
ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA

# "IMPLEMENTACIÓN DE UN SISTEMA DE AUTENTICACIÓN BIOMÉTRICA BASADO EN HUELLAS DIGITALES"

TESIS DE GRADO

Previa la obtención del título de

INGENIERO EN ELECTRÓNICA Y COMPUTACIÓN

Presentado por:

VICTORIA ALEXANDRA HIDALGO JÁCOME

RIOBAMBA - ECUADOR

2010

Agradezco a Dios por haberme dado la salud y la inteligencia para poder terminar con éxitos mis estudios.

A mi familia por su colaboración y apoyo durante mi vida llevándome a la finalización de mis estudios con éxito.

A la ESPOCH por sembrar en mi los conocimientos necesarios para poder desenvolverme en mi vida profesional con un alto nivel.

Al Ing. Hugo Moreno por guiarme en la elaboración de mi proyecto de tesis.

Dedico el presente trabajo de Tesis a una compañera y verdadera amiga, Katty Jácome, por haber estado siempre a mi lado siendo un apoyo incondicional y por hacerme ver la vida de una forma diferente.

| NOMBRE | FIRMA | FECHA |
|---|---|---|
| **Dr. Romeo Rodríguez C.** | _____ | _____ |
| **DECANO FACULTAD** | | |
| **INFORMÁTICA Y ELECTRÓNICA** | | |
| **Ing. Paúl Romero.** | _____ | _____ |
| **DIRECTOR ESCUELA DE** | | |
| **INGENIERÍA ELECTRÓNICA** | | |
| **Y TECNOLOGÍA EN COMPUTACIÓN** | | |
| **Ing. Hugo Moreno.** | _____ | _____ |
| **DIRECTOR DE TESIS** | | |
| **Ing. José Guerra.** | _____ | _____ |
| **MIEMBRO DEL TRIBUNAL** | | |
| **Lic. Carlos Rodríguez** | _____ | _____ |
| **DIRECTOR CENTRO DE DOCUMENTACIÓN** | | |

_____

**NOTA DE LA TESIS**

“Yo, Victoria Alexandra Hidalgo Jácome, soy responsable de las ideas, doctrinas y resultados expuestos en esta tesis; y, el patrimonio intelectual de la Tesis de Grado pertenece a la Escuela Superior Politécnica de Chimborazo”.

Victoria Alexandra Hidalgo Jácome

# Índice de Abreviaturas

| | |
|---|---|
| **ADO:** | Active X Data Objects |
| **AFAS:** | Automatic Fingerprint Authentication System (Sistema Automático de Verificación por Huellas Dactilares) |
| **AFIS:** | Automatic Fingerprint Identification System (Sistema Automático de Identificación por Huellas Dactilares) |
| **ANSI:** | American National Standars Institute (Instituto Americano de Estándares Nacionales) |
| **CE:** | Comunidad Europea |
| **DPI:** | Dots per inch (Número de puntos o píxeles por pulgada) |
| **FAR:** | False Acceptance Rate (Tasa de Falsa Aceptación) |
| **FBI:** | Federal Bureau of Investigation (Agencia Federal de Investigación) |
| **FCC:** | Federal Communications Commission |
| **FRR:** | False Rejection Rate (Tasa de Falso Rechazo) |
| **NIST:** | National Institute of Standars and Technology (Instituto Nacional de Estándares y Tecnología) |
| **ODBC:** | Open DataBase Connectivity (Conectividad Abierta de Bases de Datos) |
| **OLE-DB:** | Object Linking and Embedding for DataBases (Enlace e Incrustación de objetos para bases de datos) |
| **PDA:** | Personal Digital Assistant (Asistente Digital Personal) |
| **PIN:** | Personal Identification Number (Número de Identificación Personal) |
| **PYME:** | Pequeña y Mediana Empresa |
| **ROI:** | Region of Interest (Region de Interés) |
| **RoHS:** | Restriction of Hazardous Substances Directive (Restricción de Sustancias peligrosas) |
| **SQL:** | Structure Query Language (Lenguaje de Consultas Estructurado) |
| **TIFF:** | Tagged Image File Format (Formato de archivo de imágenes con etiqueta) |
| **UL:** | Underwriters Laboratories |
| **WHQL:** | Windows Hardware Quality Labs Testing |

**Índice General**

# Índice de figuras

# Índice de tablas

# Capítulo I

**Marco Referencial**

## 1.1. Introducción

El presente trabajo describe el desarrollo de algoritmos computacionales para el reconocimiento de personas por huellas dactilares utilizando LabVIEW y su módulo para procesamiento de imágenes, y su implementación en una base de datos.

## 1.2. Antecedentes

Desde hace algunos años, los sistemas automáticos de identificación biométrica de personas eran exclusivamente utilizados por instituciones forenses y/o gubernamentales como consecuencia de los enormes costos que involucraba esta tecnología, totalmente cerrada a personas e instituciones civiles. Hoy en día, el enorme crecimiento de la tecnología electrónica, las redes de computadoras y las tecnologías de información y comunicaciones (TICs) ha permitido que la sociedad actual esté caracterizada por la comunicación mutua, globalizada e inmediata de personas naturales, entidades gubernamentales, académicas, bancarias, empresariales, entre otras a través de un sistema de interconexión vulnerable.

Esto ha favorecido a que el fraude producido por falsa identidad esté alcanzando proporciones nunca antes vistas. Por ello, existe un creciente énfasis en el surgimiento de aplicaciones de identificación automática de personas basadas en sus huellas dactilares, puesto que es una de las alternativas más consolidada y fiable en la actualidad.

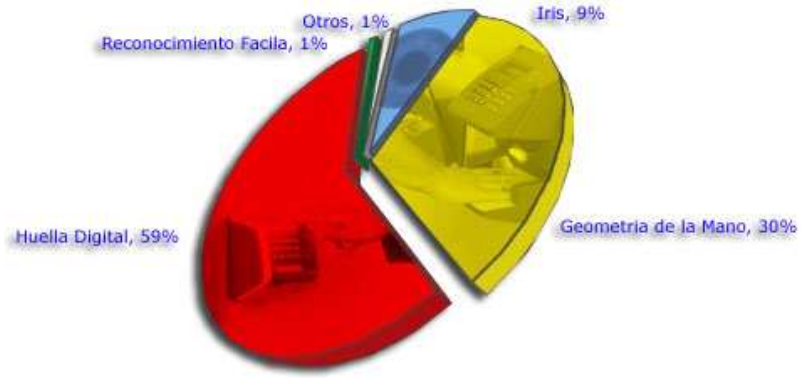



**Figura I.1** Distribución del mercado de dispositivos biométricos

Por lo que se puede concluir que los sistemas biométricos en general, y especialmente los sistemas de reconocimiento automático basado en huellas dactilares, representan una importante área de investigación y desarrollo tecnológico, ya que tiene un amplio campo de aplicación y un mercado potencial creciente en los últimos años, como se indica en la figura I.1.

## 1.3. Justificación

A pesar de que en los países desarrollados se invierten grandes sumas de dinero en investigación a fin de mejorar las técnicas y producir equipos biométricos basados en huellas dactilares a escalas industriales (debido a su alta rentabilidad), en Ecuador la tecnología con la que se cuenta es importada, evitándose así la posibilidad de crear tecnología propia. Indudablemente no es nada sencillo competir con otros sistemas hechos por países desarrollados, pero este tipo de trabajo, aparte de dar la ventaja de ofrecer un aporte al desarrollo tecnológico al país, permite formar investigadores especializados y el poder de capacitar a otros.

Además, existe la concepción errónea de que el reconocimiento automático de personas por huellas dactilares es un problema totalmente resuelto, debido a que ha sido una de las primeras aplicaciones de reconocimiento automático desde hace casi cuarenta años. Por el contrario, las metodologías computacionales requeridas para esta tarea siguen siendo en la actualidad un desafiante e importante problema de reconocimiento de patrones

## 1.4. Objetivos

**OBJETIVOS GENERALES**

- Implementar un sistema de autenticación biométrica basado en huellas digitales

**OBJETIVOS ESPECÍFICOS**

- Investigar las tecnologías sobre autenticación biométrica basada en huellas digitales.
- Estudiar y Analizar los diferentes algoritmos de adquisición y comparación que existen para el estudio biométrico.
- Definir las herramientas a utilizar para el desarrollo de la aplicación.
- Desarrollar el algoritmo para la comparación de las huellas digitales.

## 1.5. Hipótesis

La implementación de un sistema de autenticación biométrica basado en huellas digitales permite identificar personas mediante su algoritmo de comparación y representa una solución confiable y de bajo costo en relación a otros existentes en el mercado.

# Capítulo II

## Sistemas Biométricos

Si se remonta unas décadas atrás y se piensa en la forma en la que se controlaba el acceso a los lugares de máxima seguridad, indudablemente aparece en la mente una visión muy remota de los métodos del pasado. En la época medieval, los pobladores de aquellos exorbitantes castillos rodeados por extensos lagos, controlaban el acceso por medio de fornidos guerreros parados en torres ubicadas arriba de los puentes que hacían las veces de portones de ingresos, dando el visto bueno según una inspección de los datos suministrados por el forastero. Para continuar citando ejemplos recordemos que las más atractivas películas de espionaje, cuando se producía la llegada de una persona a la casa de cualquier detective o a la guardia del malhechor de turno, el invitado, indefectiblemente, tenía que pronunciar una frase en forma de contraseña, la cual era respondida del otro lado con la continuación de ese refrán.

De entonces a hoy, desde la más rudimentaria de las cerraduras mecánicas hasta el más sofisticado sistema electrónico, infinitas son las formas de controlar el ingreso a un establecimiento. Y desde que aparecieron los detectores biométricos la seguridad en el control paso a ser sin dudas uno de los más eficientes.

En el ámbito de las tecnologías de la seguridad, uno de los problemas fundamentales a solventar es la necesidad de autenticar de forma segura la identidad de las personas que pretenden acceder a un determinado servicio o recinto físico. De este modo, surge la biometría,

también conocida como técnicas de identificación biométrica, con el objetivo de resolver este problema a partir de las características propias de cada individuo, como la voz, huella dactilar, rostro, etc.

Estas técnicas de identificación biométrica, frente a otras formas de autenticación personal como el uso de tarjetas PINes o número de identificación personal, como el usado en cajeros automáticos, tiene la ventaja de que los patrones no pueden perderse o ser sustraídos, ni pueden ser usados por otros individuos en el caso de que lleguen a tener accesible nuestra tarjeta personal y/o PIN.

## 2.1. Autentificación biométrica

La palabra biometría deriva de las palabras: bio (vida) y metria (medida). La ciencia biométrica se define como el análisis estadístico de observaciones biológicas.

La biometría, es la aplicación de estos métodos estadísticos y del cálculo al estudio de los seres vivos. La identificación biométrica es entonces, la verificación de la identidad una persona midiendo digitalmente determinados rasgos de alguna característica física, comparando los con los patrones de referencia guardado es un archivo, en una base de datos o algunas veces en una tarjeta inteligente.

Así, un *dispositivo biométrico* es aquel que es capaz de capturar características biológicas de un individuo (rostro, huella dactilar, voz, etc.), comprarlas electrónicamente, contra una población de una o más de tales características y actora según el resultado de la comparación.

Las ventajas fundamentales de este producto es que cualquier método tradicional (control de acceso o asistencia de personal) requieren llaves, códigos, tarjetas de proximidad, tarjetas magnéticas, etc., lo cual implica que pueden ser prestadas, perdidas, robadas o copiadas, limitando notablemente la seguridad del control de accesos de personas. El único medio que no puede ser prestado, ni robado, ni copiado es una parte del cuerpo, que identifica en forma inequívoca a una persona, en este caso las huellas digitales.

## 2.2. Sistema de Identificación Biométrica

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

- *Universalidad:* Cualquier persona posee esa característica.
- *Unicidad:* La existencia de dos personas con una característica idéntica tiene una probabilidad muy pequeña.
- *Permanencia:* La característica no puede cambiar en el tiempo.
- *Cuantificación:* La característica puede ser medida en forma cuantitativa.

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

## 2.3. Características de un sistema biométrico para identificación personal

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

El *desempeño,* que se refiere a la exactitud, la rapidez y la robustez alcanzada en la identificación, además de los recursos invertidos y el efecto de factores ambientales y/u operacionales.

La *aceptabilidad*, que indica el grado en el que la gente está dispuesta a aceptar un sistema biomédico en su vida diaria. Es claro que el sistema no debe representar peligro alguno para los usuarios y debe inspirar "*confianza*" a los mismos.

La *fiabilidad*, que refleja cuán difícil es burlar al sistema. El sistema biométrico debe reconocer características de una persona viva, pues es posible crear dedos de látex, grabaciones digitales de voz, prótesis de ojos, etc.

## 2.4. Arquitectura

Un sistema biométrico se diseña utilizando como base los siguientes cinco módulos

**Módulo de captura**: Permite adquirir el dato biométrico de un individuo.

**Módulo de extracción de características**: El dato adquirido es procesado para extraer la plantilla de entrada o conjunto de características discriminatorias.

**Módulo de coincidencia**: La plantilla de entrada es comparada con la(s) plantilla(s) almacenada(s), generando una puntuación sobre la comparación.

**Módulo de base de datos**: Es usado para almacenar las plantillas de los usuarios registrados o inscritos en el sistema biométrico. Usualmente son almacenadas múltiples plantillas de un individuo para tomar en cuenta las variaciones en la biométrica, donde además éstas pueden ser actualizadas en el tiempo.

**Módulo de toma de decisiones**: La identidad del individuo es declarada o aceptada/rechazada en base a la puntuación de la comparación o comparaciones. Ver figura II.2.

Estos módulos en conjunto realizan dos tareas principales:

**Tarea de Inscripción**: El sistema registra a un nuevo usuario autorizado por el administrador del sistema, almacenando en la base de datos la plantilla de entrada y registrando la identidad del nuevo usuario.

**Tarea de Reconocimiento**: El sistema toma una decisión acerca de la certeza de la identidad de un individuo comparando la plantilla de entrada con la(s) previamente almacenada(s) en la base de datos.

### 2.4.1. Modos de operación

Dependiendo del contexto de la aplicación, la tarea de reconocimiento puede trabajar en los siguientes modos:

**Modo de verificación**. El sistema valida la identidad de un individuo comparando la plantilla de entrada con su plantilla correspondiente previamente almacenada en la base de datos. En este caso el individuo que desea ser reconocido declara una identidad al sistema, usualmente a través de un PIN, un nombre de usuario y luego se realiza una comparación uno a uno para determinar si la identidad declarada es verdadera o no. La verificación de la identidad es típicamente usada para el reconocimiento positivo, en donde el objetivo es impedir que múltiples personas usen la misma identidad.

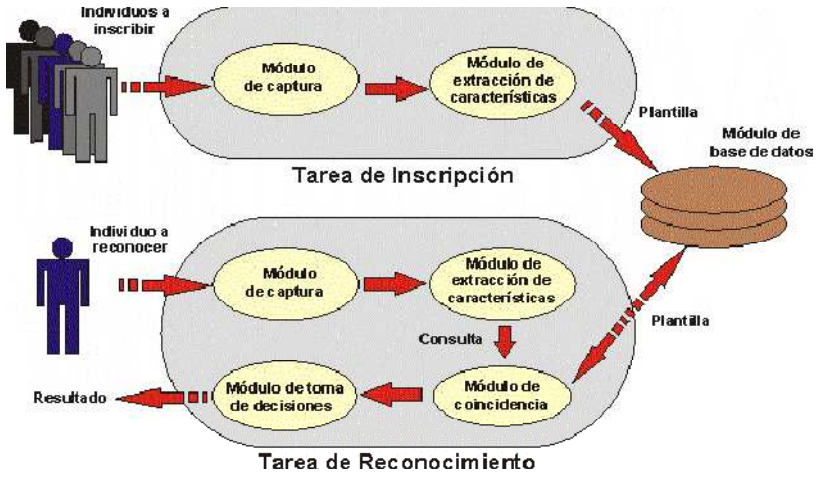



**Figura II.2** Arquitectura de un Sistema de Reconocimiento Biométrico.

**Modo de identificación**. El sistema identifica a un individuo comparando la plantilla de entrada con las plantillas de todos los usuarios registrados en la base de datos, es decir se realiza una comparación uno a muchos para establecer la identidad del individuo sin que ésta sea declarada. La identificación es un componente crítico en aplicaciones de reconocimiento negativo en donde el sistema establece si la persona es quien explícita o implícitamente niega ser. El propósito del reconocimiento negativo es impedir que una sola persona use múltiples identidades. La identificación también puede ser usada para el reconocimiento positivo en donde el usuario no requiere declarar una identidad.

Los diagramas de bloques de un sistema de verificación e identificación son mostrados en las figuras II.3 y II.4.

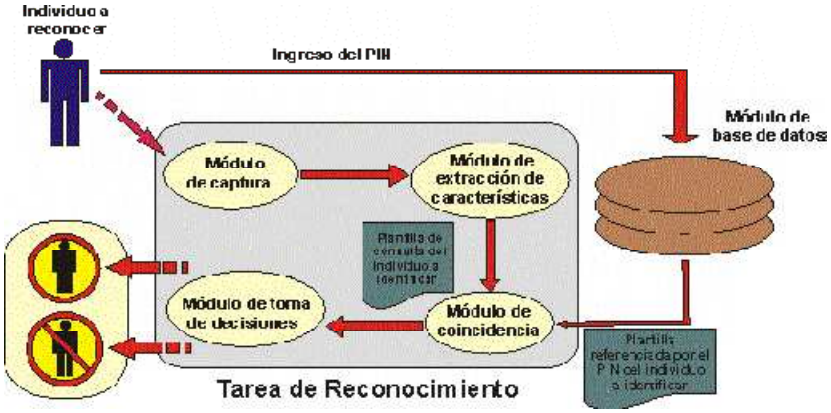



**Figura II.3** Tarea de reconocimiento en el modo verificación

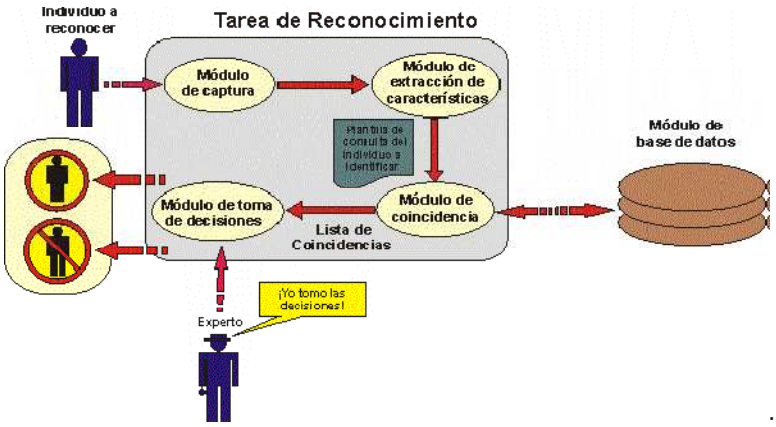



**Figura II.4** Tarea de reconocimiento en el modo identificación.

## 2.5. Sistemas biométricos basados en las huellas dactilares

Son sistemas que fundamentan sus decisiones de reconocimiento tomando como característica personal a la huella dactilar. De acuerdo con el modo de operación en que trabajen, éstos son conocidos en la literatura como:

- AFIS
- AFAS

Tradicionalmente la verificación e identificación por huellas dactilares es realizada manualmente por un experto, sin embargo es una tarea tediosa, lenta y costosa que no presenta los requerimientos de desempeño necesarios para las aplicaciones actuales. Como

consecuencia los AFIS tienen una gran demanda en el mercado, sin embargo la tecnología aplicada a estos sistemas sigue estando aún en desarrollo pues todavía existen algunos problemas por resolver.

Sin embargo las principales etapas consideradas en el diseño de un AFAS son:

**Captura y almacenamiento**. Siendo un AFAS básicamente un sistema que trabaja con impresiones dactilares es necesario definir los principales parámetros que las caracterizan, tales como: la resolución, el área, el número de píxeles por pulgada, contraste y distorsión geométrica. También puede considerarse aquí la técnica de compresión a utilizar para el almacenamiento, el formato de archivo, entre otros (ver anexo I).

**Procesamiento y Representación**: Debido al ruido comúnmente presente en las imágenes, producido generalmente por la técnica de adquisición, las características del dispositivo de captura y defectos en la imagen, usualmente es necesario utilizar alguna técnica de procesamiento para el mejoramiento o reconstrucción de la imagen. El objetivo de la representación es determinar un espacio de medidas (características) en el que las imágenes pertenecientes al mismo dedo formen un agrupamiento compacto y las que pertenecen a diferentes dedos ocupen diferentes porciones de este espacio. Una buena representación debería contener información distintiva acerca de la impresión dactilar, además de ser fácilmente extraíble y almacenada de forma compacta para la coincidencia. El proceso de obtener una representación se denomina extracción de características y se realiza en varios niveles posibles: globales y locales.

**Coincidencia**. Consiste en la comparación biunívoca entre dos impresiones dactilares devolviendo su grado de similitud. Es una tarea extremadamente difícil, debido principalmente a la gran variabilidad entre diferentes impresiones de la misma huella producida por: el desplazamiento, rotación, traslape parcial, distorsiones no lineales, presión, condiciones de la piel, el ruido y los errores en la extracción de características. Además las impresiones de diferentes huellas pueden parecer similares, especialmente en términos de su estructura global.

El desarrollo de un sistema biométrico basado en huellas dactilares está íntimamente relacionado con el procesamiento digital de imágenes y la teoría del reconocimiento de patrones. Por procesamiento digital de imágenes se entiende la manipulación de una imagen de entrada, de modo que la salida del proceso sea una nueva imagen. Análogamente, para el reconocimiento de patrones, se presenta a la entrada del proceso un patrón (imagen) obteniéndose como salida una categoría o clase. En el caso de huellas dactilares el objetivo final es la comparación de la plantilla vinculada a la impresión dactilar a ser reconocida con la(s) almacenada(s) en la base de datos.

## 2.6. Exactitud en la identificación: Medidas de desempeño

Una decisión tomada por un sistema biométrico distingue "*personal autorizado*" o "*impostor*". Para cada tipo de decisión, existen dos posibles salidas, verdadero o falso. Por lo tanto existe un total de cuatro posibles respuestas del sistema:

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

Las salidas numero 1 y 3 son correctas, mientras que las numero 2 y 4 no lo son. El grado de confidencia asociado a diferentes decisiones puede ser caracterizado por la distribución estadística del número de personas autorizadas e impostores. En efecto, las estadísticas anteriores se utilizan para establecer dos tasas de errores:

- *Tasa de falsa aceptación* **FAR** que se define como la frecuencia relativa con que un impostor es aceptado como un individuo autorizado.
- *Tasa de falso rechazo* **FRR** definida como la frecuencia relativa contra un individuo autorizado es rechazado como un impostor.

Las **FAR** y la **FRR** son funciones del grado de seguridad deseado. En efecto, usualmente el resultado del proceso de identificaron o verificación será un numero real normalizado en el intervalo [0,1], que indicara el "*grado de parentesco*" o correlación entre la característica biométrica proporcionada por el usuario y la(s) y almacenada(s) en la base de datos. Por otra parte la **FAR** y la **FRR** están íntimamente relacionadas, de hecho son duales una de la otra: una **FRR** pequeña usualmente entrega una **FAR** alta, y viceversa, como muestra la figura II.5. El grado de seguridad deseado se define mediante el umbral de aceptación ***u***, un número real perteneciente al intervalo [0,1] que indica el mínimo grado de parentesco permitido para autorizar el acceso del individuo.

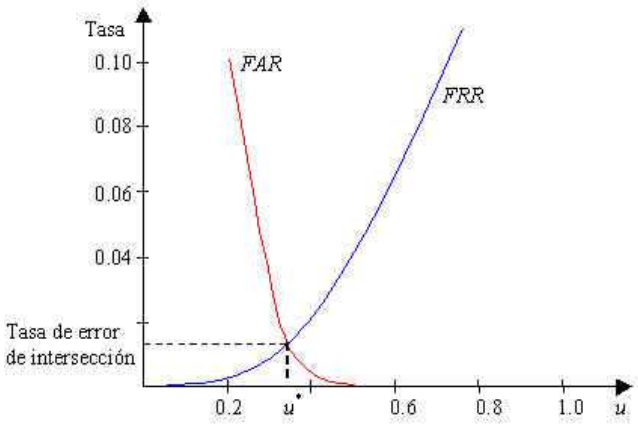



**Figura II.5** Gráfica típica de la tasa de falso rechazo (FRR) y la de falsa aceptación (FAR) como funciones del umbral de aceptación u para un sistema biométrico**.**

La **FRR** es una función estrictamente creciente y la **FAR** es una estrictamente decreciente en ***u.***

## 2.7. Funcionamiento básico de dispositivos biométricos

La figura II.6 muestra el diagrama en bloques de un sistema biométrico general y describe brevemente su funcionamiento.

La mayoría de los sistemas biométricos funcionan de maneras muy similares y se pueden resumir en dos pasos:

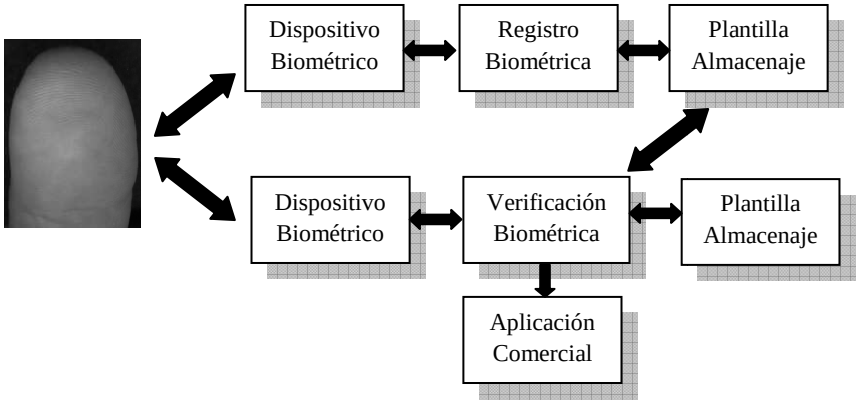



**Figura II.6.** Diagrama de bloques de un sistema Biométrico General

El primer paso consiste en que la persona debe *registrarse* (“enroll”) en el sistema. Durante el proceso de registro, el sistema captura el rasgo característico de la persona, como por ejemplo la huella digital, y lo procesa para crear una representación electrónica llamada *modelo de referencia* (“reference template”). El modelo de referencia debe ser guardado en una base de datos o en algún otro lugar del cual será extraído en cualquier ocasión futura para el segundo paso.

De acuerdo a la teoría tradicional en biometría, el segundo paso depende de si la función del sistema biométrico consiste en verificar la identidad de la persona o identificar a la persona.

En el caso de *verificación,* la persona le informa al sistema cual es su identidad ya sea presentando una tarjeta de identificación o entrando en una clave especial. El sistema captura el rasgo característico de la persona (la huella digital en nuestro ejemplo) y lo procesa para crear una representación electrónica llamada *modelo en vivo* (“live template”). Por último, el sistema compara el modelo en vivo con el modelo de referencia de la persona. Si ambos modelos parean la verificación es exitosa. De no serlos, la verificación es fallida.

En caso del que la función del sistema biométrico sea *identificación,* la persona no le informa al sistema biométrico cual es su identidad. El sistema tan solo captura el rasgo característico de la persona y lo procesa para crear el modelo en vivo. Luego el sistema procede a comparar el modelo en vivo con un conjunto de modelos de referencia para determinar la identidad de la persona.

Dependiendo de la función del sistema, este segundo paso puede ser:

### 2.7.1 Identificación positiva

La función de un sistema de *identificación positiva* consiste en probar que la identidad de la persona es registrada en el sistema. La persona hace una reclamación positiva de identidad al sistema biométrico, es decir, la persona alega que está registrada en el sistema. El sistema responde comparando automáticamente el modelo en vivo con uno o varios modelos de referencia. Si la persona es identificada, el sistema biométrico le concede a la persona ciertos privilegios, de lo contrario los privilegios son negados.

### 2.7.2 Identificación negativa

La función de un sistema de *identificación negativa* consiste en probar que la identidad de la persona no está registrada en el sistema. Un ejemplo puede ser un sistema que verifique que las personas que entran a un banco no se encuentren en una lista de delincuentes. Si la identidad no es registrada, el sistema biométrico le concede ciertos privilegios a la persona como, por ejemplo, permitirle entrar al banco. Si el sistema reconoce a la persona, este le niega ciertos privilegios y hasta quizás alerte si se deben tomar alguna acción más radical como intervenir a la persona.

### 2.7.3 Dispositivos biométricos de uso frecuente

Los sistemas biométricos descubiertos hasta hoy incluyen:

- *Identificación por olor humano:* Los sensores de olor utilizan un procesamiento químico similar al que tiene lugar entre la nariz y el cerebro. Los fabricantes de tarjetas inteligentes están esperanzados en que esta tecnología pueda incluirse en sus chips a fin de competir con los sistemas de reconocimiento dactilar.

- *Identificación por manos o huellas digitales:* Tal vez los más difundidos, estos sistemas utilizan varias técnicas para crear una imagen digital tridimensional la cual es capturada, medida y guardada en un archivo.

- *Identificación por ojo:* Existen dos tipos de sistemas que utilizan al ojo humano como identificador. Tal como se realiza en lo homeopatía los sistemas de identificación por topografía del iris, identifican en muy pocos segundos más de 4000 puntos ubicados en el iris del ojo de una persona. Los fabricantes de estos sistemas, garantizan que el diagrama del iris se establece en el momento de nacer y que, al igual que con las huellas dactilares, no hay dos personas con el mismo patrón. Por otro lado el sistema de identificación por topografía de la retina, lee la superficie del globo ocular mediante una luz infrarroja de baja intensidad midiendo en 320 puntos predefinidos el diagrama de las venas del ojo.

- *Reconocimiento facial:* Verifica las características faciales comparándolas con una imagen de la persona previamente escaneada. Debido a que es muy fácil cambia la apariencia hay varios sistemas en desarrollo que buscan el tiempo de validación con un aumento en la seguridad.

- *Identificación por voz:* Identifica las características únicas de una voz comparándolas con un patrón pregrabado, el sistema interroga a la persona utilizando en forma aleatoria algunas de las preguntas pregrabadas para cada individuo. Las respuestas a ellas son comparadas con las que están archivadas validando así el ingreso.

- *Identificación por firma:* Mide el tiempo y la presión utilizadas para crear una firma.

Los escáneres de huellas digitales y equipos de medición de geometría de la mano son los dispositivos mas corrientemente utilizados. Independiente de la técnica que se utilice, el método de operación es siempre la verificación de la identidad de la persona para una comparación de las medidas de determinado atributo físico.

# Capítulo III

## Huellas dactilares

Las huellas dactilares son patrones constituidos por las crestas papilares de los dedos de las manos, se localizan en la dermis y se reproducen en la epidermis (ver figura III.7.a), generando configuraciones diversas. Se forman en el período fetal, a partir del sexto mes, manteniéndose invariables a través de la vida del individuo, a menos que sufran alteraciones debido a accidentes tales como cortes o quemaduras. Las impresiones dactilares son las reproducciones resultantes de las huellas sobre una superficie plana, quedando almacenada en formato analógico (papel) o digital (archivo), en éstas las crestas papilares se aprecian como las líneas más oscuras y los surcos o valles inter-papilares como las líneas más claras (ver figura III.7.b).

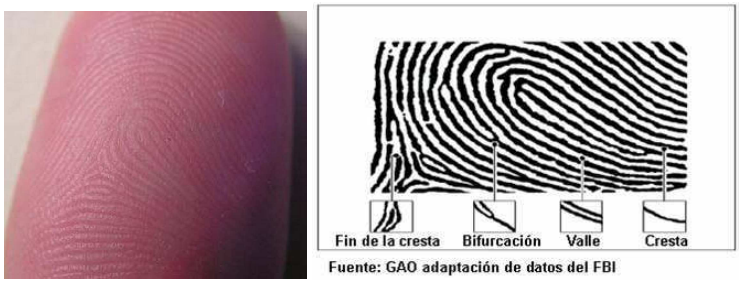



**Figura III.7 (**a) Huella dactilar; (b) impresión dactilar.

## 3.1. Características globales

Son los tipos de patrones geométricos de las crestas que son reconocibles a simple vista, usualmente la determinación del patrón al que pertenece la huella dactilar se obtiene mediante el conocimiento de sus puntos singulares. Es necesario por lo tanto explicar dos conceptos relacionados.

**Área Patrón**: Es la parte principal de la huella dactilar y está constituida por las crestas y todas sus características.

**Líneas Tipo**: Son definidas como dos crestas que se inician paralelamente y divergen sobre el área patrón. Estas crestas pueden ser continuas o no, en caso de que ocurra alguna ruptura (ver figura III.8).

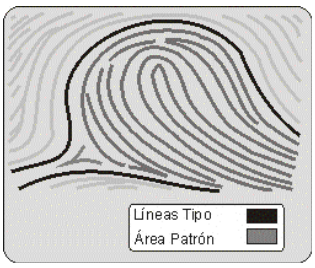



**Figura III.8** Área Patrón y Líneas Tipo.

### 3.1.1. Puntos singulares

**Punto *Core***: Está localizado dentro del Área Patrón en donde las crestas presentan una mayor curvatura. Debido a la gran variación en las configuraciones de las crestas (ver figura III.9.a), las técnicas para su determinación automática son muy complejas.

**Punto *Delta***: Es el punto de divergencia de las Líneas Tipo más internas que tienden a envolver el Área Patrón. Un *Delta* es un triángulo constituido por las crestas papilares que pueden formarse de dos maneras: por la bifurcación de una línea simple o por la brusca divergencia de dos líneas paralelas (ver figura III.9.b).

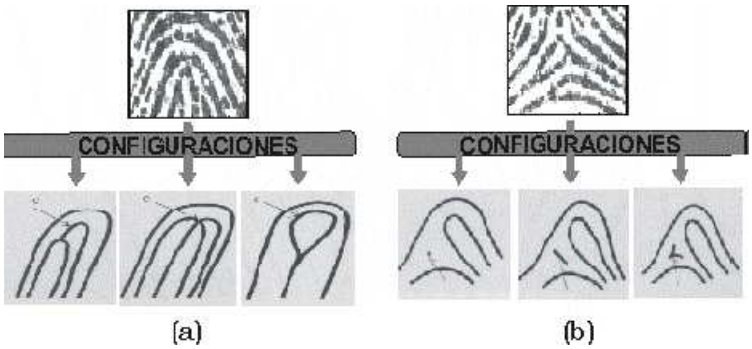



**Figura III.9** Puntos singulares (a) configuraciones del punto *Core*; (b) configuraciones del punto *Delta*.

Las primeras dificultades en el proceso de comparación de las minucias son:

1. En una imagen de calidad hay alrededor de 70 a 80 minucias en promedio, cantidad que contrasta abiertamente con las presentes en una imagen latente o parcial cuyo valor promedio es del orden de 20 a 30.

2. Hay traslaciones, rotaciones y deformaciones no lineales de las imágenes que se heredan a las minucias.

3. Aparecen minucias espurias mientras otra verídicas desaparecen.

4. La base de datos puede ser muy grande.

5. No existe un método de comparación que entregue una coincidencia exacta entre las características de la imagen de entrada y las pertenecientes a la base de datos.

Cada persona en el mundo tiene su propia forma de huellas digitales, estas son diferentes a las de cualquier otra persona que jamás haya existido. Pero aunque cada uno tiene huellas digitales únicas, hay patrones básicos que siempre se encuentran. Estos patrones ayudan a los criminalistas a clasificar las huellas digitales.

Es posible identificar el tipo de huella que cada uno tiene, ya que las huellas dactilares de todas las personas se pueden clasificar en cuatro tipos: lazo, compuesta, arco y espiral, que se pueden observar en la figura III.10.

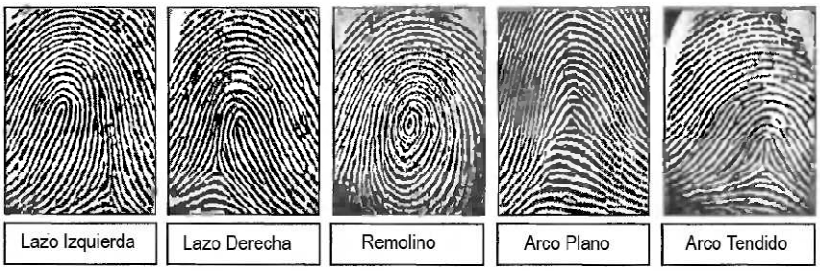



**Figura III.10** Tipos de huellas Dactilares

### 3.1.2 Características locales

Las características locales establecen la individualidad de la huella dactilar y están representadas por los puntos conocidos como minucias. Es posible que dos o más individuos tengan huellas dactilares con idénticas características globales, pero seguirán siendo distintas y únicas debido a que poseen diferentes características locales, es decir éstos son elementos distintivos que caracterizan a una huella dactilar como un objeto único.

Las crestas en una huella dactilar no son continuas ni rectas, sino más bien cambian de dirección, cortándose y bifurcándose. Los puntos en donde los cambios ocurren son denominados minucias. En una imagen de alta calidad es común encontrar entre setenta y cien minucias, las cuales proveen la suficiente información para determinar la individualidad de una huella dactilar. Los tipos de minucias son (ver figura III.11):

1. **Laguna** (*Enclosure*): Es una cresta que se divide en dos ramas y se unifica otra vez luego de recorrer una distancia corta creando un área cerrada.
2. **Isla** (*Dot*). Es una cresta muy pequeña, a tal grado que es semejante a un punto.
3. **Cresta Independiente** (*Short ridge*): Es una cresta muy corta pero lo suficientemente grande para no ser una isla.

4. **Aguijón** (*Spur*): Es una cresta que se divide en dos ramas y una de éstas recorre una distancia muy corta finalizando.
5. **Finalización** (*Ending*): Es el punto en donde una cresta termina abruptamente.
6. **Bifurcación** (*Bifurcation*): Es el punto en donde una cresta se divide en dos ramas.
7. **Trifurcación** (*Crossover*): Es producida por la unión de dos minucias de bifurcación.

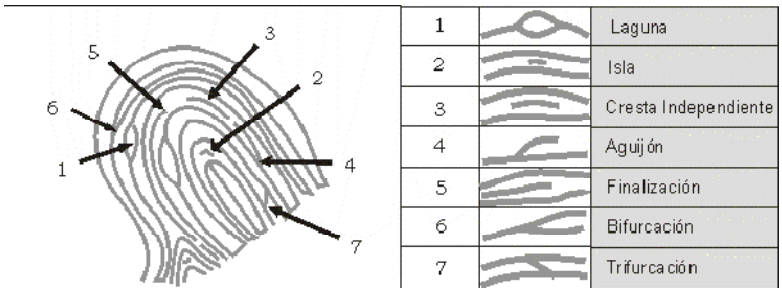



**Figura III.11** Tipos de minucias.

## 3.2. Reconocimiento de Huellas Dactilares

Existen dos técnicas para realizar la verificación de las huellas:

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

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

## 3.3. Modelo del proceso de identificación personal

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

- *Conocimiento:* la persona tiene conocimiento (por ejemplo: un código),
- *Posesión:* la persona posee un objeto (por ejemplo: una tarjeta), y
- *Característica:* la persona tiene una característica que puede ser verificada (por ejemplo: una de sus huellas dactilares.)

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

Uno de los patrones biométricos de huella dactilar más utilizados en los sistemas actuales, por su elevada fiabilidad, es aquel formado por el conjunto de puntos que informan sobre la ubicación de las llamadas *minucias* de la imagen. Recibe el nombre de minucia cualquier punto de la imagen que indica que una determinada cresta presenta un final, un comienzo o una bifurcación. Una minucia estará determinada, por tanto, por sus coordenadas espaciales dentro de la imagen. Generalmente, los patrones biométricos de huella dactilar están constituidos por las coordenadas espaciales de cada minucia.

En la figura III.12 se muestra el diagrama de bloque del sistema AFAS que es el que va a ser utilizado. En el pueden apreciarse las diferentes fases necesarias para la verificación de la identidad de una persona, en base a las características de la huella dactilar de entrada.

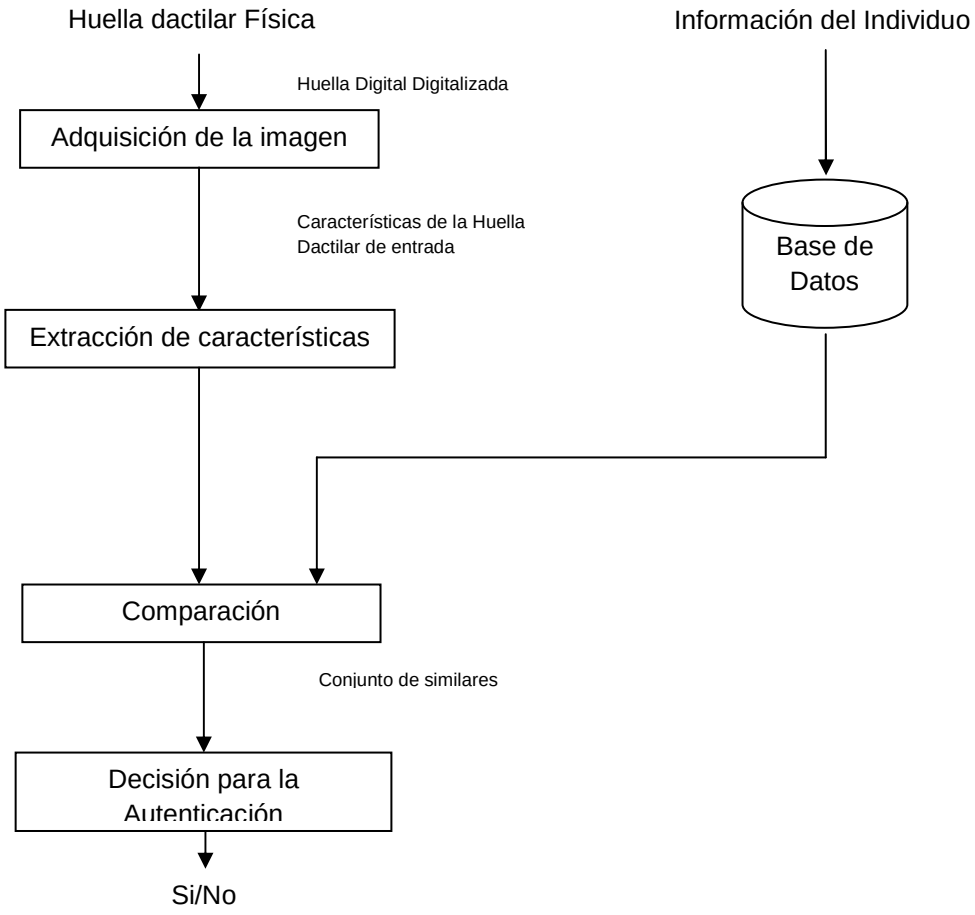



**Figura III.12** Diagrama de bloques sistema AFAS

## 3.4. Extracción de las características locales

Las características locales de mayor importancia son las minucias pues son ampliamente usadas en la etapa de coincidencia, éstas forman una representación compacta que captura un componente significativo de información individual. Comparado a otras características, las minucias son relativamente más robustas ante las variadas fuentes de degradación de las impresiones dactilares. La mayoría de los tipos de minucias no son estables y no pueden ser identificados confiablemente por técnicas automáticas de procesamiento de imágenes. Por consiguiente, para la coincidencia de impresiones dactilares en forma automática sólo los dos más prominentes tipos de minucias son usados debido a su estabilidad y robustez: las minucias de finalización y bifurcación. La representación de una impresión dactilar según el estándar ANSI-NIST está basada en las minucias de finalización y bifurcación (ver figura III.14)

incluyendo su localización y dirección. Para el proceso de extracción de minucias se analiza cada píxel de la imagen y se analiza sus vecinos. Ver figura III.13.

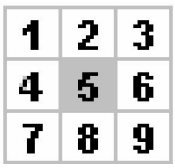



**Figura III.13** Vecinos de un pixel

Es decir que a cada píxel (número 5) le corresponden vecinos (números 1, 2, 3, 4, 6, 7,8 y 9) en los cuales se buscaran patrones para saber si existe una minucia en dicho punto.

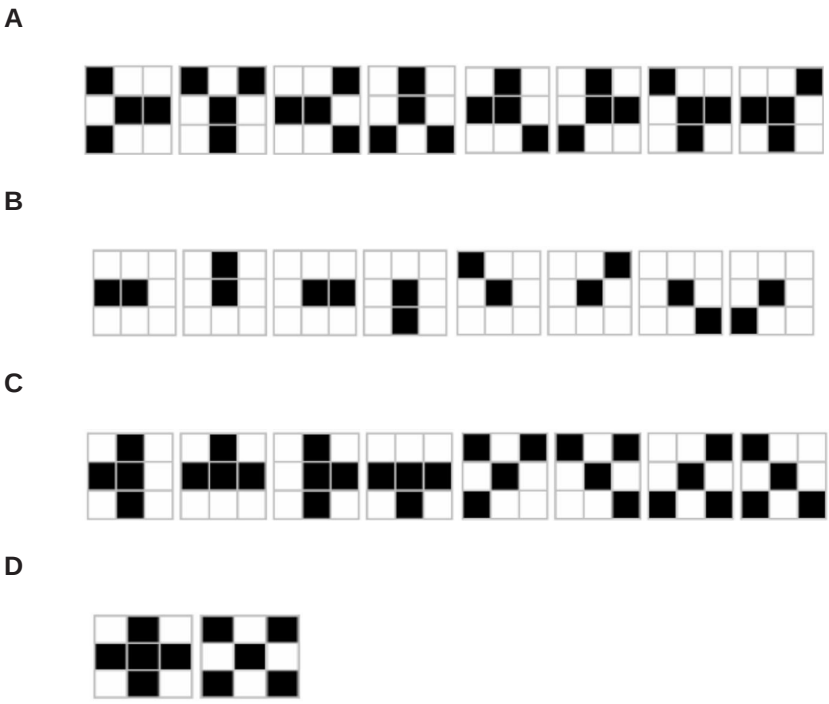



**Figura III.14** Patrones a encontrar en los vecinos de un pixel

## 3.5. Aplicaciones

Pueden ser divididas principalmente en los siguientes grupos (ver figura III.15):

**Comerciales**: Tales como el acceso a redes de computadoras, seguridad de datos electrónicos, comercio electrónico, acceso a Internet, redes ATM, tarjetas de crédito, control de acceso físico, teléfonos celulares, PDA, mantenimiento de registros médicos y aprendizaje a distancia.

**Gubernamentales**: Tales como documentos de identidad nacional, licencias de conducir, seguridad social, control en fronteras y del pasaporte.

**Forenses**: Identificación de cadáveres, investigaciones criminales, identificación de terroristas, de niños y ancianos extraviados, entre otras.

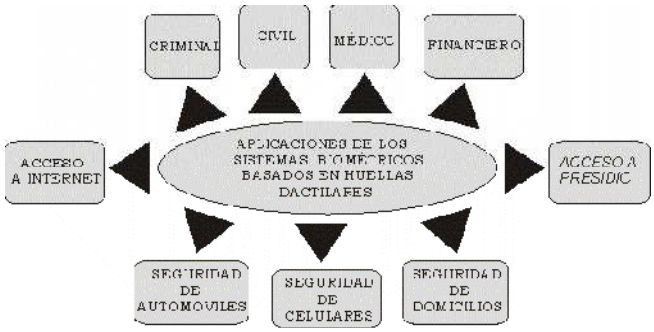



**Figura III.15** Aplicaciones de los sistemas biométricos basados en huellas dactilares.

# Capítulo IV

## Procesamiento Digital de Imágenes

Una imagen puede ser definida matemáticamente como una función bidimensional, *f(x, y),* donde *x* y *y* son coordenadas espaciales (en un plano), y la amplitud de *f* en cualquier par de coordenadas (*x, y)* es la *Intensidad* o *nivel de gris* de la imagen en esa coordenada.

Cuando x, y, y los valores de la amplitud de f son cantidades finitas, se dice que la imagen es una *Imagen Digital*. Una imagen digital está compuesta de un número finito de elementos, cada uno con un lugar y valor específicos. Estos elementos se denominan como *picture elements*, *pels* o *pixels.*

El *Pixel* es el término más ampliamente utilizado y denota los elementos de una imagen digital.

## 4.1. Niveles de Procesamiento

Existen tres tipos de procesamiento computarizado.

- **Procesos de Bajo Nivel:** Involucra operaciones primitivas tales como: el pre procesamiento de imágenes para reducir el ruido, realce de contraste y filtros de enfoque. Un proceso de bajo nivel está caracterizado por el factor de que ambos (estas son entradas y salidas) son imágenes.

- **Procesos de Nivel medio:** Involucra tareas tales como: segmentación (dividir una imagen en regiones u objetos), descripción de los objetos reduciéndolos a una forma adecuada para el procesamiento en la computadora, y clasificación de objetos individuales. Un procesamiento de nivel medio se caracteriza por el factor de que las entradas generalmente son imágenes, pero las salidas son atributos extraídos de estas imágenes (Por ejemplo: bordes, contornos, y la identidad de objetos individuales).

- **Procesos de Alto nivel**: Implica el obtener algún significado de un conjunto de objetos reconocidos – análisis de imágenes – y, finalmente, realizar las funciones cognitivas asociadas con la vista. (ejemplo de símbolos de tráfico)

## 4.2. Pasos fundamentales en el Procesamiento de una Imagen Digital

- **Adquisición de la Imagen.**

  El tipo de imágenes en los que se tiene interés se generan por la combinación de una fuente de Iluminación y la reflexión y/o refracción de energía desde esa fuente o los elementos que conforman la escena.

- **Mejoramiento de la Imagen**

  Esta entre las más simples y área más simpática del procesamiento digital de la imagen. Básicamente, la idea detrás de las técnicas de mejoramiento es la de realzar detalles que están obscurecidos, o simplemente resaltar ciertas zonas de interés de una imagen. Un ejemplo familiar de mejoramiento es cuando incrementamos el contraste de una imagen porque “se ve mucho mejor”. Esto es importante guardar en mente que el mejoramiento es un área muy subjetiva del procesamiento de la imagen.

- **Restauración de la Imagen**

  Es un área que también trata con el mejoramiento de la apariencia de una imagen. Sin embargo, a diferencia del mejoramiento, el cual es subjetivo, la restauración de la

imagen es objetiva, en el sentido de que las técnicas de restauración tienden o se basan en modelos matemáticos o probabilísticos de la degradación de la imagen.

- **Procesamiento del color de la Imagen**

  Esta es un área que ha venido ganando importancia por el incremento significativo en el uso de imágenes digitales en el Internet.

- **Compresión**

  Reduce el almacenamiento requerido para guardar una imagen, o el ancho de banda para transmitirla

- **Procesamiento Morfológico**

  Herramientas para extraer componentes de la imagen útiles para la representación y descripción de formas.

- **Segmentación**

  Divide una imagen en sus partes constituyentes

- **Representación y descripción.**

  Se toman decisiones tales como si la forma obtenida debe ser tratada como un frontera o una región, y extrae atributos que resultan en información cuantitativa de interés.

### 4.2.1. Adquisición de imágenes

En la figura IV.16 se muestra los 3 principales arreglos de sensores utilizados para transformar energía luminosa en imágenes digitales.

El proceso en todos ellos es simple: La energía entrante se transforma a un voltaje por la combinación de electricidad de entrada y el material del sensor, sensible al tipo de energía que se quiere detectar. La onda de voltaje de salida es la respuesta del sensor, y una cantidad digital se obtiene de cada sensor digitalizando su respuesta.

#### 4.2.1.1. Resolución espacial y resolución en niveles de gris

El muestreo es el factor principal para determinar la resolución espacial de una imagen. Básicamente, la resolución espacial es el grado de detalle discernible en una imagen.

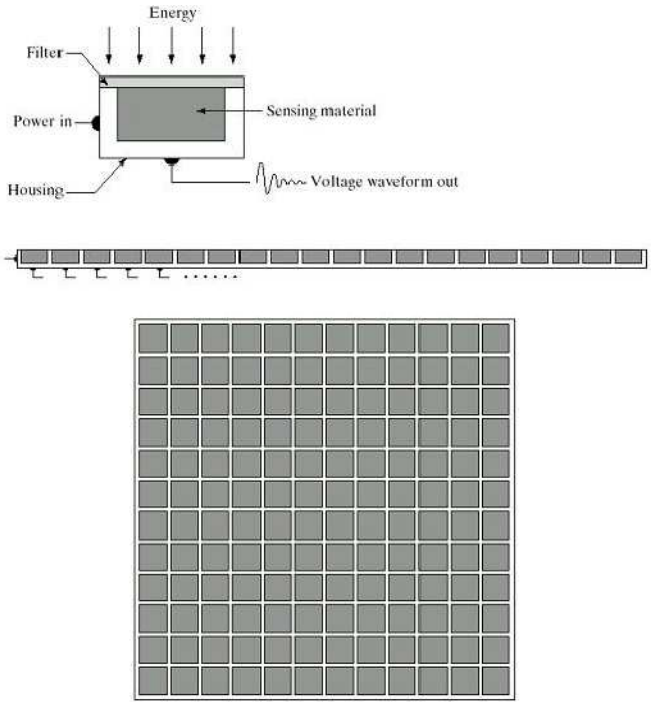



**Figura IV.16.** Tipos de sensores: sencillo, en línea y en arreglo

La potencia de 2 que determina el número de niveles de gris es usualmente 8 bits, es decir, 256 diferentes niveles de gris. Algunas aplicaciones especializadas utilizan 16 bits.

Usualmente se dice que una imagen digital de tamaño M x N con L niveles de gris tiene una resolución espacial de M x N pixeles y una resolución de nivel de gris de L niveles. Ver figura IV.17

#### 4.2.1.2. Relaciones entre Pixeles

Cuando se habla de píxeles conectados entre sí, es necesario precisar el tipo de conexión o conectividad que se acepta como válida.

En principio, un píxel de una malla rectangular[1] puede estar conectado con los ocho píxeles que le rodean en un espacio plano o solamente con los cuatro más cercanos.

[1] Se pueden utilizar otras formas, como un círculo. Los cuadrados y rectángulos son las formas más usuales

Ello dará lugar a hablar de una conexión de tipo 8 o de tipo 4. Ver figura IV.18 e IV.19.

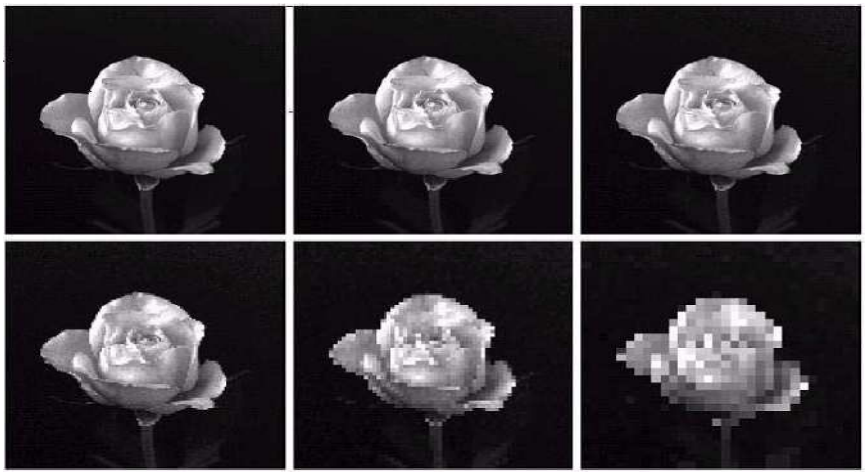


**Figura IV.17** Imagen de 1024x1024 original y sus sub muestreos (ampliados al tamaño de la primera) de 512x512, 256x256, 128x128, 64x64 y 32x32

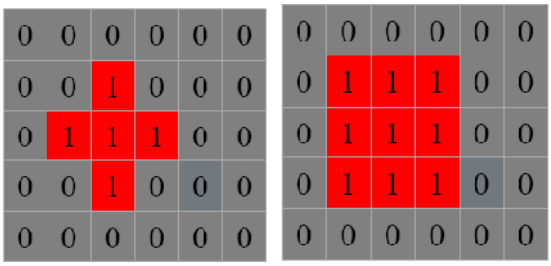



**Figura IV.18**. a) Conectividad tipo 4, b) Conectividad tipo 8

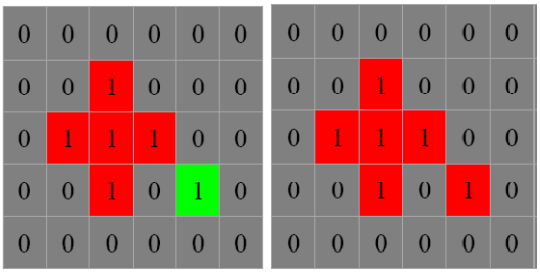



**Figura IV.19.** a) Conectividad 4: Dos objetos, b) Conectividad 8: Un solo objeto

### 4.2.2. Mejoramiento de la Imagen

El principal objetivo de la mejora es procesar una imagen para que el resultado sea más conveniente que la imagen original para una aplicación específica.

Un método conveniente para mejorar radiografías no necesariamente será el mejor para mejorar fotografías de Marte transmitidas desde el espacio.

La mejora de la imagen se divide en dos categorías: métodos del dominio espacial y métodos del dominio de la frecuencia. Los métodos del dominio espacial trabajan sobre el plano de la imagen, y en éste se manipulan directamente los pixeles de una imagen. En los métodos del dominio de la frecuencia se modifica la transformada de Fourier de una imagen. Existen técnicas que se basan en combinaciones de métodos de ambas categorías.

No hay una teoría general de mejora de la imagen. Cuando la imagen se procesa para interpretación visual, el observador es el que juzga qué tan bueno es un método: la evaluación visual de una imagen es un proceso altamente subjetivo. Cuando la imagen se procesa para ser percibida por una máquina, la evaluación es más fácil: el mejor procesamiento de la imagen es aquél que provoca un mejor reconocimiento por parte de la máquina.

#### 4.2.2.1. Procesamiento del Histograma

Los histogramas son la base de muchas técnicas de procesamiento de la imagen en el dominio espacial. En la figura IV.20 se observan 4 ejemplos de histogramas para 4 imágenes: oscura, clara, con bajo contraste y alto contraste. El eje horizontal de los histogramas es el valor de los niveles de gris, rk y el eje vertical corresponde a los valores de h (rk) = nk o p(rk) = nk /n si los valores están normalizados.

La figura IV.20 muestra la distribución del histograma de acuerdo a las características de las imágenes.

#### 4.2.2.2. Ecualización del histograma

Intuitivamente, es razonable concluir que una imagen cuyos pixeles tienden a ocupar el rango entero de posibles valores de gris y, además, tiende a estar uniformemente distribuido, tendrá una apariencia de alto contraste y exhibirá una gran variedad de tonos de gris.

Es posible obtener este histograma y al proceso se le llama ecualización del histograma, ver figura IV.21.

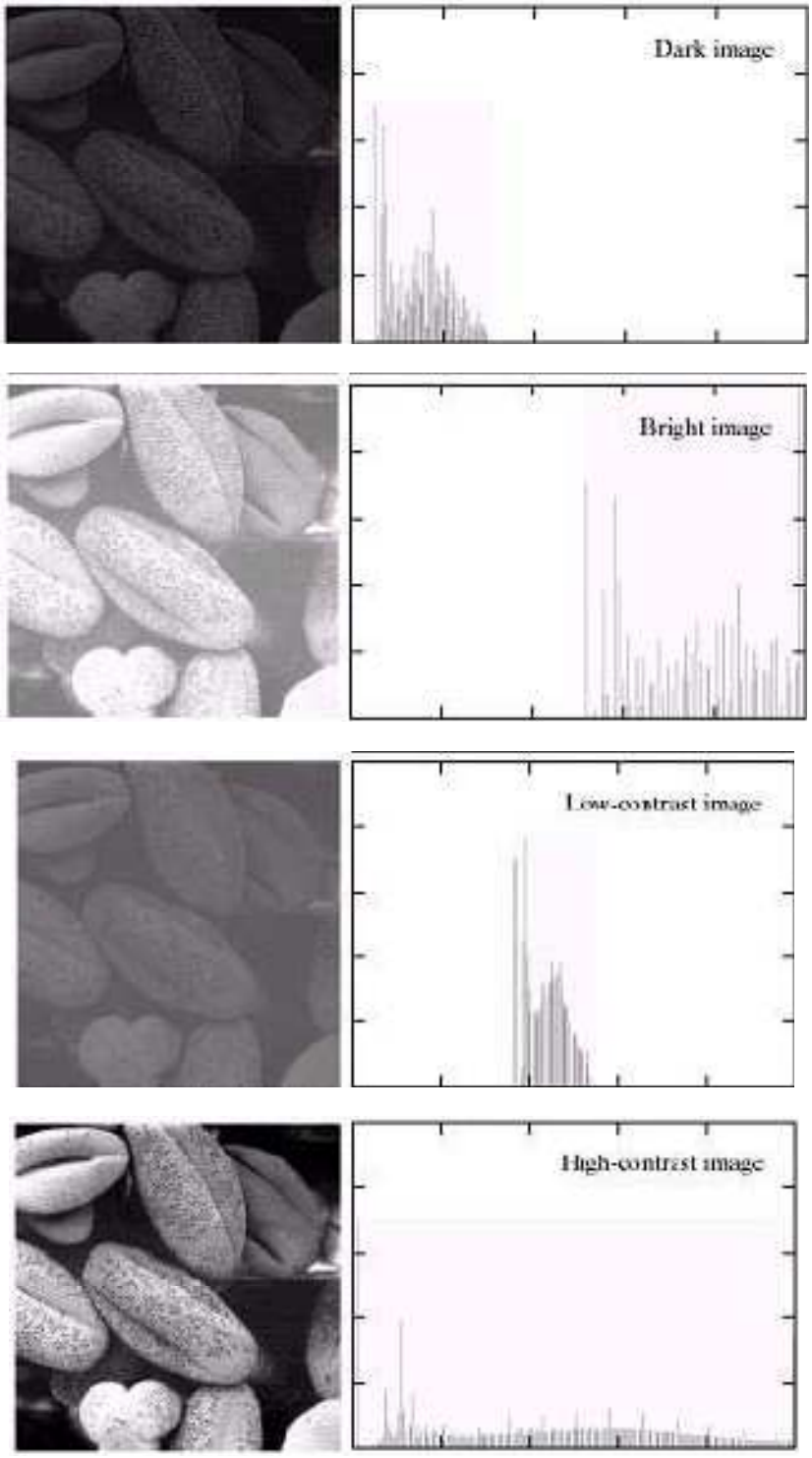



**Figura IV.20.** Cuatro ejemplos de histograma para 4 tipos de imágenes.

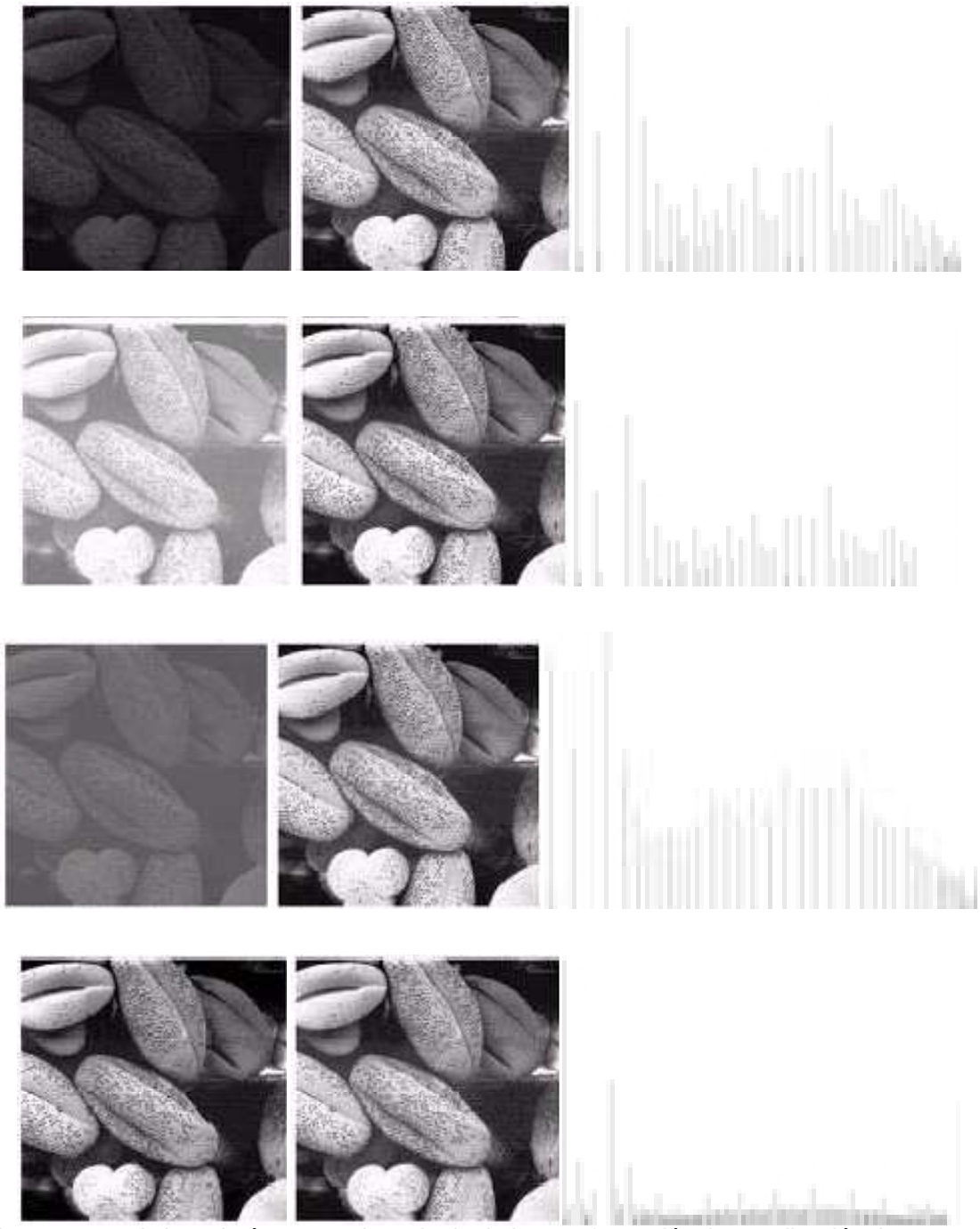


**Figura IV.21** Distintas imágenes y el resultado de la transformación de ecualización de histograma

#### 4.2.2.3. Mejora de la imagen en el dominio de la frecuencia

La idea más importante de este trabajo es que toda función que se repite periódicamente puede ser expresada como la suma de senos y/o cosenos de diferentes frecuencias, cada uno multiplicado por un coeficiente diferente. A esta suma se la llama Serie de Fourier.

Aún funciones que no son periódicas (pero con un área finita bajo la curva) pueden ser expresadas como la integral de senos y/o cosenos multiplicada por una función de ponderación. Esta es la transformada de Fourier, y su utilidad es aún más grande que la de las series de Fourier en muchos problemas prácticos.

Las dos representaciones comparten la importante característica de que una función, expresada en series de Fourier o la transformada, pueden ser reconstruidas (recobradas) completamente por un proceso inverso sin perder información.

Ya que la frecuencia se relaciona directamente con la velocidad de cambio, no es difícil asociar intuitivamente frecuencias de la transformada de Fourier con patrones de variación de intensidad de una imagen.

El componente de frecuencia que varía más lentamente (u = v = 0) corresponde al nivel de gris promedio.

Al alejarnos del origen, las frecuencias bajas corresponden a componentes que varían lentamente.

Lejos del origen, las frecuencias altas corresponden a cambios cada vez más rápidos en el nivel de gris e la imagen (por ejemplo Bordes, o ruido)

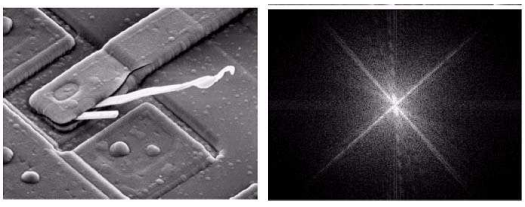


**Figura IV.22** Imagen de un circuito integrado con daño termal inducido y su espectro de Fourier

En la imagen IV.22. se puede ver un circuito integrado dañado (la parte blanca es óxido resultado del daño termal inducido). Varios detalles de la imagen pueden relacionarse con lo que se observa en su espectro de Fourier.

Los bordes prominentes corriendo a 45º y las 2 prominencias blancas de óxido corresponden a los componentes del espectro con direcciones de 45º y, a la izquierda del eje vertical un componente que sale un poco a la izquierda.

El filtrado en el dominio de la frecuencia consiste en los siguientes pasos:

**1.** Multiplicar la imagen de entrada por (-1)x+y para centrar la transformada.

**2.** Calcular F(u, v), la DFT de la imagen en el paso 1.

**3.** Multiplicar F(u,v) por una función de filtro H(u,v)

**4.** Calcular la transformada inversa del resultado del paso 3.

**5.** Obtener la parte real del resultado en 4.

**6**. Multiplicar el resultado en 5 por (-1)x+y

H (u,v) es llamado filtro porque suprime ciertas frecuencias de la transformada, pero deja otras sin cambio.

La transformada de Fourier de la imagen de salida es entonces dada por la siguiente ecuación:

$$G(u,v) = H(u,v)F(u,v)$$

La multiplicación de H y F se hace entre funciones bidimensionales y está definida elemento por elemento. Esto es, el primer elemento de H se multiplica por el primer elemento de F, y así[2].

La imagen filtrada se obtiene tomando la parte real de este resultado y multiplicando por (-1)x+y. La transformada inversa es en general, compleja, sin embargo, si la imagen de entrada y la función de filtro son reales, los componentes imaginarios de la transformada inversa deberían ser cero[3]. Ver figura IV.23.

[2] En general, los componentes de F son cantidades complejas. En este caso, cada componente de H multiplica los valores real e imaginario de la componente correspondiente en F. Estos filtros son llamados filtros de cambio de fase cero porque no alteran la fase de la transformada.

[3] En la práctica, la DFT inversa generalmente tiene componentes imaginarios parásitos por redondeo computacional. Ignoraremos estos componentes

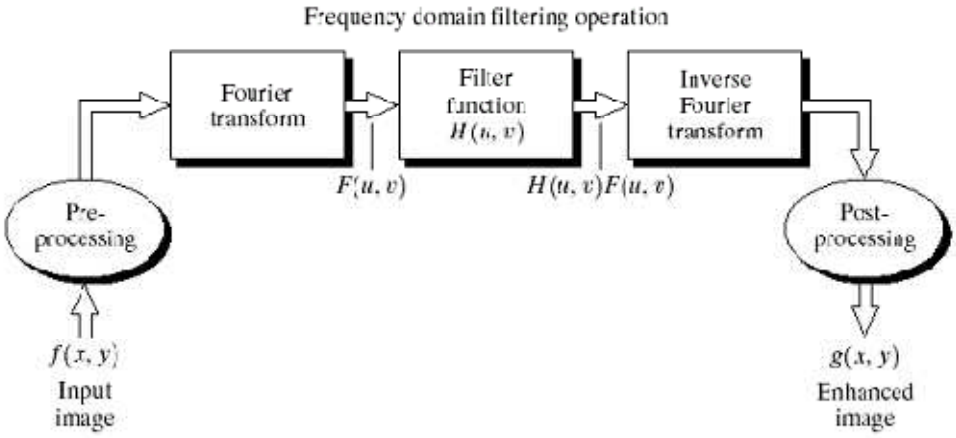



**Figura IV.23** Pasos básicos del filtrado

#### 4.2.2.4. Filtros de Afinamiento

El objetivo principal de los “sharpening filters” es resaltar detalles finos de una imagen y/o mejorar los detalles que han sido desdibujados.

**Fundamentos**

La derivada de una función digital se define en términos de diferencias.

***Condiciones a cumplir***

- Primera Derivada:

Igual a cero en segmentos planos (nivel de gris constante)

Diferente de cero al inicio de un nivel de gris rampa o escalón

Diferente de cero a lo largo de las rampas

Definición básica de una derivada de primer orden:

$$\frac{\partial f}{\partial x} = f(x+1) - f(x)$$

- Segunda Derivada:

Igual a cero en segmentos planos (nivel de gris constante)

Diferente de cero al inicio de un nivel de gris rampa o escalón

Igual a cero a lo largo de las rampas

Definición básica de una derivada de segundo orden:

$$\frac{\partial f}{\partial x} = f(x+1) + f(x-1) - 2f(x)$$

**4.2.2.5. Uso de derivadas de segundo orden para mejoramiento (El Laplaciano)**

Se pretende definir una formulación discreta y construir la máscara respectiva para esa formulación.

Se pondrá interés en filtros isotrópicos cuya respuesta es independiente de la dirección en la que se aplica el filtro que es Invariante a la rotación.

El filtro isotrópico más conocido y sencillo es el Laplaciano (Figura IV.24) cuya formulación para una imagen f(x, y) es la siguiente:

$$\nabla^2 f = \frac{\partial^2 f}{\partial x^2} + \frac{\partial^2 f}{\partial y^2}$$

Por definición el Laplaciano se representa por:

| | | | | | |
|---|---|---|---|---|---|
| 0 | −1 | 0 | −1 | −1 | −1 |
| −1 | 4 | −1 | −1 | 8 | −1 |
| 0 | −1 | 0 | −1 | −1 | −1 |

**Figura IV.24** Mascaras de filtros

En virtud de que el Laplaciano mejora los niveles de gris como se muestra en la figura IV.25 de las discontinuidades y por ende discrimina niveles de gris con poca variación (background), como resultado se producirán imágenes con detalles resaltados con nivel de gris medio súper-impuesto en un fondo las características originales de la imagen.

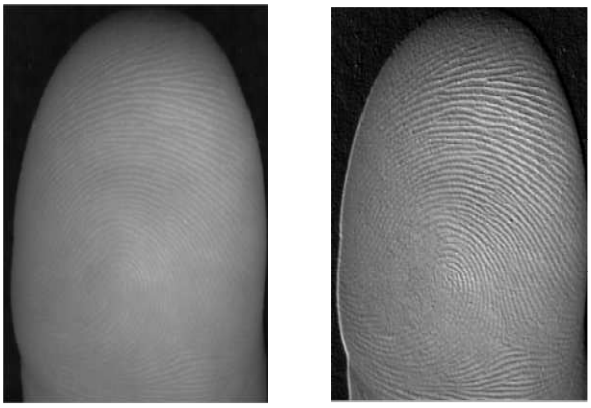


**Figura IV.25.** a) Imagen de entrada, b) el Laplaciano de la imagen

### 4.2.3. Restauración de la Imagen

Al igual que el mejoramiento de imágenes el objetivo de la restauración de imágenes es Optimizar las Imágenes de alguna forma.

- Mejoramiento: Proceso Subjetivo
- Restauración: Proceso Objetivo

La Restauración intenta recuperar o reconstruir una imagen que ha sido degradada, para lo cual requiere un conocimiento a "**priori**" de la degradación.

Las técnicas de restauración están orientadas a la modelación de la degradación, para luego aplicar el proceso inverso.

Las principales fuentes de ruido en una imagen digital se presentan durante la adquisición y transmisión de la imagen.

La descripción espacial del ruido tiene que ver con el comportamiento estadístico del mismo, para los diferentes niveles de gris de la imagen.

Cuando se refiere al contenido de frecuencia del ruido, se hace referencia al contenido espectral luego de aplicar la FFT a la imagen.

Cuando el ruido es constante, típicamente se lo llama Ruido Blanco.

- ***Ruido Gausiano***

El ruido gaussiano produce pequeñas variaciones en la imagen. Tiene su origen en diferencias de ganancias del sensor, ruido en la digitalización, etc.

$$p(z)=\frac{1}{\sqrt{2\pi\sigma}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

- ***Ruido Rayleigh***

El ruido Rayleigh está dado por

$$p(z)=\begin{cases}\frac{2}{b}(z-a)e^{\frac{(z-a)^2}{b}} & para\ z\geq a\\ 0 & para\ z<a\end{cases}$$

Donde la media y la varianza de la densidad están dadas por

$$\mu=a+\sqrt{\frac{\pi b}{4}}\qquad \sigma^2=\frac{b(4-\pi)}{4}$$

- ***Ruido Erlag (Gamma)***

El ruido Erlang está dado por

$$p(z)=\begin{cases}\frac{a^b z^{b-1}}{(b-1)!}e^{-az} & para\ z\geq a\\ 0 & para\ z<a\end{cases}$$

$$\mu=\frac{b}{a}\qquad \sigma^2=\frac{b}{a^2}$$

Donde los parámetros son que a>0, b es un entero positivo y "!" significa factorial. También se lo conoce como Densidad Gamma

- ***Ruido exponencial***

Este es un caso especial del ruido Erlang, con b=1.

$$p(z)=\begin{cases}ae^{-az} & para\ z\geq 0\\ 0 & para\ z<a\end{cases}$$

$$\mu=\frac{1}{a}\qquad \sigma^2=\frac{1}{a^2}$$

- ***Ruido uniforme***

Las amplitudes de la muestra en el dominio del tiempo son uniformes sin especificar niveles máximos o mínimos. En otras palabras, todos los valores de amplitud en algunos límites son iguales.

$$p(z)=\begin{cases}\dfrac{1}{b-a} & si\ a\le z\le b\\ 0 & cualquier\ otro\ caso\end{cases}$$

$$\mu=\frac{a+b}{2} \qquad \sigma^2=\frac{(b-a)^2}{12}$$

- ***Ruido Impulsivo (Sal y Pimienta)***

Ocurrencias aleatorias de pixeles completamente blancos y completamente negros.

$$p(z)=\begin{cases}P_a & para\ z=a\\ P_b & para\ z=b\\ 0 & cualquier\ otro\ caso\end{cases}$$

$$\mu=\frac{1}{a} \qquad \sigma^2=\frac{1}{a^2}$$

Los parámetros típicos de ruido periódico son estimados por inspección del espectro de Fourier de la imagen. El ruido periódico tiende a producir frecuencias que a menudo pueden ser detectadas incluso por análisis visual. Otro enfoque es el intento de interferir periódicamente las componentes del ruido directamente en la imagen, pero esto es posible solamente en casos simples.

### 4.2.4. Procesamiento del color

El color es un poderoso descriptor que simplifica la identificación de objetos y su extracción de una escena. En segundo lugar, el ser humano puede discernir entre miles de tonalidades de color, comparado a cerca de dos docenas de niveles de gris.

El procesamiento del color se divide en 2 áreas: Procesamiento del color y procesamiento del seudo-color. En el primer caso las imágenes se adquieren con un sensor de color como una cámara de televisión o un scanner. En el segundo caso se trata de asignar un color a una intensidad o un rango de intensidades monócromas.

#### 4.2.4.1. Fundamentos del color

Básicamente, los colores que los seres humanos y otros animales perciben en un objeto están determinados por la naturaleza de la luz reflejada desde el objeto. La luz visible (ver figura IV.26) se compone de una delgada banda de frecuencias del espectro electromagnético. Un cuerpo que refleja luz balanceada en todas las longitudes de onda visibles se verá blanco. Sin embargo, un cuerpo que favorezca la reflectancia en un rango limitado del espectro visible mostrará algunos tonos de color.

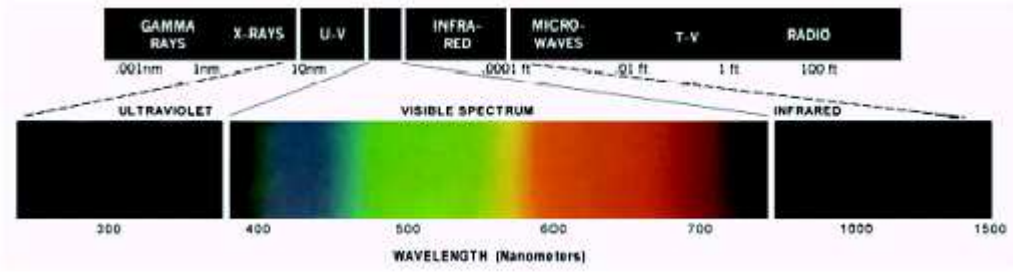



**Figura IV.26** Longitudes de onda del espectro visible

Se utilizan 3 cantidades básicas para describir la calidad de una fuente de luz cromática:

- ***Radiancia***. Es el total de energía proveniente de la fuente de luz, se mide en Watts.
- ***Luminancia***. Es una medida de la cantidad de energía percibida por un observador. Se mide en lúmenes.
- ***Brillo.*** Engloba la noción acromática de intensidad. Es una medida altamente subjetiva.

#### 4.2.4.2. Modelos de color

Un modelo de color es la especificación de un sistema de coordenadas y el sub-espacio dentro de él, donde cada color puede ser representado por un solo punto.

La mayoría de los modelos de color en uso se orientan ya sea al hardware, o a aplicaciones donde la manipulación de color es el objetivo.

Los modelos orientados a hardware más comunes son el RGB (rojo, verde, azul), para monitores a color y cámaras de video; el CMY (cian, magenta, amarillo) y CMYK para impresión a color; y el HSI (tono, saturación, intensidad), que se acerca a la manera como el ojo humano describe e interpreta el color. (Ver figura IV.27).


**Figura IV.27.** Balanceo de color

#### 4.2.4.3. Modelo HSI

El modelo de color HSI (hue, saturation, intensity: tono, saturación e intensidad) separa el componente de intensidad de la información de color en una imagen de color. Como resultado, este modelo es una herramienta ideal para desarrollar algoritmos basados en descripciones de color naturales e intuitivas para los seres humanos.

Al ajustar los componentes de color de una imagen, es importante recordar que cada acción afecta el equilibrio de color total de la imagen.

### 4.2.5. Compresión de Imágenes

El término compresión de datos se refiere al proceso de reducir la cantidad de datos requeridos para representar una cantidad dada de información.

Cuando un conjunto de datos contiene más del mínimo necesario para transmitir la información, decimos que existe redundancia de datos.

En el caso de la compresión de imágenes, se identifican y explotan 3 tipos de redundancia de datos: redundancia de código, redundancia entre pixeles y redundancia psicovisual. Al reducir o eliminar una o más de estas se consiguen comprimir los datos.

Ya que es una operación irreversible, la cuantificación conduce a una compresión con pérdida de datos.


**Figura IV.28.** Compresión de imágenes

La figura IV.28 muestra la imagen original con 256 niveles de gris y una imagen cuantificada a 16 niveles de gris, la cuantificación conduce a la presencia de falso contorno. La tercera imagen muestra la imagen cuantificada a 16 niveles de gris con un método que toma en cuenta las peculiaridades del sistema visual humano, llamado cuantificación de escala de grises mejorada (IGS).

### 4.2.6. Procesamiento Morfológico de Imágenes

En el Procesamiento Digital de Imágenes se utiliza el contexto de morfología matemática para extraer información de relevancia de las imágenes.

- Forma
- Bordes

En principio se analizan las herramientas morfológicas para imágenes binarias únicamente. (Ver figura IV.29).

#### 4.2.6.1. Operadores Lógicos involucradas en las Imágenes Binarias

Los operadores lógicos, aunque simples en naturaleza proveen un poderoso complemento en la implementación de imágenes procesando algoritmos basados en morfología. Los principales operadores lógicos usados en el procesamiento de la imagen son AND, OR y NOT. Estas operaciones son funcionalmente completas en el sentido de que pueden ser combinadas con cualquier otro operador lógico. Estas operaciones se pueden ver en la figura IV.30.

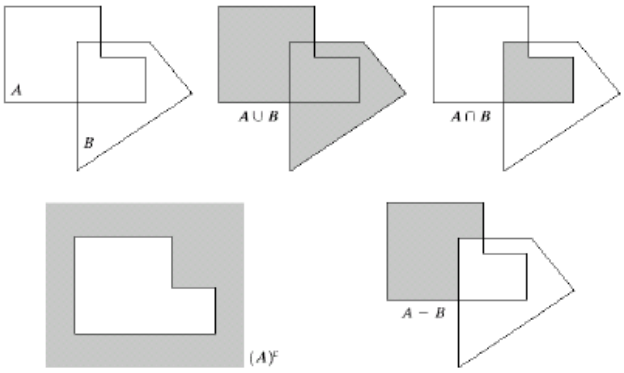



**Figura IV.29.** Operaciones morfológicas existentes

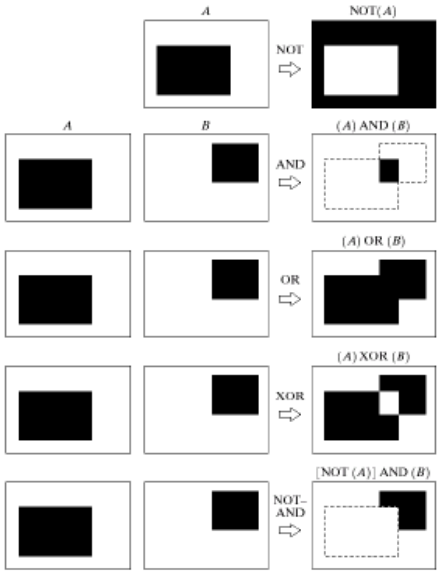



**Figura IV.30.** Algunos operadores lógicos entre imágenes binarias. El negro representa 1 binario y el blanco el 0 binario

**Operaciones de apertura y cierre**

La apertura suaviza los contornos de un objeto y elimina pequeñas uniones entre vecindarios. El cierre también suaviza los contornos, pero al contrario de la apertura, esta operación cierra agujeros y rellena discontinuidades en los contornos.

**Extracción de Bordes**

La extracción de bordes de una imagen binaria se puede realizar erosionando la imagen y luego restando el resultado de la imagen original.

**Dilatación y Erosión**

La Dilatación es la expansión de la imagen. Una de las principales aplicaciones de la dilatación es la de rellenar huecos. La Erosión es la retracción de la imagen. Una de las aplicaciones más sencillas de la erosión es eliminar detalles irrelevantes de una imagen binaria, como se observa en la figura IV.31.


**Figura IV.31.** a) Imagen con ruido, b) Elemento estructurado, c) Imagen erosionada, d) Apertura de A, e) Dilatación de la apertura, f) Cierre de la apertura.

**4.2.6.2. Esqueletización**

Representa la estructura de un objeto (conservando la conectividad, los agujeros y en cierto modo la extensión del mismo) con un número pequeño de pixeles. (Ver figura IV.32).

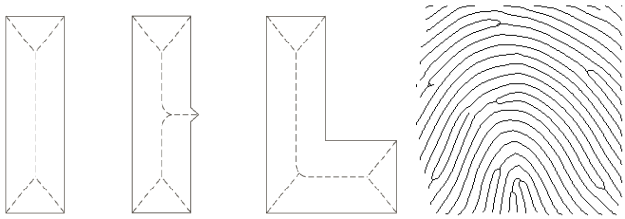


**Figura IV.32.** Ejemplos de esqueletización

- Proporciona información sobre la topología de un objeto.
- Proporciona información sobre la estructura de un objeto.
- Detección de fallos en procesos de fabricación (ej.: placas de circuitos).
- Obtención de datos biométricos (ej.: huellas dactilares, reconocimiento facial)
- Reconocimiento de formas (ej.: reconocimiento de caracteres u OCR).
- Visión artificial.
- Diseño gráfico (ej.: Corel PhotoPaint).
- Aplicaciones médicas o científicas (ej.: GPS, topografía).

## 4.2.7. Segmentación

La segmentación de imágenes es la separación de la imagen en regiones u objetos. Los algoritmos de segmentación de imágenes están basados en uno o dos propiedades básicas de valores de intensidad: Discontinuidad y Similaridad.

En la primera opción, la propuesta es la división de una imagen basada en el cambio repentino en la intensidad, tales como los límites de la imagen.

La segunda opción está basada en la división de la imagen en regiones que son similares de acuerdo al conjunto de criterios pre-definidos. Umbralización, incremento de regiones, división de regiones y unión son ejemplos de algunos métodos en esta categoría.

### 4.2.7.1. Binarización

Con éste método es posible convertir una imagen de varios niveles de gris a una nueva con solo dos, de tal forma que los objetos quedan separados del fondo

$$g(x,y) = \begin{cases} 1 \rightarrow T_a \leq f(x,y) \leq T_b \\ 0 \rightarrow en\ cualquier\ otro\ caso \end{cases}$$

El problema está en encontrar los valores de gris a tomar como umbrales entre objetos ya que debido al ruido, el objeto y el fondo no tienen un único valor de gris sino un intervalo, se solapan en algunos valores.

#### 4.2.7.2. Umbralización

Suponiendo que el histograma de escala de grises mostrado en la figura IV.33 corresponde a la imagen, f(x,y), compuesto por partes claras y un fondo oscuro, tales que los pixeles de el objeto y el fondo tienen niveles de grises agrupados dentro de dos modos dominantes. Una manera obvia de extraer el objeto del fondo es seleccionar un Umbral **u** que separe estos modos. Entonces cualquier punto (x, y) para cualquier f(x, y) > u es llamado como *punto del objeto,* por el contrario el otro punto es llamado como *punto del fondo.*

**Figura IV.33.** a) Imagen original, b) Resultado de la segmentación con un umbral estimado por interacción, c) Imagen del histograma

# Capítulo V

## Diseño e Implementación del Prototipo

## 5.1. Requerimientos

El sistema de autenticación biométrica requerido debe ser capaz de identificar a una persona que previamente este registrada en el sistema, para ello deberá hacer uso de una base de datos para el almacenamiento de los datos personales del usuario y sus huellas dactilares, las cuales serán adquiridas mediante el uso de un scanner de papel. A todo este proceso se lo conoce como modulo de Inscripción.

Para realizar la verificación de identidad se toma una nueva huella que será comparada con las huellas almacenadas en la base de datos, mediante el algoritmo de comparación realizado en LabVIEW, el cual decidirá si dicha persona está registrada en el sistema o no.

De forma general el sistema se basa en los siguientes pasos como se observa en la figura V.34.

## 5.2. Adquisición de la imagen

Cuando se observa una imagen en una pantalla o una fotografía, lo que se está observando es un conjunto grande (dependiendo de la resolución de la imagen) de puntos, coloreados de acuerdo a una regla de representación. La manera obvia, computacionalmente hablando, de

almacenar una imagen será entonces definir una matriz cuyas entradas sean todos los posibles colores observables

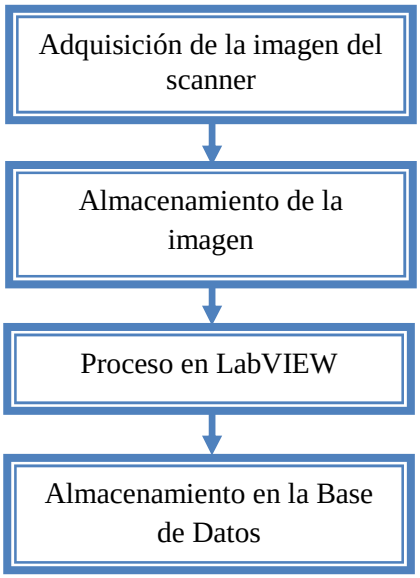



**Figura V.34.** Diagrama General del Proceso.

De esta manera una imagen puede entenderse como una señal bidimensional discretizada, por lo cual es posible realizar a ésta, procesos de filtrado o transformación de espacios.

Como se sabe existen distintos tipos de formato de imagen digital, los cuales difieren por la forma en que almacenan la información, la taza de compresión, la agregación de un canal de existencia de objeto, etc.

La imagen adquirida se toma de un scanner de papel, con un tamaño de 360x490 pixeles, con una resolución de 1200 dpi y una profundidad de 24 bits.

## 5.3. Almacenamiento de la imagen

Al principio se opto por almacenar la imagen en formato .bmp pero su tamaño en disco es bastante considerable, ya que por lo general, no se encuentran comprimidos. Por lo que se selecciono el formato .tiff que presenta la ventaja de ser compresible, con lo cual se emplea menos memoria en la base de datos, sin presentar una pérdida en la calidad de la imagen.

### 5.3.1. Formato de archivo TIFF

TIFF es un formato de fichero para imágenes. La denominación se debe a que los ficheros TIFF contienen, además de los datos de la imagen propiamente dicha, "etiquetas" en las que se archiva información sobre las características de la imagen, que sirve para su tratamiento posterior.

## 5.4. Proceso en LabVIEW

Para realizar todo el procesamiento de imágenes en LabVIEW se trabajo con el modulo Imaq Vision Development.

IMAQ es un aditamento de LabVIEW que contiene una gran cantidad de algoritmos que permiten manipular imágenes y obtener información de estas, además contiene codecs de interpretación de algunos formatos de video, que permiten descomponer el video en fotogramas para realizar el análisis de las imágenes en función del tiempo, teniendo así una forma sencilla de medir trayectorias y velocidades. IMAQ puede, con facilidad suplir una gran cantidad de costosos instrumentos, además de las ofrece posibilidades de desarrollo de otras herramientas y algoritmos. (Ver figura V.35.)

### 5.4.1. Visualización de Imágenes en LabVIEW

Lo primero que se debe aprender es como se carga una imagen en LabVIEW y que formato tiene esta en el interior del programa.

Luego de instalar IMAQ Vision en la computadora aparecerán nuevas opciones en los paneles de la interfaz de bloques (ver figura V.36); la mayoría de esas utilidades se encuentran contenidas en el cuadro “Vision and Motion” que se halla al desplegar las pestañas mediante el botón derecho del Mouse en el entorno de bloques

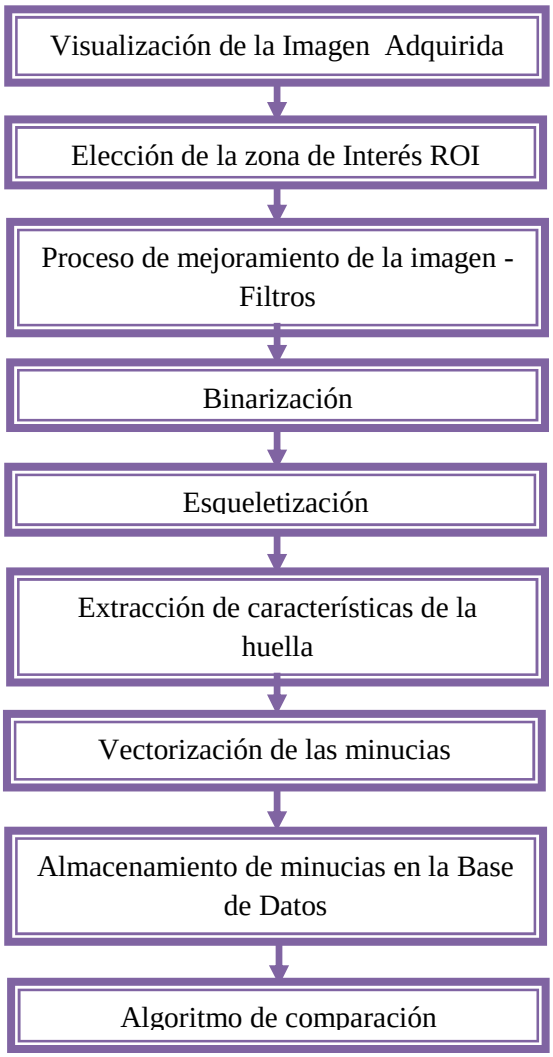



**Figura V.35.** Diagrama de las etapas desarrolladas en el software LabVIEW

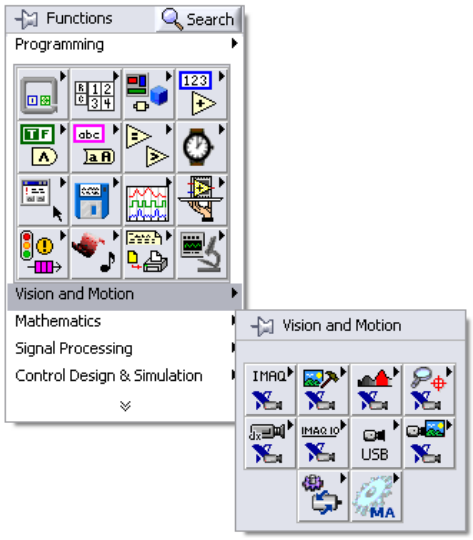



**Figura V.36.** Panel de la interfaz de bloques donde se muestra el modulo “vision and motion”

➢ **Leer y mostrar imágenes**

Para poder mostrar imágenes en LabVIEW es necesario crear un espacio de memoria que servirá para poder visualizar la imagen, esta se podrá liberar de memoria cuando se finalicen los procesos realizados. Para poder leer una imagen solo bastara con indicar el camino donde se almacenó dicha imagen, tal como lo muestra la figura V.37

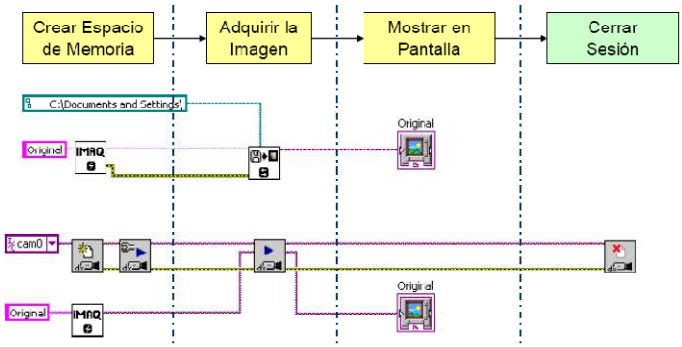



**Figura V.37.** Diagrama de visualización de imágenes en LabVIEW

## 5.4.2. Elección de la zona de interés

En LabVIEW se obtiene el ROI a través de un nodo de propiedad del visualizador de la imagen original, como se observa en la figura V.38.

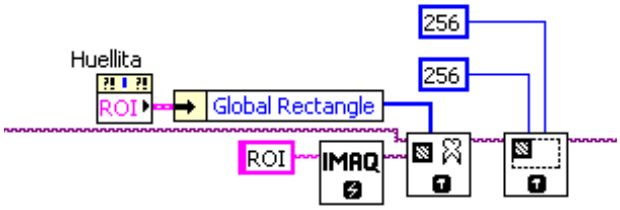



**Figura V.38.** Obtención automática de la zona de interés en una imagen.

## 5.4.3. Filtros para el mejoramiento de la imagen

En general un filtro bidimensional es una ley que permite la correspondencia de una imagen **I** con otra imagen **O**. Matemáticamente es representada por una transformación (u operador) que asigna a la entrada **I** una salida o respuesta **O**

$$\mathbf{I}(u,v) \xrightarrow{\Gamma} \mathbf{O}(u,v)$$
$$\mathbf{O}(u,v) = \Gamma\{\mathbf{I}(u,v)\}$$

Entonces un filtro requiere una señal de entrada y produce una señal de salida (ver figura V.39), la cual está relacionada con la entrada a través de la transformación del sistema.

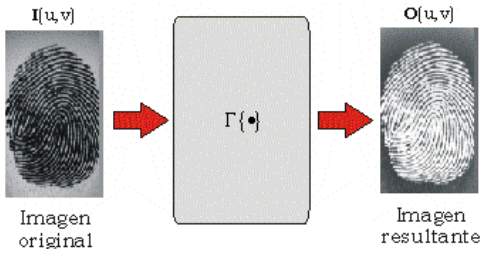



**Figura V.39** Acción de un filtro sobre la imagen de entrada **I**.

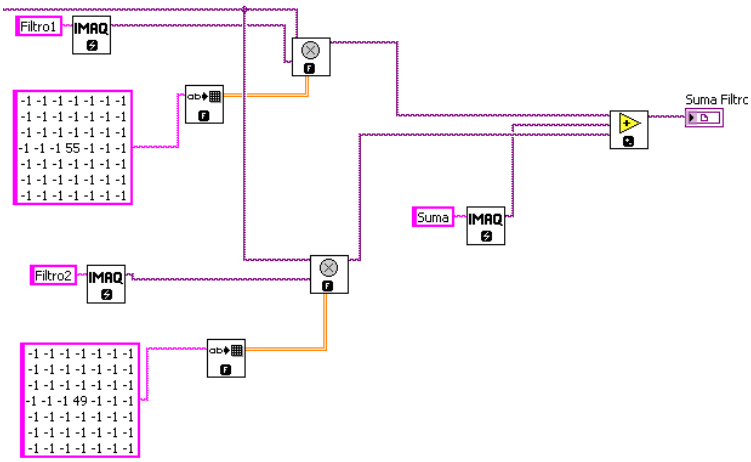



**Figura V.40** Aplicación de filtros en LabVIEW, utilizando las herramientas de visión.

- **IMAQ Convolute VI**

Filtra una imagen usando un filtro lineal. Los cálculos son desarrollados ya sea con números enteros o puntos flotantes, dependiendo del tipo de imagen y los contenidos del kernel.

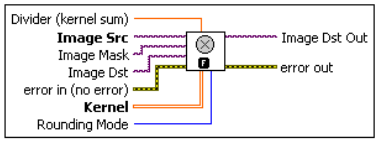
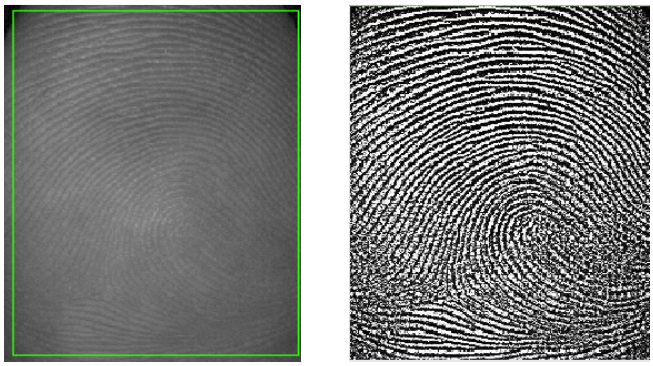
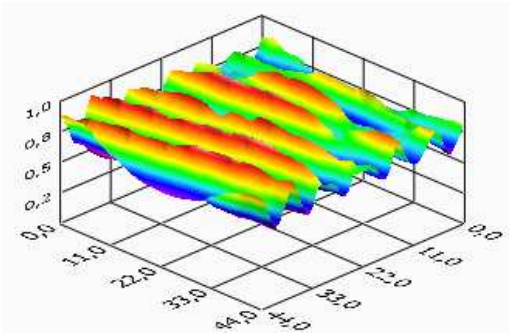



**Figura V.41.** Imaq convolute



a) b)




c)

**Figura V.42** a) imagen original, b) imagen aplicada filtro, c) Vista en 3d de una parte de la huella

## 5.4.4. Binarización

En esta etapa se busca adecuar la imagen para hacer más fácil el trabajo del algoritmo de reconocimiento, esta adecuación consiste en llevar la imagen de 255 posibles niveles de gris a solo dos posibles niveles de gris (0,1), este proceso es realizado tomando en cuenta las paletas de procesamiento y morfología de LabVIEW .En la figura V.46 se muestra el proceso para binarizar una imagen.

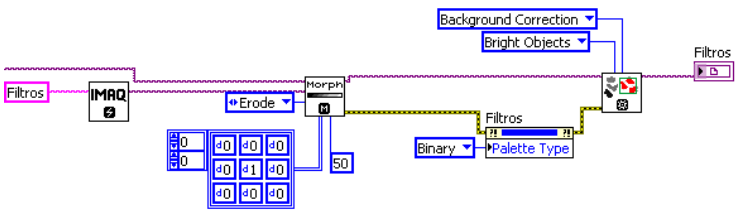



**Figura V.43** Proceso de Morfología-binarización

➢ **IMAQ GrayMorphology VI**

Realiza la transformación morfológica en escala de grises. Todos los tipos de imágenes de origen y destino deben ser los mismos. En la operación se seleccionara el tipo de morfología que se aplicara a la imagen, estas pueden ser AutoM, Close, Dilate, Erode, Gradiant, Thick, Thin, etc.

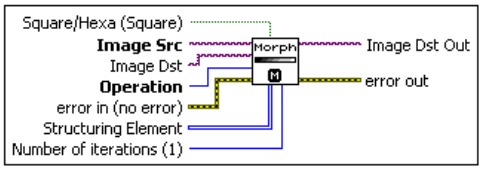



**Figura V.44** Imaq GrayMorphology

➢ **IMAQ Local Threshold VI**

Umbraliza una imagen y la convierte a binaria en base a una especificacion local que hace que el unbral sea adaptativo.

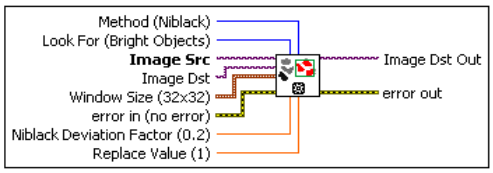



**Figura V.45** Imaq Local Threshold

Una vez binarizada la imagen y aplicada un umbral alto y bajo a la misma podemos obtener una matriz binarizada en la que se aprecian las crestas y valles, ya que en el tratamiento de una imagen es mas facil trabajar con matrices que con la imagen propiamente dicha.

## 5.4.5. Esqueletización

Luego de binarizar la imagen se necesita llevar las crestas de la huella a un ancho de un solo pixel, este proceso se lleva a cabo recorriendo las crestas o las negras de la huella y siguiendo sus tendencias buscando la mejor diagonal. Este proceso es también llamado skeleton o thining. En la figura V.47 se muestra una imagen esqueletizada y en la imagen V.48 su respectiva matriz**.**

- **IMAQ Skeleton VI**

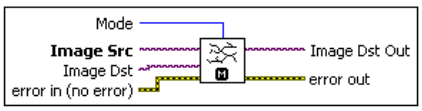



**Figura V.46.** Imaq Skeleton

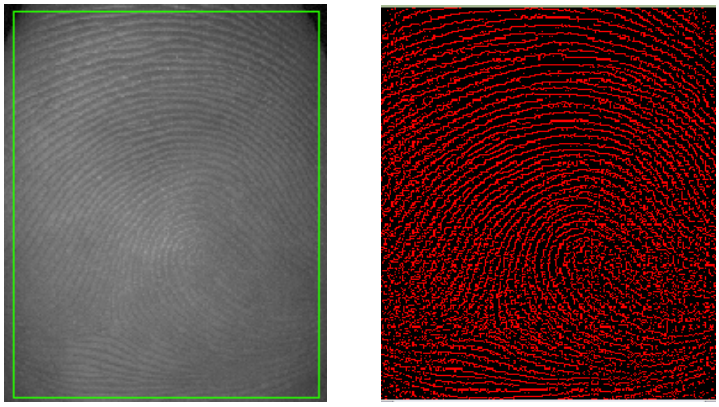


**Figura V.47** a) Imagen Original, b) Imagen esqueletizada

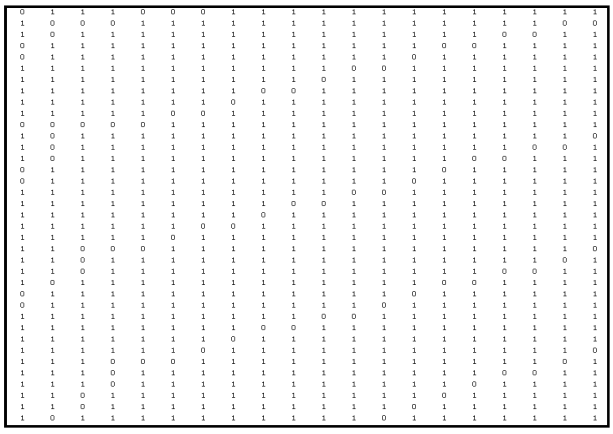


**Figura V.48** Matriz que muestra la esqueletización de la imagen

## 5.4.6. Extracción de características de la impresión dactilar

En esta etapa se diseña el algoritmo de identificación basado en la extracción de las minucias de la huella dactilar. El algoritmo diseñado se basa en el tipo de minucia, la posición de cada minucia y la distancia entre las minucias del mismo tipo. Esta información es luego almacenada en la base datos para posteriores identificaciones. Como se explicó anteriormente las minucias son conjuntos de valles y crestas que conforman los rasgos particulares de cada huella dactilar.

En la figura V.49 se muestra una huella con los 2 tipos de minucias más comunes identificadas, las cuales tienen sus diferentes variaciones, estas fueron encontradas utilizando una ventana de 3x3 que recorre toda la imagen.

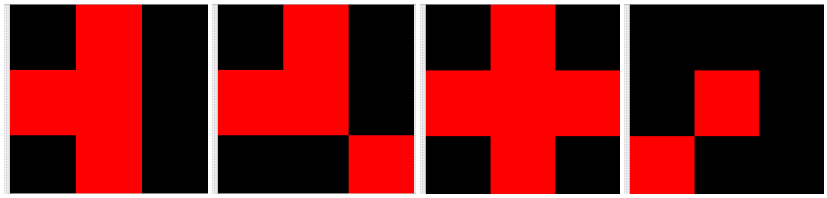


**Figura V.49.** Ventana de 3x3 utilizada para encontrar minucias de bifurcación y terminación con sus variaciones en relación a un pixel central

- **IMAQ Overlay Points**

Dibuja un punto o un array de puntos en una imagen

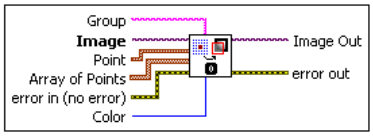



**Figura V.50.** Imaq Overlay Points

A la vez que se va barriendo la imagen en busca de minucias se va dibujando un punto en cada minucia valida hallada, tal y como se observa en la figura V.51.

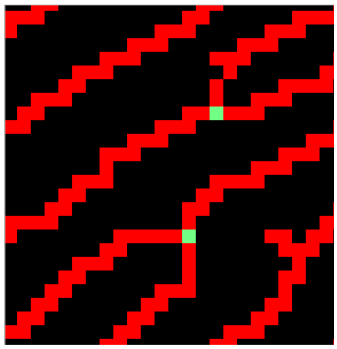


**Figura V.51.** Minucias encontradas

### 5.4.7. Vectorizacion de las minucias

Después de encontrar todas las minucias presentes en la huella digital comienza el proceso de vectorización, en este caso por cada huella se tomaran treinta puntos los cuales permitirán medir la distancia de acuerdo a sus posiciones, estas serán almacenadas en la base de datos para la posterior comparación.

### 5.4.8. Almacenamiento de minucias en la base de datos

Para la realización de este programa se empleo un complemento del LabVIEW llamado Database Connectivity Toolset, el mismo que facilita las operaciones con bases de datos, comandos SQL, etc. Primeramente se debía hacer que el programa almacene los datos del usuario así como un arreglo que represente al código de cada huella digital.

- **Database Connectivity Toolkit**

  Es un add-on o complemento de LabVIEW (ver figura V.52) para acceder a bases de datos. El paquete de herramientas contiene un conjunto de funciones de alto nivel, para realizar las más comunes tareas con bases de datos y funciones avanzadas para tareas personalizadas.

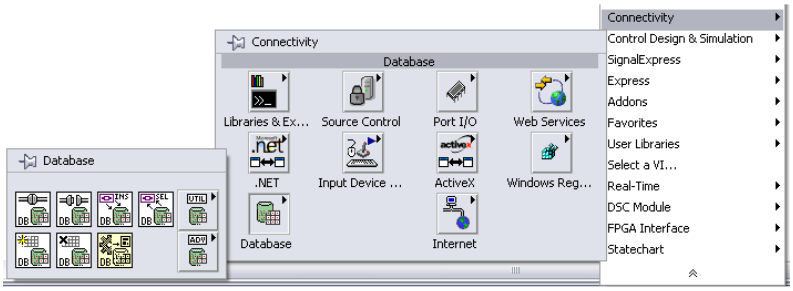



**Figura V.52.** Paletas del Database Connectivity Toolkit

A continuación se describen las principales características de LabVIEW Database

- **Connectivity Toollkit**

  Trabaja con cualquier proveedor que se adhiera al estándar Microsoft ActiveX Data Object (ADO)

  Trabaja con cualquier controlador de bases de datos que cumpla con ODBC u OLE DB.

Mantiene un alto nivel de portabilidad. En algunos casos se puede llevar los datos a otra base mediante el cambio de conexión.

Convertir una columna de datos de una base, de un tipo nativo a un estándar de LabVIEW Database Connectivity Tollkit, para mejorar su portabilidad.

Por defecto ADO ODBC permite el uso de sentencias SQL con todos los sistemas de bases soportados, aun en sistemas no SQL.

Incluye VIs para ir a traer el nombre y tipo de datos de la columna devuelta por la sentencia SELECT.

Crea tablas y selecciona, inserta, actualiza y borra registros sin usar sentencias SQL.

Para poder conectar una base de datos con LabVIEW, es imprescindible la existencia de un archivo *.udl (ver figura V.53), en cual se encargará de conectar a la base con el origen de la información.

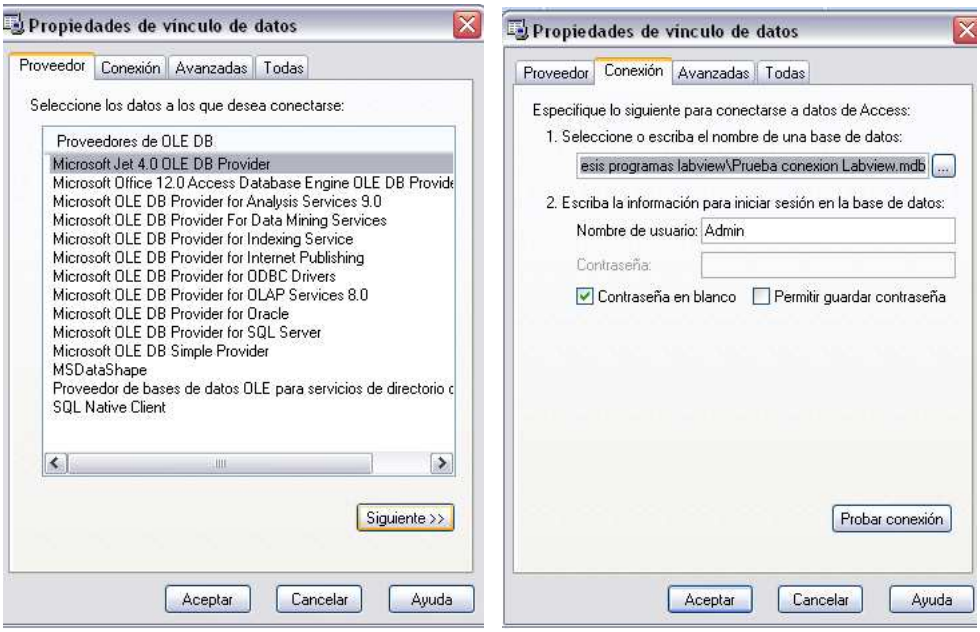



**Figura V.53.** Propiedades de archivo de vínculo de datos (udl).

- **Microsoft Access**

Es un sistema de gestión de bases de datos creado y modificado por Microsoft (DBMS) para uso personal o de pequeñas organizaciones. Su principal función es ser una potente base de datos, capaz de trabajar en si misma o bien con conexión hacia otros lenguajes de programación, tales como Visual Basic 6.0 o LabVIEW. Pueden realizarse consultas directas a las tablas contenidas mediante instrucciones SQL.

Permite el ingreso de datos de tipos: Numéricos, Texto, Fecha, Si/No, OLE, Moneda, Memo y Boolean, como se muestra en la figura V.54.

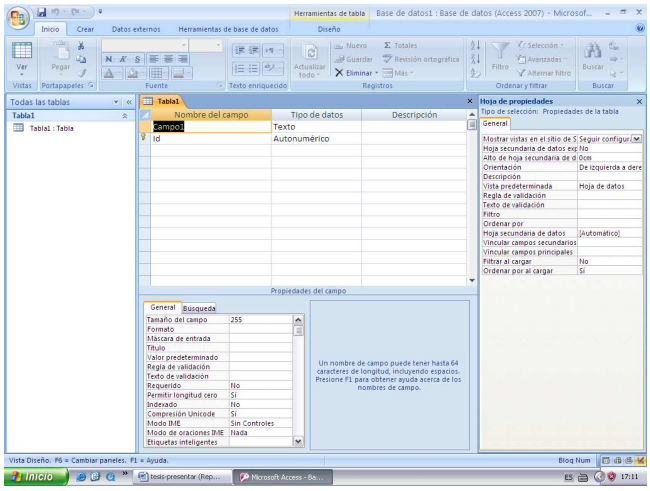


**Figura V.54.** Pantalla principal de Microsoft Access.

- **Creación de la Base de Datos de los Usuarios Autorizados.**

Para la realización de esta etapa, se partió del hecho de tener toda la información de los usuarios colocada en una tabla como se puede ver en la Figura V.55. Luego con la ayuda del comando DB Tools Insert Data se crea una tabla llamada DATOS en la base de datos distancias. En esta base de datos se almacenara toda información útil del usuario, además del código de las huellas, como se muestra en las figuras V.56 y V.57.

usuarios

| cedula | nombres | apellidos | direccion | sexo | telefono |
|---|---|---|---|---|---|
| 0201469715 | Nelly Rocio | Perez Villagomez | Garcia Moreno y 20 de Diciembre | Femenino | 32600371 |
| 0502374556 | Alfonso Manuel | Moreno Herrera | España y Ecuador | Masculino | 32949615 |
| 0502768617 | Fernando Gustavo | Tapia Carrasco | Cdla. El Rosal | Masculino | 32604461 |
| 0603288596 | Juan Miguel | Jacome Valdez | Alvarado entre 10 de Agosto y Guayaquil | Femenino | 32941309 |
| 0603602889 | Maria Lorena | Alban Ferro | 20 de Julio y Bolivar | Femenino | 2884678 |
| 0603910647 | Victoria Alexandra | Hidalgo Jacome | Duchicela 15-61 y Av. Unidad Nacional | Femenino | 32960900 |
| 0704819309 | Flor de Maria | Barragan Moncayo | Angel Martinez y Velazco | Femenino | 32967191 |
| 0802362571 | Fausto | Contero Peñafiel | Argentinos y Lavalle | Masculino | 32963101 |
| 1234567890 | Katty Alejandra | Jacome Valdez | Duchicela 15-61 y Av unidad Nacional | Femenino | 32960900 |
| 1716149255 | Carlos Ramon | Veloz Abril | Av la Naranja y Leonicio Benavides | Masculino | 32950374 |
| 1803606860 | Laila | Ponce Alarcon | Leopoldo freire y washintong | Femenino | 32600710 |
| 2100271846 | Jaime Armando | Orozco Avilez | Simon Bolivar y Miraflores | Masculino | 32961743 |

**Figura. V.55** Tabla creada en Access para el almacenamiento de los usuarios del sistema

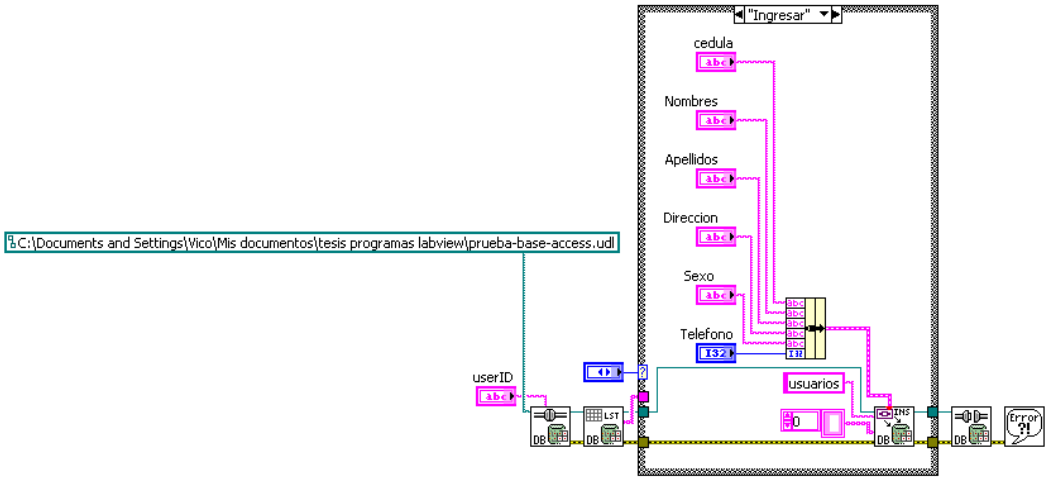



**Figura V.56.** Diagrama de Bloques del Modulo que almacena los datos del usuario en la base de datos

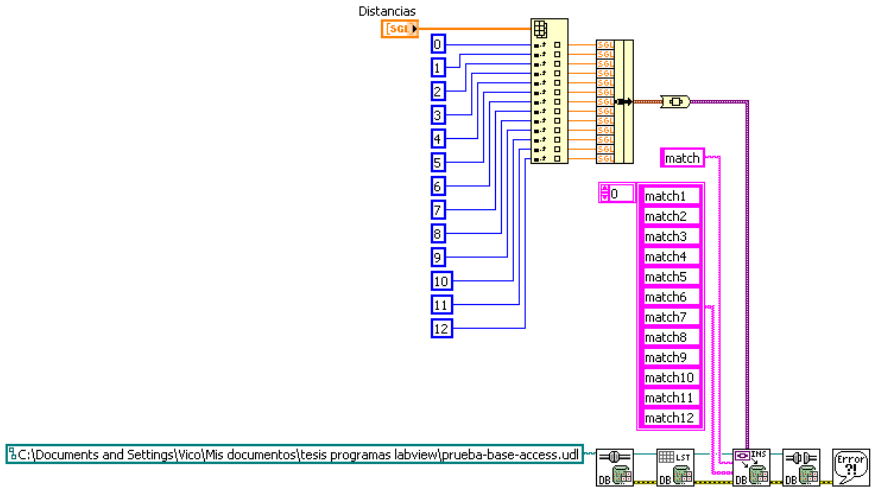



**Figura V.57.** Diagrama de bloques del modulo que almacena las distancias entre las minucias en la tabla

## 5.4.9. Algoritmo de comparación

Una vez almacenadas las distancias de cada una de las huellas en la base de datos, cuando el usuario se autentifica ante el sistema se toma una nueva huella de la cual se realiza su procesamiento y se compara con las demás huellas, según el código internacional de identificación se deben contar de ocho a doce puntos como mínimo para poder identificar a una persona. En este caso se ha realizado un promedio y se han tomado un número de diez puntos para que el usuario sea aceptado o rechazado por el sistema. Tal y como se muestra en la figura V.58.

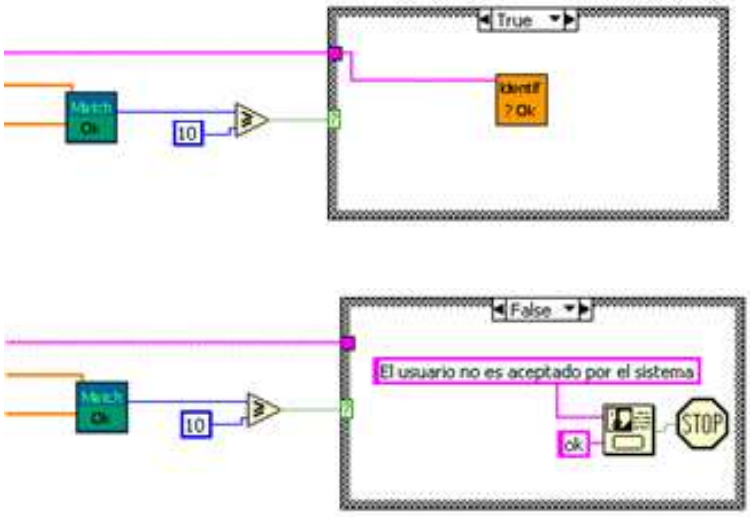



**Figura V.58.** Proceso de aceptación o rechazo del usuario

# Capítulo VI

## Estudio Comparativo de sensores biométricos

En este capítulo se analiza algunos equipos y sistemas que se encuentran en el mercado para la autenticación biométrica.

### 6.1. Lector de huella digital SECUGEN HAMSTER PLUS

Seguridad de computadoras personales. Seguridad de Redes en empresas. Comercio Electrónico. Transacciones Electrónicas. Sistemas financieros o bancarios. Sistemas de información en medicina. Cualquier aplicación basada en autentificación por contraseña


**Tabla VI.1. Características Técnicas sensor SECUGEN Hamster plus**

| | |
|---|---|
| Fingerprint Sensor | SecuGen USB Sensor |
| Dimensions (w/o stand) | 1.1" x 1.6" x 2.9" (27 x 40 x 73 mm) |
| Weight (w/o stand) | 3.5 oz. (100 g) |
| Resolution | 500 dpi ± 0.2% |
| Verification Time | Less than 1 second |
| False Acceptance Rate (FAR) | 0.001% |
| False Rejection Rate (FRR) | 0.1% |
| Operating Temperature | 32°to 104℉ (0°to 40℃) |
| Operating Humidity | < 90% relative, non-condensing |
| Interface | USB 1.1, 2.0 |
| Supported Operating Systems | Windows 7 / Vista / Server 2003 / XP / 2000 / Me / 98 SE |
| Certifications | FCC, CE, RoHS |
| Precio | $159.00 |

Fuente: Internet

## 6.2. APC Touch Biometric Pod Password Manager

El Biopod de APC permite a los usuarios iniciar sesión de un sistema simplemente colocando la yema del dedo en el sensor. A través del software y hardware del Biopod de APC se puede proporcionar identificación mediante huellas digitales para acceder a sistemas, aplicaciones y sitios web protección por contraseña, sin necesidad de emplear claves de acceso. Permite que hasta 20 usuarios puedan tener acceso a la información a través de su huella digital gracias a la gran velocidad que tiene al cambiar de usuarios.

Es un sistema de altas prestaciones, mucha precisión y larga durabilidad. Lector que se conecta directamente al ordenador y de forma muy segura reemplazamos el password que es vulnerable al fraude y difícil de recordar.

Además, el Reconocedor Digital de Huellas, posee un cable USB incorporado para facilitar la conexión a computadoras de escritorio y portátiles y es compatible con.

**Tabla VI.2. Características Técnicas sensor APC Touch Biometric**

| | |
|---|---|
| Fingerprint Sensor | Capacitivo |
| Dimensions (w/o stand) | 51.00 mm |
| Weight (w/o stand) | 25.00 mm |
| Verification Time | 1 sg |
| Interface | USB |
| Supported Operating Systems | Windows 98, Windows ME, Windows 2000, Windows XP y Windows Vista |
| Precio | $ 109.00 |

Fuente: Internet

## 6.3. Suprema Scanner en vivo RealScan-10

Verificación de calidad de imagen para huellas planas de un solo dedo, huellas giradas y de cuatro dedos

Segmentación automática de huellas de cuatro dedos en imágenes separadas de un solo dedo

Detección de deslizamiento para imágenes planas y giradas

Captura automática de imágenes planas y de presión detectando la colocación del dedo en el prisma

Compresión de imagen de la Huella dactilar certificada por la FBI

**Tabla VI.3. Características Técnicas RealScan-10**

| | |
|---|---|
| Tipo de Huellas | Roll Simple, Plano Simple, Cuatro dedos, Dos pulgares |
| Resolución | 500 dpi, 256 gris |
| Tamaño de Platina (W x L) | 3.3" x 3.1" (84 x 79 mm) |
| Tamaño de Imagen (W x L) | Cuatro dedos: 3.2" x 3.0" (81 x 76 mm)<br>Roll del Dedo: 1.6" x 1.5" (41 x 38 mm) |
| Estándar de la Calidad de Imagen | FBI IAFIS |
| Temperatura de Operación | 0-50'C |
| Humedad de Operación | Desde 10 a 90%, sin condensar |
| Dimensión (W x L x H) | 5.9" x 5.9" x 5.0"<br>(152 x 152 x 127 mm) |
| Peso | 1.60 kg |
| Interacción | USB 2.0 (datos & corriente eléctrica) |
| Sistema Operativo | Windows 2000, Windows XP 32bit/64bit,<br>Windows Vista 32bit/64bit, Linux |
| Certificado | FBI, WHQL, CE, FCC, UL, KCC |
| Precio | $ 745.00 |

Fuente: Internet

## 6.4. Lector de Huella Dactilar Usb Nitgen Hamster II con detector de huellas falsas

Puede ser utilizado en diferentes entornos de cliente / Servidor e internet.

Ideal para la seguridad informática y su entorno.

Comercio electrónico.

Seguridad para banca e instituciones financieras que requieran la identificación de sus usuarios.

Medio de pago por huella dactilar.

Sistemas de información médica / clínica.

Cualquier otro campo que requiera una identificación eficaz del usuario (SSO Single Sing-On, CRM Customer Relationship Management, control de presencia laboral, etc.).

**Tabla VI.4. Características Técnicas sensor Nitgen Hamster II**

| | |
|---|---|
| Fingerprint Sensor | Sensor digital de tipo óptico |
| Dimensions (w/o stand) | 61mm(Largo) x 80mm(Alto) x 47mm(Ancho). |
| Resolution | 500 dpi |
| False Acceptance Rate (FAR) | 0.001% |
| False Rejection Rate (FRR) | 0.1% |
| Operating Temperature | 20 ~ 60 ℃ |
| Interface | Usb 1.1/2.0 |
| Supported Operating Systems | MS Windows 98 SE o superior |
| Certifications | Certificación Common Criteria ( ISO-IEC 15408). |
| Precio | $180.00 |

Fuente: Internet

## 6.5. Lector biométrico de huella dactilar Nitgen EnBioScan F

El eNBioScan es un avanzado escáner de huellas dactilares con un área de captura de grandes dimensiones, que permite la adquisición de datos biométricos de la huella dactilar de manera más exacta y precisa. Ofrece prestaciones superiores, acorde con los estándares internacionales del FBI IQS, por lo que permite la integración con el nuevo pasaporte electrónico (E-Passport)


Existen dos modelos del escáner biométrico, el modelo eNBioScan-F (Flat Scanner) para capturar una o dos huellas dactilares sobre el plano; y el eNBioScan-R (Roll Scanner) para capturar la huella dactilar completa rotada sobre el plano.

Disponibles librerías SDK FDxDK específicas para este lector que permiten integrar el algoritmo de reconocimiento de huellas digitales de elevadas prestaciones de manera fácil en la aplicación concreta. Además permiten el control del dispositivo, altas/bajas, autenticación y extracción de datos biométricos de la huella dactilar.

**Tabla VI.5. Características Técnicas sensor Nitgen EnBioScan F**

| | |
|---|---|
| Fingerprint Sensor | Sensor óptico |
| Dimensions (w/o stand) | 63x146x81 |
| Resolution | 500 dpi |
| Verification Time | Alrededor de un segundo |
| False Acceptance Rate (FAR) | <0.0001% |
| False Rejection Rate (FRR) | <0.001% |
| Certifications | FCC, MIC, CE |
| Precio | € 548.80 |

Fuente: Internet

## 6.6. ANVIZ modelo T5


T5 es un sistema profesional de control de acceso que integra la tecnología de la biometría y lectura RFID. Diseño muy compacto lo cual permite ser instalado en el marco de una puerta. La salida estándar Wiegand permite la compatibilidad con controladores de acceso. Tiene la capacidad de almacenar 512 huellas. Tiene un procesador DSP de alta velocidad de 32 bits

**Tabla VI.6. Características Técnicas sensor Nitgen EnBioScan F**

| | |
|---|---|
| Fingerprint Sensor | óptico |
| Dimensions (w/o stand) | 55x145x37 mm |
| Resolution | 500 dpi |
| Verification Time | Alrededor de 0.7 segundos |
| False Acceptance Rate (FAR) | <0.0001% |
| False Rejection Rate (FRR) | <0.001% |
| Precio | $139.00 |

Fuente: Internet

## 6.7. Lector De Huella Digital Bio-Mini Suprema


El lector de huella dactilar USB BioMini está diseñado especialmente como una solución de seguridad de alto nivel tanto para computadoras de escritorio como para ambientes complejos en red. Este pequeño escáner ofrece durabilidad extrema con un diseño estilizado y una superficie libre de rayaduras. Con su sensor óptico de huella dactilar de 500 dpis y el algoritmo de Suprema ganador de reconocimientos internacionales, proporciona seguridad biométrica integral para aplicaciones de PC's y redes. Combinado con la solución avanzada en SDK, ofrece versatilidad única en plataformas de varios lenguajes, por lo que es ideal para procesos de desarrollo.

**Tabla VI.7 Características Técnicas sensor Bio-Mini Suprema**

| | |
|---|---|
| Fingerprint Sensor | Óptico libre de rayaduras |
| Dimensions (w/o stand) | 66x90x58 mm |
| Resolution | 500 dpi |
| Verification Time | I segundo |
| False Acceptance Rate (FAR) | <0.0001% |
| False Rejection Rate (FRR) | <0.001% |
| Operating Temperature | -10 a 50ºC |
| Interface | USB 2.0 Alta velocidad, plug and play |
| Supported Operating Systems | Microsoft Windows 98/ME/2000/XP/Vista y Linux |
| Certifications | CE, FCC, MIC |
| Precio | $159.00 |

Fuente: Internet

## 6.8. Lector De Huella Digital Uareu Digital Persona 4500


El lector U.are.U 4500 USB de huella digital ofrece una presentación elegante, con una moderna luz azul suave, diseñado para ambientes de alto uso.

Factor pequeño para horrar espacio

Construcción en carcasa metálica, pesada base para resistir movimiento involuntario.

Excelente calidad de imagen de 512 dpi

Excelente desempeño con todo tipos de huellas

Funcionamiento óptimo con huellas digitales secas, húmedas o irregulares

**Tabla VI.8. Características Técnicas sensor UareU Digital Persona**

| | |
|---|---|
| Fingerprint Sensor | optico |
| Resolution | 500 dpi |
| Supported Operating Systems | Microsoft Windows 98/ME/2000/XP/Vista y Linux |
| Precio | $179.00 |

Fuente: Internet

## 6.9. Scanner BenQ 4300

Un scanner es un dispositivo de entrada que digitaliza una imagen de un papel u otra superficie, y la almacena en la memoria de una computadora

Su modo de funcionamiento es el siguiente:

1. Una fuente de luz se desplaza sobre el papel, iluminando la sección sobre el que se desplaza.
2. Un motor mueve la cabeza de la lectora por debajo cuando se mueve captura la luz que se refleja en cada punto de la superficie. Los espacios en blanco reflejan más luz que los espacios más oscuros.
3. Esta luz capturada es reflejada a través de un sistema de espejos que continuamente mantiene estos rayos alineados con una lente.
4. La lente enfoca estos rayos hacia diodos sensibles a la luz que la traducen en una corriente eléctrica. Cuanto mayor es la luz mayor será el voltaje.
5. Un convertidor analógico digital traduce esta señal eléctrica en una señal digital. En los scanner blanco y negro cada pixel se digitaliza en un bit, de modo tal que pueda ser blanco o negro. En los de escala de grises cada punto se digitaliza en 8 bits teniendo 256 tipos de grises. Los scanner de color verdadero, por cada pixel utilizan 24 bits, teniendo así 16 millones de colores. Estos últimos, para poder tomar todos los colores realizan 3 exploraciones de la imagen, cada una pasando por un filtro distinto de color (rojo, verde, azul)
6. La información digital es enviada a la computadora donde el software se encarga de interpretarla y permitir trabajarla en su propio programa o en otro diferente como es el caso.

Existen tres tipos de scanner, el utilizado es este caso fue el más común llamado Plano o de sobremesa, que son los modelos más apreciados por su buena relación precio/prestaciones, aunque también son de los periféricos más incómodos de ubicar debido a su gran tamaño.

Sin embargo, son los modelos más versátiles, permitiendo escanear fotografías, hojas sueltas, periódicos, libros encuadernados e incluso transparencias, diapositivas o negativos con los adaptadores adecuados.

**Tabla VI.9. Características Técnicas scanner BenQ 4300**

| | |
|---|---|
| Fingerprint Sensor | cristal |
| Dimensions (w/o stand) | 412x258x73 mm |
| Resolution | 600x1200 dpi |
| Operating Temperature | 0-30ºC |
| Interface | Usb 1.1 |
| Supported Operating Systems | Microsoft Windows 98/ME/2000/XP/Vista |
| Precio | $ 40.00 |

Fuente:BenQ

# Capítulo VII

## Análisis y Resultados

Existen diferentes técnicas para la coincidencia de impresiones dactilares, sin embargo no se ha determinado cuál es la mejor técnica. Hay dos razones principales por las cuales es difícil evaluar el desempeño de las técnicas de coincidencia, siendo éstas:

1. La ejecución de la tarea de reconocimiento involucra un compromiso entre las diferentes medidas de rendimiento: exactitud, eficiencia, tamaño de la imagen, etc. Diferentes aplicaciones tienen diferentes requerimientos.
2. La mayoría de trabajos científicos publicados incluyen resultados experimentales llevados a cabo en una base de datos propia usando diferentes algoritmos, los cuales no son usualmente compartidos con la comunidad investigadora. Esto hace difícil de comparar resultados para diferentes técnicas.

## 7.1. Medidas de Evaluación

Los procedimientos de medida para los indicadores de rendimiento de mayor importancia son descritos a continuación

### 7.1.1 Cálculo de la Tasa de Aceptación (TA)

Para obtener este resultado se tomo de cada individuo registrado en el sistema diez huellas para verificar el porcentaje de aceptación que se obtiene del sistema.

Se realizó 10 prueba para cada usuario, comparándolas con las huellas almacenadas en la base de datos, de las cuales se puede observar que existe un mediano porcentaje de que un usuario sea reconocido por el sistema, los resultados pueden observarse en la figura VII.59.

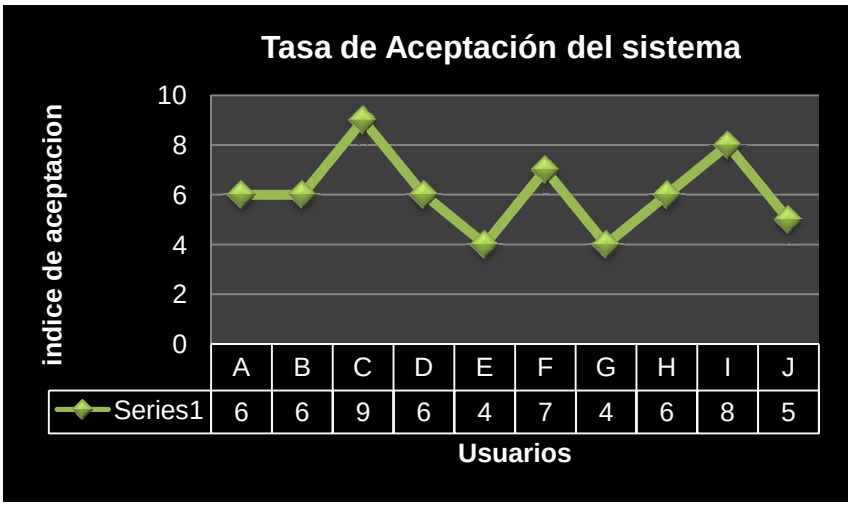



**Figura VII.59** Gráfico estadístico TA

### 7.1.2 Cálculo de la Tasa de Falso Rechazo (FRR)

De la misma manera se realizó 10 prueba para cada usuario, comparándolas con las huellas almacenadas en la base de datos, de las cuales se puede observar que existe un bajo índice de que un usuario no pueda ser reconocido por el sistema de autenticación, como se puede observar en la figura VII.60.

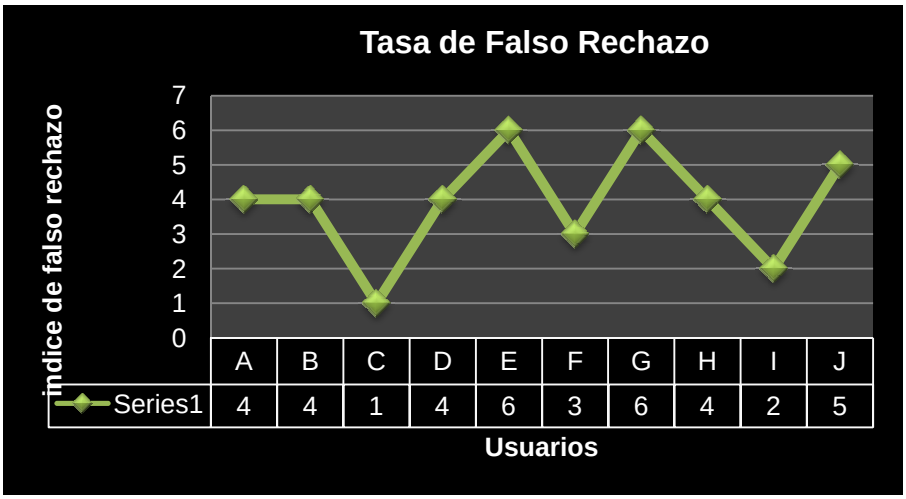



**Figura VII.60** Gráfico estadístico FRR

### 7.1.3. Cálculo de la Tasa de Falsa Aceptación (FAR):

Debido a que se trabajó en base al sistema AFAS el índice de falsa aceptación es nulo, sin embargo se realizó un estudio comparando todas las huellas almacenadas en el sistema con la de cada usuario, para poder tener una idea de cómo funcionaría el sistema si trabajara en un diferente modo de operación, a continuación en el gráfico de la figura VII.61 se puede observar este indicativo.

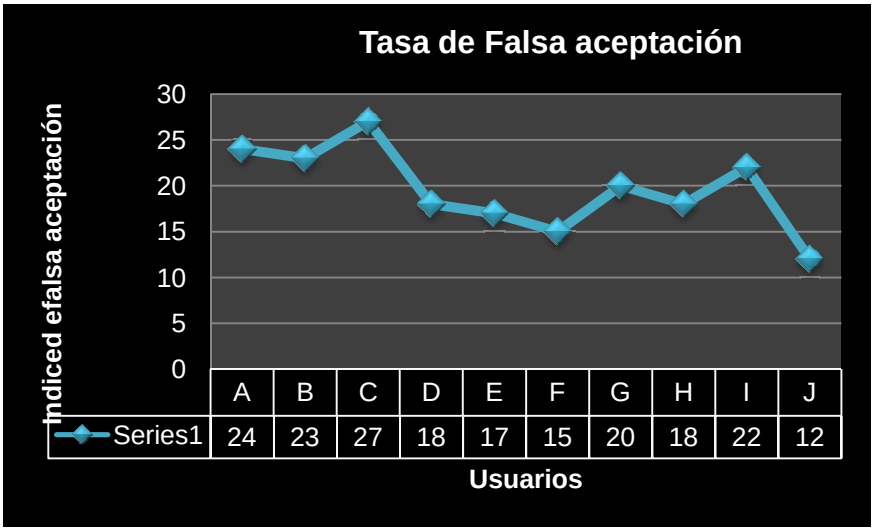



**Figura VII.61** Grafico estadístico FAR

### 7.1.4. Calculo de Totales

En el grafico de la figura VII.62, se observa de una manera más clara como se comporta el sistema en base a las consideraciones anotadas anteriormente.

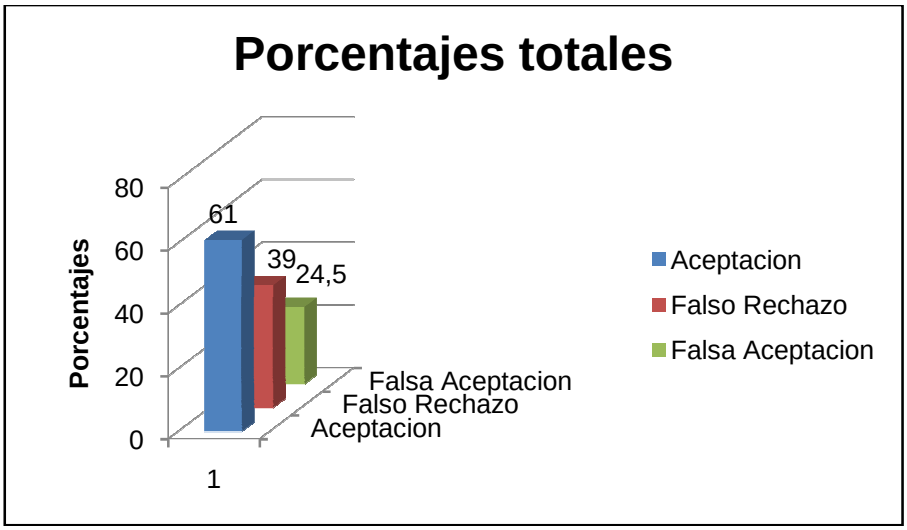



**Figura VII.62** Grafico total de Tasas calculadas

### 7.1.5. Promedio del Tiempo de Inscripción.

Para la inscripción se toma en cuenta solamente el tiempo que se demora en procesar las huellas, no se tomara en cuenta el tiempo que el usuario se demora en digitar sus datos personales, ni el proceso de comprobación de la cédula.

Como se procesan diez huellas de cada usuario, las cuales son almacenadas en la base de datos junto con sus respectivos vectores en promedio se demora 20 segundos por cada huella, teniendo en total 3minutos con 20 segundos.

### 7.1.6. Promedio del Tiempo de Coincidencia.

Se tomara en cuenta el tiempo que se demora en realizar el procesamiento de la huella y el tiempo que tarda en verificar en la base de datos, para ello en el primer caso se tarda aproximadamente 17 segundos y en el segundo caso un promedio de 1 segundo, haciendo el proceso de autenticación sumamente rápido.

## 7.2. Resultados

En esta etapa se muestra los diferentes procesos por los que pasa la imagen para luego ser comprada y sus pantallas finales.

La primera parte es la adquisición de la huella, esta es la muestra tomada desde el scanner. Figura VII.63.

**Figura VII.63** Imagen Adquirida

Se toma una región de interés, la que va a servir para el procesamiento. Esta imagen es el ROI. Figura VII.64

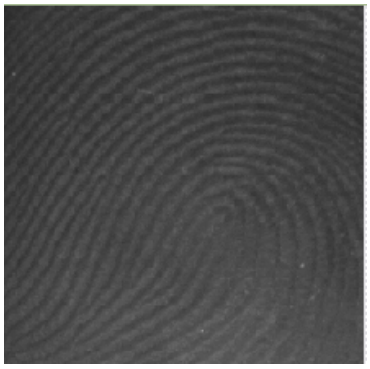


**Figura VII.64** ROI

Se aplican filtros para realzar las crestas para su posterior uso. Algunas regiones son difíciles de realzar y reconstruir por lo que la imagen en algunos sectores poco nítida. Como se muestra en la figura VII.65

**Figura VII.65** Imagen aplicada filtros

Para poder mejorar la imagen se trabajan con ventanas de 32x32 que recorren toda la imagen y se obtiene la imagen VII.66 a y la imagen ecualizada VII.66 b.

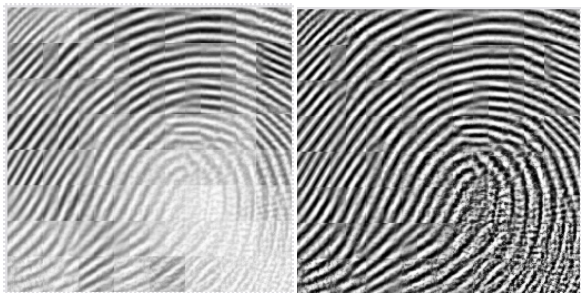


**Figura VII.66** a) normal, b) ecualizada

Luego para facilitar la búsqueda de las minucias, la imagen es adelgazada, algunas partes que no pueden mejorarse y generan imperfecciones. Ver figura VII.67

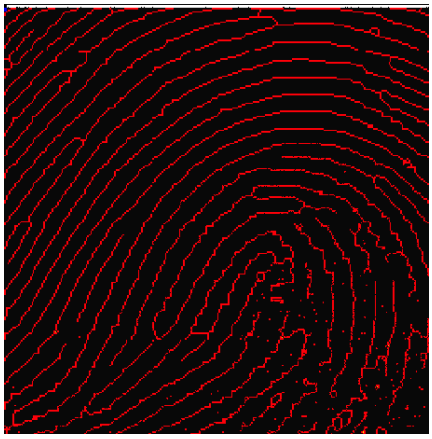


**Figura VII.67** Imagen Esqueletizada

Una vez adelgazada la imagen se encuentran las minucias, como se muestra en la figura VII.68, y su posicion dentro de la imagen (Figura VII.69), luego se calculan sus distancias (Figura VII.70).

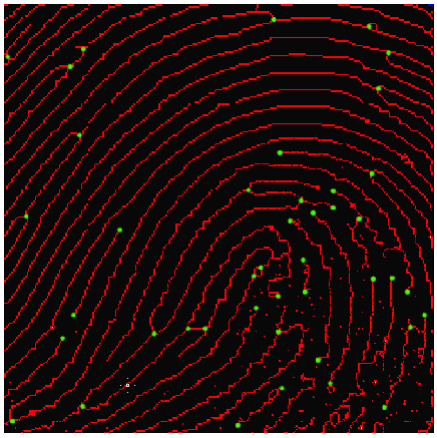


**Figura VII.68** Imagen con minucias encontradas


**Figura VII.69** Posición de cada minucia

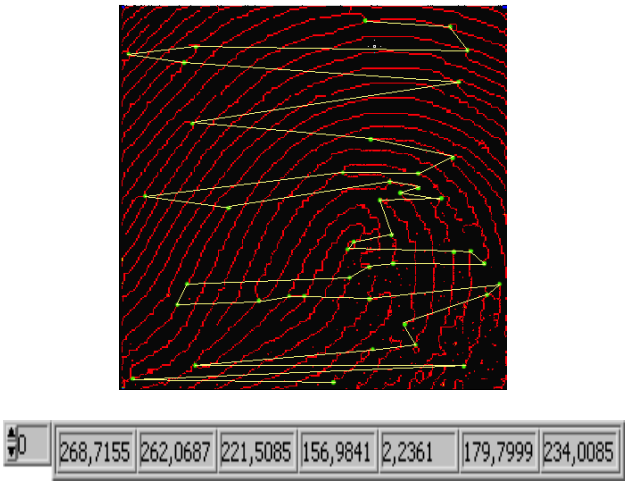
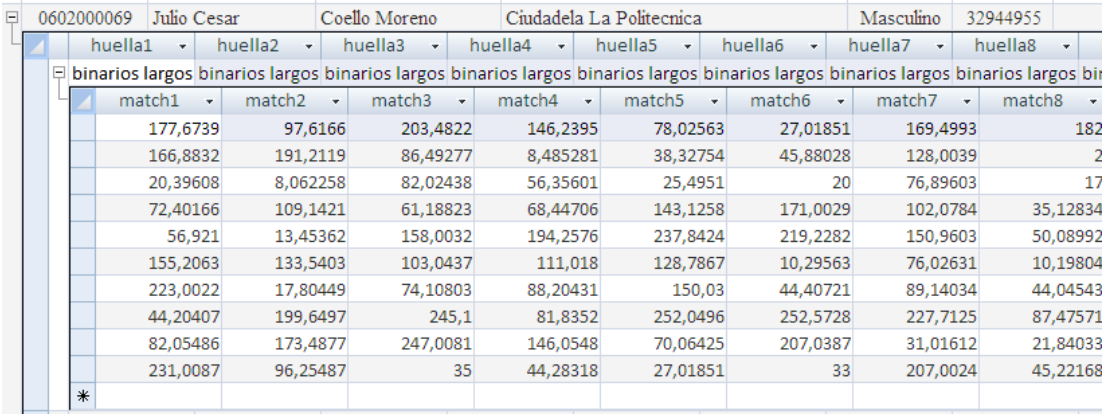



**Figura VII.70** Distancias calculadas

Estas distancias, junto con las huellas y los datos del usuario son almacenadas en la base de datos para poder compararlas en el proceso de verificación. Como se observa en la figura VII.71.



| 0602000069 | Julio Cesar | Coello Moreno | Ciudadela La Politecnica | | | | Masculino | 32944955 |
|---|---|---|---|---|---|---|---|---|
| huella1 | huella2 | huella3 | huella4 | huella5 | huella6 | huella7 | huella8 | |
| binarios largos | binarios largos | binarios largos | binarios largos | binarios largos | binarios largos | binarios largos | binarios largos | bi |
| match1 | match2 | match3 | match4 | match5 | match6 | match7 | match8 | |
| 177,6739 | 97,6166 | 203,4822 | 146,2395 | 78,02563 | 27,01851 | 169,4993 | 182 | |
| 166,8832 | 191,2119 | 86,49277 | 8,485281 | 38,32754 | 45,88028 | 128,0039 | 2 | |
| 20,39608 | 8,062258 | 82,02438 | 56,35601 | 25,4951 | 20 | 76,89603 | 17 | |
| 72,40166 | 109,1421 | 61,18823 | 68,44706 | 143,1258 | 171,0029 | 102,0784 | 35,12834 | |
| 56,921 | 13,45362 | 158,0032 | 194,2576 | 237,8424 | 219,2282 | 150,9603 | 50,08992 | |
| 155,2063 | 133,5403 | 103,0437 | 111,018 | 128,7867 | 10,29563 | 76,02631 | 10,19804 | |
| 223,0022 | 17,80449 | 74,10803 | 88,20431 | 150,03 | 44,40721 | 89,14034 | 44,04543 | |
| 44,20407 | 199,6497 | 245,1 | 81,8352 | 252,0496 | 252,5728 | 227,7125 | 87,47571 | |
| 82,05486 | 173,4877 | 247,0081 | 146,0548 | 70,06425 | 207,0387 | 31,01612 | 21,84033 | |
| 231,0087 | 96,25487 | 35 | 44,28318 | 27,01851 | 33 | 207,0024 | 45,22168 | |

**Figura VII.71.** Datos almacenados

Estas distancias son comparadas con la nueva huella del modulo de verificación, y así se comprueba la identidad del usuario.

El sistema consta de dos partes, la primera es el modulo de inscripción donde cada usuario ingresara sus datos al sistema para almacenarlos y la segunda el modulo de verificación, en la que se dará acceso al sistema dependiendo del resultado.

En la figura VII.72 se muestra la ventana de inscripción y en la figura VII.73 la ventana de verificación.


**Figura VII.72** Pantalla final Inscripción


**Figura VII.73** Pantalla final Verificación

# Conclusiones

- Se ha logrado desarrollar un sistema de autenticación biométrica basado en huellas digitales con la ayuda de un scanner de papel, el software que sirvió para su procesamiento y con la ayuda de un sistema de bases de datos para su implementación.

- Se ha analizado, implementado y comparado algunos de los algoritmos que existen para el procesamiento de las huellas dactilares, así como se ha seguido paso a paso las diferentes etapas de procesamiento, las cuales son necesarias para la mejora y la posterior extracción de características de la imagen.

- La implementación del software se realizo con la ayuda de LabVIEW 8.6 y su módulo de desarrollo Vision de National Instruments, el cual permitió realizar el procesamiento de imágenes y su interfaz de usuario. Además de utilizar Microsoft Access para la implementación de la base de datos, la que tendrá una conexión directa con LabVIEW y ayudara en el almacenamiento de la información entregada por el usuario.

- El dispositivo que sirvió para la adquisición de las huellas digitales es un scanner de papel, la principal desventaja fue que al aplicar una presión normal sobre la superficie de cristal, las crestas y valles de la huella se aplastan considerablemente y esto hace difícil el proceso de reconocimiento.

- Una desventaja de los dispositivos biométricos es el hecho de que esta sujetos a un gran margen de error. Generalmente el margen de error está relacionado con el costo de los dispositivos, cuanto más económico sea, mayor es el margen de error,

- Para poder determinar la diferencia entre usuarios se establece un umbral mínimo, el cual fue de 10 puntos característicos de coincidencia.

- Con los resultados mostrados se tiene una buena confiabilidad del sistema, esta presenta un porcentaje del 61 %, de esta manera el sistema presenta un mediano nivel de seguridad.

- En bases de datos pequeñas se aconseja en tomar como muestra de cada usuario 10 huellas para su posterior comparación, debido a que este es un prototipo de un sistema de autenticación se tiene un considerable tiempo de inscripción el mismo que reduce el factor de falsa aceptación y falso rechazo.

# Recomendaciones

- Es necesario realizar una limpieza periódica del dispositivo debido a la humedad de cada dedo y al polvo, la limpieza se debe realizar con el dispositivo apagado y con un paño seco.

- Durante la programación de la interfaz gráfica es indispensable definir cada una de las operaciones que se ejecutara en cada ventana, ya que esto permite tener una mejor visión del objetivo de desarrollo del sistema.

- Es necesario realizar un estudio minucioso sobre la relación entre tablas de la base de datos, ya que de ello depende que la información sea consistente en todo momento, además de la rapidez con la que se acceda a la información.

- Verificar que el programa en donde se realiza el sistema en esta caso LabVIEW sea compatible con el hardware para la adquisición de las imágenes, ya que no puede soportar cualquier dispositivo que sea conectado y esto presenta inconvenientes estéticos en su presentación.

- Es necesario realizar un buen diseño del dispositivo de adquisición de la huella (scanner), ya que de ello también depende que el algoritmo de comparación y en general el sistema tenga un menor margen de error en falsa aceptación o falsos rechazos.

- Debido a que existen diversos algoritmos para el procesamiento de huellas digitales se tomará en cuenta que para disminuir el margen de error se deben considerar las características locales de una huella ya que esto es lo que hace diferente a una persona de las demás.

- Es necesario que a todos los usuarios se les enseñe la forma correcta de colocar el dedo en el dispositivo de adquisición, para evitar posibles errores en el almacenamiento de datos.

- Se recomienda retirar la mayor cantidad de suciedad antes de realizar la verificación de su huella, de lo contrario esto podría ocasionar dificultades en la captura de la huella y en su verificación.

# Resumen

El presente proyecto tuvo como objetivo la implementación de un sistema de autenticación biométrica utilizando huellas digitales, en el que se diseñó el algoritmo de comparación para hacer de este sistema una solución confiable y de bajo costo. La tecnología biométrica permite resolver problemas de control de acceso y de seguridad informática sin la necesidad de olvidar objetos o recordar contraseñas. Se utilizó comunicación off-line para permitir la conexión hardware-software, para la adquisición de las huellas se utilizó un scanner de papel, la programación se realizó con LabVIEW 8.6 y para la implementación del sistema Microsoft Access 2007. Para realizar el algoritmo primero se realiza todo el procesamiento digital de imágenes con lo que la huella queda lista para poder encontrar los dos tipos más comunes de puntos característicos que existen en las huellas que son las terminaciones y bifurcaciones de las crestas, sus posiciones son únicas en cada persona por lo que con ellas es posible identificar a una persona y determinar si el individuo es aceptado o no por el sistema. El procesamiento de cada huella tiene un promedio de tiempo de 20 segundos y su verificación alrededor de 1 segundo. Para realizar las pruebas en la base de datos se contó con 100 huellas correspondiente a 10 personas de las cuales se obtuvo como tasa de aceptación el 61% y como tasa de falso rechazo el 39%, por lo tanto el sistema representa una solución confiable y de bajo costo.

# Summary

The present project had as objective the implementation of a system of biometric authentication using fingerprints, in which the comparison algorithm was designed to make of this system a reliable solution and low cost. The biometric technology allows solving problems of control of access and computer science security without the necessity to forget objects or to remember passwords. Communication was used off-line to allow the hardware-software connection, for the acquisition of the tracks was used a paper scanner, the programming was realized with LabVIEW 8,6 and for the implementation of the system Microsoft Access 2007. In order to realize the algorithm first all the digital processing of images is realized and so the fingerprint is ready to be able to both find more common types of minutiae that they exist in the fingerprint that are the terminations and bifurcations of the ridges, their positions are unique in each person reason why with them it is possible to identify a person and to determine if the individual is accepted or not by the system. The processing of each fingerprint has an average of time of 20 seconds and its verification around 1 second. In order to realize the tests in the data base it was counted on 100 fingerprint corresponding to 10 people from who 61% were obtained like rate of acceptance and rate of false rejection 39%, therefore the system represents a reliable solution and of low cost.

# Glosario

**Binarizar.-** La binarización es una herramienta del procesamiento de imágenes en el cual se deja una imagen en dos colores: blanco y negro

**Cuantificar:** En la digitalización de señales analógicas, es el proceso que le sigue al de muestreo. Consiste en asignar niveles discretos preestablecidos a los pulsos modulados en amplitud obtenidos del proceso de muestreo

**Ecualización del Histograma.-** Es una forma de manipulación de histograma que reduce automáticamente el contraste en las áreas muy claras o muy oscuras de una imagen. También expande los niveles de gris a lo largo de todo intervalo

**Filtro.-** Los filtros se utilizan para la modificación de imágenes ya sea para detectar los bordes de una escena o para modificar el aspecto, otra función de los filtros es para la eliminación de ruido de la imagen. El filtrado es una operación de convolución

**Histograma.-** El histograma no es más que una representación cartesiana de la luminosidad de una imagen En el eje horizontal (X) se representan los 256 valores de luminosidad de la imagen (0 para negro, izquierda y 255 para blanco, derecha), mientras que ell eje vertical (Y) se representa la cantidad de veces que se repite ese valor

**Minucias.-** Es un término utilizado en la medicina forense que significa “Punto característico”

**ROI.-** Es la región que nos interesa procesar, comúnmente esta se elige de acuerdo a las necesidades del procesamiento, ya sea de forma manual o automática.

**Ruido**.- El ruido caracteriza a las señales parásitas o de interferencia, es decir, las partes de la señal que han sido deformadas localmente. De este modo, el ruido de una imagen indica los píxeles de una imagen cuya intensidad es muy diferente de la de los píxeles adyacentes. Hay varios factores que pueden generar ruido en una imagen son el medio que la rodea cuando se la adquiere, la calidad del sensor, la calidad de la muestra.

**Reflectancia.- F**racción de la radiación total incidente sobre un cuerpo que es reflejada por el mismo.

**Umbralización.-** Límite en el que algo comienza o se inicia

# Anexos

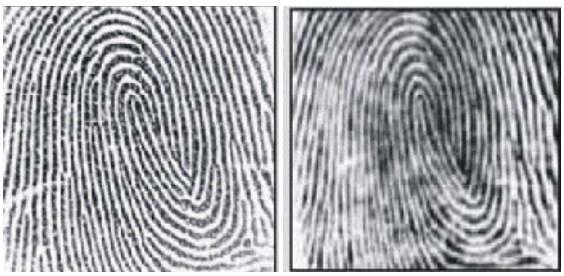
# Anexo I

## Captura de Huellas Digitales

**Parámetros Técnicos**

Los principales parámetros técnicos que caracterizan a una impresión dactilar son:

**Resolución**: Indica el número de puntos o píxeles por unidad de longitud, usualmente especificado en pulgadas (*dots per inch* - dpi). La resolución mínima establecida para los sensores del FBI es 500 dpi. Probablemente la mínima resolución requerida para detectar con precisión las minucias esté en el intervalo de 250 a 300 dpi.



**Área de captura**: Es el tamaño del área rectangular de captura. Una mayor área permite capturar más crestas y valles, proporcionando un patrón con mayor capacidad de discriminación. El área mínima requerida por las especificaciones del FBI es de 1x1 pulgadas cuadradas. Sin embargo, muchos sensores hoy en día poseen un área más pequeña, haciendo imposible que una huella dactilar completa sea capturada. Una pequeña área de captura mantiene tanto un costo bajo y un tamaño reducido, sin embargo también conlleva a innecesarios falsos rechazos.

**Rango dinámico (o profundidad):** Es el número de bits utilizados para codificar el valor de la intensidad de cada píxel en la imagen. El estándar del FBI establece el uso de imágenes en escala de grises con una profundidad de ocho bits.

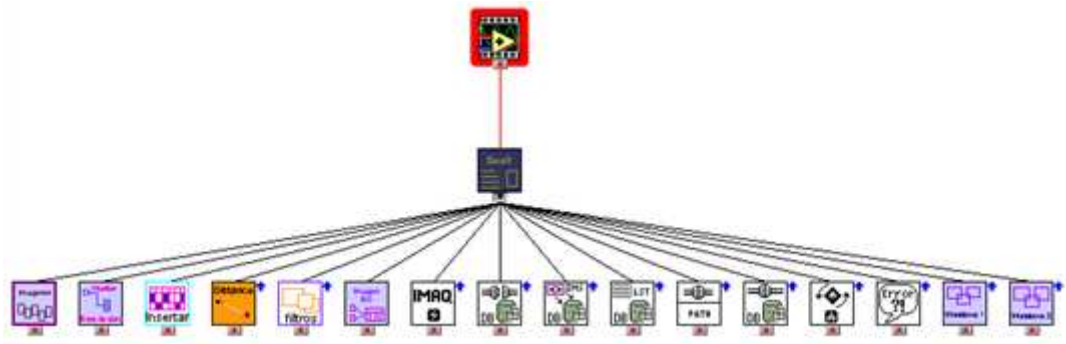
**Precisión geométrica:** Se define como la máxima distorsión geométrica presentada por el dispositivo de captura, se expresa como un porcentaje con respecto a las direcciones x e y. Muchos sensores ópticos presentan distorsiones geométricas que requieren ser compensadas pues alteran el patrón capturado.

**Calidad**: Es un parámetro difícil de medir, especialmente debido a que es complicado separar la calidad de la imagen del estado intrínseco de la huella dactilar. Todas las características anteriormente mencionadas trabajan juntas para establecer la precisión del sistema.

# Anexo II

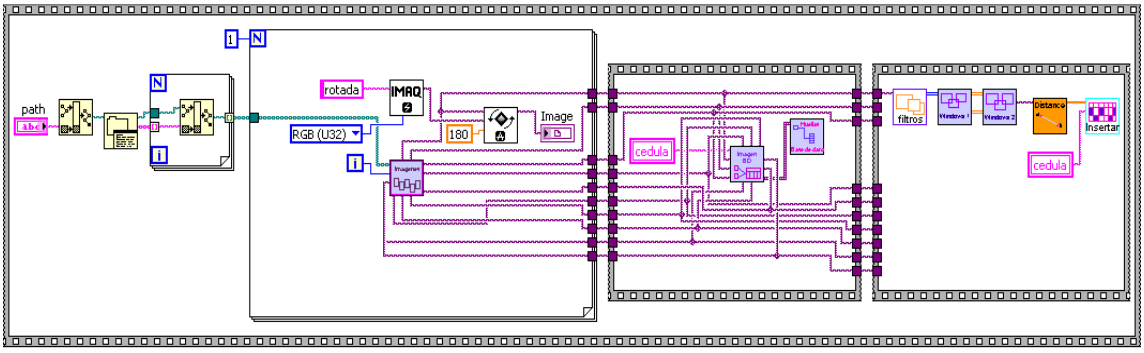
## Programación realizada en LabVIEW

**Modulo Inscripción**



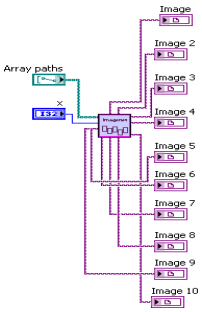
- **Inscripcion.vi**

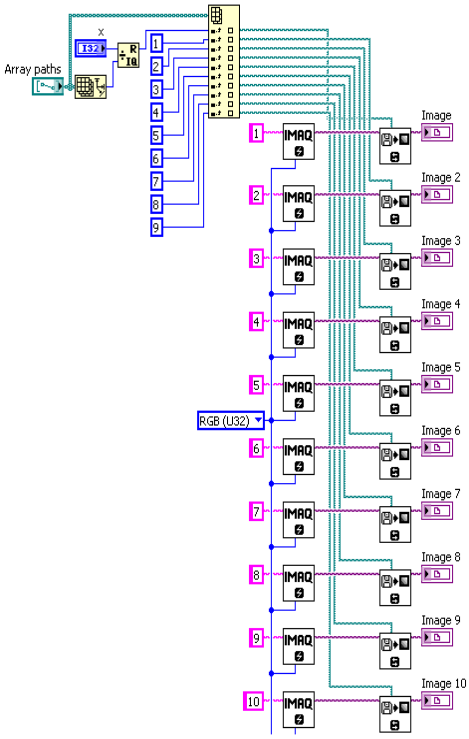
Este modulo permite al usuario enrolarse en el sistema y procesar sus huellas mediante sub-vis que se detallan a continuación.


- **10imagenes.vi**

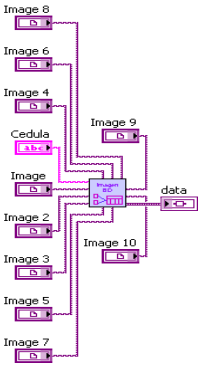
Este VI permite crear un espacio en memoria para cada imagen que va a ser adquirida, además de indicar el tipo de formato que estas deberán tener para su posterior procesamiento.

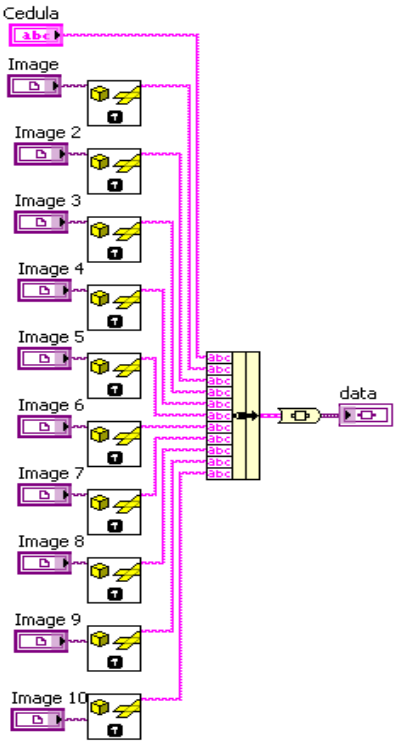



- **Imágenes-BD.vi**

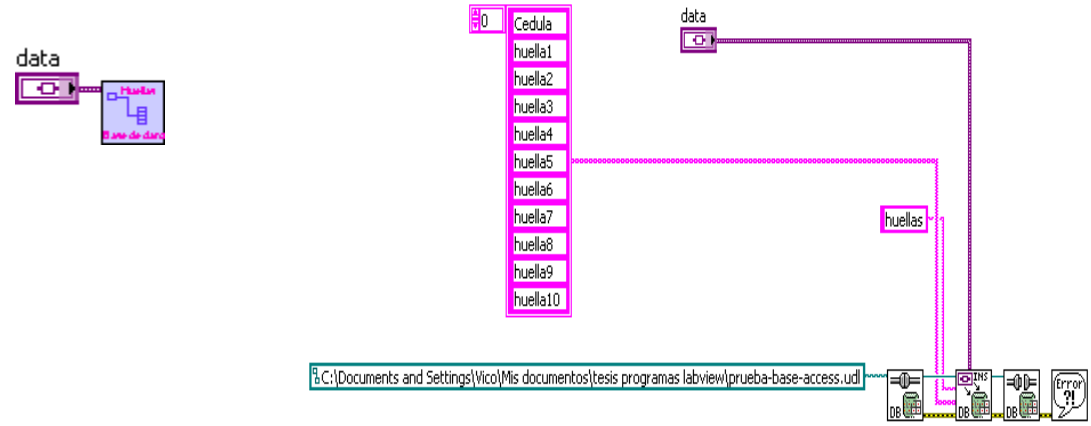
Este VI junto transformas las imágenes a un formato permitido por Microsoft Access para almacenarlas en la tabla.



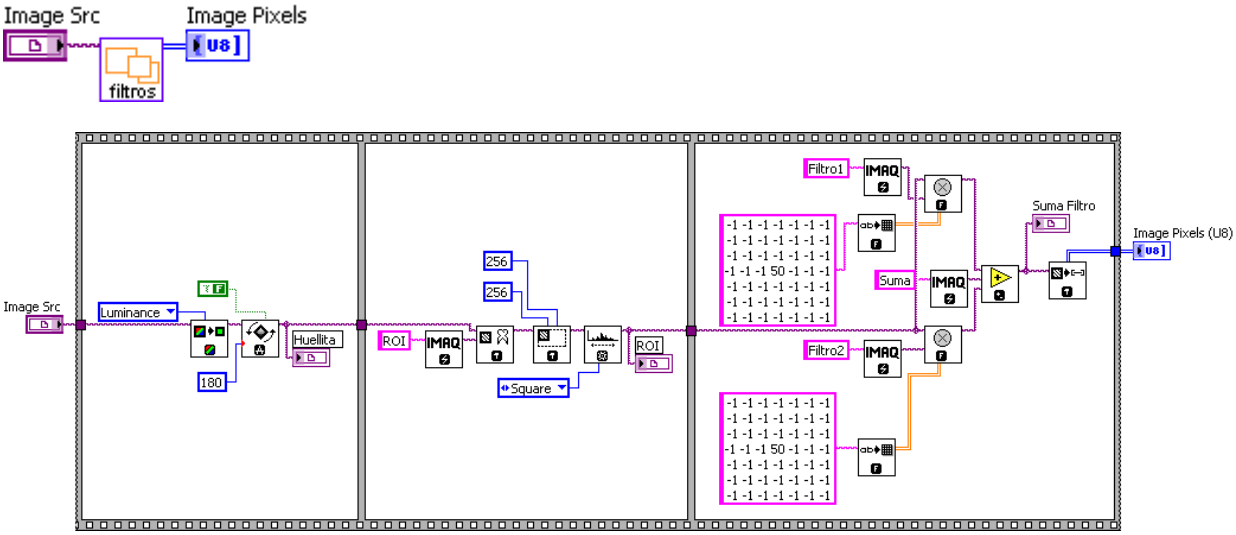
- **BD-Imagenes.vi**

Inserta cada huella capturada en la base de datos utilizando herramientas propias de LabVIEW.



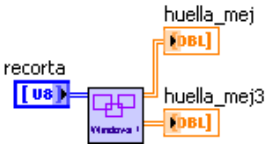

- **Filtros.vi**

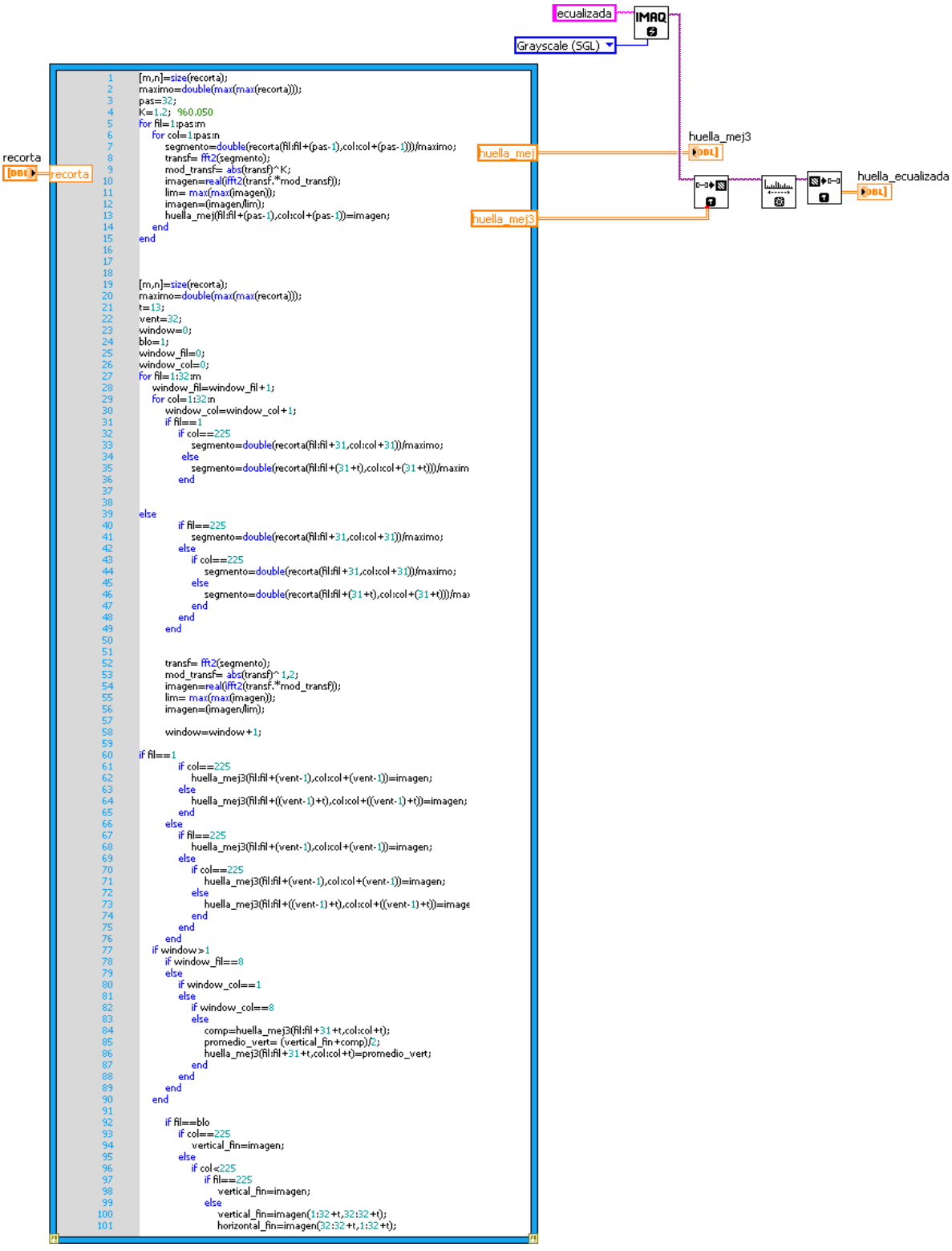
Adecua la imagen utilizando filtros para mejorar y eliminar imperfecciones.




- **Windows1.vi**

Esta parte del programa crea ventanas de 32x32 pixeles que van mejorando la imagen mediante la transformada de Fourier.

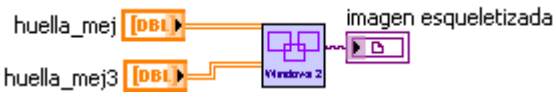


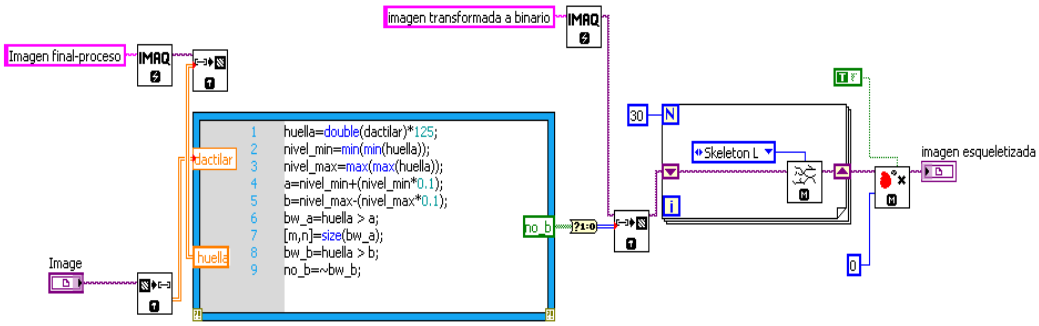




```
[m,n]=size(recorta);
maximo=double(max(max(recorta)));
pas=32;
K=1.2;  %0.050
for fil=1:pas:m
   for col=1:pas:n
      segmento=double(recorta(fil:fil+(pas-1),col:col+(pas-1)))/maximo;
      transf= fft2(segmento);
      mod_transf= abs(transf)^K;
      imagen=real(ifft2(transf.*mod_transf));
      lim= max(max(imagen));
      imagen=(imagen/lim);
      huella_mej(fil:fil+(pas-1),col:col+(pas-1))=imagen;
   end
end


[m,n]=size(recorta);
maximo=double(max(max(recorta)));
t=13;
vent=32;
window=0;
blo=1;
window_fil=0;
window_col=0;
for fil=1:32:m
   window_fil=window_fil+1;
   for col=1:32:n
      window_col=window_col+1;
      if fil==1
         if col==225
            segmento=double(recorta(fil:fil+31,col:col+31))/maximo;
          else
            segmento=double(recorta(fil:fil+(31+t),col:col+(31+t)))/maxim
         end


else
         if fil==225
            segmento=double(recorta(fil:fil+31,col:col+31))/maximo;
         else
            if col==225
               segmento=double(recorta(fil:fil+31,col:col+31))/maximo;
            else
               segmento=double(recorta(fil:fil+(31+t),col:col+(31+t)))/ma
            end
         end
      end


      transf= fft2(segmento);
      mod_transf= abs(transf)^1,2;
      imagen=real(ifft2(transf.*mod_transf));
      lim= max(max(imagen));
      imagen=(imagen/lim);

      window=window+1;

if fil==1
         if col==225
            huella_mej3(fil:fil+(vent-1),col:col+(vent-1))=imagen;
         else
            huella_mej3(fil:fil+((vent-1)+t),col:col+((vent-1)+t))=imagen;
         end
      else
         if fil==225
            huella_mej3(fil:fil+(vent-1),col:col+(vent-1))=imagen;
         else
            if col==225
               huella_mej3(fil:fil+(vent-1),col:col+(vent-1))=imagen;
            else
               huella_mej3(fil:fil+((vent-1)+t),col:col+((vent-1)+t))=image
            end
         end
      end
   if window>1
      if window_fil==8
      else
         if window_col==1
         else
            if window_col==8
            else
               comp=huella_mej3(fil:fil+31+t,col:col+t);
               promedio_vert= (vertical_fin+comp)/2;
               huella_mej3(fil:fil+31+t,col:col+t)=promedio_vert;
            end
         end
      end
   end

      if fil==blo
         if col==225
            vertical_fin=imagen;
         else
            if col<225
               if fil==225
                  vertical_fin=imagen;
               else
                  vertical_fin=imagen(1:32+t,32:32+t);
                  horizontal_fin=imagen(32:32+t,1:32+t);
```

- **Windows2.vi**

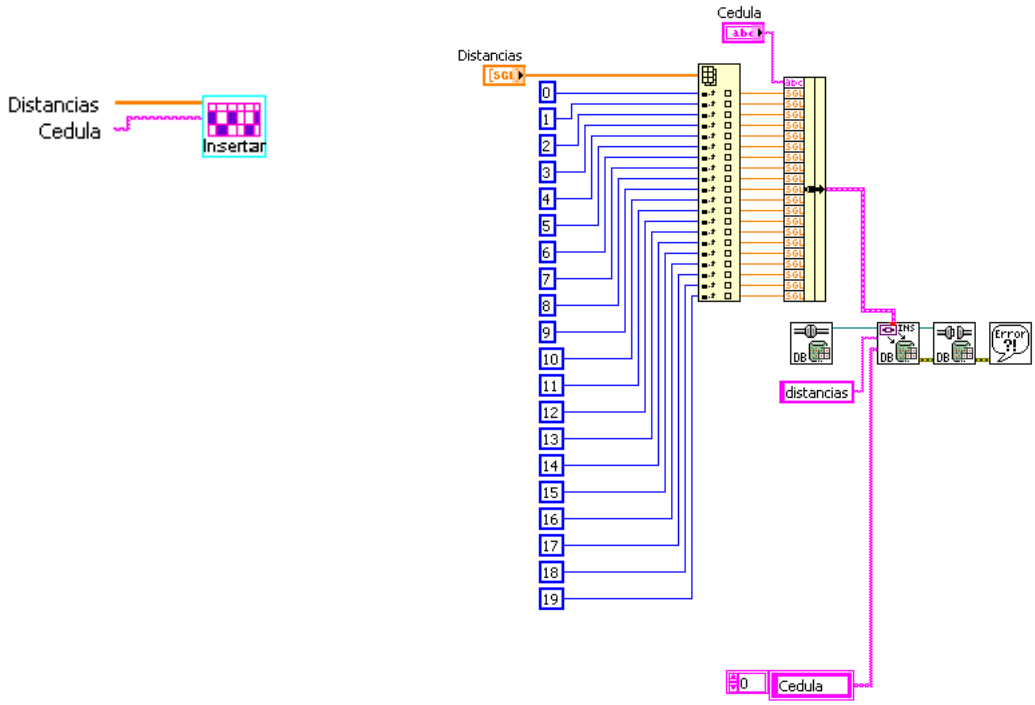
Este proceso permite adecuar la imagen para tenerla a solo un pixel de ancho.



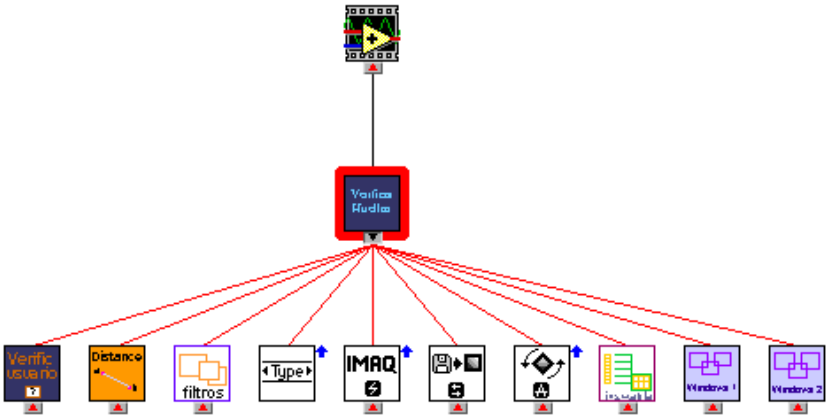




- **Distancias-BD.vi**

Luego de procesar las imágenes se obtiene como resultado las distancias entre minucias, este proceso las almacena en la  base de datos.

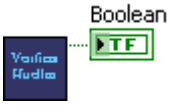


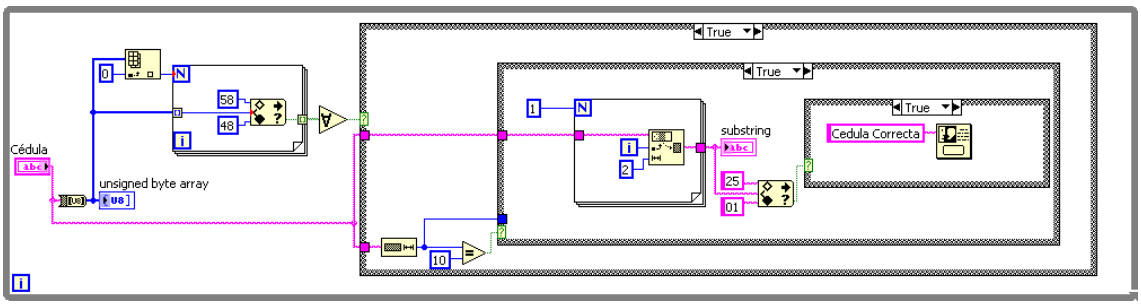
**Modulo Verificación**

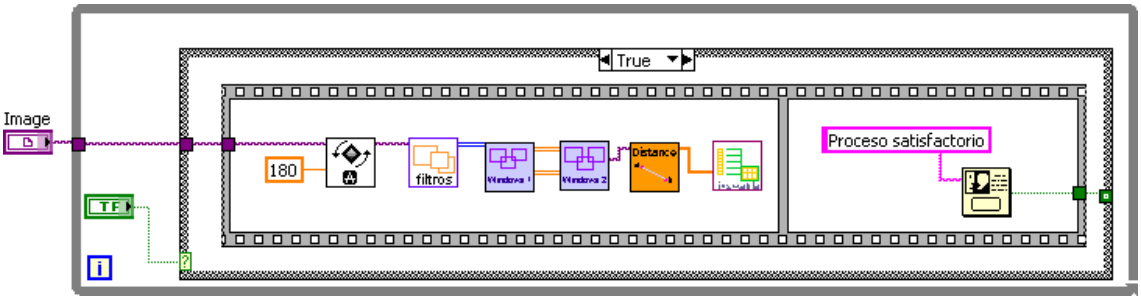



- **Verificacion.vi**

Este proceso se divide en dos partes, la primera verifica que el numero de cedula sea ingresado correctamente y la segunda parte es la que procesa la nueva huella para luego poder ser comparada.

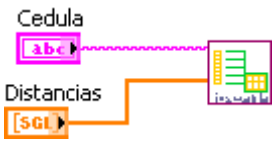


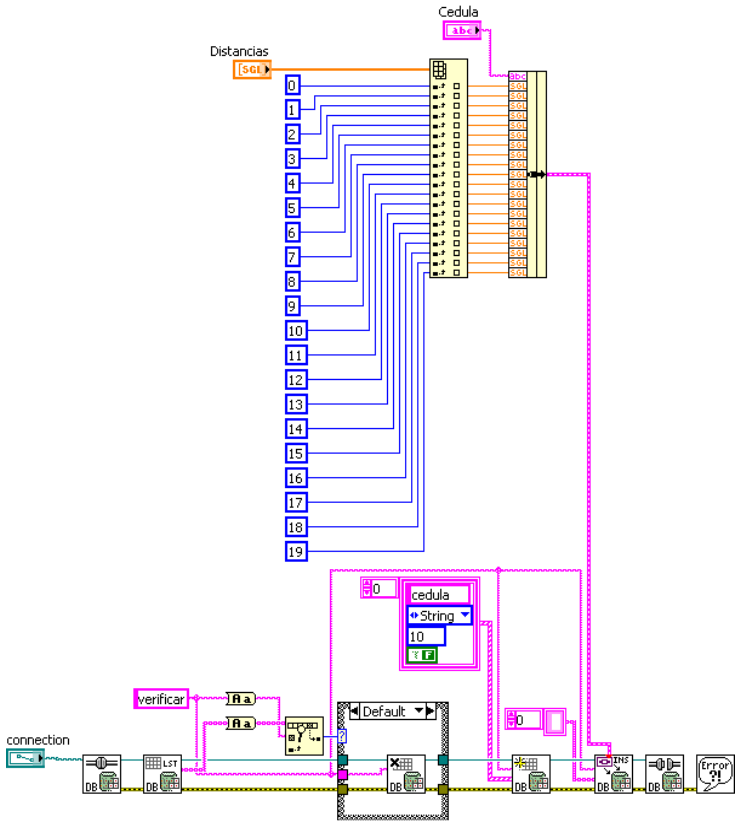



- **Borrar tabla verificar.vi**

Este proceso permite guardar temporalmente la huella que va a ser comparada y que ya está procesada en la tabla de la base de datos.



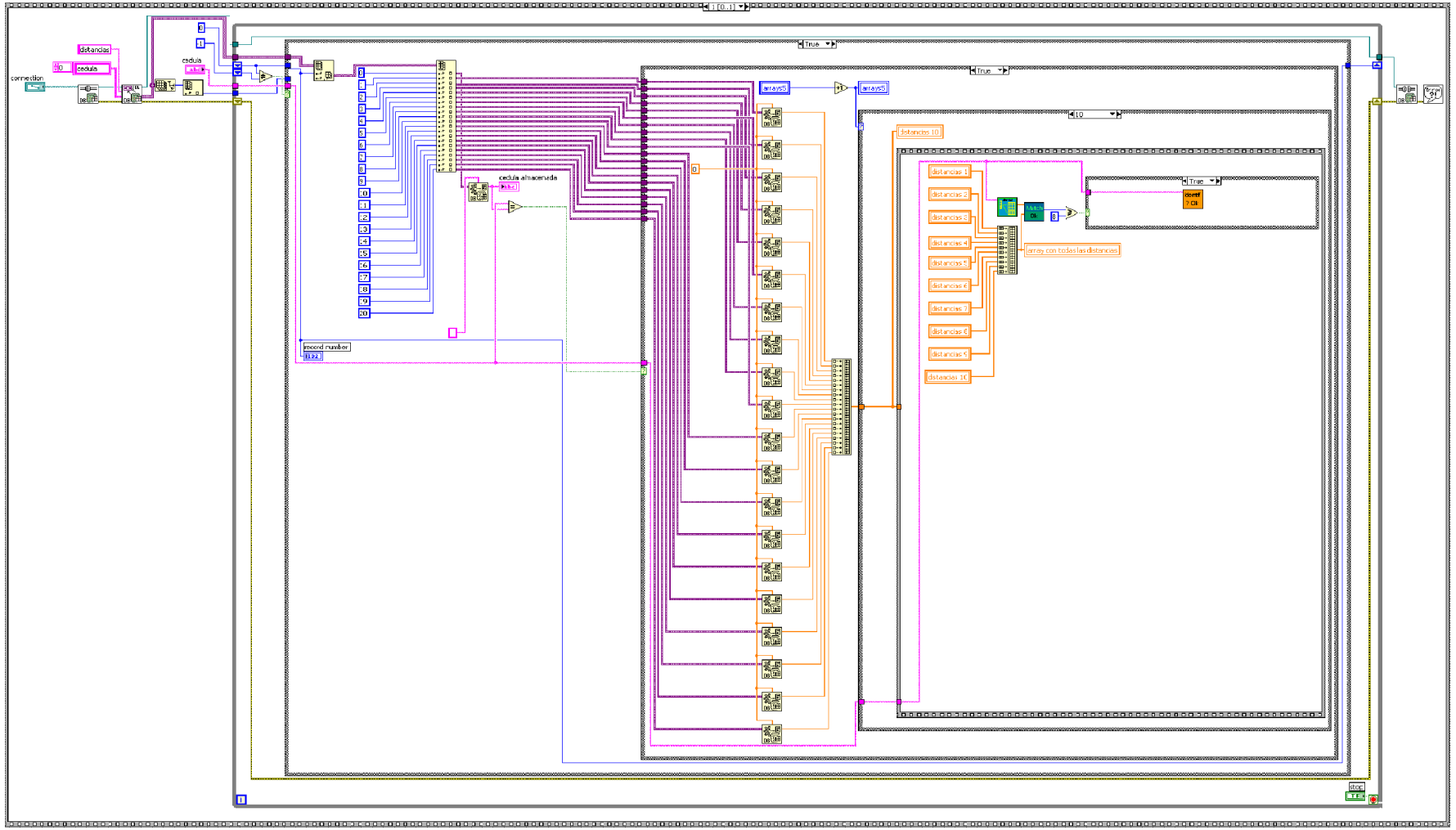




- **Autenticar.vi**

Este proceso se divide en cuatro partes, la primera almacena en un solo elemento todos los datos que están almacenados luego del proceso de inscripción, los que servirán para la posterior comparación.

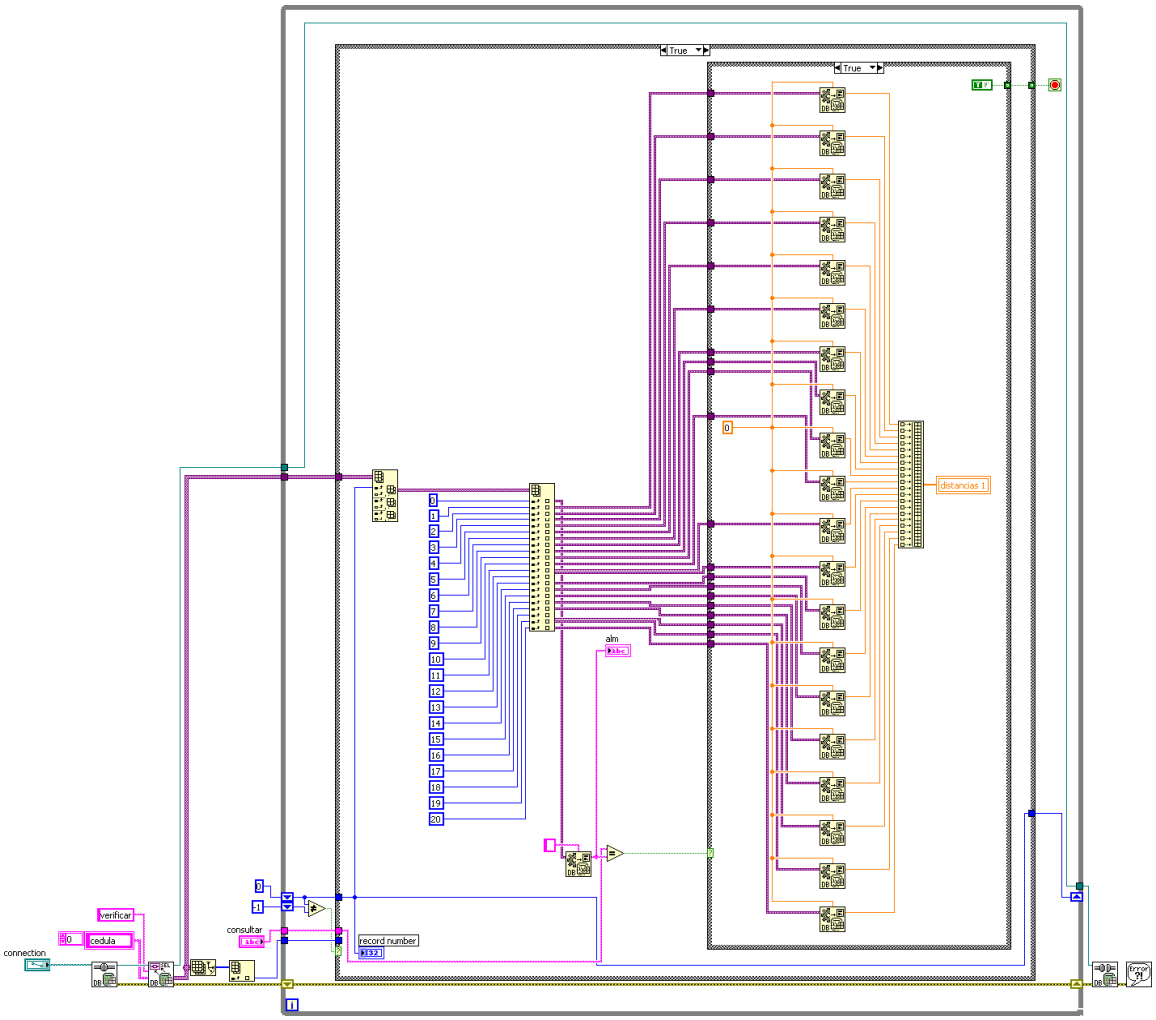
Los siguientes procesos son descritos en los siguientes sub-vis.

# Autenticar.vi



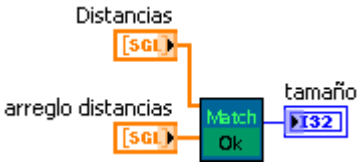
**Verificar-distancias-bd.vi**

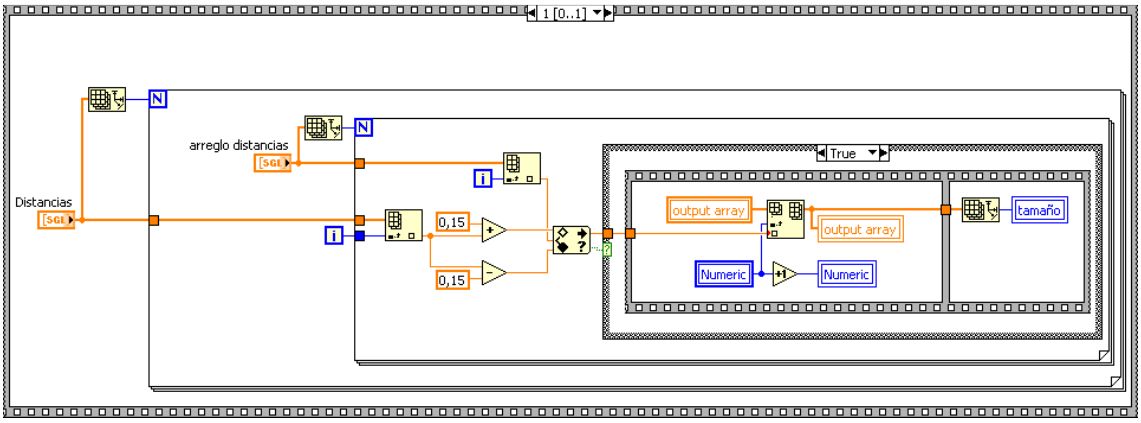
Este proceso busca al usuario en la base de datos y almacena en un solo elemento los datos de la nueva huella.


- **Match-Ok.vi**

Compara los datos de los dos procesos anteriores y dependiendo de su resultado se identificara al usuario.

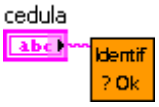


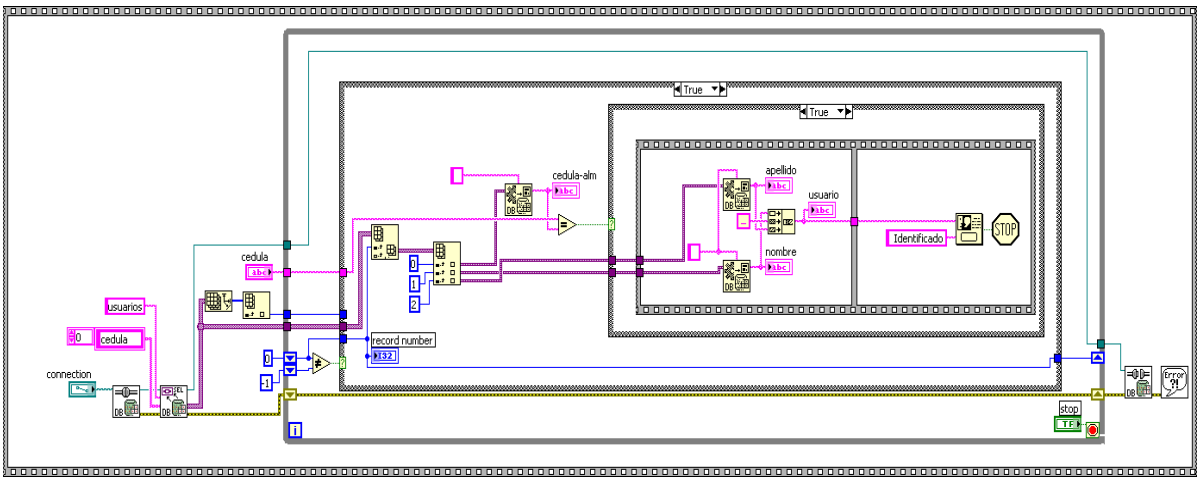



➢ **Identificacion-Ok.vi**

Si el resultado anterior es mayor o igual al umbral establecido en el sistema se realiza este proceso, el cual busca al usuario en la base de datos y extrae su nombre y apellido par luego mediante un mensaje indicar que el usuario ha sido identificado por el sistema.

Si el resultado es menor al umbral simplemente se indicara que el sistema no pudo identificar al usuario, teniendo la oportunidad de ingresar una nueva huella para luego ser autenticada.



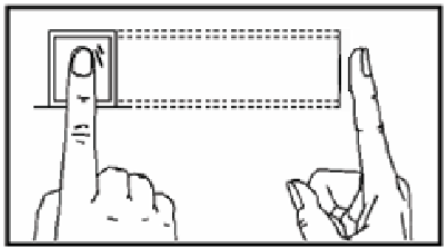
# Anexo III

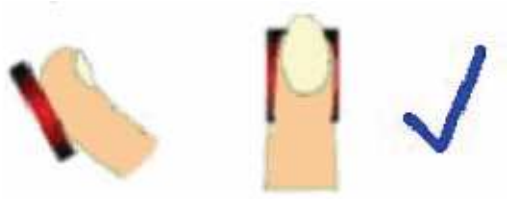
## Recomendaciones para adquirir la Huella Digital

**Recomendaciones**

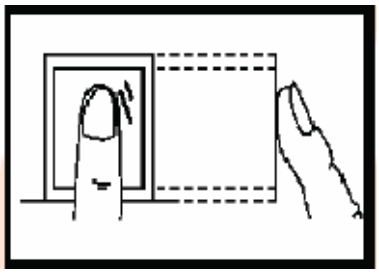
Antes de Realizar todo el proceso que se requiere para la verificación de una persona, es necesario saber la posición correcta en que se debe de adquirir la huella para realizar una verificación más eficaz. A continuación las diversas posiciones que se pueden presentar al momento de tomar una huella.

**Posición correcta**

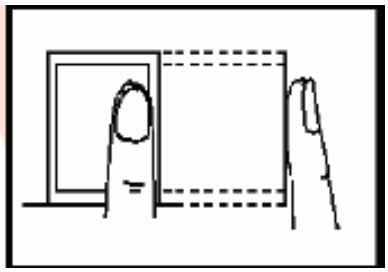




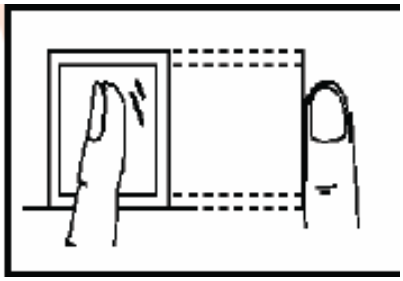
**Posiciones Incorrectas**



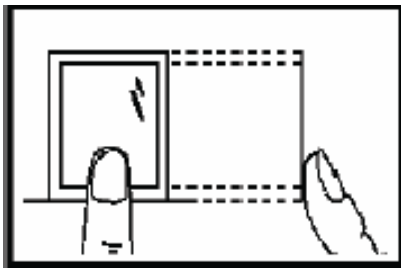
Colocar solo la punta del dedo y topando el cristal.



Colocar el dedo al extremo del sensor



Colocar el dedo de lado



Colocar el dedo muy por debajo del sensor

# BIBLIOGRAFIA


ACHING, J.; ROJAS, D. *"Algoritmos para el Reconocimiento de Imágenes de Huellas Dactilares"*. Revista Electrónica - UNMSM, No. 12, pp. 11-20, 2003.

BAZEN, A; GEREZ, S. *"Segmentation of fingerprint images"*. In Proc. ProRISC2001, 12th Annual Wokshop on Circuits, Systems and Signal Processing, Veldhoven, Netherlands, 240p 2001.

BOBUNG, S. "*Evaluation of Transformation Methods to Detect Structures in Fingerprints*". Bachelor thesis. Technical University of Hamburg-Harburg,874 p, 2002.

CAPELLI, R.; MAIO, D.; MALTONI, D. *"Indexing Fingerprint Databases for Efficient 1:N Matching"*. In Proceedings Int. Conference on Control Automation Robotics and Vision (6th), 642p, 2000.

CEGUERRA, A.; KOPRINSKA, I. *"Integrating Local and Global Features in Automatic Fingerprint Verification"*. In Proceedings Int. Conference Pattern Recognition (16th), vol. 3, pp. 347–350, 2002.

COETZEE, L.; BOTHA, E. *"Fingerprint Recognition in Low Quality Images"*. Pattern Recognition, vol. 26, No. 10, pp. 1441-1460, 1993.

DE LA ESCALERA, A. *"Visión por Computador"*. Prentice Hall, Primera edición, 416 p,2001.

DUDA, R.; HART, P.; STORK, D. *"Pattern Classification"*. Jhon Willey & Sons, inc. USA, 142p, 2001.

FARINA, A.; KOVÁCS-VAJNA, Z.; LEONE A. *"Fingerprint minutiae extraction from skeletonized binary images"*.Pattern Recognition, pp. 877-889, 1999.

GONZÁLES, R.; WOODS, R. *"Tratamiento digital de imágenes"*. Addison-Wesley/Diaz de Santos, 2da. ed, 812 p, 2002.

JAIN, A.; HONG, L.; PANKANTI, S.; BOLLE, R. *"An Identity-Authentication System using Fingerprints"*. Proceedings of the IEEE, vol. 85, No. 9, pp. 1365-1388, 1997.

KASS, M; WITKIN, A. *"Analyzing oriented patterns"*. Computer Vision, Graphics, and Image Processing, vol. 37, No. 3, pp. 362-385, 1987.

KAWAGOE, M; TOJO, A. *"Fingerprint Pattern Classification*". Pattern Recognition, pp. 295–303, 1984.

ACHING, J.; ROJAS, D. "R*econocimiento Biométrico de huellas dactilares y su Implementación en DSP*". Tesis Ing. Electrónico. Lima-Peru. Universidad Nacional Mayor de San Marcos. Facultad de Ingeniería Electrónica. 379 p. 2005.

National Instruments Corporate Headquarters. "NI Vision Assistant Tutorial". Part Number 372228K-01 Austin, Texas. 134 p. 2008

National Instruments Corporate Headquarters. "LabVIEW Tutorial
Manual". Part Number 320998A-01 Austin, Texas. 250 p. 1996

National Instruments Corporate Headquarters. "Introducción a LabVIEW Curso de Seis-Horas". Part Number 323669B-01 Austin, Texas. 93 p. 2003

National Instruments Corporate Headquarters. "Database Connectivity Toolkit User Manual". Part Number 371525A-01Austin, Texas. 66 p. 2008

National Instruments Corporate Headquarters. “IMAQ Vision for LabVIEW User Manual”. Part Number 371007A-01 Austin, Texas. 141 p. 2004

National Instruments Corporate Headquarters. “LabVIEW Fundamentals”. Part Number 374029C-01 Austin, Texas. 165 p. 2007

National Instruments Corporate Headquarters. “NI Vision Concepts Manual”. Part Number 372916G-01 Austin, Texas. 414 p. 2008

# Bibliografía Internet


Huella Digital
http://es.wikipedia.org/wiki/Huella_dactilar
27/05/2009

Reactivación de huellas dactilares sobre superficies adhesivas
http://www.criminalistica.net/forense/podium-forense/dactiloscopia/73-reactivaci-de-huellas-dactilares-sobre-superficies-adhesivas.html
12/06/2009

Manual y Estudio básico de Dactiloscopia**.**
http://www.criminalistaenred.com.ar/index.html
8/07/2009

Comparación de Plantillas de Huella Digital Basadas en Minucias vs. Basadas en Patrones
http://www.criminalistica.com.mx/
12/08/2009

Procesamiento de Imágenes. Filtros
http://www.ayc.unavarra.es/miguel.pagola/procesaminento de imagenes.htm
20/09/2009

Histograma
http://www.santalices.net/cuadernos/histograma/histograma.htm
16/10/2009

Reconocimiento de huellas dactilares
http://pds2006.galeon.com/Cap6.html
05/11/2009

Sensor de huella digital
http://es.wikipedia.org/wiki/Sensor_de_huella_digital
09/12/2009

Algoritmo de Esqueletizacion de Pavlidis
http://jalvarezb.blogspot.com/2008/09/algoritmo-de-esqueletizacion-de.html
5/01/2010

Scanneres en Vivo RealScan-10
http://www.supremainc.com/esp/product/pr_main.php
24/02/2010

Que es un scanner
http://www.monografias.com/trabajos7/scan/scan.shtml
29/02/2010

# Manual del Usuario

# Manual del Usuario

El sistema de autenticación de personal, presenta varias opciones para el usuario y el administrador. A continuación se indica el procedimiento de la operación del software.

Empieza con la ventana principal de operación de interface del usuario.


Como se observa en la figura se tienen dos opciones:

***Inscripción:*** Este botón se utiliza en el caso de que se tiene un nuevo usuario que se ingresa al sistema, es por ello que cuando se da un click en este botón, aparece una nueva ventana en la que se ingresan los datos del nuevo usuario, además de mostrar las huellas que servirán para la posterior comparación.

Es muy importante que se ingresen los datos básicos del usuario, como cedula, nombres y apellidos, ya que en el caso de omitir cualquiera de ellos en el instante de almacenar la información en la base de datos presentara un error.

Para ingresar la cédula se realiza el control respectivo para que ésta sea tomada como válida, es decir que contenga solo números, ningún espacio en blanco ni otros caracteres y que los dígitos estén dentro del rango respectivo, una vez presionado el botón OK, se realiza la verificación y dependiendo de éste, se presentará un mensaje informando al usuario el correcto

o incorrecto ingreso del número. En caso de que haya ingresado mal se da la opción de ingresar nuevamente dicho número hasta que se realice correctamente la operación.


***Verificación:*** Una vez ingresado el número de cédula inmediatamente en forma automática comprueba el sistema si este ese encuentra almacenado en la base de datos, en caso de no ser así nos presenta un mensaje de que el usuario no se encuentra registrado en el sistema, en caso contrario nos presenta un mensaje de ingreso de la huella dactilar en el scanner.

El proceso de captura y procesamiento de la información de la huella del usuario se demora alrededor de 20 segundos, en donde, al final de este tiempo nos presenta un mensaje con el nombre del usuario.