Sistema de verificación de huellas digitales

Tésis de grado

Por

Guido Pusiol

Tésis realizada para la facultad de Matemática, Astronomía y Física (Fa.M.A.F) de la Universidad Nacional de Córdoba, Argentina en orden de cumplir los requerimientos para la obtención del grado de Licenciado en Ciencias de la Computación

28 de septiembre de 2007

Supervisores:
PhD.Daniel Fridlender
Dr.Oscar Bustos

Resumen

Construimos un AFIS basado en reconocimiento de minucias al que llamamos MSAFIS, describiremos los algoritmos necesarios para la construcción del mismo y explicaremos la configuración de los algoritmos en un sistema de tubos y filtros que hacen de MSAFIS un Sistema de verificación de huellas digitales aplicable a las necesidades actuales.
En el trabajo previo se puede encontrar mucha información sobre algoritmos formales y necesarios para la construcción de un AFIS, sin embargo no se encuentra demasiada información sobre como utilizar estos algoritmos para construir un AFIS.
Para esta tesis hemos realizado modificaciones a los algoritmos de la literatura y experimentado distintas secuencias de algoritmos confluyendo en resultados aceptables a los propśitos de un AFIS.
Aportaremos un mecanismo original e implementable de un AFIS que cumple los requerimientos de un sistema “on-line” y presentaremos una variacón para un sistema “off-line”. Con esta tésis pretendemos alcanzar lectores del ambiente teório como práctico formalizando en la medida de lo posible los algorítmos utilizados y considerando las vicisitudes que surgen al llevarlos a la práctica.

Organización del trabajo

En el **Capítulo 1** a modo introductorio presentaremos los conocimientos generales y definiciones de los términos que se utilizarán en la tesis. Describiremos los tipos de AFIS y las motivaciones que nos hicieron converger en el AFIS que presentamos. El **Capítulo 2** denota los algoritmos implementados para la construcción del MSAFIS y presenta las características de funcionamiento del Sisema de verificación. En los capítulos siguentes se describe nuestra aproximación para suplir cada una de las partes de un AFIS típico dividiendo las partes en tres conjuntos actividades. **Capítulo 3** Realce de la imágen que contempla la funcionalidad de mejoramiento de le imagen de huella dactilar para su tratamiento por los algoritmos subsiguientes.**Capítulo 4** Extracción de Minucias explica los mecanismos utilizados para obtener las singularidades de una huella digital.**Capítulo 5** Matching, describirá la funcionalidad de determinar la similitud entre dos huellas dactilares. **Capítulo 6** Clasificación e interacción con la base de datos, proveemos un mecanismo sencillo para la clasificación de las huellas y un método simple para acelerar la busqueda de concordancias 1:n en la base de datos desde el punto de vista de la implementación del MSAFIS **Capítulo 7**Configuración de la construcción de MSAFIS describe la manera secuencial en que MSAFIS dispone de los algorítmos tanto para su utilización .ºn-lineçomo .ºff-line", y presenta los resultados obtenidos para cada configuración.

Índice general

Índice de figuras

Capítulo 1

Introducción

En el mundo digital actual, la certera autenticación personal se ha tornado en una actividad importante en la interfaz computacional y humana. La seguridad Nacional, comercio electrónico, acceso a redes de computadoras son ejemplos en los cuales establecer la identidad de un individuo es de vital importancia. Los métodos de seguridad actuales se basan en aproximaciones bien conocidas como claves, dispositivos magnéticos, documentación son los medios de acceso a espacios físicos o virtuales. Estos métodos no son muy seguros ya que las claves o PIN's pueden ser robados electrónicamente y las tarjetas de acceso pueden ser compartidas o robadas, mas aun, no se puede diferenciar entre individuos con permiso de acceso e individuos en poseción de herramientas para efectuar acceso aunque éstos no esten autorizados. La biometría aplicada a el reconocimiento de huellas dactilares, voz o rostro son herramientas para realizar autenticación de individuos de una manera mas feaciente que los metodos anteriormente mencionados.

1.1. Biometría

Biometría es la ciencia de verificar la identidad de un individuo a travez de medicion fisiológica o de comportamiento. Debido a que los identificadores estan permanentemente con el individuo el método de autenticación es mas confiable que la utilización de métodos basados en el conocimiento o dispositivos externos. La biometría ofrece diversas ventajas sobre las mediciones de seguridad tradicionales. Estos son

1. **No-Repudio:** Con los métodos tradicionales el perpetrador puede siempre negar que ha cometido un crimen objetando que su clave o Identidad había sido comprometida o robada. No hay manera de verificar la veracidad de este tipo de reclamo. Este problema se lo conoce como negación o de repudio. Sin embargo los sitemas biométricos estan relacionados estrictamente con individuo por lo tanto no hay posibilidad ningun robo o prestamo se puede reclamar.

2. **Seguridad y Veracidad:** Los sistemas basados en claves son propensos a ataques de fuerza bruta con utilización de diccionarios de palabras, tales sistemas son tan vulnerables como su clave mas débil. por otro lado la autenticación biométrica requiere de la presencia física del usuario lo que hace que los métodos de ataque del estilo de fuerza bruta sean inoperables. Ha sido demostrado que los sistemas protegidos biométricamente son mas seguros que los sistemas protegidos por claves [1].

3. **No Duplicación:** En muchas aplicaciones estamos interesados en prevenir que un usuario asuma múltiples identidades (e.j. Un terrorista utilice multiples pasaportes para ingresar a un pais extranjero) esto nos obliga a estar seguros que un individuo a ser enrolado no debe poseer una identidad asumida almacenada previamente en la base de datos antes de ingresar el nuevo registro de identidad. Dicho requisito no es posible utilizando los métodos de seguridad tradicionales y los metodos biométricos brindan la unica solucion posible ante el problema.

Las modalidades biométricas pueden ser categorizadas como

- **Biometría física:** Esta modalidad incluye la medición de características físicas de un individuo que pudieran ofrecer características diferenciables del mismo, como ser características de las huellas dactilares, de los iris de los ojos, del rostro, geometria de las manos etc.

- **Biometría de comportamiento:** Este tipo de mediciones estan relacionados con la forma en que un individuo realiza ciertas tareas, como ser su firma, la manera de hablar, la velocidad de tipeo por nombrar algunas.

- **Biometría química:** Este tipo de mediciones estan en desarrollo en la actualidad y estan relacionadas con la composicion quimica de los individuos.

Dependieno de la aplicación los sistemas biométricos pueden ser utilizados para identificación o validación de los individuos. El mecanismo de validación consta de asegurar que el individuo es quien dice ser, el método compara las características biométricas obtenidas del individuo a verificar, con los datos almacenados en la base de datos, correspondientes a quien el individuo dice ser, en caso de encontrar las correspondencias necesarias entre los datos obtenidos y almacenados, el individuo se dará por verificado caso contrario el individuo no sera quien dice ser. Al identificar se obtienen los datos biométricos del individuo y se busca concordancia entre esos datos y los correspondientes a los individuos almacenados en la/s base/s de datos si se encuentran las concordancias necesarias se determina la identidad del individuo.

En esta tésis nos concentramos en el tratamiento de información biométrica de huellas dactilares, en el futuro hablaremos de una huella dactilar refiriéndonos a la imágen digitalizada de la misma. Hay dos operaciones fundamentales necesarias para el tratamiento de información de las huellas dactilares:

- **Enrolamiento:** Consta en la obtención y almacenamiento de la información de las huellas dactilares asociadas con la identidad y datos suplementarios relativos a el individuo portador de la huella dactilar. A ésta huella dactilar o informacion biométrica almacenada la llamaremos template.

- **Verificación:** Consta en la obtención y comparación entre la información de una huella dactilar y la información de huellas dactilares previamente almacenadas en algun dispositivo de almacenamiento, de dicha comparación se obtendrán los resultados necesarios para la identificación o validación de la identidad de un individuo.

1.1.1. Biometría y Reconocimiento de Patrones

Hasta hace poco tiempo la biometría no existia como un campo separado. ha evolucionado a travez de la confluencioa de campos separados. Reconocimiento de huellas dactilares ha evolucionado de el campo de reconocimiento de patrones forenses. Verificaciones de voz ha evolucionado de la comunidad de procesamiento de señales. Deteccion de rostro ha sido investigado ampliamente por la comunidad de vision computacional. Mientras que biometría es principalmente considerado como una aplicacion de tecnicas de reconocimiento de patrones, consta de diferencias substanciales en los problemas de clasificación convencionales.

1.1.2. El Problema de la Verificación

Consideramos el problema de verificación biometrica de una manera mas formal. La señal biométrica de un usuario es comparada con un template simple almacenado. El template es seleccionado basandose en la identidad reclamada por el usuario. Cada usuario i esta representado por la información biométrica Bi. Se asume que hay una correspondencia uno-a-uno entre Bi y la identidad i de el individuo. La la etapa de extracción de características resulta en una representación computacional(template) Ti de la biometría. Duarante la verificación, el usuario aclama una identidad j y provee una señal biométrica Bj. El extractor de características deriva ahora en la correspondente representación computacional Tj de la biométrica. El reconocimiento consiste en computar un valor empirico de similitud al que llamaremos score $S(Ti,Tj)$. La identidad aclamada se asume cierta si $S(Ti,Tj) \geq H$ para algún humbral H. La elección del humbral determina una negociación entre conveniencia del usuario y seguridad del sistema.

1.1.3. Evaluación de performance

A diferencia de claves criptográficas y passwords, los templates biométricos tienen una alta incerteza. Hay una considerable variacione entre las distintas muestras biométricas tomadas del mismo usuario en distintos tiempos. Por lo tanto el proceso de busqueda de concoedancias (matching) se realiza siempre

de una manera probabilística. Esto es opuesto a el match exacto requerido por las aproximaciones basadas en claves o tarjetas electrónicas. En el futuro utilizaremos los términos huellas dactilares o huellas digitales indistintamente.La inexactitud en el matching nos lleva a tener dos tipos de errores

- **Falsa Aceptación** comunmente llamado falso positivo, y es el caso en que un usuario es aceptado como un usuario genuino, y esto ocurre cuando la muestra biométrica de un usuario cae dentro de la posibe variación de la muestra de un usuario genuino.

- **Falso Rechazo** o también conocido como falso negativo, que ocurre cuando la muestra es de baja calidad incluso un usuario genuino puede ser rechazado durante la autenticación.

- **Falla al enrolar** se estima que el 4 por ciento de la población tiene huellas digitales ilegibles. Este porcentaje se centra en personas mayores y en personas que utilizan mucho sus manos para trabajar y han sufrido lesiones en ellas. Debido a la pobre estructura de los surcos de estos individuos, tales usuarios no pueden ser enrolados en la base de datos y por lo tanto no pueden ser subsecuentemente autenticados. tales individuos se los denomina gotas (goats) [2]. Un sistema biométrico debe tener un mecanismo de control de excepciones para lidiar con dicho problema.

- **Falla al autenticar** este error ocurre cuando el sistema no tiene la capacidad de extraer mlas características necesarias durante la verificación por mas que la biometría había side legible durante enrolamiento. En el caso de las huellas dactilares esto puede ser causado por intenso sudor en las manos, tener una herida reciente etc. hay que notar que este tipo de error es distinto del falso rechazo ya que en falso rechazo el error ocurre en la etapa de matching, mientras que el error falla al autenticar ocurre en la etapa de extracción de características.

1.2. Huellas dactilares como Biometría

Las huellas dactilares han sido aceptadas formalmente como un sistema de identificación de personas valido, a principios del siglo veinte, desde ese entonces se ha convertido en la técnica de-facto para la autenticación en las agencias relacionadas con la seguridad mundialmente. El FBI actualmente mantiene mas de 400 millones de registros de huellas dactilares. Las huellas dactilares tienen varias ventajas sobre otros sistemas biométricos, como ser:

1. **Universalidad:** La gran mayoría de la población humana y por lo tanto puede ser facilmente autenticada. Esto esto excede la cantidad de la población que posee pasaportes, documentos de identidad o cualquier otra forma de identificación.

2. **Alta Distintividad:** Incluso gemelos idénticos que comparten el mismo ADN muestrn tener distintas huellas dactilares, debido a que la estructura de las crestas de los dedos no esta codificado en los genes de un individuo. Por esto las huellas dactilares representan un mecanismo de autenticacion mas fuerte que el de reconocimiento de ADN. Mas aún, no hay evidencia de huellas dactilares idénticas en mas de un siglo de practicas forenses. hay modelos matemáticos [3] que justifican la alta distintividad de los patrones de los dedos.

3. **Alta Permanencia:** Los patrones en la superficie de las estructuras de los dedos se crean en el nacimiento y se mantienen hasta la muerte de un individuo.

4. **Fácil recolección:** El proceso de colectar huellas dactilares se ha convertido en un proceso muy sencillo con los sensores actuales. los sensores son capaces de capturar imágenes de alta resolución de una huella dactilar en un tiempo inferior a un segundo. El proceso de colección de las huellas se puede implementar tanto con usuarios que cooperen como con los que no cooperen. Otros sistemas como el reconocimiento de iris necesita que los usuarios sean cooperativos ante la recolección de la información biométrica.

5. **Alta performamce:** Las huellas dactilares se mantienen como la modalidad biométrica mas acertada disponible en la actualidad considerando la tasa de falsos rechazos y la taza da falsos positvos.

6. **Alta aceptación:** Comparado con los otros métodos biométricos los usuarios demuestran tener mejor aceptación a la hora de insertar sus huellas dactilares en bancos de datos para su autenticación que con métodos aún en desarrollo.

La superficie de las huellas digitales esta formada por un sistema de valles y crestas que sirven como superficie de fricción en el momento de tomar objetos. Denominamos indistintamente a zurcos o valles a las líneas determinadas por las profundidades oservables en una huella digital, y llamamos crestas o picos a las líneas de la huella digital determinada por las altitudes en la huellas dactilar. La superficie exhibe información estructural muy rica de información cuando se la examina como una imágen. las imágenes de huellas digitales pueden ser representadas como características globales asi tambien como características locales. las características globales incluyen la distancia entre las líneas de las crestas, orientación de las crestas y puntos singulares como core y delta. Los puntos singulares tienen una gran importancia desde el punto de vista de clasificación de las huellas digitales. Sin embargo la vericación generalmente utiliza exclusivamente características locales llamadas minucias, decimos generalmente debido a que presentaremos en este trabajo otro tipo de algoritmo que no utiliza las minucias para realizar verificación. Sin embargo nuestro algoritmo utilizará las minucias para realizar verificación, la minucias son características de la huella

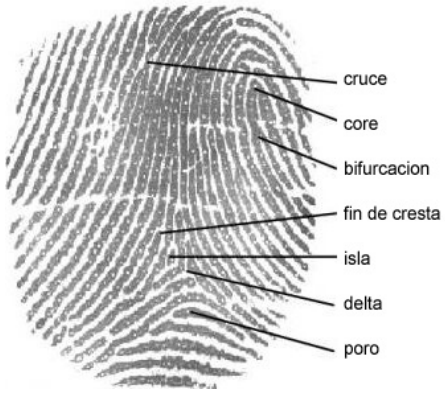

Figura 1.1: Caracteísticas globales y locales de una huella digital

determinadas por discontinuidades de las líneas de la superficie de una huella digital. Hay alrededor de 18 tipos distintos de minucias que incluyen fines de líneas, bifurcaciones, islas, cruces. Sin embargo los *fines de líneas* y *bifurcaciones* son los tipos de minucias comunmente utilizados en los procesos de verificación. un fin de línea ocurre cuando el flujo de una línea termina abruptamente y una bifurcación es determinada cuando se da una division en la línea de la superficie de la huella dactilar. Al hablar de líneas nos referimos al flujo de crestas o de valles que determinan la estructura de una huella dactilar, es indistinto hablar de una línea de crestas o una línea de valles ya que las minucias encontradas en una huella dactilar proveniente de una línea de crestas son las mismas a las que se encuentran trabajando la imájen con su correspondiente línea de valles, la diferencia única radica en que el tipo de minucias encontradas resulta ser exactamente la opuesta. Las características globales no poseen suficiente poder discriminativo por si solas, es por eso que comunmente se utilizan para clasificar el tipo de huella dactilar en lugar de verificar. Al hablar de clasificación nos referimos a un método para etiquetar los distintos tipos de huellas dactilares, esta etiquetación se utiliza para realizar de manera mas eficiente la busqueda en bases de datos con muchos registros, y realizar una verificación en un menor tiempo computacional. En este trabajo no clasificaremos a las huellas dactilares por medio de sus características globales sino que lo realizaremos directamente por la cantidad de minucias locales que cada una de las huellas dactilares posee.

1.3. Un AFIS minutiae-matching Típico

Las etapas de un sistema típico de reconocimiento de huellas digitales se muestran en la figura 1.2 La imágen es adquirida en la primera etapa, esta adquisición se puede realizar por diversos métodos como ser la creación de una imagen digitalizada de una huella digital previamente ubicada en tinta sobre

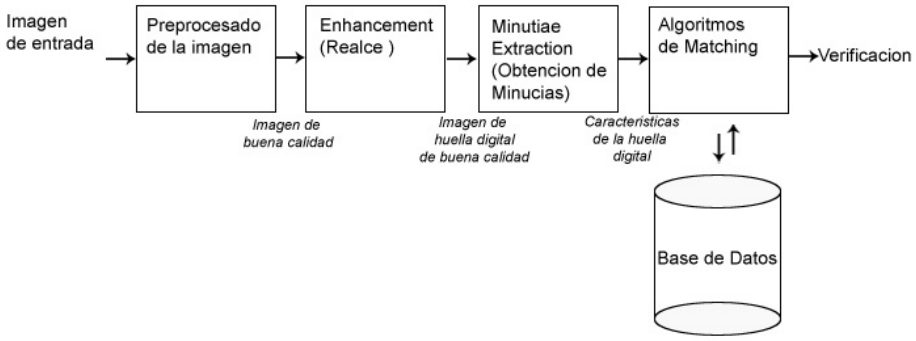

Figura 1.2: Representación típica de la etapa de verificación de un AFIS minutiae-matching

papel, o a travez de un sensor de lectura de huella digitales optico, capacitivo de ultrasonido o térmico. En éste trabajo hacemos énfasis en los sensores ópticos y de una marca en particular ya que ha sido nuestra herramienta de captura de imagenes con la que hemos construido el algoritmo de verificación.
A una imágen de huella digial se le aplica un preproceso de la imagen lo que mejorará de manera global la imagen y la normalizará para tener compatibilidad entre los distintos dispositivos de captura, este preprocesado se realiza con métodos convencionales de tratamiento de imágen como lo son el cambio de contrastes, luminosidad, eliminación de ruidos, suavizado etc.
A una imágen preprocesada se le aplican métodos para la mejora en las estructuras de las líneas de la imágen de huella digital, los métodos utilizados en la etapa de realce de la imágen generalmente son metodos construídos particularmente para el tratamiendo de imágenes de huellas digitales diseñados para explotar la naturaleza periódica y direccional de las líneas. La imagen realzada se la pasa por un mecanismo de detección de minucias, cuando estas son extraídas se representan las minucias y sus características en forma de grafo relacional el cual es utilizado en la última etapa por los algoritmos de matching para encontrar concordancias con los templates almacenados en la base de datos y asi realizar la verificación (1:n). En la figura 1.3 se puede ver el esquema de bloques de la operación de enrolamiento de un AFIS minutiae- matching típico. La operación de enrolamiento es consecuencia directa de la operación de verificación ya que se utilizan los mismos métodos hasta pasar la etapa de esxtracción de características, es aqui cuando la interacción con la base de datos es unidireccional almacenando en ella el grafo de minucias obtenido, este grafo de minucias debe

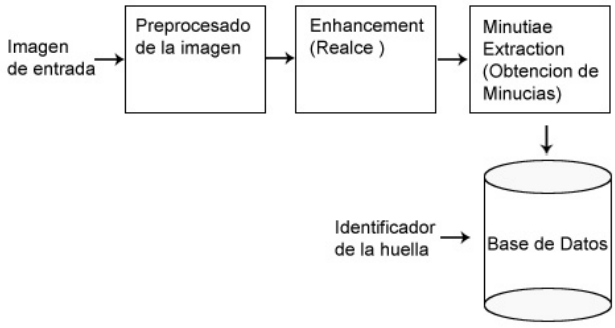

Figura 1.3: Representación típica de la etapa de enrolamiento de un AFIS minutiae-matching

estar acompañado por un identificador del mismo, es decir un atributo del grafo que indique la procedencia de la huella digital a enrolar. Generalmente en la base de datos y acompa´ nando al identificador se guardan otros atributos que le dan una funcionalidad particular al AFIS, pero estos atributos dependen de la aplicación que se quiera construir con el AFIS, por lo tanto para dar una descripción general del funcionamiento del mismo consideramos que es suficiente un identificador de la huella digital a enrolar.

1.4. Sensores de huellas digitales

Tradicionalmente las huellas digitales se adquieren al transferir una impresion de tinta de una huella digital al papel. Este proceso es denominado acquisicion off-line. Los sitemas de autenticación existentes estan basados en dispositivos que realizan la acquisición de la imagen de la huella dactilar en tiempo real, este proceso es denominado live-scan. Los dispositivos para realizar live-scan suelen estar basadon en uno de los siguientes esquemas de sensores.

1. **Sensores Ópticos:** Es la tecnología mas vieja y mas usada. En la mayoría de los dispositivos, en la malloria de los casos poseen un dispositivo charged couple device (CCD), que convierte la imagen de la huella digital, con oscuras crestas y valles luminosos, en una senal digital. Estos dispoitivos tienen bajo costo en el mercado y alcanzan a proveer de una resolución de la imagen de huella digital adquirida de mas de 500 dpi.

2. **Sensores Capacitivos:** Un sensor de silicona actúa como un extremo del capacitor y el dedo a extraer la huella digital como el otro extremo. La capacitancia entre entre el el sensor y el dedo depende inversamente de la distencia entre ellos. Dado que las crestas estan mas acercadas al

sensor les corresponde una mayor capacitancia y a los surcos por ser los mal alejados una menor capacitancia. Esta variación es convertida en una imagen digital en escala de gises de 8-bits.

3. **Sensores de Ultrasonido:** Ultrasonido es quizas la tecnología con mayor nivel de certeza dentro de las tecnologías de sensado de huellas dactilares. utiliza ondas de ultrasonido para medir la distancia, basandose en la impedancia de los dedos. Los sensores son capaces de otorgar imágenes de muy alta resolución.

4. **Sensores Térmicos:** Estos sensores estan construidos por materiales pyro-eléctricos cuyas propiedades cambian con la temperatura. Dado que la huella digital esta estirada en el sensor, existem diferencias en la conducción de calor entre los valles y las crestas. Estos sensores adquieren pequenas zonas transversales de la huella digital. Dado que la piel adquiere equilibrio térmico en poco tiempo una vez apollado el dedo en el scaner. Un scaner térmico que cubra toda la dimensión de la imágen sería poco práctico ya que el rápido equilibrio térmico lleva al scaner a una caida de la senal a medida que pasa el tiempo hasta perderla por completo una vez que se estabilizo la temperatura, para solucionar este prolema se debería ir variando la temperatura del scaner y esto lleva a una ineficiencia energética del scaner. Esta tecnología adquiere imágenes con alto contraste lo que es bueno en términos del tratamiento de la imágen, sin embargo debido a que el scaner solo puede adquirir pequenas zonas de la huella por cada proceso de adquisición, obterner unaimagen de tamano completo de la huella digital es complejo debido a que tras la adquisición de todas las zonas de la huella hay que proceder con la reconstrucción de la imágen uniendo las zonas adquiridas.

1.5. Representación de la huella digital y algoritmos de matching

Hay que describir la compraracion entre los AFIS basados en MInutiae - matching y los de comparación directa de imágenes algorítmo SIFT

Capítulo 2

Vista Previa del MSAFIS

MSAFIS es un AFIS basado en minutiae-matching, para describirlo se ha seccionado las etapas de un AFIS minutiae matching típico describiendo los algoritmos competentes a cada etapa. En la figura 22 se observa la división en etapas del MSAFIS y los algoritmos implementados y probados en cada una de ellas.

Las Imágenes de entrada:
Para la construcción y evaluación de MSAFIS se ha utilizado iágenes obtenidas por un sensor óptico comercial *(Microsoft Fingerprint Reader)* debido a que es el mas difundido en el mercado y es el que se consigue con mayor facilidad. Para su uso se ha desarrollado un driver capaz de adquirir imágenes de este dispositivo y pasarlas al software de resultado de la implementación de MSAFIS. Se considera que la imágen de entrada es de una resolución de 500 dpi y cada píxel puede tener un valor entre 0 y 255, es decir una imágen de 8-bits en escala de grises debido a que es un standar y es el tipo de imágenes que se pueden obtener en la actualidad de sensores ópticos.

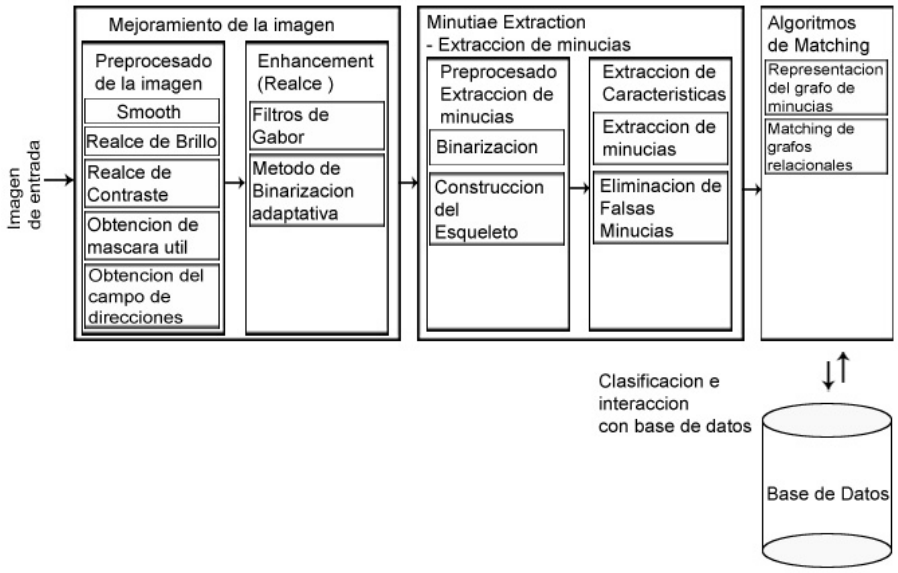

Figura 2.1: Representación típica de la etapa de enrolamiento de un AFIS minutiae-matching

Capítulo 3

Mejoramiento de la imágen

Esta es la etapa primera del AFIS la cual hemos subdividido en dos secciones. El preprocesado de la imágen tratará a la imágen de entrada con un conjunto de algoritmos típicos del tratamiento de imágenes con la finalidad de preparar la imágen para algoritmos subsiguientes y debido a que la imágen de entrada puede provenir de distintas fuentes en el preprocesado se contempla la normalización de la imagen. El Realce de la imágen consta de un conjunto de algoritmos diseñados particularmente para el mejoramiento de huellas digitales aprovechando la estructura propia de las líneas de una huella digital con la finalidad de unir y realzar líneas de la imágen de entrada.

3.1. Preprocesado de la imágen

Notación:

Una imágen en escala de grises,I , es definida como una matriz *NxN*, donde *I(i,j)* representa la intensidad del pxel en la i-ésima fila y la j-ésima columna. Las imgenes escaneadas tienen una resolución de 500 dpi (puntos por pulgada) debido a que es lo recomendado por el FBI (USA), y es la resolución estándar que actualmente se utiliza para el estudio de Huellas Digitales.
La media y la varianza de una imagen en escala de grises, I esta dada por:

$$M(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i,j) \tag{3.1}$$

$$VAR(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} (I(i,j) - M(I))^2 \tag{3.2}$$

Una imagen de orientación, O, es definida como una matriz $N\ x\ N$, donde $O\ (i,j)$ representa la orientación local del borde en un píxel $I(i,j)$. Bordes

locales son normalmente especificados por bloque en lugar de hacerlo en cada píxel; una imagen es dividida en un conjunto de w x w bloques que no se sobreponen entre ellos, y una orientación simple de un borde está definida por cada bloque. Notar que en una imagen de huella digital no hay diferencia entre un borde con orientacin de 270 y 90 grados, debido a que bordes orientados a 90 grados y bordes orientados a 270 en un vecindario local de bordes no se pueden diferenciar entre ellos.

Una Imagen de frecuencia, *F*, es una imagen *N x N*, donde *F(i,j)* representa la frecuencia de borde local, la cual está definida como la frecuencia del borde y estructura de surco en un vecindario local a lo largo de una dirección normal a la orientacin de borde local. Las estructuras de borde y surco en un vecindario local donde las minucias suelen no formar una forma sinusoidal bien definida, en tales casos la frecuencia es definida como el promedio de las frecuencias de sus vecinos.

La mscara de región útil, *R*, es una imagen *N x N* donde *R(i,j)* indica la categoría de un píxel. Un píxel puede ser:

1. Píxel inútil
2. Píxel útil

Llamammos un píxel inútil cuando éste se encuentra en una región de la imágen de baja calidad que afecta el procesamiento de los algoritmos, las secciones de la imágen compuestas por píxeles inútiles son evitadas por los algoritmos. Pixel útil son aquellos que seran procesados por los algorítmos.

3.1.1. Eliminación de ruido restante en el sensor

Debido a que para este proyecto construimos un controlador del sensor óptico, es que se cuenta con la facilidad de explotar su funcionalidad.
En la práctica al utilizar un sensor óptico de manera continua se acumula grasa sobre el lente del sensor, esta grasa es proveniente de los dedos que son continuamente sensados y tiene la propiedad de amoldarse cada vez que se coloca un dedo en el sensor a la forma de la huella digital del dedo sensado. Si bien esta capa de grasa es levemente visible al ojo humano la sensibilidad del scaner la detecta fácilmente, lo que genera un ruido innecesario al colocar un nuevo dedo sobre el lente, sobre todo en las regiones del lente no cubiertas por el dedo que se intenta sensar.

Por lo tanto una manera sencilla de minimizar este ruido y que hemos implementado es la de mantener una copia actualizada de cualquiera fuera la forma dejada por la grasa en el sensor en el último scan, asi al obtener una nueva imágen poder restar la imágen obtenida con la forma sombra que el lente mantenía previo al último scan. Logrando minimizar el ruido propio de la utilización del sensor.

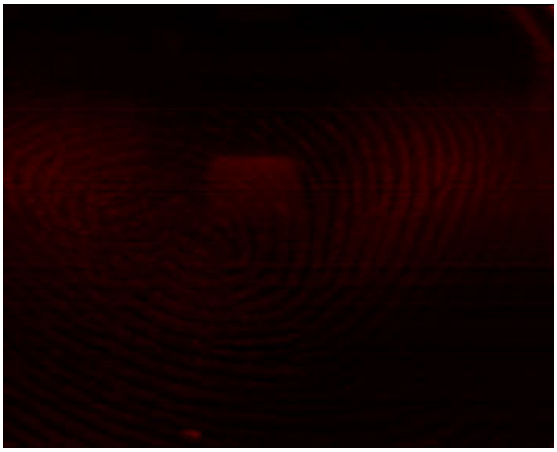

Figura 3.1: Imágen de grasa remanente en el sensor

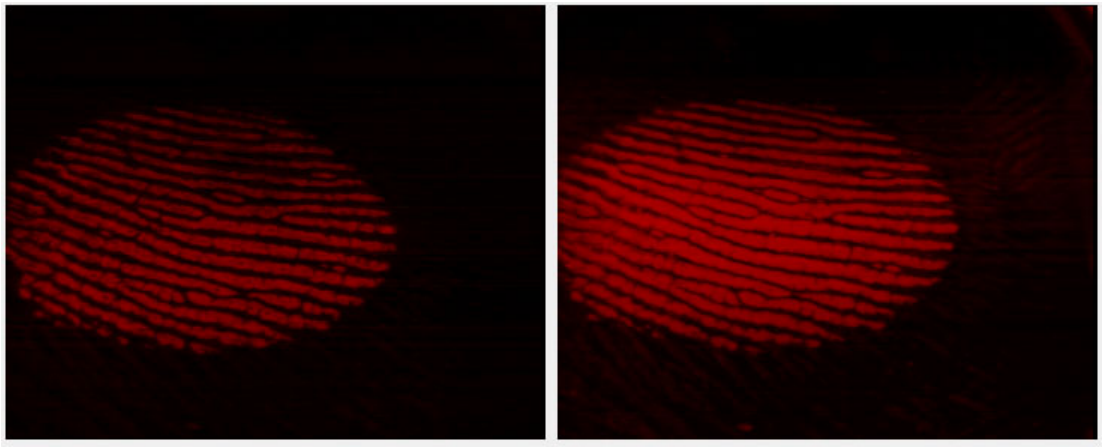

Figura 3.2: Comparación de imágenes escaneadas, Izquierda: Imágen con eliminación de grasa. Derecha: Sin eliminación de grasa

3.1.2. Invertir una imágen en escala de grises

Debido a que en la práctica manejaremos imágenes en escala de grises es útil el algoritmo que invierte el valor de los píxeles de la imágen dentro del rango 0-255 que son los posibles valores que el píxel puede tener. Sea I una imágen de entrada I(x,y) el valor del píxel en las coordenadas (x,y), sea R la imágen resultado de realizar la inversa de la imágen I, entonces

$$R(x, y) = 255 - I(x, y) \tag{3.3}$$

para cada píxel de la imágen.

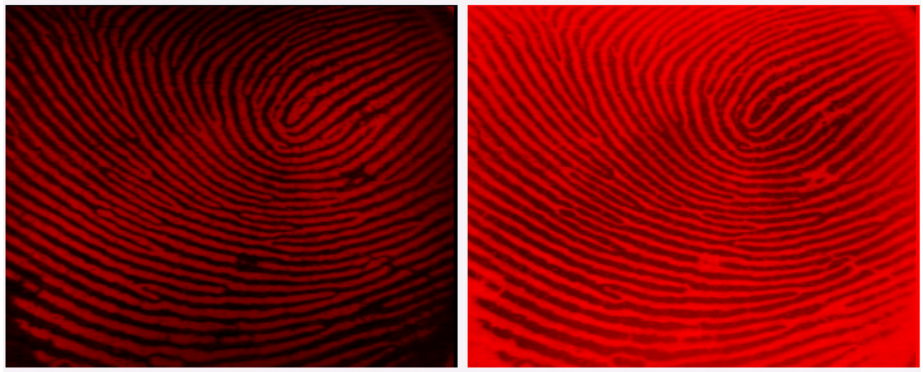

Figura 3.3: Resultado de Inversión de la imágen: Derecha, imágen de entrada. Izquierda imágen resultado de la aplicación del algoritmo a cada uno de sus píxeles.

3.1.3. Realce de contraste

Este este algorítmo realza de manera inteligente el contraste de una imágen de entrada, la idea es la de dividir la imágen de entrada en bloques no solapados de tamaño fijo **w** x w y a cada uno de esos bloques realizarles un estiramiento de el histograma forzando que el histograma resultante cubra el rango [0,255] de valores posibles.
Debido a la naturaleza de las imagenes digitalizadas la distribución de los valores de los píxeles representantes de zurcos y crestas varía en las distintas secciónes de la imágen, de esta observación se desprende la necesidad de que el estiramiento del histograma completo de la imágen sea la consecuencia del estiramiendo local de cada uno de los bloques no solapados en los que hemos dividido la imágen.
Para la implementación del algoritmo hay que tener en cuenta que la selección del tamaño de los bloques genera una zona que queda fuera de la grilla de bloques sobre la imágen, esto se puede solucionar utilizando bloques fijos de tamaño lxs donde:

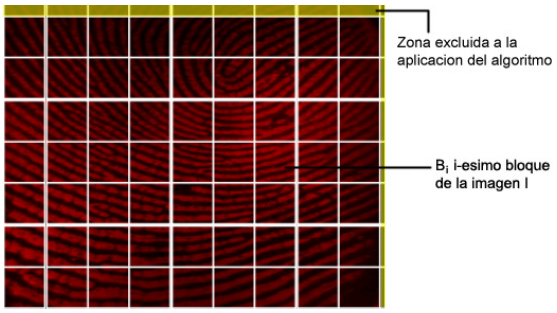

Figura 3.4: División en bloques no sobrelapados de la iágen de entrada

$$0 \equiv I_{width} mod(l)\ y \tag{3.4}$$

$$0 \equiv I_{height} mod(s) \tag{3.5}$$

Sin embargo en la práctica encontramos que no es necesario debido a que generalmente los bordes de la imágen no poseen información relevante, sin enbargo es correcto distribuir equitativamente la zona perdida en los bordes, haciendo haciendo que la grilla de bloques este alineada con el centro de la imágen.

Algoritmo

```
Imput: B - bloque de la imagen, T tolerancia
Output: B' bloque resultado

 1. i=0, j=0, s=0, m=wxw, S=0, M=0
 2. Calcular el histograma de B y almacenarlos en h[0...255]
 3. Calcular A:
    Si S >= Tolerancia, A=s e ir a 4.
    Si S < Tolerancia , S=S+h[s], s=s+1 ir a 3.
 4. Calcular B:
    Si M >= Tolerancia, B=m e ir a 5.
    Si M < Tolerancia, M=M+h[m], m=m-1 ir a 4.
 5. Calcular el nuevo valor del pixel para cada pixel del bloque B
     B'(i,j)=A  Si B(x,y)<A
     B'(i,j)=B  Si B(x,y)>A
     B'(i,j)= floor((B(x,y)-A).255)/(B-A) si no se da ninguna de las anteriores
 6. Si i != w, i= i+1 ir a 5.
    Si i  = w, continuar.
 7. Si j != w, j= j+1 ir a 5.
    Si j =w, devolver B y terminar.
```

3.1.4. Normalización

Sea I una imágen, dejemos que *I(i,j)* denote el valor en la escala de grises en el píxel *(i,j)*,M 3.1, y Var3.2 denotan la media y varianza de la imagen I,Sea G la nor-

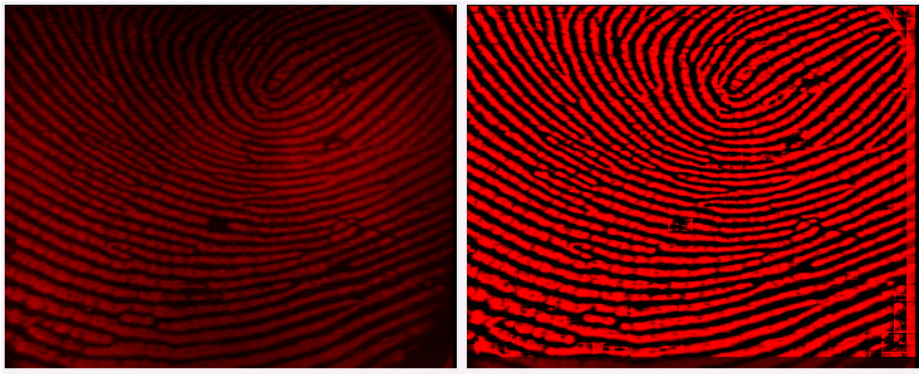

Figura 3.5: Resultado de Local Stretch: Izquierda, imágen de entrada. Derecha, resultado de la aplicación del algoritmo con tolerancia = 20 y w = 10 píxeles

malización de la imágen *I. G(i,j)* denota el valor normalizado del píxel *(i,j)*. La imágen normalizada se define:

$$G(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{VAR_0(I(i,j)-M)^2}{VAR}} & si I(i,j) > M \\ M_0 - \sqrt{\dfrac{VAR_0(I(i,j)-M)^2}{VAR}} & caso\, contrario, \end{cases} \tag{3.6}$$

Donde M_0 y VAR_0 son la media y varianza deseada. El propósito principal de realizar la normalización es el de reducir las variaciones de nivel de gris, los valores de los bordes y surcos, lo que facilita procesos subsiguientes.Asi también desde la perspectiva de la implementación de un AFIS donde las imágenes a tratar por el sistema pueden provenir de distintos medios la normalización estandarizará las imágenes haciendo que los resultados del tratamiento de imágenes provenientes de distintos medios sea posible.

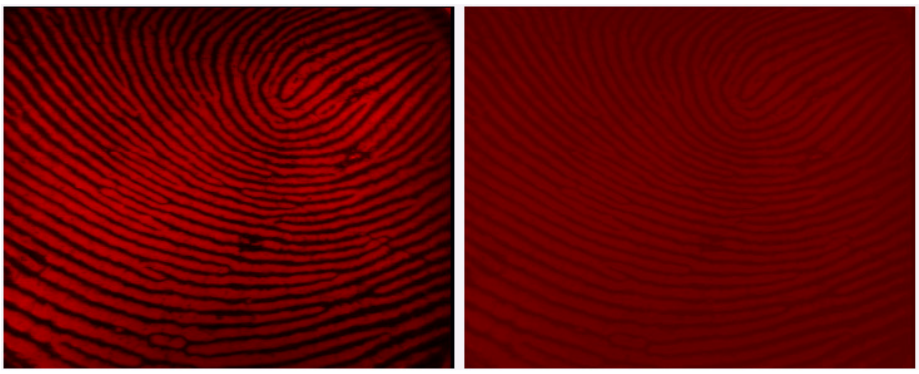

Figura 3.6: Resultado de Normalización: Izquierda, imágen de entrada. Derecha, resultado de la aplicación del algoritmo con $M_0 = 100$ y $VAR_0 = 100$

3.1.5. Obtención del campo de Frecuencias

En un vecindario local donde no existen puntos singulares ni minucias. Los niveles de gris a través de los surcos y bordes pueden ser modelados como formas sinusoidales a travs de la dirección normal a la orientación local de los bordes de una imagen de Huella digital. Dejemos que sea G la imagen normalizada, O la imagen orientada; entonces los pasos involucrados en la estimación de frecuencia de bordes está dada por:

1. Dividir G en bloques de tamao w x w
2. Para cada bloque centrado en el píxel *(i,j)*, computar una ventana orientada de tamao l x w *(32 x 16)* que esté definido en el sistema de coordenadas de bordes.
3. Para cada bloque centrado en *(i,j)*, computar la firma-X, *X[0],X[1],..X[l-1]* de bordes y surcos dentro de la ventana orientada, donde:

$$X[k] = \frac{1}{q}\sum_{d=0}^{w-1} G(u,v),\ k = 0, 1, ..., l-1 \tag{3.7}$$

$$u = i + (d - \frac{w}{2})cosO(i,j) + (k - \frac{l}{2})sinO(i,j), \tag{3.8}$$

$$v = j + (d - \frac{w}{2})cosO(i,j) + (\frac{l}{2} - k)cosO(i,j) \tag{3.9}$$

Si no se encuentran minucias y puntos singulares en la ventana orientada, la firma-X presenta una forma de onda sinusoidal discreta, que tiene la misma frecuencia que los surcos y bordes en la ventana orientada. Por lo tanto, la frecuencia de los bordes y surcos puede ser estimada por la firma-X. Consideremos que *T(i,j)* es el número promedio de píxeles entre dos picos en la firma-X, entonces la frecuencia, $\Omega(i,j)$ es computada como $\Omega(i,j) = 1/T(i,j)$.,si no hay picos consecutivos en la firma-X, entonces se asigna el valor de -1 para diferenciarla de valores válidos de frecuencia.

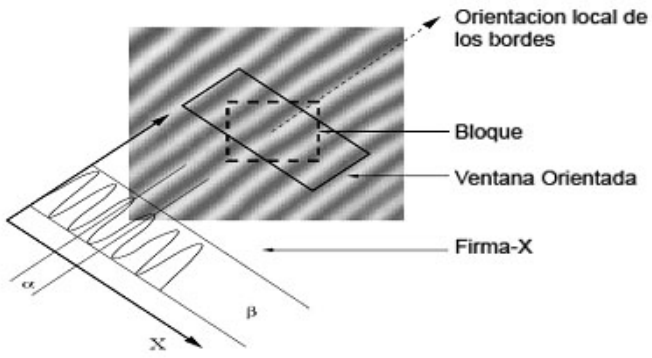

Figura 3.7: Ventana Orientada y firma-X

4. Los bloques en los que minucias y/o puntos singulares aparecen, y/o además bordes y surcos estan corruptos, no forman una onda sinusoidal correctamente definida. Los valores de frecuencia de estos bloques necesitan ser interpolados a partir de las sinusoides pertenecientes a los bloques vecinos cuya frecuencia esta certeramente definida. Así realizamos la interpolación:

   a) Para cada bloque centrado en (i,j):

$$\Omega\,'(i,j) = \begin{cases} \Omega(i,j); & si\ \Omega(i,j) \neq 0 \\ \dfrac{\sum_{u=-w_{\Omega/2}}^{w_{\Omega/2}} \sum_{v=-w_{\Omega/2}}^{w_{\Omega/2}} W_g(u,v)\mu(\Omega(i-uw, j-uw))}{\sum_{u=-w_{\Omega/2}}^{w_{\Omega/2}} \sum_{v=-w_{\Omega/2}}^{w_{\Omega/2}} W_g(u,v)\delta(\Omega(i-uw, j-uw)+1)} & caso\,contrario, \end{cases}$$

   donde,

$$\mu(x) = \begin{cases} 0, & si\, x \leq 0 \\ x, & cc, \end{cases}$$

$$\delta(x) = \begin{cases} 0, & si\, x \leq 0 \\ 1, & cc, \end{cases}$$

   W_g es un kernell Gauseano discreto con Media y Varianza 0 y 9 respectivamente, y w_Ω es el tamao del kernell.

   b) Si existe al menos un bloque con frecuencia con valor -1, entonces intercambiar Ω con Ω' e ir nuevamente a (a).

3.1.6. Suavizado - Smoothing

Para realizar el suavizado de la imágen utilizaremos un algoritmo simple que se basa en hacer el promedio de los valores de los píxeles de una ventana de tamaño s x s centrando la ventana en el píxel que se le realizará el suavido, en la implementación hay que tener en cuenta que el valor de s elegido debe ser impar para que al centrar la ventana en cada píxel la distancia entre éste y los bordes de la ventana sea el mismo en cualquier dirección.
Entonces sea I una imágen y S la imágen resultado del suavizado, el valor del píxel $S(x,y)$ es :

$$S(x,y) = (\sum_{i=x-s}^{x+s} \sum_{j=y-s}^{y+s} I(i,j))/s^2 \tag{3.10}$$

Al aplicar el procedimiento a cada uno de los píxeles de la imágen obtenemos una imágen suavizada.

3.1.7. Obtención de campo de direcciones

El campo orientación representa la orientación local de las bordes que contiene la huella. Para estimarlo, la imagen se divide en bloques de 16x16 pxeles y se calcula la inclinación para cada píxel, en coordenadas x e y. El ángulo de orientación se calcula a

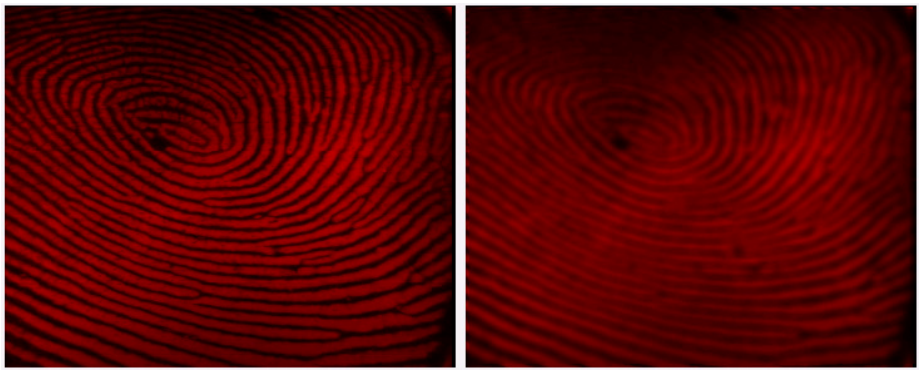

Figura 3.8: Resultado de Suavizado: Izquierda, imágen de entrada. Derecha, resultado de la aplicación del algoritmo con s=7

partir de la informacin de la inclinación. Frecuentemente, en algunos bloques, el ángulo de orientacin no se calcula correctamente debido a ruidos y daños en los valles y las bordes de la imagen capturada.

Algoritmo

1. Dividir G (la imagen preprocesada) en bloques de tamaño w x w (16 x 16) pxeles.
2. Computar los gradientes $\delta x_{i,j}$ y $\delta y_{i,j}$ en cada uno de los pxeles *(i,j)*. Dependiendo del costo computacional requerido el operador de gradiente puede variar desde el de Sobel hasta uno complejo como el de Marr-Hildreth.
3. Estimar la orientacin local de cada bloque centrado en el pxel *(i,j)* usando: Utilizando:

$$V_x = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} 2\delta_x(u,v)\delta_y(u,v) \tag{3.11}$$

$$V_y = \sum_{u=i-\frac{w}{2}}^{i+\frac{w}{2}} \sum_{v=j-\frac{w}{2}}^{j+\frac{w}{2}} (\delta_x^2(u,v) - \delta_y^2(u,v)) \tag{3.12}$$

$$\theta(i,j) = \frac{1}{2} tan^{-1}(\frac{V_y(i,j)}{V_x(i,j)}) \tag{3.13}$$

   Donde $\theta(i,j)$ representa la dirección ortogonal a la dirección dominante en el espectro de la transformada de Fourier dela ventana de tamaño w x w.
4. Aplicar un filtro pasa-bajo para corregir la orientación local que pudiera haberse visto afectada por ruido en la imagen, para hacer esto la imagen de orientacin debe ser convertida en un campo vectorial, definido como:

$$\phi_x(i,j) = cos(2\delta(i,j)), y \tag{3.14}$$

$$\phi_y(i,j) = sin(2\delta(i,j)), \tag{3.15}$$

donde δ_x y δ_y son los componentes x e y del campo vectorial, respectivamente. Con el campo vectorial obtenido, el filtro pasa-bajo se puede implementar de la siguiente manera:

$$\Phi_x^{'}(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_x(i-uw, j-vw)y \tag{3.16}$$

$$\Phi_y^{'}(i,j) = \sum_{u=-w_\Phi/2}^{w_\Phi/2} \sum_{v=-w_\Phi/2}^{w_\Phi/2} W(u,v)\Phi_y(i-uw, j-vw)y \tag{3.17}$$

donde W es un filtro pasa bajo de dos dimensiones.

5. Por último la orientación local en el punto (i,j) usando:

$$O(i,j) = \frac{1}{2}tan(\frac{\Phi_y^{'}(i,j)}{\Phi_x^{'}(i,j)}) \tag{3.18}$$

3.1.8. Obtención de máscara útil

Debido a que la imagen contiene ruido de fondo, el algoritmo de realce puede generar minucias fuera del área ocupada por la huella así como generar falsos surcos en zonas de la huella de baja calidad.
Para evitar este problema, presentamos dos algorítmos que obtienen de la iágen la zona abarcada por la huella digital.
El **Algorítmo 1** es propuesto por ... y si bien en la implementación nos ha dado resultados aceptables, consideramos que el tiempo computacional requerido para su ejecución noes aplicable para un sistema **on-line**, es por esto que se utiliza en la configuración **off-line** de MSAFIS, para la ejecución **on-line** de MSAFIS desarrollamos **Algoritmo 2**, un simple mecanismo de detección de la zona de la imágen de entrada ocupada por la huella digital, el algoritmo no verifica las regiones inútiles de la misma huella debido a que en la práctica encontramos no era necesario para el mecanismo de obtención de la imagen que utilizamos.

Algoritmo 1 Se selecciona el rea de imagen, definida por todos los bloques de tamaõ wxw, en la que existe una alta variación del nivel de grises en la dirección normal de las bordes existentes (el campo orientacin normal de las bordes se haba calculado previamente). Después de esto el área de la imagen con ruido, que será excluido en las siguientes etapas, se define por bajas variaciones en todas las direcciones.
Como se mencionó anteriormente, un píxel (o un bloque) en una imagen de entrada puede estar en una regin til o una regin inútil.
La clasificacin de píxeles en las categorías de útiles o inútiles se realiza en base a la forma de la onda formada por los bordes y surcos locales. En este algoritmo, tres propiedades son usadas para caracterizar la forma de onda sinusoidal: amplitud (α), frecuencia (β) y variancia (γ).
Dejemos que R sea la iágen de la máscara de región útil. Dejemos que *X[1], X[2],..., X[l]* corresponda a la firma-X de un bloque centrado en *(i,j)*.
Las tres caractersticas correspondientes a un pxel (bloque) *(i,j)* se computan:

Sean,
Θ = Promedio del ancho de los picos.
Ξ = Promedio de la profundidad de los valles.

$$\alpha = \Theta - \Xi \tag{3.19}$$

$$\beta = \frac{1}{T(i,j)} \tag{3.20}$$

T(i,j) es el número promedio de píxeles entre dos picos consecutivos.

$$\gamma = \frac{1}{l}\sum_{i=1}^{l}(X[i] - (\frac{1}{l}\sum_{i=1}^{l}X[i]))^2 \tag{3.21}$$

Ahora corriendo un algoritmo de *clustering*, conseguiremos la imagen R donde *R(i,j)=1* si el bloque es til, *R(i,j)=0* si el bloque no es til. Luego de la construcción de la imagen R.

Algoritmo 2 El algoritmo buscará de manera sencilla los bordes de la región de la imagen de entrada ocupados por la huella digital. Para ello el algorítmo realizará un barrido de la imágen partiendo de cada uno de los cuatro bordes de la imágen. Agregando en cada uno de los barridos información en la imágen R que representa la máscara útil de la imágen. Sea I la imagende entrada, dejemos que *I(x,y)* sea el valor del píxel en las coordenada *(x,y)* de Iy digamos que que I(0,0) es el píxel de la esquina superior izquierda de I. Describiremos el barrido comenzando del borde izquierdo de I, ya que los tres barridos restantes son análogos. Hay que tener en cuenta que el algoritmo necesita realizar los cuatro barridos modificando los valores de la misma imágen R.

Barrido comenzando por el borde izquierdo

Se recorre píxel por píxel cada una de las filas de la imágen partiendo del píxel *I(0,i)* para *i=0,1,...,*I_{width}, cuando se encuentra un píxel digamos *I(0,m)*, *0*$\leq m \leq$ $I_{width}+1$ cuyo valor es mayor a *M(I)* se calcula *Sig* el promedio de los n píxeles siguientes, si *Sig*$\leq$ *M(I)* almacenamos *R(0,0)=255,R(0,1)=255,...,R(0,m)=255* si no lo es continuamos con la búsqueda hasta completar todos los píxeles de la fila Repetimos el proceso para cada una de las filas.

```
Imput
I Imagen de entrada,
n cota,
W I_width,
H I_height;
Output
R;

1. i=0,j=0
2. Si I(i,j)>= M(I) ir a 3
   Si I(i,j)< M(I); j=j+1 ir a 2
```

```
3. Si Prom(I(i,j),...,I(i+n,j))>=M(I) ir a 5
   Si Prom(I(i,j),...,I(i+n,j))< M(I) ir a 4
4. Si j!=I_width, hacer j=j+1 e ir a 2
   Si j==I_width, ir a 5
5. R(i,k)=I(i,k) para k=0...j ir a 5
6. Si i != I_height,hacer i = i+1; ir a 2
   Si i == I_height,terminar.
```

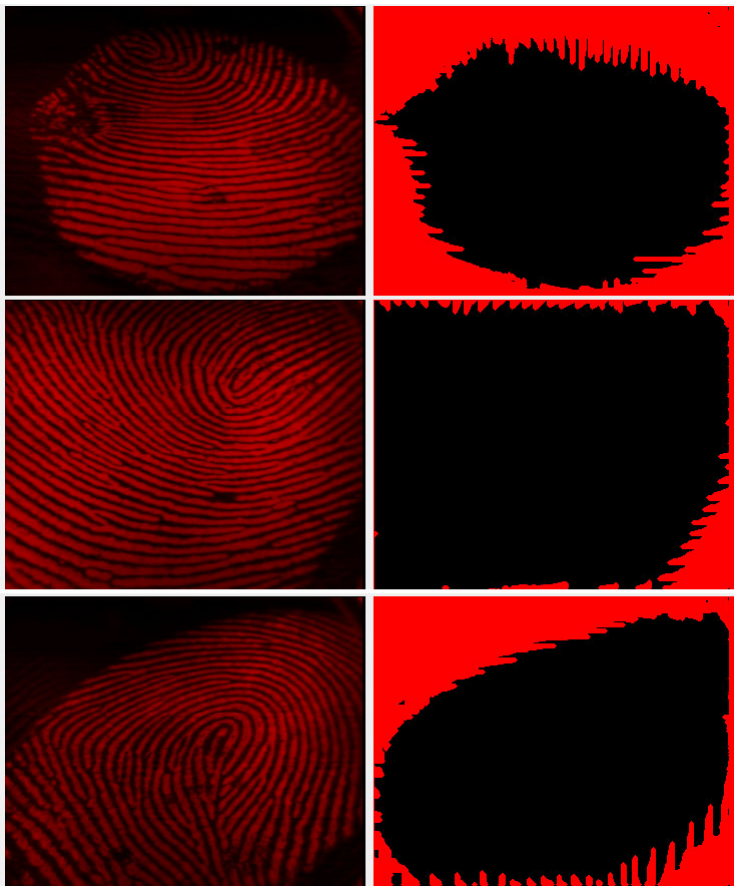

Figura 3.9: Obtención de la máscara útil con el Algoritmo2, Izquierda Imágen de entrada I, Derecha Imagen de la máscara R resultante

3.2. Realce de la imágen - Enhancement

3.2.1. Filtros de Gabor

Éste método está diseñado para la eliminación de ruido de la imagen de entrada, debido a que la configuración paralela de bordes y surcos con frecuencia y orientación bien definida en una Huella Digital provee información importante que ayuda a eliminar ruido no deseado. La forma de las ondas sinusoidales de bordes y surcos varía lentamente en una orientación local constante, por lo tanto, un filtro pasa-bandas sintonizado a la frecuencia y orientación correspondiente puede eliminar ruido innecesario preservando las estructuras de bordes y surcos.
Los filtros de Gabor poseen propiedades en cuanto a la selección de frecuencia como la selección de orientación y tienen una buena relación entre el dominio espacial y el dominio de la frecuencia. Entonces es apropiado usar filtros de Gabor como filtros pasa-bandas para eliminar ruidos y preservar las formas de bordes y surcos.
A continuación aplicaremos un filtro de Gabor en la imagen de entrada usando la dirección y frecuencia computadas previamente. La función de simetría que usaremos es la siguiente:

$$h(x, y : \phi, f) = \exp\left(\frac{\frac{1}{x'^2}}{\frac{2}{dx^2}} + \frac{y'^2}{dy^2}\right)\cos(2\pi.f.x') \tag{3.22}$$

donde

$$x' = x.\cos(\phi) + y.\sin(\phi)$$
$$y' = -x.\sin(\phi) + y.\cos(\phi)$$

El valor esta basado en datos empíricos y se utiliza 4.0 en principio, más grande sea este valor, mayor resistente al ruido se vuelve el algoritmo, pero se corre el riesgo de producir bordes espurios.

Dejemos que:

G sea la imagen preprocesada.
O el campo de orientación.
F la imágen de frecuencia.
R la máscara de zona útil.
E la imagen resultante realzada por gabor.
Wg es el tamaño del el filtro de Gabor.

Entonces se define E de la siguiente forma:

$$E(i,j) = \begin{cases} 255; & si R(i,j) = 0 \\ \sum_{u=-W_g/2}^{W_g/2} \sum_{v=-W_g/2}^{W_g/2} h(u, v : O(i,j), F(i,j)) G(i-u, j-v) & caso\, contrario, \end{cases}$$

3.2.2. Método de Binarización Adaptativa

Debido a las limitaciones en cuanto a la calidad de realce y tiempo de cómputo que consume el realce de la imagen utilizando filtros de Gabor, recorrimos los papers

de realce publicados en la ieee y encontramos que la mayoría menciona o utiliza filtros de gabor o métodos más complejos que consumen aun más tiempo de cómputo.

Tras evaluar el realce que realiza un software comercial "Verifinger", observamos que este software realizaba una optimización de la imagen de entrada de manera muy rápida en cuanto a tiempo computacional, y la calidad de la imagen era aceptable por más que agrega informacin falsa. Con éxito se desarrollo e implementó un mtodo de realce de la imagen que satisface nuestras exigencias en cuanto a consumo de tiempo computacional. En este método, cada píxel es sucesivamente examinado, asignándole un valor de 0 a 255 obteniendo de esta manera una imágen realzada y binarizada como imágen resultado de la aplicación del algoritmo.

La idea es que si un píxel se ubica dentro de una zona de bajo flujo de cresta se le asigna 0. Sin embargo si el píxel se encuentra en una zona donde la cresta esta bien definida se le asigna 255, de manera inversa la asignación ocurre para los píxeles que están en los surcos.

Para determinar si un píxel esta en un surco o cresta una ventana de 7 columnas (Width) x 9 filas (Height) es considerada. La ventana es rotada para que sus filas queden alineadas con la dirección (gradiente) asociada al pxel y la ventana es centrada en el píxel a ser binarizado. La dirección de la ventana centrada en el píxel *I(i,j)* es *O(i,j)* de la matríz de direcciónes de la imágen.

El tamaño 7x9 píxeles de la ventana es seleccionado de manera empírica para que entren en la ventana un surco y una cresta aproximadamente pero este tamaõ queda sujeto a la resolución de la imágen de entrada.

El anlisis se basa en la observacin de que si un píxel esta en una cresta entonces el

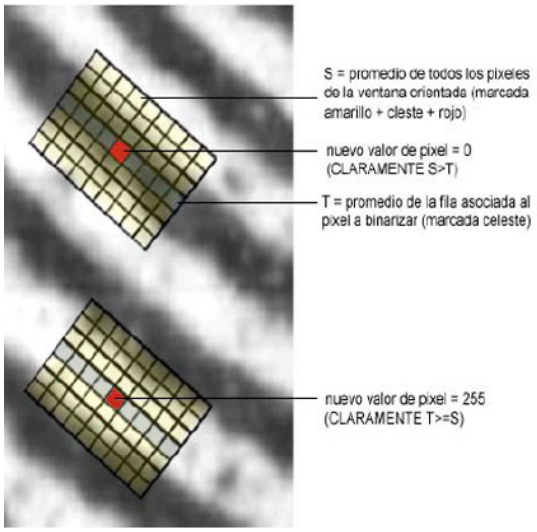

Figura 3.10: Aproximación método de binarización adaptativa

promedio de la suma de los valores de la fila central donde yace el píxel es mayor al valor del promedio de la suma de todos los valores de la ventana orientada y por lo tanto si esto ocurre a ese pxel le corresponde el valor 255. En caso que el píxel se encuentra en un surco el promedio de la suma de los valores de la fila asociada es

menor a el valor del promedio de la ventana y se le asigna 0.

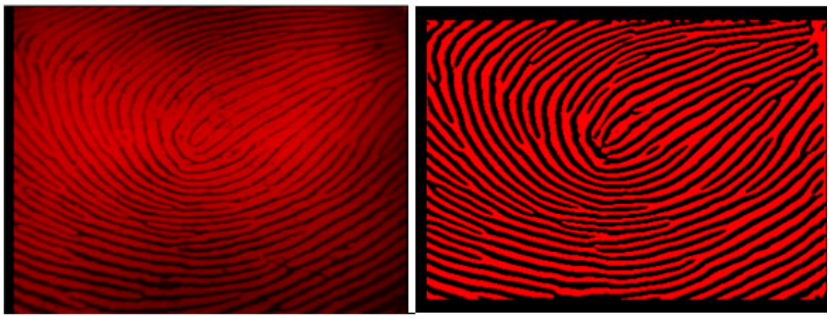

Figura 3.11: Método de binarización adaptativa, Izquierda:Imágen de entrada *I*, Derecha:Imagen resultante de la aplicación del método

Capítulo 4

Extracción de Minucias

4.1. Preprocesado Extracción de Minucias

4.1.1. Binarización

4.1.2. Construcción del esqueleto

4.2. Extracción de características

4.2.1. Extracción de minucias

4.2.2. Eliminación de falsas minucias

Capítulo 5

Matching

5.1. Representación del conjunto de minucias

5.2. Matching de grafos relacionales

Capítulo 6

Clasificación e interación con base de datos

Capítulo 7

Configuración de la construcción de MSAFIS

Bibliografía

[1] T. Jea, V. K. Chavan, V. Govindaraju, and J. K. Schneider.: *Security and matching of partial fingerprint recognition systems*,In Proceeding of SPIE, number 5404, pages 3950, 2004.

[2] Ruud Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, and A. W. Senior. : *Guide to Biometrics.*, Springer Verlag, 2003.

[3] S. Pankanti, S. Prabhakar, and A. K. Jain.: *On the individuality of fingerprints*, Transactions on PAMI, 24(8):10101025, 2002.