en el punto de venta (POS)

Extraction - Extracción

Proceso de conversión de una muestra biométrica capturada en datos biométricos para que puedan ser comparados con una referencia.

F

Face Recognition – Reconocimiento de rostro

Modalidad biométrica que utiliza una imagen de la estructura física visible del rostro de una persona para fines de reconocimiento.

Failure to Acquire (FTA) – Error de captura

Error del sistema biométrico en la captura o extracción de información útil de una muestra biométrica.

Failure to Enroll (FTE) – Error de inscripción

Error del sistema biométrico en la creación de una referencia de inscripción adecuada para un usuario final. Los errores comunes suelen ser usuarios finales quienes no están adecuadamente entrenados para proveer su información biométrica, sensores que no capturan la información de manera correcta o datos del sensor capturados de calidad insuficiente para desarrollar una plantilla.

False Acceptance Rate (FAR) – Tasa de falsa aceptación

Estadística utilizada para medir el rendimiento biométrico durante la tarea de verificación. Porcentaje de veces que un sistema produce una falsa aceptación, lo cual ocurre cuando un individuo es erróneamente vinculado con la información biométrica existente de otra persona.

False Alarm Rate – Tasa de falsa alarma

Estadística utilizada para medir el rendimiento biométrico durante una identificación de grupo abierto. Porcentaje de veces que una alarma suena incorrectamente ante un individuo que no es parte de la base de datos del sistema biométrico.

False Match Rate – Tasa de falsa coincidencia

Estadística utilizada para medir el rendimiento biométrico cuando. Similar a la tasa de falsa aceptación (FAR).

False Non-Match Rate – Tasa de falsa no coincidencia

Estadística utilizada para medir el rendimiento biométrico. Similar a la tasa de falso rechazo (FRR), excepto que la tasa FRR incluye la tasa de error de captura, mientras que la tasa de falsa no coincidencia no la incluye.

False Rejection Rate (FRR) – Tasa de falso rechazo

Estadística utilizada para medir el rendimiento biométrico durante la tarea de verificación. Porcentaje de veces que el sistema produce un falso rechazo. Ocurre un falso rechazo cuando un individuo no es vinculado con su propia plantilla biométrica existente.

Feature(s) – Característica(s)

Características matemáticas distintivas derivadas de una muestra biométrica, utilizadas para generar una referencia.

Fingerprint Recognition – Reconocimiento de huellas dactilares

Modalidad biométrica que utiliza la estructura física de la huella dactilar de un individuo para fines de reconocimiento. Los puntos característicos importantes utilizados en la mayoría de los sistemas de reconocimiento de huellas dactilares son las minucias, las cuales incluyen bifurcaciones y finales de crestas.

Friction Ridge – Cresta de fricción

Crestas en la piel de los dedos y de las palmas de las manos, y en los dedos y las suelas de los pies, las cuales hacen contacto con una superficie incidente ante el roce normal. En los dedos, patrones distintivos formados por las crestas de fricción que forman las huellas dactilares.

G-H

Gallery - Galería

Base de datos del sistema biométrico o grupo de personas conocidas, usados para una implementación específica o experimento de evaluación.

GS1

Asociación Europea de Numeración o EAN (European Article Numbering por sus siglas en inglés). En 1974 nace con el nombre de Asociación EAN con 12 países europeos que la integraban. En 1977 por la internacionalización de la Asociación, EAN lo cambia por EAN Internacional, ahora GS1. Actualmente existen 104 organizaciones miembro representadas en 145 países. Estas organizaciones proporcionan el apoyo total y la información a sus compañías locales. Más de un millón de compañías a nivel mundial se benefician de usar el Sistema GS1. AMECE es el organismo que representa a México.

GSMP

GS1 desarrolla esta Plataforma llamada "Procesos Globales en el Manejo de los Estándares"

GSMP (por sus siglas en inglés Global Standards Management Process). Tiene como objetivo principal asegurar la calidad y el desarrollo veraz del sistema GS1, de acuerdo con el manejo de los negocios. Este desarrollo necesita emerger de los usuarios alrededor del mundo.

GTIN

Número Mundial de Artículo Comercial o Número Global de Artículo Comercial o GTIN (Global Trade Ítem Number por sus siglas en inglés) se utiliza para identificar cualquier artículo (producto o servicio) sobre los cuales hay necesidad de recuperar la información predefinida, logrando entregar, pedir o facturar desde cualquier punto de la cadena de abastecimiento.

GTIN-8

Formado por 8 dígitos. Este código puede ser utilizado en artículos muy pequeños donde, por su tamaño y sistema de impresión, no puede aplicarse un GTIN-13 y/o un GTIN-12.

GTIN-12

Formado por 12 dígitos. Este código puede ser utilizado para exportar sus productos a todos los países del mundo, incluyendo a empresas de Estados Unidos y Canadá.

GTIN-13

Formado por 13 dígitos. Este código puede ser utilizado para exportar sus productos a todos los países del mundo, incluyendo a algunas empresas de Estados Unidos y Canadá.

GTIN-14

Formado por 14 dígitos. Es el código que identifica a la unidad de expedición y que también conocido como ITF/DUN-14, cuya estructura está basada en la identificación primaria de un artículo y una variable logística (1 dígito) que identifica el contenido de la unidad de expedición.

Hand Geometry Recognition – Reconocimiento de geometría de la mano

Modalidad biométrica que utiliza la estructura física de la mano de un individuo para fines de reconocimiento.

I

Identification - Identificación

Tarea en la cual el sistema biométrico busca en una base de datos una referencia que coincida con la muestra biométrica suministrada y, de encontrarla, devuelve la identidad correspondiente. Se recopila información biométrica y se la compara con todas las referencias en la base de datos. La identificación es “de grupo cerrado” si se sabe que la persona es parte de la base de datos. En identificación "de grupo abierto”, no existe garantía de que la persona sea parte de la base de datos.

El sistema debe determinar si la persona es parte de la base de datos, y luego devolver la identidad.

Identification Rate – Tasa de identificación

Tasa en la cual un individuo que es parte de la base de datos es correctamente identificado.

Identity Management – Administración de identidad

Combinación de sistemas, reglas y procedimientos que define el acuerdo entre individuo y organizaciones respecto de la titularidad, el uso y la protección de la información personal.

Impresión a Solicitud

Se refiere a los procesos de impresión en donde la imagen del símbolo del Código de Barras se genera e imprime directamente en una etiqueta u otro sustrato, por ejemplo, impresión térmica, de transferencia térmica, de inyección de tinta.

Impresión con Tinta Húmeda

Impresión convencional usando tintas líquidas o en pasta, como las que se usan principalmente para la producción de empaques y materiales impresos similares, por ejemplo, offset, litografía, flexo grafía, fotograbado, proceso de malla, etc.

Impresión Directa

Un proceso en donde el aparato de impresión imprime el símbolo haciendo contacto físico con un sustrato (por ejemplo, flexo grafía).

Infrared - Infrarrojo

Luz que cae fuera del espectro visible humano, en el lado rojo (de baja frecuencia).

Iris Recognition – Reconocimiento de iris

Modalidad biométrica que utiliza una imagen de la estructura física del iris de una persona para fines de reconocimiento.

IrisCode© - IrisCode©

Formato de característica biométrica utilizado en el sistema de reconocimiento de iris Daugman (John Daugman, Universidad de Cambridge, Reino Unido).

ISBN

Internacional Standard Book Number o Número Internacional Normalizador de Libros.

ISSN

Internacional Standard Serial Number o Número Internacional Normalizador para Publicaciones Seriadas.

Ítems

Ítem = producto y/o servicio.

L

Latent Fingerprint – Huella dactilar latente

“Imagen” de una huella dactilar que queda en una superficie tocada por un individuo. La impresión transferida resulta del contacto de la superficie con las crestas de fricción, generalmente causada por los residuos grasosos producidos por las glándulas sudoríparas de los dedos.

Lector

Sistema para iluminar el símbolo del Código de Barras, que recoge la luz reflejada desde este y la decodifica. Comprende al lector y las sub-unidades de decodificadores.

Loop - Lazo

Patrón de huella dactilar en el cual las crestas de fricción entran por cualquiera de los dos lados, se curvan acentuadamente y salen cerca del mismo lado por el cual entraron, como se observa a continuación. Este patrón presenta un núcleo y un delta.

M

Match - Coincidencia

Decisión según la cual una muestra biométrica y una plantilla almacenada provienen de la misma fuente humana, basada en el alto grado de semejanza (diferencia o distancia de Hamming).

Matching – Proceso para coincidencia

Proceso que incluye la comparación de una muestra biométrica con una plantilla almacenada anteriormente, y el cálculo del grado de semejanza (diferencia o distancia de Hamming). Los sistemas toman las decisiones basándose en este resultado y en la relación (por encima o por debajo) con la escala predeterminada.

Minutia(e) Point – Minucia(s)

Características de las crestas de fricción que se utilizan para identificar una imagen de huella dactilar. Las minucias son los puntos donde las crestas de fricción comienzan, terminan o se dividen en dos o más crestas (Figura G.5.) En muchos sistemas de huellas dactilares se realizan comparaciones de las minucias (a diferencia de las imágenes) con fines de reconocimiento.

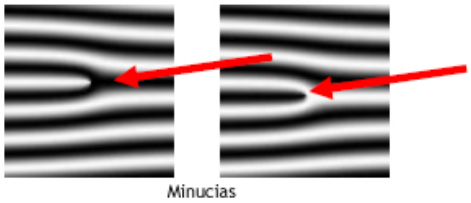

Figura G.5.

Modality - Modalidad

Tipo o clase de sistema biométrico. Por ejemplo: reconocimiento de rostro, reconocimiento de huellas dactilares, reconocimiento de iris, etc.

Modulación

Como parámetro calificado, el Contraste de Borde más bajo en el perfil de reflectancia de lectura dividido entre el Contraste del Símbolo.

Módulo

La unidad de medida del ancho nominal más angosto en un símbolo de Código de Barras. En ciertas simbologías, los anchos de los elementos pueden especificarse como múltiplos de un módulo. Equivalente a la dimensión X.

Multimodal Biometric System – Sistema biométrico multimodo

Sistema biométrico en el cual dos o más de los componentes de modalidad (característica biométrica, tipo de sensor o algoritmo de extracción de característica) se utilizan al mismo tiempo.

N-O

Noise - Ruido

Componentes no deseados en una señal que degradan la calidad de los datos o interfieren con las señales deseadas que procesa el sistema.

One-to-many – (1:N) Uno a muchos

Frase utilizada en el campo de la biometría para describir un sistema que compara una referencia con muchas referencias registradas para la toma de decisiones.

One-to-one – (1:1) Uno a uno

Frase utilizada en el campo de la biometría para describir un sistema que compara una referencia con otra referencia registrada para la toma de decisiones. Por lo general, la frase se refiere a la tarea de verificación (aunque no todas las tareas de verificación son verdaderamente uno a uno). La tarea de identificación puede realizarse por medio de una serie de comparaciones uno a uno.

Open-set Identification – Identificación de grupo abierto

Tarea biométrica que sigue las condiciones del sistema operativo biométrico más de cerca para 1) determinar si una persona es parte de la base de datos y 2) encontrar el registro de dicha persona en la base de datos.

P

Palm Print Recognition – Reconocimiento de palma (Figura G.6.)

Modalidad biométrica que utiliza la estructura física de la palma de la mano de un individuo para fines de reconocimiento, como se observa a continuación.

Figura G.6.

Película Maestra

Original fotográfico (negativo o positivo) de un símbolo de Código de Barras, usado para reproducción en procesos de impresión convencionales o de tinta húmeda.

Performance - Rendimiento

Frase general utilizada para describir la medición de las características, como precisión o velocidad, de un algoritmo o sistema biométrico.

PIN - Personal Identification Number – Clave de identificación personal

Método de seguridad utilizado para validar junto con un dato biométrico la identidad de una persona. El PIN puede ser ingresado vía teclado.

Pixels Per Inch (PPI) – Píxeles por pulgada

Medida de la resolución de una imagen digital. Cuánto más píxeles por pulgada, mayor información incluida en la imagen y mayor el tamaño del archivo.

Punto de Venta

Se les conoce también como terminales POS (Point of Sale) por sus siglas en inglés o lo que antes se conocía como la caja registradora.

R

Radio Frequency Identification (RFID) – Identificación por radio frecuencia

Tecnología que utiliza transmisores de radio de baja frecuencia para leer datos almacenados en un transponder. Los equipos de RFID pueden utilizarse para administrar inventarios, autorizar procesos de identificación de bienes y actuar como claves electrónicas. La identificación RFID no es biométrica.

Recognition - Reconocimiento

Término general utilizado en la descripción de sistemas biométricos (por ejemplo, reconocimiento de rostro o reconocimiento de iris) en relación con su función principal. El término “reconocimiento” no implica necesariamente verificación, identificación de grupo cerrado ni identificación de grupo abierto (lista de vigilancia).

Record - Registro

Plantilla y demás información sobre el usuario final (por ejemplo, nombre, permisos de acceso).

Reference - Referencia

Datos biométricos de un individuo, almacenados para ser usados en reconocimiento posterior. Una referencia puede ser una o más plantillas, modelos o imágenes.

Resolution - Resolución

Cantidad de píxeles por distancia de unidad en la imagen. Describe la definición y claridad de la imagen.

Ridge Ending - Final de cresta (Figura G.7.)

Minucia al final de una cresta de fricción, como se observa a continuación.

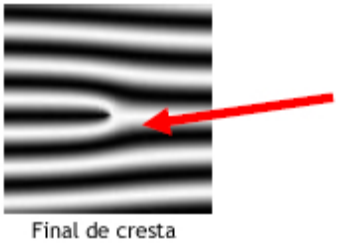

Figura G.7.

S

Scanner

Componente de un lector del Código de Barras, que ilumina el símbolo del Código de Barras, recoge la luz reflejada desde éste y envía una salida de una señal eléctrica (al decodificador) que representa el perfil de reflectancia de lectura.

Segmentation - Segmentación (Figura G.8.)

Proceso de análisis de la señal biométrica de interés de todo el sistema de datos adquiridos. Por ejemplo, la clasificación de imágenes dactilares individuales de una impresión grupal, como se observa a continuación.

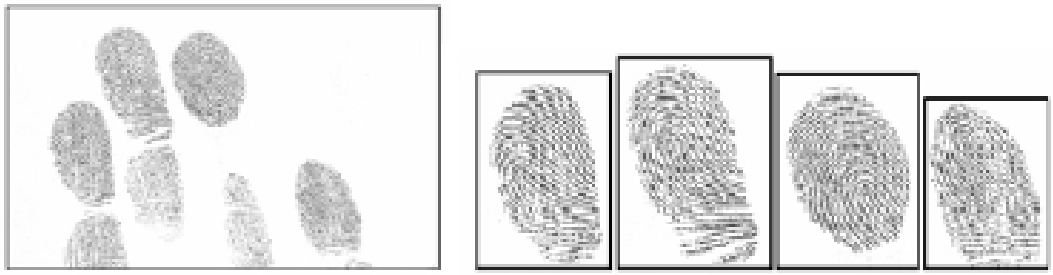

Figura G.8.

Sensor - Sensor

Hardware en un dispositivo biométrico que convierte los datos biométricos de entrada en una señal digital, y transmite esta información al dispositivo de procesamiento.

Signature Dynamics – Dinamismo de firma

Modalidad biométrica de comportamiento que analiza las características dinámicas de la firma de un individuo; como el tamaño y la velocidad de la firma, la presión de la lapicera y los movimientos de la misma en el aire, para su reconocimiento.

Similarity Score – Resultado de semejanza

Valor obtenido a través de un algoritmo biométrico, que indica el grado de semejanza o correlación entre una muestra biométrica y una referencia.

Símbolo

La combinación de caracteres y características del símbolo requeridas por una simbología en particular, incluyendo la Zona de Silencio, los Caracteres Iniciales y de Paro, los caracteres de datos y otros patrones auxiliares.

Simbología

Un método definido para representar caracteres numéricos o alfabéticos en un Código de Glosario Barras; un tipo de Código de Barras.

SKU

Stock Keeping Unit es una herramienta que sirve para identificar de manera única los ítems o artículos, permitiéndonos tener una visión completa de las existencias del producto. Este identificador sirve para identificar de manera personalizada e interna las mercancías. El SKU no es un sistema de identificación mundial como lo es el Sistema GS1.

Speaker Recognition – Reconocimiento de hablante

Modalidad biométrica que utiliza el habla de una persona, una característica influenciada tanto por la estructura física del tracto vocal del individuo como por las características de comportamiento del individuo, para fines de reconocimiento. Se lo suele llamar “Reconocimiento de voz”. “Reconocimiento del habla” reconoce las palabras que se pronuncian, y no es una tecnología biométrica.

Speech Recognition – Reconocimiento del habla

Tecnología que permite que una máquina reconozca las palabras pronunciadas. El reconocimiento del habla no es una tecnología biométrica.

Submission – Sometimiento

Proceso durante el cual un usuario final suministra su muestra biométrica a un sistema biométrico.

Sustrato

El material en el que se imprime el símbolo del Código de Barras.

T

Template – Plantilla

Representación digital de las características distintivas de un individuo, que contiene la información extraída de una muestra biométrica. Las plantillas se utilizan durante la autenticación biométrica como base de comparación.

True Accept Rate (TAR) – Tasa de verdadera aceptación

Estadística utilizada para medir el rendimiento biométrico durante la tarea de verificación. Porcentaje de veces que un sistema (correctamente) verifica una declaración verdadera de identidad.

True Reject Rate – Tasa de verdadero rechazo

Estadística utilizada para medir el rendimiento biométrico durante la tarea de verificación. Porcentaje de veces que un sistema (correctamente) rechaza una declaración falsa de identidad.

Truncamiento

Acción de realizar la impresión de un símbolo más pequeño que las recomendaciones de altura mínima de las especificaciones de la simbología. El truncado puede hacer que se dificulte la lectura del símbolo por el operador.

U-V

Unidad de Consumo

También conocidos como productos para el consumidor final o artículos comerciales. Son aquellos artículos comerciales previstos para ser comercializados al consumidor final en el Punto de Venta de las tiendas. Estos son identificados con un único GTIN (GTIN-8, GTIN-12 o GTIN-13).

Unidad de Expedición

También se les conoce como corrugados, bultos, bulto continente o unidad logística. Sirve para identificar el nivel de embalaje para los artículos comerciales donde el socio comercial requiere de una identificación de un GTIN, entonces estos artículos se convierten en un Grupo de Artículos Comerciales Estándar.

User - Usuario

Persona, como un administrador, que interactúa con los usuarios finales o controla la interacción de estos con el sistema biométrico.

Verification - Verificación

Tarea durante la cual el sistema biométrico intenta confirmar la identidad declarada de un individuo, al comparar la muestra suministrada con una o más plantillas registradas con anterioridad.

Verification Rate – Tasa de verificación

Estadística utilizada para medir el rendimiento biométrico durante la tarea de verificación. Tasa en la cual los usuarios finales legítimos son correctamente verificados.

Vulnerability - Vulnerabilidad

Potencial para el funcionamiento de un sistema biométrico de verse comprometido por dolo (actividad fraudulenta), defecto de diseño (error de uso incluido), accidente, falla en el hardware, o condición ambiental externa.

Z

Zona de Silencio

Un espacio claro que no contiene marcas legibles por la máquina, que precede al carácter Inicial de un símbolo de Código de Barras y sigue el Carácter de Paro. Anteriormente, se conocía como “Área Clara”, “Zona Tranquila”, “Zona Muda” o “Margen Claro”.

BIBLIOGRAFÍA

Biometría e identificación de personas. Kimaldi. 2008.
http://www.kimaldi.com

Lectores de huella digital. TEC Electrónica, S.A. de C.V.
http://www.tecmex.com.mx/promos/bit/bit0903-bio.htm

Reconocimiento de voz. Universidad de las Américas Puebla, México.
http://ict.udlap.mx/people/ingrid/Clases/IS412/index.html

Reconocimiento facial: enfoques predominantes. Ministerio Interior de Argentina.
http://www.biometria.gov.ar/referencia/ref_rf_approaches.php

OLGUÍN S, Patricio. Sensores Biométricos. Revista de la escuela de Electrónica
http://neutron.ing.ucv.ve/revista-e/No6/default.htm

Reconocimiento facial.
http://www.biometria.gov.ar/referencia/ref_rf_approaches.php

http://vismod.media.mit.edu/vismod/demos/facerec/basic.html