UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

"UTILIZACIÓN DE UN MÉTODO HÍBRIDO PARA LA IDENTIFICACIÓN DE HUELLAS DIGITALES PERTURBADAS CON UN ALTO NIVEL DE RUIDO"

TESIS

QUE PRESENTA:

GILBERTO VELÁZQUEZ MARTÍNEZ

PARA OBTENER EL TÍTULO DE:

INGENIERO ELÉCTRICO Y ELECTRÓNICO

ASESOR: DR. FRANCISCO GARCÍA UGALDE

MÉXICO, D.F. 2009

JURADO ASIGNADO

_____

Ing. Gloria Mata Hernández, Presidente

_____

Dr. Francisco Javier García Ugalde, Vocal

_____

M.I. Larry Hipólito Escobar Salguero, Secretario

_____

M.A. Víctor Damián Pinilla Morán, 1er Suplente

_____

Ing. Ricardo Mota Marzano, 2do Suplente

Agradecimientos

A Dios porque con el amor y ternura que nos brinda nos hace ser mejores personas en todo momento y por permitirme llegar a esta meta.

A mi Esposa por ser el pilar en mi vida, por amarme tanto, por apoyarme incondicionalmente en todo y por impulsarme como nadie jamás lo ha hecho.

A mi Suegra quien ha sido ejemplo de honradez, humildad y sinceridad y quien siempre me ha apoyado incondicionalmente.

A Salvador y a Ruth por apoyarme siempre y por el gran voto de confianza que han tenido en mí.

A la Madre Elvia Jaimes por brindarme apoyo, motivación y cariño en las diversas etapas de mi vida.

A la Familia Velázquez por abrirme sus brazos y por permitirme compartir los momentos mas importantes de mi vida.

A mi Bisabuela (QEPD) por ser un ejemplo de humanidad y cariño.

Al Doctor Francisco García Ugalde por motivarme tanto de estudiante, apoyarme con paciencia y sabiduría en el desarrollo de este trabajo y por aconsejarme tan humanamente.

A todos los Profesores que con su ejemplo y dedicación lograron activar el gusto por la carrera.

A mis Amigos y Compañeros por todo el apoyo y la motivación que me han brindado.

A mis Abuelos por todo el apoyo que me brindaron.

ÍNDICE GENERAL

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE TABLAS

PREFACIO

En esta tesis se pretende estudiar el desarrollo de un sistema de identificación de huellas digitales, basándose en las características propias de las huellas dactilares, que caracterizan la identidad de un individuo dentro de un universo de personas.

En el presente trabajo, la estructura del mismo presenta al inicio una introducción de los diversos sistemas de seguridad biométrica, el planteamiento del problema, las hipótesis y diversos objetivos generales y específicos.

Al inicio de cada capítulo , se encuentra una breve introducción al mismo, lo que brinda un acercamiento mas ameno a cada uno de los temas a desarrollar en este trabajo.

Posteriormente, se explica la biometría, su historia, sus características, la forma en que trabaja, los errores en los sistemas biométricos, su caracterización y su funcionamiento.

En particular, como en esta tesis se hace un análisis de las huellas dactilares, en seguida se estudia de una manera mas profunda la composición y clasificación de las huellas dactilares, sus formas y sus propiedades.

Una vez planteado este panorama, se lleva al lector por un análisis mas profundo del estudio de los diversos métodos de identificación de las

huellas dactilares, para que posteriormente se describa paso a paso, de una manera secuencial el método propuesto en esta tesis, contemplando las dificultades y solución de problemas que conforman el método propuesto.

Finalmente, se enumera al final de este trabajo las conclusiones obtenidas de la realización de este trabajo; así como una sugerencia a trabajos futuros que tomen como punto de partida el presente trabajo.

Capítulo I Introducción y planteamiento del problema

1.1 Introducción

Con la evolución de las tecnologías asociadas a la información, nuestra sociedad está cada día más conectada electrónicamente. Labores que tradicionalmente eran realizadas por seres humanos son, gracias a las mejoras tecnológicas, realizadas por sistemas automatizados. Dentro de la amplia gama de posibles actividades que pueden automatizarse, aquella relacionada con la capacidad para establecer la identidad de los individuos ha cobrado importancia y como consecuencia directa, la biometría se ha transformado en un área emergente [1].

La biometría es la ciencia que se dedica a la identificación de individuos a partir de una característica anatómica o un rasgo de su comportamiento. Una característica anatómica tiene la cualidad de ser relativamente estable en el tiempo, tal como una huella dactilar, la silueta de la mano, patrones de la retina o el iris. Un rasgo del comportamiento es menos estable, pues depende de la disposición psicológica de la persona, por ejemplo la firma o la forma de caminar.

No cualquier característica anatómica puede ser utilizada con éxito por un sistema biométrico. Para que esto así sea debe cumplir con las siguientes características: Universalidad, Unicidad, Permanencia y Cuantificación [2].

Un indicador biométrico que satisface estos requisitos es la huella dactilar. Este indicador ha sido utilizado por los seres humanos para identificación personal durante más de cien años [3]. En la actualidad las huellas dactilares representan una de las tecnologías biométricas más maduras y son consideradas pruebas legítimas de evidencia criminal en cualquier corte del mundo.

Una huella dactilar es la representación de la morfología superficial de la epidermis de un dedo. Posee un conjunto de líneas que, en forma global, aparecen dispuestas en forma paralela. Sin embargo, estas líneas se intersectan y a veces terminan en forma abrupta. Los puntos donde éstas terminan o se bifurcan se conocen técnicamente como minucias.

Para concluir si dos huellas dactilares corresponden o no a la misma persona se lleva a cabo un procedimiento que comienza con la clasificación de la huella dactilar y termina con el matching o comparación de las minucias de ambas huellas.

Los diversos métodos de identificación de huellas han permitido crear una evolución en seguridad, rapidez y confianza; lo que se traduce en ahorro de tiempo, dinero y esfuerzo, agregando un máximo de confiabilidad al desempeño de los sistemas biométricos.

Recientemente y desde hace algún tiempo, la investigación relacionada a huellas digitales ha explorado significativamente diversas posibilidades, como por ejemplo tomar en cuenta las características físicas de la huella, métodos basados en las formas generales de la distribución de formas irregulares compuestas de valles y crestas, obtención de discontinuidades, comparación de patrones o la medición de ángulos de las líneas paralelas de los valles que forman la huella, entre otros.

Actualmente en nuestro país, se gastan enormes sumas de dinero en la adquisición de sistemas automatizados de identificación de huellas digitales (AFIS), por sus siglas en inglés, para el combate a la delincuencia en varias agencias periciales, como son la PGR y la AFI [4].

Este sistema, conocido como IAFIS (Integrated Automated Fingerprint Identification System), se desarrolla en la división CJIS (Criminal Justice Information Services) del FBI (Federal Bureau of Investigation), con sede en Virginia, y que ha venido trabajando en el desarrollo de seguridad biométrica y en su propio sistema de identificación de huellas dactilares [5].

El sistema AFIS, adquirido por las oficinas mexicanas, tiene acceso a la base de datos más grande del mundo, con más de 55 millones de sospechosos en el rubro criminalístico. Las huellas digitales, la historia criminal y la información relacionada con el sospechoso son adicionadas voluntariamente por las oficinas locales, federales y estatales que poseen dicho sistema [6].

Todas estas características y peculiaridades, hacen del sistema AFIS un sistema muy costoso, que debe de ser renovado constantemente, lo cual ocasiona una dependencia total, tanto económica como de soporte dentro del marco de seguridad nacional hacia las empresas dedicadas a proporcionar los elementos necesarios para llevar a cabo la implementación del sistema AFIS.

Es por eso, que mediante este trabajo, se analiza un método de obtención de huellas dactilares, utilizando una técnica robusta, rápida y económica.

La técnica propuesta en esta tesis, contempla todo el proceso de obtención de huellas, la extracción de singularidades de las huellas digitales, el filtrado de la imagen obtenida propia de la huella digital; así como la creación de un algoritmo único de identificación para cada huella, basado en la naturaleza propia de la imagen, obteniéndose un poliedro único para cada huella digital.

A lo largo de este trabajo, se irán abordando diversas técnicas propuestas por expertos en la materia, como marco de referencia dentro del propio método propuesto, se hará una valuación para determinar si el método propuesto cumple con los requerimientos mínimos para poder desenvolverse como un sistema confiable y eficaz de seguridad biométrica.

Como eje fundamental del desarrollo de este método, y como validador principal, se agrega a este trabajo el factor económico, desde este punto de vista, se busca desarrollar un sistema lo más económico posible, para lo cual se realizaron los trabajos de adquisición de huellas con un lector comercial que se conecta a una computadora vía USB, el cual no excede los 25 dólares.

Para la obtención de las minucias propias de cada huella digital, se utilizó una librería estandarizada, la cual ha sido probada y utilizada ampliamente en ese campo, es la librería con funciones de adquisición y barrido de imágenes libfprint , que forma parte del proyecto fprint, sólo disponible para Linux.

Los algoritmos de filtrado de la imagen con sus minucias se desarrollaron en MATLAB 7, utilizando las librerías de procesamiento de imágenes (Image processing Toolbox), el algoritmo de creación de prismas únicos para cada huella está alojado en MATLAB de igual forma.

El código de generación de prismas es la técnica de Delaunay y Voronoi, ambos algoritmos muy utilizados en la obtención de imágenes en 3D, son técnicas ampliamente estudiadas, que dan una solidez mayor al proceso de identificación del individuo por medio de la huella dactilar.

Todos estos procesos deben ser ejecutados en una computadora, y como el factor económico es determinante en este trabajo, se prestó especial atención al uso de recursos dentro de la computadora, haciendo eficiente tanto los filtros del procesamiento de imagen como la obtención de datos. Es por eso que, al utilizar el proyecto fprint se decidió trabajar en la plataforma Linux, instalándole MATLAB 7 a dicha computadora trabajando todos los algoritmos en Linux.

Es por esto que, trabajando en Linux todo el proceso de el método propuesto, desde la adquisición de datos, su extracción de minucias, el filtrado de la imagen y la caracterización en forma única de la huella digital se desarrolla un sistema que se compone de:

- Un lector de huellas externo que se conecta vía USB
- Una computadora igual o superior a x386
- Una distribución de Linux (se recomienda xubuntu por su bajo consumo de recursos dentro de la computadora)
- El proyecto fprint de linux
- MATLAB 7

Estos aspectos unidos, dan como resultado un sistema único que permite la obtención de huellas dactilares de cualquier individuo en forma eficiente, robusta y económica.

La robustez del sistema presentado en esta tesis se define como la inmunidad al ruido proveniente del lector de huellas digitales. Hoy en día

existen diversos fabricantes de lectores de huellas, ofreciendo una amplia gama de posibilidades para todos los consumidores, ofreciendo una gran diversidad en precio y calidad de la imagen obtenida, así como en tamaño y materiales de composición, que permiten una mejor obtención de la imagen del dedo colocado en el lector.

La eliminación del ruido y la discriminación de redundancias, así como la selección objetiva de las características propias de la huella digital, son ventajas considerablemente distintivas que permiten una mayor interacción entre el usuario final y el sistema propuesto con un alto nivel de intuición, permitiendo la pronta familiarización con el método propuesto, evitando el tiempo de adaptación y conocimiento previo a la utilización de un sistema nuevo.

Por su muy bajo costo y su gran efectividad, seguridad y rendimiento, este trabajo se propone como una alternativa a la identificación dactilar biométrica, para contrarrestar las ofertas disponibles en el mercado hoy en día, ofreciendo los mismos resultados que sus competidores comerciales.

En México existe una dependencia directa a la adquisición de tecnología del extranjero, y en el caso de las tecnologías biométricas, la incursión a los mercados nacionales por parte de una empresa mexicana es una labor doblemente difícil.

Los altos costos de los sistemas desarrollados en el extranjero no sólo se limitan a la adquisición del algoritmo de reconocimiento de huellas, sino también a la adquisición del hardware explícito para este fin, hardware que es ofrecido por separado y con un alto costo por las compañías dedicadas a la seguridad biométrica únicamente.

Pensando en estos problemas es como se desarrolló la presente tesis, con el fin de brindar una solución a un mercado creciente, con un amplio desarrollo en México y en el mundo; un mercado nuevo y renovado que día a día se abre camino en nuevos sectores, como las computadoras personales y el acceso al hogar.

Planteamiento del problema

1.2 Problema

Como efecto de la modernización de la sociedad, ha sido necesario el mejoramiento de autentificación de individuos, tanto para mantener su privacidad y su individualidad, como también para lograr la confianza necesaria en los medios electrónicos que permiten día a día llevar a cabo nuestras actividades.

Con el creciente uso de la tecnología, mas personas tienen la facilidad de obtener los conocimientos necesarios para llevar a cabo actividades ilícitas que involucren la seguridad de bienes y servicios tanto de una como de miles e incluso millones de personas.

Durante muchos años, las únicas entidades capaces de invertir en tecnología capaz de identificar con veracidad y rapidez a individuos de entre un grupo de miles o más, han sido las oficinas gubernamentales, quienes destinan miles de millones de dólares en la obtención de sistemas para la autentificación y verificación de individuos, así como en obtener huellas digitales de los principales criminales de todo el mundo.

¿Es posible crear un método económico, robusto y compatible con cualquier imagen proveniente de los diferentes lectores existentes en el mercado?

1.3 Justificación

Con el uso de la tecnología en todas las actividades del ser humano, es de vital importancia tener la seguridad de la identidad de una persona; y al ser los sistemas más vulnerables a ataques por el uso de contraseñas el uso de la biometría viene a llenar un hueco en el ámbito de la seguridad informática. Sin embargo, los costos de adquisición e implementación de un sistema biométrico superan los millones de dólares.

Software más económico es posible encontrarlo en el mercado, pero los resultados no son satisfactorios principalmente por problemas de incompatibilidad, vulnerabilidad y poca o nula información útil debido al ruido.

La conjunción de las dos bondades de un sistema caro, como son compatibilidad y alta confiabilidad se implementan en un sistema con los mínimos recursos para su óptimo funcionamiento.

1.4 Objetivo General

Desarrollar un sistema biométrico de identificación de huellas digitales cuyas características sean el bajo costo, una tolerancia al ruido considerable y una clasificación de huellas única.

1.5 Objetivos Específicos

Obtener el máximo aprovechamiento de las herramientas para el desarrollo del sistema propuesto con el mínimo gasto económico.

Llevar a cabo la caracterización única de huellas digitales.

Lograr una compatibilidad con cualquier imagen proveniente de distintos tipos de lectores biométricos.

1.6 Hipótesis

Si se presenta un método de identificación de huellas digitales económico, robusto, estable y compatible con diversos lectores biométricos, entidades públicas y privadas, con fines comerciales, de seguridad o investigación podrán acceder a una tecnología pionera en el ámbito de seguridad, mejorando sus sistemas de manera local y global.

1.7 Procedimiento

La tesis es la implementación de un sistema biométrico compuesto de una propuesta de captura de imagen, un método de reconocimiento de minucias e identificación de una huella digital.

El procedimiento de investigación se basa en la consulta de fuentes de información:

Escritas (libros, publicaciones, revistas)

Virtuales (páginas de Internet)

En primer lugar se plantea el alcance de la tesis.

Enseguida se conseguirá un lector biométrico económico y con características técnicas compatibles con las herramientas disponibles.

A continuación se investigará la forma más económica y eficaz de obtener la información proveniente del lector biométrico.

Se llevará a cabo la investigación pertinente a la extracción de singularidades de las huellas digitales.

Después se realizará la extracción de minucias propias de las huellas digitales.

Posteriormente se implementará un proceso para la eliminación de ruido.

Inmediatamente después se llevará a cabo la investigación pertinente a la generación de un código único y se procederá con su implementación.

Acto seguido, toda la información será depurada y posteriormente concentrada en un documento.

Finalmente dicho documento será dividido en capítulos para así cumplir con los objetivos planteados, y así dar respuesta a los problemas formulados y comprobar o desmentir la hipótesis propuesta.

Capítulo II

Sistemas Biométricos

Al inicio del presente capítulo se brinda un panorama general de los sistemas biométricos, el origen de la tecnología, su significado y una descripción de su evolución a lo largo de la historia, lo cual permite comprender su evolución y observar su desarrollo en distintas áreas a través de los años.

Posteriormente se describen las características que poseen y hacen únicos a los sistemas biométricos, se analiza su confiabilidad y se hace una descripción de cada uno de los errores presentes en los métodos de identificación biométrica.

A continuación se describen los dos modos de trabajo de los sistemas biométricos, el modo verificación y el modo identificación.

Para concluir el primer capítulo de esta tesis, se brinda una descripción de las diversas herramientas que permiten una caracterización gráfica de las características de los sistemas biométricos en general.

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

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

En las tecnologías de la información (TI), la autentificación biométrica se refiere a las tecnologías para medir y analizar las características físicas y del comportamiento humanas con propósito de autentificación.

Las huellas dactilares, las retinas, el iris, los patrones faciales, de venas de la mano o la geometría de la palma de la mano, representan ejemplos de características físicas (estáticas), mientras que entre los ejemplos de características del comportamiento se incluye la firma, el paso y el tecleo (dinámicas). La voz se considera una mezcla de características físicas y del comportamiento, pero todos los rasgos biométricos comparten aspectos físicos y del comportamiento [7].

Los Sistemas Biométricos son métodos automáticos de verificación e identificación de un individuo utilizando características físicas y comportamientos precisos [8].

De acuerdo al diccionario de la real academia de la lengua española “biometría” es el estudio mensurativo (perteneciente o relativo a la medida) o estadístico de los fenómenos o procesos biológicos; el significado de biometría es el conjunto de métodos automatizados que analizan determinadas características humanas para identificar o autentificar personas.

2.1 Historia de la Biometría

Parece ser que en la antigua Babilonia, las tabletas de arcilla se firmaban con la huella digital.

En la Persia del siglo XIV varios documentos oficiales tenían huellas dactilares y un oficial del Gobierno observó que no había dos huellas dactilares iguales.

En la legislación de la antigua China se establecía que para divorciarse había que exponer siete motivos y, con las huellas dactilares, firmar el documento.

Según reportes de João de Barros en el siglo XIV en China, los mercaderes estampaban las huellas de la palma de la mano y los pies de los niños en un papel con tinta para distinguir a los niños uno de otro.

En 1686 el Italiano Marcello Malpighi, fue el primero que identificó que los patrones de la piel en los dedos eran diferentes.

En 1823 John Evangelista Purkinje, médico y científico natural checo, quien trabajaba como catedrático de anatomía de la Universidad de Breslau, identificó la naturaleza única de las huellas digitales de los individuos, el identificó las espirales, elipses y triángulos en las huellas digitales y publicó una tesis en la que se mencionaba que había 9 tipos de formas de huellas dactilares, pero no hizo ninguna mención a que pudieran usarse para identificar individuos.

Fue Sir William Hershel, en 1856, quien empezó a usar las huellas digitales para validar contratos.

En 1858 Sir William Herschel, trabajador del servicio civil de la India, quien empezó a usar las huellas digitales para validar contratos; imprimió la huella de la mano al reverso de un contrato para cada

trabajador para distinguir los empleados de otros que intentaran suplantar a los trabajadores el día de pago. Su idea era la de que los comerciantes nativos pusieran la huella de su mano derecha detrás del papel del contrato, para evitar que dijeran que la firma no era suya. Después exigió solamente las huellas del dedo índice y del medio. Herschel comenzó a notar que esas huellas eran únicas para cada persona, pero era un convencimiento individual sin apoyo científico.

Alphonse Bertillon desarrollo el sistema “Bertillonaje” o antropometría descriptiva en 1870 como un método para identificar individuos basado en registros detallados de medidas de su cuerpo.

Henry Faulds publicó el 28 de octubre de 1880 en "Nature" un artículo sobre como identificar criminales a partir de sus huella digitales llamado “On the Skin-Furrows of the Hand”.


NATURE

Figura 2.1. Artículo de Henry Faulds publicado en "Nature" en 1880

Desde 1882 y hasta 1890 fue utilizado en Francia la técnica desarrollada por Bertillion como instrumento de las investigaciones de la policía.

En 1883 Mark Twain publica el libro “life on the Mississippi”, donde un asesino es identificado usando la identificación de huellas digitales

El primero de Septiembre de 1891 comenzó a utilizarse oficialmente el método Juan Vucetich en el servicio de identificación por medio de impresiones digitales en Argentina basado en lo ideado por Francis Galton. Vucetich inventó los elementos para captar lo más perfectamente posible los dibujos dactilares de los dedos de ambas manos y puso en práctica todo cuanto fue necesario para sistematizar el método.

Vucetich logró simplificar el método de Galton basándolo en cuatro rasgos principales: arcos, presillas internas, presillas externas y verticilos.

Sir Francis Galton publicó en 1892 un libro llamado “Finger Prints”, detallado estudio de huellas digitales en donde presentó un nuevo sistema de clasificación usando las huellas digitales de los 10 dedos de las manos. El método Galtoneano o Icnofalangometría.

Figura 2.2 Portada libro “Finger Prints” publicado por Macmillan and Co.

El interés de Galton era descubrir rasgos de inteligencia y raciales en las huellas. Fue su hijo quien "demostró" científicamente lo que Herschel y Fauld sospechaban que las huellas dactilares no cambian con

la edad y que no hay dos huellas idénticas. Sus cálculos decían que la probabilidad de que dos huellas individuales fueran iguales era de 1 en 64 000 millones.

Galton hijo también determinó la forma de identificar una huella que es esencialmente el mismo método que se utiliza hoy. El primer fichero de huellas digitales lo estableció en 1891 el policía argentino Juan Vucentich. Al año siguiente, el 29 de Junio en la ciudad de Necochea, Argentina, se logró identificar mediante las huellas dactilares a una mujer llamada Francisca Rojas como la asesina de sus dos hijos. Su huella ensangrentada dejada en el buzón de la puerta la delató.

Figura 2.3 Huella pulgar derecho de Francisca Rojas[10].

En 1894 Mark Twain publica un libro llamado “The Tragedy of Pudd’nhead Wilson”, que es una novela que habla sobre el uso de las huellas digitales en un juicio en la corte.

Sir Edward Henry, Inspector General de la Policía de Bengal, En 1896 una vez que el sistema de huella digital fue implementado, Azizul Haque, un trabajador de Henry, desarrolló un método de clasificación y almacenamiento de información, haciendo más sencillo y eficiente el proceso de búsqueda. Más tarde Sir Henry estableció el primer archivo de huellas digitales en Londres. El sistema de clasificación de Henry como se llegó a conocer, fue el precursor de los sistemas de clasificación usados durante muchos años por organizaciones de justicia criminal.

En 1900 Scotland Yard adopta el sistema de huellas digitales de Henry.

En 1901 las policías de Gales e Inglaterra establecieron las huellas digitales como sistema de identificación en los delitos. El sistema se basaba en el sistema de Galton, modificado por Sir Edward Richard Henry.

En 1902 en el caso de Denmark Hill en el Reino Unido, se usa por primera vez la huella digital para conectar al acusado con la escena del crimen.

En 1903 el departamento de policía de New York empieza los archivos de huellas digitales de personas arrestadas

En 1903 El sistema Bertillon Colapsa al ser sentenciados dos hombres, posteriormente determinados gemelos idénticos, en la penitenciaria norteamericana de Leavenworth, Kansas. Sus nombres Eran Will y William West.

Entre 1905 y 1908 se implementa el uso de sistemas de huellas digitales en la Fuerza Aérea, Ejército y Armada de Estados Unidos.

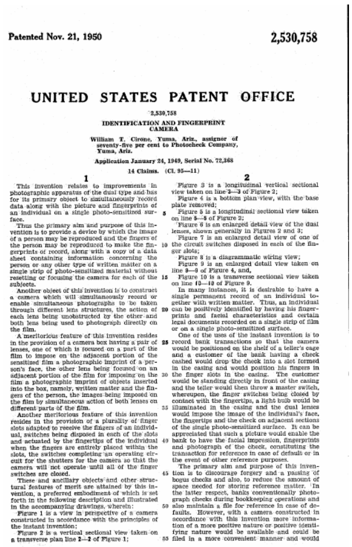
El 4 de Agosto de 1915 el Inspector Harry H. Caldwell del departamento de policía de Oakland (California, USA) solicitó a “Criminal Identification Operators” realizar una reunión en Oakland con el propósito de crear una organización para llevar mas allá los ideales de la profesión de identificación. Un grupo de veintidós hombres se encontraron y como resultado en Octubre de 1915 se fundó la asociación internacional para Identificación criminal (IAI).

En 1918 Edmond Locard escribió que si 12 puntos o detalles Galton coinciden en una comparación de dos huellas digitales, es suficiente para una identificación positiva, sin embargo no hay un estándar mundial sobre el uso mínimo de puntos para identificación positiva y algunos países tienen sus propios estándares al respecto.

Los oftalmólogos Carleton Simon y Isodore Goldstein escriben un artículo para New York State Journal of Medicine que fue publicado en Septiembre de 1935 y se titulo “A new Scientific Method of Identification”, en este artículo plantean que los patrones vasculares de la retina son únicos en cada individuo.

El oftalmólogo Frank Burch propone el concepto de usar los patrones del iris como método de reconocimiento individual en 1936.

La primera patente que registra el uso de huellas digitales es la No.2530758 del 21 de Noviembre de 1950 en Estados Unidos que se trataba de una cámara de identificación y huellas digitales, desarrollada por William T. Cirone,



Patented Nov. 21, 1950 2,530,758

UNITED STATES PATENT OFFICE

2,530,758

IDENTIFICATION AND FINGERPRINT CAMERA

William T. Cirone, Yuma, Ariz., assignor of seventy-five per cent to Photocheck Company, Yuma, Ariz.

Application January 24, 1949, Serial No. 72,368

14 Claims. (Cl. 95—11)

1

This invention relates to improvements in photographic apparatus of the dual type and has for its primary object to simultaneously record data along with the picture and fingerprints of an individual on a single photo-sensitized surface.

Thus the primary aim and purpose of this invention is to provide a device by which the image of a person may be reproduced and the fingers of the person may be reproduced to make the fingerprints of record, along with a copy of a data sheet containing information concerning the person or any other type of written matter on a single strip of photo-sensitized material without resetting or focusing the camera for each of the subjects.

Another object of this invention is to construct a camera which will simultaneously record or enable simultaneous photographs to be taken through different lens structures, the action of each lens being unobstructed by the other and both lens being used to photograph directly on the film.

A meritorious feature of this invention resides in the provision of a camera box having a pair of lenses, one of which is focused on a part of the film to impose on the adjacent portion of the sensitized film a photographic imprint of a person's face, the other lens being focused on an adjacent portion of the film for imposing on the film a photographic imprint of objects inserted into the box, namely, written matter and the fingers of the person, the images being imposed on the film by simultaneous action of both lenses on different parts of the film.

Another meritorious feature of this invention resides in the provision of a plurality of finger slots adapted to receive the fingers of an individual, switches being disposed in each of the slots and actuated by the fingertips of the individual when the fingers are entirely placed within the slots, the switches completing an operating circuit for the shutters for the camera so that the camera will not operate until all of the finger switches are closed.

These and ancillary objects and other structural features of merit are attained by this invention, a preferred embodiment of which is set forth in the following description and illustrated in the accompanying drawings, wherein:

Figure 1 is a view in perspective of a camera constructed in accordance with the principles of the instant invention;

Figure 2 is a vertical sectional view taken on a transverse plan line 2—2 of Figure 1;

2

Figure 3 is a longitudinal vertical sectional view taken on line 3—3 of Figure 2;

Figure 4 is a bottom plan view, with the base plate removed;

Figure 5 is a longitudinal sectional view taken on line 5—5 of Figure 2;

Figure 6 is an enlarged detail view of the dual lenses, shown generally in Figures 2 and 3;

Figure 7 is an enlarged detail view of one of the circuit switches disposed in each of the finger slots;

Figure 8 is a diagrammatic wiring view;

Figure 9 is an enlarged detail view taken on line 9—9 of Figure 4, and,

Figure 10 is a transverse sectional view taken on line 10—10 of Figure 9.

In many instances, it is desirable to have a single permanent record of an individual together with written matter. Thus, an individual can be positively identified by having his fingerprints and facial characteristics and certain legal documents recorded on a single strip of film or on a single photo-sensitized surface.

One of the uses of the instant invention is to record bank transactions so that the camera would be positioned on the shelf of a teller's cage and a customer of the bank having a check cashed would drop the check into a slot formed in the casing and would position his fingers in the finger slots in the casing. The customer would be standing directly in front of the casing and the teller would then throw a master switch, whereupon, the finger switches being closed by contact with the fingertips, a light bulb would be illuminated in the casing and the dual lenses would impose the image of the individual's face, the fingertips and the check on adjacent sections of the single photo-sensitized surface. It can be appreciated that such a picture would enable the bank to have the facial impression, fingerprints and photograph of the check, constituting the transaction for reference in case of default or in the event of other reference purposes.

The primary aim and purpose of this invention is to discourage forgery and a passing of bogus checks and also, to reduce the amount of space needed for storing reference matter. In the latter respect, banks conventionally photograph checks during bookkeeping operations and also maintain a file for reference in case of defaults. However, with a camera constructed in accordance with this invention more information of a more positive nature or positive identifying nature would be available and could be filed in a more convenient manner and would

Figura 2.4. Hoja principal de la patente 3480911

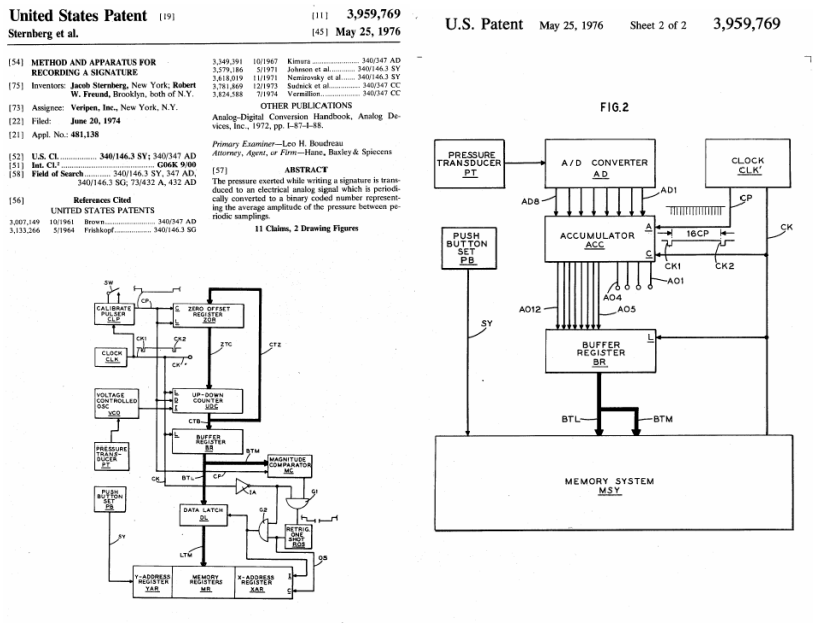
En los setentas Goldstein A.J. , Harmon, L.D. y Lesk, A.B. usaron 22 marcas específicas subjetivas como el color de cabello y grosor de labios para automatizar el reconocimiento facial. El problema con estas soluciones es que las mediciones y localización eran digitadas manualmente. En Mayo de 1971 publicaron en Proceedings of the IEEE un articulo sobre el tema, titulado “Identification of human faces”.

En 1970 Componentes conductuales del discurso son modelados por primera vez por el Dr. Joseph Perkell, que uso rayos-x de movimientos e incluyo la lengua y la mandíbula.

El 25 de Mayo de 1971 se patenta en Estados Unidos un sistema de identificación de la palma de la mano por parte de Norman G. Altman, con la patente No. 3581282.

El FBI consolidó en 1975 el desarrollo de escáneres y tecnología que extrae minucias, que llevó al desarrollo de un prototipo lector. Solo se almacena las minucias de la huella digital y los lectores usaban técnicas capacitivas para recolectar las características de las huellas digitales.

El 25 de mayo de 1976 Jacob Sternberg y Robert W. Freund patentaron en Estados Unidos un Método y aparato para grabar la firma con la patente No. 3959769 y asignada a Veripen Inc.



United States Patent [19]
Sternberg et al.
[11] 3,959,769
[45] May 25, 1976

[54] METHOD AND APPARATUS FOR RECORDING A SIGNATURE
[75] Inventors: Jacob Sternberg, New York; Robert W. Freund, Brooklyn, both of N.Y.
[73] Assignee: Veripen, Inc., New York, N.Y.
[22] Filed: June 20, 1974
[21] Appl. No.: 481,138
[52] U.S. Cl. ..... 340/146.3 SY; 340/347 AD
[51] Int. Cl.² G06K 9/00
[58] Field of Search ..... 340/146.3 SY, 347 AD, 340/146.3 SG; 73/432 A, 432 AD

[56] References Cited
UNITED STATES PATENTS

3,007,149	10/1961	Brown	340/347 AD
3,133,266	5/1964	Frishkopf	340/146.3 SG
3,349,391	10/1967	Kimura	340/347 AD
3,579,186	5/1971	Johnson et al.	340/146.3 SY
3,618,019	11/1971	Nemirovsky et al.	340/146.3 SY
3,781,869	12/1973	Sudnick et al.	340/347 CC
3,824,588	7/1974	Vermillion	340/347 CC

OTHER PUBLICATIONS
Analog-Digital Conversion Handbook, Analog Devices, Inc., 1972, pp. I-87–I-88.

Primary Examiner—Leo H. Boudreau
Attorney, Agent, or Firm—Hane, Baxley & Spiecens

[57] ABSTRACT
The pressure exerted while writing a signature is transduced to an electrical analog signal which is periodically converted to a binary coded number representing the average amplitude of the pressure between periodic samplings.

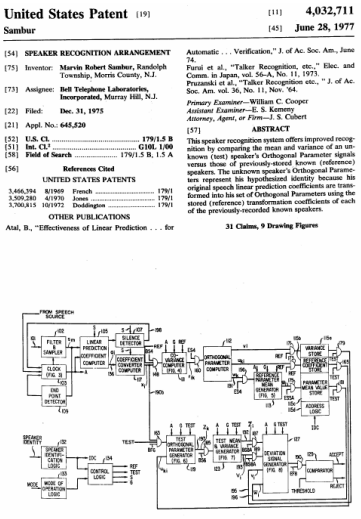
11 Claims, 2 Drawing Figures

U.S. Patent May 25, 1976 Sheet 2 of 2 3,959,769

FIG.2

Figura 2.5 Hoja 1 y 2 de la patente 3959769

El 28 de Junio de 1977 se patentó un arreglo de reconocimiento del hablante por parte de Marvin Robert Sambur y asignado a Bell Telephone Laboratories con la patente No. 4032711 de Estados Unidos.



United States Patent [19]
Sambur
[11] 4,032,711
[45] June 28, 1977

[54] SPEAKER RECOGNITION ARRANGEMENT
[75] Inventor: Marvin Robert Sambur, Randolph Township, Morris County, N.J.
[73] Assignee: Bell Telephone Laboratories, Incorporated, Murray Hill, N.J.
[22] Filed: Dec. 31, 1975
[21] Appl. No.: 645,520
[52] U.S. Cl. ..... 179/1.5 B
[51] Int. Cl.² G10L 1/00
[58] Field of Search ..... 179/1.5 B, 1.5 A

[56] References Cited
UNITED STATES PATENTS

3,466,394	8/1969	French	179/1
3,509,280	4/1970	Jones	179/1
3,700,815	10/1972	Doddington	179/1

OTHER PUBLICATIONS
Atal, B., "Effectiveness of Linear Prediction . . . for Automatic . . . Verification," J. of Ac. Soc. Am., June 74.
Furui et al., "Talker Recognition, etc.," Elec. and Comm. in Japan, vol. 56-A, No. 11, 1973.
Pruzanski et al., "Talker Recognition etc.," J. of Ac. Soc. Am. vol. 36, No. 11, Nov. '64.

Primary Examiner—William C. Cooper
Assistant Examiner—E. S. Kemeny
Attorney, Agent, or Firm—J. S. Cubert

[57] ABSTRACT
This speaker recognition system offers improved recognition by comparing the mean and variance of an unknown (test) speaker's Orthogonal Parameter signals versus those of previously-stored known (reference) speakers. The unknown speaker's Orthogonal Parameters represent his hypothesized identity because his original speech linear prediction coefficients are transformed into his set of Orthogonal Parameters using the stored (reference) transformation coefficients of each of the previously-recorded known speakers.

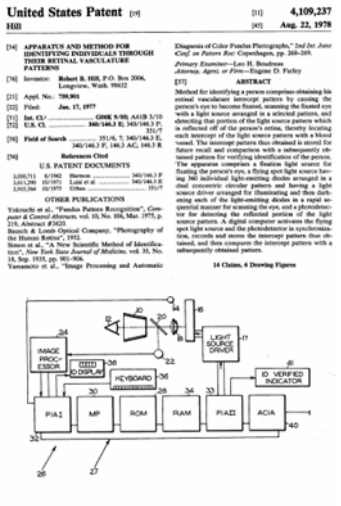
31 Claims, 9 Drawing Figures

Figura 2.6 Primera hoja de la patente US4032711

El 12 de Julio de 1977 fue patentado en Estados Unidos un aparato para identificación personal por parte de Austin G. Boldridge y

Robert W. Freund, asignado a Veripen Inc. y patente No. 4035768, esta es considerada la primera patente de adquisición de información dinámica de una firma.

El 22 de Agosto de 1978 se patentó un aparato y método para identificar individuos a través de sus patrones vasculares de la retina, fue patentado por Robert Hill B. en Estados Unidos No. 4109237, Japón 53105090, Gran Bretaña 1593001 y Alemania 2801927


United States Patent [19]
Hill

[11] 4,109,237
[45] Aug. 22, 1978

[54] APPARATUS AND METHOD FOR IDENTIFYING INDIVIDUALS THROUGH THEIR RETINAL VASCULATURE PATTERNS

[76] Inventor: Robert B. Hill, P.O. Box 2006, Longview, Wash. 98632

[21] Appl. No.: 788,901

[22] Filed: Jan. 17, 1977

[51] Int. Cl.² G06K 9/00; A61B 3/10

[52] U.S. Cl. ..... 340/146.3 E; 340/146.3 F; 351/7

[58] Field of Search ..... 351/6, 7; 340/146.3 E, 340/146.3 F, 146.3 AC, 146.3 R

[56] References Cited

U.S. PATENT DOCUMENTS

OTHER PUBLICATIONS

[57] ABSTRACT

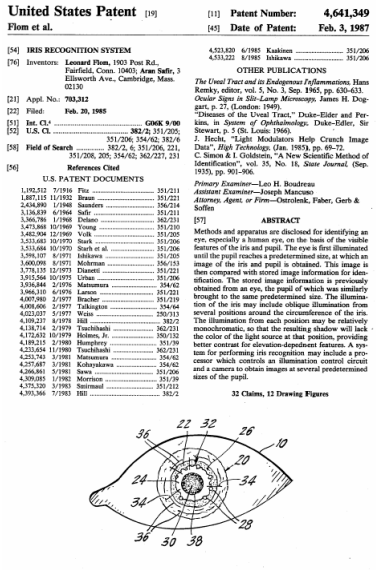
14 Claims, 6 Drawing Figures

Figura 2.7 Página principal de la patente No. 4109237

En los ochentas El instituto nacional de estándares y tecnología (NIST) creó el Grupo de Discurso de NIST para estudiar y promover el uso de técnicas de procesamiento del discurso.

En 1983 en la película de James Bond “Never Say Never Again”, se usa la tecnología de reconocimiento de iris para el acceso a un arsenal nuclear de Estados Unidos, este sistema trabajaba reconociendo el iris derecho del presidente de Estados Unidos.

El 3 de febrero de 1987 Leonard Flom y Aran Safir patentaron en Estados Unidos bajo la patente No. 4641349 un sistema de reconocimiento de iris.



United States Patent [19]
Flom et al.

[11] Patent Number: 4,641,349
[45] Date of Patent: Feb. 3, 1987

[54] IRIS RECOGNITION SYSTEM

[76] Inventors: Leonard Flom, 1903 Post Rd., Fairfield, Conn. 10403; Aran Safir, 3 Ellsworth Ave., Cambridge, Mass. 02130

[21] Appl. No.: 703,312

[22] Filed: Feb. 20, 1985

[51] Int. Cl.[4] G06K 9/00
[52] U.S. Cl. 382/2; 351/205; 351/206; 354/62; 382/6
[58] Field of Search 382/2, 6; 351/206, 221, 351/208, 205; 354/62; 362/227, 231

[56] References Cited
U.S. PATENT DOCUMENTS

1,192,512	7/1916	Fitz	351/211
1,897,115	11/1932	Braun	351/221
2,434,890	1/1948	Saunders	356/214
3,136,839	6/1964	Safir	351/211
3,366,786	1/1968	Delano	362/231
3,473,868	10/1969	Young	351/210
3,482,904	12/1969	Volk	351/205
3,533,682	10/1970	Stark	351/206
3,533,684	10/1970	Stark et al.	351/206
3,598,107	8/1971	Ishikawa	351/205
3,600,098	8/1971	Mehrman	356/153
3,778,135	12/1973	Dianetti	351/221
3,915,566	10/1975	Urban	351/206
3,936,844	2/1976	Matsumura	354/62
3,966,310	6/1976	Larson	351/221
4,007,980	2/1977	Bracher	351/219
4,008,606	2/1977	Talkington	354/64
4,023,037	5/1977	Weiss	250/313
4,109,237	8/1978	Hill	382/2
4,138,714	2/1979	Tsuchihashi	362/231
4,172,632	10/1979	Holmes, Jr.	350/132
4,189,215	2/1980	Humphrey	351/39
4,233,634	11/1980	Tsuchihashi	362/231
4,253,743	3/1981	Matsumura	354/62
4,257,687	3/1981	Kobayakawa	354/62
4,266,861	5/1981	Sawa	351/206
4,309,085	1/1982	Morrison	351/39
4,375,320	3/1983	Smirmaul	351/212
4,393,366	7/1983	Hill	382/2
4,523,820	6/1985	Kashinos	351/206
4,533,221	8/1985	Ishikawa	351/206

OTHER PUBLICATIONS

The Uveal Tract and its Endogenous Inflammations, Hans Remky, editor, vol. 5, No. 3, Sep. 1965, pp. 630-633.
Ocular Signs by Slit-Lamp Microscopy, James H. Doggart, p. 27, (London: 1949).
"Diseases of the Uveal Tract," Duke-Elder and Perkins, in *System of Ophthalmology*, Duke-Edler, Sir Stewart, p. 5 (St. Louis: 1966).
J. Hecht, "Light Modulators Help Crunch Image Data", *High Technology*, (Jan. 1985), pp. 69-72.
C. Simon & I. Goldstein, "A New Scientific Method of Identification", vol. 35, No. 18, *State Journal*, (Sep. 1935), pp. 901-906.

Primary Examiner—Leo H. Boudreau
Assistant Examiner—Joseph Mancuso
Attorney, Agent, or Firm—Ostrolenk, Faber, Gerb & Soffen

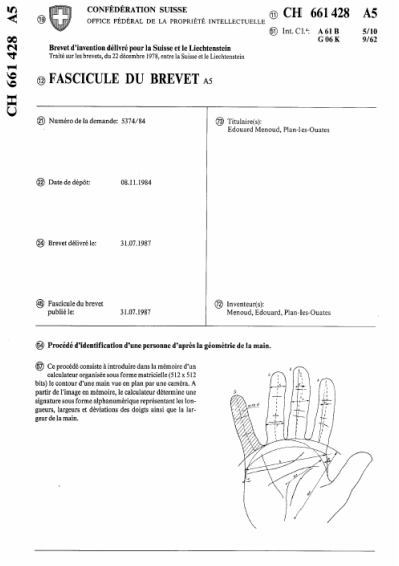
[57] ABSTRACT

Methods and apparatus are disclosed for identifying an eye, especially a human eye, on the basis of the visible features of the iris and pupil. The eye is first illuminated until the pupil reaches a predetermined size, at which an image of the iris and pupil is obtained. This image is then compared with stored image information for identification. The stored image information is previously obtained from an eye, the pupil of which was similarly brought to the same predetermined size. The illumination of the iris may include oblique illumination from several positions around the circumference of the iris. The illumination from each position may be relatively monochromatic, so that the resulting shadow will lack the color of the light source at that position, providing better contrast for elevation-dependent features. A system for performing iris recognition may include a processor which controls an illumination control circuit and a camera to obtain images at several predetermined sizes of the pupil.

32 Claims, 12 Drawing Figures

Figura 2.8 Primera página de la patente US4641349

El 31 de Julio de 1987 Eduard Menoud patentó en la Confederación Suiza un método para identificar una persona a partir de la geometría de su mano, patentado con el No. CH661428A5.



CH 661 428 A5

CONFÉDÉRATION SUISSE
OFFICE FÉDÉRAL DE LA PROPRIÉTÉ INTELLECTUELLE

(11) CH 661 428 A5

(51) Int. Cl.[4] A 61 B 5/10
G 06 K 9/62

Brevet d'invention délivré pour la Suisse et le Liechtenstein
Traité sur les brevets, du 22 décembre 1978, entre la Suisse et le Liechtenstein

(12) FASCICULE DU BREVET A5

(21) Numéro de la demande: 5374/84

(22) Date de dépôt: 08.11.1984

(24) Brevet délivré le: 31.07.1987

(45) Fascicule du brevet publié le: 31.07.1987

(73) Titulaire(s):
Edouard Menoud, Plan-les-Ouates

(72) Inventeur(s):
Menoud, Edouard, Plan-les-Ouates

(54) Procédé d'identification d'une personne d'après la géométrie de la main.

(57) Ce procédé consiste à introduire dans la mémoire d'un calculateur organisée sous forme matricielle (512 x 512 bits) le contour d'une main vue en plan par une caméra. A partir de l'image en mémoire, le calculateur détermine une signature sous forme alphanumérique représentant les longueurs, largeurs et déviations des doigts ainsi que la largeur de la main.

En 1988, la división Lakewood del departamento de Sheriff del condado de Los Ángeles empezó a usar dibujos compuestos ó imágenes de video para realizar búsquedas en bases de datos de fotografías de criminales, es considerado el primer sistema semi-automático de reconocimiento facial.

James R. Young y Robert W. Hammon patentaron el 14 de febrero de 1989 un método y aparato para verificar la identidad de un individuo, la patente fue asignada a Int. Bioaccess systems corp. En Estados Unidos No. 4805222. Esta invención se basa en la dinámica de pulsaciones de tecla de un individuo para identificarlo.

United States Patent [19]
Young et al.

[11] Patent Number: 4,805,222
[45] Date of Patent: Feb. 14, 1989

[54] METHOD AND APPARATUS FOR VERIFYING AN INDIVIDUAL'S IDENTITY

[75] Inventors: James R. Young, Palo Alto; Robert W. Hammon, San Jose, both of Calif.

[73] Assignee: International Bioaccess Systems Corporation, New York, N.Y.

[21] Appl. No.: 813,262

[22] Filed: Dec. 23, 1985

[51] Int. Cl.* G06K 9/00

[52] U.S. Cl. 382/2; 382/30; 340/825.31; 340/825.34

[58] Field of Search 380/2, 23; 382/2, 16, 382/30; 364/550, 569, 200, 900; 340/527, 528, 543, 825.3, 825.31, 825.32, 825.33, 825.34

[56] References Cited

U.S. PATENT DOCUMENTS

3,993,976 11/1976 Ginsburg 382/21
4,197,524 4/1980 Salem 340/825.31
4,455,588 6/1984 Mitchiells et al. 340/825.31
4,621,334 11/1986 Garcia 364/550

OTHER PUBLICATIONS

Gaines, R. Stockton et al., "Authentication by Keystroke Timing: Some Preliminary Results", Rand Co., R-2526-NSF, 5/80.
Umphress, David et al., "Identity Verification Through Keyboard Characteristics", *Int. J. Man–Mach. St.*, pp. 263–273, 1985.
Riganati, John P., "An Overview of Electronic ID Systems", *WESCON Tech. Papers*, 1975.
Resnick, R. J. et al., "Multi-A Multi-Function ID System", *WESCON Tech. Papers*, 1975.
Cotton, Ira W. et al., "Approaches to Controlling Personal Access to Computer Terminals", *Proceeding Computer Networks: Trends & Appns.*, 1975.
"Guidelines on Evaluation of Techniques for Automated Personal ID", U.S. Dept. of Comm./NBS, FIPS, PUB 48, 4.1.77.
"Keystroke Dynamics Authentication of Computer Terminal Users", Bioaccess System 2000, 2000A, 2001, 2011, and OEM, 6.29.84.
Kullback, Solomon, *Information Theory & Statistics*, John Wiley & Sons Inc., pp. 3383, 1959.

Primary Examiner—Leo H. Boudreau
Assistant Examiner—Jose L. Couso
Attorney, Agent, or Firm—Blakely, Sokoloff, Taylor & Zafman

[57] ABSTRACT

A device and method for verifying the identity of an individual based on keystroke dynamics comprising a keyboard for the inputting of data in the form of alphanumeric characters by keystrokes, a timing encoder coupled to the keyboard for timing periods between keystrokes, a CPU coupled to RAM and to the timing encoder for generating a template for the individual, the template comprising a first plurality of features based upon a first set of time periods between keystrokes from a first set of keystrokes of the individual and the CPU determining a plurality of extracted features based upon a second set of time periods from a second set of keystrokes, and comparing the template to the plurality of extracted features such that the identity of the individual may be verified.

3 Claims, 11 Drawing Sheets

Figura 2.10 Página principal de la patente No. 4805222

En Enero de 1990 M. Kirby y L. Sirovich publicaron “Application of the Karhunen-loeve procedure for the characterization of human faces”, un paper que trata sobre el uso de simetrías naturales (imágenes espejo) en una familia de patrones bien definida (rostros humanos). Anteriormente en 1987 ellos habían publicado otro paper titulado “A Low-Dimensional Procedure for the Characterization of Human Faces” y que también trataba el tema de reconocimiento facial.

En 1991 Matthew Turk y Alex Pentland publican un paper llamado “Eigenfaces for recognition” en “Journal Cognitive Neuroscience”, donde se planteaba que el reconocimiento facial en tiempo real era posible.

En Octubre de 1992 tuvo su primera reunión Biometric Consortium una organización establecida por La agencia de seguridad nacional (NSA) de Estados Unidos; este consorcio inicialmente estaba compuesto por agencias gubernamentales, miembros de la industria privada y de la academia.

De 1993 a 1997 corrió el programa FERET (FacE REcognition Technology) patrocinado por el departamento de defensa hasta la Agencia de Investigación de Productos de Avance de Defensa (DARPA) de Estados Unidos, su misión principal fue el desarrollo de capacidades de reconocimiento facial automático que pudiera ser empleado por personal de seguridad, inteligencia y justicia en el desarrollo de sus labores.

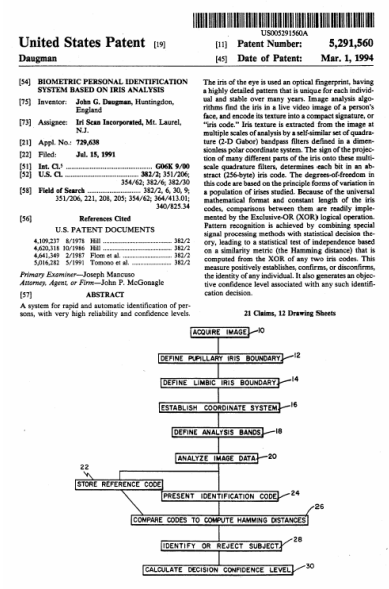
En 1993 la agencia de defensa nuclear de Estados Unidos inicio trabajos con IriScan, Inc. (empresa creada por Leonard Flom y Aran Safir) para probar y entregar un prototipo de unidad de reconocimiento de iris.

En 1994 al final de la competencia de un sistema de identificación de huellas digitales integrado y automatizado (IAFIS), donde se investigaba y se identificaron tres grandes retos: 1. Adquisición de la huella digital, 2. extracción local de las características de las ondulaciones y 3. Comparación de patrones de las características de las ondulaciones, Lockheed Martin Inc. fue seleccionado para construir el IAFIS del FBI.

El primer sistema AFIS conocido que se construyó y que soporta huellas palmares se cree que fue desarrollado en 1994 por una compañía húngara conocida como RECOWARE y el sistema se conoce con el nombre de RECOderm^{TM}.

Figura 2.11 Estación de trabajo de ingreso de datos del sistema RECOderm^{TM}

El primero de marzo de 1994 John G. Daugman patentó en Estados Unidos un Sistema biométrico de identificación personal basado en el análisis del iris, patente asignada a IriScan Incorporated, con la patente No. 5291560, también fue patentado ante la organización mundial de propiedad intelectual con el No. 9409446 el 28 de abril de 1994. Los algoritmos presentados en esta patente son la base de todos los algoritmos actuales de sistemas de reconocimiento de iris.



US005291560A

United States Patent [19]
Daugman

[11] **Patent Number: 5,291,560**
[45] **Date of Patent: Mar. 1, 1994**

[54] **BIOMETRIC PERSONAL IDENTIFICATION SYSTEM BASED ON IRIS ANALYSIS**

[75] Inventor: **John G. Daugman**, Huntingdon, England

[73] Assignee: **Iri Scan Incorporated**, Mt. Laurel, N.J.

[21] Appl. No.: **729,638**

[22] Filed: **Jul. 15, 1991**

[51] **Int. Cl.**[5] **G06K 9/00**

[52] **U.S. Cl.** **382/2**; 351/206; 354/62; 382/6, 382/30

[58] **Field of Search** 382/2, 6, 30, 9; 351/206, 221, 208, 205; 354/62; 364/413.01; 340/825.34

[56] **References Cited**
U.S. PATENT DOCUMENTS

4,109,237	8/1978	Hill	382/2
4,620,318	10/1986	Hill	382/2
4,641,349	2/1987	Flom et al.	382/2
5,016,282	5/1991	Tomono et al.	382/2

Primary Examiner—Joseph Mancuso
Attorney, Agent, or Firm—John P. McGonagle

[57] **ABSTRACT**

A system for rapid and automatic identification of persons, with very high reliability and confidence levels.

The iris of the eye is used an optical fingerprint, having a highly detailed pattern that is unique for each individual and stable over many years. Image analysis algorithms find the iris in a live video image of a person's face, and encode its texture into a compact signature, or "iris code." Iris texture is extracted from the image at multiple scales of analysis by a self-similar set of quadrature (2-D Gabor) bandpass filters defined in a dimensionless polar coordinate system. The sign of the projection of many different parts of the iris onto these multi-scale quadrature filters, determines each bit in an abstract (256-byte) iris code. The degrees-of-freedom in this code are based on the principle forms of variation in a population of irises studied. Because of the universal mathematical format and constant length of the iris codes, comparisons between them are readily implemented by the Exclusive-OR (XOR) logical operation. Pattern recognition is achieved by combining special signal processing methods with statistical decision theory, leading to a statistical test of independence based on a similarity metric (the Hamming distance) that is computed from the XOR of any two iris codes. This measure positively establishes, confirms, or disconfirms, the identity of any individual. It also generates an objective confidence level associated with any such identification decision.

21 Claims, 12 Drawing Sheets

Figura 2.12 Página 1 de la patente No. 5291560

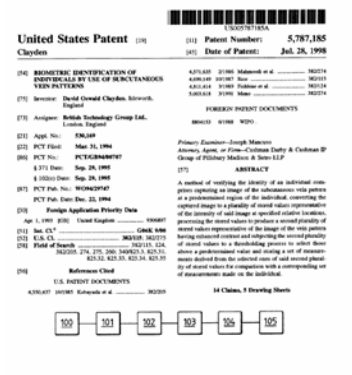
OKI Electric Industry Ltd., uno de los líderes mundiales en el suministro de cajeros automáticos (ATM) en 1995 ofrece la tecnología de reconocimiento de iris a los bancos clientes en Japón.

En 1997 se presenta el proyecto HA-API (Human Authentication API), un estándar de interoperabilidad biométrico genérico y centrado en facilitar la integración y permitir el intercambio e independencia del vendedor.

En 1998 el FBI lanza CODIS (Combined DNA Index System) para el almacenamiento digital, búsqueda y recuperación de los marcadores de ADN con el propósito de la entrada en vigor de la ley forense en Estados Unidos.

El 28 de Julio de 1998 Clayden David Oswald patentó una identificación biométrica de individuos usando patrones de venas subcutáneas, esta patente fue asignada a British tech group y patentada en Estados Unidos No. 5787185, Gran Bretaña No. GB2276749, Organización Mundial de patentes No. 9422370 y European Patent Office

No. 691822. El nueve de octubre de 2001 se patentó una segunda invención, esta vez por parte de Hwan-Soo Choi, asignada a BK Systems y titulada Aparato y método para identificar individuos a través de sus patrones de venas subcutáneas y sistema integrado usando dicho aparato y método, se patento en Estados Unidos No. 6301375 y en Japón No. 10295674.



United States Patent [19]
Clayden

[11] Patent Number: 5,787,185
[45] Date of Patent: Jul. 28, 1998

[54] BIOMETRIC IDENTIFICATION OF INDIVIDUALS BY USE OF SUBCUTANEOUS VEIN PATTERNS

[75] Inventor: David Oswald Clayden, Isleworth, England

[73] Assignee: British Technology Group Ltd., London, England

[21] Appl. No.: 536,169

[22] PCT Filed: Mar. 31, 1994

[86] PCT No.: PCT/GB94/00707

§ 371 Date: Sep. 29, 1995

§ 102(e) Date: Sep. 29, 1995

[87] PCT Pub. No.: WO94/25947

PCT Pub. Date: Dec. 22, 1994

[30] Foreign Application Priority Data

Apr. 1, 1993 [GB] United Kingdom 9306897

[51] Int. Cl.[6] G06K 9/00

[52] U.S. Cl. 382/115; 382/275

[58] Field of Search 382/115, 124, 382/205, 274, 275, 280; 340/825.3, 825.31, 825.32, 825.35, 825.34, 825.35

[56] References Cited

U.S. PATENT DOCUMENTS

4,393,437 10/1985 Kobayashi et al. 382/205

4,571,635 2/1986 Mahowald et al. 382/274
4,699,149 10/1987 Rice 382/115
4,811,414 3/1989 Fishbine et al. 382/124
5,003,618 3/1991 Mintz 382/274

FOREIGN PATENT DOCUMENTS

0806153 6/1968 WIPO

Primary Examiner—Joseph Mancuso
Attorney, Agent, or Firm—Cushman Darby & Cushman IP Group of Pillsbury Madison & Sutro LLP

[57] ABSTRACT

A method of verifying the identity of an individual comprises capturing an image of the subcutaneous vein pattern at a predetermined region of the individual, converting the captured image to a plurality of stored values representative of the intensity of said image at specified relative locations, processing the stored values to produce a second plurality of stored values representative of the image of the vein pattern having enhanced contrast and subjecting the second plurality of stored values to a thresholding process to select those above a predetermined value and storing a set of measurements derived from the selected ones of said second plurality of stored values for comparison with a corresponding set of measurements made on the individual.

14 Claims, 5 Drawing Sheets

100 101 102 103 104 105

Figura 2.13 Página Principal de la patente No. 5787185

En 1999 la Organización Internacional de Aviación Civil (ICAO) se inició el estudio de la aplicabilidad de la tecnología actual disponible en biometría con la emisión y procesos de inspección pertinentes a la Maquina lectora de Documentos de Viaje (MRTD), como resultado se estableció que a más tardar el primero de Abril del 2010, los países que hacen parte de la ICAO deben implementar el e-passport con todas las recomendaciones que figuran en el documento de la MRTD.

En el 2000 se dio inicio a la prueba de reconocimiento facial del vendedor (FRVT) que proporciona evaluaciones gubernamentales independientes de tecnologías y prototipos de reconocimiento facial. Estas evaluaciones se diseñan para proporcionar la información al gobierno de Estados Unidos y agencias de ley con información que los ayude a determinar donde y como tecnología de reconocimiento facial puede ser mejor desarrollada, se considera que es el reemplazo del programa FERET.

En Enero de 2001 se usó el sistema de reconocimiento facial en el Super Bowl en Tampa Florida, en búsqueda de identificar individuos buscados que entraran al estadio. La demostración no encontró individuos buscados pero manejo el fallo en identificación en más de una docena de fanáticos. En consecuencia los medios y el congreso presentó grandes preocupaciones en cuanto a la introducción de biométricos y lo relacionado con la privacidad.

En Marzo de 2001 el "Journal of the Korean Physical Society" publica un paper de Sang-Kyun Im, Hyung-Man Park, Young-Woo Kim, Sang-Chan Han, Soo-won Kim y Chul-Hee Kang titulado "An Biometric identification system by extracting hand vein patterns", que explica el uso de los patrones de la venas en las manos para la identificación de una persona.

La organización Internacional de Estándares (ISO) estableció el subcomité 37 en el Comité de Junta Técnica (JTC) 1 en el 2002 para apoyar la estandarización de tecnologías biométricas genéricas.

El 1 de febrero de 2002 se creo el programa FEARID (Forensic ear identification) con una duración de 40 meses, un programa de la Unión Europea y que era manejado por CORDIS (Community Research & Development Information Service) en el se estudiaba propuestas para un procedimiento estandarizado para la recolección de impresiones de oreja y un procedimiento para la clasificación y comparación. El 10 de febrero de 2004 publicaron un paper en Forensic Science Internacional titulado "Exploratory study on classification and individualisation of earprints, escrito por Lynn Meijerman, Sarah Sholl, Fracesca De Conti, Marta Giacon, Cor van der Light, Andrea Drusini, Meter Vanezis, y George Maat.

El 30 de Mayo de 2002 se publica la concesión de una patente en Colombia a Jean François Mainguet cuyo dueño es Thomson CSF, la patente se titula “Sistema de lectura de huellas dactilares”.

En el 2003 se establece el Foro Europeo de Biométricos (European Biometrics Forum) una organización europea independiente apoyada por la comisión europea cuya visión global es establecer a la Unión Europea como el líder mundial en excelencia biométrica.

En Colombia Trek 2000 International Ltd. solicita la patente para un “dispositivo portátil que tiene capacidades de autentificación basadas en biometría”, inventado por Poo Teng Pin y Lim Lay Chuan y publicada el 30 de Enero de 2004

En Mayo de 2004 empezó El gran reto del reconocimiento facial (The Face Recognition Grand Challenge FRGC) consiste en una serie de problemas reto que son progresivamente mas difíciles, el objetivo principal de FRGC es mejorar la calidad de los sistemas de reconocimiento facial sobre la prueba de reconocimiento facial del vendedor (the Face Recognition Vendor Test FRVT)

En el 2005 Sarnoff Corporation demostró en la conferencia 2005 del Biometrics Consortium, la finalización de la investigación y sistema prototipo capaz de recolectar imágenes de iris de individuos caminando a través de un portal, llamado Iris on the Move^{TM}, este sistema puede identificar 20 personas por minuto, caminando a paso normal a través de un portal de reconocimiento. El sistema fue patentado el 14 de Diciembre de 2006 ante la Organización Mundial de Propiedad Intelectual con el nombre de Método y aparato para obtener información biométrica del iris de un sujeto en movimiento, sus inventores fueron Dominick Loiacono y

James R. Matey, se patentó con el No. WO2006132686A2 y WO2006132689A2

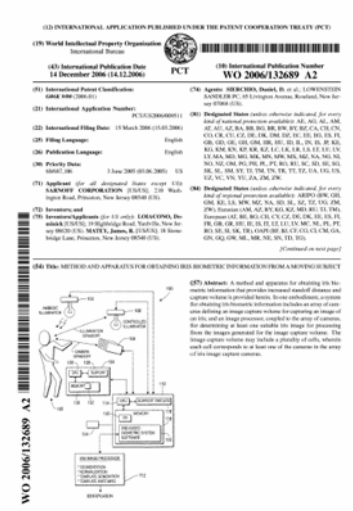


Figura 2.14 Página Principal de la patente No. WO2006132689A2

2.2 Características

La biometría aprovecha que existen ciertas características biológicas o conductuales singulares e inalterables, por lo que pueden ser analizados y medidos para crear una huella biométrica. Estas características son difíciles de perder, transferir u olvidar y son perdurables en el tiempo.

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

- Universalidad: que tan común es encontrar este biométrico en los individuos.
- Singularidad: que tan único o diferenciable es la huella biométrica entre uno y otro individuo.
- Permanencia: que tanto perdura la huella biométrica en el tiempo de manera inalterable.
- Recolectable: Que tan fácil es la adquisición, medición y almacenamiento de la huella biométrica.

- Calidad: que tan preciso, veloz y robusto es el sistema en el manejo de la huella biométrica.
- Aceptabilidad: Que tanta aprobación tiene la tecnología entre el público.
- Fiabilidad: Que tan fácil es engañar al sistema de autenticación.

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

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

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

No todo rasgo físico o conductual es propicio para establecer la identidad biométrica. La elección del rasgo está condicionada por la rapidez y la confiabilidad requeridas, así como por el presupuesto y el equipo con que se cuenta [11].

En general un sistema biométrico se puede esquematizar de la siguiente manera:

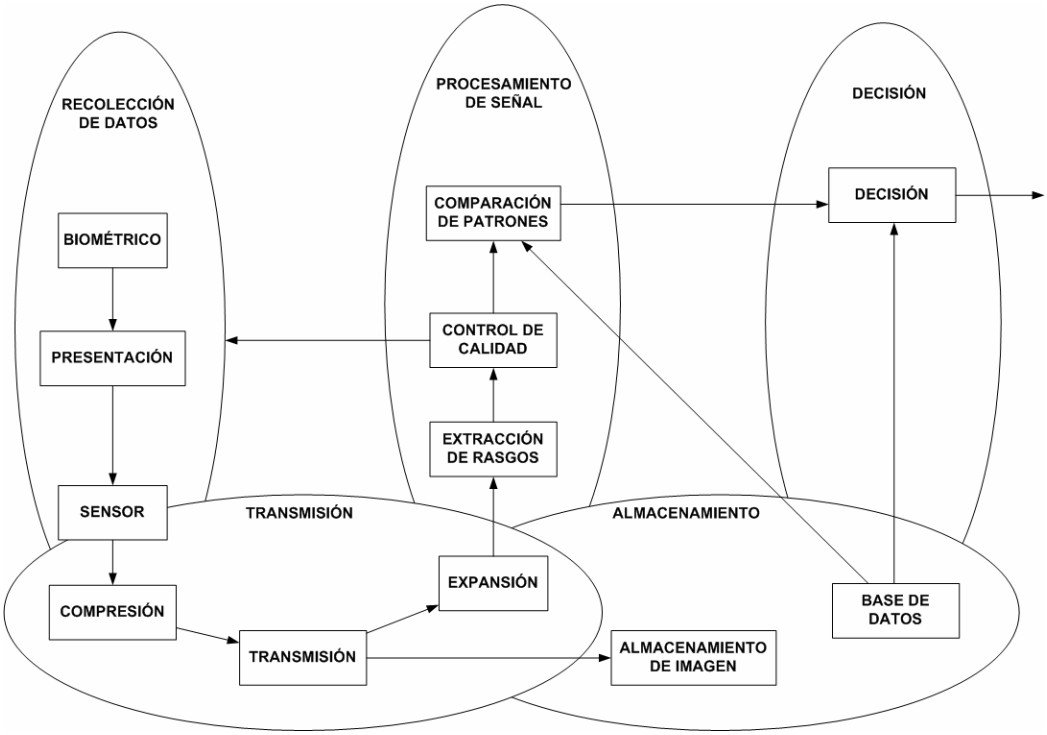


Figura 2.15 Sistema biométrico genérico [12]

En la biometría hay tres términos de uso muy frecuente que son: reconocimiento, verificación e identificación, cada uno de estos términos que a simple vista parecen muy similares, tienen significados muy diferentes y se desglosan a continuación:

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.

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, una tarjeta inteligente, etc. 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.

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.

El término autenticación es utilizado usualmente como sinónimo de verificación, sin embargo en el lenguaje de las tecnologías de información, autenticar significa hacer saber al sistema la identidad del usuario sin importar el modo de operación.

2.3 Confiabilidad

Los sistemas biométricos tienen el propósito y la finalidad de discernir entre si un individuo pertenece o no a una base de datos con los datos previamente establecidos, así como la determinación específica de un individuo basado sólo en las características biométricas de la persona.

Los diferentes tipos de identificación son:

Identificación cerrada: En el proceso de comparación uno a muchos, el usuario presenta su(s) dato(s) biométrico(s) y el dato

biométrico se compara contra la base de datos, donde se sabe que existe, buscando la identidad más probable del usuario.

Identificación abierta: es un proceso hibrido entre la verificación y la identificación cerrada, donde la persona no reclama una identidad específica, entonces se compara contra toda la base de datos para verificar si existe en la base de datos, una vez se verifica que posiblemente existe, dentro de las coincidencias más probables, determina quién es el usuario.

Para la toma de decisiones el resultado de cualquiera de las comparaciones que se hagan puede presentar una de tres posibilidades dependiendo la puntuación que se alcance en la comparación de la plantilla y el dato biométrico y del umbral que se le haya dado al sistema; las tres posibles alternativas son:

– Hay correlación: es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación esta dentro de los umbrales de coincidencia.

– No hay correlación: es decir que al comparar el dato biométrico capturado con la(s) plantilla(s) almacenada(s) la puntuación esta fuera de los umbrales de coincidencia.

– Imposibilidad de alcanzar conclusión definitiva: es decir que hay falta de información para poder hacer una comparación adecuada.

La precisión de un sistema biométrico está determinado por una serie de pruebas, que están divididas en tres categorías: tecnología, escenario y operacional; y para su evaluación se consideran varios conceptos que se pueden generalizar en dos conceptos: la probabilidad

de que alguien autorizado sea rechazado y la probabilidad de que alguien no autorizado sea aceptado, el término a usar varía, a grandes rasgos, dependiendo el tipo de comparación que se haga y en que categoría se haga la evaluación.

Los términos comúnmente observados son los siguientes:

La Tasa de falsa aceptación: (FAR – False Acceptance Rate) Es una estadística que muestra la actuación del biométrico, típicamente cuando opera en la tarea de verificación.

En general entre más bajo sea el valor de la tasa de falsa aceptación, más alto es la precisión del sistema biométrico. En esta tasa se muestra el porcentaje de número de veces que el sistema produce una falsa aceptación.

Es decir cuando un individuo es identificado como usuario de manera incorrecta. Este valor debe ser lo suficientemente bajo como para que no se impida el ingreso a los usuarios, pero no tanto que permita el ingreso de personal no autorizado.

El valor depende de lo sensible del área o sistema a proteger y de la necesidad del usuario. A nivel de fabricantes la mayoría tienen esta tasa entre el 0.0001% y el 0.1%. La tasa dada normalmente asume intentos pasivos del impostor.

FAR= PR x FMR x (1-FTA)

Tasa de Falso Rechazo (FRR - False Reject Rate) La probabilidad de que un dispositivo rechace una persona autorizada. Comercialmente su valor varía entre el 0.00066% y el 1%.

FRR=FTA+(1-FTA)x BER +(1-FTA)x(1-BER)x FNMR

El punto de intersección entre la tasa de falsa aceptación y la tasa de falso rechazo se conoce como la **tasa de error igual** (EER - Equal Error Rate), algunas veces se llama tasa de error cruzada (CER – Crossover Error Rate).

Es una estadística que muestra la actuación del biométrico, típicamente cuando opera en la tarea de verificación. En general entre más bajo sea el valor de la tasa de error igual, más alto es la precisión del sistema biométrico.

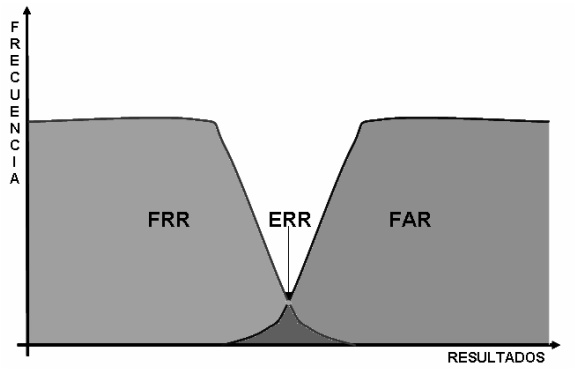


Figura 2.16 Definición de la tasa de error igual.

Otros términos utilizados son:

Tasa de Falsa alarma: (False Alarm Rate) Una estadística usada para medir la calidad del biométrico cuando opera en el modo de identificación abierta (watchlist ó comparación uno a pocos). Este es el porcentaje de veces que una alarma suena incorrectamente en un individuo que no esta en el sistema de la base de datos.

Tasa de falsa coincidencia: (FMR - False Match Rate) La probabilidad de que un sistema biométrico identifique incorrectamente un

individuo o que falle para rechazar un impostor. Alternativa a Tasa de falsa aceptación (FAR).

Tasa de falsa no-coincidencia: (FNMR - False Non-Match Rate) es parecida a la tasa de falso rechazo (FRR), con la diferencia de que la FRR incluye la tasa de falla para capturar el error (Failure to Adquire error rate).

Error tipo I: Este tipo de error ocurre en una prueba estadística cuando una reclamación valida es rechazada. Es decir cuando falla al rechazar una reclamación valida. Por ejemplo Claudia reclama ser Claudia, pero el sistema niega el reclamo de manera incorrecta.

Error Tipo 2: Este tipo de error ocurre en una prueba estadística cuando una reclamación falsa es aceptada. Es decir cuando falla al aceptar una reclamación falsa. Por ejemplo Erika reclama ser Sandra y el sistema acepta el reclamo de manera incorrecta.

2.4 Tipos de Sistemas Biométricos

Los sistemas biométricos se pueden clasificar en dos grandes grupos, los que pertenecen a la biometría estática y los que pertenecen la biometría dinámica.

La biometría estática comprende las características propias de cada individuo, éstas son inalterables y no cambian con el paso del tiempo, así como tampoco influye el estado de ánimo del individuo en su identificación.

La biometría dinámica se refiere a la medición de las características del comportamiento de un individuo. [13]

Biometría estática

• Huellas dactilares.
• Biometría del ojo: por un lado, el iris y por otro, la retina.
• Geometría de la mano.
• ADN.
• Emisiones térmicas.
• Características estáticas de la cara.
• Venas de muñecas y manos.
• Composición química del olor corporal.
• Rayas de la mano (quiromancia).
• Poros de la piel.

Biometría dinámica

• Gestos y movimiento corporal.
• Dinámica del tecleo.
• Manuscritos.
• Firma.
• Voz.

La clasificación de las técnicas biométricas puede realizarse según tres criterios comerciales y gubernamentales:

Mercados desarrollados

• Reconocimiento facial.
• Reconocimiento del iris.
• Reconocimiento de la distribución de las venas de la retina.
• Reconocimiento de la forma de las manos.

• Reconocimiento de las huellas dactilares.
• Reconocimiento de la huella de la palma.

Mercados emergentes

• Reconocimiento de la voz (de cómo se dice algo).
• Reconocimiento de la forma de firmar.
• Imagen infrarroja de la mano para ver la distribución de las venas.
• Imagen infrarroja de la cara para determinar un perfil superficial de las venas de la cara.

En el laboratorio y con alta tecnología

• Reconocimiento de ADN.
• Reconocimiento de la forma de caminar.
• Dinámica del tecleo.
• Reconocimiento de la forma de las orejas y las uñas [14].

2.5 Errores en sistemas biométricos

La mayoría de los sistemas biométricos son capaces de verificar la identidad con un margen de error de menos del 1/100.000 [15].

Un típico sistema biométrico de verificación comete dos tipos de errores:

Equivocarse al tener la certeza que las impresiones de dos diferentes huellas provengan del mismo dedo (llamada falsa coincidencia) y al tener la certeza de que dos impresiones de la misma huella provengan de diferentes dedos (llamada falsa no coincidencia).

Estos dos tipos de errores son usualmente denotados como falsa aceptación y falso rechazo, sin embargo es necesario hacer una distinción de acuerdo a la aplicación.

En sistemas de reconocimiento positivo (por ejemplo, un sistema de control de acceso) una falsa coincidencia determina la falsa aceptación de un impostor, mientras que una falsa no coincidencia causa el falso rechazo de un usuario genuino. Por otro lado, en una aplicación de reconocimiento negativo (por ejemplo, impidiéndoles a los usuarios obtener los beneficios de bienestar bajo falsas identidades) una falsa coincidencia resulta en el rechazo de una petición genuina, mientras que una falsa no coincidencia resulta en la falsa aceptación del intento de un impostor. En consecuencia, la utilización de la notación de "falsa coincidencia/no coincidencia" no depende de la aplicación y además es preferida antes que "falsa aceptación/falso rechazo". Sin embargo, la Tasa de Falsa Aceptación (False Acceptance Rate - FAR) y la Tasa de Falso Rechazo (False Rejection Rate - FRR) son indicadores ampliamente utilizados en entornos comerciales, militares, etc.

El rendimiento de un sistema de identificación se mide calculando el número relativo de veces (por medio de un porcentaje) que el sistema falla en identificar correctamente al usuario de entrada, o lo que es lo mismo, con qué frecuencia una realización de prueba es asignada a una identidad errónea.

Este valor es directo para cada usuario. A continuación se muestra el procedimiento para la generalización en un sistema general.

Se define como ci al conjunto de individuos que conforman el sistema biométrico.

Si se define ci ≠ 0, se define el error de clasificación para el usuario Xi como:

$$\gamma_i = 1 - \frac{1}{C_i} \sum \delta\left[\bar{i}\left(x_i^k\right), i\right] \quad \text{.....(1)}$$

De forma general, se conoce como ‘ovejas’ (sheep) a los usuarios con bajo error de clasificación (son dóciles frente al grupo y se dejan llevar), y ‘cabras’ (goats) a los usuarios con alto error de clasificación (son pocos los que dan problemas, pero son los que marcan las características del grupo).

A partir de las tasas usuario a usuario, el error de clasificación promedio del sistema se puede obtener como:

$$\bar{\gamma} = \frac{1}{m^*} \sum_{\substack{i=1 \\ C_i \neq 0}}^{m} \gamma_i \quad \text{.....(2)}$$

Y a partir de:

$$\bar{\gamma}_M = \frac{1}{m_M^*} \sum_{\substack{i=1 \\ X_i \in M \\ c_i \neq 0}}^{m} \gamma_i \qquad \text{y} \qquad \bar{\gamma}_F = \frac{1}{m_F^*} \sum_{\substack{i=1 \\ X_i \in F \\ c_i \neq 0}}^{m} \gamma_i \quad \text{.....(3)}$$

Se puede calcular el error de clasificación balanceado por sexos como:

$$\bar{\gamma}_{MF} = \frac{1}{2}\left(\bar{\gamma}_M + \bar{\gamma}_F\right) \quad \text{.....(4)}$$

Los valores anteriores son diferentes al error de clasificación del conjunto de prueba, calculado como:

$$\gamma = 1 - \frac{1}{c}\sum_{i=1}^{m}\sum_{k=1}^{c_i}\delta\left[\hat{i}\left(x_i^k\right), i\right] = \sum_{i=1}^{m} p_i \gamma_i \qquad \text{.....(5)}$$

2.6 Funcionamiento en modo identificación

Desde el punto de vista del funcionamiento de los sistemas automáticos de reconocimiento de personas mediante rasgos biométricos, se hace necesario clasificar las dos perspectivas fundamentales de trabajo de los mismos en dos grandes grupos: el modo identificación y el modo verificación [16].

En el modo identificación, el objetivo es clasificar una realización determinada de un rasgo biométrico de identidad desconocida como perteneciente a uno de entre un conjunto de N posibles individuos.

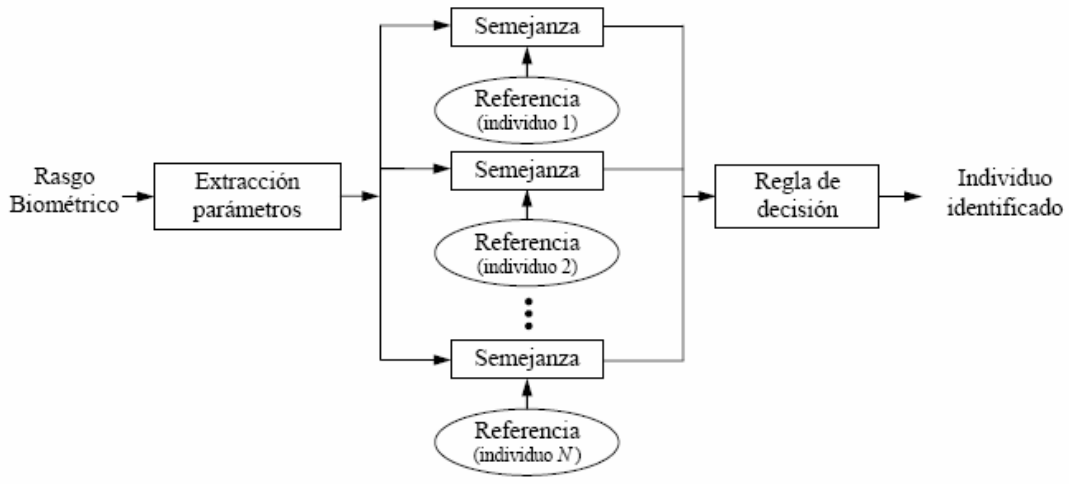


Figura 2.17 Diagrama a bloques de la estructura típica de un sistema de identificación.

Dentro de estos sistemas, es necesario diferenciar dos posibles casos:

• **Identificación en conjunto cerrado**: en este caso, el resultado del proceso es una asignación de identidad a uno de los individuos modelados por el sistema, y conocidos como usuarios. Existen, por tanto, N posibles decisiones de salida posibles.

• **Identificación en conjunto abierto**: en este caso, se debe considerar una posibilidad adicional a las N del caso anterior: que el individuo que pretende ser identificado no pertenezca al grupo de usuarios, con lo que el sistema de identificación debería contemplar la posibilidad de no clasificar la realización de entrada como perteneciente a las N posibles decisiones.

2.7 Funcionamiento en modo verificación

Los sistemas de verificación de individuos, por el contrario de los sistemas en modo identificación, toman dos entradas:

• Una realización del rasgo biométrico a verificar,

• Una solicitud de identidad, que puede ser realizada de diversas formas (lectura de tarjeta magnética individual, introducción mediante teclado o mediante voz de un código de locutor, etc.).

De este modo, las dos únicas salidas o decisiones del sistema son la aceptación o rechazo del individuo como aquél que pretende ser. De esta forma, el locutor solicitante será catalogado como usuario auténtico o bien como impostor, respectivamente [17].

La decisión de aceptar ó rechazar la locución de entrada como correspondiente al locutor solicitado dependerá de si el valor de parecido o probabilidad obtenido supera o no un determinado umbral de decisión.

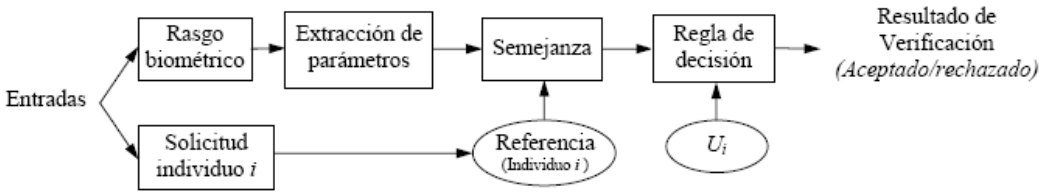


Figura 2.18 Diagrama a bloques de la estructura típica de un sistema de verificación.

2.8 Caracterización gráfica de sistemas de verificación

A partir de los valores actuales de falsa aceptación y falso rechazo no es posible predecir cuál será el comportamiento del sistema en otro punto de trabajo diferente.

De esta forma, si se quiere estimar el rendimiento del sistema bajo otras condiciones, es necesario modelar el comportamiento del sistema de forma independiente a cualquier condición inicial.

Ante una entrada al sistema, se tienen dos casos posibles:

• ‘s’, la realización de entrada pertenece al usuario

• ‘n’, la realización no pertenece al usuario, que es la condición opuesta.

Asimismo, el sistema puede tomar dos decisiones:

• ‘S’, la realización es aceptada como perteneciente al usuario solicitado

• ‘N’, la realización es rechazada

Estas condiciones se combinan para formar las cuatro probabilidades condicionales siguientes:

• P(S|s).- probabilidad de aceptación correcta
• P(S|n).- probabilidad de falsa aceptación (FA)
• P(N|s).- probabilidad de falso rechazo (FR)
• P(N|n).- probabilidad de rechazo correcto

Si estas condiciones se agrupan en una tabla se obtiene el siguiente resultado:

	Condición de entrada	
Decisión	s (usuario)	n (impostor)
S (aceptación)	P(S|s)	P(S|n)
N (rechazo)	P(N|s)	P(N|n)

Tabla 2.1 Probabilidades de entrada-respuesta en un sistema biométrico.

Y debe cumplirse:

$$P(S|s) + P(N|s) = 1 \quad (6)$$

y

$$P(S|n) + P(N|n) = 1 \quad (7)$$

Es posible estudiar el comportamiento del sistema representando las curvas de falso rechazo (error tipo I) y de falsa aceptación (error tipo II) en función del umbral de verificación, tal y como se muestra en la siguiente figura:

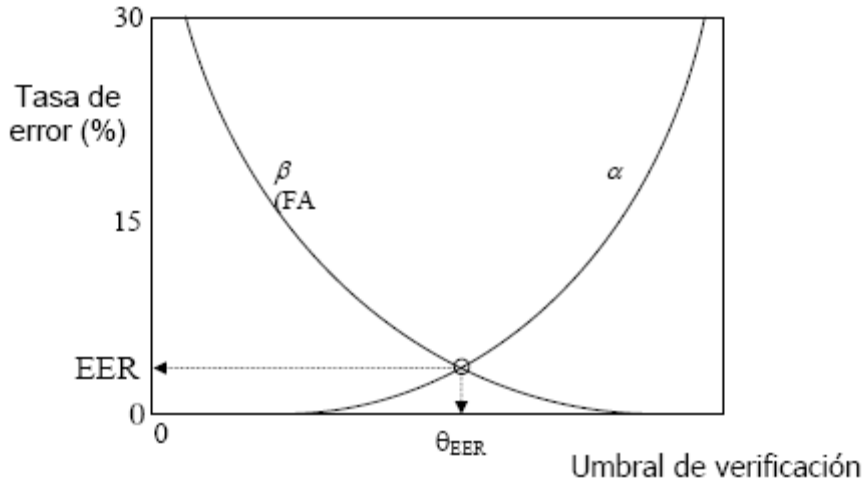


Figura 2.19 Curvas de Tasa de Error vs. Umbral de Verificación.

En el caso de umbrales independientes de usuario (único umbral común para todos los usuarios), las tasas de falso rechazo y falsa aceptación se pueden escribir en función de un único parámetro, $\alpha=\alpha(\theta)$ y $\beta=\beta(\theta)$.

Entonces, es posible resumir el comportamiento del sistema de una forma más compacta expresando β directamente como función de α:

$$\beta = f(\alpha)$$

En la figura anterior, se tienen representados tres posibles umbrales de decisión:

(a) *Criterio de decisión estricto:* Es aquel con muy pocas falsas aceptaciones, a costa de aumentar el número de falsos rechazos.

(b) *Criterio de decisión relajado:* Es aquel donde se permiten falsas aceptaciones, pero hay muy pocos falsos rechazos.

(c) *EER (equal error rate):* Este es el punto generalmente buscado, donde se igualan a posteriori los dos tipos de error (FA y FR).

Usando terminología de Teoría de la Comunicación, se denomina a la función f curva ROC (Receiver Operating Characteristic, o curva característica de funcionamiento del receptor).

De forma genérica, la función f es monótona decreciente y satisface las condiciones límite f(0)=1 y f(1)=0, como se puede observar en la figura siguiente:

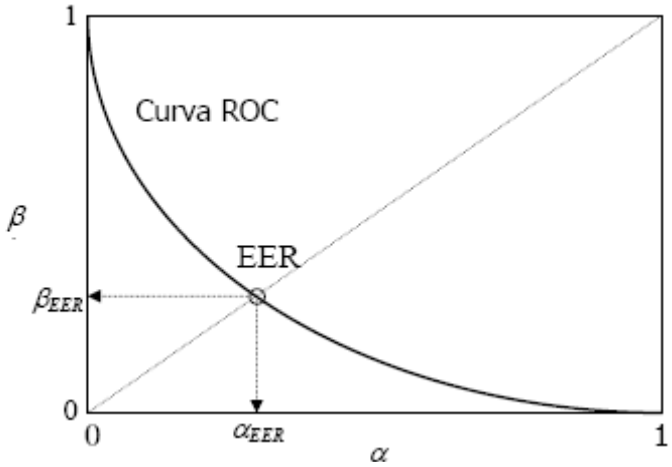


Figura 2.20 Curva ROC en relación con el punto EER.

Como se observa en la figura anterior, conociendo la función f completa, es posible evaluar de forma instantánea nuevos puntos de funcionamiento para el sistema.

Además, el valor de referencia dado por el EER se calcula rápidamente como intersección de la curva ROC con la curva α=β.

En la práctica, existen diferentes curvas ROC, en función del tipo de tasas de falso rechazo y falsa aceptación usadas. Así, en forma general se tienen:

- Curva ROC balanceada por sexos: $\beta_{MF} = f(\alpha_{MF})$
- Curva ROC promedio: $\beta = f(\alpha)$
- Curva ROC del conjunto de prueba: $\beta = f(\alpha)$

Sin embargo, trabajar manteniendo las diferentes curvas ROC resulta confuso, y se prefiere proceder con datos más concisos, como el EER, hablándose entonces de ε_{MF}, ε y ε.

Capítulo III. Huellas Digitales

En este capítulo se estudian las características propias de las huellas digitales, se comenta su unicidad, se definición y la forma en que puede ser almacenada.

Se mencionan y se analizan sus características en una forma global y posteriormente en una forma local, lo que añade más seguridad a la identificación de las huellas digitales.

Inmediatamente después se enumeran los diversos métodos biométricos basados en el reconocimiento de las huellas digitales y las dos formas en que se puede llevar a cabo la identificación biométrica.

Este capítulo está enlazado con los siguientes de manera que los conceptos enumerados en este punto son válidos para cualquier método de identificación biométrica basado en huellas dactilares.

Una huella dactilar o huella digital es la impresión visible o moldeada que produce el contacto de las crestas papilares. Depende de las condiciones en que se haga el dactilograma (impregnando o no de substancias de color distinto al soporte en que asiente), y de las características del soporte (materias plásticas o blandas, en debidas condiciones) [18].

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 interpapilares como las líneas más claras.

3.1 Características

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, generando configuraciones diversas.

Está demostrado científicamente que los dibujos que aparecen visibles en la epidermis que son perennes, inmutables y diversiformes:

Son perennes porque, desde que se forman en el sexto mes de la vida intrauterina, permanecen indefectiblemente invariables en número, situación, forma y dirección hasta que la putrefacción del cadáver destruye la piel.

Son inmutables, ya que las crestas papilares no pueden modificarse fisiológicamente. Si hay un traumatismo poco profundo, se regeneran y si es profundo, las crestas no reaparecen con forma distinta a la que tenían, sino que la parte afectada por el traumatismo resulta invadida por un dibujo cicatrizal.

Son diversiformes, pues no se ha hallado todavía dos impresiones idénticas producidas por dedos diferentes.

3.1.1. Características globales

Son los tipos de patrones geométricos de las crestas que son reconocibles a simple vista, basados en estos patrones las huellas dactilares se dividen en tres grupos principales: Loop, Arch y Whorl.

Estos grupos también se subdividen en grupos más pequeños, como el caso del Loop que se subdivide en Left loop y Right loop.

Usualmente la determinación del patrón al que pertenece la huella dactilar se obtiene mediante el conocimiento de sus puntos singulares.

Figura 3.1. (a) *(b)* *(c)*

Figura 3.1 (a) Huella digital tipo Arch; (b) Huella digital tipo Loop;(c) Huella digital tipo Whorl [19].

Área Patrón: Es la parte principal de la huella dactilar y está constituida por las crestas y todas sus características. Generalmente se coloca alrededor del centro del dedo a identificar, ya que en esta zona se concentra la mayor cantidad de información.

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.

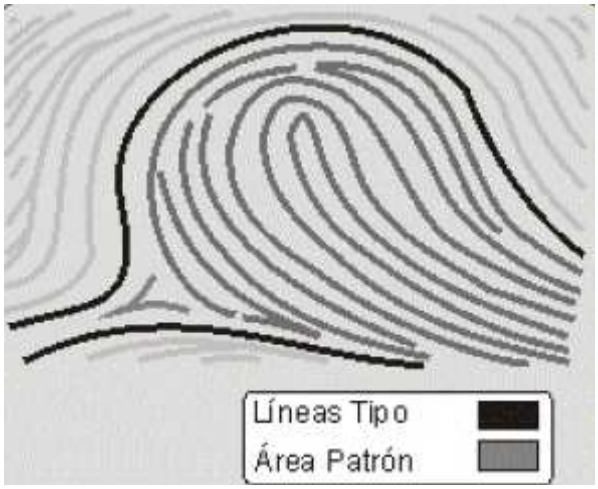


Figura 3.2 Área patrón y líneas tipo.

Dos individuos pueden tener las mismas características globales pero siempre tendrán diferentes características locales de la huella [20].

3.1.1.1 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, las técnicas para su determinación automática son muy complejas.

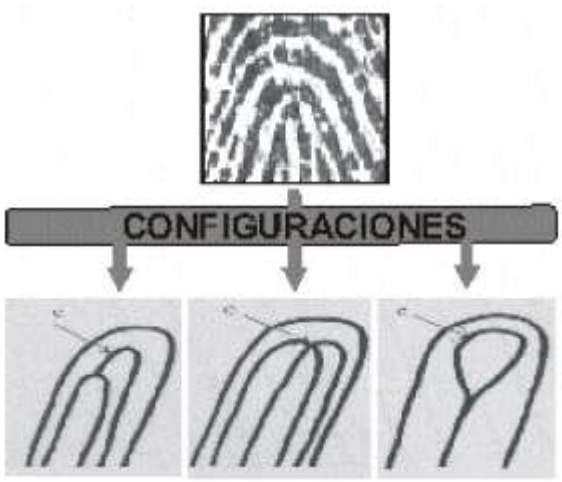


Figura 3.3 Puntos singulares, configuraciones del punto Core

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.

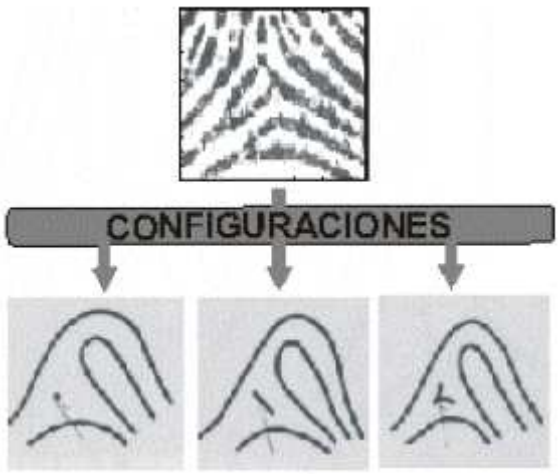


Figura 3.4 Puntos singulares, configuración del punto Delta

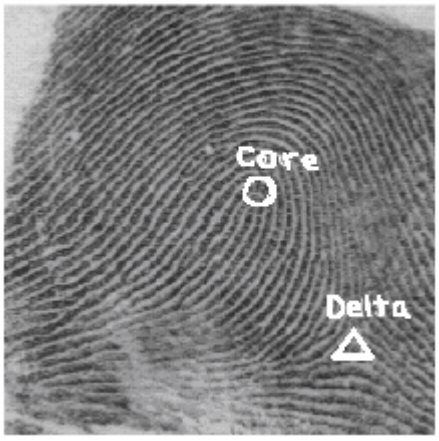


Figura 3.5 Puntos singulares de la huella dactilar [21].

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 las mismas 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 [22].

3.1.2.1 Minucias

Minucias, minutia, trivia, minutiae; Sinónimos: pequeñeces, nimiedades, detalles minuciosos, pequeñas cosas, trivialidades [23].

Las crestas en una huella dactilar no son continuas ni rectas, sino más bien cambian de dirección, cortándose y bifurcándose [24]. 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:

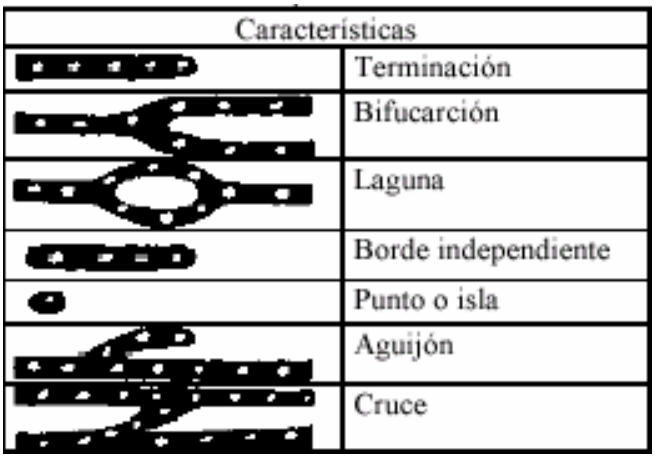


Figura 3.6 Tipos de minucias

1. Laguna (Enclosure): Es una cresta que se divide en dos ramas y se vuelve a unir otra vez luego de recorrer una distancia corta creando un área cerrada.

2. Punto (Dot). Es una cresta muy pequeña, a tal grado que es semejante a un punto.

3. Borde 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. Terminación (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. Cruce (Crossover): Es producida por la unión de dos minucias de bifurcación [25].

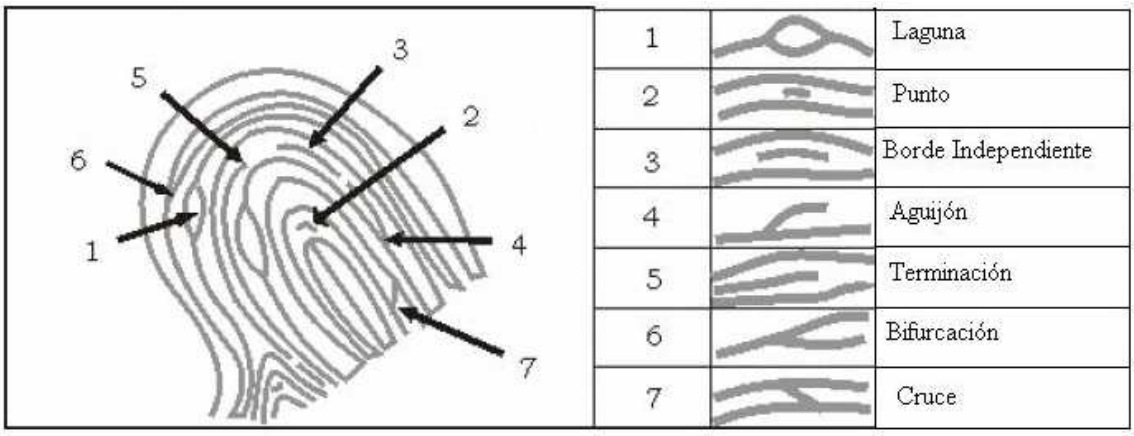


Figura 3.7 Tipos de minucias en una huella digital.

Las minucias son clasificadas en dos categorías: tipos básicos y compuestos.

Los tipos compuestos están constituidos a partir de los tipos básicos. Las minucias de finalización y bifurcación son consideradas como los tipos básicos y el resto de las minucias son consideradas como los tipos compuestos. Por ejemplo, una laguna es la unión de dos bifurcaciones de direcciones opuestas; una cresta corta es la unión de dos minucias de finalización con una separación muy pequeña.

Los principales atributos de una minucia son:

Dirección: Cada minucia posee una dirección particular, siendo ésta concordante con la dirección de la cresta a la que pertenece.

Posición: Es la ubicación geométrica de la minucia con respecto al eje de referencia de la imagen o con respecto a algún punto de referencia.

Frecuencia espacial: Es la inversa de la distancia entre dos crestas consecutivas en la vecindad de una minucia.

Curvatura: Es el índice de variación en la dirección de las crestas.

El tipo, posición y dirección de cada minucia son almacenadas para la tarea de reconocimiento.

La confiabilidad de trabajar con minucias, independientemente de poder distinguir individuos que poseen características globales idénticas se ve reforzada con métodos de obtención de características locales, como se muestra en el siguiente gráfico:

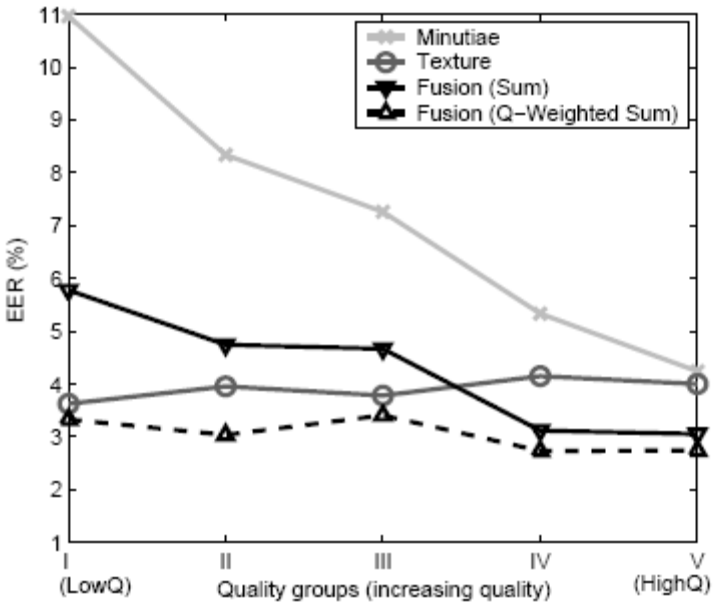


Figura 3.8 Nivel de confiabilidad de distintos tipos de identificación por huellas digitales. [26]

3.1.3 Sistemas Biométricos basados en las huellas dactilares.

Año con año, se publican estudios de mercado en donde se puede apreciar el crecimiento, la aceptación y el uso de diversos sistemas biométricos en todo el mundo; el organismo que funge como principal investigador de mercado de la industria biométrica, el International Biometric Group, desde su creación en 1996 ha venido publicando el reporte de mercado de Tecnología Biométrica, para el año 2008 se obtuvieron los siguientes resultados:

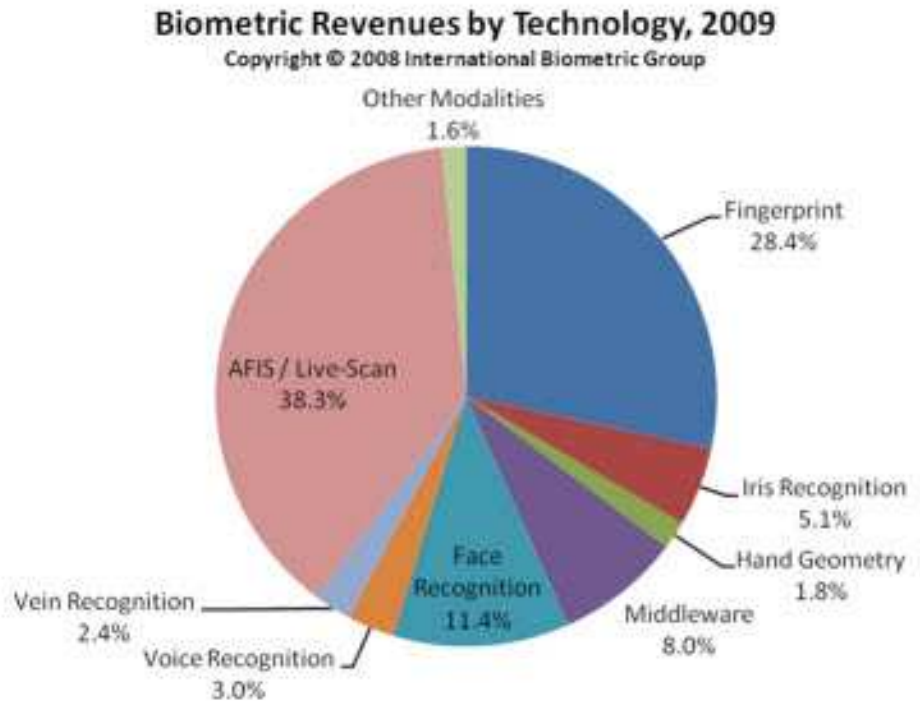


Figura 3.9 Distribución de Tecnología Biométrica referente al año 2008. [27]

En este estudio se ubica al AFIS/LiveScan con un 38.3%, (sistema automatizado de identificación que transfiere la información de la huella dactilar a través de un scanner o cámara de video); en segundo lugar, se ubicó el Fingerprint con un 28.4%, y el Face Recognition con un 11.4% entre los de mayor aceptación.

Utilizando el mismo estudio del año 2007, publicado por el International Biometric Group (IBG), se ubica al AFIS/LiveScan con un 36%; en segundo lugar, se ubicó el Fingerprint con un 25.3%, y el Face Recognition con un 12.9% [28], lo que muestra la creciente demanda de sistemas biométricos a nivel mundial; específicamente los relacionados con huellas digitales.

Los sistemas biométricos basados en huellas digitales 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 como:

• Sistema Automático de Identificación por Huellas Dactilares (Automatic Fingerprint Identification System - AFIS)
• Sistema Automático de Verificación por Huellas Dactilares (Automatic Fingerprint Authentication System - AFAS)

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.

3.2. Formas básicas de identificación utilizando huellas digitales

Los tipos de identificación de huellas digitales son un paso indispensable en cualquier método de identificación que se base en la biometría, y es más clara su diferenciación utilizando huellas digitales.

Hay dos tipos de identificación: uno a uno y uno para muchos, los cuales se explican a continuación.

3.2.1 Uno para uno

El método de identificación de huellas digitales uno a uno corresponde a la autenticación del individuo previamente almacenado.

Es decir, el procedimiento de identificación 1:1 consiste en validar que una huella dactilar que se tome corresponde con una que previamente se ha almacenado o se encuentra en memoria en ese momento [29].

3.2.2 Uno para muchos

Este proceso es similar al anterior, aunque conceptualmente diferente en un paso previo a la construcción de la unidad de almacenamiento de los individuos.

En este proceso, se realiza una identificación a partir de una huella obtenida en el momento contra todas las previamente almacenadas en una base de datos [30]. Conceptualmente, primero se lleva a cabo una identificación y posteriormente una verificación de uno a uno en distintas formas de cada uno de los individuos existentes.

Capítulo IV. Métodos de identificación de huellas

A lo largo de este capítulo se estudiarán los métodos más característicos con que se pueden identificar las huellas digitales.

Cada uno de los métodos analizados en este capítulo parten desde el momento en que la huella dactilar ya ha sido almacenada y puede accederse a ella como imagen.

También, todos los métodos descritos en este capítulo finalizan con la identificación de las huellas digitales, sin la implementación en una base de datos y tampoco proponiendo un método de comparación entre datos.

Con éstas restricciones, éste capítulo y el subsecuente tienen las mismas características y alcances, con lo cual es más sencillo discriminar a un método, analizar sus ventajas, etc.

4.1 Método de Orientación de valles

Uno de los primeros desarrollos en materia de algoritmos ha sido sin duda, la implementación y mejoramiento de la obtención de las características de la huella digital, y su comparación con las seis formas predefinidas de las huellas digitales de manera general, las cuales son:

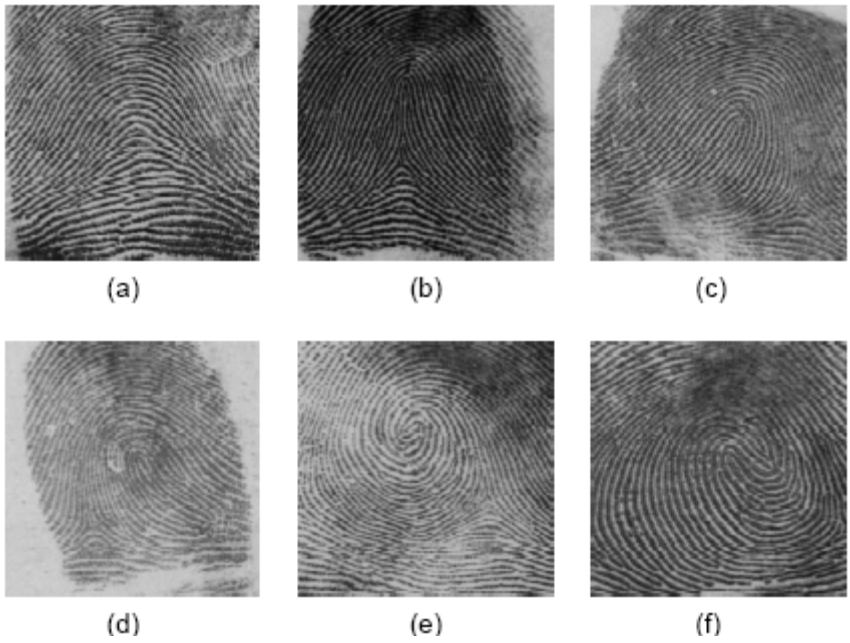


Figura 4.1 Clasificación de las huellas digitales en seis categorías generales: (a) Arch. (b) Tented Arch. (c) Right Loop. (d) Left Loop. (e) Whorl. (f) Twin Loop [31].

El método de orientación de valles tiene como objetivo el filtrado y adelgazamiento de una huella digital previamente obtenida. El procesamiento de la imagen se realiza mediante ventanas de tamaño definido, lo que causa una rigidez en el sistema considerando la correcta y única dimensión de las ventanas a utilizar.

Como primer paso de este método es necesario capturar una huella digital y guardarla como imagen; posteriormente convertirla a

imagen de tonalidades de gris conservando la dimensión original de la huella digital.

Posteriormente es necesario aplicar un algoritmo que extrae información direccional a partir de las tonalidades de gris de cada punto. El objetivo del algoritmo es determinar el sentido o circulación de las líneas (crestas o valles) alrededor de cada punto de la imagen.

La imagen es almacenada como una matriz, donde el valor de cada elemento de ella es el nivel de gris del punto correspondiente. Existen diferentes estimadores para la dirección de las líneas alrededor de un punto.

Para su procesamiento digital, el modelo de una imagen es una matriz $A = (a_{ij}) = (a[i, j])$ donde a es el valor correspondiente, tanto en color o gris del píxel con coordenadas [i,j], donde i corresponde a los renglones y j a las columnas, teniendo como punto de origen la esquina superior izquierda.

Para obtener esta representación se utilizan diversos procesos de conversión de la señal lumínica proveniente de la imagen real, hasta llevarla a una matriz de valores discretos. Sobre esta matriz se definen las vecindades de radio N de un punto [i , j] como los conjuntos R[i, j]:

$$R_N[i, j] = \{a[k, l] : \|k - i\| \leq N, \|l - j\| \leq N\} \quad \text{.....(8)}$$

La selección del radio de las vecindades usado para el procesamiento es muy importante ya que se debe garantizar que en la vecindad de cada punto haya suficiente información acerca de la dirección de las líneas vecinas. Es por esto que N depende del grosor de

las crestas y valles de la huella, lo cual es un parámetro muy ligado con el método de adquisición y su resolución.

Para construir la transformación se define:

$$\delta(a[i,j],a[k,l]) = \|a[i,j] - a[k,l]\| \quad \text{.....(9)}$$

A partir de cualquier píxel, se definen M posibles direcciones numeradas de 0 a M − 1, y se logra definir como dirección M, la que se presenta en regiones con alto nivel de ruido o en regiones muy uniformes donde no se pueda estimar la dirección; en este caso el conjunto de direcciones posibles está dado por:

$$S = \{0, 1, 2, 3 .. M\}$$

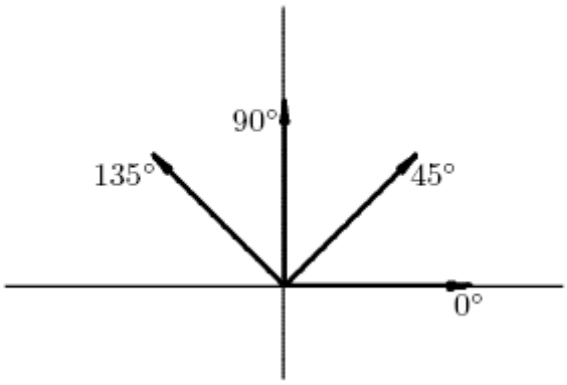


Figura 4.2 Ejemplo de M posibles direcciones en una imagen.

El ángulo correspondiente a cada dirección está dado por:

$$\theta_k = \frac{180^o}{M-1} k, k = 0,1,...M-1 \quad \text{.....(10)}$$

A lo largo de cada dirección y dentro de la vecindad de cada punto, se define un conjunto de puntos:

$$T_{[i,j]}^{k} = \{[m,n][m,n] \in R_N[i,j] y [m,n]\} \quad \text{.....(11)}$$

Que está en la dirección de k

En cada punto se puede definir un estimador $S_{[i,j]}^{k}$ para cada una de las direcciones posibles, así:

$$S_{[i,j]}^{k} = \sum_{[m,n] \in T^k[i,j]} \delta(a[m,n], a[i,j]) \quad \text{.....(12)}$$

La transformación asigna al punto la dirección donde $S_{[i,j]}^{k}$ toma el valor mínimo en caso de existir. Es posible que $S_{[i,j]}^{k}$ sea el mismo para todo k, lo cual indicaría que el punto [i, j] está localizado en una región muy ruidosa o donde no se presentan valles o crestas.

De esta forma la transformación dirección [i, j] queda definida por:

$$direccion[i,j] = \left\{k : S_{[i,j]}^{k} = \max\left\{S_{[i,j]}^{k} \middle| m = 0,1,...,M\right\}\right\} \quad \text{.....(13)}$$

Considerando la fórmula anterior, se puede observar que el máximo se puede presentar en varias direcciones, es por eso que como resultado se puede presentar un valor no único para la imagen de un punto; para solventar este inconveniente se realiza la siguiente consideración:

En el momento de calcular el máximo de las sumas $S_{[i,j]}^{k}$ alrededor de un punto, éste se presenta en dos direcciones adyacentes, es decir, recordando la definición de ángulos adyacentes, dos ángulos que

comparten el mismo vértice y un mismo lado. Los dos lados que no están compartidos forman un ángulo más grande [32]; se toma una dirección, de cualquier otra forma se asigna otra dirección llamada M, que se conoce como dirección indefinida.

Con esta consideración se consigue asignar a cada punto de la imagen original de la huella un valor en el rango 0, . . . ,M que identifica la dirección del flujo de la cresta o valle al cual pertenece el punto.

Sin embargo, al hacer un análisis más profundo de las sumas $S^k_{[i,j]}$ es posible apreciar la presencia de un sesgo en las direcciones 0º, 90º, 180º, 270º, ya que la distancia entre puntos consecutivos en la misma dirección para estas direcciones es más pequeña que para puntos consecutivos en las otras direcciones.

Por ejemplo, en el caso de la dirección 45º, el punto [i+1, j +1] en la imagen continua de la huella está a una distancia de $\sqrt{2}$ unidades del punto [i, j], mientras que en la dirección 0º, el punto [i + 1, j] está a una distancia de 1 del punto [i, j].

Esto hace que si la variación de la tonalidad de gris es uniforme, los estimadores $S^k_{[i,j]}$ tengan un valor mayor para las direcciones diferentes a 0º, 90º, 180º, 270º. Este fenómeno se puede corregir realizando un proceso de interpolación entre los puntos de estas direcciones y corrigiendo por medio de un factor de proporcionalidad los elementos de la suma $S^k_{[i,j]}$

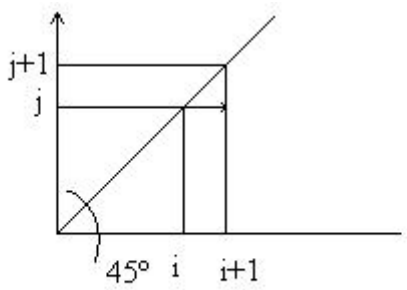


Figura 4.3 Ejemplo de análisis de sumatoria $S^k_{[i,j]}$

Todos los resultados de las direcciones, después de aplicar la consideración anterior son almacenados en una matriz que obtiene el nombre de matriz de direcciones, posteriormente se agrupan los puntos de la imagen en regiones llamadas segmentos, e inmediatamente después se procede a calcular la dirección predominante en el segmento; de esta forma se obtiene una matriz de dimensión más pequeña, en la cual se ha reducido la redundancia pero se sigue conservando la información acerca de las direcciones de las líneas, la cual va a ser de fundamental importancia en la clasificación de la huella.

El **proceso de segmentación** consiste en dividir la huella en regiones separadas; esto se garantiza por la conectividad de la imagen. En este caso las regiones son cuadradas y su tamaño es fijo para toda la imagen. En cada una de estas regiones se aplica un algoritmo para calcular la dirección predominante en la región.

Básicamente, el proceso se reduce a definir una variable aleatoria X que represente la dirección de un determinado punto dentro de un segmento de la imagen.

Se realiza el cálculo de la distribución de probabilidades de esta variable aleatoria, hallando la frecuencia de cada dirección en el segmento y se almacena en un arreglo. Esta distribución de

probabilidades puede tener diversas formas, las cuales se analizan a continuación.

Uniforme: Si las frecuencias de todas las direcciones son iguales. Esto indica que el segmento contiene líneas en varias direcciones, que el segmento contiene mucho ruido o que es una región plana. Por esto es imposible asignarle la dirección específica al segmento en el intervalo 0, . . .M, y entonces se le asigna el valor M.

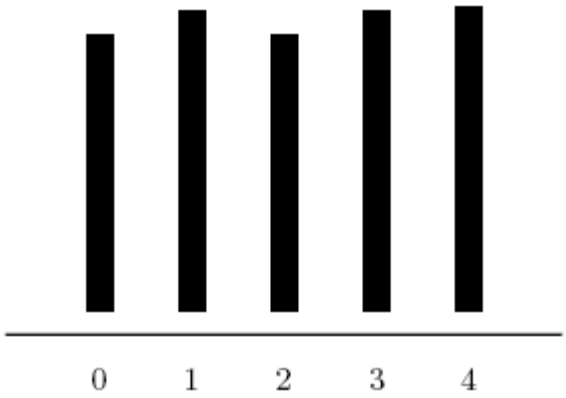


Figura 4.4 Distribución Uniforme

Unimodal: Si se presenta un máximo de frecuencia, y la relación entre éste y el siguiente es superior a un determinado umbral. En este caso hay una frecuencia predominante y la dirección de ésta es asignada al segmento estudiado.

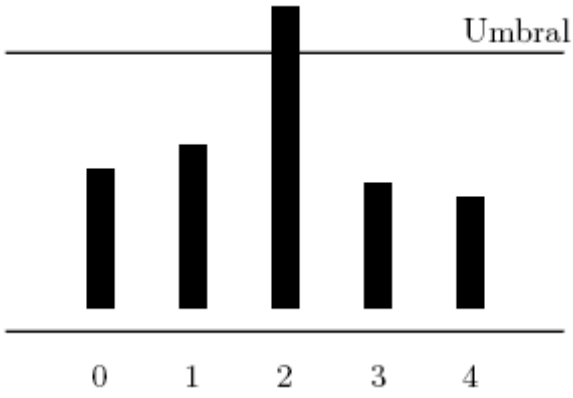


Figura 4.5 Distribución Unimodal.

Bimodal: Si se presenta un máximo de frecuencia en una dirección k, y hay exactamente otra dirección con un valor de frecuencia muy cercano (determinado por un umbral). En este caso existen dos direcciones predominantes, y se asigna al segmento en cuestión la dirección del ángulo medio (aproximada) entre las dos predominantes.

Si son adyacentes, se puede escoger cualquiera de las dos.

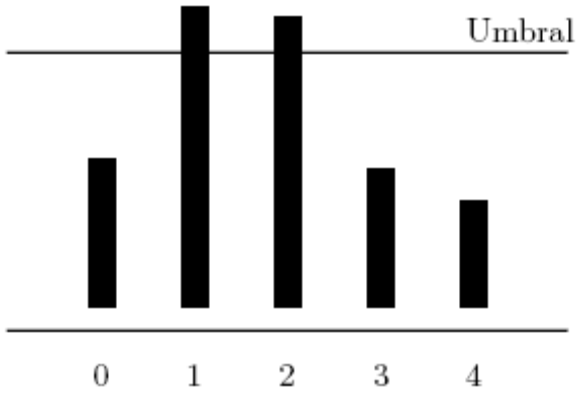


Figura 4.6 Distribución Bimodal

Otra: si existen varias frecuencias con valores muy cercanos al máximo, se asigna al segmento la dirección M (indefinida).

Existen diversos **métodos para escoger la dirección del segmento**, entre los más importantes se tienen:

– se escoge como dirección predominante del segmento el valor esperado de la dirección recorriendo todo el segmento,

– se escoge la mediana,

– se escoge la moda.

El estudio estadístico de estos estimadores y de los tipos de distribuciones permite concluir que la moda es el más robusto en este tipo de imágenes, y el algoritmo de asignación de direcciones a cada segmento se reduce a calcular la moda de la distribución, es decir, el valor de dirección más repetido o de mayor probabilidad.

Es necesario determinar un umbral que determina el nivel de indecisión cuando se tienen dos direcciones cuyas probabilidades son muy cercanas. Si la relación entre las dos direcciones con probabilidades muy cercanas es menor al umbral, se escoge como dirección predominante la moda de la distribución, es decir la dirección más probable.

Si esta relación no es superior al umbral, se compara con la siguiente dirección en orden de probabilidades y se verifica de nuevo la condición del umbral entre el segundo y el tercero. Si esta se cumple, se decide por el promedio entre el primero y el segundo; si no, se determina el punto con una dirección indefinida, que se representa con un código direccional especial.

Básicamente se trata de tener un criterio de decisión basado en la dispersión de la distribución de direcciones en un segmento.

Debe tenerse en cuenta que cuando se cumpla la condición del umbral entre el segundo y el tercer valor de la distribución, el promedio de las direcciones debe hacerse de tal forma que no se genere error, como se ve en el siguiente ejemplo:

Dirección	Probabilidad
0º	0.4
45º	0.001
90º	0.009
135º	0.39

Tabla 4.1 Promedio de las direcciones sin generación de error.

Por poner un ejemplo, si se elige un umbral de 0.5, la razón entre las direcciones predominantes entre las direcciones 0º y 135º es mayor al umbral y se escogería el promedio de éstas direcciones.

Por otro lado, si se hiciera el promedio aritmético se incurriría en un error (67.5º). En este caso se puede considerar la dirección 0º como 180º y el promedio obtenido es 157.5º.

Una vez asignada a cada segmento de la matriz de imagen una dirección específica, esta nueva matriz es utilizada para detectar la presencia de regiones singulares dentro de la huella. Se conocerán como *regiones singulares* a los segmentos de la imagen donde la circulación de las líneas presente patrones de tipo delta, núcleo o espiral.

Un *delta* es un patrón de flujo de líneas en el cual, estas llegan paralelas a un punto y en el se bifurcan, saliendo por dos direcciones diferentes.

Un *núcleo*, por otra parte, es una región donde las líneas llegan a un punto y se devuelven para salir por la misma dirección en que llegaron.

Una *espiral* es el patrón de flujo en el cual las líneas no entran ni salen al segmento sino que circulan en el.

Para la detección de puntos singulares se realiza el cálculo de la variación del ángulo entre la dirección de los segmentos vecinos y la dirección del segmento que es necesario calcular, a lo largo de una circunferencia que lo rodee. Este ángulo neto permite determinar si la región analizada es singular o no, y qué tipo de singularidad se presenta.

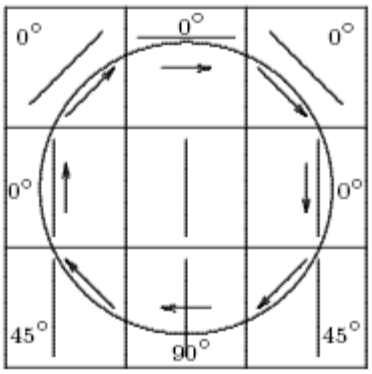


Figura 4.7 Región Tipo núcleo.

Resumiendo, en el método ridge-valley o mejor conocido como cresta-valle el proceso de filtrado se realiza simultáneamente mientras la imagen se vuelve binarizada, es por eso que se pueden tener grandes cantidades de niveles de gris. En este método se realiza un filtrado direccional que además de definir un umbral local determina también la dirección de cada punto. Como resultado final se obtiene que cada punto tiene asociado un valor (blanco o negro) y una dirección que lo caracterizan.

Finalmente, se agrupan los pixeles en ventanas más grandes para definir una matriz de direcciones, la cual es muy útil para el análisis de los puntos característicos.

Para el análisis de las huellas comúnmente se definen ventanas del tamaño adecuado, es decir, es aquel que tenga un ancho superior al

ancho de las crestas, para poder abarcar la información suficiente y necesaria donde el píxel central corresponde al punto al cual se le va a determinar su valor y dirección. En la siguiente figura, este punto está marcado con una P.

Los puntos marcados con números iguales conforman líneas de una dirección definida que atraviesan la ventana pasando por el punto en consideración y son los empleados en el análisis, en tanto que los que aparecen como blancos son puntos que no importan.

7		6		5		4		3
8		7	6	5	4	3		2
		8				2		
1		1		**P**		1		1
		2				8		
2		3	4	5	6	7		8
3		4		5		6		7

Figura 4.8 Ventana con punto para análisis de huellas

Al tomar en cuenta esta ventana general, se define un parámetro conocido como slit sum (suma direccional) el cual consiste en realizar la suma de los pixeles en una de las ocho direcciones posibles.

Esas ocho direcciones corresponden al ángulo respectivo de la numeración de la ventana, es decir:

Dirección	Ángulo
1	0º
2	26.5º
3	45º
4	63.5º
5	90º
6	116.5º
7	135º
8	153.5º

Y la sumatoria se representa como:

$$S_i = \sum_{j=0}^{3} p_{ij} \quad \text{.....(14)}$$

Donde Si es una slit sum; i = 1, 2, . . . 8 y los p_{ij} son los puntos que comparten igual dirección. Estas sumas son empleadas en el análisis que se muestra a continuación.

El binarizador busca definir un umbral a partir del cual se puedan clasificar los puntos como blancos (surcos) o negros (crestas). Se realizan dos aproximaciones [33]: definición local del umbral, y comparación de sumas direccionales.

El método de definición de un umbral local asigna a un píxel el color blanco si la suma S es mayor que el promedio de los pixeles considerados en la ventana.

Aprovechando las sumas direccionales, un píxel será blanco si:

$$S \geq \frac{1}{8}\sum_{i=1}^{8} s_i$$
$$S = 4P$$ .....(15)

El valor de S es 4 veces el valor del punto analizado porque cada suma direccional es la suma de cuatro pixeles.

La comparación de sumas direccionales toma el promedio de los valores máximo y mínimo de estas sumas como parámetro para definir el umbral. Así, un punto será blanco si:

$$\frac{s_{\max} + s_{\min}}{2} \geq \frac{1}{8}\sum_{i=1}^{8} s_i$$ .....(16)

Si un píxel se encuentra en un valle, al menos una de sus sumas direccionales tendrá un valor alto, en tanto que las otras no lo tendrán, esto se ocasiona porque se deben cruzar algunas crestas cuyos pixeles tienen un valor bajo.

Un caso idéntico ocurre cuando el píxel está en una cresta, sólo que en este caso, una suma tendrá un valor muy bajo, mientras las demás no tanto.

El método de orientación de valle unifica estos dos criterios para definir el umbral, de tal forma que un punto será considerado blanco si:

$$S + S_{\max} + S_{\min} \geq \frac{3}{8}\sum_{i=1}^{8} S_i$$ .....(17)

A medida que se realiza la binarización, cada píxel es asociado con la dirección de su mayor o menor suma direccional si pertenece a un valle o cresta, respectivamente, completando así su caracterización.

La dirección de cada punto no brinda ninguna información acerca de los detalles que pueda tener una huella. Por lo tanto, es necesario agruparlos en ventanas cuya dimensión permita identificar los puntos característicos. Esto genera una matriz de direcciones cuyo tamaño depende de las dimensiones de la imagen y de la ventana que, además de disminuir la información requerida, realiza un proceso de suavizamiento de las direcciones al promediar las de los pixeles dentro de la ventana.

Promediar las direcciones trae como efecto el suavizamiento de las direcciones y el aumento de los niveles del cuantificador.

Hay que tener cuidado al realizar el promedio de las direcciones: si se realiza el promedio normal $\left(\frac{a+b}{2}\right)$, se introduce un gran error; concretamente, ángulos de 153.5 º 0º promediados dan un resultado de 76.75º, cuando seguramente la dirección más apropiada es la de 167.0º (correspondiente al promedio entre 153.5º y 180º).

Para evitar este error, se emplean las componentes vectoriales de cada uno de los pixeles en términos de su ángulo: (cos θ, sin θ). Así, la ventana final estará caracterizada por un vector $\bar{q}$ tal que:

$$\sphericalangle \bar{q} = \arctan \frac{\sum_{i=1}^{n^2} sen(2\theta_i)}{\sum_{i=1}^{n^2} \cos(2\theta_i)} \quad \text{.....(18)}$$

$$\|\bar{q}\| = \frac{i}{n^2} \sqrt{\left(\sum_{i=1}^{n^2} \cos(2\theta_i) \right)^2 + \left(\sum_{i=1}^{n^2} sen(2\theta_i) \right)^2} \quad \text{.....(19)}$$

Donde n es la longitud de un lado de la ventana.

La magnitud del vector arroja como resultado la confiabilidad del resultado. En una región muy borrosa o con poca legibilidad $\|\bar{q}\| \langle\langle 1$, de tal forma que en una región bien definida $\|\bar{q}\| \approx 1$.

Este método es de los que tienen menor costo computacional, el problema radica en los resultados obtenidos; las estimaciones de dirección proporcionadas por este método no son tan buenas, ya que a menudo se detectan errores en las direcciones resultantes (cerca del 20% en una imagen de buena calidad).

El motivo es la poca información, en cuanto a número de píxeles procesados, que utiliza la máscara de estimación, lo que la hace muy vulnerable al ruido.

En imágenes de muy alta calidad es común que se encuentren buenos resultados, pero no siempre se va a poder disponer de ellas.

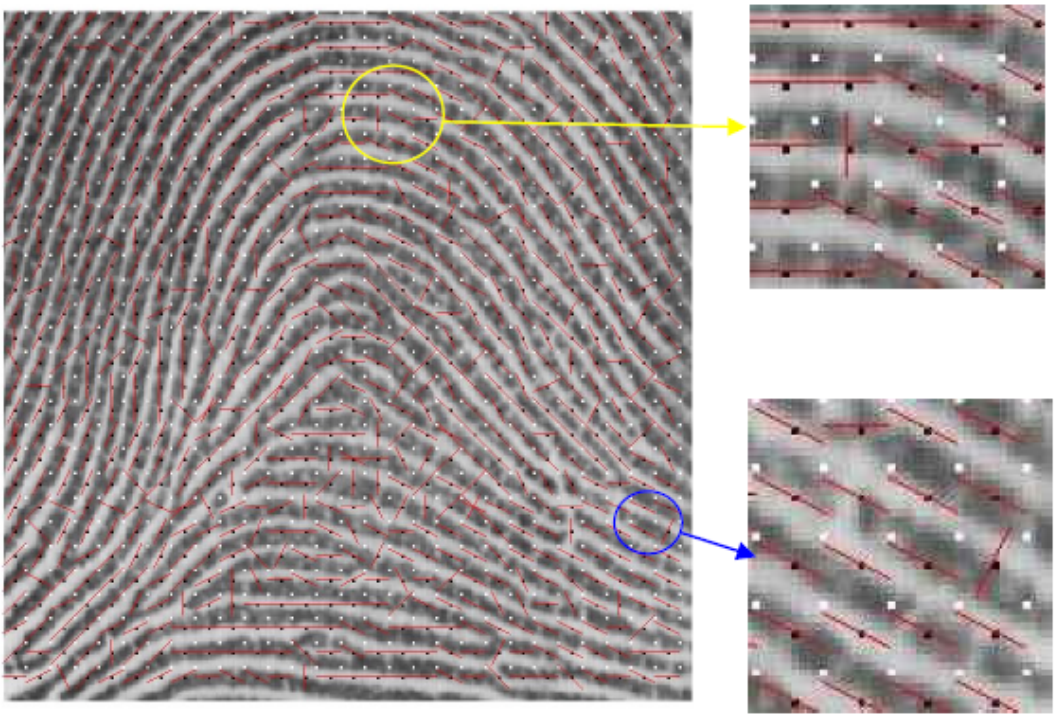


Figura 4.9 Errores en la estimación de direcciones.

En la figura anterior se puede observar un número apreciable de estimaciones erróneas, de las que se han ampliado un par de casos a modo de ejemplo.

Haciendo algunas consideraciones en los resultados se puede concluir que:

En primer lugar se aprecia que un gran número de errores se producen en zonas en las que el píxel que se está estimando, correspondiente al punto central C de la máscara, está situado en zonas de grises suaves, frontera entre valles y crestas. En segundo lugar, se destaca el hecho de que, en un gran número de casos, la dirección estimada erróneamente es perpendicular a la dirección correcta. Todo ello lleva a considerar la posibilidad de que el criterio para determinar si se está en una cresta o un valle, es decir, si se debe buscar el máximo o el mínimo, no funciona al 100%.

Para apreciar mejor este hecho, en la figura se ha marcado con un punto negro el píxel central de la ventana, y con un punto blanco su esquina superior izquierda, delimitándose así la zona empleada para cada estimación.

4.2. Método de identificación por núcleo y deltas

En cada huella dactilar, existen singularidades globales que por su posición relativa son capaces de clasificar una huella según la disposición de crestas y valles. Éstas son el núcleo y los deltas.

El *Núcleo* se define como el punto más al norte de la línea de cresta más interna.

El *Delta* se define como el lugar de fusión o aproximación de los sistemas de crestas que dan lugar a un dibujo en forma de trípode o triangulo.

Las huellas dactilares se pueden clasificar basándose en la ausencia o no del delta, el número de los mismos, y la posición de éstos con respecto al núcleo.

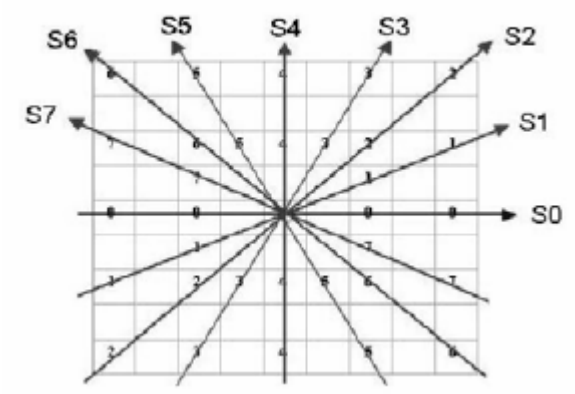
Este método consiste en los siguientes pasos:

1) Cálculo de la imagen direccional de la huella
2) Simplificación de la imagen direccional tratando ésta por bloques
3) Localización y clasificación de las singularidades
4) Clasificación de la imagen de la huella atendiendo al número y posición relativa de los puntos singulares.

4.2.1 Cálculo de la imagen direccional de la huella

La imagen direccional es una matriz del mismo tamaño que la imagen de la huella, donde el elemento (i,j) contiene la dirección de las crestas al pasar por el píxel (i,j).

Al igual que en el método de crestas y valles se vuelven a considerar 8 posibles direcciones, determinadas por los siguientes ángulos.



Dirección S	Ángulo
0	0º
1	22.5º
2	45º
3	67.5º
4	90º
5	112.5º
6	135º
7	157.5º

Figura 4.10 Pixeles involucrados en cada dirección

En este caso, el método de identificación por deltas difiere del anterior no en el proceso de la obtención de la imagen direccional sino en la definición de las ventanas propias utilizadas para la obtención de la máxima información de las huellas utilizadas.

Para determinar qué dirección hay en el píxel (i,j), es necesario aplicar sobre un cuadrado de la imagen de dimensiones 9x9 centrado en dicho píxel, 8 máscaras diferentes, asociadas cada una de ellas a una de las direcciones citadas anteriormente.

Se define por S(n) el valor de gris de los píxeles alineados en la dirección n.

Éstos se calculan como se muestra a continuación:

$$S(0)=\sum_{k=-2}^{2} I(i, j+2k)-I(i, j) \qquad S(4)=\sum_{k=-2}^{2} I(i+2k, j)-I(i, j)$$
$$S(1)=\sum_{k=-2}^{2} I(i+k, j-2k)-I(i, j) \quad S(5)=\sum_{k=-2}^{2} I(i+2k, j+k)-I(i, j)$$
$$S(2)=\sum_{k=-2}^{2} I(i+2k, j-2k)-I(i, j) \; S(6)=\sum_{k=-2}^{2} I(i+2k, j+2k)-I(i, j) \quad \text{.....(20)}$$
$$S(3)=\sum_{k=-2}^{2} I(i+2k, j-k)-I(i, j) \quad S(7)=\sum_{k=-2}^{2} I(i+k, j+2k)-I(i, j)$$

Una vez calculados, se denota por Sp al mínimo de ellos y por Sq al máximo.

Por practicidad se identifica p y q a las direcciones que dieron las sumas de valor mínimo y máximo respectivamente.

La dirección del píxel (i,j) será p si se cumple que:

$$4I(i, j)+S_p+S_q \langle \frac{3}{8}\sum_{n=0}^{7} S(n) \quad \text{.....(21)}$$

La dirección del píxel será q sino se cumple la ecuación anterior.

El valor de 3/8 se determinó experimentalmente por Srinivasan y Murthy [34] y es el mismo valor de normalización que el método de crestas y valles.

4.2.2 Imagen direccional por bloques

Para este método es necesario homogeneizar la imagen y crear una representación de las direcciones; esto es, a cada bloque se le asigna una dirección. Para determinar dicha dirección, como se mencionó anteriormente se puede utilizar la moda, la mediana, el promedio, etc.

Existe un método más robusto que la moda, es conocido como el método de Karu Jain [35], y consiste en asignar a cada bloque una dirección que se calcula mediante un promedio de ángulos dobles: Si α grados es el ángulo de la dirección de un píxel, es posible transformar éste en un vector normalizado de ángulo 2α.

La razón de trabajar con ángulos dobles es que, de esta manera, a la hora de promediar se descartarán parejas de píxeles que tienen direcciones perpendiculares entre sí.

Se asigna un par de coordenadas (x,y) al vector resultante de promediar todos los vectores normalizados de ángulo doble asociados a los píxeles de un bloque. La dirección de cada bloque será el valor de:

$$\frac{1}{2}\arctan\left(\frac{y}{x}\right) \quad \text{.....(22)}$$

Discretizando a una de las 8 posibles direcciones establecidas anteriormente.

En muchas aplicaciones, antes de proseguir con el método, varios autores llevan a cabo la aplicación de un filtro para suavizar la imagen direccional por bloques.

4.2.3 Localización de puntos singulares

En este método es posible determinar qué bloques corresponden a zonas donde se hallan puntos singulares mediante el cálculo del índice de Poincaré de cada bloque.

Éste fue propuesto inicialmente por Kawagoe y Tojo [36] y mejorado posteriormente por Karu y Jain y por Maltoni, Maio, Jain y Prabhakar [37].

El primer paso para la obtención del índice de Poincaré es fijar un bloque arbitrario, dentro de cualquier zona de la imagen. El método consiste en determinar si los bloques existentes en un cuadrado de dimensiones 3x3 y centrado en él, se corresponden o no con la discretización de una curva que gire en torno al bloque central.

Además, el valor resultante del índice indica cuántas vueltas daría la supuesta curva en torno al bloque central y en qué sentido.

El índice de Poincaré del bloque (i,j), denotado por P(i,j), se define como la rotación total de los vectores de las direcciones de los bloques que rodean al bloque (i,j).

Se calcula algebraicamente sumando los ángulos formados por los vectores de las direcciones de parejas bloques adyacentes que rodean al bloque (i,j). Si se nombran las direcciones cómo se indica en la siguiente figura:

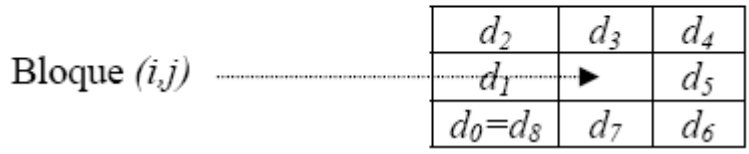


Figura 4.11 Ejemplo de la distribución de los vectores de direcciones

El índice de Poincaré P(i,j) toma el valor $\sum_{k=0}^{7} angulo(d_k, d_{k+1})$ donde ángulo(dk,dk+1), indica el valor del ángulo formado por los vectores de las direcciones dk y dk+1.

Para poder calcular estos ángulos se requiere que a cada dirección se le asigne uno de los dos ángulos, comprendidos entre 0º y 360º, que los determinan.

Por ejemplo, a la dirección 2 se le pueden asignar 45º o bien 225º, según el sentido que convenga. Asignando a la primera dirección, d0, un ángulo entre 0º y 157’5º y a cada una de las direcciones restantes se le asigna el sentido que haga que el valor absoluto del valor en grados del ángulo entre dk y dk+1 sea menor o igual que 180. Se puede comprobar fácilmente que en curvas cerradas el índice de Poincaré sólo puede tomar los valores 0º, ±180º y ±360º.

Para este método, si el bloque toma el valor 0º, no existe ninguna singularidad en dicho bloque; si toma el valor 180º, existe un núcleo; si toma -180º, existe un delta y si toma el valor de 360º se tiene una espiral o whorl. Este último caso suele aparecer generalmente en las huellas bideltas y en forma de dos núcleos muy próximos.

Al aplicar éste método se observa que existen minucias que dan lugar a falsos “núcleos” y “deltas”.

En estos casos, es necesario suavizar la imagen direccional por bloques mediante un filtro gaussiano, y repetido el proceso del cálculo del índice de Poincaré de manera reiterada, hasta que se han eliminado estas irregularidades.

Si existe un núcleo o un delta, éste no suele estar localizado únicamente en un bloque, sino que existen bloques contiguos con idéntico índice. Es por ello que bloques contiguos con similar comportamiento se deben tratar como uno solo.

4.2.4 Clasificación de las huellas dactilares.

Según el número de núcleos y deltas se tiene la siguiente clasificación:

Si no se encuentra ningún núcleo se dice que la huella es adelta.
Si tiene dos núcleos, se clasifica como bidelta.
Si tiene un núcleo es necesario observar el número de deltas:
Si tiene 2 deltas recibe el nombre de bidelta.

Si tiene 1 delta es necesario identificar si el delta está a la izquierda del núcleo, sinistrodelta, o a la derecha, dextrodelta.

Si no tiene deltas, esto se puede deber a que se encontraban demasiado escorados en la huella y pueden no haber aparecido en la imagen, o a que se ha descartado el delta en el paso anterior pensando que éste era falso.

Por tanto, se comprueba en primer lugar el último caso, y si no es así, se intenta clasificar la huella a partir de la disposición del núcleo en la imagen de la misma.

Figura 4.12 Diferentes tipos de huellas basados en su Delta y su Núcleo

4.3 Método de Rao

Este método es el propuesto por Ravishankar Rao [38], y es uno de los más citados en la bibliografía. En su libro, Rao se centra en la obtención del mapa de direcciones de imágenes que presentan una textura visual que recuerda el movimiento de un fluido, como una superficie de madera.

Trata de texturas caracterizadas por presentar, de forma local, una selectividad en su orientación, aunque ésta puede variar arbitrariamente en el conjunto de la imagen.

A cada punto de la imagen se le asocia una orientación local dominante, así como una medida local de la coherencia, o grado de anisotropía del patrón de orientación. Según Rao, una forma de visualizar texturas orientadas es pensar en la representación de la imagen como una serie de crestas, cuya orientación e intensidad puede variar continuamente; particularmente destaca la similitud de ese tipo de imágenes con la de una huella dactilar.

Como primer paso en este método, se utilizan las máscaras de Sobel para determinar los gradientes de la imagen en un sistema de ejes cartesianos X e Y.

-1	0	1
-2	0	2
-1	0	1

Gx

-1	-2	-1
0	0	0
1	2	1

Gy

Figura 4.13 Máscaras de Sobel para el cálculo del gradiente.

Esto es considerado como el vector gradiente, y está dado por $\begin{bmatrix} G_x & G_y \end{bmatrix}^T$, el cual se convierte a coordenadas polares, pasando a estar representado como:

$$\begin{bmatrix} \rho & \varphi \end{bmatrix}^T$$

Ésta transformación se realiza con el propósito de duplicar su ángulo y elevar su módulo al cuadrado.

$$\begin{bmatrix} \rho \\ \varphi \end{bmatrix} = \begin{bmatrix} \sqrt{G_x^2 + G_y^2} \\ tg^{-1}\dfrac{G_y}{G_x} \end{bmatrix} \quad \text{.....(23)}$$

El vector gradiente puede volver a representarse en el sistema cartesiano mediante la transformación inversa:

$$\begin{bmatrix} G_x \\ G_y \end{bmatrix} = \begin{bmatrix} \rho \cdot \cos(\varphi) \\ \rho \cdot sen(\varphi) \end{bmatrix} \quad \text{.....(24)}$$

Con lo cual se observa que la información se conserva intacta.

Empleando las siguientes identidades trigonométricas se obtiene una expresión para los vectores gradiente al cuadrado en función de las componentes cartesianas:

$$\begin{bmatrix} G_{s,x} \\ G_{s,y} \end{bmatrix} = \begin{bmatrix} \rho^2 \cdot \cos(2\varphi) \\ \rho^2 \cdot sen(2\varphi) \end{bmatrix}$$

$$\cos(2\varphi) = \cos^2\varphi - sen^2\varphi \quad \text{.....(25)}$$

$$sen(2\varphi) = 2sen(\varphi)\cos(\varphi)$$

Por lo tanto:

$$\begin{bmatrix} G_{s,x} \\ G_{s,y} \end{bmatrix} = \begin{bmatrix} G_x^2 - G_y^2 \\ 2G_xG_y \end{bmatrix} \quad \text{.....(26)}$$

Se trata del mismo resultado que podría haberse obtenido tratando el vector gradiente como si fuese un número complejo:

$$G_{s,x} + jG_{s,y} = \left(G_x + jG_y\right)^2 = \left(G_x^2 - G_y^2\right) + j\left(2G_xG_y\right) \quad \text{.....(27)}$$

Una vez elevados al cuadrado, los gradientes pueden promediarse dentro de una ventana W, de forma que la media de cuadrados está dada por:

$$\begin{bmatrix} \overline{G_{s,x}} \\ \overline{G_{s,y}} \end{bmatrix} = \begin{bmatrix} \sum_W G_{s,x} \\ \sum_W G_{s,y} \end{bmatrix} = \begin{bmatrix} G_{xx} - G_{yy} \\ 2G_{xy} \end{bmatrix} \quad \text{.....(28)}$$

Donde:

$$\begin{aligned} G_{xx} &= \sum_W G_x^2 \\ G_{yy} &= \sum_W G_y^2 \\ G_{xy} &= \sum_W G_xG_y \end{aligned} \quad \text{.....(29)}$$

Son las estimaciones de la varianza y la covarianza de Gx y Gy, que están promediadas dentro de la ventana W. Así, la dirección promedio del vector gradiente, que es ortogonal a la dirección de las crestas, se calcula como se muestra a continuación:

$$\varphi = \begin{cases} \frac{1}{2} tg^{-1}\left(\frac{\overline{G_{s,y}}}{\overline{G_{s,x}}}\right) & si \quad \overline{G_{s,x}} \geq 0 \\ \frac{1}{2} tg^{-1}\left(\frac{\overline{G_{s,y}}}{\overline{G_{s,x}}}\right) + \pi & si\, \overline{G_{s,x}} \langle 0, \quad \overline{G_{s,y}} \geq 0 \\ \frac{1}{2} tg^{-1}\left(\frac{\overline{G_{s,y}}}{\overline{G_{s,x}}}\right) - \pi & si \quad \overline{G_{s,x}} \langle 0, \quad \overline{G_{s,y}} \langle 0 \end{cases} \quad \text{.....(30)}$$

La estimación de la coherencia está dada por:

$$Coh = \frac{\left|\sum_W \left(G_{s,x}, G_{s,y}\right)\right|}{\sum_W \left|\left(G_{s,x}, G_{s,y}\right)\right|} \quad \text{.....(31)}$$

Si todos los vectores gradiente elevados al cuadrado apuntan en la misma dirección, la suma del módulo de los vectores será igual a la suma de los vectores, esto es, resultando en una coherencia de 1.

Si, por otro lado, los vectores gradiente al cuadrado están uniformemente distribuidos en todas las direcciones, el módulo del vector suma será igual a 0, con lo que, por consiguiente, la coherencia será también 0.

Una ventaja evidente en este método, es que no se hace ninguna suposición relativa al tamaño de la ventana W empleada para realizar el promedio, pero es evidente que el tamaño de la ventana guarda relación directa con la escala a la que se está analizando el flujo de las crestas papilares, como con cualquier otro método de análisis de huellas dactilares.

La siguiente figura muestra algunos aspectos críticos en la elección del tamaño de la ventana de muestreo.

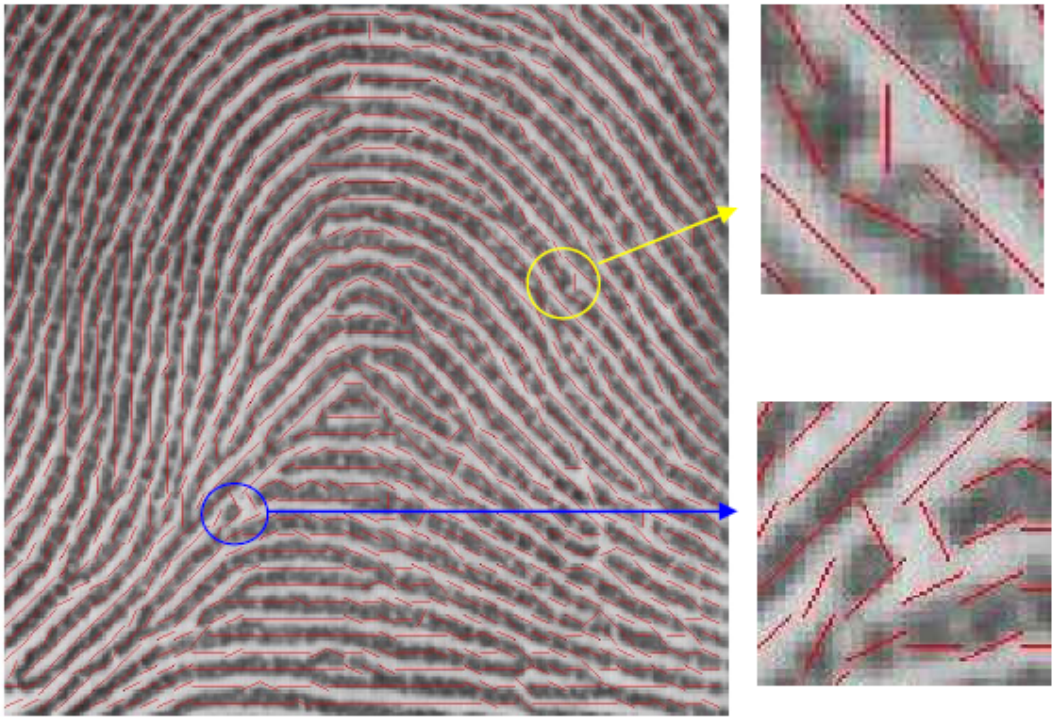


Figura 4.14 Problemas en el cálculo del mapa de direcciones.

En el centro del círculo azul hay dos estimaciones de dirección que dan como resultado una orientación perpendicular a la cresta; el corte que se observa en la cresta tiene un tamaño lo suficientemente grande como para estimar una orientación errónea, si bien se trata de la dirección correcta a nivel local.

En este caso se presenta el agravante de que posiblemente se va a detectar un final de cresta y se le va a asignar una dirección incorrecta.

Este problema, debido al uso de ventanas excesivamente pequeñas, se aprecia también en los casos, como el del círculo amarillo, en los que la ventana abarca un poro de la cresta papilar; si el poro es de gran tamaño respecto del número de píxeles de la cresta abarcados por la ventana, la dirección se estimará de forma errónea.

Hoy en día, y con bastante tiempo estudiando las huellas digitales, aún no existe un valor exacto que optimice el tamaño de la ventana de estimación; en general, cuanto menor sea la escala empleada, mejor será la estimación de la dirección local, pero también será mayor la vulnerabilidad a errores en la imagen de la huella o a los propios poros de la cresta papilar.

Por otro lado, cuanto mayor sea el tamaño de la ventana, mayor será la inmunidad al ruido, pero se realizará un efecto de filtro paso bajas, que dificultará el seguimiento de las crestas en las zonas en la que éstas presenten cambios destacados.

Es precisamente en estas zonas en las que cambia el flujo normal de la cresta, las que corresponden a la localización de las minucias; con el agravante de que el efecto de realizar un mal seguimiento de las zonas con mayor curvatura será la detección de minucias falsas.

Se han propuesto diversos métodos para tratar de solucionar este problema, uno de ellos es el de Anil K. Jain, quien propone una implementación del método de Rao para el cálculo de orientaciones que, mediante la evaluación de cierto “nivel de consistencia”, ajusta de forma dinámica el tamaño de la ventana, y por lo tanto el nivel de granularidad (crestas y valles), a las características locales de la imagen.

Éste método presenta el grave inconveniente del aumento del costo computacional, por el excesivo consumo de recursos, pero no deja de ser eficaz debido a que las características de la huella varían enormemente de unas zonas a otras.

Por otro lado, Maio en su artículo, en el que emplea un tamaño fijo para la ventana de estimación de orientación.

A continuación se presentan diversos casos de obtención de orientación de direcciones con diferentes ventanas; si se observan las direcciones obtenidas para distintos tamaños de la ventana, superpuestas sobre la imagen de la huella, se aprecia que para ventanas pequeñas, como en el caso de la figura siguiente, se obtienen direcciones muy variables.

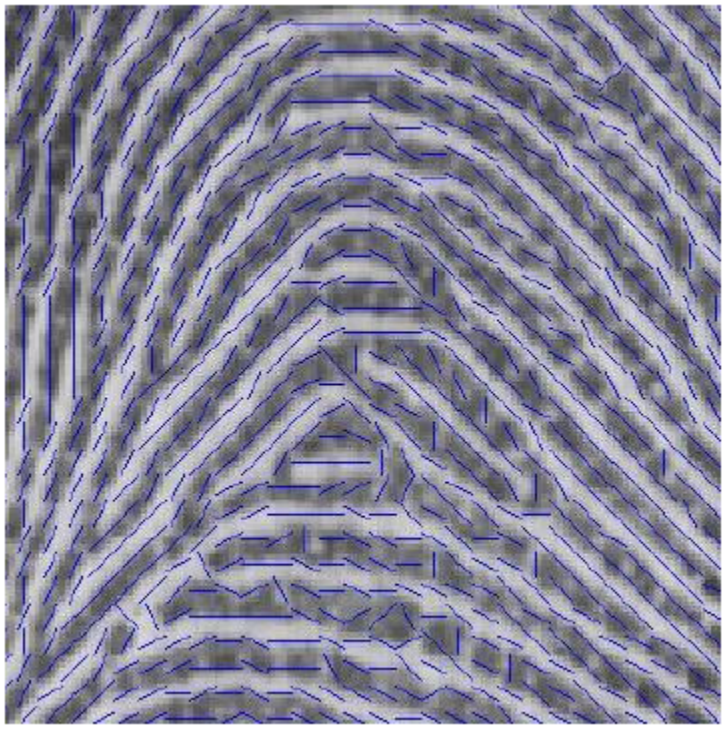


Figura 4.15 Representación del mapa de direcciones obtenido aplicando ventanas de 5x5 píxeles.

El ruido hace que las orientaciones obtenidas presenten variaciones de cierta importancia entre puntos muy cercanos. También se puede apreciar que este tamaño de ventana es demasiado pequeño para incluir tanto crestas como valles en una misma medida, lo que dificulta la obtención de la dirección correcta.

Es muy difícil determinar la dirección en una zona ampliada de 5x5 píxeles con muy poca variación de nivel de gris en su interior. El efecto

del ruido también será importante, dado que al procesar un número de puntos relativamente bajo no va a poderse compensar el efecto del error inducido que producen los puntos o discontinuidades que presenten ruido.

Por otro lado, las ventanas más grandes (14x14 píxeles) detectan mucho mejor la dirección de las crestas, pero se observa una pérdida de detalles en zonas de elevada curvatura. La pérdida de resolución en estas zonas puede ser crítica, puesto que, habitualmente, va a concentrar un número elevado de minucias. La siguiente figura muestra el resultado de aplicar el método de RAO en una ventana de 14x14 píxeles.

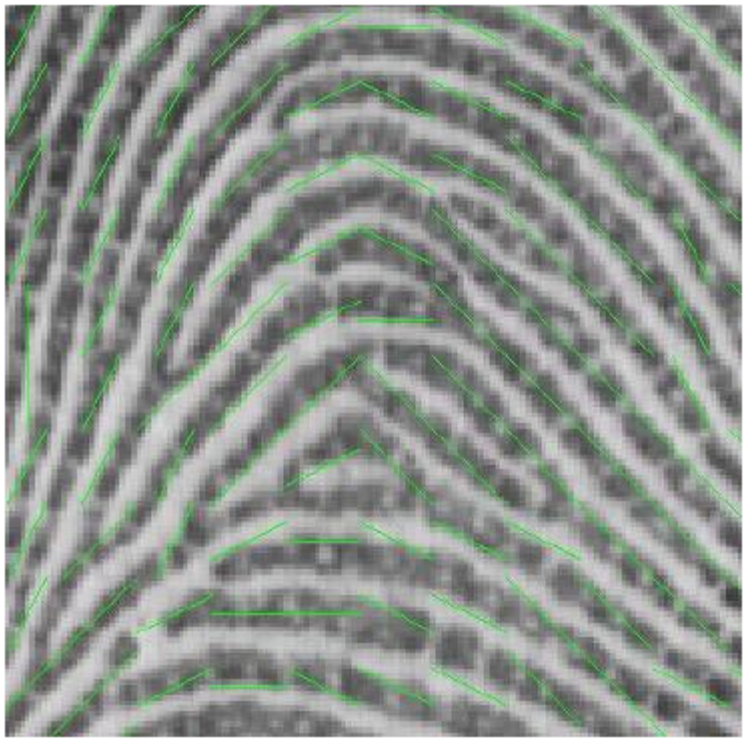


Figura 4.16 Representación del mapa de direcciones obtenido aplicando ventanas de 14x14 píxeles.

Comparando las dos imágenes previas, es de esperarse que la ventana óptima sea un valor intermedio entre la ventana menor de (5x5)

pixeles y la ventana mayor de (14x14) pixeles; los mejores resultados se obtienen empleando un tamaño medio (máscaras alrededor de 10x10 píxeles); se trata, como en cualquier proceso de filtrado, de aplicar el umbral adecuado para obtener el nivel de detalle deseado.

La siguiente figura muestra el resultado para una ventana de 10x10 píxeles.

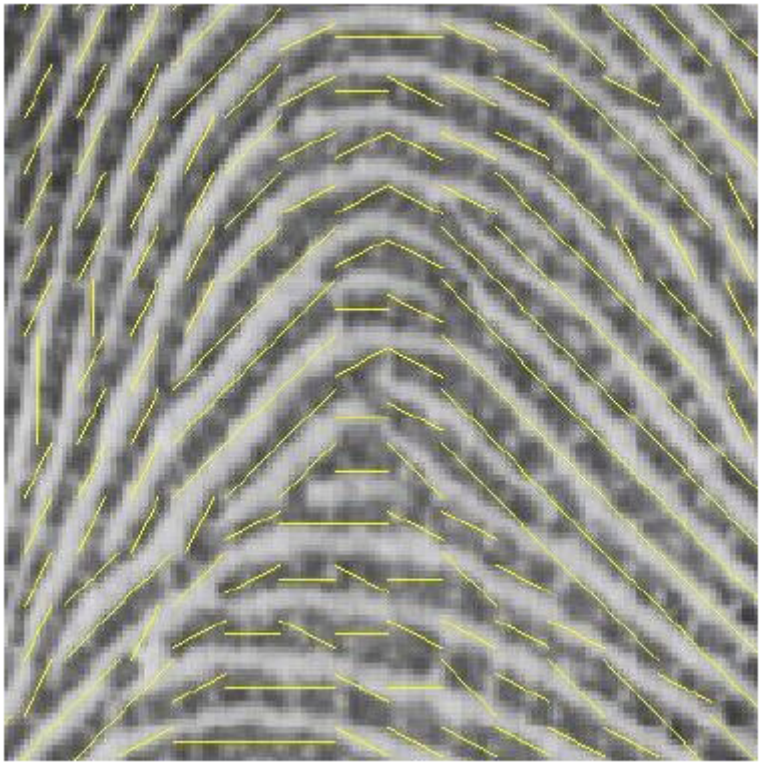


Figura 4.17 Representación del mapa de direcciones obtenido aplicando ventanas de 10x10 píxeles.

Como puede apreciarse, tanto en este caso como en el anterior, correspondiente a la ventana de 14x14 píxeles, no se producen los problemas mostrados en la figura correspondiente a los problemas en el cálculo de direcciones (Figura 4.14). La posible pérdida de detalle que se aprecia en las figuras correspondientes a las ventanas de (14x14) y (10x10) pixeles (Figura 4.16 y 4.17, respectivamente), o la dificultad de seguir los cambios de dirección más bruscos, pueden aminorarse

solapando las ventanas, de modo que el hecho de hacerlas mayores no implique un menor número de estimaciones; de hecho, durante el seguimiento, la dirección va a calcularse de nuevo en cada iteración, centrando la ventana de estimación en el punto de interés.

En la siguiente figura se representa la superposición de las orientaciones obtenidas empleando distintos tamaños de ventana, para así poder comparar mejor las distintas estimaciones.

Los cálculos se han realizado en los puntos centrales de una rejilla imaginaria superpuesta a la huella; cada tamaño de máscara se ha representado con una recta de un color distinto, de forma que su dirección coincida con la de la dirección estimada (discretizada a 12 posibles valores) y su longitud corresponda al tamaño de la ventana. Con la intención de facilitar la comparación, en unos casos se dibujan las líneas desplazadas, para poder verlas todas aún coincidiendo sus direcciones, mientras que en otros puntos se superponen para apreciar fácilmente las diferencias en las respectivas estimaciones.

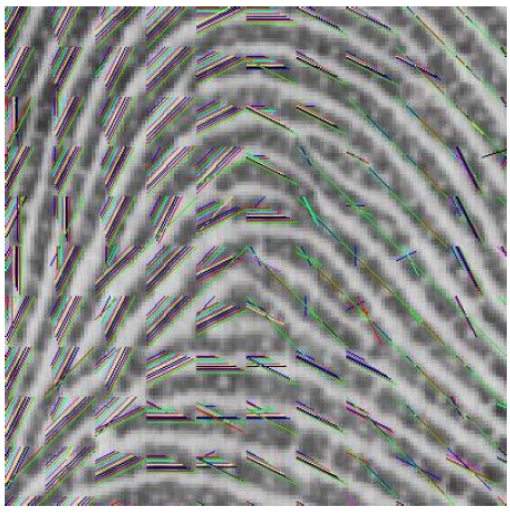


Figura 4.18 Superposición de las representaciones obtenidas con las distintas máscaras.

Como puede apreciarse, los tamaños de ventana más pequeños presentan mayores variaciones, debido a los efectos de pequeñas alteraciones en la imagen.

Para el caso contrario, las ventanas de mayor tamaño, por su efecto de filtro paso bajas, presentan una mayor inmunidad al ruido y determinan mejor la dirección, pero se tiene el riesgo latente de perder información en zonas de mucha variación.

El hecho de tener pequeñas irregularidades que alteren la estimación va a ser especialmente importante si la dirección estimada se va a asociar a una zona mayor, como seria el caso de preestimación de direcciones, aplicación de filtros con máscaras mayores que la ventana de estimación o de segmentación de imágenes por análisis de la coherencia de las orientaciones.

En el caso del algoritmo de Maio es conveniente que, si se emplea un desplazamiento de μ píxeles, la estimación de la dirección se realice en una ventana próxima a los $2\mu+1$ píxeles de lado, es decir en la ventana que forman los píxeles situados a una distancia menor o igual a μ desde el punto donde se realiza la estimación.

De esta forma, si se produce una desviación local por ruido, la siguiente estimación puede recuperar el sentido correcto; la figura correspondiente a los problemas del cálculo de direcciones (Figura 4.14) presenta muchos cambios de dirección, aunque desde un punto de vista local se están dando las direcciones correctas.

Aunque a simple vista puede parecer que los efectos de emplear una ventana excesivamente grande no son graves, lo cierto es que, en

algunos casos, estos errores pueden facilitar el salto a crestas adyacentes o generando, en el caso del algoritmo de Maio, falsos errores en el seguimiento de la cresta por un exceso de curvatura.

Además, a igualdad de condiciones es necesario emplear ventanas menores, puesto que se van a reducir las necesidades de cálculo asociadas.

Se concluye que, empleando el método de estimación de direcciones de RAO, los mejores resultados se obtienen para ventanas cercanas a los 10 píxeles de lado.

Puesto que a menudo es aconsejable centrar la ventana en el punto de interés, se deberá trabajar con tamaños de 9x9 u 11x11 píxeles. Los estudios realizados recomiendan la de 11x11, si bien las diferencias son poco importantes y no debe descartarse el empleo de máscaras de 9x9 píxeles si se desea priorizar la reducción de la carga computacional; aunque la reducción no sea generosamente notable.

Es necesario definir para éste método el sensor utilizado, estudiar sus características y su nivel de ruido, lo que da a priori la ventana con la que se puede trabajar, factor que, mezclado con el ruido es de vital importancia para este método.

4.4 Método de Donahue y Rokhlin

Para estimar la dirección tangencial de la cresta papilar, Maio y Maltoni emplean el método presentado por Donahue y Rokhlin [39]. El método utiliza un operador gradiente para obtener una estimación de la dirección en una ventana de NxN píxeles centrada en el punto de interés.

Para Donahue y Rokhlin, la imagen de la huella digital se considera una representación bidimensional, en forma de curvas de nivel, de una superficie tridimensional. La primera derivada de la función que representa dichas curvas de nivel será, en el punto de interés, el vector tangente a la cresta, es decir su orientación. En una imagen digitalizada, los valores de los valles y crestas sólo se conocen en un conjunto discreto de puntos, por lo que las orientaciones, derivadas de las curvas de nivel, sólo van a poderse aproximar. En lugar de calcular la derivada en el punto de interés (i_o, j_o), Donahue y Rokhlin estiman un valor promediado dentro de una ventana rectangular centrada en (i_o, j_o) mediante minimización de mínimos cuadrados. Puesto que los efectos del ruido aleatorio se minimizan al promediar, éste método va a añadir tolerancia al ruido.

El tamaño óptimo de la ventana va a depender del tamaño relativo de las características de interés, en relación al tamaño del píxel, y del nivel de ruido, existiendo, en general, un compromiso entre la tolerancia al ruido (ventana grande) y precisión (ventana pequeña). En los trabajos presentados por Maio [41] y Maltoni no se especifica el tamaño de ventana empleado, indicándose sólo el elevado coste computacional que representa el empleo de ventanas locales de 19 píxeles de lado.

Sea (i_o, j_o) el píxel en el que se desea estimar la dirección φ_0. Para cada píxel (i_h, j_k) perteneciente a la ventana en la que va a promediarse la dirección, una región cuadrada de α. píxeles de lado y centrada en el píxel (i_o, j_o), se define un vector $\overline{nhk}$ ortogonal a la superficie $S(i, j)$. El vector tangente en cada píxel (i_h, j_k) pertenece al plano ij y es ortogonal al correspondiente vector $\overline{nhk}$.

Y el vector tangente promedio $\bar{t}$, que representa la dirección φ_0, es el vector unidad, situado sobre el plano ij y que es el "más ortogonal" a todos los vectores $\overline{nhk}$ calculados.

En la siguiente figura se representa una superficie S que contiene una cresta en la dirección j, junto con los vectores $\overline{nhk}$, ortogonales a la superficie (se representan los vectores de la fila h=5 en una ventana con α=9 píxeles de lado) y el vector tangente promedio t.

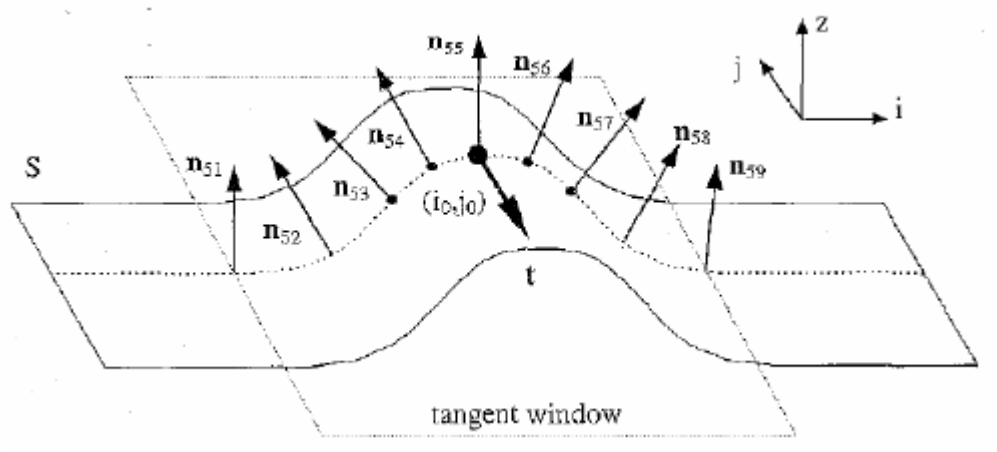


Figura 4.19 Figura que muestra al vector tangente t en dirección de la cresta.

La forma de calcular el vector $\bar{t}$ es la siguiente:

Para cada píxel (i_h, j_k) dentro de la ventana en la que se va a estimar la dirección se localizan sus 4 píxeles adyacentes tal y como se muestra en la figura siguiente: (i_h+1, j_k+1), (i_h-1, j_k+1), (i_h-1, j_k-1) y (i_h+1, j_k-1), y se definen sus respectivos niveles de gris como: a1=gris (i_h+1, j_k+1), a2=gris (i_h-1, j_k+1), a3=gris (i_h-1, j_k-1) y a4=gris (i_h+1, j_k-1).

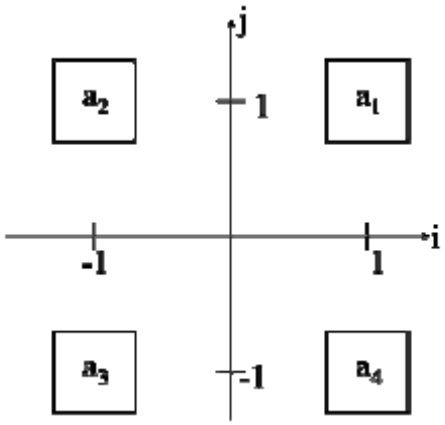


Figura 4.20. Sistema de coordenadas local con centro en el píxel (ih,jk)

Para cada (i_h, j_k) se calcula, por el método de mínimos cuadrados, el vector $\overline{nhk}$=[a_{hk},b_{hk},1] normal a la superficie determinada por (a1,a2,a3,a4). Las componentes de dicho vector son:

$$a_{hk} = \frac{-a_1 + a_2 + a_3 - a_4}{4}$$
$$b_{hk} = \frac{-a_1 - a_2 + a_3 + a_4}{4} \quad \text{.....(31)}$$

El valor de la componente en chk correspondiente al eje z es irrelevante para el cálculo del vector t, que se encuentra en el plano ij, por lo que el método normaliza su valor a 1 y evita su cálculo. Así, la magnitud del vector nhk depende de su ángulo respecto del plano ij. Si es paralelo al eje z su módulo toma el valor 1. A partir de este mínimo, la magnitud va aumentando y el ángulo con el plano ij va decreciendo.

Como es de esperarse, se puede elegir una vecindad mayor, con lo que se aumenta la tolerancia al ruido y se mejora la estimación de la dirección. De todos modos, la tolerancia al ruido no es un problema, puesto que el ruido aleatorio ya se filtra al realizar la media en toda la ventana.

Actualmente se sabe que las orientaciones estimadas mediante operadores gradiente como éste tienen cierto sesgo debido a la discretización, por lo que hay un grado de resolución del que no va a poder pasarse.

Una vez calculados todos los vectores nhk, h=1,.. α, k=1,.. α, en la ventana de estimación, se busca el vector tangente promedio t, como el vector unidad sobre el plano ij, que es “más ortogonal” a todos los nhk. Sean vhk= (ahk, bhk), h=1,.. α, k=1,.. α, los vectores obtenidos al suprimir la componente z de los correspondientes vectores nhk, y sea t= (t1, t2). Entonces, debe determinarse por el método de mínimos cuadrados:

$$\min \sum_{\substack{h=1...\alpha \\ k=1...\alpha}} \left|(v_{hk}, t)\right|^2 \left|\|t\| = 1\right. \quad \text{.....(32)}$$

Donde (v_{hk}, t) representa el producto escalar de los dos vectores.

A continuación se definen tres parámetros útiles en el procesamiento de estimación del direccionamiento, los cuales son:

$$A = \sum_{\substack{h=1..\alpha \\ k=1..\alpha}} (a_{hk})^2$$

$$B = \sum_{\substack{h=1..\alpha \\ k=1..\alpha}} (b_{hk})^2 \quad \text{.....(33)}$$

$$C = \sum_{\substack{h=1..\alpha \\ k=1..\alpha}} (a_{hk} b_{hk})^2$$

$$t = \begin{cases} \left[1, \frac{B-A}{2C} \cdot \operatorname{sgn}(C) \cdot \sqrt{\left(\frac{B-A}{2C}\right)^2 + 1}\right] & si \quad C \neq 0 \\ [1,0] \quad si \quad C = 0, A \leq B \\ [0,1] \quad si \quad C = 0, A > B \end{cases} \qquad \text{.....(34)}$$

Donde sgn (c) devuelve un número entero que indica el signo de un número. Si el número es:

Mayor que cero => 1

Igual a cero => 0

Menor que cero => -1

Con esto, la dirección φ_0 se calcula como se muestra a continuación:

$$\varphi_0 = \begin{cases} tg^{-1}\left(\frac{t_2}{t_1}\right) & si \quad t_1 \neq 0 \\ \frac{\pi}{2} & si \quad t_1 = 0 \end{cases} \qquad \text{.....(35)}$$

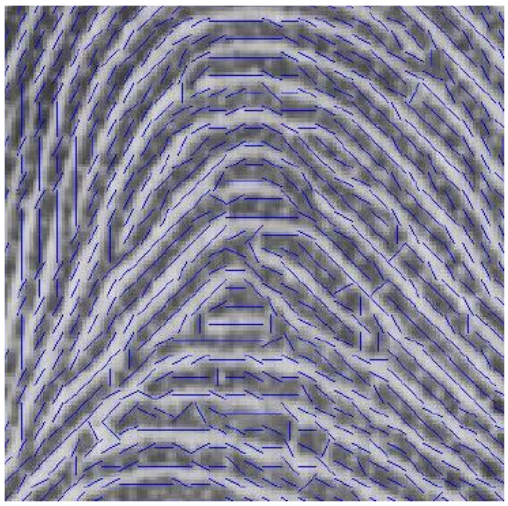


Figura 4.21. Representación del mapa de direcciones obtenido aplicando ventanas de 5x5 píxeles.

A continuación se muestran los mapas de direcciones obtenidos para diferentes tamaños de la ventana de estimación.

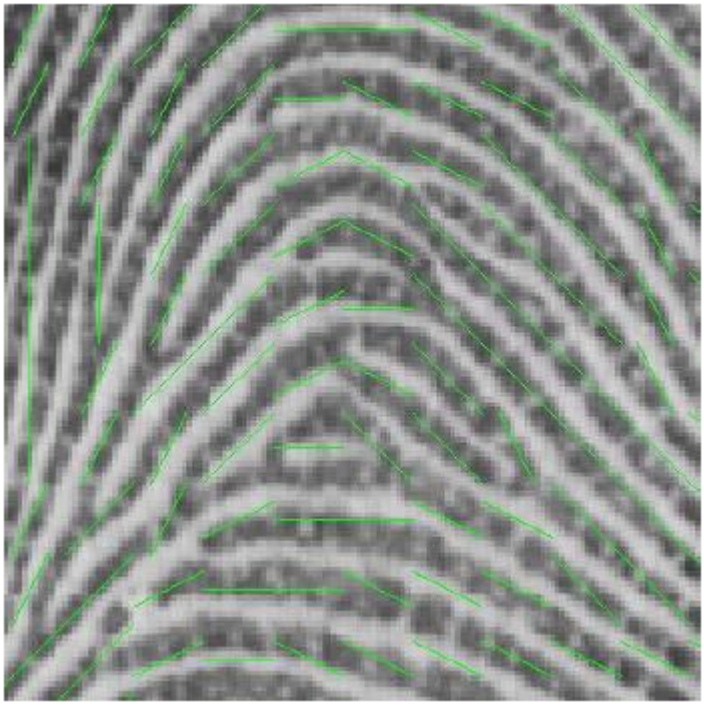


Figura 4.22 Representación del mapa de direcciones obtenido aplicando ventanas de 14x14 píxeles.

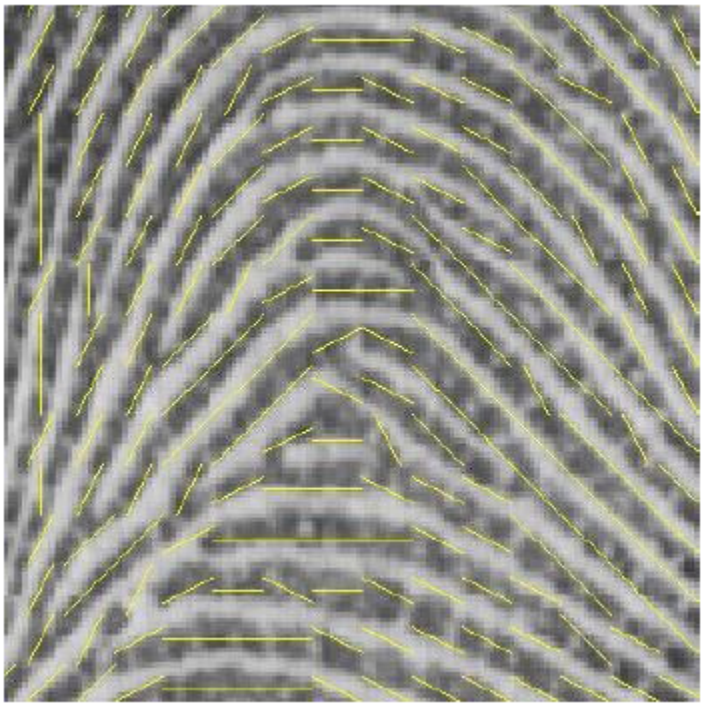


Figura 4.23 Representación del mapa de direcciones obtenido aplicando ventanas de 10x10 píxeles.

Experimentalmente se ha determinado que la ventana de 10x10 pixeles resulta ser la óptima, incluso haciendo una comparación con el método de Rao, en ciertos tamaños de la ventana, el propio método de Rao parece tener una mayor inmunidad al ruido siendo el método de Donahue más sensible a los defectos de la imagen dactilar.

Esto se debe al hecho de que, mientras que Rao realiza la media de gradientes encontrados mediante máscaras de 3x3 píxeles, el método de Donahue promedia los resultados obtenidos empleando máscaras de 2x2 píxeles que, en principio, van a presentar una mayor sensibilidad a la presencia de píxeles ruidosos.

Este método, genera una gran carga computacional y los resultados obtenidos son muy parecidos al método de Rao; incluso proponiendo la reducción de carga computacional al tabular la raíz cuadrada necesaria en el cálculo, posteriormente es necesario calcular el arco tangente, la tabla debe almacenar la respuesta con una precisión elevada para evitar una excesiva propagación del error.

Capítulo V. Método de identificación de huellas propuesto

En este capítulo se describe en primera parte, la obtención de la huella digital, con las características necesarias para su posterior análisis.

Posteriormente, se estudiará la compatibilidad entre lectores comerciales y el algoritmo propuesto; sin dejar de lado el factor económico.

A través del capítulo se irán enumerando las diversas técnicas para la extracción de minucias, su separación del resto de la imagen, la calidad de la información, la selección de información realmente útil y por último la generación de un código único que permita la identificación plena y satisfactoria de las huellas digitales.

Los continuos ataques que sufren los sistemas de seguridad existentes, así como la necesidad de proteger aún más y mejor los entornos de tecnologías de la información, está llevando a que se pongan las miras en nuevas alternativas que cobran fuerza frente a la actual oferta de hardware y software de protección.

En este escenario, la biometría se abre paso como una opción que, debido a sus características, basadas en los rasgos biométricos de las personas, la hace más difícil, sino imposible, de robar o falsificar, validándola como una opción para la seguridad con un gran futuro por delante.

Los peligros a los que están expuestos hoy en día los sistemas de información, así como aquellos espacios que tienen el acceso restringido, están llevando a los responsables de la seguridad en las empresas a buscar nuevas fórmulas que solucionen esta problemática [42].

La creciente demanda en materia de seguridad ha disparado las ventas de sistemas biométricos, como lo muestra el estudio generado por el International biometric Group, en este mismo estudio, se analiza el crecimiento en tecnologías biométricas hasta el año 2014, como se aprecia en la imagen presentada a continuación.

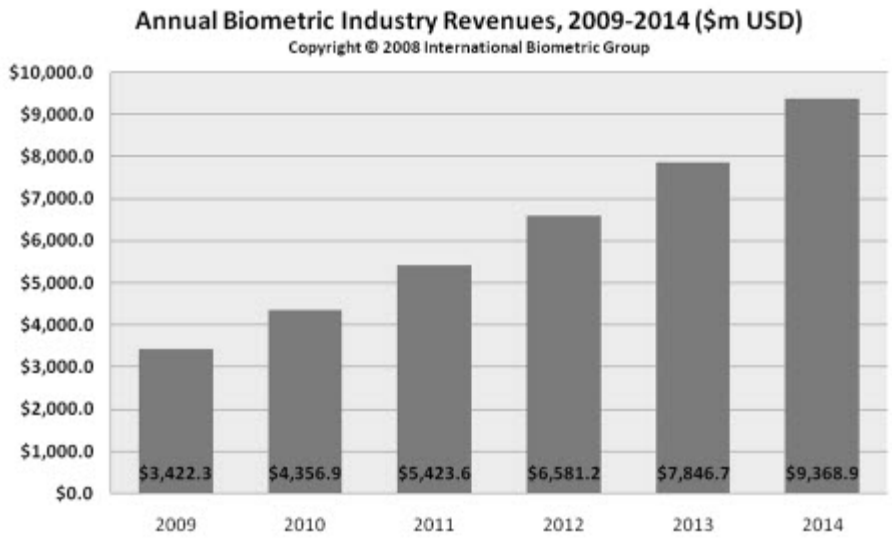


Figura 5.1 Prospección de crecimiento en ganancias de los sistemas biométricos de 2009-2014.

Como ya se mencionó, la tecnología más utilizada es la de reconocimiento de huellas digitales, y la creciente demanda ocasiona que surjan día con día más compañías que quieran incursionar en este negocio.

La importancia de que se ofrezca una gran diversidad de oferta en el mercado biométrico es que todas las empresas deben cumplir con los requisitos mínimos de identificación, autenticación, verificación de identidad, inmunidad al ruido y rapidez para el que fueron diseñados.

Esta creciente preocupación se ha visto manifestada por diversas entidades internacionales encargadas de estudiar, analizar y crear estándares para el óptimo funcionamiento de estas tecnologías, como se presenta en el siguiente comunicado:

El Grupo de Trabajo Europeo de INTERPOL sobre Identificación de Huellas Dactilares está sumamente preocupado por el aumento de la utilización de las llamadas unidades de escanerización directa. Este

sistema se utiliza para la toma de huellas dactilares y su transmisión rápida a los sistemas AFIS. Aunque se entiende la necesidad de proceder al envío rápido de las huellas dactilares, el Grupo opina que los sistemas que se están fabricando no producen la calidad de imagen necesaria para que los expertos examinen las huellas dactilares con todo detalle, dado que las imágenes procedentes de estos sistemas:

1. Están comprimidas y, en consecuencia, pierden datos y generan anomalías.

2. Son un conjunto de datos tomados uno tras otro, con dedos que pueden moverse y un escáner móvil y tienden a presentar anomalías.

3. Son de calidad inferior a las impresiones tomadas con tinta y papel.

4. Son más costosas (estimación: 50.000 USD o más).

5. No son más rápidas de tomar.

Las ventajas percibidas son la posibilidad de tomas repetidas y la rápida transmisión de las imágenes. Esta última propiedad podría también obtenerse con equipos modernos.

Los sistemas de escanerización directa promueven un entorno sin papel, pero al mismo tiempo suprimen datos valiosos. Estos datos no sólo son muy importantes para el proceso de evaluación, sino que tienen también una importancia trascendental para las mejoras futuras de los algoritmos de codificación basados en los detalles de la cresta y, en consecuencia, frenan el progreso de identificación de las huellas dactilares.

Por consiguiente, el Grupo recomienda encarecidamente que se efectúen investigaciones a fondo para crear un sistema que produzca una "imagen en bruto" (conforme a la original y no manipulada por ningún programa informático). Este sistema debe ser fácil de utilizar y producir imágenes incluso mejores que las obtenidas con tinta y papel independientemente de la pericia del operador. Unas imágenes mejores podrían fomentar considerablemente la eficiencia (precisión en las búsquedas) de las operaciones de dactiloscopia.

La "imagen en bruto" aumentaría la capacidad de proporcionar pruebas positivas gracias a la reproducción exacta de todas las características de la impresión que se está captando (imagen análoga) [43].

En nombre del Grupo de Trabajo,

A.J. Zeelenberg,
Presidente

Retomando la preocupación del grupo de trabajo Europeo de la INTERPOL en rubro de huellas digitales, los sistemas expuestos anteriormente en este trabajo no son totalmente vulnerables al ruido, considerando que son los más estudiados y además que tienen como soporte el ser desarrollados por los mejores especialistas, el temor a utilizar algoritmos desarrollados sólo de manera comercial es evidente, al destacar deficiencias en la captura, extracción de minucias, mapeo de información y falsas aceptaciones.

Aunque la mayoría de aplicaciones comerciales vienen listas para su utilización, es posible comprar las librerías de desarrollo para poder generar una aplicación específica. Estas librerías son conocidas como librerías de desarrollo SDK para los productos biométricos.

Como ejemplo se pueden mencionar:

SDK Nitgen eNBSP

Librerías de desarrollo SDK para los productos biométricos de huella digital de Nitgen.

Permite implementar software con una interface de usuario de forma fácil y rápida

Descripción:

eNBSP SDK 4.0 es un kit de desarrollo de software que combina el SDK 3.0 existente (ahora denominado BSP - Biometric Solution Provider) y un algoritmo de reconocimiento de huellas 1:N, no sólo para aplicaciones básicas, sino también para aplicaciones que utilizan las huellas de base de datos de gran capacidad y donde se requiere una velocidad de búsqueda de huellas muy elevada.

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

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

Principales características:

1.- Proporciona una interface de programación API óptimo para el desarrollo de software de reconocimiento
2.- Proporciona una aplicación de software de ayuda y una interfase de

usuario de rápida y fácil utilización
3.- Permite un fácil desarrollo mediante funciones de registro y autentificación de huellas que operan de forma transparente para el programador
4.- Funciones de identificación 1:N muy rápidas
- Algoritmo eNSearch: para aplicaciones grandes o medianas (función que requiere una licencia adicional)
5.- Hasta 10 huellas por persona
6.- Permite una fácil personalización de la interface de usuario minimizando el coste y tiempo empleados en el desarrollo
7.- Seguridad en la utilización de la información de la huella mediante un algoritmo de encriptación de 128 bits
8.- Soporta la conversión de distintos formatos de imágenes de huella (BMP, JPG, WSQ, etc.) [44]

La compañía que tiene como clientes a las empresas con mayores ventas en el mundo (HP, Dell, IBM y Microsoft entre otros) es Digital Persona, quien proporciona SDK's de forma gratuita para diferentes plataformas, como son C, Visual Basic, java, entre otros y para diversos sistemas operativos, como son Windows 98, 2000, Xp, Vista y 2003 server, así como para diferentes versiones de Linux y Unix.

Con SDK's de prueba, en teoría, es suficiente para lograr hacer aplicaciones sencillas que involucren huellas digitales; sin embargo esto no sucede así en la práctica, ya que los SDK's de prueba de Digital Persona vienen agrupados por librerías, esto es, al descargar el SDK de prueba para Windows, éste pesa 70 Mb y contiene los bloques de extracción de huellas, minucias, etc.

Al momento de implementar éstas funciones, se hace referencia a librerías con los componentes en código hexadecimal para conectar al

dispositivo, por ejemplo, en el SDK de prueba viene una aplicación ya compilada, en Visual Basic 6, donde sólo se adquiere la huella digital del lector USB.

Al recrear el código para poder desarrollar la misma aplicación, se percata el usuario o desarrollador que hacen falta las librerías para llevar a cabo la función de apertura o extracción de minucias, etc.

Esas librerías sólo vienen en la versión profesional del SDK, el cual se puede complementar con librerías específicas, por ejemplo las librerías para el mapeo de información contra una base de datos, el envío de paquetes encriptados, la lectura de diversas imágenes, el guardado de imágenes o vectores característicos, etc.

También es necesario mencionar que en la mayoría de los casos, los SDK's creados por compañías que desarrollan hardware y software, las librerías adquiridas están optimizadas para los dispositivos propios de dicha compañía, liberándose de toda responsabilidad de utilizar sensores biométricos diferentes.

Este aspecto es de suma importancia, ya que si se desea adquirir las librerías de desarrollo de una compañía, la cual también proporciona el hardware, a la cotización inicial es altamente recomendable incluir e costo de los dispositivos biométricos, como parte del "kit" de desarrollo, para evitar problemas futuros de incompatibilidad o de que algunas funciones no lleven a cabo su cometido al 100% por un fallo de comunicación con el dispositivo.

Entre los principales clientes en México de Digital Persona se encuentran Telmex, Grupo Elektra, Banco Azteca y Pemex entre otros [45].

El alto costo de estas librerías y dispositivos los hace accesibles sólo a compañías que dependen directamente de una identificación eficaz, segura y confiable, como es el caso de bancos o acceso a zonas de máxima seguridad; mencionando el caso de Banco Azteca quien tiene registrados 1.2 millones de usuarios quienes día a día realizan operaciones bancarias utilizando el software y hardware proporcionado por Digital Persona [46].

Para el desarrollo de ésta tesis se adquirió un lector de la marca Microsoft, el modelo Fingerprint reader USB compatible, siendo este el mas económico en su categoría, en un estudio que se llevó a cabo comparando los precios de lectores de la marca IBM, Digital Persona, HP, IBM, etc.

Al adquirir un lector biométrico, viene con un programa que permite la configuración de éste y utilizarlo en la casa u oficina en todos los lugares en donde hay una contraseña, “sustituirla” por la huella digital.

Por ejemplo, la adquisición de el lector U.are.U 4500 placement reader con el software DigitalPersona Personal 4.0 tiene un costo de $69.95 dólares [47] adquiriéndolo directamente en la página de Internet del fabricante, de hacerlo en tiendas establecidas, el costo se incrementa considerablemente.

Otra opción con muchos años en el desarrollo de software biométrico, que posee SDK’s gratuitos y además, que es compatible con diversos dispositivos, son las librerías creadas por Griaule Biometrics.

Esta compañía pone a la disposición de los usuarios los SDk’s de prueba o gratuitos para el desarrollo de software, haciendo una

clasificación por sistema operativo, plataforma a utilizar y dispositivo biométrico adquirido.

Las librerías tienen un espacio de 122 Mb, y al ser descomprimidas ocupan poco menos del doble en disco duro; vienen diversos ejemplos para casi todas las plataformas, entre ellas se encuentran: Java, C, C++, Visual BASIC 6, etc.

El funcionamiento de los SDK's de Griaule Biometrics difiere de los de Digital Persona principalmente en que los primeros sí aceptan diversos lectores biométricos, entre los que se encuentra el utilizado para este trabajo, el fingerprint reader de Microsoft.

Es muy estable y permite fácilmente la incursión de nuevas herramientas, como búsqueda en bases de datos y diversos algoritmos de obtención y filtrado de las huellas.

A continuación se presenta una comparación de las diferentes características de SDK's actuales:

Feature	Fingerprint SDK	Fingerprint reader manufacturer software [?]	Other biometric recognition products [?]
Microsoft Fingerprint Reader support	Yes	No	No
Support for several fingerprint readers	Yes	No	No
Recognition quality and speed	Very high	Usually slow	Usually slow
Supports Linux PC	Yes	Sometimes	Sometimes
NIST FpVTE LST evaluated	Yes	No	Usually not
Free trial version available	Yes	No	No
Support for ActiveX, DLL, Java, .NET	Yes	No support or Additional fee	No support or Additional fee
Publicly available support forum	Yes	No	No
Large scale, standardization and AFIS experience	Yes	No	No
In-house state-of-art technology development and research	Yes	Sometimes	Sometimes

Figura 5.2 Cuadro comparativo de los diversos SDK's en el mercado [48].

A continuación se presenta el programa compilado por la compañía Griaule, como parte del SDK gratuito.

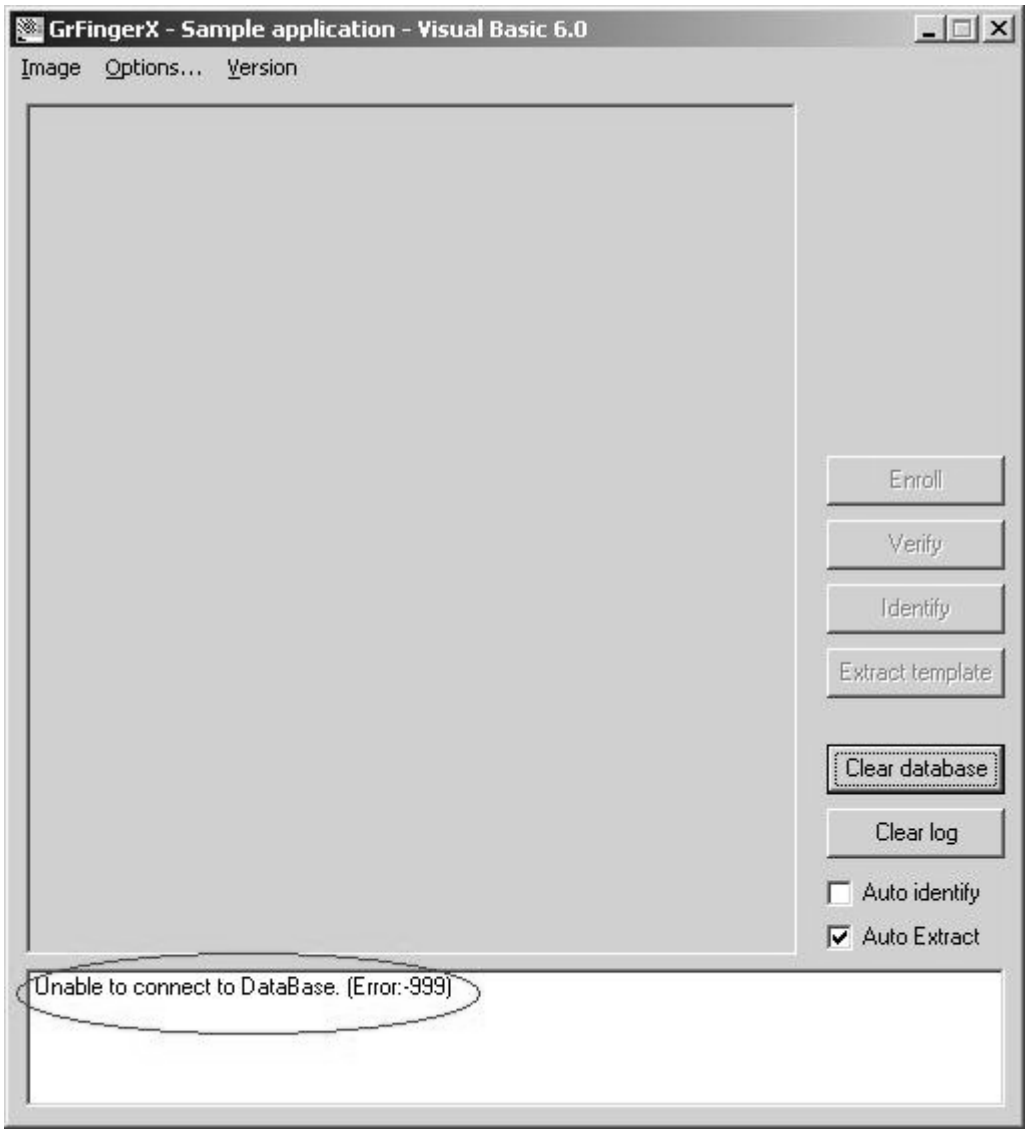


Figura 5.3 Demo de Griaule con SDK gratuito.

Al instalar el SDK propio de Griaule, se instalan archivos dll's, binarios y de clase, quienes contienen el código hexadecimal para comunicarse con el dispositivo, el código para capturar la huella, las instrucciones propias para almacenar la información y los protocolos para poder guardar la imagen como mapa bits (bmp); lo cual lo constituye una matriz de pixeles que se le asigna una dirección asociada a un código de color específico.

La ventaja de guardar imágenes de huellas en este formato es que poseen una compresión sin pérdida de calidad, la desventaja es que ocupan mucho espacio en disco duro de la computadora.

Como se aprecia en la figura correspondiente a la captura del programa demo de Griaule (figura 5.3) hay un error que impide la ejecución plena del mismo, el cual al ejecutarse lo marca en la ventana de mensajes, este error ocurre porque no encuentra una base de datos, la cual es la base de datos de el propio Griaule.

Al instalarse en la raíz de C los dll's de Griaule se obtiene información única de la computadora donde se está instalando el sistema, ya que se pide posteriormente conectarse a Griaule para pedir una licencia de prueba, esto se comprobó al instalar el demo en dos computadoras, ambas con Windows XP Home Edition, y en el momento en que Griaule solicita información de la instalación, se intercambiaron los reportes de instalación entre ambas computadoras, lo cual generó un error y no se liberó la licencia que permitiera la ejecución del programa demo.

Posteriormente se efectuó el registro de la aplicación y se pudieron obtener imágenes de huellas y sus correspondientes minucias; salvo que hay un problema muy grande e irreversible.

Con esta aplicación es suficiente para obtener las imágenes de la huella digital, el gran inconveniente es que la licencia dura solamente 90 días, lo cual ocasiona que pasado ese tiempo sea indispensable adquirir la licencia del SDK, lo cual incrementa enormemente el costo del presente trabajo.

A continuación se presenta una pantalla con el mensaje de advertencia de la duración de la licencia.

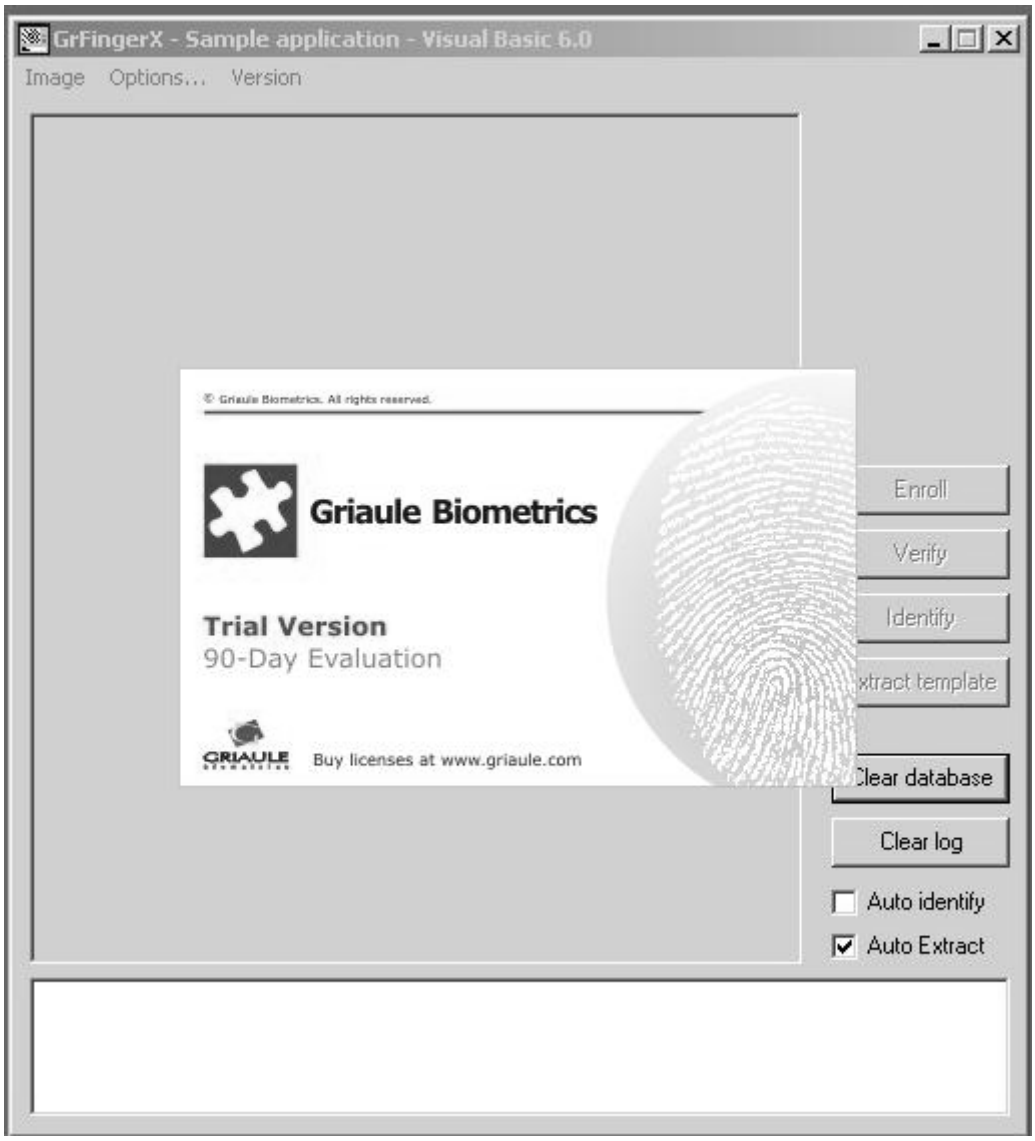


Figura 5.4 Imagen de caducidad de periodo de prueba en licencias en programa demo de Griaule Biometrics.

Posteriormente el error correspondiente a no encontrar la base de datos vuelve a aparecer, impidiendo la ejecución del programa; en la red existen diversas forma de “hackear” al sistema con licencias no legales o piratas, con lo que se fomentan las actividades ilícitas, se incurre en un delito y tampoco se logra efectuar la obtención de minucias, ya que se pone una cinta roja con la leyenda “Trial Version” y “Evaluation Day

Expired", quedando marcada en las imágenes dentro del programa y al momento de guardarlas en el disco duro.

El costo de las licencias se muestra a continuación:

Nombre de la aplicación	Costo	Descripción
AFIS SDK Country Single Computer	US$ 280.00	Licencia para sólo una máquina en sistema AFIS
AFIS SDK Country Integrator 50	US$ 6,000.00	Licencia para 50 máquinas
AFIS SDK Country Integrator 150	US$ 10,000.00	Licencia para 150 máquinas
AFIS SDK State Single Computer	US$ 160.00	Licencia para ser usada estrictamente en una sola máquina

Tabla 5.1 Costo en dólares de las licencias de las librerías de desarrollo SDk's para sistemas AFIS.

Las licencias mostradas están enfocadas a sistemas AFIS, que por sus siglas en inglés significa Sistema de Identificación Automático de Huellas Digitales [49].

A continuación se presentan más costos relativos al reconocimiento únicamente de la huella digital, sin tomar en cuenta bibliotecas relativas al sistema completo de identificación biométrica [50].

Nombre de la aplicación	Costo	Descripción
Fingerprint SDK 2009 Single Computer	US $ 36.00	Licencia necesaria para que el sistema se instale en cada computadora.
Fingerprint SDK 2009 Integrator 150	US $ 3,200.00	Licencia para que el SDK funcione en 150 máquinas
Fingerprint SDK 2009 Integrator 15000	US $ 25,000.00	Licencia para 15000 máquinas

Tabla 5.2 Costo en dólares de las librerías SDK's para el reconocimiento de huellas digitales.

Esta situación obliga a pensar en una situación en la que el sistema sea lo mas económico, robusto, estable y confiable posible, sin que, por ningún motivo no lleve a cabo la detección correcta de las características propias de la huella digital.

5.1 Diagrama a bloques del sistema propuesto

Durante este apartado se describirá la forma en que la información propia de un ser humano es introducida y caracterizada de la mejor manera para poder usarla fielmente por el método propuesto.

Se define como sistema propuesto a los procesos de capturar la huella digital, extraer sus puntos singulares, caracterizar a la huella de una manera única y almacenar esa información fielmente .

El método parte, propiamente como los enumerados anteriormente, desde el momento en que la huella está digitalizada bajo un estándar de trabajo fiel y seguro y posteriormente concluye con la garantía de poder identificar a un individuo de otro, dejando como trabajo futuro el reconocimiento automático y su posterior almacenamiento en una base de datos.

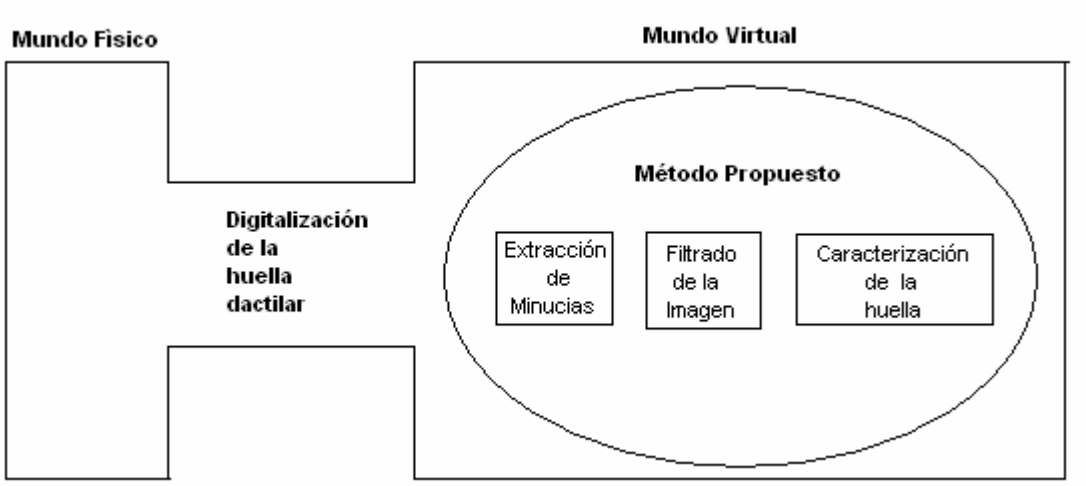


Figura 5.5 Esquema general del sistema propuesto.

En la figura anterior se muestra el paso entre la entrada al sistema por un medio físico, en este caso el lector de huella digital Microsoft fingerprint reader, conectado a una computadora vía USB.

Para llevar a cabo la digitalización de la huella dactilar, es necesario encontrar una forma económica, estable y confiable, pero cualquiera que sea esta forma, se encuentra dentro de la computadora, es decir, se hará de una forma virtual.

A continuación se muestra el diagrama a bloques del sistema completo propuesto en este trabajo.

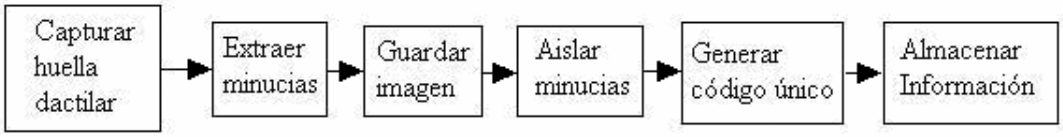


Figura 5.6 Diagrama a bloques del sistema propuesto.

5.2 Captura de Huella dactilar

Al adquirir el lector Microsoft fingerprint reader, viene con un software de uso personal elaborado por Digital Persona, el cual administra contraseñas de cualquier tipo, por ejemplo correos electrónicos, inicio de sesión y uso de programas y acceso a archivos.

Para los propósitos de este trabajo, podría ser una opción viable si se guardaran las imágenes de las huellas digitales, mas sin embargo, la forma en que trabaja el software de reconocimiento es la siguiente:

1) Configurar dispositivo para la administración de contraseñas.

2) Mientras el dispositivo esté conectado, siempre se mantendrá latente esperando el momento de identificar una huella digital.

3) El dispositivo emite un veredicto si la huella entrante había sido previamente almacenada o no.

4) En caso negativo, se niega el acceso a la aplicación o archivo.

5) En caso positivo, la contraseña es enviada a la aplicación que lo solicite o se accede a algún sistema de archivos, etc.

Este sistema es efectivo, salvo que no almacena las huellas como imágenes, almacena un vector encriptado el cual se encuentra distribuido por varias carpetas del sistema operativo Windows.

Pese a estas grandes medidas de seguridad este sistema ya ha sido hackeado, por Mikko Kiviharju, un investigador que trabaja para el ejército finlandés.

Dado que la contraseña que libera la huella dactilar no es cifrada en ningún momento, Kiviharju ha demostrado en Black Hat Europe 2006 que puede ser interceptada por un sniffer y utilizarse para acceder al ordenador -o al sitio web- presuntamente protegido [51].

En el año 2005, cuando fue presentado el Microsoft fingerprint reader, fue pionero en esta tecnología, y estar con lo último en esa época costaba $70 euros.

Para ilustrar mejor el proceso por el cual el sistema ha sido hackeado se presenta la siguiente imagen:

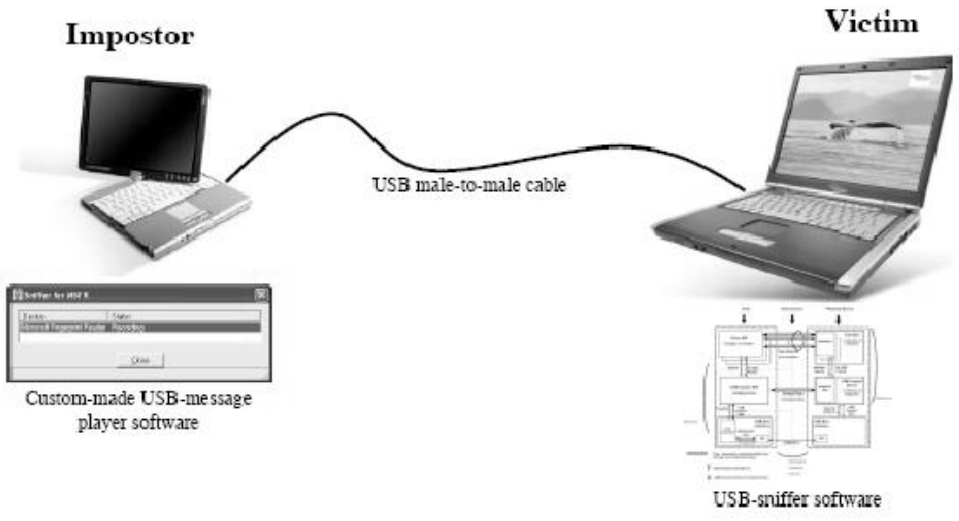


Figura 5.7 Esquema de hackeo del sistema Microsoft Fingerprint reader y Digital Persona.

El impostor o falso dato de identidad se comunica vía USB, enviando el protocolo de información de una huella. Con esto, la computadora que posee el software debe poseer la capacidad de discernir si es una huella real o no.

El sistema en conjunto no pasó la prueba, el lector por que la comunicación USB lo hace de manera estandarizada, y la huella no va encriptada al momento de entrar en la computadora para ser procesada, y el algoritmo provisto con el software no fue capaz de detectar la falsa identidad.

Al momento de ser presentado el dispositivo Microsoft citó: 'Microsoft Fingerprint Reader' no debe usarse para proteger información confidencial o para acceder a redes corporativas, ya que esos casos será mejor seguir utilizando una contraseña apropiada [52].

Figura 5.8 Lector Microsoft Fingerprint Reader

El dispositivo empleado funciona correctamente, una ventaja mayor es que no entrega huellas codificadas o comprimidas, lo cual permite obtener la información 100% pura, sin pérdidas o distorsiones; aún falta determinar el medio por el cual se almacenará la huella como

imagen, se extraerán las minucias y se ejercerá total control sobre el dispositivo de la mejor manera posible, incluyendo el aspecto técnico y económico.

Para extraer las características de la huella se cuentan con las ventajas de que el protocolo de intercambio es USB sin alteraciones, la imagen no está cifrada y los datos no vienen comprimidos.

5.3 Extracción de minucias

A lo largo de este trabajo se han presentado varios métodos para obtener las características singulares de una huella dactilar, conocido como minucias.

Para el presente trabajo se debe seleccionar un programa, aplicación, interface, etc. que sea capaz de:

Guardar la huella digital como imagen sin distorsionarla

Preferentemente extraer minucias

Desde el 13 de noviembre de 2007 ha surgido de manera estable para distribuciones Linux el proyecto fprint.

Este proyecto, encabezado por Daniel Drake tiene una meta muy clara: utilizar los dispositivos captores de huellas digitales en Linux.

Tiene las siguientes características:

Es estable en la mayoría de las distribuciones, siendo de las más probadas Ubuntu, Gentoo y Suse

Cuenta con una lista de dispositivos lectores de huellas digitales que son soportados y para que distribución de Linux.

Es open source, por lo que es gratuito.

Este código es abierto y se encuentra en los repositorios de Linux. Permite utilizar sin restricciones los lectores de huellas, así como las imágenes que de él provengan, sin restricciones de ningún modo.

Para su utilización es necesario tener instalada una versión de Linux, para el presente trabajo se optó por XUBUNTU, una distribución optimizada para computadoras con pocos recursos en memoria RAM.

La computadora utilizada tiene 256 Mb en ram, y para la instalación de XUBUNTU se necesitan como mínimo 198 Mb en memoria RAM.

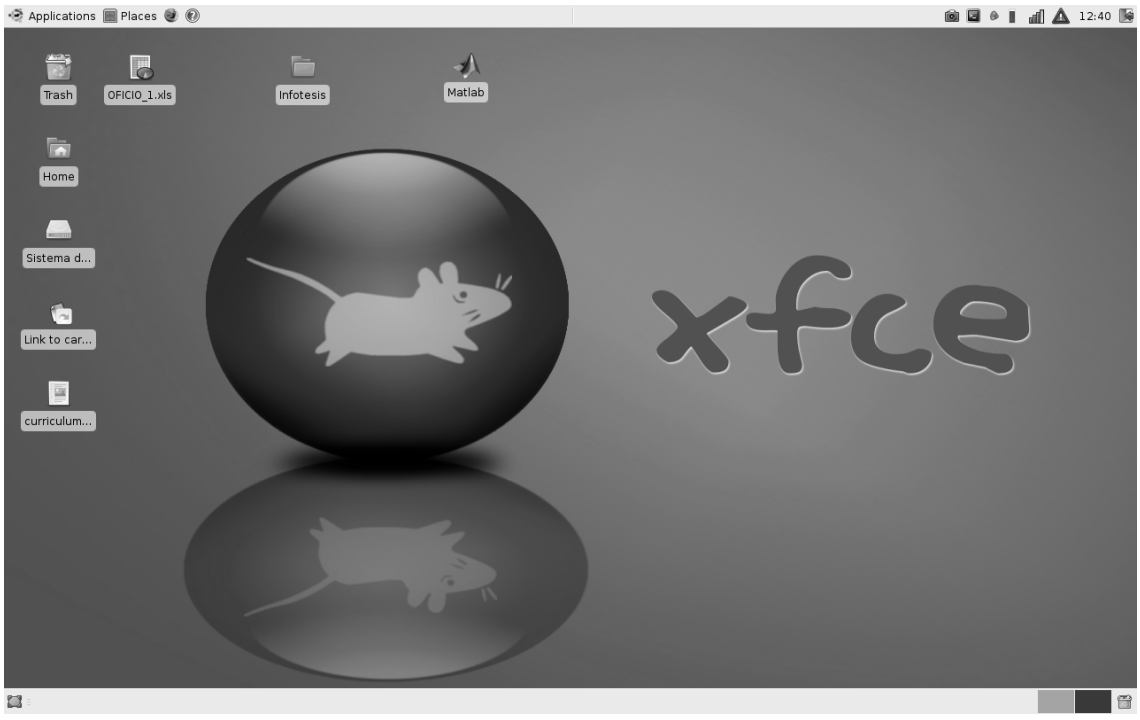


Figura 5.9 Entorno de escritorio de Xubuntu para desarrollo de el presente trabajo.

En esta distribución se incluyen las aplicaciones necesarias para el funcionamiento del sistema operativo y la instalación solo toma 25 minutos, sin embargo como cualquier instalación directa en el disco duro, es necesario llevar a cabo un particionamiento de la unidad de almacenamiento de la computadora donde se va a instalar [53].

El entorno de la distribución XUBUNTU es gráfico en su mayoría, como se muestra a continuación:

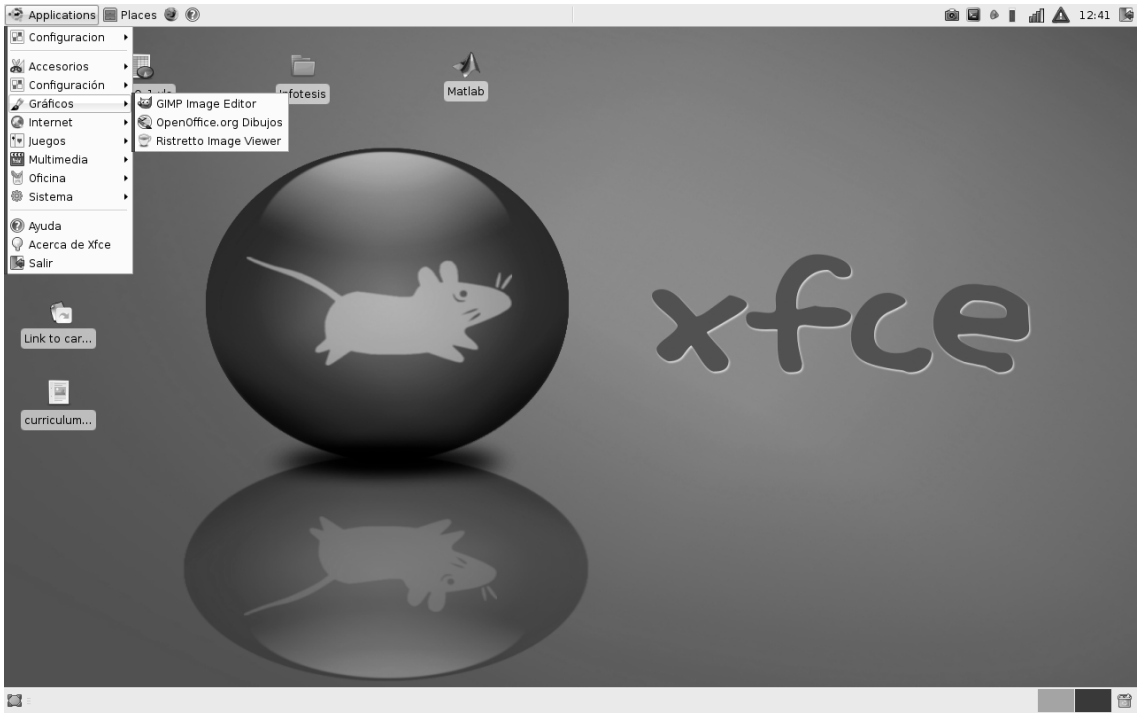


Figura 5.10 Entorno gráfico de XUBUNTU

Existen diversos componentes dentro de el proyecto fprint, la librería pam_fprint es la encargada de pedir la huella digital al inicio del sistema, en vez de contraseña al iniciar sesión en Linux.

El paquete fprint_demo es una aplicación visual, o en Linux aplicación GUI la cual engloba y hace trabajar conjuntamente las capacidades de la librería libfprint.

La librería libfprint es el núcleo central de este proyecto, es el componente donde se lleva a cabo la lectura del dispositivo y la manipulación de la imagen. Esta librería trabaja bajo el principio de que las huellas digitales provenientes de diferentes dispositivos no son necesariamente compatibles; es decir, diferentes captores de huellas tienen considerablemente mayores áreas de interés unos con otros, así como condiciones en su superficie y comparar imágenes entre ellos no es trascendente [54].

Aún hay funciones que no se han implementado del todo dentro del proyecto fprint, como por ejemplo la captura directa de la imagen, aunque la aplicación fprint_demo permite guardar imágenes y, conjuntamente con la librería fprint la extracción de minucias.

Una vez instalado el proyecto fprint, es necesario instalar la aplicación fprint_demo para los fines que se persiguen en el presente trabajo. Más no es indispensable la instalación de las librerías PAM y la librería fprintd, quien se encarga de resolver problemas de comunicación entre los dispositivos.

La razón por la que no es necesaria la librería fprintd es porque el dispositivo adquirido, el Microsoft Fingerprint reader si es soportado con gran compatibilidad en el proyecto fprint, como se muestra a continuación en la tabla que muestra las compatibilidades de los dispositivos y el proyecto fprint [55].

Compañía	Nombre del producto	Driver
ASUS	F3Sv laptop embedded	aes1610
ASUS	R1F tablet embedded	upekts
ASUS	Z37E laptop embedded	upeksonly
Cherry	SmartTerminal SFR-1244U	upektc
Covadis	Alya	uru4000
Covadis	Atria	uru4000
DigitalPersona	U.are.U 4000 Reader	uru4000
DigitalPersona	U.are.U 4000B Reader	uru4000
DigitalPersona	U.are.U Fingerprint Keyboard	uru4000
Fujitsu-Siemens	FP-Sensor S26381-K342-V1 GS:01	aes2501
Fujitsu-Siemens	Lifebook S7110	aes2501
HP	2510p laptop embedded	aes2501
HP	6510b laptop embedded	aes2501
HP	6710b laptop embedded	aes2501
HP	6910p laptop embedded	aes2501
HP	8710w laptop embedded	aes2501
HP	nc6400 laptop embedded	aes2501
HP	nx6125 laptop embedded	aes2501
HP	nx6325 laptop embedded	aes2501
HP	Nw9440 laptop embedded	aes2501
HP	Pavilion dv6640ew laptop embedded	aes2501
HP	Pavilion HDX9494nr laptop embedded	aes2501

HP	Pavilion tx1302au tablet embedded	aes1610
HP	Pavilion tx2108ca laptop embedded	aes1610
IBM	ThinkPad T43p embedded	upekts
IBM	ThinkPad T61 embedded	upekts
IBM	ThinkPad X41 embedded	upekts
IBM	ThinkPad X60 embedded	upekts
Lenovo	V100 laptop embedded	aes1610
Lenovo	3000 N100 laptop embedded	aes2501
Lenovo	ThinkPad R61i laptop embedded	upeksonly
Medion	MD85264	aes2501
Microsoft	Keyboard with Fingerprint Reader	uru4000
Microsoft	Wireless Intellimouse with Fingerprint Reader	uru4000
Microsoft	Fingerprint Reader	uru4000
Microsoft	Fingerprint Reader	uru4000
Precise Biometrics	100 XS	aes2501
Samsung	P35 laptop embedded	upektc
Samsung	X65 laptop embedded	aes1610
Sony	SZ61VN embedded	upeksonly
System76	Pangolin laptop embedded	upeksonly
Targus	PA460U DEFCON Authenticator	aes4000
Toshiba	A-105 laptop embedded	upekts
UPEK	Eikon	upekts
Veridicom	5thSense	vcom5s

Verinex	XM550	uru4000
Verinex	XM570	uru4000

Tabla 5.3 Tabla de compatibilidad entre lectores biométricos comerciales y el proyecto fprint.

La instalación se lleva a cabo desde la página oficial del proyecto, y siguiendo las instrucciones de instalación se logra un resultado favorable [56].

Para acceder a la aplicación fprint es necesario introducir en modo administrador (sudo en Linux) el nombre del Gui, escrito bajo lenguaje C y con licencia GNU.

Conectar el lector de huellas al puerto USB y posteriormente desde terminal escribir sudo fprint_demo

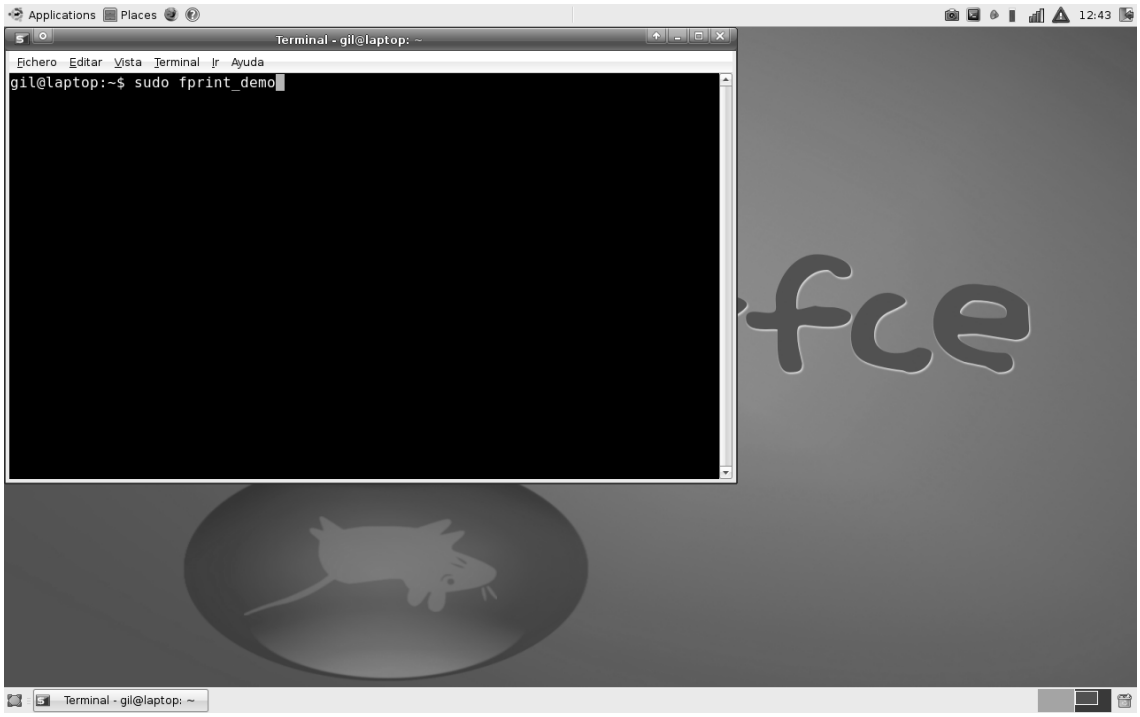


Figura 5.11 Ejecución en terminal de el Gui del proyecto fprint.

A continuación se mostrará la pantalla siguiente, que corresponde a la aplicación mencionada:

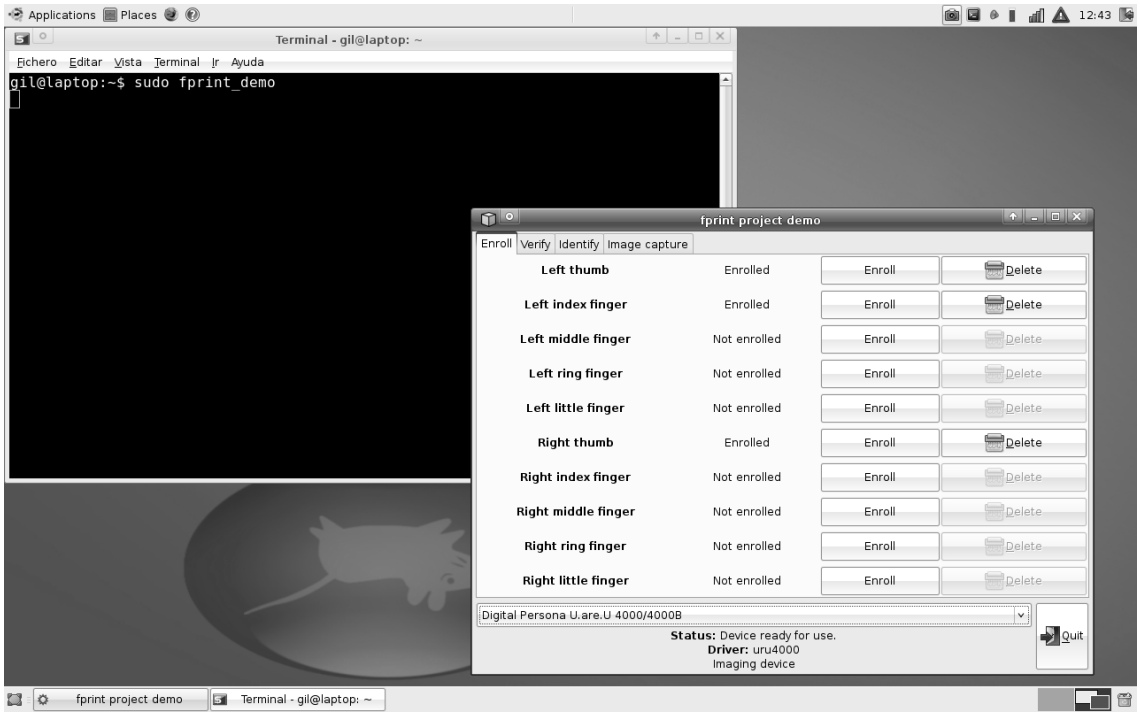


Figura 5.12 Aplicación Gui del proyecto fprint.

Como se observa en la imagen anterior, la aplicación detecta el lector, lo identifica con el nombre localizado en la tabla anterior y garantiza su funcionamiento.

A continuación se muestra una descripción general de la aplicación a utilizar.

La primera opción de la librería libfprint es la de “enroll” que permite guardar un dedo para su posterior verificación. Por defecto la aplicación sólo trae opción para 10 huellas en modo administrador, en modo usuario esta opción no está disponible; esta aplicación sólo hace acciones de verificación y de obtención de imagen de huellas digitales.

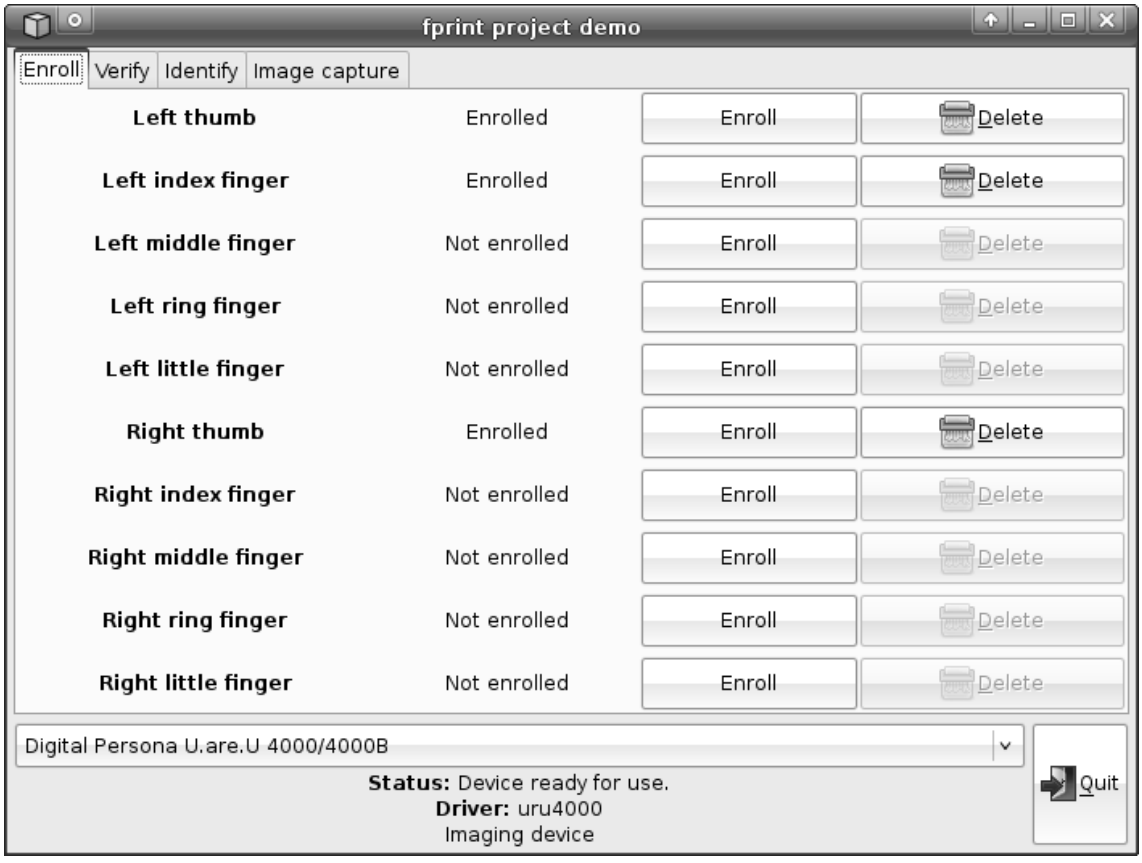


Figura 5.13 Imagen de la opción enroll de la aplicación del proyecto fprint.

La siguiente opción es Verify, con la cual se verifica si una huella digital pertenece o no a las previamente almacenadas. Esta opción es la que se utilizará para la obtención de la imagen del lector de huellas y para la extracción de las minucias.

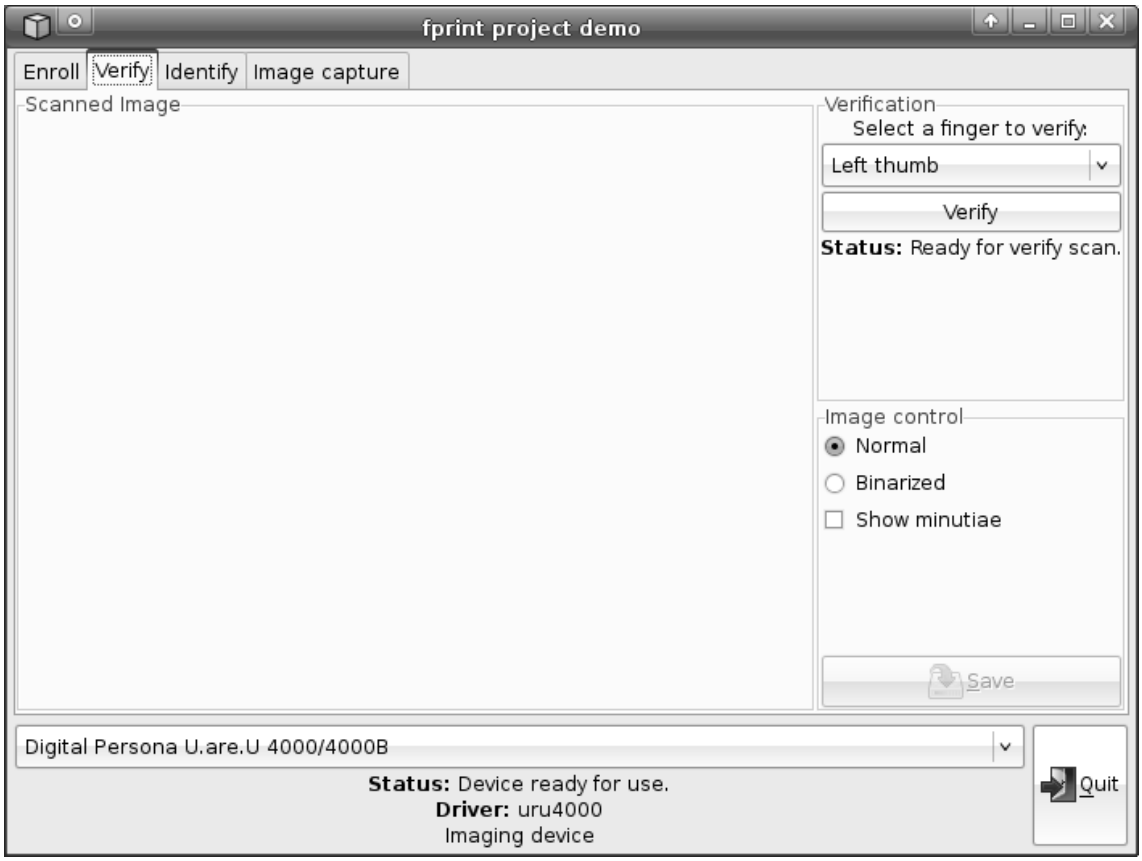


Figura 5.14 Imagen de la opción verify de la aplicación del proyecto fprint.

En esta opción, el lector está listo desde su lanzamiento, hacer click en la opción verify, con lo que el lector de huellas se iluminará y esperará la colocación del dedo a verificar.

Una vez retirado el dedo, la imagen proveniente del lector es desplegada en la ventana de la izquierda tal como se muestra a continuación:

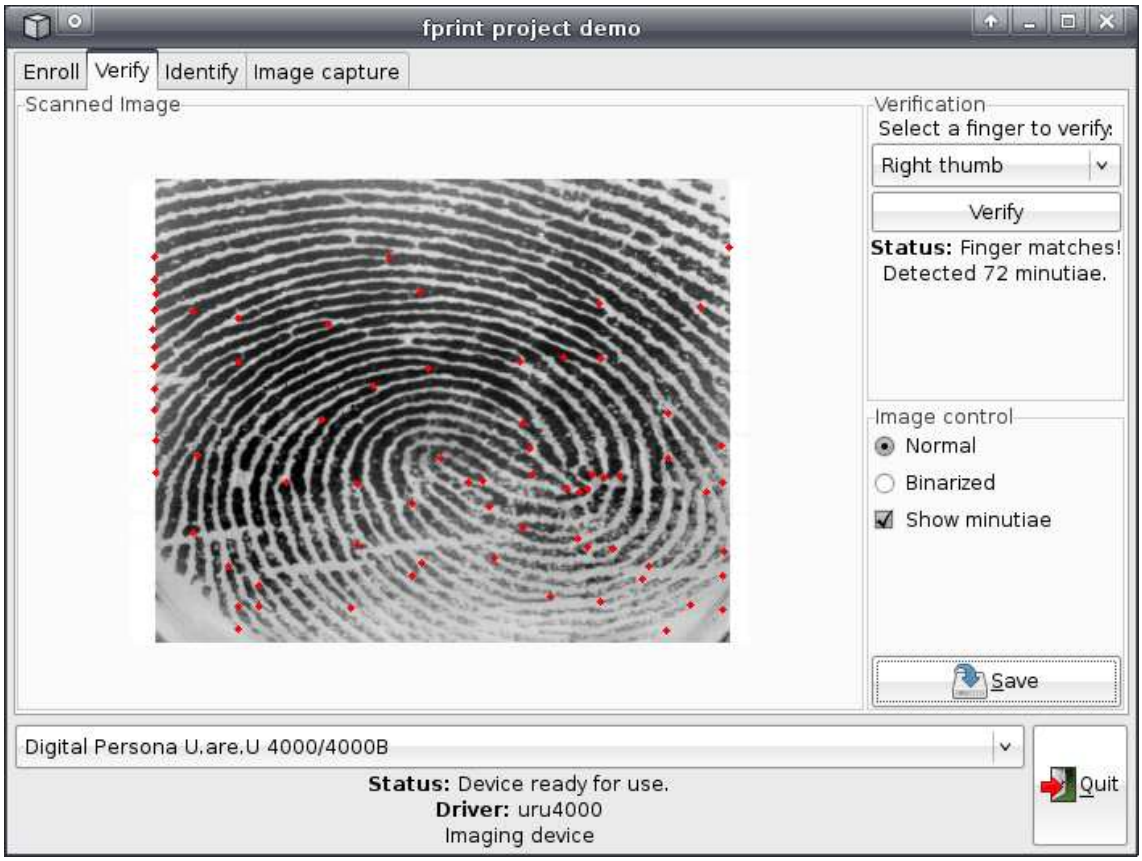


Figura 5.15 Imagen de captura de dedo pulgar con el fprint_demo

Como se aprecia en la imagen se puede guardar la imagen con o sin extracción de minucias, en forma normal o binarizada. Internamente, el dispositivo asigna 32 bits únicos para identificar al dispositivo lector de huellas digitales, este dato único es asociado a las imágenes en varios dispositivos captores de huellas, en este caso, este valor se pone en cero en los lectores permitidos por la aplicación, lo que elimina información redundante al momento de guardar la imagen [57].

La imagen no se almacena binarizada por la pérdida de información, es decir, al extraer las minucias y aparte binarizar no hay una clara diferencia entre las minucias encontradas y los valles captados por el lector.

El proceso de binarización de la imagen es importante para reducir el tamaño de la imagen y para optimizar recursos en los algoritmos de identificación de la huella digital, y por eso este proceso no es omitido del presente trabajo, solamente es realizado en un mejor momento.

Una imagen guardada se aprecia a continuación:

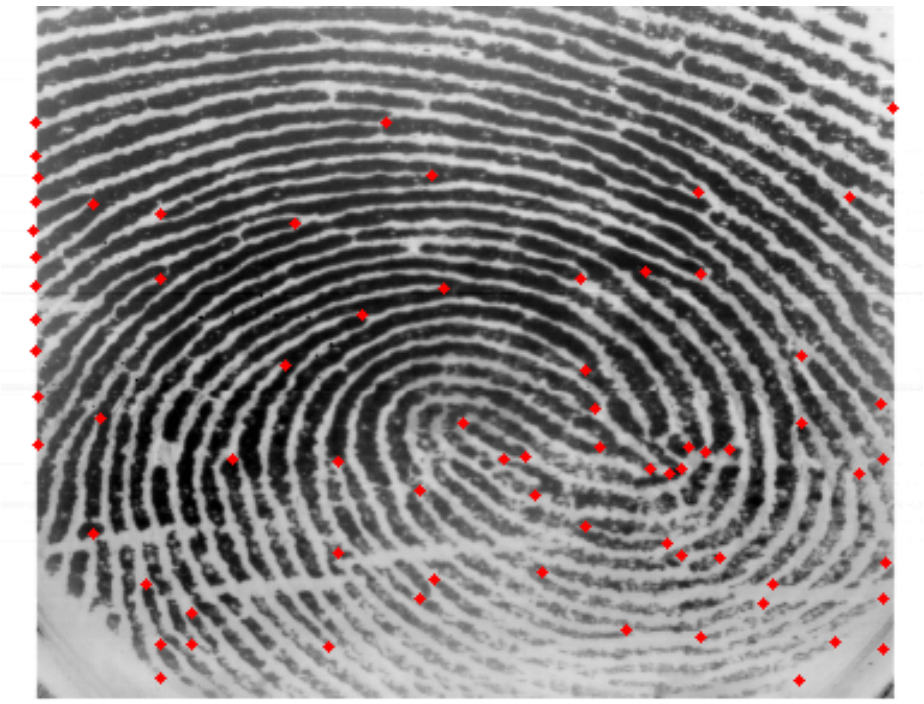


Figura 5.16. Imagen del dedo pulgar derecho guardada con la aplicación del proyecto fprint.

Esta imagen, y en general todas las imágenes capturadas con este método son imágenes de 384 x 289 pixeles, del tipo PNG (Portable Network Graphics), que es un formato gráfico basado en un algoritmo de compresión sin pérdida para bitmaps no sujeto a patentes. Este formato fue desarrollado en buena parte para solventar las deficiencias del formato GIF y permite almacenar imágenes con una mayor profundidad de contraste y otros datos importantes [58].

La imagen de buena calidad depende directamente de la limpieza y nitidez del dispositivo, se realizó la prueba de colocar diversos dedos para su obtención de la huella dactilar sin realizar la limpieza sugerida por el fabricante, Microsoft, y después de 70 capturas se obtuvo el siguiente resultado:

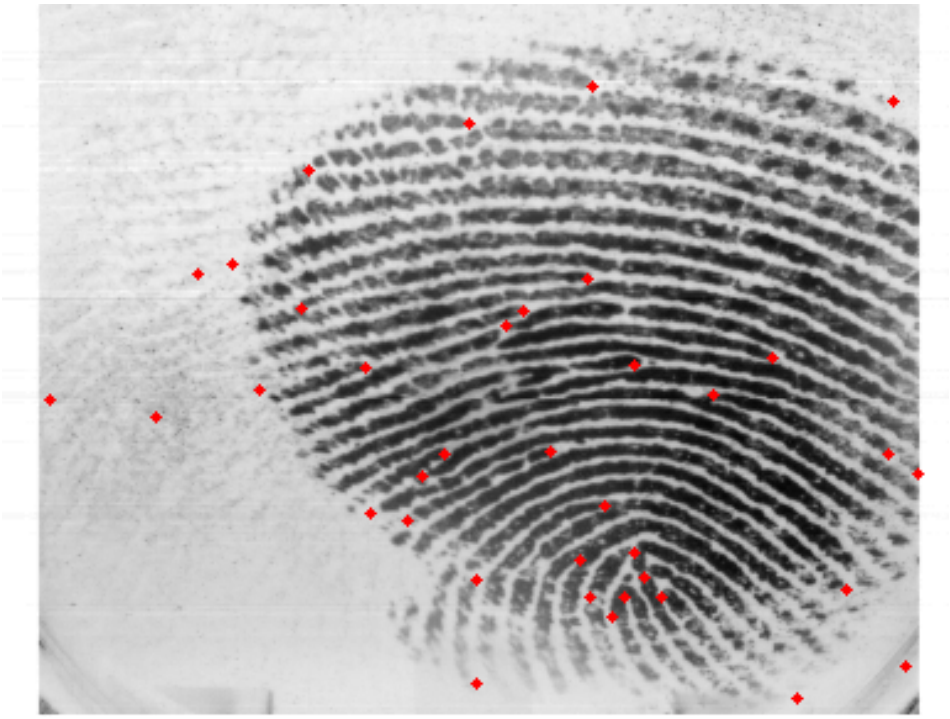


Figura 5.17 Imagen con excesivo ruido de índice derecho.

Como es de esperarse, la cantidad de ruido es considerable, y en zonas donde no hay huella captada se detectan minucias, lo cual genera un grave error. La diferencia de tonalidades de negro reflejan cuáles áreas tuvieron mayor presión sobre el lector.

A lo largo del presente trabajo se demostrará que imágenes con este nivel de ruido son capaces de ser identificadas sin alterar el desempeño del sistema propuesto.

Otra opción de la aplicación es la de identify, la cual se muestra a continuación:

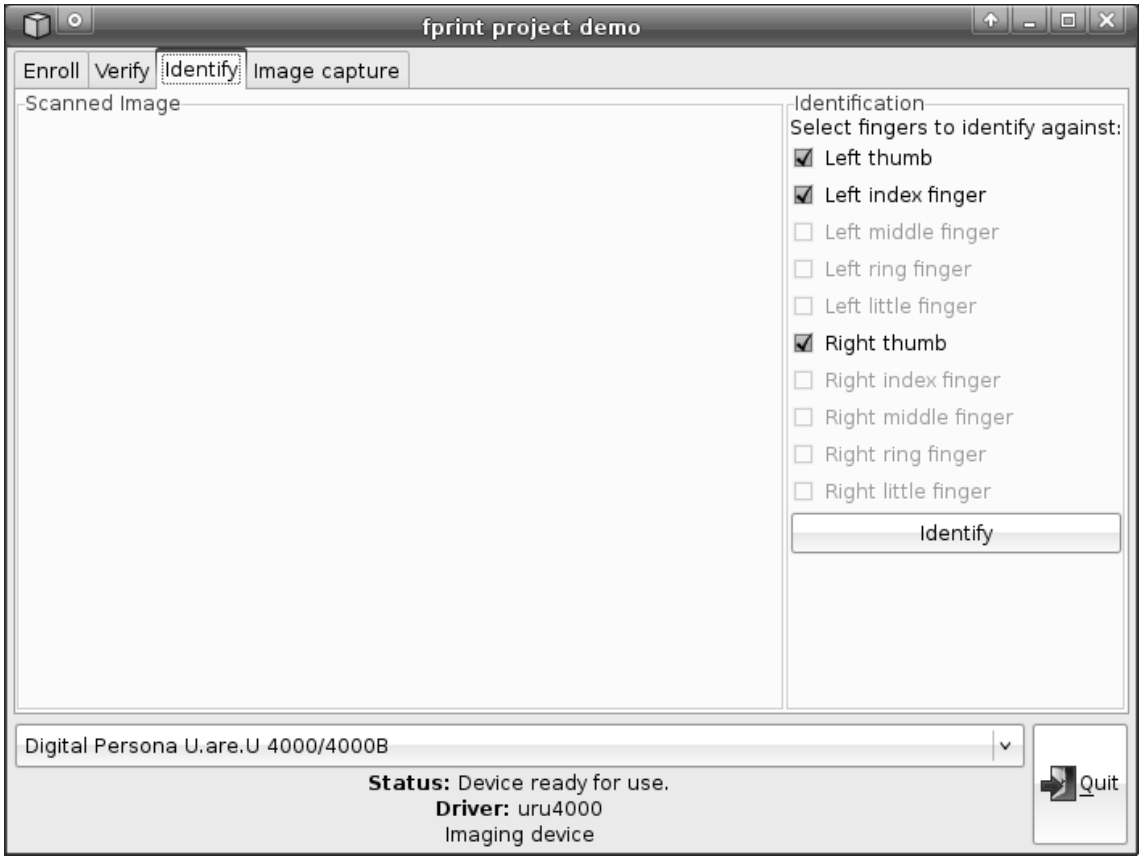


Figura 5.18 Opción Identify de la aplicación del proyecto fprint.

En esta opción, se selecciona con que dedos de los cuales previamente almacenados se comparará la huella que será escaneada en el momento de hacer click en el botón Identify. Como es de apreciarse este es un método de identificación 1:N, o se podría pensar así, pero lo que sucede es que las funciones de la libfprint verifican sólo los dedos seleccionados, no hacen un mapeo general de todos los dedos capturados.

En esta situación sólo se da el proceso de verificación 1:1 de manera secuencial por todos los dedos seleccionados, cuyo máximo es diez.

La última opción de la aplicación es la de guardar directamente la imagen o capture.

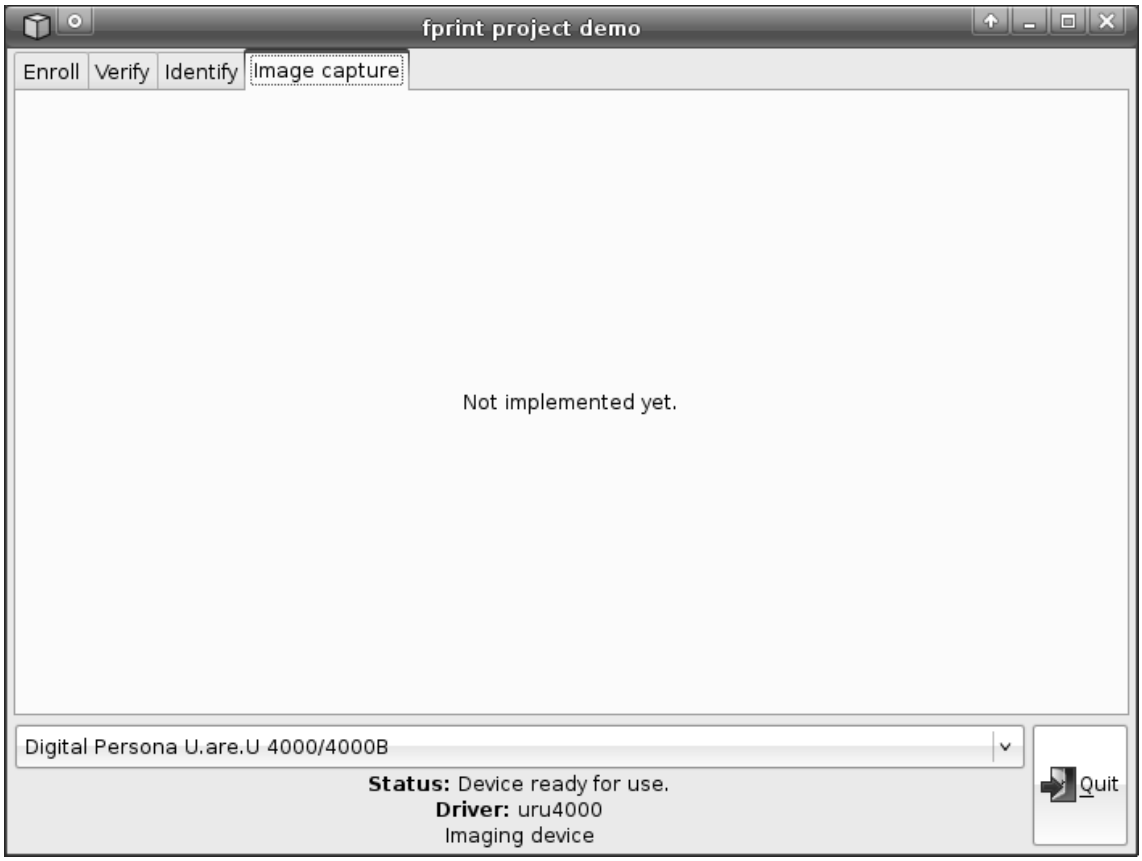


Figura 5.19 Imagen de la opción capture de la aplicación del proyecto fprint.

Esta opción aun no está implementada, pero con la opción descrita anteriormente se cumple el mismo cometido.

5.4 Aislar minucias de huella digital

En el presente apartado se analiza la manera en la cual se separan las minucias de la huella digital de una forma que no se genere ningún error y obteniendo la mejor confiabilidad, así como reducir el costo computacional al mínimo.

Para poder desarrollar las herramientas de cálculo propias de este trabajo es necesario instalar MATLAB 7 con los toolboxes de Image processing versión 6.2 o posteriores.

El software MATLAB se instaló en XUBUNTU de igual forma que en Windows, con lo que se comprobó que el mismo algoritmo escrito en un sistema operativo funcionaba perfectamente en el otro.

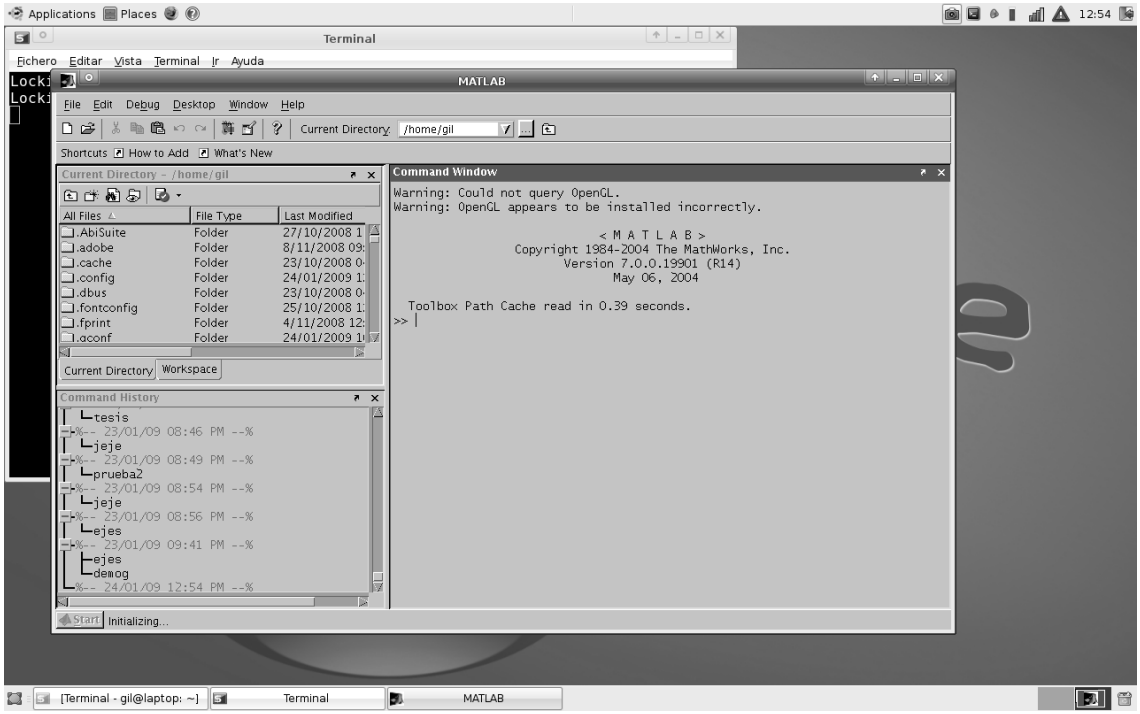


Figura 5.20 Imagen de Matlab 7 instalado en Xubuntu.

Tanto en Windows como en Linux, Matlab consume alta cantidad de memoria RAM al iniciarse por primera vez; en XUBUNTU se agregó el software Conky, con el cual es posible medir los recursos del sistema, y se observó que al arrancar Matlab, el consumo de memoria RAM aumentaba en un 60%, después disminuía y se estabilizaba en un 45%.

En Windows XP, el aumento es mayor y la respuesta del sistema se vuelve mucho más lenta, considerablemente si se tienen aplicaciones

en segundo plano como MS Office, Internet, etc., situación que no se presentó en Linux-Ubuntu.

Como primer método de separar las minucias se planteó separarlas aplicando un filtro de color rojo, ya que las minucias identificadas son señaladas por 13 pixeles de ese color, formando una cruz.

A continuación se muestra una imagen aleatoria obtenida del lector de huellas digitales:

Figura 5.21 Huella del dedo pulgar izquierdo.

Como se puede observar en esta imagen, el nivel de ruido máximo se encuentra cercano a la zona con mayor información, si se aplica el filtro correspondiente a la separación de color se obtiene:

Minucias aisladas

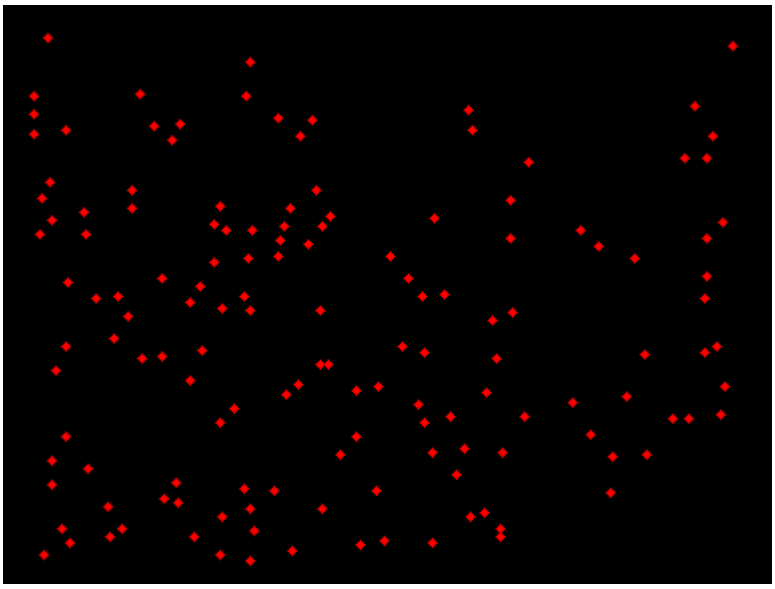


Figura 5.22 Resultado de filtro color rojo.

Los resultados son satisfactorios, y el filtro color rojo se encuentra en el apéndice A completo

Para analizar el filtro se describe por etapas el filtro mencionado:

1) Limpiar espacio de trabajo

2) Abrir imagen

3) Carga región en rojo, ya que es el color base y el color que se va a aislar.

4) Convertir imagen RGB a un espacio vectorial

5) Calcular parámetros a y b, los cuales fungen como delimitadores de color en el espacio vectorial.

6) Leer imagen y clasificar píxel vecino

7) Iniciar matriz de imagen tomando en cuenta parámetros a y b y calcular la distancia del espacio vectorial entre uno y otro por medio del triángulo de Pitágoras.

8) Desplegar las imágenes separadas por colores.

9) Desplegar distribución de colores.

El caso de las minucias aisladas es el color púrpura, ya que es el color con menos variación cercano al rojo.

Utilizando un software de prueba, el Neopaint, se determinó que la extracción de minucias se realiza de forma satisfactoria filtrando el color magenta, el color magenta es el color que sigue al púrpura en el filtro anterior.

Esta comparación de filtros llevó a probar el filtro de color de las minucias en diversas huellas digitales y para probar su validez se utilizó una imagen con grandes cantidades de color, demostrando su validez y robustez, para observar el código y resultados obtenidos referirse al apéndice B.

A continuación se muestra una imagen con un excesivo nivel de ruido.

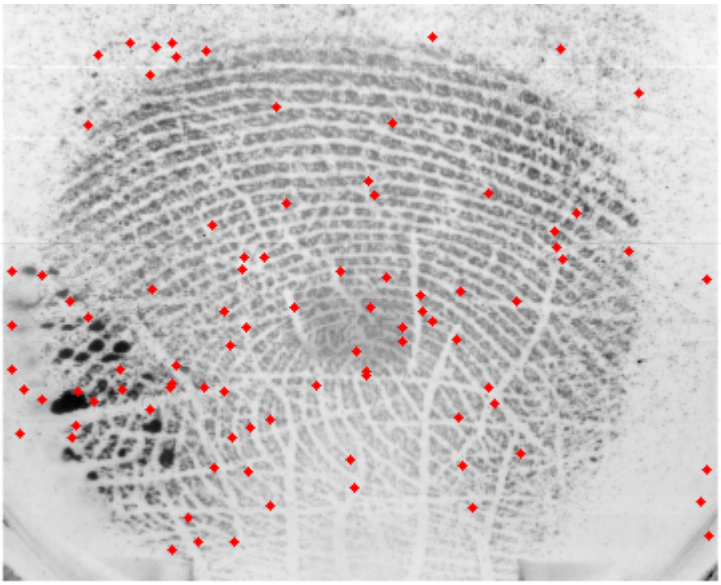


Figura 5.23 Índice derecho con exceso de ruido.

En la figura anterior se puede apreciar un exceso en la cantidad de ruido, principalmente en la zona inferior izquierda, donde hay regiones negras más grandes que las marcadas por las minucias presentes, minucias detectadas fuera del área comprendida por la huella impresa y un muy bajo contraste entre los valles y crestas, que hacen difícil la identificación de minucias.

Al utilizar esta imagen para separar las minucias se observó el siguiente resultado:

Minucias aisladas

Figura 5.24 Resultado de aplicar filtro de colores a una imagen excesivamente ruidosa.

Como se observa en la figura anterior, el filtro no logra determinar las minucias. El filtro propuesto no logró identificar las minucias en una toma con exceso de ruido.

El método propuesto es un método que pretende ser infalible a la mayoría de los ataques por ruido, por lo que este método, si bien puede

ser aceptable para muchas otras aplicaciones, éste no es el caso, para observar el proceso completo referirse al apéndice C.

Este filtro no funcionó totalmente porque está basado en el proceso de cuantización de una imagen, que tiene como objeto reducir el número de colores diferentes que se emplean en una imagen. Una de las familias de métodos de cuantización es aquella en la que se basa en dividir el espacio de color de la imagen en un determinado número de segmentos en función del número de colores diferentes que se desea conseguir. Es decir, hay que dividir más el espacio de la imagen en las zonas en que ocurra una variación mayor de color.

A grandes rasgos el proceso de cuantización consta de las siguientes etapas:

Obtener los segmentos de color representativos de la imagen original

Calcular la paleta de colores

Generar la imagen cuantizada

Para obtener los segmentos de color representativos de la imagen original, para cada uno de los pixeles de la imagen, Insertar el valor de cada color en el vector ordenado por color correspondiente

Inicialmente el número de segmentos será tres, uno para cada color, que se corresponden con los tres vectores ordenados y,

Mientras((n_segmentos_R*n_segmentos_G*n_segmentos_B) <_colores))

Dividir el segmento con mas variabilidad en dos segmentos y así sucesivamente.

Para calcular la paleta de colores es necesario calcular el valor medio correspondiente y, finalmente, para generar la imagen cuantizada y también para cada píxel de la imagen original hay buscar que el valor de la paleta equivalente para cada color y posteriormente substituir el valor de cada color por su equivalente de la paleta.

Suponiendo una imagen de tan sólo tres colores, para cada píxel se tiene que buscar a que valor de la paleta equivale cada uno de los tres valores del color de la imagen original, para ello se utiliza el campo media (promedio calculado anteriormente). El campo media es el valor representante del color correspondiente para cada segmento de la paleta [59].

Un criterio sencillo para adjudicar su valor equivalente en la paleta puede ser el siguiente:

Para cada color

Para cada segmento

-si el valor del color del píxel de la imagen original es <= valor medio, se adjudica el valor medio de ese segmento como valor del color en la imagen cuantizada

-si no, se pasa a comprobar el valor medio del siguiente segmento [60]

5.5 Transformación a escala de grises

A continuación se propone transformar la imagen a color a una imagen en escala de grises, la imagen a color es una matriz que varía su composición en tres matrices, cada una con valores de 0 a 256.

En una imagen en escala de grises la imagen se compone únicamente de una sola matriz, que van desde el valor mínimo (0) hasta el valor máximo (255).

La transformación de una imagen de 8 bits de profundidad en formato RGB, es decir a color, como las imágenes provenientes del lector de huellas digitales se lleva a cabo mediante una función establecida en MATLAB, que cumple con el estándar NTSC.

La función está basada en la luminiscencia monocromática y aplica una serie de coeficientes referentes a la sensibilidad del ojo respecto a los colores RGB(Red, Green, Blue) rojo, verde y azul.

La función es:

```
I = .2989*rgb_img(:,:,1)...
   +.5870*rgb_img(:,:,2)...
   +.1140*rgb_img(:,:,3)
```

.....(36)

Y devuelve como resultado la matriz I, que ahora es una matriz en cuyos renglones y columnas se encuentra la intensidad de diferentes tonos de gris [61].

Imagen en escala de grises

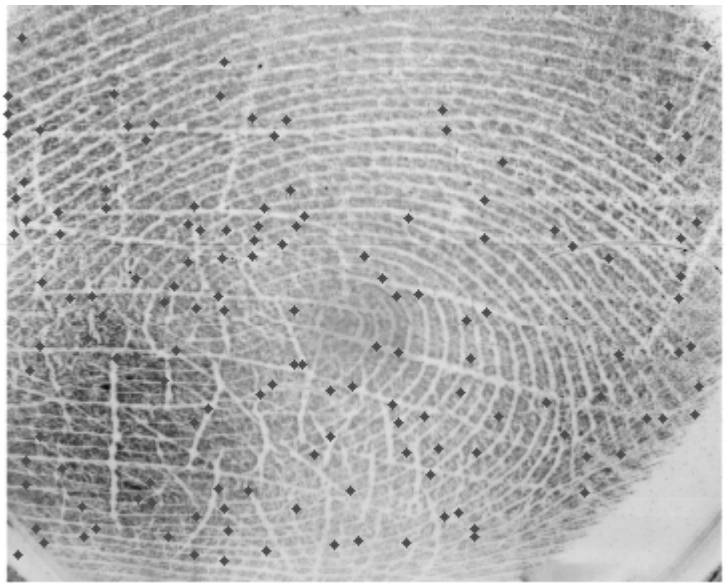


Figura 5.25 Huella digital en escala de grises.

Con esta transformación la imagen se limita a estar comprendida en un parámetro, es decir, en una matriz entre 0 y 256. Analizando la imagen con la herramienta image viewer de MATLAB, se logró determinar la intensidad de gris que corresponde a las minucias.

Esta intensidad es 76. Con esta intensidad detectada, ahora se implementará un filtro tal, que sólo permita el paso de la intensidad 76. Explorando las características de las funciones del toolbox referente al procesamiento de imágenes, la función roicolor cumple con esta función.

La razón por la cual roicolor satisface las necesidades es porque es un filtro paso-banda, implementado para procesamiento de imágenes. Recordando el concepto de filtro paso-banda es aquel que permite sólo el paso de un intervalo de frecuencias y atenúa el paso del resto [62].

La fórmula de un filtro paso-banda lo describe con gran claridad como se muestra a continuación [63]:

$$H(W) = \begin{cases} 1 & W_a \leq |W| \leq W_b \\ 0 & |W| \langle W_a \quad \acute{o} \quad |W| \rangle W_b \end{cases} \quad \text{.....(37)}$$

Donde W es la frecuencia central, Wa es la frecuencia de corte menor y Wb es la frecuencia de corte mayor.

La función roicolor tiene los siguientes parámetros:

Roicolor (imagen, Wa, Wb)

Para los propósitos que se persiguen en este trabajo, Wa= 75 y Wb=77, para que la frecuencia central sea 76, que es el valor correspondiente a las minucias dentro de la imagen.

```
BW = roicolor (I, 75,77);

figure(3),imshow(~BW),title('Minucias extraidas');
```

Y se obtienen los siguientes resultados:

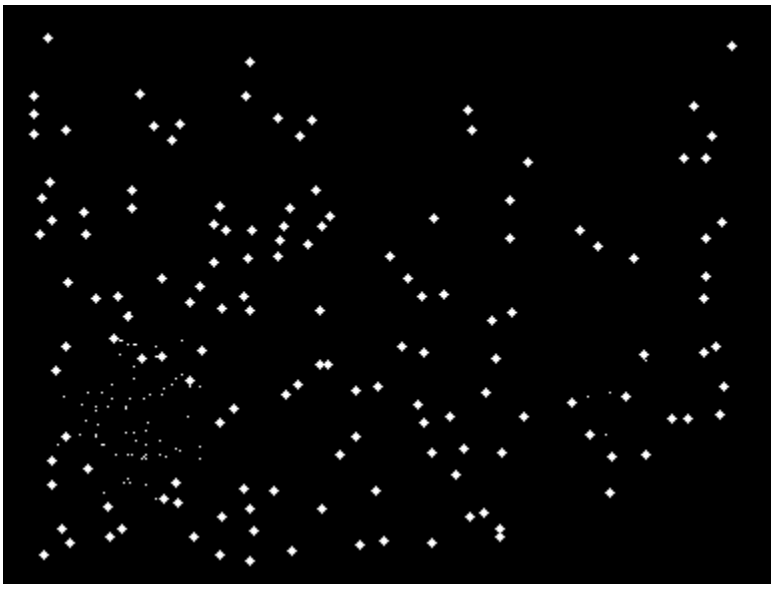


Figura 5.26 Minucias extraídas con roicolor.

5.6 Selección de Minucias

Como es posible apreciar en la imagen, el nivel de ruido está presente de una forma tal, en la que las minucias son filtradas, mas sin embargo también son incluidas pequeñas regiones del tamaño de un píxel o dos, que generan un error al permitirles el paso.

Tampoco se ha solucionado el problema de minucias que estén fuera del área de captura de la huella digital, esto es, que solamente se han filtrado exitosamente las minucias y, como resultado de ese proceso han sido incluidas en la imagen pequeños pixeles de ruido.

El proceso de selección de minucias reales, confiables, certeras y únicas propuesto es mediante la creación de una ventana interactiva, donde se puedan seleccionar una agrupación de pixeles.

El proceso de seleccionar la agrupación de pixeles permite tener la confianza de que se están seleccionando minucias y con eso se discrimina el ruido proveniente del filtrado anterior.

Otra ventaja de esta ventana interactiva es eliminar esas minucias que no están en el área dentro de la huella digital capturada, así como minucias detectadas por el lector debido a la suciedad en los procesos de adquisición de datos.

Con el método de extraer minucias, con que se cumpla un 30% de coincidencias se garantiza con un 99.999% de probabilidad la identidad del individuo; es por eso que, al aumentar las minucias reales y sin ruido, la imagen a procesar es totalmente pura, con lo que de 90 minucias detectadas en un comienzo, si quedan 70 es una muy buena cantidad de referencia, ya que sólo se necesitan alrededor de 20 minucias coincidentes para determinar la identidad.

En caso de seguir trabajando con ruido y minucias no totalmente identificables lo que sucede es que se necesitan mas puntos coincidentes, y si la mayoría es ruido o minucias no válidas la identificación no se podrá dar de manera adecuada.

La creación de la ventana interactiva se realizó en MATLAB, y se utilizó la función bwselect, la cual hace un análisis de vecindad de los pixeles.

La función bwselect requiere de un parámetro, el cual especifica cuantos pixeles contrarios debe haber alrededor del punto seleccionado; es con esto que si se da click en una región donde no hay punto, éste no

es marcado y no se toma encuentra para el análisis siguiente. Aumentando la seguridad y confiabilidad del sistema.

La ventana interactiva se caracteriza porque al mostrarse la imagen de las minucias extraídas, cambia el cursor a una forma de cruz, lo que indica que es posible seleccionar las minucias. Otra ventaja evidente es que se puede maximizar y minimizar el tamaño de la ventana para una mejor utilización, así como tener la imagen original para poder discriminar las minucias no realmente útiles.

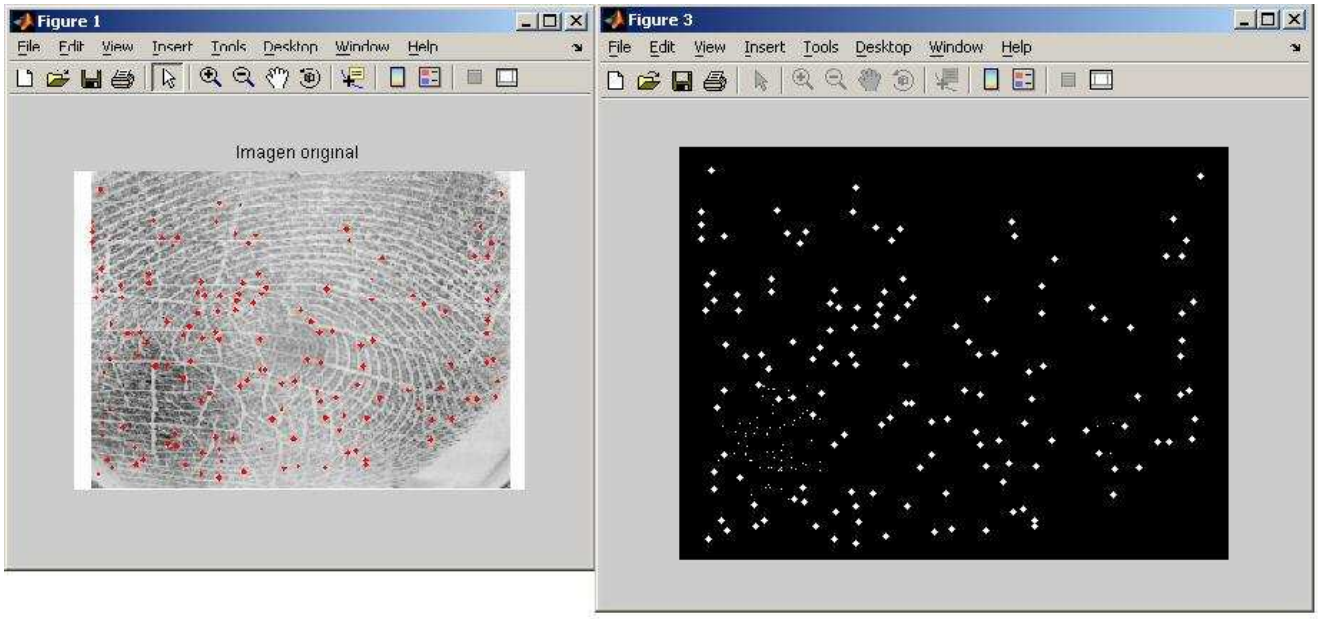


Figura 5.27 Ejemplo de utilización de ventana interactiva.

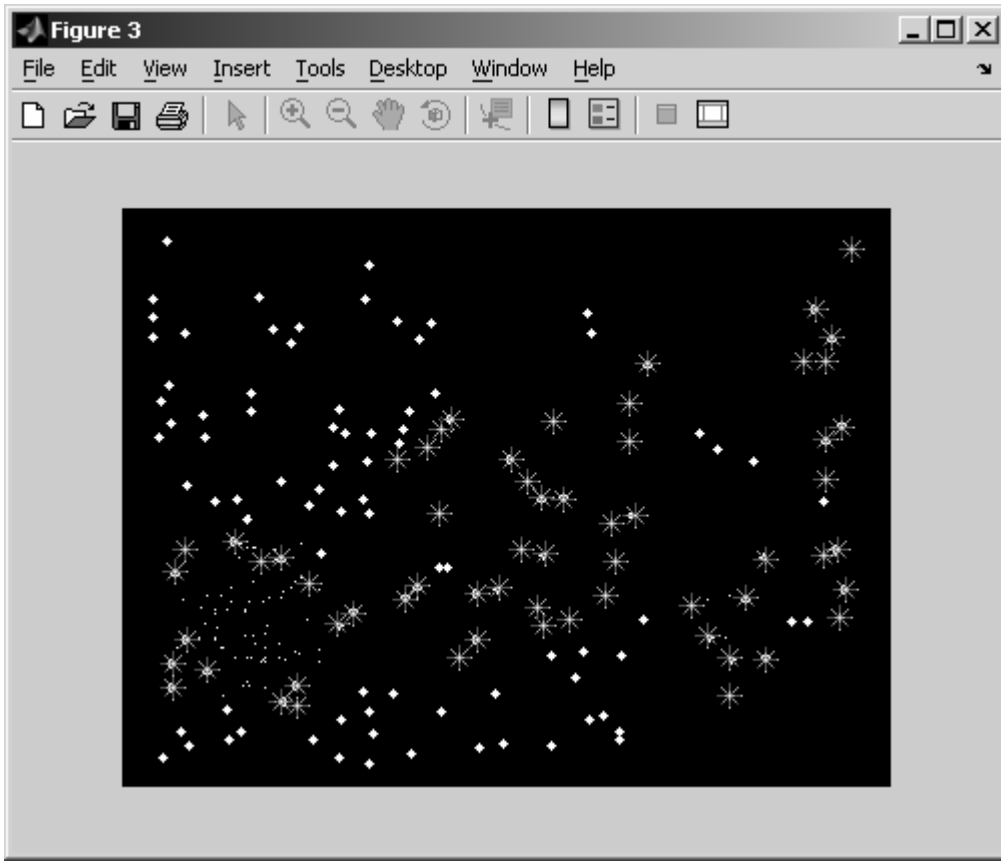


Figura 5.28.Selección de minucias realmente con información vital y trascendente.

Como se puede apreciar en la figura anterior, los puntos marcados se distinguen de los otros con un asterisco, si por alguna razón se quisiera borrar un punto, solo hay que dar click en la tecla “backspace” para ir borrando punto a punto sin perder el proceso de selección que ya se había hecho.

La selección es filtrada y se obtienen los siguientes resultados:

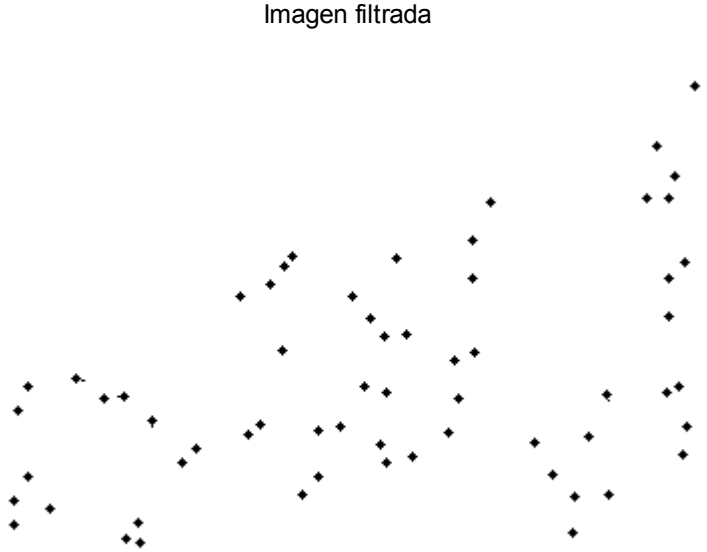


Figura 5.29 Minucias extraídas de ventana interactiva.

5.7 Generación de código único

Después de la extracción satisfactoria de minucias, se vuelve indispensable generar un código único que identifique a la huella digital una de otra, la generalidad de la extracción de minucias, su certeza y su seguridad se ven complementadas con un código que aumenta la robustez.

Las minucias son vistas como una nube de puntos en el espacio, donde se tiene el punto y su coordenada espacial, es necesario entonces un código que una todos estos puntos y los represente de manera única.

Si se toma como ejemplo los gráficos 3D provenientes de objetos del mundo real, un objeto es sectorizado uniendo puntos espaciales, si la superficie no tiene cambios los triángulos son más grandes y si la

profundidad varía los triángulos son más pequeños. Este concepto se conoce como triangulación.

La triangulación en el caso de dos dimensiones puede llevarse a cabo simplemente uniendo todos los puntos; pero esto no es único y no representa a la imagen, no hay ningún criterio de rechazo o aceptación.

Por eso se propone una triangulación especial, una triangulación capaz de identificar de una única forma a la nube de puntos conocido como minucias.

La triangulación propuesta es la triangulación de Delaunay, Se le denomina así por el matemático ruso Boris Nikolaevich Delone (Борис Николаевич Делоне, 1890 - 1980) quien lo inventó en 1934 [1]; el mismo Delone usó la forma francesa de su apellido, «Delaunay», como apreciación a sus antecesores franceses.

Una triangulación de Delaunay es una red de triángulos que cumple la condición de Delaunay. Esta condición dice que la circunferencia circunscrita de cada triángulo de la red no debe contener ningún vértice de otro triángulo.

5.8 Condición de Delaunay

La circunferencia circunscrita de un triángulo es la circunferencia que contiene los tres vértices del triángulo.

Según la definición de Delaunay la circunferencia circunscrita es vacía, si no contiene otros vértices aparte de los tres que la definen.

La condición de Delaunay dice que una red de triángulos es una triangulación de Delaunay si todas las circunferencias circunscritas de todos los triángulos de la red son vacías. Esa es la definición original para espacios bidimensionales. Es posible ampliarla para espacios tridimensionales usando la esfera circunscrita en vez de la circunferencia circunscrita. También es posible ampliarla para espacios con más dimensiones pero no se usa en la práctica.

Esa condición asegura que los ángulos del interior de los triángulos son lo más grandes posible. Es decir, maximiza la extensión del ángulo más pequeño de la red [65].

La triangulación de Delaunay tiene las siguientes propiedades:

- La triangulación forma la envolvente convexa del conjunto de puntos.
- El ángulo mínimo dentro de todos los triángulos está maximizado.
- La triangulación es unívoca si en ningún borde de circunferencia circunscrita hay más que tres vértices.

Gráficamente se presenta el siguiente caso de flipping(invertir).

Contemplando dos triángulos ABD y BCD con la arista común BD

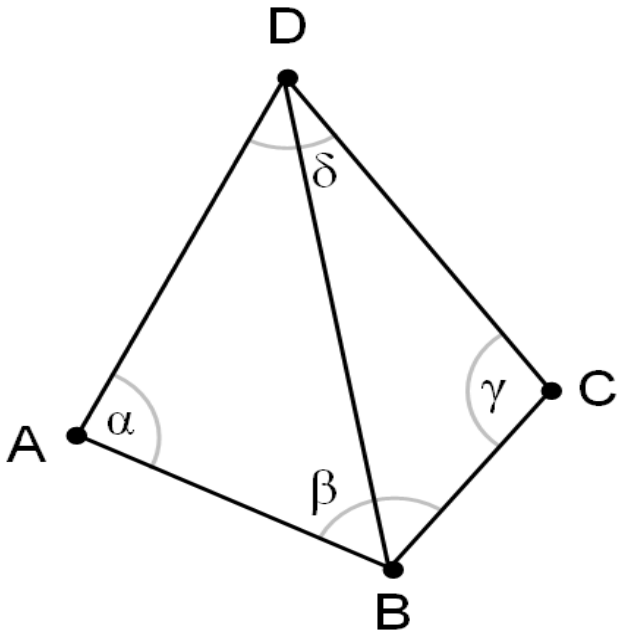


Figura 5.30 Triangulo para ejemplo gráfico.

Si la suma de los ángulos α y γ es menor o igual a 180°, los triángulos cumplen la condición de Delaunay.

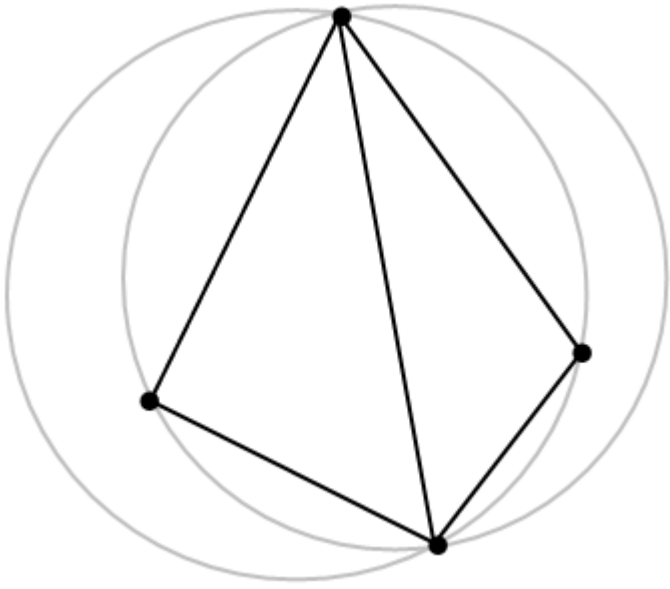


Figura 5.31. Triangulación que no cumple la condición de Delaunay.

En caso que esta situación se presente, si los dos triángulos no cumplen la condición de Delaunay, reemplazando la arista común BD por la arista común AC produce una triangulación de Delaunay, como se muestra a continuación.

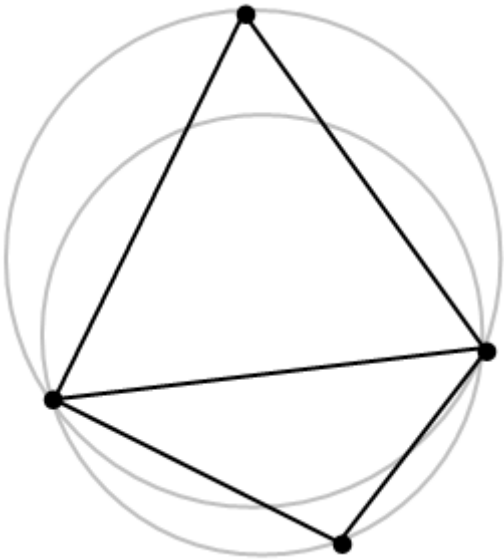


Figura 5.32. Cambio de arista que cumple la condición de Delaunay.

5.9 Cálculo de la triangulación de Delaunay

Hay varios métodos para el cálculo de la triangulación de Delaunay, se pueden clasificar en dos grandes métodos: método del intercambio de aristas y al segundo método de la envolvente convexa 3D.

5.9.1 Método del intercambio de aristas

La triangulación de Delaunay es más comprensible si previamente se menciona el método o algoritmo de Graham para resolver una triangulación única.

El algoritmo consta de dos fases. En la primera se ordenan los puntos angularmente alrededor de un punto interior al cierre convexo. Para hallar un punto interior al cierre convexo basta tomar el baricentro de tres de los puntos dados que no estén alineados. El ordenamiento es una tarea habitual en algorítmica que se repite un gran número de veces. Por eso se han desarrollado buenos algoritmos para hacerlo. En este caso, a pesar de que se trata de un ordenamiento angular, no es preciso recurrir a funciones trigonométricas (que complicarían el cálculo efectivo). Para ordenar la lista basta emplear como función básica el área signada.

En la segunda se suprimen de la lista ordenada los puntos que no son vértices del cierre convexo. Para ello se hace un recorrido de la lista (conocido como el scan de Graham) en el que, de nuevo, se emplean áreas signadas para decidir si un punto debe ser eliminado o no. Si los puntos están ordenados en sentido antihorario, el área signada de los puntos Pi-1, Pi, Pi+1 permite decir si el punto Pi debe ser eliminado. En efecto, si el área no es positiva, el punto Pi es interior al triángulo Pi-1, O, Pi+1, donde O es el centro del ordenamiento, y, por tanto, interior al cierre convexo. En este caso debe ser eliminado.

Para que esta segunda fase proporcione la lista correcta de vértices del cierre convexo es preciso incluir un detalle más: cada vez que se elimine un punto de la lista, se debe dar un paso atrás en el recorrido, ya que al eliminar un punto puede suceder que los tres que pasan a ser consecutivos den lugar a un área signada no positiva, en cuyo caso habría que eliminar el punto intermedio de nuevo.

Este algoritmo realiza solo tres operaciones básicas: comparaciones de números, sumas y productos. Además, el número total de estas operaciones que se realizan es de orden O(n log n).

Habiendo planteado de manera general el método de Graham se procede con el *método de intercambio de aristas*.

El método consta de dos pasos:

-Primer paso: hallar una triangulación cualquiera del conjunto de puntos.
-Segundo paso: modificar la triangulación mejorándola sucesivamente hasta obtener la triangulación de Delaunay.

El algoritmo de Graham proporciona, sin costo adicional, una triangulación de los puntos además del cierre convexo. Para ello basta con dos ligeras modificaciones: La primera consiste en elegir un punto cualquiera del conjunto de puntos de entrada como punto para ordenar angularmente los puntos. El punto puede ser el primero de la lista y podemos incluirlo en la lista final ordenada en primer lugar. La segunda modificación consiste en crear una lista de triángulos, que contendrá los triángulos de la triangulación, en la que se incluirán los siguientes triángulos: De momento todos los triángulos P1, Pi, Pi+1, para i desde 2 hasta n (entendiendo los índices módulo n). Además, durante el proceso del escaneo de Graham, se añadirán en la lista los triángulos Pi-1, Pi, Pi+1 cada vez que se elimine el punto Pi debido a que dicho punto resulta interior.

La lista de triángulos resultante es una triangulación del conjunto de puntos. Como vemos, la complejidad, en términos de su orden de magnitud, no aumenta respecto del algoritmo de Graham. Sigue siendo O(n log n).

El segundo paso consta en tratar de revisar las aristas (segmentos) de la triangulación una a una, todas las veces que sea necesario, hasta que no quede ninguna ilegal.

Una arista de la triangulación, si no es de la envolvente convexa, separa dos triángulos de la triangulación. Si esos dos triángulos forman un cuadrilátero convexo, la arista será una de sus dos diagonales. En estas circunstancias se dice que la arista es ilegal si el círculo circunscrito a uno de los dos triángulos que separa la arista contiene en su interior por completo al otro triángulo.

Cualquier otra arista se conoce con el nombre de legal. Legalizar una arista ilegal consiste en sustituirla por la otra diagonal del cuadrilátero descrito. Es claro que, salvo que los cuatro vértices del cuadrilátero sean concíclicos, de las dos diagonales de dichos cuadriláteros convexos siempre habrá una que será arista legal y otra ilegal.

Tampoco resulta difícil observar que al legalizar una arista, cambiando los dos triángulos correspondientes por los nuevos que se generan, se obtiene una triangulación con un vector de ángulos mayor, y, por lo tanto una mejor triangulación.

En consecuencia, partiendo de una triangulación cualquiera y legalizando una a una las aristas ilegales, se llega necesariamente al máximo vector de ángulos y su correspondiente triangulación: la triangulación de Delaunay.

Para la validez del algoritmo así como para analizar su complejidad es importante observar que el proceso de mejora no lleva a bucles que podrían hacer que el proceso no termine. En efecto, cada legalización de una arista ilegal significa una mejora estricta de la triangulación, o, lo que es lo mismo, a un vector de ángulos estrictamente mayor respecto del orden correspondiente. En consecuencia el proceso termina

necesariamente en un número finito de pasos y necesariamente encontrando la mejor de las triangulaciones, la de Delaunay.

La complejidad en el peor caso es $O(n^2)$, ya que puede suceder que exista solo una arista legal en la triangulación de partida que nos exija revisar todas las aristas para encontrarla y que genere otra arista ilegal única al legalizarla para la que de nuevo es necesario revisar la lista completa de arista de nuevo. Este suceso se puede repetir tantas veces como número de aristas interiores tiene la triangulación, que son siempre una cantidad lineal. A pesar de ello, y de que existen algoritmos que calculan la triangulación de Delaunay con O(n log n) operaciones, el algoritmo descrito es muy recomendable por su sencillez, lo que conlleva un código de programación sencillo y robusto, y porque en general la complejidad es O(n log n) y no $O(n^2)$ como la del peor caso.

5.9.2 Método del cierre convexo en 3D

En este caso, es un método ampliamente estudiado en geometría computacional debido a su importante uso en volver objetos reales en tercera dimensión, utilizando una malla de triángulos.

Existen muy buenos algoritmos para calcular el cierre convexo de puntos en 3D. Teniendo éstos resultados con él se puede calcular la triangulación de Delaunay de un conjunto de puntos del plano.

En efecto, si se amplían las coordenadas (x; y) de cada uno de los puntos dados del plano con una tercera coordenada (x; y; x2 + y2), se han transformado los puntos en puntos del espacio situados sobre el paraboloide z = x2 + y2. Con ello es posible conseguir que todos los puntos estén en posición convexa (todos forman parte de la envolvente convexa). Además, y lo que es más interesante, cada triángulo de la

envolvente inferior del cierre convexo determina un plano que deja todos los demás puntos por encima de él y que corta al paraboloide en una elipse que se proyecta en el plano XY en una circunferencia circunscrita a los puntos proyectados de los vértices del triángulo. El hecho de que los demás puntos estén por encima del plano, equivale a que la circunferencia proyección de la elipse no contenga a ningún punto de los de partida. Esta condición caracteriza los triángulos de la triangulación de Delaunay: tres puntos de un conjunto de puntos del plano son los vértices de un triángulo en la triangulación de Delaunay si, y sólo si, el círculo circunscrito no contiene a ningún punto del conjunto en su interior (aquí se supone que no hay cuatro puntos concíclicos entre los dados).

En consecuencia, las observaciones anteriores llevan al siguiente resultado:

La proyección de la envolvente convexa inferior de los puntos (xi; yi; x2i + y2i) sobre el plano XY es la triangulación de Delaunay de los puntos

(xi; yi); i = 1; _ _ _ ; n.

En resumen, si se cuenta con un algoritmo para calcular cierres convexos en 3D, se tiene además un algoritmo para calcular triangulaciones de Delaunay en el plano.

El cálculo de triangulaciones de Delaunay no viene incluido en ninguna librería de MATLAB, es por eso que se necesita agregar desde las librerías, hasta el código y variables locales y globales.

Existen diversos algoritmos para el cálculo de la triangulación de Delaunay, y para su funcionamiento en MATLAB, deben estar escritos en C, manejar diversos tipos de datos, variables dobles y flotantes y ser compatibles con el lenguaje de scripts de MATLAB.

El código utilizado se obtuvo de qhull, descargándolo de la página principal [66], se realiza la instalación de forma automática.

El proceso de cálculo de la triangulación de Delaunay se lleva a cabo mediante la obtención del determinante de una matriz. En dos dimensiones, que es el caso de estudio, sean los puntos A,B y C los vértices de un triángulo denotados en sentido contrario a las manecillas del reloj, el punto D está dentro de su circunferencia circunscrita si se cumple que:

$$\begin{vmatrix} A_x & A_y & A_x^2+A_y^2 & 1 \\ B_x & B_y & B_x^2+B_y^2 & 1 \\ C_x & C_y & C_x^2+C_y^2 & 1 \\ D_x & D_y & D_x^2+D_y^2 & 1 \end{vmatrix} = \begin{vmatrix} A_x-D_x & A_y-D_y & (A_x-D_x)^2+(A_y-D_y)^2 \\ B_x-D_x & B_y-D_y & (B_x-D_x)^2+(B_y-D_y)^2 \\ C_x-D_x & C_y-D_y & (C_x-D_x)^2+(C_y-D_y)^2 \end{vmatrix} > 0 \quad \text{.....(37)}$$

Es decir, si el determinante de esta matriz es mayor que 0. En este caso es suficiente conocer el signo aritmético, así que este cómputo puede ser acelerado fácilmente [67].

Entonces, generando la triangulación de Delaunay para la huella digital con las minucias extraídas se obtiene el siguiente resultado:

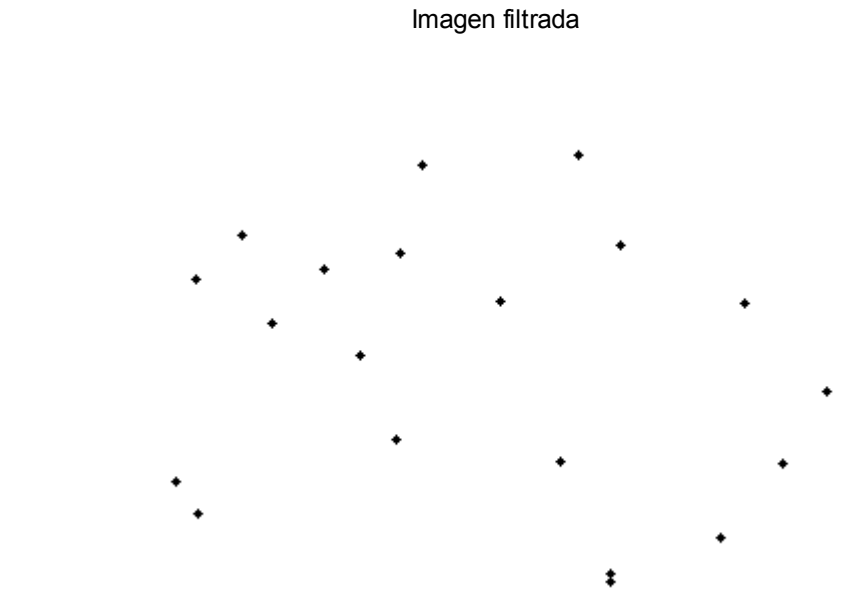


Figura 5.33 Minucias extraídas de una huella digital.

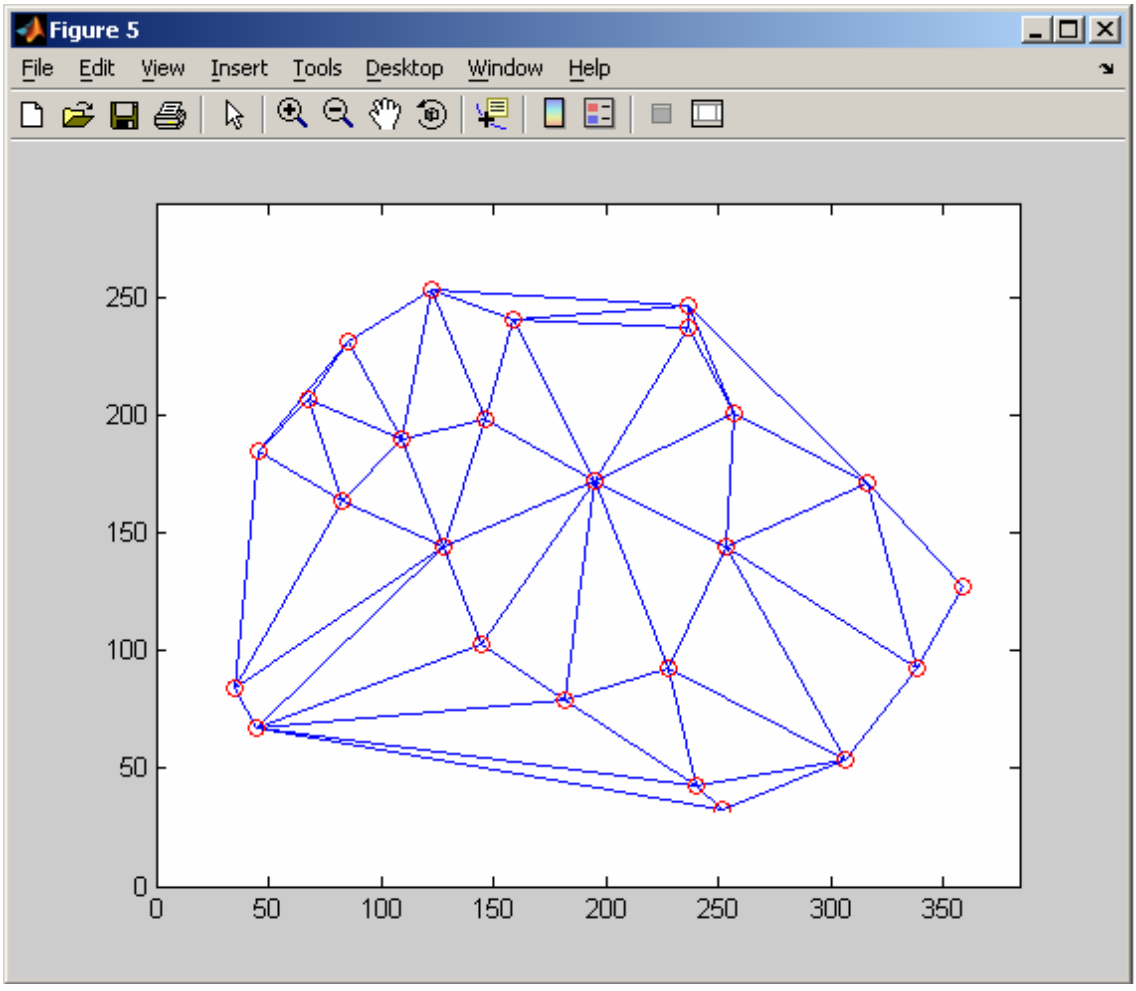


Figura 5.34 Triangulación generada con código de Delaunay

Con este código se obtiene una imagen única, con características sólidas de individualidad, de solidez, de firmeza y de confiabilidad, que viene a dar soporte a una tecnología en busca de seguridad absoluta y confianza total en la identificación de individuos basados en características únicas que poseemos todos; las huellas digitales.

Este código es único, ocupa el mínimo de espacio, es inviolable, tiene el antecedente de provenir de puntos seleccionados con un margen de error nulo, no están presentes cálculos redundantes y no hay posibilidad de incluir puntos que no sean minucias.

Es por eso que este sistema propuesto brinda las características necesarias para ser un sistema utilizable en el corto mediano y largo plazo en procesos de seguridad civil, de gobierno y de investigación.

Capítulo VI. Conclusiones y Trabajos futuros

En este último capítulo se plasman las conclusiones obtenidas después de la implementación del sistema de reconocimiento de huellas digitales.

También en este capítulo se compara uno a uno los objetivos, tanto general como específicos y se determina si se cumplieron satisfactoriamente o no.

Finalmente se sugieren diversos trabajos futuros que contengan como parte de su desarrollo el presente trabajo.

6.1 Conclusiones

Encontrar un balance entre rapidez, eficacia y economía es una labor que lleva a explorar más de una solución para un mismo problema. Es por eso que a lo largo de esta tesis se fue llevando al lector desde una visión global a un entendimiento particular y posteriormente un análisis centrado en las características de las huellas digitales.

El objetivo general de esta tesis, planteado previamente fue cubierto de una manera satisfactoria, y, como ya se mencionó el factor principal fue la parte económica ya que la única adquisición nueva fue el lector biométrico, que no es de un costo exorbitante; se recomienda la distribución de Linux Xubuntu, ya que está optimizada para computadoras a partir de arquitecturas x386 con sólo 192 Mb en memoria RAM para su instalación.

El primer objetivo específico está íntimamente ligado con el objetivo general, que es aprovechar al máximo los recursos con los que se cuenta, la implementación del método propuesto nunca rebasó la memoria RAM ni se quedó a medio cálculo por falta de localidades para los cálculos; en varios métodos explicados se consumen muchos recursos al obtener distancias relativas u orientaciones, ya que esos cálculos implican la extracción de raíces y elevación de potencias al cuadrado; motivo por el cual se diseñó el método propuesto.

El segundo objetivo específico se cumplió satisfactoriamente, permitiendo la caracterización de las huellas digitales de una manera única, utilizando la triangulación de Delaunay, lo que garantiza que el método es único, robusto y utiliza una de las técnicas mas eficientes de

la triangulación de Delaunay, situación que optimiza el código empleado y optimiza los recursos de la computadora donde se ejecuta el algoritmo.

El tercer objetivo se logró satisfactoriamente ya que la imagen es leída en MATLAB como matriz, así que la imagen puede tener la dimensión que sea y cualquier formato de los soportados por MATLAB, entre los que se encuentran los más utilizados por los diversos lectores y plataformas, como por ejemplo las imágenes con terminación .bmp, .png. .tiff, etc.

Como complemento del objetivo anterior, cualquier huella digital incluye ruido, unas en menor medida que otras, dependiendo específicamente del lector, de su falta de limpieza con el uso constante, del deterioro propio, etc. Con el método propuesto el ruido proveniente de cualquier lector es discriminado por el usuario al momento de seleccionar la agrupación correspondiente a las minucias, sin importar la calidad de la imagen o su origen; la ventana interactiva de selección funciona con todas las imágenes.

Otro balance importante dentro de este sistema es la interacción entre el método y el usuario final; tomando en cuenta la simplicidad de los entornos gráficos propuestos que permiten al usuario un acercamiento directo al sistema propuesto. Una ventaja considerable es la selección de minucias teniendo como referencia a la imagen original y a la imagen filtrada; permitiendo eliminar minucias irrelevantes y que no pertenecen al individuo por la suciedad acumulada en el lector biométrico.

Concluyendo, el sistema propuesto es dinámico, ágil, flexible, y se adapta plenamente a las diferentes etapas de todo un sistema biométrico

genérico, la propuesta de captura de huellas y extracción de minucias aquí propuesto cumple con el objetivo de la economía y la generalidad de almacenar las imágenes con las minucias extraídas. También es posible adaptarse a imágenes previamente adquiridas de otros lectores biométricos y obtener los mismos resultados.

El sistema propuesto está sustentado en pilares sólidos basados en el reconocimiento de minucias que brindan un nivel de seguridad mayor que el reconocimiento de formas de la huella dactilar y el filtro paso-banda propuesto tiene un intervalo de frecuencias claramente definidas, que, en el caso de imágenes que provengan de otro lector son fácilmente adaptables para un mejor filtrado. Dicho sistema se complementa con la ventana interactiva para la selección correcta de minucias, la cual discrimina puntos que no estén unidos. Por última observación el código generado es único y representa de una sola forma las huellas digitales con el máximo de confiabilidad e información proveniente de las huellas digitales.

Como conclusión final, el método propuesto es un método híbrido interactivo compuesto por la extracción de minucias explicada en el método de Rao; la mejora en cálculo de algoritmos de refinamiento de imagen, como en el caso de Donahue y Rokhlin, y finalmente la triangulación de Delaunay ampliamente estudiada y utilizada en diversos métodos, principalmente de reconocimiento de objetos en tercera dimensión y levantamientos topográficos.

6.2 Trabajos Futuros

Como trabajos futuros se proponen los siguientes:

1) Elaborar una base de datos que almacene la triangulación resultante como vector de comparación.

Este trabajo futuro se propone ya que la implementación de una base de datos es necesaria para el ordenamiento de la información, especialmente cuando se van a almacenar cientos o miles de individuos.

La correcta implementación de una base de datos permite que se desarrollen con mayor facilidad diversas técnicas de ordenamiento y búsqueda de la información.

Al obtener las imágenes propias de las huellas dactilares desde la plataforma Linux, también se propuso trabajar en MATLAB desde Linux, sin embargo se pueden trabajar las imágenes tanto en MATLAB instalado en Windows como en Linux. Igualmente, es posible implementar una base de datos en MATLAB o en alguna otra plataforma, como por ejemplo SQL o ACCESS de Windows.

2) Implementar un algoritmo de comparación basado únicamente en la triangulación resultante que permita la identificación y la autenticación.

Este trabajo futuro se propone como método de búsqueda óptima de entre todos los individuos almacenados previamente en la base de datos creada.

El resultado de la creación de un código único para cada huella digital se mide en la efectividad para poder almacenar la información, en este caso es mucho mejor almacenar una red de triángulos que toda una imagen con profundidad de 256 colores en un tamaño de 384x289.

También es más eficiente almacenar el par de coordenadas que se obtienen de seleccionar las minucias en la ventana interactiva y al momento de hacer la comparación efectuar la triangulación de Delaunay. Eso depende de la forma en que se efectúe la identificación y verificación del individuo; pero cualquiera que sea la forma, el fondo es el mismo: el resultado obtenido a partir del sistema planteado en esta tesis.

3) Automatizar la extracción de minucias

Este punto se propone como trabajo futuro bajo una advertencia, ya que, una forma de automatizar la extracción de minucias es ampliar la ventana del filtro paso-banda y como se observó en las imágenes con un alto nivel de ruido esta ampliación discrimina las crestas y los valles pero permite el paso a manchas ocasionadas por la grasa acumulada en la ventana del lector y también permite el paso a minucias detectadas por la librería fprint que no pertenecen al escaneo del dedo, como ya se mostró en la imagen con alto nivel de ruido.

En este punto se debe valorar con muchísimo cuidado si permitir la automatización de una forma computarizada y permitir el paso de cierto nivel de ruido; el cual afecta directamente a la imagen y reduce la confiabilidad en el sistema o si se desea continuar con la vectorización sin niveles de ruido.

Actualmente en los sistemas analizados se toma en cuenta el ruido y no es posible discriminarlo tan puramente como en el sistema propuesto.

Aún con el nivel de ruido el nivel de aceptación de un individuo es el siguiente: si se detecta un 30% de las minucias registradas en una huella digital, se tiene un 99% de confiabilidad de identificar al individuo. El promedio de minucias obtenidas en sistemas profesionales en promedio van desde los 40 hasta las 70 minucias, incluyendo el ruido.

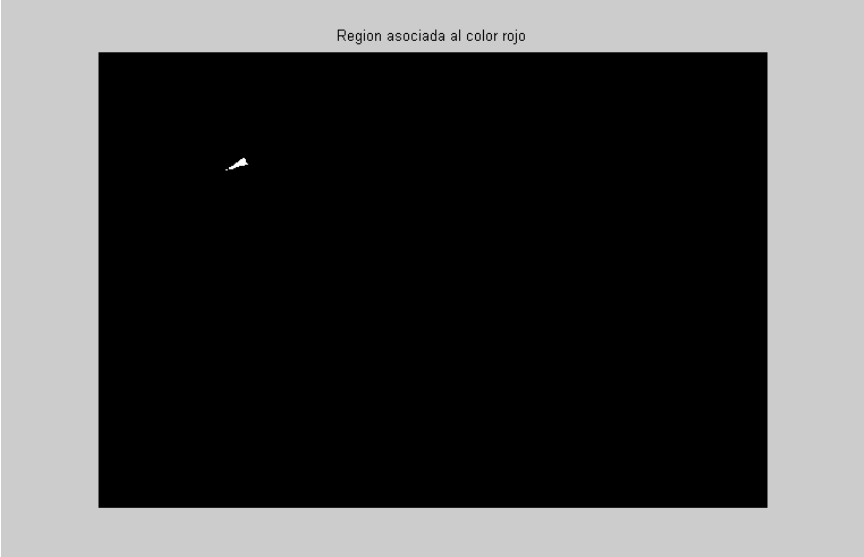
Anexo A

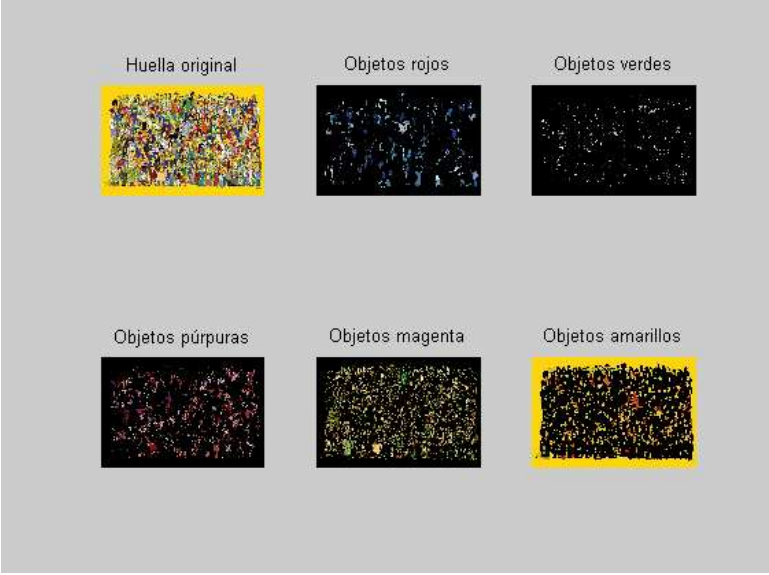
```
%Limpia todo
clear,close all

%Abre imagen
huella=imread('simpsons.jpg');
figure(1),imshow(huella),title('Huella original');

%Carga region en rojo
load regioncoordinates;
ncolors=6;
sample_regions=false([size(huella,1) size(huella,2) ncolors]);

for count=1:ncolors

sample_regions(:,:,count)=roipoly(huella,region_coordinates(:,1,count),...
                                  region_coordinates(:,2,count));

end

figure(2),imshow(sample_regions(:,:,2)),title('Region asociada al color rojo');


%Convertir imagen RGB en un espacio vectorial con makecform y applycform
cform=makecform ('srgb2lab');
lab_huella=applycform(huella,cform);

%Calculando el valor a y b para el area dada.
%a y b sirven como delimitadores de color en el espacio

a=lab_huella(:,:,2);
b=lab_huella(:,:,3);
color_markers=repmat(0,[ncolors, 2]);

for count=1:ncolors
   color_markers(count,1)=mean2(a(sample_regions(:,:,count)));
   color_markers(count,2)=mean2(b(sample_regions(:,:,count)));
end

%Clasificando cada pixel usando a su vecino
color_labels=0:ncolors-1;
%Iniciando la matriz para ser usada en el vecino inmediato

a=double(a);
b=double(b);
distance=repmat(0,[size(a), ncolors]);

for count =1:ncolors
   distance(:,:,count)=((a-color_markers(count,1)).^2+...
                        (b-color_markers(count,2)).^2).^0.5;
end

[value, label] = min(distance,[],3);
label=color_labels(label);
```

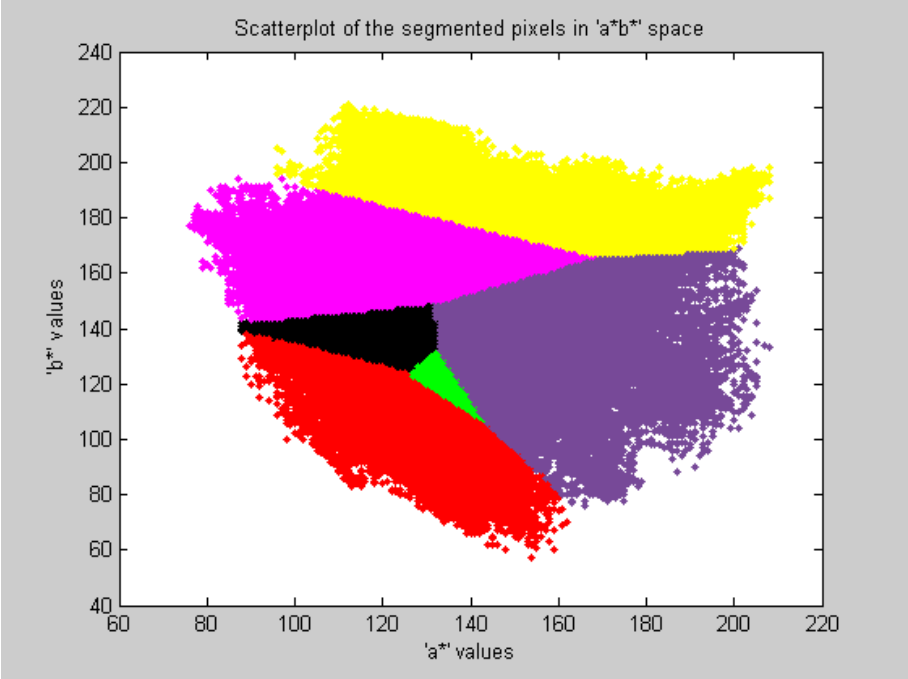
```
clear value distance;

%Desplegar las imagenes separadas

rgb_label=repmat(label,[1 1 3]);

segmented_images=repmat(uint8(0),[size(huella),ncolors]);

for count=1:ncolors
   color=huella;
   color(rgb_label ~= color_labels(count)) = 0;
   segmented_images(:,:,:,count)=color;
end

%Muestra en imagen la separacion

figure (3),title('Separación en colores');

subplot(2,3,1)
imshow(huella),title('Huella original');

subplot(2,3,2)
imshow(segmented_images(:,:,:,2)),title('Objetos rojos');

subplot(2,3,3)
imshow(segmented_images(:,:,:,3)),title('Objetos verdes');

subplot(2,3,4)
imshow(segmented_images(:,:,:,4)),title('Objetos púrpuras');

subplot(2,3,5)
imshow(segmented_images(:,:,:,5)),title('Objetos magenta');

subplot(2,3,6)
imshow(segmented_images(:,:,:,6)),title('Objetos amarillos');

%Despliegue de colores cercanos al rojo y su correspondiente distribucion
purple = [119/255 73/255 152/255];
plot_labels = {'k', 'r', 'g', purple, 'm', 'y'};

figure(4)
for count = 1:ncolors
  plot(a(label==count-1),b(label==count-1),'.','MarkerEdgeColor', ...
      plot_labels{count}, 'MarkerFaceColor', plot_labels{count});
  hold on;
end

title('Scatterplot of the segmented pixels in ''a*b*'' space');
xlabel('''a*'' values');
ylabel('''b*'' values');

figure (5),imshow(segmented_images(:,:,:,4)),title('Minucias aisladas');
```

Warning: Image is too big to fit on screen; displaying at 75% scale.
Warning: Image is too big to fit on screen; displaying at 75% scale.

Warning: Image is too big to fit on screen; displaying at 75% scale.






Scatterplot of the segmented pixels in 'a*b*' space
'b*' values
'a*' values
240
220
200
180
160
140
120
100
80
60
40
60
80
100
120
140
160
180
200
220


Minucias aisladas

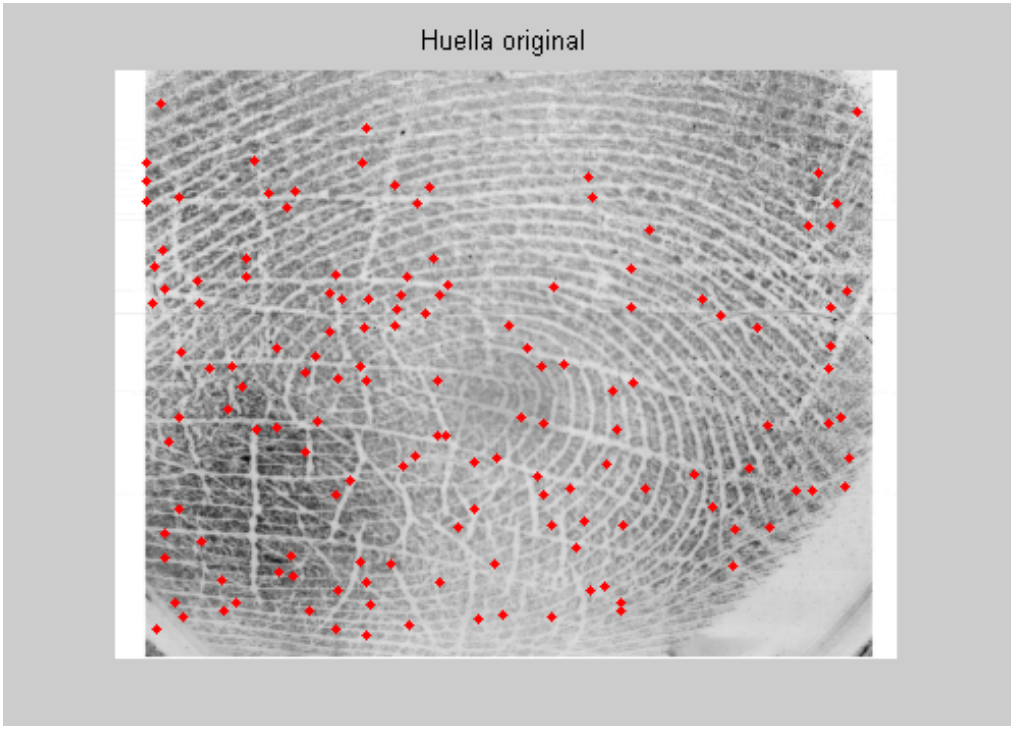
Anexo B

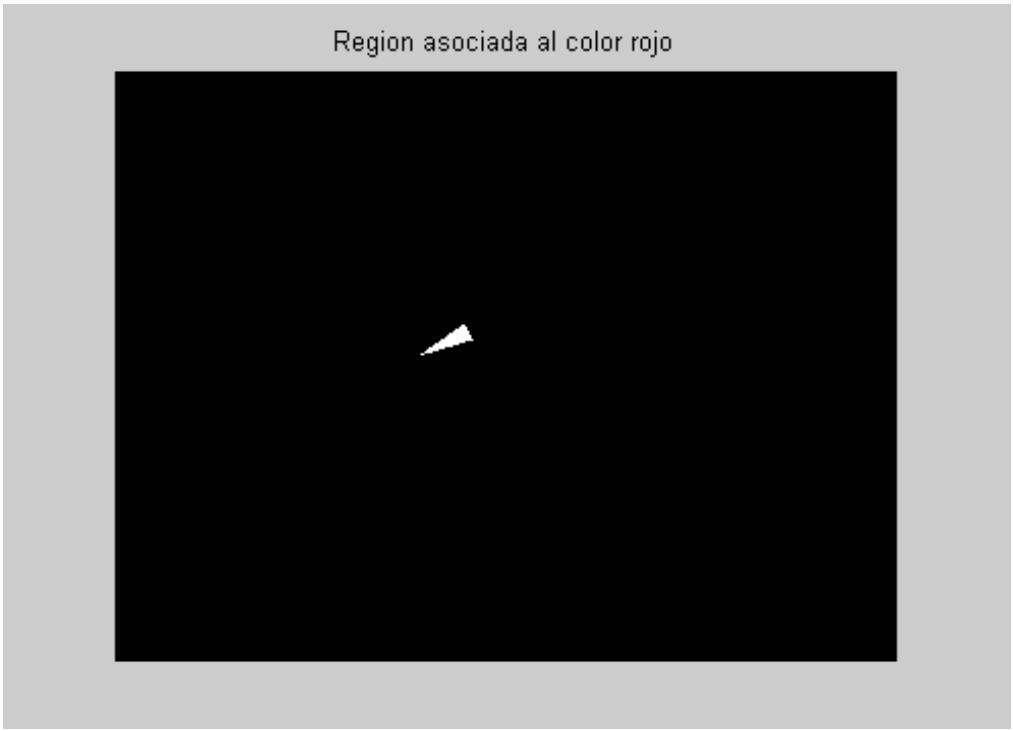
```
%Limpia el espacio de trabajo
clear,close all

%Abre imagen
huella=imread('pi.png');
figure(1),imshow(huella),title('Huella original');

%Carga region en rojo
load regioncoordinates;
ncolors=6;
sample_regions=false([size(huella,1) size(huella,2) ncolors]);

for count=1:ncolors

sample_regions(:,:,count)=roipoly(huella,region_coordinates(:,1,count),...
                                  region_coordinates(:,2,count));

end

figure(2),imshow(sample_regions(:,:,2)),title('Region asociada al color rojo');


%Convertir imagen RGB en un espacio vectorial con makecform y applycform
cform=makecform ('srgb2lab');
lab_huella=applycform(huella,cform);

%Calculando el valor a y b para el area dada.
%a y b sirven como delimitadores de color en el espacio

a=lab_huella(:,:,2);
b=lab_huella(:,:,3);
color_markers=repmat(0,[ncolors, 2]);

for count=1:ncolors
   color_markers(count,1)=mean2(a(sample_regions(:,:,count)));
   color_markers(count,2)=mean2(b(sample_regions(:,:,count)));
end

%Clasificando cada pixel usando a su vecino
color_labels=0:ncolors-1;
%Iniciando la matriz para ser usada en el vecino inmediato

a=double(a);
b=double(b);
distance=repmat(0,[size(a), ncolors]);

for count =1:ncolors
   distance(:,:,count)=((a-color_markers(count,1)).^2+...
                  (b-color_markers(count,2)).^2).^0.5;
end

[value, label] = min(distance,[],3);
```

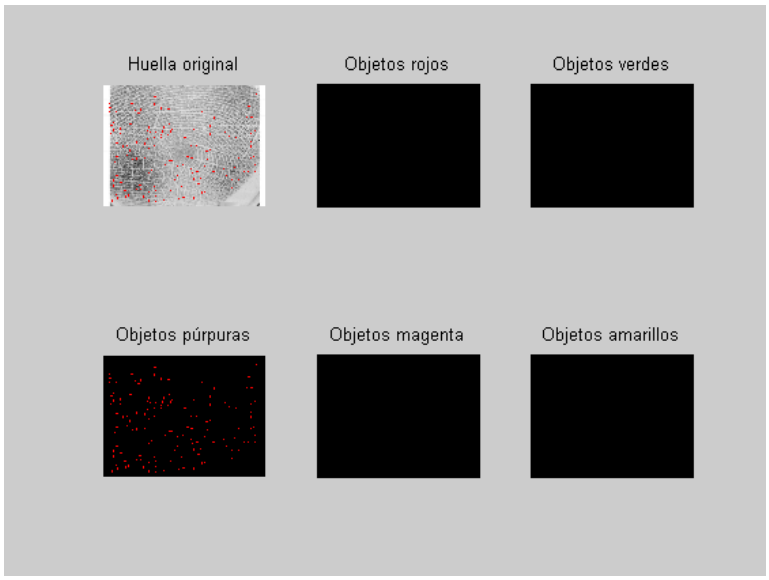
```
label=color_labels(label);
clear value distance;

%Desplegar las imagenes separadas

rgb_label=repmat(label,[1 1 3]);

segmented_images=repmat(uint8(0),[size(huella),ncolors]);

for count=1:ncolors
   color=huella;
   color(rgb_label ~= color_labels(count)) = 0;
   segmented_images(:,:,:,count)=color;
end

%Muestra en imagen la separacion

figure (3),title('Separación en colores');

subplot(2,3,1)
imshow(huella),title('Huella original');

subplot(2,3,2)
imshow(segmented_images(:,:,:,2)),title('Objetos rojos');

subplot(2,3,3)
imshow(segmented_images(:,:,:,3)),title('Objetos verdes');

subplot(2,3,4)
imshow(segmented_images(:,:,:,4)),title('Objetos púrpuras');

subplot(2,3,5)
imshow(segmented_images(:,:,:,5)),title('Objetos magenta');

subplot(2,3,6)
imshow(segmented_images(:,:,:,6)),title('Objetos amarillos');

%Despliegue de colores cercanos al rojo y su correspondiente distribucion
purple = [119/255 73/255 152/255];
plot_labels = {'k', 'r', 'g', purple, 'm', 'y'};

figure(4)

title('Scatterplot of the segmented pixels in "a*b*" space');
xlabel('"a*" values');
ylabel('"b*" values');

for count = 1:ncolors
  plot(a(label==count-1),b(label==count-1),'.','MarkerEdgeColor', ...
       plot_labels{count}, 'MarkerFaceColor', plot_labels{count});
  hold on;
end
```

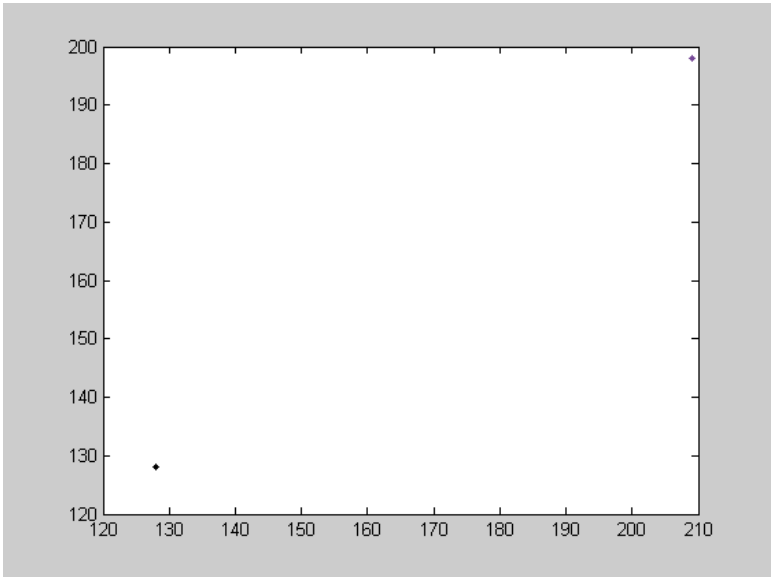
```
figure (5),imshow(segmented_images(:,:,:,4)),title('Minucias aisladas');
```

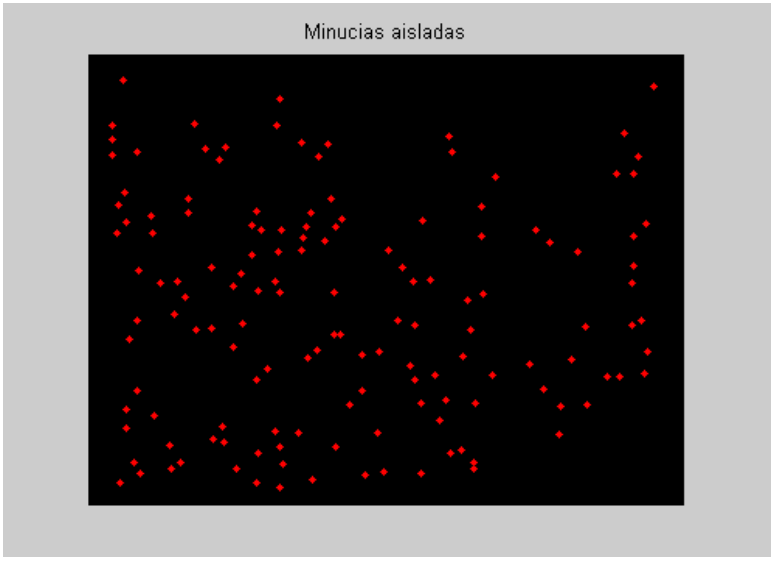
Warning: Divide by zero.
Warning: Divide by zero.
Warning: Divide by zero.
Warning: Divide by zero.






Huella original
Objetos rojos
Objetos verdes
Objetos púrpuras
Objetos magenta
Objetos amarillos


200
190
180
170
160
150
140
130
120
120
130
140
150
160
170
180
190
200
210


Minucias aisladas

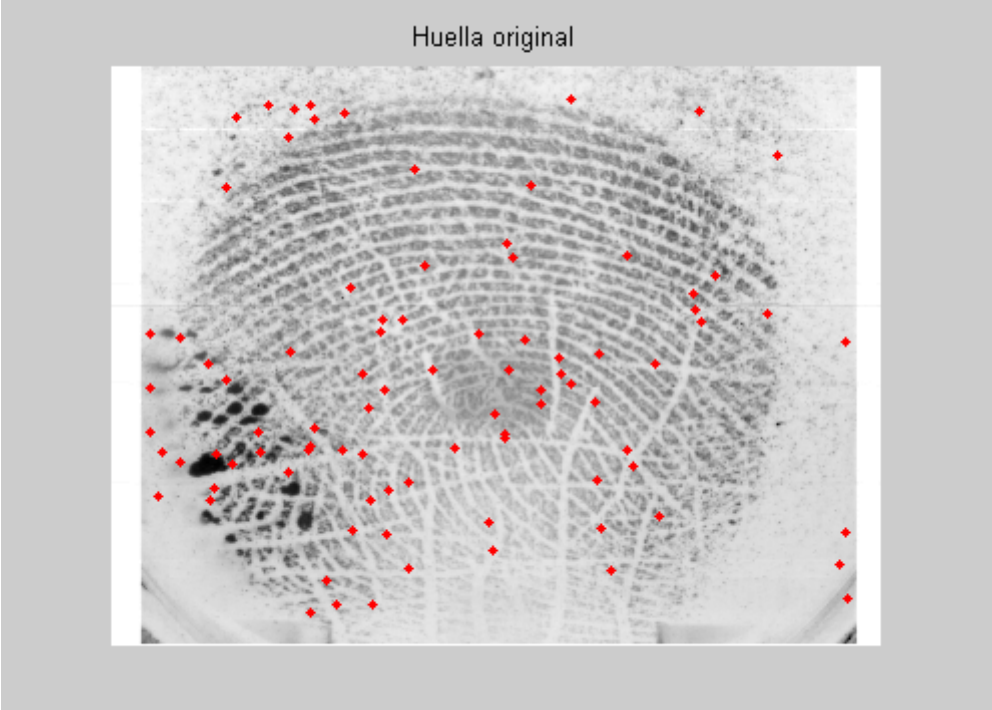
Anexo C

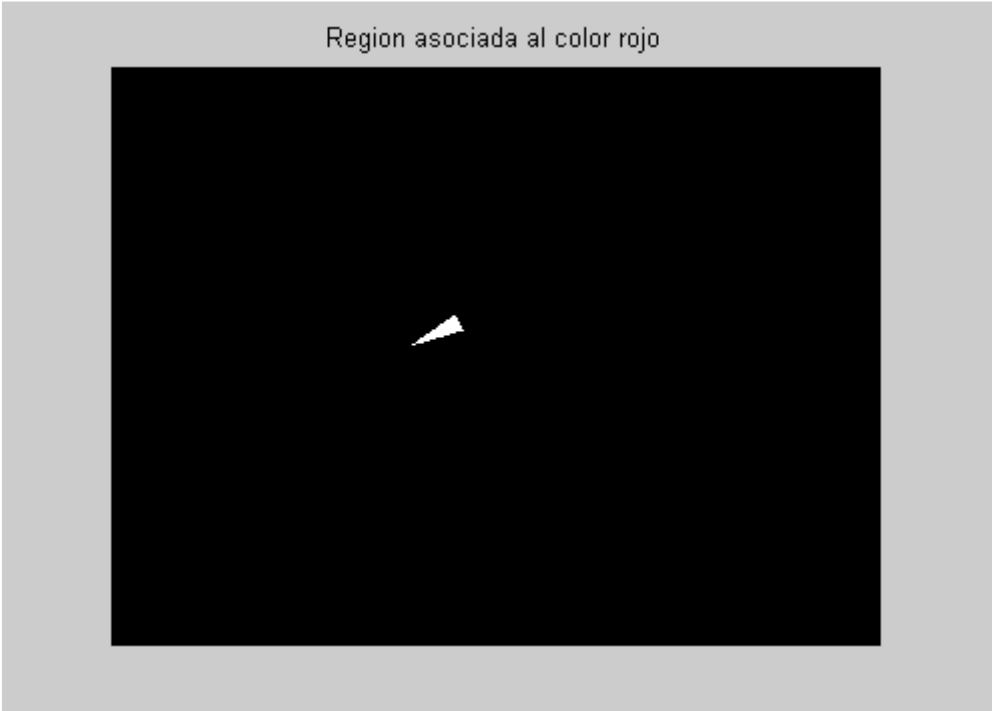
```
%Limpia todo
clear,close all

%Abre imagen
huella=imread('id.png');
figure(1),imshow(huella),title('Huella original');

%Carga region en rojo
load regioncoordinates;
ncolors=6;
sample_regions=false([size(huella,1) size(huella,2) ncolors]);

for count=1:ncolors

sample_regions(:,:,count)=roipoly(huella,region_coordinates(:,1,count),...
                                  region_coordinates(:,2,count));

end

figure(2),imshow(sample_regions(:,:,2)),title('Region asociada al color rojo');


%Convertir imagen RGB en un espacio vectorial con makecform y applycform
cform=makecform ('srgb2lab');
lab_huella=applycform(huella,cform);

%Calculando el valor a y b para el area dada.
%a y b sirven como delimitadores de color en el espacio

a=lab_huella(:,:,2);
b=lab_huella(:,:,3);
color_markers=repmat(0,[ncolors, 2]);

for count=1:ncolors
   color_markers(count,1)=mean2(a(sample_regions(:,:,count)));
   color_markers(count,2)=mean2(b(sample_regions(:,:,count)));
end

%Clasificando cada pixel usando a su vecino
color_labels=0:ncolors-1;
%Iniciando la matriz para ser usada en el vecino inmediato

a=double(a);
b=double(b);
distance=repmat(0,[size(a), ncolors]);

for count =1:ncolors
   distance(:,:,count)=((a-color_markers(count,1)).^2+...
                    (b-color_markers(count,2)).^2).^0.5;
end

[value, label] = min(distance,[],3);
label=color_labels(label);
```

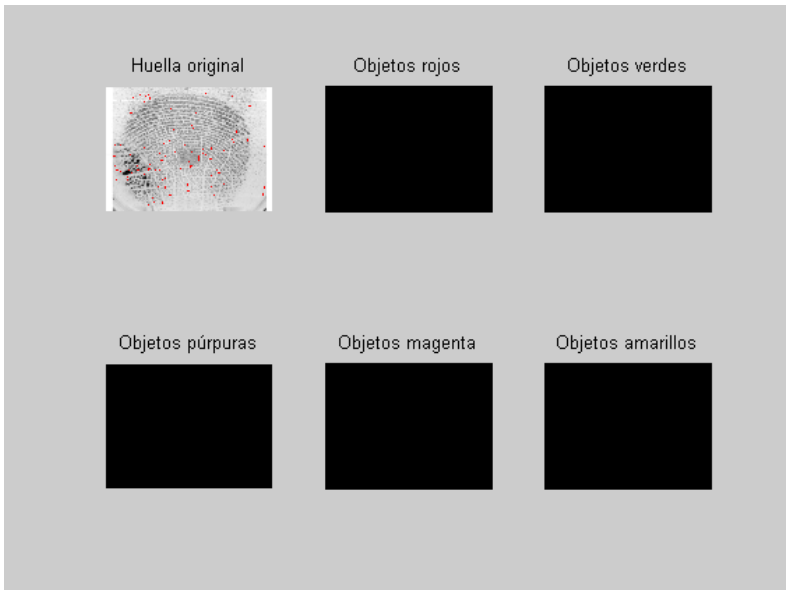
```
clear value distance;

%Desplegar las imagenes separadas

rgb_label=repmat(label,[1 1 3]);

segmented_images=repmat(uint8(0),[size(huella),ncolors]);

for count=1:ncolors
   color=huella;
   color(rgb_label ~= color_labels(count)) = 0;
   segmented_images(:,:,:,count)=color;
end

%Muestra en imagen la separacion

figure (3),title('Separación en colores');

subplot(2,3,1)
imshow(huella),title('Huella original');

subplot(2,3,2)
imshow(segmented_images(:,:,:,2)),title('Objetos rojos');

subplot(2,3,3)
imshow(segmented_images(:,:,:,3)),title('Objetos verdes');

subplot(2,3,4)
imshow(segmented_images(:,:,:,4)),title('Objetos púrpuras');

subplot(2,3,5)
imshow(segmented_images(:,:,:,5)),title('Objetos magenta');

subplot(2,3,6)
imshow(segmented_images(:,:,:,6)),title('Objetos amarillos');

%Despliegue de colores cercanos al rojo y su correspondiente distribucion
purple = [119/255 73/255 152/255];
plot_labels = {'k', 'r', 'g', purple, 'm', 'y'};

figure(4)
for count = 1:ncolors
  plot(a(label==count-1),b(label==count-1),'.','MarkerEdgeColor', ...
      plot_labels{count}, 'MarkerFaceColor', plot_labels{count});
  hold on;
end

title('Scatterplot of the segmented pixels in ''a*b*'' space');
xlabel('''a*'' values');
ylabel('''b*'' values');

figure (5),imshow(segmented_images(:,:,:,4)),title('Minucias aisladas');
```

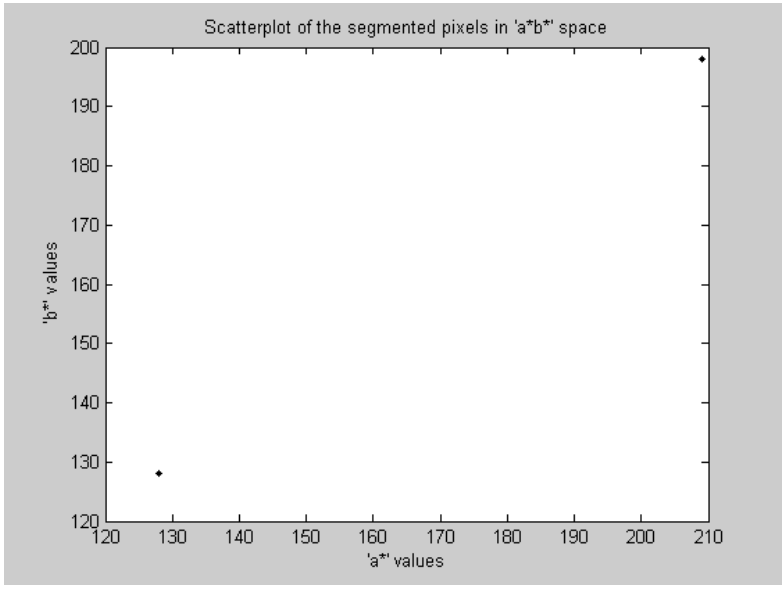
Warning: Divide by zero.
Warning: Divide by zero.

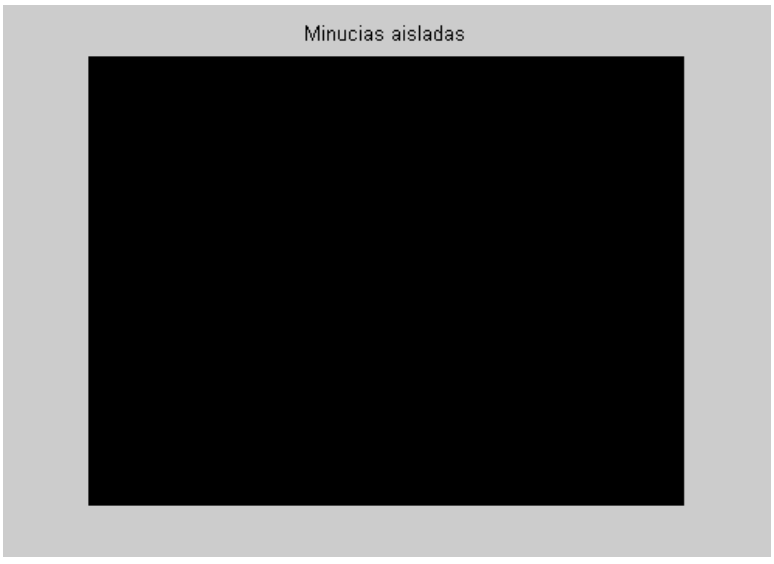
Warning: Divide by zero.
Warning: Divide by zero.






Huella original
Objetos rojos
Objetos verdes
Objetos púrpuras
Objetos magenta
Objetos amarillos


Scatterplot of the segmented pixels in 'a*b*' space
'b*' values
'a*' values
200
190
180
170
160
150
140
130
120
120
130
140
150
160
170
180
190
200
210


Minucias aisladas

Anexo D

```
%Borra todo
clear,close all,imview close all


rgb_img = imread('pi.png');

figure(1),imshow(rgb_img),title('Imagen original');
%Convirtiendo a escala de grises

I = .2989*rgb_img(:,:,1)...
   +.5870*rgb_img(:,:,2)...
   +.1140*rgb_img(:,:,3);


figure(2),imshow(I),title('Imagen en escala de grises');

%Aplicando filtro para extraer minucias
BW = roicolor(I,75,77);

figure(3),imshow(~BW),title('Minucias extraidas');

%figure,imview(BW),title('Analisis de region de pixel');


%Se aplica el agrupamiento a toda la imagen
%BW2 = bwselect(BW);

%Se aplica agrupamiento guardando las variables
[x,y,BW2,idx,xi,yi]=bwselect(BW,8)

figure(4),imshow(~BW2),title('Imagen filtrada');
%Despliega imagen filtrada
%imshow(BW), figure, imshow(BW2);

%IM=improfile;

TRI = delaunay(xi,yi);
figure (5),triplot(TRI,xi,yi)
```

Referencias

[1] B. Miller, "Vital Signs of Identity", IEEE Spectrum, vol. 31, no. 2, 22-30, 1994.

[2] L. Hong and A. Jain, "Integrating Faces and Fingerprints for Personal Identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, 1998

[3] M. Eleccion, "Automatic Fingerprint Identification", IEEE Spectrum, vol. 10, 36-45, 1973.

[4]http://www.pgr.gob.mx/combate%20a%20la%20delincuencia/Servicios%20Periciales/Especializacion%20de%20servicios%20periciales/Sistema%20AFIS.asp

[5] http://www.fbi.gov/hq/cjisd/cjis.htm

[6] http://www.fbi.gov/hq/cjisd/iafis.htm

[7] http://es.wikipedia.org/wiki/Biometr%C3%ADa

[8] http://www.ibix.com.mx/sistemas_biometricos.htm

[9] http://www.dialogica.com.ar/medline/2005/11/huellas_digitales.html

[10] http://es.wikipedia.org/wiki/Juan_Vucetich

[11] http://www.comoves.unam.mx/ant_107_02.html

[12] Tomado de “Fundamentals of Biometric Authentication Technologies”, James I. Wayman, 1999.

[13] www.neotec.com.pa/pdf/introduccionalosbiometricos.pdf

[14]http://www.rs.ejercito.mil.ar/contenido/Nro663/Revista/inteligencia.html

[15] http://www.biometco.com/tecnologia/procesos_biometricos.php

[16] http://www.cienciadigital.es/hemeroteca/reportaje.php?id=83

[17] https://www.proyecto-hesperia.org/hesperia/publicos/061201_ivl.jsp

[18] http://es.wikipedia.org/wiki/Dactiloscop%C3%ADa

[19] http://www.cyberbee.com/whodunnit/classify.html

[20] http://www.cein.es/pdf_servicios/ntic/CursoAutenticacionRobusta.pdf

[21] http://kime25.tripod.com/avance.htm

[22] http://www.tress.com.mx/boletin/julio2005/biometricos.htm

[23] http://www.wordmagicsoft.com/diccionario/es-en/minucias.php

[24]http://www.itnogales.edu.mx/formatos/Reconocimiento%20de%20huellas%20dactilares.pdf

[25] http://www.chymist.com/Fingerprints%20and%20minutiae.pdf

[26] http://www.coit.es/pub/ficheros/t_france_ec8f04b8.pdf

[27] http://www.biometricgroup.com/reports/public/market_report.php

[28]http://www.universia.edu.pe/noticias/principales/destacada.php?id=66036

[29] http://www.cika.com/novedades/novedades_pdf/CAN-026_FingerprintBFS-2S-Rabbit.pdf

[30] http://www.bioidentidad.com/biometria_sdk.htm

[31] Anil Jain, Lin Hong, Ruud Bolle, “On-Line Fingerprint Verification”,IEEE Transactions on pattern analysis and machine intelligence, vol 19, no. 4, abril 1997

[32] http://www.toolingu.com/definition-801155-23928-angulos-adyacentes.html

[33] C. Watson, Ridge Valley Algorithm using parallel computing, NBS report, 1993

[34] Srinivasan V.S. and Murthy N.N. Detection of Singular Point in Fingerprint Images, Pattern Recognition, 1992

[35] Karu K. and Jain A.K., Fingerprint Classification, Pattern Recognition, 1996

[36] Kawagoe M., Tojo A., Fingerprint Pattern Classification, Pattern Recognition 17 pp. 295-303, 1984

[37] Maltoni D., Maio D.,. Jain A.K and Prabhakar S., Handbook of fingerprint recognition, Springer, New York, 2003

[38] A.R. Rao, “A Taxonomy for Texture Description and Identification”, Springer-Verlag, New York, 1990

[39] M.J. Donahue, S.I.Rokhlin, “On the Use of Level Curves in Image Analysis”, Image Understanding, vol. 57, no. 2, 1993

[40] M.J. Donahue, S.I.Rokhlin, “On the Use of Level Curves in Image Analysis”, Image Understanding, vol. 57, no. 2, 1993.

[41] D. Maio, D. Maltoni, “Direct Gray-Scale Minutiae Detection In Fingerprints” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol 19, No. 1. January 1997.

[42] http://www.idg.es/pcworldtech/Seguridad-biometrica.-Prolifera-la-adopcion-de-sis/art191165-seguridad.htm

[43]http://www.interpol.int/Public/Forensic/fingerprints/WorkingParties/IEEGFI/ieegfiEs.asp#def

[44] http://www.sisdid.com/lectores/lectorhuella.html

[45] http://www.digitalpersona.com/

[46]http://oldwww.digitalpersona.com/company/news/clippdfs/BTT06-08.pdf?Number=30407

[47] http://www.digitalpersona.com/index.php?id=home_catalog

[48] http://www.griaulebiometrics.com/page/en-us/fingerprint_sdk/comparison

[49] http://www.griaulebiometrics.com/page/en-us/afis_sdk

[50] http://www.griaulebiometrics.com/page/en-us/fingerprint_sdk

[51]http://www.kriptopolis.org/otra-de-molaware-jaqueado-el-lector-de-huellas-dactilares-de-microsoft

[52]http://www.elmundo.es/navegante/2005/04/27/laimagen/1114595742.html

[53] http://www.xubuntu.org/contribute

[54] http://www.reactivated.net/fprint/api/index.html

[55] http://reactivated.net/fprint/wiki/Libfprint:Supported_devices

[56] http://reactivated.net/fprint/wiki/Fprint_demo

[57] http://www.reactivated.net/fprint/api/group__dev.html

[58] http://es.wikipedia.org/wiki/PNG

[59] www.mailxmail.com/curso/informatica/photodraw/capitulo7.htm

[60]studies.ac.upc.edu/EPSC/TCP/documentos/Enunciado_Cuantizador_0506Q1.doc

[61] Ayuda de MATLAB

[62] http://es.wikipedia.org/wiki/Filtro_paso_banda

[63]http://images.google.com.mx/imgres?imgurl=http://arantxa.ii.uam.es/~pedro/ccii/teoria/TFDFiltrado/3d01ece4.jpg&imgrefurl=http://arantxa.ii.uam.es/~pedro/ccii/teoria/TFDFiltrado/TFDFiltrado.htm&usg=__efcPeR7TCcPC4IoSuDhWBIDjjXU=&h=43&w=254&sz=4&hl=es&start=15&um=1&tbnid=4TZRDNDSmOj5AM:&tbnh=19&tbnw=111&prev=/images%3Fq%3Dfiltro%2Bpaso-banda%2Bideal%26um%3D1%26hl%3Des%26sa%3DN

[64] B. Delaunay: Sur la sphere vide. A la mémoire de Georges Voronoi. Izvestia Akademii Nauk SSSR, Otdelenie Matematicheskikh i Estestvennykh Nauk (Bulletin of Academy of Sciences of the USSR), 7, págs. 793-800, 1934

[65] http://es.wikipedia.org/wiki/Condici%C3%B3n_de_Delaunay

[66] http://www.qhull.org/

[67] Jonathan Richard Shewchuk: Adaptive Precision Floating-Point Arithmetic and Fast Robust Geometric Predicates. In Discrete & Computational Geometry, 18:305-363, 1997

[68] Sharath Pankanti, Salil Prabhakar, Anil K. Jain, “On the individuality of Fingerprints”, IEEE transactions on pattern analysis and machine intelligence, vol 24, no. 8 Agosto 2002 pp. 1010 - 1025.

[69] Abdelmonem A. Saleh, Reza R. Adhami, “Curvature Based Matching Approach for Automatic fingerprint Identification”, IEEE, 2201 p. 171 - 175

[70]Lin Hong, Anil Jain, sharath Pankanti, Ruud Bolle, “Fingerprint Enhancement”, IEEE Spectrum Vol 5, 1996, p 202 - 207

[71] Anil K. Jain, Salil Prabhakar, Lin Hong, Sharath Pankanti. “Filterbank Based Fingerprint Matching”, IEEE transactions on image processing, vol. 9, No 5, may 2000. p 846 - 859.

[72] Ugur Halici, GüÇlü, Ongun. “Fingerprint Classification Through Self-Organizing Feature Maps Modified to Treat Uncertainties. Proceeedings of the IEEE, Vol. 84, No. 10, Octubre 1996, p 1497 – 1512

[73] Tami R. Randolph, Mark J. T. Smith. “Fingerprint Image Enhancement using a Binary Angular Representation”. IEEE ICNN, 2001 p 1561-1564

[74] Anil Jain, Lin Hong, Ruud Bolle, “On-Line Fingerprint Verification”. IEEE Transactions on pattern analysis and machine intelligence, Vol. 19, No 4, Abril 1997. p 302-314.

[75] Sharath Pankanti, Salil Prabhakar, Anil K. Jain. “On the Individuality of Fingerprints”. IEEE, 2001, p. I-805-I-812.

[76] Wang, S. and Wang, Y.S. ‘Fingerprints Enhancement in the Singular Point Area’, IEEE Signal Processing Letters, 2004, Vol. 11 (1) , pp.16-19.

[77] Dominguez Bágena Victor, Rapún Banzo Maria Luisa. “Matlab en cinco lecciones en numérico.”, Febrero 2006 . Disponible en http://www.unavarra.es/personal/victor dominguez/

[78] Rajib Paul, Mustafa Sarwar Nasif, S. M. Farhad.” FINGERPRINT RECOGNITION BY CHAIN CODED STRING MATCHING TECHNIQUE “.International Conference on Information and Communication Technology ICICT 2007, 7-9 March 2007, Dhaka, Bangladesh

[79] B. Chazelle, On the convex layers of a planar set, IEEE Trans. Inform. Theory, IT-31:509-517, 1985.

[80] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Recommended Security Controls for Federal Information Systems [DISK] NIST 2006.

[81] Srinivasan V.S. , Murthy N.N. “Detection of Singular Point in Fingerprint Images”, Pattern Recognition, 25, Nº2, pp. 139-153, 1992.

[82] Wayman J.L., “Technical testing and evaluation of biometric identification devices, in Biometrics: Personal Identification in a Networked Society”, Jain A.K., Bolle R., Pankanti S. (Eds.), pp. 345-368, Kluwer, New York, 1999 .