UNIVERSIDAD NACIONAL DE CATAMARCA

FACULTAD DE TECNOLOGÍA Y

CIENCIAS APLICADAS

LICENCIATURA EN
SISTEMAS DE INFORMACIÓN

TRABAJO FINAL

APLICACIÓN PARA EL RECONOCIMIENTO AUTOMÁTICO DE HUELLAS DIGITALES

Autores:

RASGIDO, DIEGO ALEJANDRO

MERELES, E. CHRISTIAN URIEL

Profesores Guía:

LIC. JUAN PABLOMORENO

MGTR. CAROLA VICTORIA FLORES

Catamarca, Julio de 2017

AGRADECIMIENTOS

A nuestros tutores Carola y Juan, que desinteresadamente nos supieron guiar para la finalización de este proyecto.

A mis padres y hermanos que nunca perdieron la fe en mí.

A mis dos amores Adriana y Matias que tuvieron la paciencia y me acompañaron en este largo camino, sin ellos nunca lo podría haber logrado.

A mi amigo Diego que siempre me dio aliento y supo entender mis objetivos.

Diego Alejandro

A mi familia, lo más importante de mi vida.

Para Ana, que es mi alma gemela

Para Nahu, que me enseñó a ser padre

Para Elías, que es la luz de mis ojos

Para Vos, que todavía no llegaste y ya me haces el hombre más feliz del mundo.

"Sé que donde estés estarás velando por nosotros..."

Christian 家

RESUMEN

Este trabajo final aborda el tema de reconocimiento automático de personas a partir de sus patrones de huellas digitales, para lo cual se realizó una investigación bibliográfica de las distintas técnicas de reconocimiento existentes, a partir de esta investigación se decidió utilizar para el trabajo final la técnica de reconocimiento basado en minucias. Para la aplicación de la técnica seleccionada se realizó una búsqueda, adaptación e integración de algoritmos de extracción y comparación de huellas. Con el objetivo de evaluar las prestaciones que brinda la técnica basada en minucias se desarrolló una aplicación biométrica para la evaluación del módulo adaptado.

Para el desarrollo del aplicativo biométrico se utilizó la metodología orientada a objetos siguiendo el Proceso Unificado de Rational (RUP). La interfaz de usuario se separó del modelo del negocio, utilizando el patrón de diseño Modelo Vista Presentador (MVP), lo que facilita la integración del módulo de reconocimiento.

Para la evaluación del módulo de reconocimiento se han descargado e importado bases de datos públicas de imágenes de huellas digitales, la evaluación se realizó siguiendo el estándar ISO/IEC 19795, además se calcularon otros indicadores, Tasa de Igual Error (EER Error Equal Rate.), FMR100, FMR1000, ZeroFMR, ZeroFNMR.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Los sistemas biométricos son métodos automatizados para la identificación de personas basados en sus características físicas (huella digital, rostro, iris, retina). Los rasgos biométricos, a diferencia de las contraseñas, no pueden ser fácilmente modificados, transferidos, olvidados, copiados o perdidos. En los últimos años, el interés en los sistemas biométricos por parte de las universidades y la industria ha crecido considerablemente debido a la gran demanda de técnicas de autenticación seguras y por la disponibilidad y el bajo costo de los sensores biométricos. Además, los sistemas automatizados de identificación pueden ser usados en varias aplicaciones, como control de acceso, control de asistencia, vigilancia automatizada, protección de datos y otros, siendo hoy en día, los sistemas de verificación y los sistemas de vigilancia los campos que más utilizan estas tecnologías.

Las huellas digitales son, en términos de unicidad y aceptabilidad, una muy buena solución, y son ampliamente utilizadas en aplicaciones civiles y gubernamentales. Además, los sistemas de reconocimiento automático de huellas digitales son rápidos y precisos. Originalmente el uso de huellas digitales estaba limitada solo al campo forense, pero con el paso del tiempo tanto las aplicaciones civiles como gubernamentales han incrementado el uso de estas tecnologías. A pesar que este tipo de sistemas de reconocimiento está disponible en el mercado, su investigación es todavía muy activa, por la necesidad de sistemas más confiables, rápidos y seguros.

Las técnicas existentes para la comparación de huellas digitales comprenden tanto la comparación manual, donde los expertos usan una combinación de rasgos visuales y su experiencia (Leiva Muñoz, Mayorga, & Serrano S, 2008); la comparación basada en correlación, la cual realiza la correlación de los pixeles de la imagen; la comparación basada en textura, trata la huella digital como una imagen orientada de textura y es de muy poca precisión debido a la poca carga de texturas de las huellas, y las técnicas basadas en minucias, que determina la posición relativa de los puntos característicos de las huellas, para su posterior comparación.

El objetivo de este trabajo final fue el desarrollo de una aplicación para el reconocimiento automático de huellas digitales de una persona basado en la técnica de minucias, para lo cual se integraron algoritmos de extracción y comparación de huellas. Así como también, se evaluó el rendimiento del módulo de reconocimiento donde se calculó tasas de error y tiempos de ejecución, siguiendo el estándar ISO/IEC 19795, esta norma se aplica a la evaluación del rendimiento empírico de los sistemas biométricos y los algoritmos que forman parte de las decisiones y puntuaciones de comparación del sistema. Para el desarrollo del aplicativo se utilizó la metodología orientada a objeto siguiendo el Proceso de Desarrollo Unificado de Rational (RUP).

El trabajo final se organizó en capítulos cuyo contenido es el siguiente:

En el Capítulo I “Marco Metodológico”, se plantea el contexto, antecedentes, objetivos y la metodología de trabajo y procedimientos llevado a cabo para el desarrollo del trabajo final.

En el Capítulo II “Marco Teórico”, expone los conocimientos aplicados en el trabajo, se introducen las principales características de la biometría, reconocimiento de huellas

digitales, descripción detallada del reconocimiento basado en minucias, evaluación de rendimiento del sistema biométrico de huellas digitales utilizando el estándar ISO/IEC 19795. Por último se expone la metodología de desarrollo de software utilizada para la implementación del aplicativo.

En el Capítulo III “Desarrollo de la aplicación de reconocimiento de huellas digitales”, se presentan los resultados obtenidos al aplicar el Proceso Unificado Racional (RUP).

En el Capítulo IV “Evaluación de rendimiento”, se describe el procedimiento llevado a cabo para la evaluación siguiendo el estándar ISO/IEC 19795, y otros indicadores que no se encuentran en el estándar para reflejar el comportamiento de la aplicación. También se describen las bases de datos de huellas digitales utilizadas y se hace un análisis de los resultados obtenidos.

En el Capítulo V “Conclusiones”, se exponen las conclusiones obtenidas del desarrollo del trabajo final.

CAPÍTULO I

Marco Metodológico

1.1 Introducción

El presente capítulo presenta el enfoque metodológico y describe en forma general la labor llevada a cabo para la obtención del presente trabajo final, en él se muestran aspectos como: el tipo de investigación, las técnicas y procedimientos que fueron utilizados para llevar a cabo el trabajo.

1.2 Consideraciones sobre el tema abordado

El método de identificación mediante huella digital es uno de los más difundidos para identificar a una persona. En los últimos años este tipo de tecnología ha tenido un creciente uso y se ha acercado al público en general. No resulta extraño ver en algunas organizaciones la utilización de lectores de huellas digitales para el control de acceso del personal, algunas notebooks hacen uso de esta tecnología para la seguridad del dispositivo, incluso los últimos teléfonos inteligentes y tablets brindan la posibilidad de utilizar la pantalla para capturar la huella digital y permitir el acceso al dispositivo.

Han sido numerosas las técnicas empleadas en la verificación e identificación de las personas por medio de sus huellas digitales. Actualmente, el objetivo de los nuevos sistemas es el diseño de algoritmos capaces de discriminar a los individuos de manera eficiente, con tasas de funcionamiento relativamente elevadas. Cabe destacar aquellas aplicaciones en las que se manejan grandes bases de datos, donde el empleo de algoritmos de clasificación de las huellas en diferentes tipos, permite mejorar significativamente los resultados.

Algunos antecedentes indican que la utilización de huellas digitales para la identificación de personas se usa desde hace más de 100 años. De hecho existen referencias de capturas de huellas de las manos con fines de identificación, en India, Japón, China, mucho antes de que los sistemas de clasificación fueran desarrollados (Komarinski, 2005). Particularmente en EEUU en los años 30, varios estados ya implementaban un registro criminal el cual consistía en la captura y procesamiento manual de las huellas digitales. El avance de la tecnología permitió el procesamiento automático de las huellas. Esta tecnología se ha trasladado, de un uso exclusivo en aplicaciones forenses, a otras áreas tales como, control de acceso (RPP Noticias, 2012), control de asistencia, acceso a sistemas de cómputos etc. En Argentina, particularmente en la provincia de Buenos Aires, se utiliza el sistema AFIS de "*SAGEM"* para llevar el registro criminal de la provincia (Morosi, 2003). Por decreto del Poder Ejecutivo Nacional Argentino número 1766/11, impulsado desde el Ministerio de Seguridad de la Nación se implementó el Sistema Federal de Identificación Biométrica para la Seguridad *"SIBIOS"*, el cual tiene un alcance federal, permitiendo a las provincias adherirse al mismo (Tomoyose, 2013).

Se determinó trabajar este tema debido a que la clasificación manual para identificar una huella digital es un proceso complejo y bastante lento. Si bien existen diversas técnicas para la identificación automática de una huella digital (Maltoni D. , Maio, Jain, & Prabhakar, 2003), el presente trabajo se centró en la técnica de extracción de minucias, fue una opción factible para realizar el estudio e implementación del aplicativo, ya que sus procesos pueden implementarse mediante software, no demandando hardware especializado o de alto costo.

1.3 Objetivos

A continuación se presenta el objetivo general y los objetivos específicos planteados para el desarrollo del trabajo final.

Objetivo General

Desarrollar una aplicación que permita realizar el reconocimiento automático de huellas digitales de una persona, mediante la técnica de extracción de minucias.

Objetivos Específicos

- Fundamentar la selección de la técnica de minucias, para el reconocimiento de una persona, basado en los estudios preliminares de los algoritmos que utiliza dicha técnica.
- Adaptar/Integrar algoritmos de procesamientos y comparación de la técnica de extracción de minucias para el desarrollo del módulo de reconocimiento.
- Desarrollar una aplicación que utilice la técnica de minucias para reconocer una persona.
- Determinar las prestaciones, del módulo de reconocimiento desarrollado, en términos de FAR, FRR y tiempos de ejecución.
- Propulsar en el medio el interés por el tema planteado y sentar las bases para nuevos trabajos de investigación.

1.4 Metodología de trabajo

El trabajo final involucró una investigación aplicada, donde para desarrollar la aplicación propuesta se utilizó de la Metodología orientada a objetos y RUP.

1.4.1 Técnicas e Instrumentos

Para la recolección de datos se utilizaron las siguientes Técnicas e Instrumentos:

- Análisis de Contenidos: permitió realizar la sistematización bibliográfica, mediante el instrumento de *documento de anotaciones o registros*.
- Observación indirecta: permitió acumular y normalizar información sobre la técnica de minucias a implementar, para ello se utilizó el cuaderno de notas como instrumento.

1.4.2 Procedimiento

Para el desarrollo del trabajo se cubrieron las tareas que se describen a continuación.

A. Análisis exploratorio

Consistió en la búsqueda, recolección, lectura comprensiva y análisis de las fuentes de información (bibliografía, publicaciones, sitios web, entre otros) referidas al tema que trata el trabajo, que permitió expresar las bases teóricas y conceptuales para la aplicación de la metodología RUP. También se realizó la búsqueda, estudio, validación y adaptación de componentes de software que fueron útiles para el desarrollo propuesto.

B. Elaboración del marco teórico

En esta fase se elaboró el marco teórico que presenta todos los elementos relacionados con la investigación y sustenta el trabajo realizado.

C. Desarrollo del prototipo de la aplicación

Para el desarrollo del prototipo de la aplicación se utilizó la metodología de desarrollo de software Orientada a Objetos (OO) y el Proceso Unificado de Rational (RUP). Para el Modelado OO se utilizó el lenguaje de modelado UML (Unified Modeling Language) para realizar los modelos de las diferentes fases del desarrollo de la aplicación. Se utilizó el lenguaje de desarrollo C# para la implementación.

Los Flujos de trabajos de proceso realizados fueron:

- Modelado de Negocio
- Requerimientos
- Análisis y Diseño
- Implementación
- Pruebas
- Despliegue

D. Evaluación

La tarea de evaluación de las prestaciones del módulo de reconocimiento de huellas digitales, consistió en considerar la velocidad de ejecución y como *métricas de evaluación* tasas definidas en el estándar ISO/IEC 19795 y otros indicadores. A continuación se describen las tasas utilizadas:

- **Tasa de Error de No Concordancia (FNMR *"False Non-Match Rate"*):** proporción de muestras de intentos de usuarios legítimos que el sistema indica que no concuerda con el patrón almacenado.
- **Tasa de Error de Concordancia (FMR *"False Match Rate"*):** proporción de intentos de falsificación aleatoria que el sistema declara que corresponden con el patrón almacenado.
- **Tasa de Falso Rechazo (FRR: "False Reject Rate")**: proporción de intentos de verificación legítimos a los que el sistema deniega el acceso.
- **Tasa de Falsa Aceptación (FAR: "False Accept Rate"):** proporción de intentos de verificación ilegítimos que el sistema acepta erróneamente.
- **Tasa de Error Igual (EER "*Equal Error Rate"*):** valor donde las tasas FAR y FRR son iguales, utilizado para caracterizar con un único número el rendimiento de un sistema biométrico.
- **FMR100:** es el valor más bajo de FNMR para FMR <= 1%.
- **FMR1000:** es el valor más bajo de FNMR para un FMR <= 0.1%.
- **ZeroFMR:** es el valor más bajo de FNMR en el cual no se producen FMR.
- **ZeroFNMR:** es el valor más bajo de FMR en el cual no se producen FNMR.

A. Análisis e Interpretación de los resultados

En este punto se evaluaron los resultados obtenidos en el transcurso del trabajo y el desarrollo del sistema.

B. Redacción del informe de Trabajo Final

Esta etapa involucró la redacción del informe del trabajo final, y la aplicación de diferentes técnicas para la documentación de la totalidad de los recursos obtenidos y/o utilizados a lo largo del trabajo. Se efectuó el informe correspondiente donde se comunican y socializan los resultados y conclusiones del trabajo realizado.

CAPÍTULO II

Marco Teórico

2.1 Introducción

Este capítulo aborda el marco teórico en el que se basó el trabajo, el cual surgió del análisis bibliográfico y del contexto de la investigación. En primer lugar se expone el tema *Biometría y Sistemas biométricos* ya que es el contexto en el que está inmerso el tema abordado, luego se exponen los conceptos de *Reconocimiento de huelas digitales basado en minucias* y *Evaluación de rendimiento de sistema biométrico de huellas digitales*, al finalizar se expone la *Metodología de desarrollo de software* y el *lenguaje de modelado UML* utilizados para el desarrollo del prototipo de la aplicación.

2.2 Biometría y sistemas biométricos

El concepto biometría proviene de las palabras “bio” (vida) y “metría” (medida), lo que significa que todo equipo biométrico mide e identifica alguna característica propia de la persona. Todos los seres humanos tenemos características morfológicas únicas que nos diferencian. La Biometría es definida como características fisiológicas y de comportamiento que pueden ser utilizadas para verificar la identidad de un individuo. Esto incluye las huellas digitales, reconocimiento de iris, geometría de la mano, reconocimiento facial y otras técnicas (Miller, 1994).

Es decir que, la biometría es la disciplina que permite identificar y/o obtener rasgos de la persona basándose en sus características físicas y/o en sus pautas de comportamiento (Fuenmayor, 2004). De esta forma estas tecnologías permiten establecer una relación entre una persona y un determinado patrón o plantilla biométrica asociada a ella de forma segura e intransferible.

Los métodos clásicos de identificación presentan el inconveniente que no pueden discriminar de manera fiable entre individuos legítimos e impostores, ya que la identidad que la persona tiene puede ser robada, extraviada etc. En cambio, la utilización de rasgos biométricos para identificar una persona proporciona una mayor fiabilidad, ya que son propios del individuo, no se pierden, no se pueden robar y su falsificación resulta, por lo menos, costosa. Hay que tener en cuenta que, como los métodos clásicos de identificación, estos métodos no son infalibles aunque si son rápidos y repetitivos (Fuenmayor, 2004).

Existen distintas características biométricas y son usadas en varias aplicaciones. Cada biométrico tiene sus fortalezas y debilidades, las características fisiológicas en las que se basan más frecuentemente los sistemas biométricos son: la huella digital, la huella de la palma de la mano, la geometría de la mano, la cara, el iris.

2.2.1 Sistemas biométricos

En la actualidad, los sistemas biométricos son componentes fundamentales de las arquitecturas de seguridad avanzada. El rango de aplicación de los sistemas biométricos va desde el control de acceso, aplicaciones militares y vigilancia hasta la protección copyright de multimedia. El despliegue a gran escala de sensores biométricos en una variedad de dispositivos electrónicos, como teléfonos móviles, notebooks y asistentes personales digitales (PDA), han acelerado aún más el ritmo de la demanda de tecnologías biométricas.

En general un sistema de reconocimiento biométrico se puede representar como un diagrama en bloque *Figura 2-1*, el cual consta de tres módulos básicos: un *módulo de*

registro, una *base de datos* y un *módulo de reconocimiento*. Estos módulos realizan las funciones necesarias para reconocer a una persona que accede al sistema.

Módulo de registro: Este módulo está formado por un sistema de captura, encargado de proporcionar la señal biométrica que representa al individuo. Por ejemplo, en el caso de un sistema de huella digital, un sensor de huella será el encargado de proporcionar los datos digitales que representan la huella.

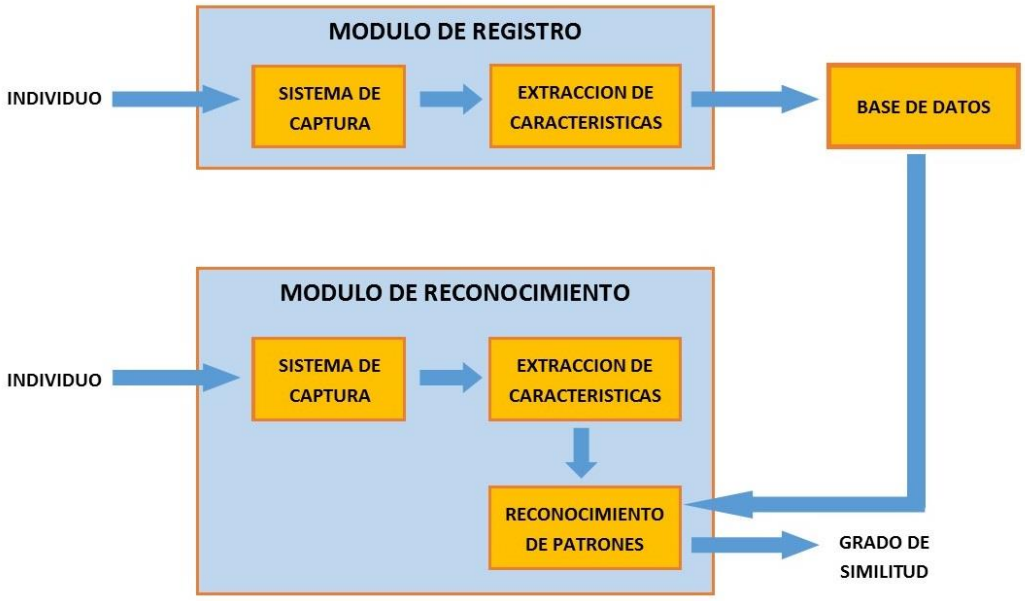


Figura 2-1. *Diagrama en bloque de un sistema de reconocimiento biométrico*

Tras la adquisición de la señal biométrica se procede a la extracción de las características, se toman una serie de muestras del usuario y se procesan, para posteriormente extraer un patrón, el cual se almacenará y será el conjunto de datos que caracterizará a ese usuario. Si se captura más de una muestra, el patrón suele ser el resultado de una media de las características obtenidas. Este proceso se hace de forma supervisada, es decir, existe una persona encargada de controlar cómo se produce la captura de los datos, así como de asegurar la identidad de la persona que se está registrando en el sistema.

Base de datos: El patrón biométrico extraído por el módulo de registro es almacenado en la base de datos del sistema de reconocimiento. La base de datos contendrá, todos los patrones biométricos de los individuos que sean usuarios legítimos del sistema.

Módulo de reconocimiento: Este módulo se encarga de identificar a un individuo que accede al sistema. Para ello, luego de la adquisición del rasgo biométrico del individuo se extraen las características y se obtiene el patrón biométrico, que posteriormente es comparado con los patrones almacenados en la base de datos. Los resultados de estas comparaciones son cuantificados y valorados, permitiendo así la toma de decisión respecto a la identidad del individuo en función del grado de similitud obtenido.

A la hora de juzgar una técnica biométrica, son muchos los parámetros que hay que considerar, de los que se pueden destacar los siguientes (Marin , Rodriguez Uribe, & Olivares Morales, 2008):

- **Universalidad**: si las características se pueden extraer de cualquier usuario o no.
- **Unicidad**: la probabilidad de que no existan dos sujetos con las mismas características.
- **Estabilidad**: si las características que se extraen permanecen inalterables en relación con diversos parámetros (tiempo, edad, enfermedades, etc.).
- **Facilidad de captura**: si existen mecanismos sencillos de captura de los datos biológicos o de comportamiento del sujeto.
- **Rendimiento**: o tasas de acierto y error.
- **Aceptación por los usuarios**
- **Robustez frente a la burla del sistema**: si la técnica puede reconocer el falseamiento de los datos capturados (uso de fotos, dedos de látex, etc.).
- **Costo**: Por tanto, para cada situación y entorno, con un determinado requisito de seguridad, habría que seleccionar la técnica óptima para unos buenos resultados en el funcionamiento del sistema de identificación.

En la Tabla 2-1, se presenta una comparación de las tecnologías biométricas (Jain, Ross, & Prabhakar, 2004).

Identificador biometrico		Universalidad	Unicidad	Estabilidad	Facilidad de captura	Rendimiento	Aceptabilidad	Robustez
Fisiologico	ADN	A	A	A	B	A	B	B
	Oreja	M	M	A	M	M	A	M
	Facial	A	B	M	A	B	A	A
	Termico Facial	A	A	B	A	M	A	B
	Huellas Digitales	M	A	A	M	A	M	M
	Geometria de la mano	M	M	M	A	M	M	M
	Venas de la mano	M	M	M	M	M	M	B
	Retina	A	A	M	B	A	B	B
	Iris	A	A	A	M	A	B	B
	Olor	A	A	A	B	B	M	B
	Palma de la mano	M	A	A	M	A	M	M
Comportamiento	Dinámica de tipeo	B	B	B	M	B	M	M
	Forma de caminar	M	B	B	A	B	A	M
	Firma	B	B	B	A	B	A	A
	Voz	M	B	B	M	B	A	A

Tabla 2-1. *Comparación de varias tecnologías biométricas. Alta, Baja y Media se expresan con A, M y B respectivamente.*

2.2.2 Técnicas de sistemas biométricos

El ser humano ha utilizado el reconocimiento facial como método principal para reconocer a sus semejantes, sin embargo, el ser humano dispone de otros métodos que le permiten reconocer a una persona como ser la voz, la forma de caminar, el ruido de sus zapatos al subir unas escaleras, el perfume.

No todos estos métodos pueden ser replicados por la biometría computarizada, no obstante, existen muchos reconocimientos biométricos que permiten identificar a una persona y no pueden ser reproducidos por el ser humano.

Hasta la fecha se han desarrollado diversos métodos biométricos, con diferentes grados de aceptación y prestaciones. Entre los más destacados se encuentran los siguientes:

- Reconocimiento Huellas Digitales.
- Reconocimiento Facial.
- Reconocimiento Características de la Mano.
- Reconocimiento de la Huella de la Palma.
- Reconocimiento Iris.
- Reconocimiento Retina

Además de estos métodos existen muchos otros que, o bien están en fase de desarrollo o su uso está menos extendido, ejemplos de estos sistemas pueden ser los basados en el olor de una persona, la forma de sus orejas, la forma de firmar, su forma de caminar, etc., que nos demuestran que existen numerosas características entre personas que, aunque se escapan a nuestros propios sentidos, permiten diferenciarnos mediante métodos automáticos.

De los anteriores sistemas, el sistema más seguro en la actualidad es el reconocimiento por iris (Jain, Ross, & Prabhakar, 2004), utilizado en aeropuertos, centrales nucleares y centros de gran seguridad. Las huellas digitales han sido siempre relacionadas con temas policiales y cada vez son más aceptadas por el público en general, el reconocimiento facial permite la detección automática de personas incluso sin su conocimiento. Podemos decir entonces que cada método biométrico tiene un ámbito de aplicación determinado.

Para reconocer a una persona el sistema biométrico debe extraer características de ésta y, a partir de ellas generar un patrón que permita su identificación. El sistema biométrico no guarda la característica en sí como puede ser la mano, el iris, sino que guarda pequeños patrones asociados a éstos, lo que supone a la vez una mayor privacidad, ya que estos datos sólo pueden ser tratados desde el propio sistema de reconocimiento y una disminución de la velocidad de procesado.

Las técnicas de autenticación biométrica más extendidas y aplicables se pueden clasificar según sus características fundamentales en términos de precisión (**P**), costo (**C**), aceptación por parte del usuario (**A**), y grado de intrusión de la técnica (**I**). Obviamente, la técnica ideal tendría precisión y aceptación máximas, y costo e intrusión mínimas (P++++, A++++, C+, I+). De este modo, se analizan de la siguiente manera:

- Reconocimiento de huella digital: el usuario sólo tiene que situar la yema de un dedo sobre un lector de huella. Evaluación: P++++, C++, A+++, I++.

- Reconocimiento facial: el sistema dispone de una cámara que graba al usuario, analizando el rostro del individuo. Evaluación: P++, C+++, A++, I+.
- Reconocimiento de voz: la persona pronuncia un código de acceso prefijado (nombre y/o apellidos, DNI, número de teléfono, PIN, etc.), o una frase diferente cada vez por invitación del sistema, siendo reconocido por el sistema a partir de las características de la voz grabada en el momento del acceso. Evaluación: P+++, C+, A++, I+.
- Reconocimiento de la forma de la mano: la persona sitúa su mano abierta sobre un escáner específico, siendo reconocido a partir de la forma y geometría de la misma. Evaluación: P++, C+++, A++, I++.
- Reconocimiento de iris: el sistema obtiene una imagen precisa del patrón de iris del individuo, y lo compara con el patrón previamente guardado del usuario. Evaluación: P++++, C++++, A+++, I+++.
- Reconocimiento de firma: el individuo firma sobre una superficie predeterminada, y la misma es verificada frente a un patrón previamente obtenido de la misma persona.

Sin embargo, sea cual sea la técnica seleccionada para una determinada aplicación, hay que ponderar en cada caso las restricciones o particularidades que pueden tener cada una de ellas, frente al grado de seguridad añadido que se consigue y que anteriormente no se disponía. Estas características a ponderar vienen dadas básicamente por los siguientes aspectos:

- Necesidad de un dispositivo de adquisición específico (lector de huella digital, micrófono, cámara, etc.) allí donde esté el usuario.
- Posible variabilidad con el tiempo del patrón a identificar (afonías o catarros en voz, uso de gafas/bigote/barba/etc. en rostro, etc.).
- Probabilidad de error individual de cada una de las técnicas (entre uno por cien y uno entre varios millones, en función de la técnica elegida).
- Aceptación por parte del usuario de cada una de las técnicas, en función de si son o no técnicas intrusivas, cómodas, que mantengan la privacidad, sencillas de usar, etc.

De este modo, en función de la situación en que se necesite realizar la autenticación segura del usuario o individuo, se busca cuál es la técnica (o combinación de técnicas) biométrica más adecuada en función de estos cuatro parámetros fundamentales.

Muchas de estas técnicas ya están siendo utilizadas en sistemas reales, como tarjetas de Seguridad Social basada en huella digital, cajeros automáticos con autenticación por iris, o sistemas de compra por teléfono con autenticación por voz.

Aunque las técnicas biométricas usan una combinación de factores corporales y de comportamiento (por ejemplo la medición de la biometría basada en huella digital variará de acuerdo a la manera en que se coloca el dedo), la clasificación de las técnicas biométricas facilita su estudio. La medición de las características corporales de las personas es conocida como biometría estática. Los principales estudios y aplicaciones de la biometría estática están basados en la medición de huellas digitales, geometría de la mano, iris, forma de la cara, retina y venas del dorso de la mano. Existen también, pero menos usadas, las técnicas biométricas basadas en forma de las orejas, temperatura corporal (termografía) y forma del cuerpo.

La medición de las características de comportamiento de las personas es conocida como biometría dinámica. Los principales estudios y aplicaciones de la biometría dinámica están basados en el patrón de voz, firma manuscrita, dinámica del tecleo, cadencia del paso y análisis gestual.

Cada sistema biométrico utiliza una cierta clase de interfaz para recopilar la información sobre la persona que intenta acceder. Un software especializado procesará esa información en un conjunto de datos que se pueden comparar con los modelos de los usuarios que se han introducido previamente al sistema. Si se encuentra un "matching" con la base de datos, se confirma la identidad de la persona y se concede el acceso.

2.2.2.1 Huella digital

Las huellas digitales son características exclusivas de los primates. En la especie humana se forman a partir de la sexta semana de vida intrauterina y no varían en sus características a lo largo de toda la vida del individuo. Son las formas variables que adopta la piel que cubre las yemas de los dedos. Están constituidas por rugosidades que forman salientes y depresiones. Las salientes se denominan crestas papilares y las depresiones surcos interpapilares. En las crestas se encuentran las glándulas sudoríparas. El sudor que éstas producen contiene aceite, que se retiene en los surcos de la huella, de tal manera que cuando el dedo hace contacto con una superficie, queda un residuo de ésta, lo cual produce un facsímil o negativo de la huella *Figura 2-2*.

Figura 2-2. *Imagen de una Huella Digital*

Técnicas de reconocimiento. Las técnicas automáticas de reconocimiento de individuos a partir de la huella digital tienen sus orígenes a finales de los años 70. Desde entonces y hasta ahora, han sido numerosas las técnicas empleadas en la identificación y verificación automática de personas por medio de sus huellas digitales (Maio, 1997) (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Jain, Bolle, & Pankanti, 1999) (Ratha, Connell, & Bolle, 1999) (Zhang D. D., 2000). Actualmente, el objetivo de los nuevos sistemas es el diseño de algoritmos capaces de discriminar a los individuos de manera eficiente, con tasas de funcionamiento relativamente elevadas. Son de destacar aquellas aplicaciones en las que se

manejan grandes bases de datos, donde el empleo de algoritmos de clasificación de las huellas en diferentes tipos, permite mejorar significativamente los resultados (Tojo & Kawagoe, 1984) (Karu, 1996) (Maltoni & Maio, 1996) (Ratha, Karus, Chen, & Jain, 1996) (Cappelli, Lumini, Maio, & Maltoni, 1999). También tiene especial interés la integración o fusión de la huella digital con otros rasgos biométricos, sobre todo en aquellas aplicaciones en las que las condiciones de adquisición no son siempre favorables para los diferentes rasgos implicados (Hong & Jain, 1998) (Kittler, Hater, Duin, & Matas, 1998) (Jain, Hong, , & Kulkarni, 1999).

2.2.2.2 Facial

Un sistema de reconocimiento facial es una aplicación dirigida por ordenador para identificar automáticamente a una persona en una imagen digital mediante la comparación de determinadas características faciales en la imagen y en la base de datos facial.

El reconocimiento facial automatizado es relativamente un concepto nuevo. Desarrollado en los años 60, el primer sistema semiautomático para reconocimiento facial requería del administrador para localizar rasgos (como ojos, orejas, nariz y boca) en las fotografías antes de que este calculara distancias a puntos de referencia en común, los cuales eran comparados luego con datos de referencia (Chellappa, Wilson, & Sirohey, 1995).

El método más común utiliza una cámara para capturar una imagen de nuestra cara, que es analizada en función de ciertos 'puntos claves', como la distancia entre los ojos o la anchura de la nariz.

Funcionamiento. El primer paso en el reconocimiento facial es la adquisición de una imagen real o una imagen bidimensional del objetivo. El sistema determina la alineación de la cara basándose en la posición de la nariz, la boca, etc. En una imagen en 2D no debe estar más desplazada de 35 grados. Después de la alineación, orientación y ajuste de tamaño, el sistema genera una plantilla facial única (una serie de números) de modo que pueda ser comparada con las de la base de datos.

Un factor importante en los sistemas de reconocimiento facial es su capacidad para distinguir entre el fondo y la cara. El sistema hace uso de los picos, valles y contornos dentro de un rostro (los denominados puntos duros del rostro) y trata a estos como nodos que pueden medirse y compararse contra los que se almacenan en la base de datos del sistema. Hay aproximadamente 80 nodos en un rostro de los que el sistema hace uso (entre ellos se incluye el largo de la línea de la mandíbula, la profundidad de los ojos, la distancia entre los ojos, la forma del pómulo, la anchura de la nariz etc.).

Los nuevos sistemas de reconocimiento facial hacen uso de imágenes tridimensionales, y por lo tanto son más precisos que sus predecesores. Al igual que en los sistemas de reconocimiento facial en dos dimensiones, estos sistemas hacen uso de distintas características de un rostro humano y las utilizan como nodos para crear un mapa del rostro humano en tres dimensiones de la cara de una persona. Empleando algoritmos matemáticos similares a los utilizados en búsquedas de Internet, la computadora mide las distancias entre determinados puntos de la muestra en la superficie del rostro *Figura 2-3*. Estos sistemas en 3D tienen la capacidad de reconocer una cara incluso cuando se encuentra girada 90 grados. Por otra parte, no se ven afectados por las diferencias en la iluminación y las expresiones faciales del sujeto.

Figura 2-3. *Imagen de puntos característicos en el reconocimiento facial*

Otros sistemas de reconocimiento facial. Ciertos software interpretan cada imagen facial como un conjunto bidimensional de patrones brillantes y oscuros, con diferentes intensidades de luz en el rostro. Estos patrones, llamados eigenfaces, se convierten en un algoritmo que representa el conjunto de la fisionomía de cada individuo. Cuando un rostro es escaneado para su identificación, el sistema lo compara con todas las eigenfaces guardadas en la base de datos. Este tipo de sistemas está sujeto a limitaciones, como las condiciones ambientales en el momento de capturar la imagen. Así, aunque normalmente interpreta correctamente los cambios de luz en interiores, su funcionamiento al aire libre, con luz natural, es todavía una asignatura pendiente. También la posición de la cabeza y la expresión del rostro pueden influir en el "veredicto".

2.2.2.3 Iris

El iris es una membrana coloreada y circular que separa las cámaras anterior y posterior del ojo. Posee una apertura central de tamaño variable, la pupila. Las fibras musculares del iris la constituyen dos músculos, el esfínter del iris y el dilatador de la pupila. El iris está constantemente activo permitiendo así a la pupila dilatarse (midriasis) o contraerse (miosis). Está función tiene su objetivo en la regulación de la cantidad de luz que llega a la retina. Se trata de la estructura indivisible del cuerpo humano más distintiva matemáticamente. En sus 11 milímetros de diámetro cada iris concentra más de 400 características que pueden ser usadas para identificar a su propietario (criptas, surcos, anillos, fosos, pecas, corona en zig-zag, etc.). Cuenta con un número de puntos distintivos 6 veces superior al de una huella digital.

Hay que tener en cuenta que el iris no cambia a lo largo de la vida, y que sus patrones no están determinados genéticamente, por lo que incluso el ojo izquierdo y el derecho de un mismo individuo son diferentes. Asimismo, se trata de un órgano interno protegido por la córnea y el humor acuoso pero visible externamente a una distancia de hasta un metro. Las lentes de contacto y las gafas no afectan a la identificación. Y, por si todo esto fuera poco, los sistemas basados en el reconocimiento de iris son veinte veces más rápidos que cualquier otro sistema biométrico.

Funcionamiento. El procedimiento, base de los dispositivos actuales, resulta extraordinariamente sencillo. Basta con colocarse frente a una cámara, con los ojos

correctamente alineados en su campo de visión. La cámara genera una imagen que es analizada por medio de los algoritmos de Daugman (Daugman, 1999) para obtener el IrisCode personal, un patrón único del iris que apenas ocupa 256 bytes de información. Tan reducido tamaño permite una rápida búsqueda de su homólogo en una base de datos hasta identificar a su propietario.

Para la codificación del patrón del iris, usualmente se realiza una conversión de la imagen del iris de coordenadas cartesianas a polares para facilitar la extracción de información, al pasar de una forma circular a una rectangular. A la nueva representación, se le aplican filtros multicanal, ya sean de Gabor, Fourier o Wavelet, para extraer los coeficientes que finalmente conformaran el código del iris *Figura 2-4*.

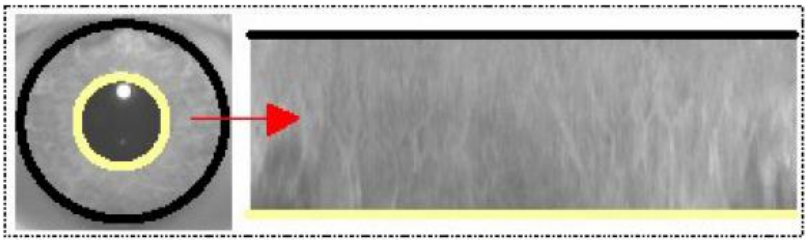


Figura 2-4. *Imagen de Iris después de Aplicar el Filtro de Gabor*

2.2.2.4 Firma Manuscrita

La verificación en base a firmas es algo que todos utilizamos y aceptamos día a día en documentos o cheques; no obstante, existe una diferencia fundamental entre el uso de las firmas que hacemos en nuestra vida cotidiana y los sistemas biométricos; mientras que habitualmente la verificación de la firma consiste en un simple análisis visual sobre una impresión en papel, estática, en los sistemas automáticos no es posible autenticar usuarios en base a la representación de los trazos de su firma. En los modelos biométricos se utiliza además de la forma de firmar, las características dinámicas (por eso se les suele denominar *Dynamic Signature Verification, DSV*), el tiempo utilizado para rubricar, las veces que se separa el bolígrafo del papel, el ángulo con que se realiza cada trazo etc.

Para utilizar un sistema de autenticación basado en firmas se solicita en primer lugar a los futuros usuarios un número determinado de firmas ejemplo, de las cuales el sistema extrae y almacena ciertas características; esta etapa se denomina de aprendizaje, y el principal obstáculo a su correcta ejecución son los usuarios que no suelen firmar uniformemente. Contra este problema la única solución (aparte de una concientización de tales usuarios) es relajar las restricciones del sistema a la hora de aprender firmas, con lo que se produce un decremento en su seguridad. Una vez que el sistema conoce las firmas de sus usuarios, cuando estos desean acceder a él se les solicita tal firma, con un número limitado de intentos (generalmente más que los sistemas que autentican mediante contraseñas, ya que la firma puede variar en un individuo por múltiples factores). La firma introducida es capturada por un lápiz óptico o por una lectora sensible (o por ambos), y el acceso al sistema se produce una vez que el usuario ha introducido una firma que el verificador es capaz de distinguir como auténtica.

Por lo tanto, en lo referente al reconocimiento de firma, existen dos líneas de investigación claramente diferenciadas: reconocimiento de firma estática (off-line) y reconocimiento de firma dinámica (on-line). La principal diferencia entre ambas líneas radica en la información de firma de partida para el reconocimiento (Plamondon & Srihari, 2000).

Técnicas de Reconocimiento Off-Line. En este campo, el reconocimiento parte de firmas realizadas previamente, por lo que la única información de que se dispone es la imagen de la firma (adquisición mediante escáner). Esto va a determinar tanto las características extraídas de la firma (aproximaciones de la geometría de la firma mediante polígonos, relación de aspecto, distribución granulométrica, localización de inicio y final de trazos, concavidad de los trazos, centro geométrico de la firma o inclinación de los trazos verticales: slant, etc.), como las técnicas de procesado de la información adquirida (técnicas de procesado de imágenes en general: filtrados, umbralización, wavelet, etc.).

Técnicas de Reconocimiento On-Line. A diferencia del reconocimiento off-line, ahora la información de la firma se adquiere durante la realización de la misma por el firmante. El proceso de adquisición requerirá por tanto el empleo de dispositivos especiales, como tabletas digitalizadoras, etc. Esto hace que los sistemas on-line dispongan de información temporal de la misma (duración total, duración de levantamientos respecto a la total, posiciones, velocidades y aceleraciones instantáneas, velocidades y aceleraciones de escritura máximas, mínimas y medias, posiciones relativas entre levantamientos y/o contactos con el papel, etc.).

Además, puesto que la adquisición en estos sistemas suele consistir en el muestreo periódico de características de la firma durante la ejecución de la misma (posiciones vertical y horizontal, presión instantánea, etc.), las técnicas de procesado aplicadas a la información adquirida, son típicas de señales unidimensionales, (filtrado, escalado de amplitudes, etc.).

En resumen, se podría decir que la principal diferencia entre ambas líneas de trabajo reside en la simultaneidad entre los procesos de realización de la firma y adquisición de la información para el reconocimiento. Como se puede imaginar, puesto que los sistemas on-line disponen de mayor información para realizar el reconocimiento (información estática y dinámica), serán más eficientes en lo referente a verificación de firmantes. Además, como el firmante realiza su firma de forma automática (se podría decir que el movimiento de la mano durante la ejecución de la firma es un movimiento no supervisado o pseudorreflejo) la información dinámica no es fácilmente falsificable por un impostor, y menos aún si para entrenarse en la realización de la falsificación dispone de una imagen de la firma, donde no se conoce ni la dinámica del movimiento durante la ejecución original de la firma, ni la secuencia ordenada de trazos.

2.2.2.5 Otras técnicas biométricas

Además de las técnicas ya descriptas existen otras que se enumeran a continuación:

- Huella palmar
- Geometría de la mano
- Termograma facial
- Venas de la mano
- Retina
- Modo de pulsar un teclado,

- Modo de andar.

Huella palmar. La huella de la palma de la mano es un rasgo muy estable en el tiempo y presenta una elevada capacidad de representación de las características de los individuos (Lu & Zhang, 2002) (Zhang D. D., 2002). Por ese motivo, tiene gran aceptación en los ámbitos legal y forense. Al igual que las huellas digitales, la palma de la mano tiene gran aceptación, no es percibida como una técnica intrusiva y requiere de poca cooperación por parte de los individuos.

Geometría de la mano. Este rasgo biométrico incluye diversas características, como son: el contorno de la mano, la longitud y anchura de los dedos, el contorno de los dedos, etc. La obtención de estas características conlleva la captura de una imagen en la que se representa la silueta de la mano en dos vistas: una lateral y otra alzada. Esta técnica presenta el inconveniente de requerir un elevado grado de cooperación por parte del individuo; además de su baja capacidad de discriminación, especialmente cuando se trata con poblaciones grandes de individuos. Otro gran inconveniente es su variabilidad con el tiempo. Por todo ello, es un rasgo biométrico que no tiene muchas aplicaciones por si solo; sin embargo, si se utiliza conjuntamente con otros rasgos (por ejemplo, la huella palmar) en los sistemas de fusión multimodales. Cuenta con la ventaja de su gran aceptabilidad y fácil implementación (Zunkel, 1999) (Sánchez Reillo & Sánchez-Ávila, 2001).

Termograma facial. El calor radiado, a través de la piel, por el sistema vascular que irriga la cara de un individuo, puede capturarse fácilmente con una cámara de infrarrojos (Prokoski & Riedel, 1999). La imagen así obtenida constituye su termograma facial. Puede considerarse que dicho termograma es particular para cada individuo. Tiene la ventaja de que no depende de las condiciones de iluminación, pudiendo capturarse la imagen incluso en ausencia total de luz. Es una técnica biométrica no invasiva, que no precisa de la cooperación del individuo. Lo cierto es que, a pesar de las ventajas que presenta esta técnica, la investigación actual no se ha centrado en este rasgo biométrico, puesto que el termograma facial no permanece invariable en el tiempo. Tampoco se ha podido probar que sea un rasgo suficientemente discriminatorio entre los individuos. Presenta, además, otros inconvenientes, como son su dependencia con el estado de ánimo del sujeto y con su temperatura corporal.

Venas de la mano. El patrón biométrico que proporcionan las venas de la mano es un patrón lo suficientemente robusto y estable, como para constituir por si solo un sistema de reconocimiento automático. Sin embargo, al igual que sucede con la geometría de la mano, las tasas de funcionamiento que se obtienen no son nunca mejores que las obtenidas con la cara, la huella digital, la firma o la voz, por lo que su utilización se restringe casi siempre al entorno de los sistemas multimodales. Las venas de la mano presentan como ventaja la gran aceptación por parte de la población, y la fácil adquisición de los patrones utilizando una cámara de infrarrojos (Prokoski & Riedel, 1999).

Retina. El patrón biométrico proporcionado por la retina es un patrón único para cada persona y muy estable a lo largo de la vida, aunque en determinadas circunstancias pueden producirse ciertas alteraciones con la edad. Los sistemas basados en los patrones de retina son los de alta seguridad. Sin embargo, debido a que el método de captura de la imagen es un método invasor, cuenta con muy poca aceptación pública. Generalmente, las personas intentan proteger sus ojos durante el tiempo que dura la adquisición de la imagen. Por este

motivo, y debido también a su elevado costo económico, su aplicación se restringe a los controles de acceso de alta seguridad; como por ejemplo, plantas nucleares, prisiones, ejercito y servicios médicos (Hill, 1999).

Modo de pulsar un teclado. El patrón biométrico que un individuo genera al pulsar un teclado está condicionado por factores neurofisiológicos similares a los que intervienen en el proceso de escribir o firmar, proporcionando las características de individualidad que el reconocimiento automático requiere (Odaidat & Sadoun, 1999). El patrón biométrico, en este caso, se basa principalmente en la señal temporal que puede extraerse de la secuencia de pulsaciones. Es una técnica muy apropiada para la autenticación de individuos mediante palabras clave (passwords). El desarrollo y estandarización actual de los teclados favorece la dinámica de las pulsaciones, reduciéndose en gran parte la variabilidad de las adquisiciones. No obstante, la invariabilidad de los patrones y su dependencia del número de pruebas de entrenamiento y de la longitud de las palabras, siguen siendo aspectos importantes de la investigación actual en este ámbito.

Modo de andar. La forma de andar de una persona es un rasgo biométrico espacio-temporal muy complejo (Yam, Nixon, & Carter, 2003). No se trata de un rasgo con muy alta capacidad de discriminación de las personas, pero es lo suficientemente característico como para permitir el reconocimiento en entornos de seguridad media. Es un rasgo biométrico de comportamiento y puede no ser invariante en el tiempo, sobre todo si se consideran largos periodos en los que el individuo puede experimentar importantes cambios fisiológicos de su cuerpo, como por ejemplo: el peso, la distribución de la masa corporal, posibles daños en las articulaciones o sistema nervioso, etc. El reconocimiento se basa en diferentes patrones de movimiento efectuados por cada articulación al caminar.

2.2.3 Sistemas automáticos de reconocimiento

Los sistemas automáticos de reconocimiento no solo han automatizado procesos existentes de identificación de personas, sino que han cambiado todo el proceso de reconocimiento. El software reemplazó a las personas encargadas de clasificar los rasgos biométricos y las bases de datos reemplazaron las tarjetas de identificación. Se ha podido optimizar un proceso de identificación laborioso, caro de mantener, completamente dependiente del papel y relativamente lento. El sistema automatiza el proceso de reconocimiento a través del uso de imágenes digitales que pueden ser codificadas y posteriormente examinadas (Komariski, 2005).

2.2.4 Modelo genérico de un sistema biométrico

Aunque los sistemas biométricos utilizan diferentes características biométricas y se basan en tecnologías muy diferentes, en general, mantienen la misma estructura central. Fundamentalmente, un sistema biométrico es un sistema de reconocimiento de patrones que adquiere datos biométricos de un individuo, extrae un conjunto de características, compara estas características con las características almacenadas en una base de datos y ejecuta una acción basada en el resultado de la comparación (Jain, Ross, & Prabhakar, 2004). Por lo tanto, un sistema biométrico genérico puede ser visto como cuatro módulos principales *Figura 2-5*:

i. **Módulo de sensor:** el cual captura los datos biométricos de una persona. Por ejemplo un lector de huellas digitales que digitaliza las crestas y surcos del dedo del usuario.
ii. **Módulo de extracción de características:** el cual procesa los datos biométricos adquiridos para extraer un conjunto de características principales.
iii. **Módulo de comparación:** que compara las características extraídas con los patrones biométricos almacenados para generar una puntuación o valor de coincidencia.
iv. **Módulo de base de datos:** que almacena información biométrica.

Dependiendo del contexto, un sistema biométrico posee dos características principales de funcionamiento, *verificación* e *identificación*, pero es necesaria una fase previa, *registro*, común a ambas características (Jain, Ross, & Prabhakar, 2004).

- **Modo registro**: Se registran en la base de datos los patrones biométricos de los diferentes usuarios del sistema. Se realiza adquisición de la señal biométrica, la extracción de características, la generación del patrón biométrico correspondiente y su almacenamiento en la base de datos *Figura 2-5 a)*. Una vez creada la base de datos el sistema podrá entrar en funcionamiento en modo identificación o en modo verificación, además siempre se puede volver a la fase de registro para agregar, borrar o modificar usuarios.
- **Modo verificación**: El sistema valida la identidad de una persona comparando los datos biométricos con su propio patrón biométrico almacenado en la base de datos *Figura 2-5 b)*. En general, la persona que desea ser reconocida, indica su identidad, vía PIN (*Personal Identification Number*), nombre de usuario o tarjeta inteligente, y el sistema extrae el patrón biométrico de la persona y compara (comparación 1 a 1) con el patrón biométrico de dicha identidad, que fue registrado previamente en la base de datos. Si el grado de similitud entre el patrón adquirido y el patrón almacenado supera un determinado nivel de decisión (umbral), se considera que la identificación suministrada es verdadera. En caso contrario, la identidad es considerada falsa y se declara el usuario como impostor. Este tipo de operación, es típicamente usada para reconocimiento positivo, donde el objetivo es prevenir que múltiples personas utilicen la misma identidad.

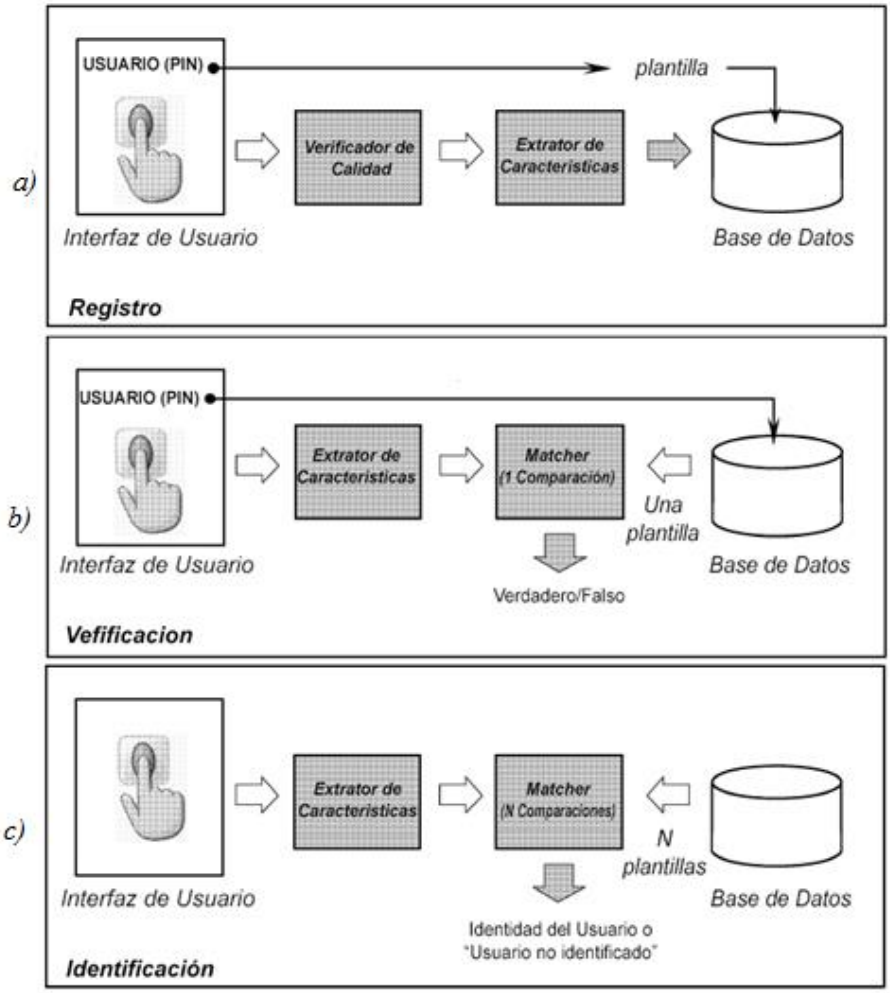


Figura 2-5. *Modos de operación de un sistema biométrico.*

- **Modo identificación:** El sistema reconoce una persona buscando en un conjunto de *N* patrones biométricos almacenados en la base de datos, tratando de encontrar la que corresponda con los datos biométricos suministrados como entrada *Figura 2-5 c)*. Por lo tanto, el sistema realiza una comparación uno a muchos (1 a N) para determinar la identidad de una persona (o falla si la persona no está registrada en la base de datos). La identificación es el componente principal en las aplicaciones de reconocimiento negativo, donde el sistema establece si la persona es quien (implícita o explícitamente) niega ser. El propósito del reconociendo negativo, es prevenir que una persona use múltiples identidades.

2.2.5 Caracterización del funcionamiento de un sistema biométrico

Resulta difícil en la práctica caracterizar y comparar el funcionamiento de los sistemas de reconocimiento, debido a que el entorno en el que se desenvuelven las distintas modalidades biométricas es muy heterogéneo. Los factores que definen este entorno son: el tipo de aplicación, el escenario en el que se realizan la inscripción y/o las pruebas de evaluación, el tamaño de la población de usuarios, el control de las adquisiciones, etc.

Existen además diversos factores propios de cada modalidad que hacen inviable la comparación de sistemas en términos absolutos. Ejemplos de estos factores son: el tipo de dispositivo empleado en la adquisición de huellas digitales, la iluminación en el reconocimiento de cara, el canal de transmisión en la verificación de locutores, la habilidad de los falsificadores en el reconocimiento de firma, etc.

En el intento de caracterizar el funcionamiento de los sistemas biométricos, (Ortega-Garcia, Bigun, Reynolds, & Gon, 2003) establecen una clasificación de las tasas de error según diferentes rangos. A modo de ejemplo se consideran cuatro modalidades biométricas ampliamente extendidas: huella digital, voz, cara y firma. Distinguen cuatro niveles de funcionamiento:

1. Nivel de funcionamiento muy alto (EER: 0.1% - 1%).
    - Huella: alta calidad de las imágenes adquiridas, sin variabilidad de la posición, sin presencia de suciedad ni humedad.
    - Voz: voz dependiente de texto, pronunciación de frases fijas, alta relación señal/ruido en la señal grabada, multisesión, 3 minutos para entrenamiento, 2 minutos para pruebas.
    - Cara: condiciones controladas en laboratorio con adquisición manual, imágenes frontales, iluminación, fondo y pose fijas, número suficiente de muestras para entrenamiento de modelos.
    - Firma: verificación on-line, técnica basada en funciones, habilidad media-alta de las falsificaciones, 5 a 10 muestras para entrenamiento.
2. Nivel de funcionamiento alto (EER: 1% - 5%).
    - Huella: calidad media de las adquisiciones, nivel bajo de variabilidad de la posición, sin presencia de suciedad ni humedad.
    - Voz: dependiente de texto, pronunciación de secuencias de 10 dígitos, voz telefónica, variabilidad en el tipo de teléfono, multisesión, 2 secuencias de datos para entrenamiento, 1 secuencia de datos para verificación.
    - Cara: imagen frontal, iluminación, fondo y pose fijas, muestras suficientes para entrenamiento de modelos, cara sin artefactos.
    - Firma: verificación on-line, técnica basada en funciones y características, habilidad muy alta de las falsificaciones, menos de 5 muestras para entrenamiento.
3. Nivel de funcionamiento medio (EER: 5% - 15%).
    - Huella: adquisiciones de calidad media-baja, alta variabilidad de la posición, diferentes sensores, presencia de suciedad y humedad.
    - Voz: independiente de texto, conversación normal, señal vía canal telefónico, variabilidad en el tipo de teléfono, multisesión, 2 minutos para entrenamiento, 30 segundos de pruebas.
    - Cara: imágenes estáticas, buena iluminación, pose controlada, con cooperación del individuo, menos de 4 muestras para entrenamiento.
    - Firma: verificación off-line, imágenes extraídas del fondo, habilidad media-alta de falsificaciones, 5 a 10 muestras para entrenamiento.
4. Nivel de funcionamiento bajo (EER: 15% - 35%):
    - Huella: imágenes de baja y muy baja calidad, varios sensores, alta variabilidad de la posición, perdidas de impresión, presencia de suciedad, daños en la piel.

- Voz: texto independiente, frases leídas, voz vía canales de radio de baja relación señal/ruido, variabilidad en el tipo de micrófono, multisesión, 30 segundos de entrenamiento, 15 segundos de pruebas.
- Cara: imágenes de video en situaciones reales, sin control de la iluminación y la pose, no cooperación del individuo, variabilidad de los sensores, distorsión óptica de imágenes.
- Firma: verificación off-line, falsificaciones perfectas, imágenes con ruido de fondo, menos de 5 muestras para entrenamiento.

Como puede deducirse de estos ejemplos el funcionamiento de los sistemas biométricos mejora significativamente a medida que los requisitos exigidos a la aplicación son mayores: mayor calidad de la entrada, mayor número de muestras, menor distorsión y ruido, correcto funcionamiento de los dispositivos de adquisición, menor variabilidad en las adquisiciones, cooperación de los individuos, etc. En general, el intento de mejorar el funcionamiento conlleva la valoración previa del beneficio que puede suponer la modificación de cualquiera de los requisitos anteriores, el costo relativo de los errores cometidos por el sistema y la robustez del mismo frente a los intentos de acceso de los impostores.

2.3 Reconocimiento de huellas digitales

La huella digital ha sido siempre un rasgo biométrico utilizado por la humanidad para la identificación de las personas. Es un rasgo particular de cada individuo cuyo origen tiene lugar durante la etapa fetal y permanece inmutable a lo largo de toda la vida. La huella digital permite, además, discriminar perfectamente a los diferentes individuos y su grado de aceptabilidad es relativamente alto. No obstante, se precisa de cierta cooperación por parte del individuo, para que la imagen adquirida de la huella tenga la suficiente calidad, como para permitir el empleo de algoritmos de reconocimientos sencillos, en muchas aplicaciones, las condiciones de adquisición no son lo suficientemente favorables y, por lo tanto, la mala calidad de las huellas adquiridas obliga al empleo de algoritmos complejos, tanto en la etapa de extracción de características, como en la etapa de reconocimiento de patrones.

2.3.1 Historia de las huellas digitales

Existe un gran número de artefactos arqueológicos e históricos *Figura 2-6*, que proporcionan evidencias que los pueblos antiguos eran conscientes de las características de las huellas digitales para identificar una persona, por ejemplo, los sellos de arcilla chinos y las lámparas palestinas fueron usados para indicar la identidad de sus proveedores. Sin embargo, aunque la capacidad de individualizar una persona por su huella digital era conocida en esa época, no existe ninguna base científica de esto.

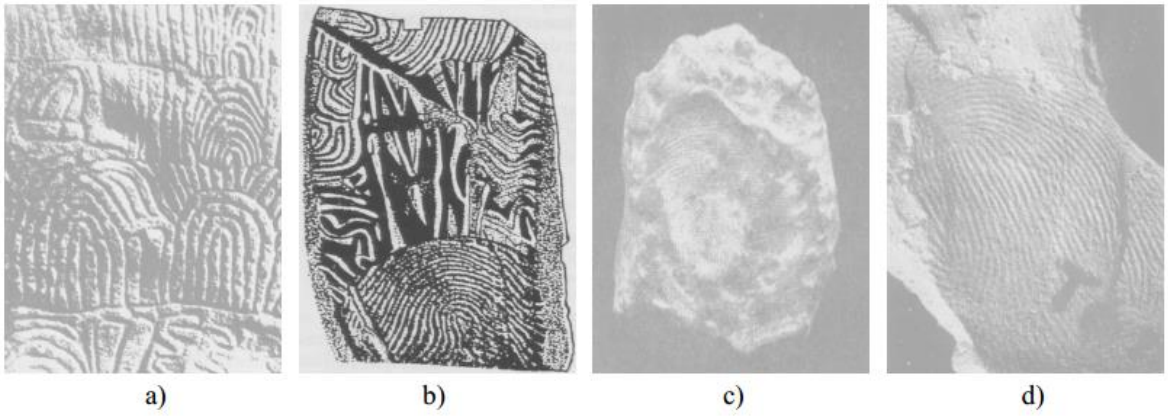


Figura 2-6. *Ejemplos huellas digitales arqueológicas talladas e impresión de huellas digitales históricas. (a) Tallado Neolítico; (b) Piedras (Isla de las cabras 2000 A.C.); (c) Sello de arcilla chino (300 A.C.); (d) Impresión de una lámpara Palestina.*

A finales del siglo XVI, se comenzaron a utilizar las técnicas modernas de huellas digitales (Maltoni D. , Maio, Jain, & Prabhakar, 2003). En 1684, el morfologista inglés Nehemiah Grew, publicó el primer estudio científico de la estructura de crestas, surcos y poros en las huellas digitales. Desde entonces, un gran número de investigadores se han abocado al estudio de las huellas digitales. En 1788, Mayer realizó una descripción detallada de la formación anatómica de las huellas digitales en el cual, un número de crestas fueron identificadas y caracterizadas. A principios de 1890, Thomas Bewick comenzó a utilizar su huella digital como su marca registrada *Figura 2-7,* el cual fue unos de los hitos más importantes en el estudio científico de huellas digitales. En 1823, Purkinje propuso un esquema de clasificación de nueve clases teniendo en cuenta la configuración de la

estructura de crestas *Figura 2-8*. Estos estudios establecieron la fundación del reconocimiento de huellas digitales moderno. A finales del siglo XIX, Francis Galton llevó a cabo un estudio extensivo de huellas digitales, introdujo el uso de minucias para la comparación de huellas digitales. En 1899 Edward Henry, realizó un importante avance, estableciendo el "Sistema Henry" de clasificación de huellas digitales. A principios del siglo XX, ya se contaba con el estudio y entendimiento suficiente para definir lo siguiente:

1. Las crestas y surcos epidérmicas individuales tienen diferentes características para diferentes huellas.
2. La estructura de crestas y surcos de un individuo, aunque pueden variar, lo hacen dentro de límites tan reducidos, que hacen posible una clasificación sistemática.
3. La estructura de crestas, surcos y minucias individuales, son permanentes y no varían con el tiempo.

La primera y tercera característica constituyen los principios por los que se rige la identificación de individuos por sus huellas digitales. La segunda característica constituye el principio que permite la clasificación de huellas digitales (Maltoni D. , Maio, Jain, & Prabhakar, 2003).

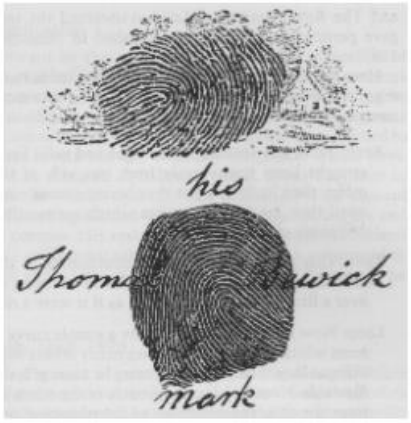


Figura 2-7. *Marca registrada de Thomas Bewick*

Desde principios de 1800, la identificación de personas a partir de sus huellas digitales estuvo formalmente aceptada, comenzando a ser una práctica rutinaria en las aplicaciones forenses, en todo el mundo se instauraron las agencias policiales de identificación de huellas digitales y se crearon las bases de datos criminales. Se desarrollaron diferentes técnicas de adquisición de huellas latentes, de identificación, de clasificación y de comparación de patrones. En 1924, por ejemplo, se instauró la primera división de identificación de huellas digitales del FBI.

El reconocimiento automático de huellas digitales comenzó a principios de los años 60. Desde entonces, los sistemas de identificación de huellas digitales se utilizan en las instituciones policiales del todo el mundo. En los años 80, con el desarrollo de las computadoras personales y los dispositivos de captura electrónicos, se comenzaron a utilizar los sistemas automáticos de identificación en aplicaciones no criminales; como por ejemplo el control de acceso en entornos de seguridad. A finales de los 90, el desarrollo de

los dispositivos de captura de estado sólido, su bajo costo y el desarrollo de algoritmos precisos y fiables de reconocimiento de patrones, han contribuido a la rápida expansión de los sistemas de reconocimiento biométrico basados en las huellas digitales.

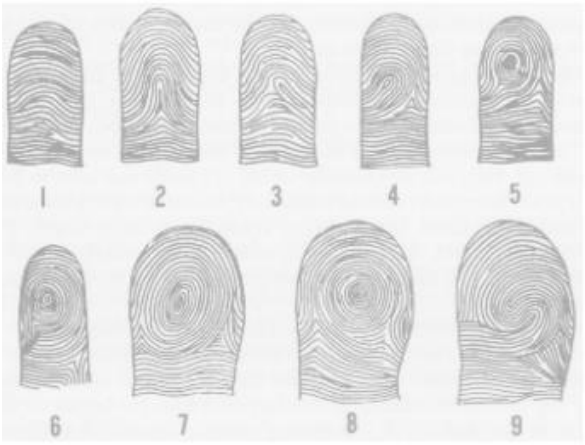


Figura 2-8. *Nueve patrones ilustrados en la tesis de Purkinje.*

2.3.2 Características de las huellas digitales

Una huella digital es la reproducción de la epidermis del dedo, generada al presionar la yema del dedo en una superficie suave. Las huellas digitales de cualquier ser humano están constituidas por una multitud de crestas y surcos con cierta orientación. Las crestas (crestas de fricción) forman un relieve ondulado en la piel y están formadas por glándulas sudoríparas *Figura 2-9*. Una vez que el sudor sale, se derrama por todas las crestas y se mezcla con la grasa natural de la piel; lo que da lugar a que, cuando se toque o manipule un objeto apto para la retención de huellas, las crestas dejen una impresión en él. Las formaciones de las huellas digitales dependen de las condiciones iniciales del desarrollo embrionario y se caracterizan por ser inmutables, permanentes y únicas para cada individuo (Jain A. K., Hong, Pankanti, Sharath, & Bolle, 1996). Lesiones, como quemaduras superficiales, desgastes o cortes no afectan las estructuras de las crestas, ya que el patrón original es restaurado al regenerarse la piel.

Figura 2-9. *Yema del dedo pulgar.*

2.3.3 Huellas digitales como biometría

Las huellas digitales han sido aceptadas formalmente como un sistema de identificación de personas valido y se ha convertido en la técnica más usada mundialmente para la autenticación en las agencias relacionadas con la seguridad. El FBI actualmente mantiene más de 400 millones de registros de huellas digitales. Las huellas digitales tienen varias ventajas sobre otros sistemas biométricos, como ser:

1. Universalidad: La gran mayoría de la población humana y por lo tanto puede ser fácilmente autenticada. Esto excede la cantidad de la población que posee pasaportes, documentos de identidad o cualquier otra forma de identificación.
2. Alta distintividad: Incluso gemelos idénticos que comparten el mismo ADN muestran tener distintas huellas digitales, debido a que la estructura de las crestas de los dedos no está codificado en los genes de un individuo. Por esto las huellas digitales representan un mecanismo de autenticación más fuerte que el de reconocimiento de ADN. Más aun, no hay evidencia de huellas digitales idénticas en más de un siglo de prácticas forenses.
3. Alta Permanencia: Los patrones en la superficie de las estructuras de los dedos se crean en el nacimiento y se mantienen hasta la muerte de un individuo.
4. Fácil recolección: El proceso de colectar huellas digitales se ha convertido en un proceso muy sencillo con los sensores actuales, capaces de capturar imágenes de alta resolución de una huella digital en un tiempo inferior a un segundo. El proceso de recolección de las huellas se puede implementar tanto con usuarios que cooperen como con los que no cooperen.
5. Alta performance: Las huellas digitales se mantienen como la modalidad biométrica más acertada disponible en la actualidad considerando la tasa de falsos rechazos y la taza de falsos positivos.
6. Alta aceptación: Comparado con los otros métodos biométricos los usuarios demuestran tener mejor aceptación a la hora de insertar sus huellas digitales en bancos de datos para su autenticación que con métodos aun en desarrollo.

2.3.4 Primeras prácticas de identificación

La identificación automática de personas por medio de sus huellas digitales, han automatizado un proceso existente de identificación. Agencias gubernamentales empleaban cientos de personas a las que se les confiaba la responsabilidad de confirmar, basadas en las imágenes de huellas digitales, si un individuo poseía o no un registró criminal. Un examinador experto en las complejas reglas de clasificación de huellas digitales, debía examinar el patrón utilizando un retículo *Figura 2-10*, e iniciaba la clasificación de las imágenes de huellas digitales basado en, por ejemplo, arcos, terminación incluso en los espirales formados en las huellas. Se debían contar el número de crestas desde el núcleo hasta el delta. Mientras la huella era clasificada, otros técnicos revisaban los registros para ver si el individuo ya se encontraba en los archivos de huellas digitales. Los sistemas de reconocimiento automático de huellas digitales basados en la técnica de minucias, imitan el proceso de reconocimiento manual, procesando la imagen de la huella digital, buscando y guardando las minucias en las huellas para su posterior comparación.

Figura 2-10. *Retículo examinador de huellas digitales*

2.3.5 Técnicas de reconocimiento de patrones biométricos

Existen en la literatura diversos métodos para el reconocimiento de patrones biométricos en el reconocimiento automático de huella digital. Las técnicas empleadas dependen de los tipos de patrones comparados y pueden ser:

- Técnica basadas en minucias, donde se trabaja con la comparación de patones de puntos (minucias) extraídos de la estructura de las crestas.
- Técnicas basadas en las características de la estructura de crestas y surcos.
- Técnicas basadas en la textura de la imagen.

Técnicas basadas en patrones de minucias

La comparación de patrones basada en la extracción de minucias es la técnica más utilizada en los sistemas de reconocimiento actuales (Lee & Gaensslen, 2001).

El número de minucias en una huella digital puede variar ampliamente de una huella a otra y de una imagen a otra por muchas razones. Pero, en promedio, se pueden encontrar alrededor de 70 a 150 minucias en una imagen de huella digital completa. Sin embargo, se puede realizar una identificación positiva emparejando un número mucho menor de pares de minucias y sus respectivas relaciones topológicas.

Existen diversos enfoques para la extracción de minucias de una imagen de huella digital. La mayoría, primero convierte la imagen en una imagen binaria y luego realizan un proceso de adelgazamiento que reduce las crestas a un ancho de un pixel, y las minucias se localizan en la imagen adelgazada.

Las comparaciones de las minucias, se basan generalmente en técnicas de comparación euclidiana. Estos comparadores realizan transformaciones matemáticas entre los patrones de puntos para poder estimar el grado de similitud entre ellos. La mayoría de ellos, mediante procesos iterativos, pueden comparar los patrones con suficiente exactitud, a pesar de que en el proceso de extracción de características se hayan podido perder minucias verdaderas o se hayan podido introducir minucias falsas (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Maio, 1997) (Garcia Gomar, 2000) (Jain K. P., 2000) (Prabhakar, 2000). Algunos ejemplos importantes de estas técnicas son:

Técnica de Relajación. En (Ranade, 1983) se propone un método de comparación de patrones de puntos mediante el procedimiento matemático de relajación. Se trata de un método iterativo en el que, mediante aproximaciones sucesivas, se va desplazando un patrón de puntos sobre el otro, al tiempo que se van ajustando las distancias entre las parejas de minucias más o menos coincidentes. El desplazamiento efectuado en cada iteración se basa en el resultado obtenido de la iteración inmediatamente anterior, de acuerdo con el valor que toma un factor de mérito que evalúa el grado de proximidad entre las parejas de puntos comparados. Existen algunas alternativas basadas en este algoritmo, que intentan simplificar el proceso de comparación; sin embargo, debido a su naturaleza iterativa, el proceso es relativamente lento. Presentan el inconveniente de que no funcionan bien cuando los patrones a comparar proceden de imágenes muy distorsionadas; situación relativamente frecuente en el caso de las huellas digitales.

Técnica basada en el alineamiento de patrones. Según el método anterior, la comparación entre dos huellas digitales supone la comparación de todas las posibles combinaciones que pueden hacerse con las agrupaciones de minucias de las dos huellas. Por este motivo, el tiempo de respuesta del sistema puede hacerse muy grande. Como solución a este problema se han propuesto métodos de reconocimiento que incluyen el alineamiento de las huellas antes de efectuar su comparación. Gracias al proceso de alineamiento se consigue reducir el número de comparaciones necesarias para establecer el grado de similitud entre las huellas, reduciéndose significativamente el tiempo de respuesta. Un procedimiento muy frecuente es alinear las agrupaciones de las huellas con respecto a sus puntos singulares (núcleos y deltas). La determinación de los puntos singulares conlleva siempre la estimación previa del campo de orientación local de la estructura de crestas, y el cálculo del índice de Poincaré (Sherlock B. G., 1993) (Karu, 1996) (Kawagoe & Tojo, 1984) (Srinivasan, 1992). Este índice se calcula para cada bloque de imagen del campo de orientación; de manera que, el valor obtenido en cada bloque indica la existencia de un núcleo, una delta o un punto ordinario.

Existen otros métodos de alineamiento, todos ellos con el objetivo común de reducir la carga computacional de la etapa de comparación de minucias. Estos métodos son especialmente apropiados en los casos de identificación, ya que el ordenamiento de las minucias se realiza una sola vez con cada huella, mientras que las comparaciones se realizan tantas veces como patrones contenga la base de datos. En (Jain A. K., Hong, Pankanti, & Bolle, 1997), se exponen un método de comparación de patrones basado en el alineamiento de minucias, y carga computacional muy eficiente. Puesto que la capacidad de discriminación que aporta una minucia es muy pequeña, el método hace uso de información adicional para describir a cada minucia, como puede ser la longitud y la curvatura de las crestas asociadas a las minucias. El reconocimiento se lleva a cabo en dos etapas: en la primera se efectúa el alineamiento, y en la segunda, la comparación. Para efectuar el alineamiento, primero se determinan los parámetros de traslación y rotación existentes entre los dos patrones de puntos. Seguidamente, se alinean las minucias de patrón de entrada con respecto al patrón de la base de datos. A continuación se convierten dichos patrones en sendas cadenas de minucias representándolas en un sistema de coordenadas polares, y ordenándolas según el valor creciente de su coordenada angular. Para efectuar la comparación de cadenas se propone un algoritmo de comparación elástico, con el que evalúa el grado de similitud entre las dos cadenas. El proceso de comparación se realiza mediante la técnica de programación

dinámica, distancia de edición, con la cual se calcula el costo de la transformación de una cadena en la otra. A partir de dicho costo se determina el grado de similitud entre los dos patrones comparados. Como el patrón de minucias de una huella digital es un patrón bidimensional, la transformación del mismo en una cadena de una dimensión puede dar lugar a valores de similitud, durante la comparación, no del todo correctos. Puesto que el orden de colocación de las minucias a la hora de formar las cadenas condiciona significativamente el costo de la operación de conversión de una cadena en la otra, en (Prabhakar, 2000), se propone un método de comparación de patrones bidimensional de minucias mediante programación dinámica 2D, con el objetivo de establecer el máximo número de correspondencias entre minucias.

En (O'Gorman, 1998), se menciona un método de alineamiento de minucias en el que, partiendo de un punto central de la huella, previamente determinado, se hace una exploración en espiral de dentro hacia afuera, ordenando consecutivamente las minucias detectadas. Se obtienen así, unos vectores de características ordenados que permiten una comparación de patrones más eficiente.

Técnicas basadas en la transformada de Hough. En (Ratha, Karus, Chen, & Jain, 1996) (Ballard, 1981) se utiliza esta transformación para el caso de la comparación de patrones de minucias. La transformada de Hough generalizada transforma el problema de la comparación de patrones de puntos en un problema de detección de máximos en el espacio de Hough de los parámetros de transformación. El método busca la mejor transformación posible para que el conjunto de minucias de la huella de entrada se solape con el conjunto de minucias de la huella de la base de datos. Para que dos puntos sean considerados coincidentes deben tener las mismas coordenadas espaciales dentro de unos márgenes de tolerancia, y el mismo ángulo de orientación. El procedimiento permite la coexistencia de puntos no coincidentes. Se hace discreto el conjunto de todas las posibles transformaciones, y para cada transformación se obtiene una puntuación. El espacio de transformaciones está formado por cuádruplas de parámetros del tipo $(s, \theta, \Delta x, \Delta y)$, donde cada parámetro se hace discreto según un conjunto de valores; donde: s, es un factor de escala, Δx y Δy, son las traslaciones en los ejes x e y, respectivamente; y θ, es el ángulo de rotación. El algoritmo se desarrolla en dos fases: en la primera, para cada par de minucias, pertenecientes a los dos patrones que se comparan, se calculan todas las posibles transformaciones que las hacen coincidentes. En la segunda fase, se alinean los dos conjuntos de minucias con los parámetros estimados, y se hace el recuento de todas las parejas de minucias coincidentes dentro de una caja de tolerancia. El valor de la puntuación se escala entre 0 y 99. La transformación cuya puntuación es mayor se toma como la óptima, deduciéndose de ella, el valor de similitud entre los dos patrones comparados. El método proporciona un valor de similitud no muy fiable cuando las huellas contienen un número reducido de minucias, ya que en este caso, resulta difícil acumular suficiente evidencia en el espacio de la transformada de Hough. Tampoco es un método fiable cuando la distorsión de las minucias originadas por la elasticidad de la piel es grande.

Técnicas basadas en grafos. Existen también varios comparadores topológicos basados en grafos (Isenor, 1986). Estos comparadores toleran bien las transformaciones originadas entre los patrones, los errores de posición de las minucias, las minucias espurias y las minucias perdidas. Las características de las huellas, tales como la posición de los núcleos,

la frecuencia de crestas, el número de crestas entre minucias, y toda información de alineamiento, son utilizadas para efectuar las comparaciones.

En (O'Gorman, 1998), se hace mención a una de las primeras técnicas automáticas empleadas para el reconocimiento de patrones de minucias. En ella, cada huella es descompuesta en pequeñas agrupaciones de minucias, generalmente de dos a cuatro minucias. La comparación de patrones se realiza a dos niveles. En uno de ellos, se analizan las disposiciones espaciales de las minucias dentro de las agrupaciones de una misma huella digital, y se comparan con las de otra huella, obteniéndose así, un grado de similitud. En el otro nivel de comparación se analizan y comparan entre sí las configuraciones globales de las diferentes agrupaciones dentro de cada una de las huellas.

Técnicas basadas en la estructura de crestas

A diferencia de la técnica de comparación de minucias, otras técnicas efectúan comparaciones considerando la información completa de toda la estructura de crestas. Así, para efectuar la comparación entre dos huellas digitales calculan la correlación entre sus respectivas imágenes. Estas técnicas reciben el nombre de técnicas de comparación de patrones mediante correlación. El grado de similitud entre dos huellas se basa en que la correlación espacial entre dos imágenes se hace máxima cuando las dos imágenes son idénticas. De esta propiedad se deduce que si dos imágenes proceden de la misma huella cabe esperar que la correlación entre ellas alcance un máximo relativo. Sin embargo en la práctica no es siempre así, ya que pueden darse las siguientes circunstancias:

- Las huellas pueden estar desplazadas entre sí, como consecuencia del proceso de adquisición. Se puede tomar un punto de referencia, como por ejemplo, un núcleo o una delta, para alinear las imágenes antes de efectuar la correlación. El problema se produce cuando dicho punto no aparece en alguna de las imágenes o cuando no se calcula con suficiente precisión.
- Además de la traslación anterior, durante la adquisición de las huellas, puede producirse la rotación de una imagen con respecto a la otra. Al igual que antes, tomando un punto singular como referencia, pueden determinarse los parámetros de traslación y rotación entre las imágenes, para proceder a su alineamiento antes de hacer la correlación. Los problemas que suelen aparecer son los mismos que en el punto anterior.
- Debido a la elasticidad de la piel, se originan sobre la misma, deformaciones no lineales, que impiden el correcto alineamiento de las imágenes, a pesar de estar correctamente determinados los parámetros de traslación y rotación. Este hecho puede disminuir muy significativamente el valor de la correlación entre las imágenes, aún en el caso de tratarse de la misma huella digital.
- La aparición del “ruido” en la imagen puede hacer fracasar el reconocimiento de los patrones, cuando las imágenes no son de buena calidad. Además, dadas dos adquisiciones de una misma huella, son muy frecuentes los siguientes casos:
  a) las calidades de las imágenes son diferentes.
  b) las crestas aparecen delgadas en una imagen y gruesas en la otra, debido a los cambios de presión sobre la superficie del escáner.
  c) las discontinuidades en las crestas son diferentes, debido a la sequedad de la piel.
  d) la región capturada de cada una de las huellas es diferente. En todos ellos, el método de correlación deja de ser un método eficiente.

Técnicas basadas en la información de textura

La comparación de patrones basada en la extracción de minucias no utiliza la información de textura orientada, presente en las crestas. Los sistemas basados en la extracción de textura tienen en cuenta tanto la información global como la información local de las huellas. El algoritmo de extracción de textura se desarrolla en cuatro etapas:

1. Determinación de un punto de referencia y de la región de interés de la huella. El punto de referencia es el punto en el que las crestas presentan su máxima curvatura, y la región de interés es un círculo, de determinado radio, cuyo centro es el punto de referencia.
2. Definición de un mallado sobre la región de interés y normalización en media y varianza.
3. Filtrado de la región de interés según ocho direcciones diferentes utilizando un banco de ocho filtros de Gabor. Con ocho direcciones se captura toda la información local de las crestas de la huella y con cuatro direcciones se captura la información global. Tras este filtrado se obtienen ocho sub-imágenes.
4. Cálculo de la desviación media respecto a la media de grises, en cada sector de cada sub-imagen. Esta desviación se considera como una característica de la huella puesto que cuantifica la estructura de las crestas. Se forma así un vector de características, llamado *fingercode*, que contiene las características de cada sector de la imagen filtrada.

El vector de características así generado es invariante a la traslación de la imagen. Para que sea también invariante a la rotación, se almacenan diez vectores correspondientes a diez rotaciones diferentes de la imagen. A continuación, se calcula la distancia euclidiana entre el vector de características de entrada y los diez vectores de la base de datos almacenados. La mínima de las distancias obtenidas indicará el grado de similitud.

2.4 Reconocimiento basado en minucias

Uno de los puntos claves en cualquier ***proceso de reconocimiento*** es el correcto tratamiento de la información biométrica, para poder extraer las características que nos permitan modelar y comparar con el resto de patrones biométricos con el fin de reconocer al individuo.

El proceso de reconocimiento considera:

- Captura de huellas digitales
- Extracción de características y la generación de un patrón biométrico que permita identificar a cada individuo.
- Comparación de patrones de minucias.

2.4.1 Análisis y representación de huellas digitales

La propiedad estructural más evidente es un patrón de crestas y surcos intercalados, que en una imagen de una huella digital las crestas aparecen oscuras mientras que los surcos claros *Figura 2-11*. El ancho de las crestas varía entre 10µm en crestas muy delgadas, y 300µm en crestas gruesas. Las crestas y surcos por general son paralelas, algunas veces se bifurcan o terminan. Una terminación de cresta es una línea discontinua o bien una línea que llega a su fin en el flujo de crestas y surcos. Por otra parte, una bifurcación es una línea que se divide para dar origen a dos nuevas crestas en la huella digital.

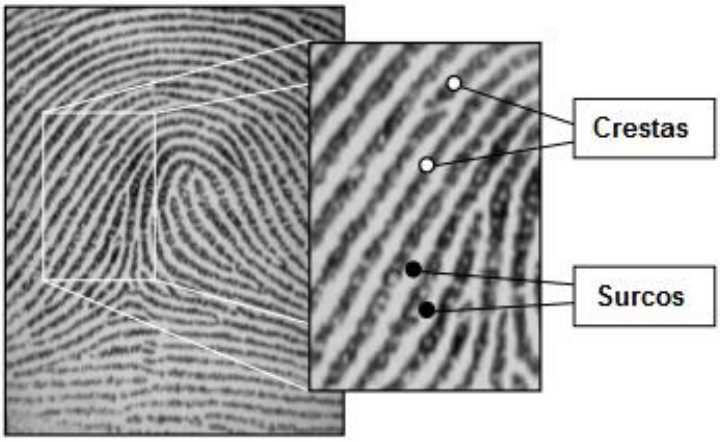


Figura 2-11. *Crestas y surcos en una imagen de huella digital*

Cuando se realiza un análisis a nivel global, los patrones presentan algunas regiones (regiones singulares) donde las líneas de crestas generan formas distintivas (caracterizados por curvaturas pronunciadas, terminaciones frecuentes, etc.), estas regiones pueden ser divididas en tres categorías: *lazo, delta* y *espiral Figura 2-12.* Varios algoritmos de comparación realizan un pre-alineado según un punto de referencia o punto central llamado *Núcleo*. Para aquellas huellas digitales que no poseen regiones singulares (*lazos* y *espirales*) es difícil definir el núcleo, en estos casos el núcleo es generalmente asociado con el punto de máxima curvatura de la línea de cresta. Desafortunadamente, debido a la gran variabilidad de patrones de huellas digitales, es difícil localizar el núcleo en todas las imágenes de huellas digitales. Las regiones singulares, se utilizan generalmente para clasificar huellas digitales, asignando las huellas digitales a algunas de las clases más comunes *Figura 2-13,* permitiendo la simplificación de las búsquedas.

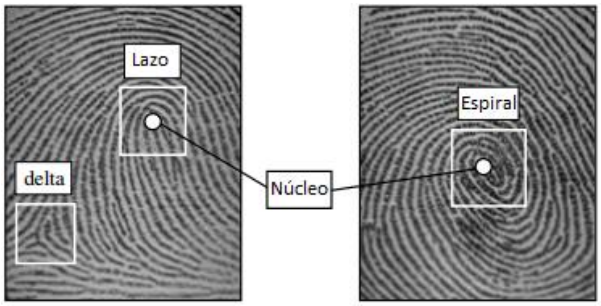


Figura 2-12. *Regiones en una huella digital.*

A nivel local se pueden encontrar, en los patrones de huellas digitales, otras características importantes llamadas minucias y tanto su orientación como su distribución espacial es lo que hace diferente a una huella digital de otra (Maltoni D. , Maio, Jain, & Prabhakar, 2003). En el contexto de las huellas digitales las minucias se refieren a las distintas formas que una cresta es discontinuada. Por ejemplo, cuando una cresta termina repentinamente (terminación) o se divide en dos (bifurcación). A pesar de existir

varios tipos de minucias, solo se consideran algunas para el reconocimiento automático. El Instituto Nacional de Estándares (ANSI), propone una taxonomía de minucias basada en cuatro clases: *terminaciones, bifurcaciones, trifurcaciones* y *minucias indefinidas.* El modelo de coordenadas y minucias del FBI, solo considera dos: *terminaciones* y *bifurcaciones*, donde cada minucia se denota por su clase, coordenadas (x, y), y ángulo entre la tangente a la línea de cresta y el eje horizontal *Figura 2-14*.

Figura 2-13. *Clases más comunes de huellas digitales.*

.

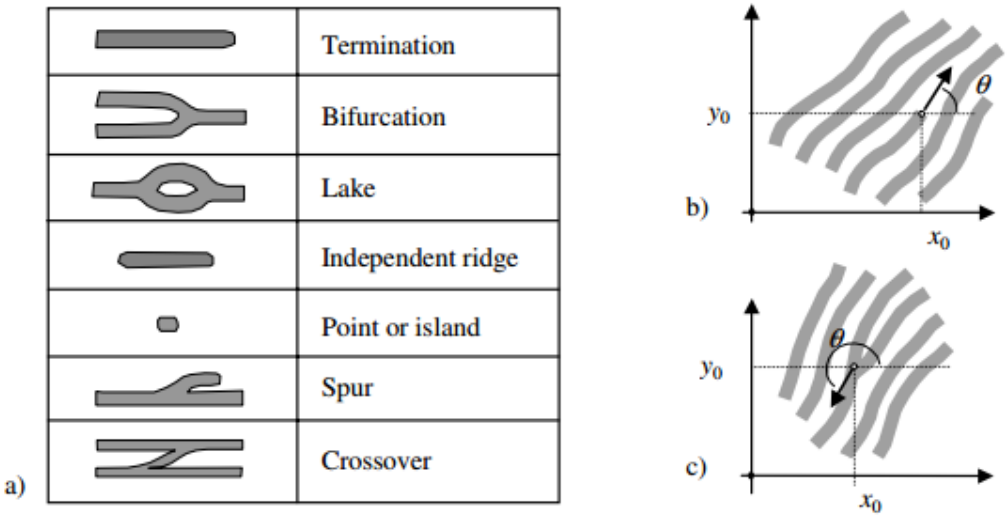


Figura 2-14. *Tipos de minucias y modelo de coordenadas*

Otra característica, denominada dualidad terminación/bifurcación, es la relación existente entre las minucias terminación y bifurcación, donde toda terminación puede ser vista como bifurcación y viceversa. Por ejemplo, en la *Figura 2-15 a);* se muestra una porción de una imagen de huella digital donde las líneas de cresta aparecen en tono oscuro sobre un fondo claro, se muestran dos terminaciones (1, 2) y una bifurcación (3). En la imagen negativa *Figura 2-15 b)* las correspondientes minucias toman la misma posición pero su tipo es intercambiado.

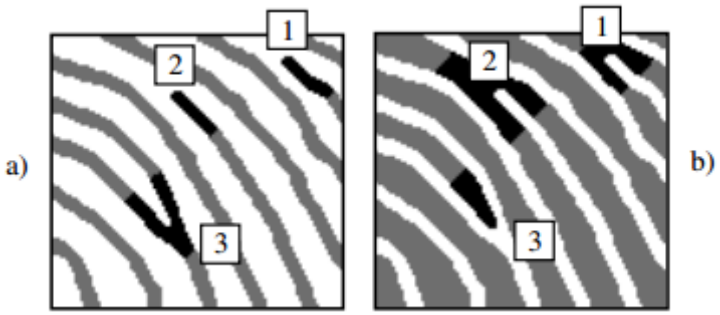


Figura 2-15. *Dualidad terminación/bifurcación.*

La superficie de las huellas digitales está formada por un sistema de crestas y surcos que sirven como superficie de fricción en el momento de tomar objetos. Denominamos indistintamente a surcos o valles a las líneas determinadas por las profundidades observables en una huella digital, y llamamos crestas o picos a las líneas de la huella digital determinada por las altitudes en la huellas.

La superficie exhibe información estructural muy rica de información cuando se la examina como una imagen. Las imágenes de huellas digitales pueden ser representadas como características globales así también como características locales *Figura 2-16*. Las características globales incluyen la distancia entre las líneas de las crestas, orientación de las crestas y puntos singulares como *núcleo* (*core)* y *delta*. Los puntos singulares tienen una gran importancia desde el punto de vista de clasificación de las huellas digitales. Sin embargo la verificación generalmente utiliza exclusivamente características locales llamadas minucias determinadas por discontinuidades de las líneas de la superficie de una huella digital. Hay alrededor de 18 tipos distintos de minucias que incluyen líneas, bifurcaciones, islas, cruces etc. Sin embargo las terminaciones de líneas y bifurcaciones son los tipos de minucias comúnmente utilizados en los procesos de verificación.

Una terminación de línea ocurre cuando el flujo de una línea termina abruptamente y una bifurcación es determinada cuando se da una división en la línea de la superficie de la huella digital. Al hablar de líneas nos referimos al flujo de crestas o de surcos que determinan la estructura de una huella digital, es indistinto hablar de una línea de crestas o una línea de surcos ya que las minucias encontradas en una huella digital proveniente de una línea de crestas son las mismas a las que se encuentran trabajando la imagen con su correspondiente línea de surcos, la única diferencia radica en que el tipo de minucias encontradas resulta ser exactamente la opuesta. Las características globales no poseen

suficiente poder discriminativo por si solas, es por eso que comúnmente se utilizan para clasificar el tipo de huella digital en lugar de verificar.

Clasificación de huellas digitales. La clasificación de huellas digitales se realiza normalmente en aquellos sistemas de identificación que manejan grandes bases de datos, con el fin de limitar en lo posible el campo de búsqueda de las huellas que se desean reconocer (Kawagoe & Tojo, 1984) (Fitz & Green, 1996) (Karu, 1996) (Maltoni & Maio, 1996) (Jain, Prabhakar, & Hong, 1999). Dicha clasificación se basa en la particular distribución de las crestas y surcos de la huella digital en la zona central de la imagen. Las configuraciones características que ahí aparecen, presentan cierta variabilidad dentro de la misma clase; sin embargo, tales variaciones son lo suficientemente pequeñas como para permitir establecer reglas sistemáticas de clasificación.

Figura 2-16. *Características globales y locales de una huella digital*

Puntos singulares de la estructura de crestas de una huella. En la clasificación de patrones de huella digital, solamente resulta de interés una zona de la imagen, que es la que se toma como patrón. El *área patrón* de una huella está formada por todas aquellas crestas y surcos circunscritos entre dos crestas llamadas crestas de referencia. Estas crestas se definen como las dos crestas divergentes más internas de la estructura de la imagen que circunscriben la zona central de la huella *Figura 2-17*. Considerando solamente las áreas patrón de las huellas, se definen dos tipos de puntos singulares, llamados *deltas* y *núcleos.* Resulta difícil definir el concepto de delta y núcleo, si bien existen criterios para determinar sus coordenadas de forma automática (Karu, 1996) (Ratha, Karus, Chen, & Jain, 1996).

- **Delta**. El punto delta, también conocido como punto singular externo, se define como el punto más próximo al centro geométrico en el que tiene lugar la divergencia de las dos crestas de referencia. Puede tratarse de un punto perteneciente a un final de cresta, de un punto a partir del cual se produce una bifurcación de crestas, o de un punto perteneciente al valle en el que se produce la divergencia de las crestas de referencia *Figura 2-18*.
- **Núcleo**. El núcleo o punto singular interno, se define como el punto situado sobre las crestas curvas más internas de la estructura. Debido a las diferentes estructuras de

crestas curvas existentes, las reglas para seleccionar la posición del núcleo son muy complejas. En la *Figura 2-18* pueden observarse varios ejemplos de núcleos.

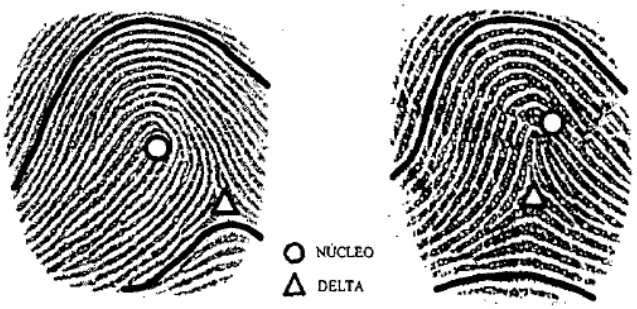


Figura 2-17. *Dos ejemplos de área patrón de una huella digital y sus correspondientes crestas de referencia*

- Computo de crestas. Al igual que en el ámbito forense, un parámetro importante para establecer la clasificación automática de huellas digitales es el computo de crestas entre puntos singulares. Es decir, el cómputo del número de crestas que cruzan la línea imaginaria que une una delta con un núcleo. Al igual que antes debido a la complejidad en la configuración de las crestas, resulta difícil establecer un criterio para realizar el cómputo preciso de crestas.

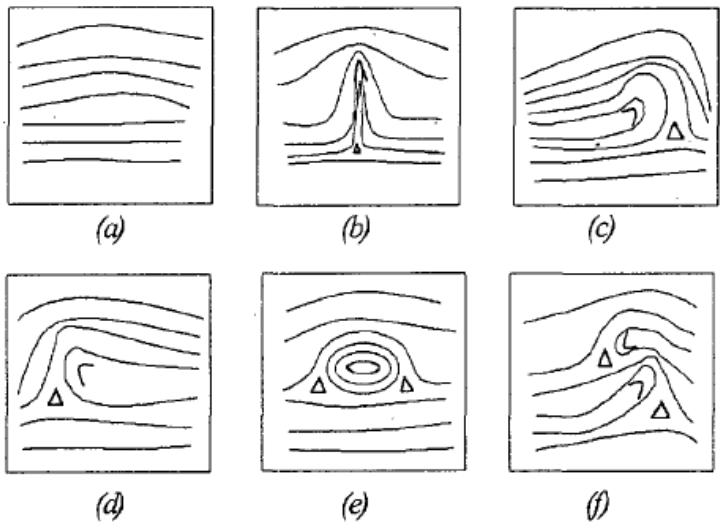


Figura 2-18. *Disposición de núcleos y deltas en las diferentes clases de huellas. (a) Arco; (b) Arco Tensado; (c) Lazo Izquierdo; (d) Lazo Derecho; (e) Rizo; (f) Doble Rizo.*

Problemas en la clasificación. Dada la gran variedad de configuraciones existentes en la estructura de crestas de las huellas digitales, la elección de criterios universales para su clasificación sigue siendo hoy día un problema muy complejo, tanto a nivel humano como a

nivel automático. Las dificultades que pueden aparecer a la hora de establecer la clasificación se acentúan más, debido a la pequeña variabilidad inter-clase y a la gran variabilidad intra-clase que presentan las huellas digitales. Así, es muy frecuente que diferentes huellas parezcan de la misma clase sin realmente serlo (baja inter-variabilidad). Sin embargo, huellas que son de la misma clase, en muchas ocasiones presentan características muy diferentes (alta intra-variabilidad). Por otra parte, el ruido presente en muchas imágenes y la baja calidad de las imágenes adquiridas, dificulta todavía más la toma de decisiones.

La práctica por inspección visual requiere de mucha experiencia para llegar a unos criterios de clasificación aceptables. La principal dificultad es la de definir, de manera precisa e inequívoca, a cada una de las clases. El número de clases que se ha establecido para la clasificación automática es relativamente pequeño, y además, en la práctica, la distribución de las huellas en estas clases no está siempre clara.

Técnicas de clasificación. A pesar de ser la clasificación de huellas digitales uno de los problemas más representativos del reconocimiento de patrones, y a pesar del gran interés demostrado por la comunidad científica en este tema, durante los últimos 30 años, son pocas las características extraídas de las huellas, que han sido empleadas por las diferentes técnicas. De hecho, casi todas ellas utilizan una o más de las siguientes características:

- Flujo de líneas de cresta. Son líneas que fluyen paralelas a las líneas de cresta, sin necesidad de que exista coincidencia con ellas ni con los surcos. El único requisito es que estas líneas mantengan la orientación local de la estructura de crestas, por lo que generalmente se dibujan a partir de la información que aporta el campo de orientación.
- Campo de orientación. Es una de las características de la imagen utilizada por la mayoría de las técnicas, ya que contiene toda la información necesaria para poder efectuar la clasificación y, además, puede calcularse con suficiente precisión.
- Puntos singulares. Se determinan analizando el campo de orientación. Existen varias aproximaciones para determinar la localización de estos puntos con exactitud (Kawagoe & Tojo, 1984) (Ratha, Karus, Chen, & Jain, 1996) (Maltoni D. , Maio, Jain, & Prabhakar, 2003).
- Respuesta a filtros de Gabor. El filtrado de la estructura de crestas con filtros localmente orientados de Gabor, puede proporcionar información de textura útil para la clasificación.

Las técnicas de clasificación de huellas digitales pueden dividirse en:

- Técnicas basadas en reglas: establecen la clasificación de las huellas a partir del número de puntos singulares que presentan y su distribución espacial.
- Técnicas estructurales: estos esquemas se basan en la representación de las características de bajo nivel mediante estructuras de alto nivel.
- Técnicas estadísticas: en este caso, los vectores de características, de longitud fija, extraídos de cada huella digital son clasificados estadísticamente.
- Técnicas basadas en redes neuronales: la mayoría de estos métodos se basan en el empleo de perceptores multicapa y vectores de características derivados del campo de orientación.
- Técnicas basadas en múltiples clasificadores: representan la tendencia actual de los sistemas de clasificación de huellas digitales.

2.4.2 Captura de huellas digitales

Tradicionalmente las huellas digitales se adquieren al transferir una impresión de tinta de una huella digital al papel. Este proceso es denominado adquisición *off-line*. Los sistemas de autenticación existentes están basados en dispositivos que realizan la adquisición de la imagen de la huella digital en tiempo real, este proceso es denominado *live-scan*.

2.4.2.1 Adquisición de huellas digitales

La forma en la que se realiza el proceso de captura de huellas digitales es muy diferente, dependiendo del tipo de aplicación biométrica en la que se van a procesar las imágenes obtenidas. El método tradicional de adquisición de huellas digitales tintadas ha tenido siempre, y sigue teniendo lugar, en el ámbito judicial y forense. Actualmente, los sistemas automáticos de reconocimiento de huellas digitales tienen también aplicación en otros contextos, como por ejemplo, los sistemas de acceso a entornos de seguridad, donde los requisitos de funcionamiento y exigencias de la aplicación, obligan al uso de técnicas on-line. En estos casos, las huellas son capturadas a través de dispositivos de adquisición electrónicos. El esquema general de estos dispositivos comprende las siguientes partes: (i) sensor de lectura, encargado de capturar la imagen de la huella; (ii) conversor analógico/digital, encargado de convertir la imagen analógica entregada por el sensor en una señal digital; (iii) interfaz de comunicaciones con otros dispositivos externos (por ejemplo, una pc). Dependiendo del principio físico de funcionamiento del sensor, se definen los diferentes tipos: óptico, de estado sólido y ultrasónico.

Características de las imágenes. La imagen de una huella digital reproduce el patrón de crestas y surcos de la epidermis, y normalmente es adquirida cuando se coloca la yema del dedo sobre la superficie sensible del escáner. El grosor de las crestas oscila entre 100 y 300 µm, y el periodo espacial de repetición de crestas suele ser de aproximadamente 500 µm, generalmente las heridas producidas en la piel, como por ejemplo, las quemaduras superficiales, las abrasiones o los cortes, no afectan a la estructura de crestas, ya que los daños producidos son restaurados con el crecimiento de la nueva piel. En estas condiciones, puede afirmarse que los patrones representados por las imágenes adquiridas contienen toda la información biométrica necesaria, y estable en el tiempo, para poder reconocer de forma automática a un individuo. Las características que presentan las imágenes digitales proporcionadas por un escáner de huella digital son:

- **Resolución**: dependiendo del tipo de dispositivo de captura empleado, la resolución de las imágenes obtenidas varia, desde 250 dpi hasta 625 dpi., siendo un estándar la resolución de 500 dpi. El valor de 250 dpi es la resolución mínima que permite efectuar con precisión la extracción de puntos característicos (minucias) de la estructura de crestas de una huella digital.
- **Área de captura**: es el tamaño de la superficie sensible del escáner. Cuanto mayor es el área de captura del sensor, mayor es la zona del dedo que puede adquirirse y, por tanto, mayor es el número de características identificadas que pueden obtenerse. La impresión completa de la yema del dedo implica, generalmente, un área de captura de 1 a 1.25 pulgadas (6.5 a 10.1 cm^2). La tendencia a reducir el tamaño de los dispositivos de captura en algunas aplicaciones conlleva también la necesaria reducción del tamaño de los sensores. El tamaño más pequeño que permite la extracción de un numero de características suficientemente identificativo es de 0.5 pulgadas (1.6 cm^2). En estos

casos, la aparición de un elevado grado de variabilidad intra-clase puede empeorar el funcionamiento del sistema de reconocimiento, debido a un aumento del número de falsos rechazos.

- **Número de píxeles**: conocidas, la resolución R en dpi, y el área de captura del sensor A x B (alto x ancho) en pulgadas cuadradas, el número de pixeles viene dado por: RA x RB pixeles.
- **Rango dinámico**: es el número de valores posibles de luminancia de la imagen y está relacionado con el número de bits utilizados para codificar la luminancia de cada pixel. El color no aporta información al reconocimiento por lo que no se adquiere. El estándar actual es el de representar las imágenes capturadas en escala de grises de 8 bits/pixel, lo que supone un rango dinámico de 0 a 255.

En la *Figura 2-19* se muestra el aspecto físico que presentan los escáneres de Digital Persona.

Figura 2-19. *Escáneres Digital Persona*

Adquisición de huella off-line. Con esta técnica, la adquisición se efectúa imprimiendo directamente la huella del dedo sobre papel. Para ello, se extiende uniformemente unas gotas de tinta sobre una tableta plana. La piel queda impregnada al hacer rodar la yema del dedo sobre la superficie, de izquierda a derecha. A continuación, se hace rodar de nuevo el dedo sobre un papel blanco para que el patrón de crestas quede definitivamente impreso. Este procedimiento ha sido el empleado tradicionalmente en la captura de huellas digitales. Tiene el inconveniente de presentar deformaciones en la estructura de crestas, originadas por el propio procedimiento de adquisición. También puede imprimirse la huella sobre el papel sin hacer rodar el dedo. La imagen obtenida es más pequeña pero, generalmente, presenta menor grado de distorsión. Una vez adquirida la huella, puede capturarse y digitalizarse por medio de un escáner óptico o una cámara de video. En cualquier caso, en un contexto de reconocimiento automático, el proceso completo resulta muy incómodo y lento, y además, requiere de cierta habilidad.

Adquisición de huellas on-line. Las huellas on-line, se obtienen mediante la adquisición directa de la huella digital al colocar el dedo sobre la superficie sensible del sensor electrónico. El procedimiento de conversión de la huella capturada en una imagen digital

depende de los principios físicos de funcionamiento del sensor utilizado. Atendiendo a estos principios físicos, puede establecerse la siguiente clasificación de sensores:

- **Sensores ópticos**. Entre estos sensores están aquellos que se basan en la reflexión de la luz sobre la yema del dedo (*FTIR, Frustrated Total Internal Reflection*), los sensores basados en fibra óptica, los electro-ópticos y los sensores sin contacto.
- **Sensores de estado sólido**. A este grupo pertenecen los sensores capacitivos, térmicos, de campo eléctrico y piezoeléctrico.
- **Sensores ultrasónicos**.

Los objetivos comunes a todas las técnicas de adquisición son: (i) la reducción del costo económico del dispositivo; (ii) la reducción del tamaño del sensor; (iii) la mejora de la calidad de imagen; (iv) el aumento de la resolución; y (v) la reducción de la distorsión generada por el propio procedimiento de captura.

Por ejemplo, los dispositivos de estado sólido permiten cierta funcionalidad que no proporcionan los dispositivos ópticos: el control automático de ganancia y el control del sensor por programa. La ganancia en la mayoría de los captadores ópticos solo puede variarse manualmente para cambiar la calidad de la imagen. Los dispositivos de estado sólido permiten modificar la sensibilidad de determinadas zonas del sensor para controlar la calidad. Pueden combinar el control automático de ganancia con la realimentación para conseguir altas calidades de imagen. Por ejemplo, en estos dispositivos es frecuente el bajo contraste de la imagen originada cuando la piel del dedo está muy seca. Como consecuencia, puede aumentarse la sensibilidad, para que en una segunda adquisición, se mejore la calidad. También puede aumentarse localmente la sensibilidad de determinados pixeles del sensor, cuando se detecta que la presión ejercida en determinadas zonas de su superficie origina un bajo contraste en la imagen.

Los sensores ópticos tienen la ventaja de proporcionar imágenes de gran tamaño. Resulta muy caro fabricar captadores de estado sólido de grandes dimensiones. La posible necesidad de sensores ópticos de reducido tamaño conlleva también la reducción del tamaño de la imagen adquirida al disminuirse la distancia focal. Además, la combinación escáner pequeño imagen grande origina siempre distorsión geométrica de la imagen en los bordes, debido a que el plano de reflexión de la luz no es paralelo al plano del receptor.

A continuación se hace una breve descripción de las técnicas de captura de huellas de acuerdo a la clasificación anteriormente mencionada.

Sensores ópticos

- *Sensores basados en FTIR*. (Karen, 1989) La técnica de captura FTIR es la más antigua y también la más utilizada. En el momento en el que el dedo se apoya sobre la superficie de cristal del sensor (prisma), un diodo LED proyecta un haz de luz difusa por debajo del cristal. La luz que atraviesa el prisma e incide sobre las crestas de la huella se dispersa, reflejándose de manera aleatoria en múltiples direcciones. La luz que incide en el interior de la estructura de crestas (surcos) se refleja en una determinada dirección (reflexión total). Esta luz direccional es focalizada mediante un sistema de lentes hacia un dispositivo CCD o CMOS, capturándose así la imagen de la huella digital. Recientemente, se ha desarrollado una variante de esta técnica en la que se sustituye el prisma de cristal por una lámina de pequeños prismas distribuidos a lo largo de la

superficie sensible. La calidad de las imágenes adquiridas es ligeramente menor, pero tiene la ventaja de que el tamaño del dispositivo se reduce significativamente (Xia & O'Gorman, 2003).

- *Sensores basados en fibra óptica*. En este caso, los sensores disponen de una distribución bidimensional de fibras ópticas que hacen incidir, perpendicularmente, un haz de luz por debajo de la superficie del cristal sobre la que se apoya el dedo (O'Gorman, 1998). La luz reflejada incide sobre un CCD/CMOS que, directamente acoplado a la superficie de fibras, obtiene la imagen de la huella. También pueden utilizarse conjuntos de micro prismas dispuestos sobre una superficie plana y elástica. Las diferencias de presión ejercidas por las crestas y surcos de la huella modifican de diferente manera la superficie de micro prismas, capturándose la imagen a partir de las diferencias de intensidad de luz reflejada por estos. El aumento del tamaño del CCD, asociado al aumento del área capturada, incrementa notablemente el costo de estos dispositivos.
- *Sensores electro-ópticos*. Estos sensores están formados por dos capas. La primera está compuesta por un polímero que, debidamente polarizado, emite luz de intensidad proporcional al voltaje aplicado en una de sus caras. La colocación del dedo sobre la cara opuesta da lugar a diferencias de potencial entre crestas y surcos, originando como consecuencia diferencias de emisión de luz. La segunda capa está formada por fotodiodos distribuidos a lo largo de toda la superficie, que en contacto con ésta, capturan la luz procedente de la primera capa y proporcionan la imagen digital de la huella.
- *Sensores sin contacto*. En este grupo se engloban las técnicas de captura con cámara, en las que no se produce el contacto físico entre dedos y sensor. Tienen la ventaja de no introducir en la imagen la distorsión elástica, tan frecuente en las técnicas de contacto. EL principal inconveniente es la dificultad de obtener imágenes bien enfocadas y contrastadas.

Sensores de estado sólido

Los sensores de estado sólido fueron desarrollados en los años 80, si bien no han comenzado a utilizarse comercialmente hasta mediados de los 90. Presentan la ventaja de no necesitar ningún componente óptico ni CCD/CMOS. Atendiendo a la forma de conversión de la información física en señal eléctrica, se distinguen cuatro tipos de sensores:

- *Sensores capacitivos*. Estos dispositivos se forman por la distribución de un conjunto de micro capacitores (aproximadamente 10 a la cuarta potencia) en una superficie plana, sobre la cual se extiende un dieléctrico. Todas las placas conductoras a un lado del dieléctrico forman eléctricamente el mismo punto. El conjunto va integrado en un único chip. Las placas necesarias para completar los capacitores aparecen al otro lado del dieléctrico cuando se coloca el dedo sobre la superficie. La medida del voltaje en estos capacitores determina la imagen de la huella digital, puesto que dicho valor depende de la distancia entre placas. Los capacitores formados por las crestas de la huella presenta mayor tensión eléctrica, al estar estas más próximas a la superficie que los surcos. La superficie en contacto con el dedo precisa de una fina capa protectora con toma de tierra, resistente a la abrasión y a las posibles descargas electrostáticas de la piel. Estos sensores permiten el ajuste de algunos parámetros eléctricos con el fin de mejorar la

calidad de la imagen adquirida cuando las condiciones de la piel no son las ideales (piel seca o húmeda). Presentan el inconveniente de que deben limpiarse a menudo, ya que la grasa y la suciedad empeoran notablemente la calidad de imagen.

- *Sensores térmicos*. Estos sensores están construidos con materiales termo-eléctricos capaces de crear corrientes a partir de diferencias de temperatura. El sensor se mantiene eléctricamente a alta temperatura, comparada con la del dedo, con el fin de crear diferencias térmicas significativas. La imagen de la estructura de crestas se forma cuando el contacto de las crestas y surcos de la huella con la superficie del sensor origina diferencias de temperatura. Las diferencias originadas por las crestas son menores que las originadas por los surcos, al estar estos más alejados del sensor. La imagen térmica formada desaparece rápidamente, una vez que el dedo entra en contacto con el sensor, debido a que el equilibrio térmico se alcanza muy rápidamente. Por este motivo, estos sensores se emplean en combinación con técnicas de barrido, en la que la adquisición se realiza deslizando el dedo sobre una ranura abierta, térmicamente sensible. Tienen la ventaja de no ser sensibles a las descargas electrostáticas y de poder utilizar gruesas capas protectoras, ya que la información térmica se propaga fácilmente a lo largo de ellas.
- *Sensores de campo eléctrico*. Estos dispositivos están formados por un anillo emisor de señal sinusoidal de baja potencia, bajo el cual se distribuye una matriz de pequeñas antenas receptoras. La amplitud de señal recibida por cada antena se modifica al producirse el contacto del dedo con el escáner, pudiendo, a partir de esta información, diferenciarse el patrón de crestas y surcos. La dermis de la piel es la capa causante de los cambios de amplitud en la señal.
- *Sensores piezoeléctricos*. La superficie de estos dispositivos es sensible a la presión ejercida durante el contacto dedo-sensor. Esta superficie está compuesta por un material elástico, de naturaleza piezoeléctrica, que proporciona las características topográficas del relieve de la huella digital al convertir las diferencias de presión en diferencias de tensión eléctrica. Presentan el inconveniente de no ser muy sensibles a las pequeñas diferencias de relieve que pueden darse en el patrón de crestas y surcos; sensibilidad que se ve aún más reducida por la cubierta protectora. Además, la imagen entregada por el sensor es binaria, lo que supone una pérdida muy significativa de información.

Sensores ultrasónicos

Las técnicas ultrasónicas empleadas en estos sensores son capaces de obtener imágenes muy claras de las huellas, aún en el caso de que la estructura de crestas parezca dañada a simple vista. Esto se consigue explorando la superficie de contacto mediante la proyección, sobre la misma, de pulsos ultrasónicos; de forma similar a como lo hace el haz láser en los dispositivos ópticos. En este caso, el eco reflejado por la superficie del dedo permite determinar la profundidad del relieve formado por los surcos y crestas. Este método de exploración presenta la ventaja de ser menos susceptible a la suciedad, al sudor o a la grasa de la piel, por lo que las imágenes obtenidas son más fiables. Los inconvenientes son: el tamaño del dispositivo, su elevado costo, y el proceso de adquisición requiere de cierto tiempo. No es, por tanto, una técnica actualmente muy extendida.

2.4.2.2 Imágenes de huellas digitales

Los principales parámetros que caracterizan a una imagen de una huella digital, son:

- **Resolución**: Indica el número de puntos o pixeles por pulgada (dpi – pixels per inch). En Imágenes de baja resolución, es más difícil detectar las crestas y surcos y aislar las minucias de la huella digital *Figura 2-20*. Imágenes adquiridas con resolución entre 200 y 300 dpi, aún pueden ser procesadas con técnicas de correlación de pixeles.
- **Area**: el tamaño del área rectangular capturada por el escáner de huella digital es un parámetro fundamental. A mayor área, mas crestas y surcos son capturados y más distintiva es la imagen de la huella digital.
- **Nuemro de pixeles**: el número de pixeles en una imagen de huella digital puede ser derivado por la resolución y área de la imagen. Un escáner trabajando a *r* dpi sobre un área de *altura (h)* x *ancho (w)*, tiene *rh x rw* pixeles. Por ejemplo, un escáner que trabaja a 500 dpi sobre una área de 20,32 x 15,24 mm2, produce imágenes de 500 (20,32/25,4) x 500(15,24/25,4) = 400 x 300 pixeles.
- **Rango dinamico (profundidad)**: representa el numero de bits usados para codificar la intensidad de cada pixel. Informacion de color no es considerado importante para el reconocimiento de huellas digitales, por lo que la mayoria de los escaneres adquieren imágenes en escala de grises. El estandar establecido por el FBI, es de imágenes de 8 bits de profundidad, que produce 256 niveles de grises. Actualmente, algunos sensores capturan solo 2 o 3 bits y se ajustan al rango dinamico de 8 bits por software.
- **Precisión geométrica**: es usualmente especificado por la máxima distorsión geométrica introducido por el dispositivo de adquisición. La mayoría de los escáneres ópticos introducen una distorsión geométrica, la cual si no es compensada, altera el patrón de la huella digital dependiendo de la posición relativa del dedo en la superficie del sensor.
- **Calidad de la imagen**: no es fácil definir precisamente la calidad de una imagen de huella digital, y es incluso más difícil separar la calidad de la imagen de huella digital de la calidad intrínseca del dedo. De hecho, cuando las crestas de los dedos están gastadas (especialmente trabajadores que realizan tareas manuales o personas de avanzada edad), cuando los dedos están húmedos o secos, la mayoría de los escáneres producen imágenes de mala calidad.

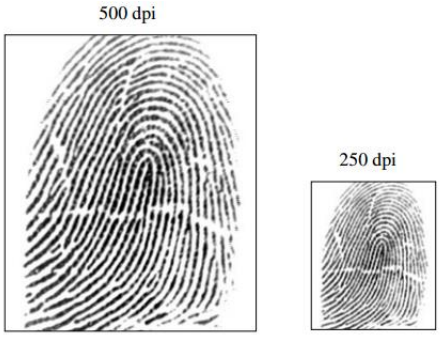


Figura 2-20. *Distintas resoluciones de una huella digital*

2.4.3 Extracción de características

La extracción de características de una huella digital tiene como objetivo la generación de un patrón biométrico que permita identificar a cada individuo de una manera fiable, incluso cuando las condiciones de adquisición de las imágenes no sean las óptimas. En este sentido, la etapa de mejora de la calidad de imagen determina el funcionamiento global del sistema de reconocimiento. A continuación se hace una revisión de las técnicas empleadas para la mejora de la calidad de imagen, con el objetivo de reconstruir la estructura de crestas y separarla del ruido de fondo.

2.4.3.1 Procesado para la mejora de la calidad de imagen

El objetivo de esta etapa de procesado es el de proporcionar una imagen de la huella digital, cuyo grado de calidad permita la extracción precisa y fiable de las características biométricas. Son numerosas las referencias que aparecen en la literatura con este propósito; entre ellas: (Election, 1973) (Knutsson, Wilson, & Granlund, 1983) (Mehtre, Murthy, & Kapoor, 1987) (Xiao & Raafat, 1991) (Hung, 1993) (Ratha N. C., 1995) (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Simon Zorita, Ortega Garcia, & Cruz Llanas, 2001).

Uno de los patrones biométricos de huella digital más utilizados, por su elevada fiabilidad, es el *patrón de minucias* (Ratha N. C., 1995) (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Maio, 1997) (Jain, Ross, & Prabhakar, 2001). Recibe el nombre de *minucia* cualquier punto de la imagen que indica que una determinada cresta presenta un final/comienzo o una bifurcación. Una minucia estará determinada, por tanto, por sus coordenadas espaciales dentro de la imagen. Generalmente, los patrones biométricos están constituidos por las coordenadas espaciales de cada minucia, los ángulos de orientación de las crestas asociadas a las misma (una minucia pertenece siempre a una cresta).

En la mayoría de las ocasiones, la calidad de las imágenes proporcionadas por los sensores en la etapa de adquisición de las huellas digitales no es suficiente para garantizar la correcta extracción de sus características biométricas. Lo mismo puede decirse en el caso de las huellas impresas con tinta sobre papel. Los motivos de esta baja calidad son: el estado de la piel (humedad, sequedad, grietas, arrugas), el ruido del sensor, la presión excesiva o insuficiente del dedo sobre el sensor, el deterioro de la piel por el tipo de trabajo, edad, etc. Generalmente, aparece ruido de fondo en la imagen, el contraste y el brillo de la misma no siempre son uniformes, ni en muchas ocasiones es el adecuado; también es frecuente la aparición de manchas, de zonas de pérdida o zonas de sobreexposición de la imagen. Desde el punto de vista del deterioro producido en la estructura de crestas, estos defectos de calidad se traducen en:

- La aparición de discontinuidades a lo largo de las líneas que definen las crestas.
- La aparición de discontinuidades transversales a dos o más líneas de crestas.
- La falta de paralelismo entre las crestas. La presencia de ruido puede provocar la falsa unión de crestas entre sí (conexión de crestas y/o empastamiento de crestas).

Como consecuencia de todas las imperfecciones derivadas de la baja calidad de las imágenes, las minucias detectadas por los algoritmos de extracción de características pueden no coincidir con las minucias reales, ya que se produce:

- La pérdida de determinadas minucias presentes en la estructura de crestas (minucias borradas o eliminadas).
- La inserción de minucias falsas, no presentes en la estructura de crestas (minucias espurias).
- Error en la determinación de las coordenadas de las minucias y sus orientaciones en la imagen.

En estas circunstancias, el funcionamiento del sistema de reconocimiento empeora notablemente, ya que las comparaciones entre los patrones de entrada y los patrones almacenados originan un aumento de los errores de falsa aceptación y falso rechazo. El intento de mejorar estas tasas de funcionamiento justifica el empleo de una etapa de procesado, previa a la etapa de extracción de características, para situar el nivel de calidad de las imágenes de entrada dentro de unos límites que aseguren la correcta extracción de minucias. No obstante, esta etapa es un proceso relativamente largo comparado con el proceso completo de generación del patrón biométrico desde que la imagen ha sido adquirida. La eliminación de la mejora de imagen o el empleo de algoritmos más rápidos pero menos eficientes, con el fin de reducir la carga computacional del sistema, tiene como consecuencia el aumento de las tasas de funcionamiento. Generalmente, se busca un valor de compromiso entre el tiempo de respuesta y las tasas de funcionamiento del sistema.

Extracción de la estructura de crestas. Las técnicas más utilizadas para la mejora de imagen se basan en el empleo de filtros adaptativos (o filtros de contexto), cuyo objetivo es el de proporcionar, a partir de la imagen de entrada, una estructura de crestas lo más precisa y fiable posible desde el punto de vista de la extracción de características. Este tipo de filtrado supone la adaptación de las características del filtro dependiendo del contexto local de la imagen. El análisis de la estructura de la imagen de una huella digital evidencia una de las propiedades más importantes en las que se basan las técnicas de mejora de imagen; y es que las crestas y surcos fluyen localmente paralelos. Por tanto, el contexto suele definirse a partir de la orientación local y de la frecuencia local de las crestas de la imagen.

Existen diferentes funciones para definir al filtro extractor de crestas: funciones de Gauss, de Gabor, etc. (Xiao & Raafat, 1991) (Hung, 1993) (Jain A. K., Hong, Pankanti, Sharath, & Bolle, 1996) (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Hong & Jain, 1998) (Jain & Pankanti, 2001) (Simon Zorita, Ortega Garcia, & Cruz Llanas, 2001). Sintonizando adecuadamente el filtro elegido en función del contexto, se reduce el ruido de fondo y se incrementa la definición de las crestas y surcos de la estructura. Esto es debido a los siguientes efectos:

- EL efecto de promediado (filtrado paso bajo) en la dirección de las crestas, que elimina las pequeñas discontinuidades que suelen aparecer a lo largo del flujo de líneas, y las pequeñas estructuras espurias originadas por los poros de la epidermis y el ruido de fondo.
- El efecto de filtrado paso banda (diferenciación) en la dirección ortogonal a las líneas de cresta, que aumenta la discriminación entre crestas y surcos, y separa las posibles uniones de crestas que puedan haberse producido en dicha dirección (empastado de crestas). Al mismo tiempo, se reduce gran parte de ruido de la

imagen, ya que toda componente de ruido que no está orientada en la misma dirección que la máscara es también eliminada.

Parámetros de control de los filtros de extracción de crestas. El número de parámetros empleados para definir los filtros localmente adaptativos varía dependiendo de la técnica utilizada. Los más utilizados son:

- Ángulo de orientación local de las crestas. El análisis local de la imagen a nivel bloques, de tamaño previamente definido, permite hacer una estimación precisa de los ángulos de orientación del flujo de crestas. Los ángulos así obtenidos determinan el llamado campo de orientación local de la huella digital (Bigun J., 1987) (O´Gorman L., 1989) (Rao, 1990) (Bigun, 1991) (Ratha N. C., 1995) (Karu, 1996) (Ratha, Karus, Chen, & Jain, 1996) (Jain A. K., Hong, Pankanti, & Bolle, 1997) (Hong L. W., 1998).
- Frecuencia local de crestas y surcos. A nivel local, los niveles de gris a lo largo de las crestas y valles, varían aproximadamente de forma sinusoidal en la dirección ortogonal a la dirección de las crestas. Haciendo uso de esta característica, se propone un método para determinar la frecuencia local de crestas, analizando la imagen en bloques de 16x16 pixeles.
- Anchura entre crestas. Aunque es un parámetro directamente relacionado con el anterior, algunas técnicas de mejora de imagen hacen uso de él, puesto que permite el ajuste local de las máscaras de los filtros a la anchura de las crestas, proporcionando así, un mayor realce de los bordes a lo largo de toda la estructura. La explicación detallada de un método para extraer este parámetro puede encontrarse en (O´Gorman L., 1989) (Hong L. W., 1998).

Dentro de las técnicas de extracción de crestas encontramos las siguientes a destacar:

- Análisis Orientado: es uno de los primeros métodos de mejora de imagen de huellas digitales que hicieron uso de los filtros de contexto (O´Gorman L., 1989).
- Filtrado en el dominio de Fourier: en este caso, el filtrado se realiza en el dominio de Fourier (Sherlock D. M., 1994).
- Filtros de Gabor: estos filtros son selectivos en frecuencia y en orientación, por lo que son muy apropiados para eliminar el ruido de fondo de la imagen sin deteriorar la estructura de crestas de la huella digital (Hong L. W., 1998).
- Filtrado sin análisis orientado: estas técnicas efectúan el filtrado basado en el contexto de la imagen sin necesidad de estimar el campo de orientación ni la frecuencia local de crestas (Willis, 2001).

Un extractor de características busca las terminaciones y bifurcaciones de las crestas en una imagen de la huella digital de entrada. Si las crestas pueden ser perfectamente localizadas en la imagen, la extracción de minucias se reduce a la extracción de puntos singulares en un mapa de crestas. Sin embargo, en la práctica, no siempre es posible obtener un mapa de crestas perfecto. El desempeño de los algoritmos de extracción de minucias depende fuertemente de la calidad de las imágenes de entrada. Debido a varios factores (deformación epidermial en las yemas de los dedos, cicatrices, marcas debido al trabajo, problemas con los dispositivos de adquisición, etc.) las imágenes de las huellas digitales no siempre tienen bien definido la estructura de crestas. Los algoritmos de extracción de minucias confiables, no deberían asumir estructuras de crestas perfectas y no

deberían degradarse con la calidad de la imagen (Jain A. K., Hong, Pankanti, Sharath, & Bolle, 1996).

El número de características que determinan la identidad de un individuo depende, generalmente, del volumen de individuos que pueden acceder al sistema de reconocimiento. Teniendo en cuenta esta consideración, la extracción de características se realiza en una o dos etapas. En un sistema de identificación, por ejemplo, cuando se trabaja con grandes bases de datos, es más eficiente hacer una clasificación previa de los individuos atendiendo a las características globales de las huellas digitales. Tales características están determinadas por las posiciones relativas de los puntos singulares (*núcleos* y *deltas*). En una segunda fase se extraen las características de detalle que proporcionan las *minucias* de la estructura de crestas. En sistemas de pocos individuos es suficiente trabajar directamente con patrones de minucias, sin necesidad de establecer una clasificación previa.

Representación de una huella digital. Los sistemas de reconocimiento de huellas digitales utilizan dos esquemas diferentes para representar una huella:

- La representación basada directamente en la propia imagen de la huella en escala de grises (*direct gray-scale representation*). En este caso, la individualidad de una huella puede representarse en el dominio espacial y frecuencial, puesto que, tanto el flujo de crestas como su orientación local, permiten hacer una representación suficientemente precisa a partir de la transformada de Fourier de la imagen. Los principales inconvenientes de esta forma de representación son: (i) la necesidad de almacenar la imagen de la huella, y (ii) la dificultad de diseñar algoritmos precisos de reconocimiento de patrones. Puesto que la comparación se lleva a cabo entre imágenes, el funcionamiento del sistema puede empeorar a causa de diversos factores, como por ejemplo: las variaciones de brillo, de contraste o de calidad, las deformaciones y daños en la piel, etc.
- La representación basada en las características de la huella (*feature representation*). Esta forma de representación tiene su origen en la comprobación de que las imágenes de dos huellas pertenecen a un mismo individuo si un número determinado de singularidades locales, presentes en las crestas, aparecen en ambas imágenes. Este hecho permite hacer una representación precisa, fiable y compacta a partir de dichas singularidades. Las características locales más utilizadas son: las minucias, los núcleos y deltas, los poros de las crestas, la orientación local y la frecuencia local de las crestas.

La mayoría de los sistemas de reconocimiento basados en patrones de minucias requieren la conversión de la imagen de la huella digital de entrada (en escala de grises) en una imagen binaria. En gran parte los esquemas propuestos, tras la etapa de mejora de imagen, se procede directamente a la conversión de la imagen mejorada en una imagen binaria. Una vez adelgazada la estructura de crestas binaria, se procede a la extracción de características. Algunos autores proponen esquemas de extracción de minucias basados en la representación de la huella a partir de la imagen, sin recurrir a los procesos de binarización y adelgazado. Esto es debido a las siguientes consideraciones; (i) una parte significativa de información puede perderse durante el proceso de binarización; (ii) los procesos de binarización y adelgazado suponen una carga computacional significativa; (iii) el adelgazado puede introducir minucias espurias; y (iv) la binarización no proporciona buenos resultados cuando la calidad de las imágenes es mala y no se aplica previamente ningún esquema de mejora de imagen.

Patrones de minucias. Las propiedades de exclusividad de las huellas digitales están presentes en las estructuras locales, denominadas *minucias*, que forman las crestas y que se distribuyen espacialmente sobre la imagen. Dichas estructuras locales tienen la cualidad de repetirse en diferentes partes de la imagen en un número suficiente de veces como para permitir el reconocimiento de cada individuo. El reconocimiento automático de huellas resulta más preciso mediante la comparación de patrones de minucias que mediante la comparación de imágenes o patrones de crestas. En total, se han identificado más de 60 tipos diferentes de estructuras locales. En la práctica resulta muy difícil la extracción automática, rápida y fiable, de esas estructuras, ya que su identificación depende del grado de detalle de la estructura de crestas obtenida, lo cual supone una gran limitación si se desea que el sistema de reconocimiento sea capaz de responder ante imágenes de diferente calidad. Por otra parte, algunas de las estructuras locales son muy similares entre sí, lo que dificulta su discriminación. La solución adoptada por los sistemas actuales de reconocimiento es la de considerar únicamente dos estructuras locales de crestas: la estructura *comienzo/final* de cresta y la estructura bifurcación de cresta. Cualquiera de las demás estructuras presentes en una imagen de huella digital puede expresarse como una combinación determinada de comienzos/finales y bifurcaciones de crestas. Una imagen de huella digital de buena calidad puede contener entre 40 y 100 minucias.

2.4.3.2 Normalización o ecualización

Con la etapa de normalización se consigue que el rango de valores de luminancia de todas las imágenes adquiridas este comprendido entre unos mismos valores previamente determinados. La normalización no modifica la definición de la estructura de la imagen de entrada, sino el rango de variación de grises entre crestas y surcos de la imagen. De esta manera, normalizando todas las imágenes por un mismo factor, se facilita el procesado de las siguientes etapas. El factor de normalización se calcula teniendo en cuenta la media y la varianza de la luminancia en la imagen.

Una vez que es capturada la imagen de la huella digital, se obtiene una imagen en escala de grises *I*, representada por una matriz en la que el elemento *I(i, j)* representa la intensidad de un pixel en la fila *i* y la columna *j*. La media *M(I)* y la varianza *V(I)* se definen como:

$$M(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i,j) \qquad \textbf{(2.1)}$$

$$V(I) = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} [\, I(i,j) - M(I)]^2 \qquad \textbf{(2.2)}$$

Llamando *G(i,j)* al valor normalizado de luminancia en media y varianza del pixel *(i,j)*, se define la imagen normalizada G, como:

$$G(i,j) = \begin{cases} M_0 + \sqrt{\dfrac{V_0\left[I(i,j) - M(I)\right]^2}{V(I)}} & \text{si } I(i,j) > M \\ M_0 - \sqrt{\dfrac{V_0\left[I(i,j) - M(I)\right]^2}{V(I)}} & \text{si } I(i,j) \leq M \end{cases} \quad \textbf{(2.3)}$$

Donde, M_0 y V_0 son los valores deseados de media y varianza de la imagen resultante *Figura 2-21*.

Figura 2-21. *Imagen original – Imagen normalizada*

2.4.3.3 Segmentación

La segmentación en una huella digital, consiste en separar el área que contiene información de la huella del fondo de la imagen *Figura 2-22*. Esta separación es útil para evitar la extracción de características en zonas de la imagen con ruido o del fondo de la imagen. No se suelen emplear técnicas que dependan de la intensidad de los píxeles, pues el fondo suele ser ruidoso, sino que se busca separar zonas con regiones estriadas (crestas y surcos) de zonas sin variaciones predominantes, isotrópicas. Lo que distingue el primer plano del fondo de la imagen es un patrón de rayas orientado en el primer plano y un patrón que no contiene una orientación predominante en el fondo. Existen varias técnicas para la segmentación de una imagen de una huella digital. Por ejemplo se separa la imagen en bloques de 16x16 pixel y se discrimina el fondo de la imagen utilizando la magnitud media del gradiente en cada bloque, debido que el área de la huella digital posee muchos bordes, debido a la alternancia crestas/surcos, la respuesta del gradiente es elevada en el área de la huella y baja en el fondo de la imagen.

Figura 2-22. *Imagen después de la etapa de segmentación*

2.4.3.4 Campo de orientación

La determinación del campo de orientación de la imagen permite conocer el ángulo de orientación local de las crestas de la huella digital. La estimación de este ángulo se lleva a cabo con cada bloque de *N x N* pixeles de la imagen. El campo de orientación servirá para fijar los parámetros en los filtros adaptativos que se emplearan en etapas posteriores. Existen varios algoritmos para realizar la estimación de dicho campo.

Calculo de gradiente de iluminancia de la imagen: se divide la imagen de entrada, en este caso la imagen normalizada, en bloques de *N x N* pixeles, y se calculan los gradientes de luminancia, *Gx(i,j) Gy(i, j),* en cada pixel *(i,j)*, según las dirección de *x* e *y*, respectivamente. Teniendo en cuenta que la resolución de las imágenes procesadas es de por ejemplo de 500 dpi, se toma el valor de N=8 o N=16. La elección de estos valores depende del grado de precisión exigido a la hora de estimar el campo de orientación y del tiempo de respuesta global del sistema. Generalmente, es suficiente el análisis de la imagen en bloques de N=16 pixeles, sin embargo, la determinación de la estructura de crestas en zonas de la imagen donde la curvatura de las crestas es muy pronunciada, puede requerir del análisis en bloques de N=8 pixeles.

Estimación del ángulo de orientación local. Con la información de los gradientes obtenidos, se estima el ángulo de orientación local de las crestas, en cada bloque centrado en el pixel *(i, j)*, de la siguiente manera:

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_x(i,j)}{V_y(i,j)}\right) \qquad \textbf{(2.4)}$$

donde:

$$V_x(i,j) = \sum_{u=i-\frac{N}{2}}^{i+\frac{N}{2}} \sum_{v=j-\frac{N}{2}}^{j+\frac{N}{2}} 2G_x(u,v)G_y(u,v) \quad \textbf{(2.5)}$$

$$V_y(i,j) = \sum_{u=i-\frac{N}{2}}^{i+\frac{N}{2}} \sum_{v=j-\frac{N}{2}}^{j+\frac{N}{2}} (G_x^2(u,v)G_y^2(u,v)) \quad \textbf{(2.6)}$$

Por lo tanto, $\theta(i,j)$ es la estimación por mínimos cuadrados del ángulo de orientación local de las crestas en el bloque centrado en el pixel *(i, j)*.

Reestimación del campo de orientación. En muchos casos, debido al ruido de fondo en la imagen y a los desperfectos en las crestas y surcos ocasionados por las faltas de impresión de determinadas zonas de la imagen, el ángulo de orientación $\theta(i,j)$ en algunos bloques se estima incorrectamente. Puesto que, localmente en una huella, en zonas de la imagen donde no existen puntos singulares, no pueden existir grandes variaciones entre los ángulos de orientación de bloques vecinos, haciendo un filtrado paso bajo del campo de orientación estimado, se consigue mejorar la estimación de los ángulos previamente calculados. Para efectuar el filtrado paso bajo se convierte el campo de orientación en otro campo definido por:

$$\phi_x(i,j) = \cos(2\theta(i,j))$$
$$\phi_y(i,j) = sen(2\theta(i,j)) \quad \textbf{(2.7)}$$

Donde: $\emptyset_x \, y \, \emptyset_y$ son los componentes *x* e *y* de dicho campo, respectivamente. Llamando *h(i,j)* a la respuesta impulsiva del filtro paso bajo bidimensional, de dimensiones *W x W* e integral unidad, puede ponerse que las componentes filtradas resultantes $\emptyset_x'(i,j) \, y \, \emptyset_y'(i,j)$, vienen dadas por:

$$\phi_x'(i,j) = \phi_x(i,j) * h(i,j) = \sum_{u=-W/2}^{W/2} \sum_{v=-W/2}^{W/2} \phi_x(i-uN, j-vN)h(u,v) \quad \textbf{(2.8)}$$

$$\phi_y'(i,j) = \phi_y(i,j) * h(i,j) = \sum_{u=-W/2}^{W/2} \sum_{v=-W/2}^{W/2} \phi_y(i-uN, j-vN)h(u,v) \quad \textbf{(2.9)}$$

Finalmente se obtiene el nuevo campo de orientación haciendo:

$$\varphi(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{\phi_y'(i,j)}{\phi_y'(i,j)}\right) \quad \textbf{(2.10)}$$

La eliminación de las altas frecuencias, como consecuencia del filtrado paso bajo del campo de orientación, da como resultado el suavizado de dicho campo, en el que la variación de los ángulos entre bloques sucesivos se realiza lentamente. Puede observarse que dicho suavizado se realiza a nivel de bloques. El filtro utilizado, para huellas tintadas y huellas de escáner, es de dimensión W=5 pixeles. De esta manera, durante el proceso de convolución de la imagen con el filtro, se efectúa la corrección del valor del ángulo de orientación en cada bloque a partir de los 24 valores de los ángulos de todos los bloques circundantes. El resultado de esta etapa se puede ver en la *Figura 2-23*.

Figura 2-23. *Imagen después de la etapa de orientación*

2.4.3.5 Filtrado y binarización

Para acelerar el proceso de cálculo sólo se filtran los pixeles que no han sido segmentados; el resto se consideran como blancos. El objetivo de esta etapa es determinar qué píxeles forman parte de los surcos (blancos) o de las crestas (negros). Un filtro Gabor responde a la siguiente expresión:

$$G(x,y) = \cos(2\pi . f . x_0).e^{-0.5(\frac{x_\theta^2}{\tau_x^2}+\frac{y_\theta^2}{\tau_y^2})} \quad \textbf{(2.11)}$$

Donde:

$x_\theta = x.cos\theta + y.sen\theta$

$y_\theta = x.sen\theta + y.cos\theta$

θ = *es la orientación del pixel*

f = *es la frecuencia espacial 1/6 Hz*

$f = 1/d$

d = *es la distancia entre dos crestas (máximos o mínimos)*

$\tau_x = \tau_y = d/2$

Estos filtros se caracterizan por ser selectivos en frecuencia y orientación, dado que ambos parámetros aparecen en la expresión. La idea de aplicar un filtro Gabor sobre la imagen se basa en que esta tiene precisamente a su vez propiedades: por un lado las crestas a nivel local se caracterizan claramente por tener una separación que marca una frecuencia espacial determinada, y por otro tienen una orientación particular obtenida en la etapa anterior. Si el filtro se sintoniza a la frecuencia y orientación asociada con las crestas el resultado del filtrado realzará la estructura cresta-surco de la huella digital.

Empíricamente puede demostrarse que la sensibilidad del filtrado con la orientación permite cierta flexibilidad, de forma que ángulos con orientaciones similares (inferiores a 20 grados) dan resultados muy parecidos. Por otro lado, según la expresión una orientación con respecto a otra orientación +180º dan lugar al mismo filtro (simetría). Una forma de acelerar el proceso de cálculo consiste en considerar únicamente un número finito de orientaciones, con el objetivo de poder pre-calcular la estructura de los filtros (valores de los pixeles de sus máscaras asociadas) únicamente al principio de la ejecución del algoritmo. Típicamente el número de filtros es 16, lo que representa saltos de 11.25 grados comprendidos entre –180º y 180º.

El funcionamiento del algoritmo es el siguiente: Mediante un bucle anidado se recorren todos los pixeles de la imagen. Si el píxel no está segmentado se elige el filtro cuya orientación es la más cercana al valor obtenido en la etapa anterior para este pixel. En función del resultado del filtrado se procede a la binarización del píxel, de forma que si este es mayor que un determinado umbral (100) se asigna el valor “1”, en caso contrario se asigna el valor “0”.

En la *Figura 2-24* se observa el resultado de la imagen después de ejecutar el algoritmo de filtrado y binarización.

Figura 2-24. *Imagen binarizada*

2.4.3.6 Adelgazamiento

El adelgazamiento o también denominado esqueletización o "thinning", realiza una reducción del grosor de las líneas hasta que presenten un grosor igual a un pixel, facilitando de esta manera el proceso de reconocimiento. Por ejemplo el siguiente algoritmo (Zhang & Suen, 1984), donde se define a los ocho vecinos de un pixel según se muestra en el la *Figura 2-25*

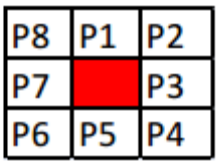


Figura 2-25. *Representación del bloque, su pixel central y definición de sus vecinos.*

Se aplican de forma iterativa dos conjuntos de condiciones. Aquellas que cumplen todas las condiciones de la etapa A se cambiarán y se pondrán de color blanco:

Etapa A:

- Si se cumple que el número de vecinos distintos de "0" es mayor o igual que dos y menor o igual que seis. (se asegura que los puntos finales se preservan).
- Que solamente una vez se pasa de valor "0" a valor "1" si se recorre el borde, (se preservan los puntos que se encuentran entre ellos).
- Que alguno de "P1", "P3" y "P5" es un "0".
- Que alguno de "P3", "P5" o "P7" es un "0".

Una vez cambiados los pixeles que cumplan las condiciones de la "Etapa A", se cambiarán aquellos que cumplan las cuatro condiciones siguientes de la "Etapa B".

Etapa B:

- Si se cumple que el número de vecinos distinto de “0” es mayor o igual a dos y menor o igual a seis.
- Que solamente una vez se pasa del valor “0” a “1”, si se recorre el borde.
- Que alguno de “P1”,”P3” y “P7” es un “0”.
- Que alguno de “P1”,”P5” o “P7” es un “0”.

Este algoritmo se realizará de forma iterativa hasta que ningún pixel cambie su color de negro a blanco.

Una manera de realizar este algoritmo de una manera mucho más eficiente y rápida es haciendo la convolución de la imagen con un filtro, con los siguientes valores *Figura 2-26*

Los ocho vecinos quedan codificados en un número entre “0” y “255”. Pueden calcularse de antemano los valores numéricos que darían las condiciones expresadas antes, por ello deben eliminarse los puntos que cumplan:

128	1	2
64		4
32	16	8

Figura 2-26. *Representación del peso de los pixeles del bloque.*

S1={3,6,7,12,14,15,24,28,30,48,56,60,62,96,112,120,129,131,135,143,192,193,195,199,207,224,225,227,231,240,241,243,248,249}.

S2={3,6,7,12,14,15,24,28,30,31,48,56,60,62,63,96,112,120,124,126,129,131,135,143,159,192,193,195,224,225,227,240,248,252}.

Representando S1, los posibles casos que cumplen el primer conjunto de condiciones de la Etapa A y S2 los de la Etapa B. Así por ejemplo el valor “207” corresponde la convolución con una imagen como la de la *Figura 2-27*.

1	1	1
1		1
0	0	1

Figura 2-27. *Matriz de tres x tres.*

Al hacer la convolución de la *Figura 2-26* con la *Figura 2-27* se observa que el resultado de esta convolución es “207”.

En *Figura 2-28* se puede ver con claridad como el grosor de las líneas se ha reducido considerablemente después de ejecutar el algoritmo de adelgazamiento.

Figura 2-28. *Imagen adelgazada*

2.4.3.7 Extracción de minucias y generación del patrón biométrico

El objetivo de esta etapa es la obtención del patrón biométrico de la hulla digital a partir de la imagen adelgazada y que se obtiene en etapas anteriores. En estas circunstancias, para una calidad dada de la imagen de entrada, la extracción de características puede determinar con suficiente exactitud la posición de las estructuras que definen las minucias del patrón biométrico. No obstante, a pesar del pre-procesado realizado en las etapas anteriores para aumentar la fiabilidad del patrón biométrico, la extracción de características no puede reducirse a una mera búsqueda de minucias sobra la imagen adelgazada. El ruido presente en la imagen de entrada puede dar lugar a la generación de varias estructuras adelgazas falsas muy próxima entre si y por lo tanto, a la aparición de agrupaciones de falsas minucias. También son fuente de generación de minucias falsas las estructuras próximas al borde que delimita la región de interés de la hulla digital. Por estos motivos, la extracción de características debe realizarse en sucesivas etapas, eliminando en cada una de ellas las estructuras que sean consideradas falsas.

La correcta localización de las estructuras que determinan las minucias de una huella digital, sobre una imagen adelgazada, es una tarea relativamente sencilla, sean *x* e *y*, las coordenadas del pixel P_1, perteneciente a una cresta y situado en el centro de la ventana de análisis *3 x 3* pixeles. Sean P_2, P_3,…P_9, sus ocho pixeles vecinos, según se muestra en la *Figura 2-29*.

P_3	P_2	P_9
P_4	P_1	P_8
P_5	P_6	P_7

Figura 2-29. *Numeración de pixeles en ventana de análisis*

Considerando que un pixel perteneciente a una cresta tiene un valor uno (negro), y que en caso contrario tiene valor cero (blanco), el procedimiento para determinar si un pixel de la imagen constituye o no una minucia de la huella es el siguiente (Bansal, Sehgal, & Bedi, 2011).

1. Un pixel pertenece a una cresta *Figura 2-30*, si tiene dos pixeles vecinos negros dentro de la ventana de análisis, es decir:

$$\sum_{i=2}^{9} P_i = 2$$

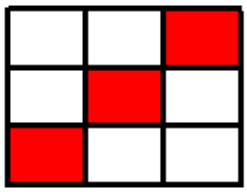


Figura 2-30. *Pixeles que representan una cresta.*

2. Un pixel, que pertenece a una cresta, es final de cresta *Figura 2-31*, si tiene únicamente un pixel vecino en negro dentro de la ventana de análisis, es decir:

$$\sum_{i=2}^{9} P_i = 1$$

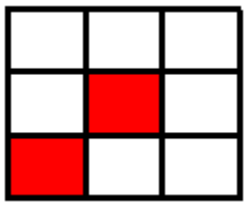


Figura 2-31. *Pixeles que representan una terminación de cresta.*

3. Un pixel, que pertenece a una cresta, constituye una bifurcación *Figura 2-32*, si tiene tres pixeles vecinos en negro dentro de la ventana de análisis, o sea:

$$\sum_{i=2}^{9} P_i = 3$$

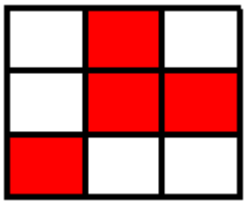


Figura 2-32. *Pixeles que representan una bifurcación de cresta.*

Parámetros almacenados de cada minucia: una vez fijadas las condiciones de detección anteriores, se analiza la imagen pixel a pixel en el entorno de 3 x 3. Si para un determinado pixel, perteneciente a una cresta, se cumplen las condiciones de final de cresta o de bifurcación, se toma dicho pixel como candidato a ser minucia del patrón biométrico de la huella. Para cada una de las minucias candidatas se almacenan los siguientes parámetros:

1. Coordenadas *x* e *y* del pixel que constituye la minucia, (x_0, y_0).
2. Angulo de orientación local *Θ*, de la cresta al que pertenece dicho pixel.
3. Tipo de minucia, terminación o bifurcación.

Los parámetros almacenadas *(x_0, y_0, Θ, ti)* para una minucia, se muestra en la *Figura 2-33.*

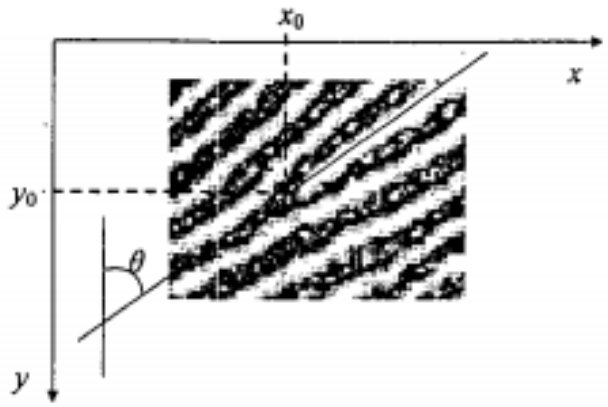


Figura 2-33. *Parámetros almacenados (x_0, y_0, Θ) de una minucia bifurcación.*

El resultado de la extracción será un vector de *N* componentes (minucias encontradas), donde cada componente del vector tendrá cuatro elementos (x_0, y_0, *Θ, ti*).

Donde:

x_0: es el eje de abscisas (horizontal),

y_0: es el eje de ordenadas (vertical),

Θ: orientación del píxel,

ti: es el tipo de minucia (final/inicio o bifurcación).

En la *Figura 2-34,* se observan las minucias encontradas y marcadas, como resultado de este proceso.

Figura 2-34. *Imagen original de huella digital y su correspondiente imagen con minucias marcadas*

2.4.4 Comparación de patrones de minucias

La comparación o matching de huellas es una de las fases más críticas en un sistema de verificación de huella digital. Comparar dos huellas puede ser un proceso muy complejo ya que en general las dos huellas a comparar habrán sufrido desplazamientos, rotaciones, distorsiones o quizá su calidad pueda ser baja. Por lo tanto, un buen algoritmo de comparación deberá ser robusto frente a la variabilidad en las huellas a comparar.

Las principales dificultades ante las que debe actuar un algoritmo de comparación son las siguientes:

- Desplazamiento y rotación: son el resultado de que la persona sitúe su dedo en un lugar diferente del sensor en cada ocasión. Pueden ocasionar que una parte de la huella se encuentre fuera del área de captura, por lo que las huellas a comparar tendrán un área menor en común a la real. Este problema afecta en gran medida a los sensores con una reducida área de captura.
- Distorsión no lineal: es la consecuencia de plasmar en una imagen de dos dimensiones una huella digital de tres dimensiones, con una elasticidad que provoca deformaciones no lineales en su superficie.
- Diferencias de presión y de las condiciones de la piel: la presión que se ejerza contra el sensor y la humedad o sequedad de la piel hacen que la captura sea diferente en cada situación. También afectan sustancias corporales como el sudor o la grasa.

- Errores en la extracción de características: los algoritmos de extracción de minucias tienden a producir minucias falsas en las huellas de baja calidad que enmascaran a menudo minucias reales.

Figura 2-35. *Impresiones de la misma huella en condiciones diferentes*

En la *Figura 2-35* se observan dos impresiones de la misma huella de una persona tomadas en condiciones diferentes. Existen en la literatura un gran número de algoritmos automáticos de comparación o matching para huellas digitales (Jain A. K., 2006). La mayor parte de ellos presentan un buen rendimiento cuando las huellas digitales que se les presentan son de buena calidad, sin embargo, conseguir discernir entre huellas de baja calidad o entre huellas digitales incompletas sigue siendo un foco de interés científico. Una muestra clara de ello son las competiciones internacionales celebradas periódicamente con el fin devaluar el rendimiento de los sistemas que son propuestos en la actualidad, como las competiciones FVC (*Fingerprint Verification Competition*) http://bias.csr.unibo.it/fvc2006.

Algoritmo de "matching" basado en estructura local y global

En la etapa de "extracción de minucias" se ha generado un vector de entrada de "N" elementos, donde cada uno de ellos contiene cuatro componentes que indican la posición, orientación y el tipo de minucia (x, y, Θ, ti). En esta etapa de "matching", lo que se hace es comparar el vector de entrada, hallado en las etapas previas, con el vector patrón de las minucias de la huella almacenada en la base de datos. El resultado del algoritmo de matching es la puntuación de similitud entre ambos vectores.

Se tienen que tener una serie de consideraciones sobre la posición de la huella:

- Desplazamiento. Dos huellas iguales capturadas bajo las mismas condiciones (sequedad, suciedad, etc.), seguramente están desplazadas, porque es prácticamente imposible que el dedo se ponga exactamente en la misma posición en el sensor las dos veces.
- Rotación. Se debe ser capaz de emparejar las minucias de la misma huella digital independientemente si una con respecto a la otra esta rotada un ángulo determinado.
- Escalabilidad. Se debe tener en cuenta que la piel es elástica. Por lo tanto en función de la presión ejercida sobre la superficie del sensor la huella capturada puede estar escalada un factor *alfa* que debe tenerse en cuenta en la etapa de matching. Otra

posibilidad es que la misma huella haya sido capturada mediante dos sensores de características diferentes (básicamente resolución) que den lugar a un factor de escala entre ambas.

El proceso de comparación de ambos vectores se realiza en dos fases: análisis local y global de los patrones de minucias.

2.4.4.1 Análisis local

En esta fase se analiza a nivel local la vecindad de cada una de los puntos característicos. Cada minucia es identificada y caracterizada a partir de la disposición espacial relativa a ella misma con sus doce minucias vecinas más próximas.

Cada minucia es parametrizada con los siguientes datos: tipo *ti* de la minucia (bifurcación o final/inicio de cresta), tipos *tiv* de las minucias vecinas, distancia relativa *d* entre la minucia de referencia o central y sus minucias vecinas y, por último, ángulos relativos ϕ y γ entre la orientación que toma la cresta de la huella en la minucia objeto de estudio β_i y los ejes que unen a ésta con sus minucias vecinas *Figura 2-36*.

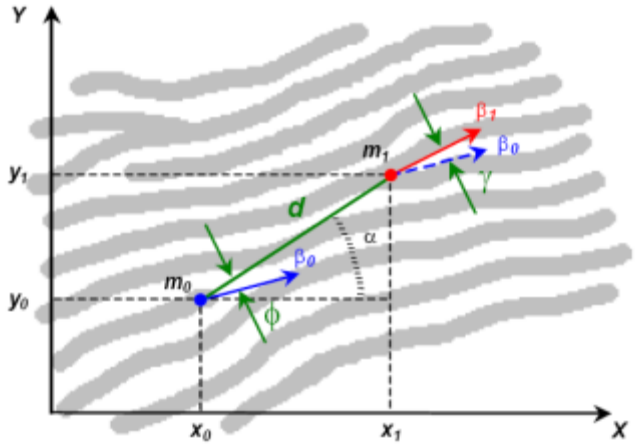


Figura 2-36. *Análisis estructural local y global de minucia*

Una vez caracterizadas a nivel local tanto la minucia recién adquirida como la minucia patrón almacenada, se lleva a cabo un estudio de correlación entre ambas estructuras locales. Para ello se construye una matriz de similitud que asocia el nivel de semejanza de la estructura local de cada minucia de la huella capturada con las minucias de la huella patrón *Figura 2-37.*

Donde:

p1...pn = son las minucias de la matriz patrón.

q1…qn =son las minucias de la matriz de entrada.

S_{ij} = Nivel de similitud entre las estructuras locales q_i y p_i.

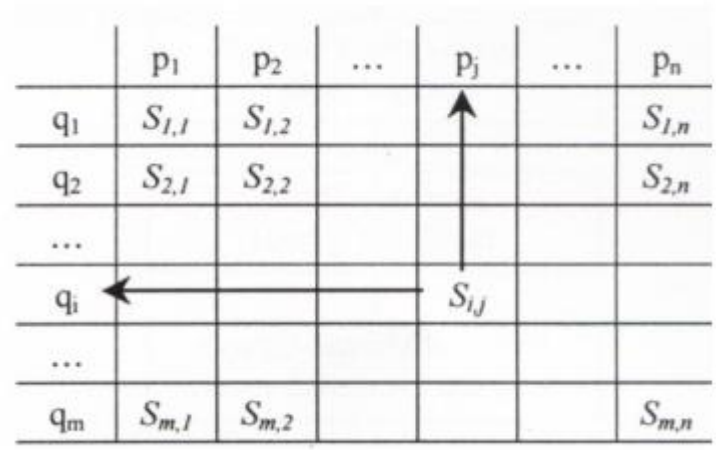


Figura 2-37. *Matriz de similitud*

Concretamente el grado de similitud se calcula de la siguiente forma (tanto para la minucia central del vector de entrada como patrón):

- Las 12 minucias vecinas se ordenan de menor a mayor según su distancia con respecto a la minucia central.
- Atendiendo al orden resultante, la minucia vecina ubicada en el puesto $j_{entrada}$ (j<=12) de entrada y su equivalente ubicada también en la posición $j_{patrón}$ patrón se comparan del siguiente modo:
  i. Si son del mismo tipo se suma un punto al grado de similitud.
  ii. Para el vecino *j* (tanto de entrada como patrón), se calcula la distancia con respecto a la minucia central *d Figura 2-36*. Si la diferencia entre las distancias obtenidas para los vectores entrada y patrón es menor que un umbral (5 pixeles) se suma un punto al grado de similitud.
  iii. Se repite el paso ii pero en este caso para los ángulos ϕ y γ sumándose un punto si la diferencia es menor de 15 grados.

El proceso se repite para las 12 minucias vecinas.

La minucia (tanto para el vector de entrada como patrón) que obtenga el grado de similitud mayor será considerada como la minucia de referencia (o central) de las imágenes de entrada y patrón, respectivamente.

2.4.4.2 Análisis global

Una vez obtenidas las minucias centrales el siguiente paso consiste en repetir el análisis espacial pero en este caso a nivel global. Las minucias centrales se consideraran como puntos de referencia para corregir los errores introducidos por traslaciones y rotaciones de la huella. La forma de emparejar las minucias de las imágenes de entrada y patrón es la siguiente:

- Se toma la minucia *k* del vector de entrada y se calcula su distancia d_e con respecto a la minucia central.

- Se calcula la distancia d_p de todas la minucias del vector patrón con respecto a la minucia central de dicho vector. Se toman como candidatas a ser emparejadas aquellas cuya diferencia (d_p – d_e) sea inferior a un umbral (20 pixeles en valor absoluto). Las minucias candidatas reciben una puntuación igual 1-abs (d_p - d_e)/20. Este umbral trata de corregir los errores de escalado entre huellas.
- Para las minucias candidatas se calculan nuevamente los ángulos ϕ_e y γ_e, para el vector de entrada, y ϕ_d y γ_d para el vector patrón, definidos en la *Figura 2-36*. Si la diferencia entre los ángulos obtenidos para la minucia de entrada (ϕ_e - ϕ_d y γ_e - γ_d) y patrón es inferior a un umbral (15 grados para ϕ y 20 grados para γ) se suma a la puntuación anterior los valores 1-abs (ϕ_e - ϕ_d)/15 y 1-abs (γ_e - γ_d)/20, respectivamente. La minucia que haya obtenido la mayor puntuación es la emparejada.
- El proceso se repite para todas las minucias del vector de entrada.

El resultado del proceso de matching se da como una puntuación que surge de la similitud entre las minucias emparejadas y minucias totales del vector entrada.

2.4.4.3 Representación gráfica del proceso

En la *Tabla 2-2*, se observan todas las etapas del proceso, desde la extracción de las características a la imagen de la huella digital hasta la comparación del patrón biométrico generado, con los parámetros de entrada y salida de cada uno de ellas.

ETAPAS	ENTRADA	SALIDA
Normalización	Imagen, media y varianza deseada.	Imagen normalizada
Segmentación	Imagen normalizada, tamaño ventana y umbral de segmentación.	Imagen segmentada.
Orientación	Imagen normalizada y tamaño ventana.	Orientación de las crestas.
Binarización	Imagen normalizada y valor umbral para la binarización.	Imagen binarizada. (surco="0", cresta="1")
Adelgazamiento	Imagen binaria.	Imagen adelgazada.
Extracción de minucias	Imagen adelgazada y segmentada.	Vector de N componentes de minucias encontradas.
Comparación	Vectores patrón y entrada, porcentaje mínimo de minucias cotejadas.	Resultado del reconocimiento.

Tabla 2-2. *Etapas del reconocimiento basado en minucias*

2.5 Evaluación del rendimiento de sistema biométrico de huelas digitales

Para determinar las prestaciones de un sistema de reconocimiento, es necesaria una medida objetiva del rendimiento del mismo. El rendimiento de un sistema biométrico, se entiende como la precisión en el proceso de reconocimiento.

A la hora de poner en funcionamiento un sistema biométrico, hay que tener en cuenta que dos muestras de un mismo rasgo biométrico no son exactamente iguales debido a imperfecciones generadas en la captura de la imagen, cambios en los rasgos fisiológicos o de comportamiento del usuario, factores ambientales, la interacción del usuario con el sensor entre otros. Por lo tanto, la respuesta del comparador de un sistema biométrico consiste en una puntuación que cuantifica la similitud entre la entrada y el patrón de la base de datos con el que se está comparando. Cuanto mayor sea la semejanza entre las muestras, mayor será la puntuación devuelta por el comparador y más seguro estará el sistema de que las dos medidas biométricas pertenecen a la misma persona.

La decisión del sistema está regulada por un umbral, los pares de muestras que generen puntuaciones mayores o iguales que el umbral se supondrán correspondientes a la misma persona, mientras que los pares de muestras cuya puntuación sea menor que el umbral se consideraran de personas diferentes.

2.5.1 Norma ISO/IEC 19795 (ISO JTC1/SC37, 2006)

Los objetivos de la norma son:

- Establecer los principios generales para la evaluación del rendimiento de los sistemas biométricos en términos de tasas de error y tiempo de procesamiento para distintos propósitos, como la predicción del rendimiento, la comparación de rendimientos y la verificación del cumplimiento de los requisitos.
- Especificar las métricas del rendimiento para sistemas biométricos.
- Especificar los requisitos de los métodos de evaluación, captura de datos y comunicación de los resultados.
- Proporcionar un marco para el desarrollo y evaluación de protocolos, para ayudar a lograr la mejor estimación del rendimiento y para la comprensión de los límites de aplicación de los resultados de las evaluaciones.
- Desarrollar y describir protocolos para evaluaciones de tecnología y escenario.

Esta norma se aplica a la evaluación del rendimiento empírico de los sistemas biométricos y los algoritmos que forman parte de las decisiones y puntuaciones de comparación del sistema, sin que sea necesario un conocimiento detallado de los algoritmos o las características biométricas.

Sin embargo, este estándar tiene ciertas limitaciones. Se encuentran fuera del ámbito de esta norma la medida de errores y tiempos para personas que tratan de engañar deliberadamente al sistema biométrico. Además, en este estándar no se incluyen aspectos de los sistemas biométricos como la aceptabilidad, la disponibilidad, el mantenimiento, vulnerabilidades, factores humanos, costos o cumplimientos de la regulación. Finalmente este estándar no contempla la evaluación de sistemas biométricos de verificación en entornos de mundo abierto.

2.5.1.1 Nomenclatura y definiciones

Para la correcta definición de los aspectos claves de las evaluaciones biométricas de acuerdo a esta norma, es preciso introducir previamente cierta nomenclatura. Estos términos y definiciones se han obtenido del estándar ISO/IEC 19795.

Datos Biométricos

Este vocabulario trata de los datos y definiciones relacionados con la información biométrica:

- **Muestra**: Es la señal o imagen obtenida a partir del sistema de captura. Por ejemplo, una imagen de una huella digital.
- **Características**: Son las representaciones digitales de la información extraída a partir de una muestra, que serán utilizadas para construir o comparar contra un patrón. Por ejemplo, coordenadas de una minucia.
- **Patrón**: Es un conjunto de características almacenadas que se asocian con la identidad de un usuario.
- **Puntuación de similitud o de comparación**: Es la medida de la similitud entre las características de una muestra y un patrón almacenado. También se define como una medida de cuan bien encajan esas características en un modelo de referencia de un usuario.
- **Decisión de verificación:** Es la determinación de si un usuario es quien dice ser.
- **Lista de candidatos:** Es el conjunto de potenciales identificadores de usuarios registrados producidos por un intento e identificación.
- **Decisión de identificación:** Es la determinación del candidato o la lista de candidatos más probables.

Iteración del usuario con un sistema biométrico

Estos términos definen las acciones que involucran la adquisición de datos biométricos y la interacción con el sistema:

- **Presentación:** Presentación de una única muestra biométrica por parte de un usuario.
- **Intento:** Presentación de una (o una secuencia de) muestras biométricas al sistema
- **Transacción:** Secuencia de intentos por parte de un usuario a los fines de un registro, verificación o identificación.
- **Intento genuino:** Un solo intento de buena fe por un usuario para comparar con su propio patrón biométrico almacenado.
- **Intento de impostor de esfuerzo cero:** Intento en el que un individuo presenta sus propias características biométricas como si estuviera intentando verificar con éxito contra su propio patrón biométrico, pero la comparación se hace con el patrón de otro usuario.
- **Intento de impostor activo:** el individuo intenta comparar el patrón almacenado de un individuo diferente presentando una característica biométrica simulada o reproducida, o modificada intencionalmente.

Aplicaciones Biométricas

Los términos más comunes asociados con las operaciones biométricas son:

- **Verificación:** en esta aplicación el usuario en primer lugar declara su identidad y a continuación presenta unos rasgos biométricos que confirman su identidad mediante la comparación de las características extraídas de las muestras de acceso y el patrón almacenado asociado a su persona. Por lo tanto requiere una comparación *1 : 1*, donde se procesa la muestra y se compara con el patrón del usuario. Existen dos tipos de verificación:
  - **Verificación de mundo cerrado:** en este tipo de verificación todos los posibles usuarios son conocidos por el sistema.
  - **Verificación de mundo abierto:** en esta forma de verificación existen usuarios no conocidos por el sistema.
- **Identificación:** esta aplicación consiste en buscar en una base de datos de usuarios registrados y proporcionar una lista de 0, 1 o más candidatos. De esta manera, requiere una comparación *1 : N*, donde se compara la muestra con todos los usuarios de la base de datos. Existen dos tipos de identificación:
  - **Identificación de mundo cerrado:** en este tipo de aplicación todos los posibles usuarios están registrados en el sistema.
  - **Identificación de mundo abierto:** en este tipo de aplicación existen usuarios no registrados en el sistema.

2.5.1.2 Métricas del rendimiento

Se definen las métricas de rendimiento definidas en el estándar ISO/IEC 19795.

Métricas fundamentales

Para el presente trabajo del estándar se toman las siguientes tasas:

- **Tasa de Error de Adquisición (FTA: "Failure To Adquire Rate"):** proporción de intentos de verificación o identificación en los que el sistema falla en la captura de la muestra o captura una muestra de baja calidad.

- **Tasa de Error de No Concordancia (FNMR: "False Non-Match Rate"):** proporción de muestras de intentos de usuarios legítimos que el sistema indica que no concuerda con el patrón almacenado. Por ejemplo, se comparan los patrones biométricos pertenecientes a un mismo individuo entre sí y cada rechazo se computa para el cálculo de la tasa, utilizando la Ecuación (2.12).

$$\boldsymbol{FNMR = \frac{Cantidad\ de\ Rechazos}{Cantidad\ de\ Comparaciones}} \qquad \textbf{(2.12)}$$

$$\boldsymbol{Cantidad\ de\ Comparaciones = \frac{hi * (hi - 1) * i}{2}} \qquad \textbf{(2.13)}$$

donde:

hi, es la cantidad de patrones por individuos

i, es la cantidad de individuos.

- **Tasa de Error de Concordancia (FMR: "False Match Rate"):** proporción de intentos de falsificación aleatorio que el sistema declara que corresponden con el patrón almacenado. Por ejemplo, se comparan las muestras de patrones de diferentes usuarios, al aceptar alguna comparación como válida se computa para el cálculo de la tasa, utilizando la Ecuación (2.14):

$$\boldsymbol{FMR = \frac{Cantidad\ Aceptaciones}{Cantidad\ Comparaciones}} \quad \textbf{(2.14)}$$

$$\boldsymbol{Cantidad\ de\ Comparaciones = \frac{i * (i-1)}{2}} \quad \textbf{(2.15)}$$

dónde:

i, es la cantidad de individuos.

Métricas de un sistema de verificación

En los sistemas de verificación, un usuario declara su identidad y a continuación la confirma con un rasgo biométrico, comparándose la muestra de acceso con el patrón almacenado. De acuerdo con esto, existen dos métricas:

- **Tasa de Falso Rechazo (FRR: "False Reject Rate"):** proporción de intentos de verificación legítimos a los que el sistema deniega el acceso. Se calcula mediante la Ecuación (2.16)

$$FRR = FTA + FNMR(1 - FTA) \quad \textbf{(2.16)}$$

- **Tasa de Falsa Aceptación (FAR: "False Accept Rate"):** proporción de intentos de verificación ilegítimos que el sistema acepta erróneamente. Se calcula mediante la Ecuación (2.17)

$$FAR = FMR(1 - FTA) \quad \textbf{(2.17)}$$

Las tasas de FAR y FRR se calculan sobre el número de transacciones de verificación, mientras que las tasas de FNMR y FMR se calculan sobre el número total de comparaciones. Por lo tanto, las tasas FAR y FRR no son sinónimos de FMR y FNMR, ya que incluyen los errores de adquisición obtenidos por muestras de baja calidad. No obstante, si no se tiene en cuenta la tasa FTA las tasas FAR, FRR y FMR, FNMR son iguales.

Representación gráfica de resultados

General

Los resultados de las comparaciones o desempeño de un sistema biométrico sobre un rango de un umbral de decisión deben ser representados gráficamente utilizando una curva ROC o una curva DET, peno no ambas.

Escala de ejes

Se deben mostrar los valores máximos y mínimos además de utilizar escalas logarítmicas para la claridad de los resultados presentados.

Comparación de sistemas

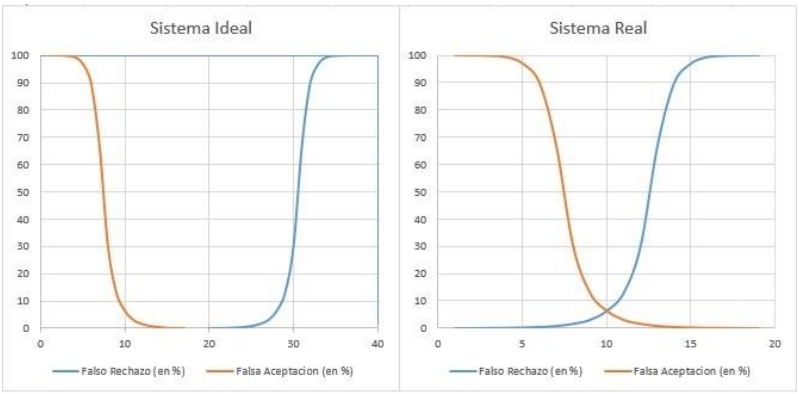
La utilización de curvas ROC o DET, serán más útiles que los gráficos que muestran las tasas de error fundamental.

Otros indicadores de rendimiento

A pesar de no estar incluidos en el estándar ISO/IEC 19795, es también muy común en la evaluación de sistemas biométricos los el uso de otros indicadores (Ferrara, Franco, & Maltoni, 2007) como **Tasa de Igual Error (EER)**, **FMR100**, valor más bajo de FNMR para FMR <= 1%; **FMR1000,** valor más bajo de FNMR para un FMR <=0.1%; **ZeroFMR**: valor más bajo de FNMR en el cual no se producen FMR*;* **ZeroFNMR**: valor más bajo de FMR en el cual no se producen FNMR.

2.5.2 Descripción de las tasas e indicadores

En un sistema ideal, los rangos de variación de las puntaciones obtenidas para usuarios impostores y genuinos están separados, de manera que no hay solapamiento entre sus distribuciones, pudiéndose establecer un umbral de decisión que discrimine perfectamente ambas clases *Figura 2-38 a)*. Sin embargo, en un sistema real existe una región en la que se solapan ambas distribuciones *Figura 2-38 b)*. Si se fija un umbral, todas las puntuaciones cuyo valor sea superior a ese umbral serán interpretadas por el sistema como usuarios genuinos.



a) b)

Figura 2-38. *Sistema Ideal - Sistema Real.*

Diferentes tasas de error son usadas como métricas para la capacidad operativa de un sistema de autenticación biométrica en general y para sistemas de reconocimiento de imágenes de huellas digitales en particular.

El resultado de una comparación en el módulo de comparación dentro de un sistema biométrico, es llamado Medida o Puntuación de Similitud *"s" (Matching Score).* El cual establece la semejanza entre la señal de entrada y el patrón biométrico almacenado en la base de datos.

Cuanto más próximo se encuentre *"s"* de 1 (si el rango esta normalizado entre [0,1]), es más probable que ambos patrones biométricos provengan del mismo individuo. Por otro lado, si *"s"* se encuentra cercano a 0, será menos probable que ambos patrones sean de la misma persona.

Si el patrón biométrico almacenado en la base de datos se representa con *T* y la imagen de entrada se representa por *I*, entonces:

- **I <> T**, la imagen de entrada y el patrón almacenado no provienen de la misma persona.
- **I = T**, la imagen de entrada y el patrón almacenado pertenecen a la misma persona.

Las decisiones asociadas son:

- La persona no es quien dice ser
- La persona es quien dice ser

La verificación implica hacer coincidir *T* e *I* utilizando una medida de similitud *s*. Si la medida o puntuación es menor que el umbral del sistema *t* la persona no es quien dice ser, de lo contrario la persona es quien dice ser. De modo que el sistema puede presentar dos tipos de errores:

- **Tipo I**: Falsa Concordancia (el sistema decide que la persona es quien dice ser, cuando la señal de entrada y el patrón biométrico son distintos).
- **Tipo II**: Falsa No Concordancia (el sistema decide que la persona no es quien dice ser, cuando la señal entrada y el patrón biométrico pertenecen a la misma persona).

Tasa de Error de Concordancia (FMR) es la probabilidad del tipo de error I y la Tasa de Falso Rechazo (FNMR) es la probabilidad del tipo de error II.

Para evaluar la exactitud de un sistema biométrico, se debe evaluar las puntuaciones generadas de un número de pares de huellas del mismo dedo, la distribución de estos puntajes se denomina distribución genuina, y las puntuaciones generadas por un número de pares de huella de diferentes dedos, la distribución de estos puntajes se denomina distribuciones de impostores (Maltoni D. , Maio, Jain, & Prabhakar, 2003) *Figura 2-39*.

Existe una estrecha relación entre FMR y FNMR, ambas son funciones del umbral del sistema *t*, si se disminuye *t* el sistema se vuelve más tolerante y FMR se incrementa, y viceversa, si se incrementa *t* para hacer el sistema más seguro, entonces FNMR se incrementa. En aplicaciones de alta seguridad, el punto de trabajo suele situarse en valores bajos de FM, para evitar que accedan impostores, a costa de tener alta FNM. Por el contrario, en aplicaciones forenses se trabaja en baja FNM para no perder individuos buscados, a costa de una alta FAM. Las aplicaciones civiles suelen trabajar en un punto intermedio.

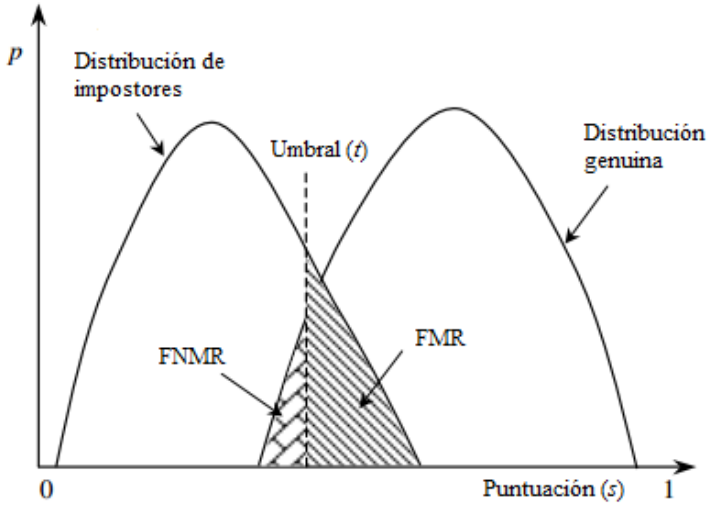


Figura 2-39. *Gráfico de distribuciones genuinas e impostoras*

Un punto de dichas graficas que nos permite caracterizar de forma directa el funcionamiento del sistema es el punto de igual error EER (*Equal Error Rate*) *Figura 2-40*, que es el punto donde las curvas de Falsa Concordancia (FM) y Falsa No Concordancia (FNM), en función del umbral, se cruzan. Por ello la tasa de igual error EER suele usarse para caracterizar con un único número el rendimiento de un sistema biométrico.

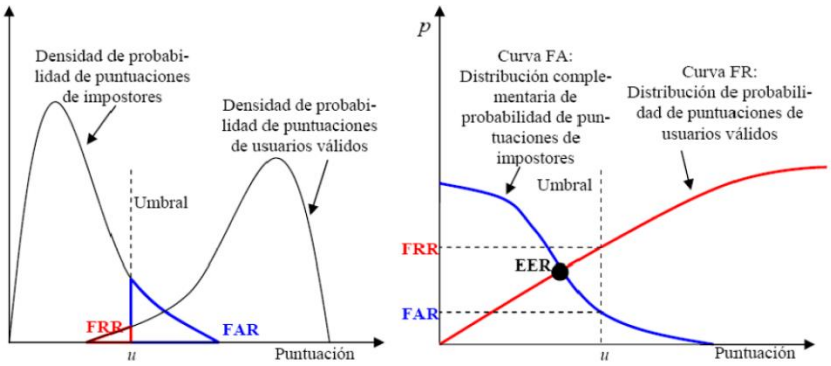


Figura 2-40. *Densidades y distribuciones de probabilidad de usuarios e impostores.*

A pesar de que el punto de EER corresponde al umbral donde se igualan FM y FNM, esto no implica que el sistema deba trabajar en ese punto. Para establecer el punto de trabajo del sistema se suele emplear la representación en forma de curvas DET (*Detection Error Tradeoff)*, que consiste en la presentación de FNMR (eje-Y) frente a FMR (eje-X), es decir, Tasa de Falsos Concordancia vs. Tasa Falsas No Concordancias *Figura 2-41*, obteniéndose así una única curva para ambos tipos de error definida por todos los posibles puntos de trabajo del sistema. La tasa EER, se localiza en la bisectriz del ángulo formado

por la parte positiva del eje de FMR y FNMR. Como el eje Y muestra el número de errores de coincidencia, la curva que está más cerca de la parte inferior del grafico corresponde al mejor rendimiento biométrico. Por ejemplo, la curva que se encuentra por encima de las otras (color rojo) *Figura 2-41* corresponde al peor rendimiento biométrico, muestra un FNMR de casi 8% para un FMR 1/1.000, mientras que la curva que se encuentra por debajo de las otras (línea puntos) presenta un FNMR menor al 2% para un FMR 1/1000.

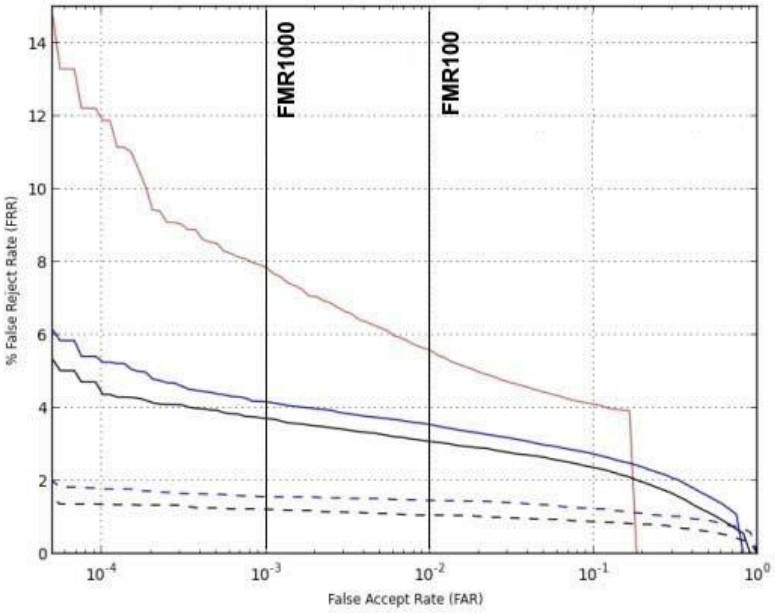


Figura 2-41. *Curva DET (Detection Error Tradeoff)*

Además de las distribuciones y las tasas FMR y FNMR, otros indicadores (Ferrara, Franco, & Maltoni, 2007) también son usados para expresar las prestaciones del sistema *Figura 2-42*:

- **Tasa de Igual Error (EER)**: denota la tasa de error del umbral *t* en el cual Tasa de Falsa Concordancia es igual a la Tasa de Falsa No Concordancia: FMR (*t*) = FNMR (*t*), A pesar de que ERR es un importante indicador, en la práctica no es común utilizar el punto de operación ERR, ya que por lo general se utiliza un umbral más alto para incrementar la seguridad del sistema.
- **FMR100**: el valor más bajo de FNMR para FMR <= 1%.
- **FMR1000**: el valor más bajo de FNMR para un FMR <=0.1%.
- **ZeroFMR**: es el valor más bajo de FNMR en el cual no se producen Falsas Concordancias.
- **ZeroFNMR**: es el valor más bajo de FMR en el cual no se producen Falsas No Concordancias.

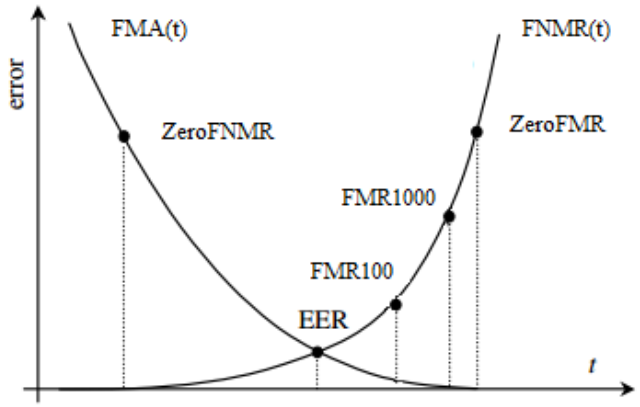


Figura 2-42. *Indicadores de las prestaciones de un sistema biométrico*

2.5.3 Selección de datos

La calidad de los datos de prueba de un sistema automático de reconocimiento biométrico y las condiciones en las que estos han sido adquiridos influye decisivamente en los resultados finales de evaluación. Las diferentes condiciones en las que se realiza el proceso de adquisición de las señales biométricas, que hacen que un mismo individuo, para un mismo rasgo, proporcione diferentes señales en diferentes adquisiciones, deben estar reflejadas en la base de datos de prueba. El empleo único de datos de baja o alta calidad refleja siempre el comportamiento del sistema en las peores o mejores condiciones que pueden darse en la práctica, respectivamente. La utilización de datos de prueba que no recogen todas las posibles situaciones puede dar lugar a una evaluación errónea, de la cual no pueden extrapolarse resultados aplicables al funcionamiento en condiciones normales. Por lo tanto, la selección de los datos de prueba, necesaria para conseguir una evaluación fiable y precisa, debe hacerse siempre teniendo en cuenta la generalidad de todas las situaciones que pueden darse durante el funcionamiento normal del sistema. Los resultados obtenidos tras la evaluación deben hacer siempre referencia a la base de datos de prueba utilizada.

2.6 Metodología de desarrollo de software utilizada

El trabajo final utiliza la Metodología Orientada a Objetos y el proceso de desarrollo RUP (*Rational Unified Process*), a continuación se describirá la metodología en forma general y también se darán los conceptos sobre el Lenguaje Unificado de Modelado (UML) utilizado.

2.6.1 Rational Unified Process

La metodología RUP (*Rational Unified Process*) emplea varias de las mejores prácticas en el desarrollo de software de manera que es aplicable para un amplio rango de proyectos y organizaciones a la vez que provee a cada miembro de un equipo un fácil acceso a una base de conocimiento con guías, plantillas y herramientas para todas las actividades de desarrollo (Lopez Illescas, Peña Herrera Aroca, & Rodriguez Veintimilla, 2004).

RUP es una metodología de desarrollo de software que intenta integrar todos los aspectos a tener en cuenta durante todo el ciclo de vida del software, con el objetivo de abarcar tanto pequeños como grandes proyectos de software. Los tres principios básicos de RUP son:

- Dirigido por casos de uso: La razón de ser de un sistema software es servir a usuarios (personas u otros sistemas), un caso de uso es una facilidad que el software debe proveer a sus usuarios. Los casos de uso reemplazan la antigua especificación funcional y constituyen la guía fundamental establecida para las actividades a realizar durante todo el proceso de desarrollo incluyendo el diseño, la implementación y las pruebas del sistema. Los casos de uso dirigen y controlan el proceso de desarrollo en su totalidad.
- Centrado en la arquitectura: La arquitectura de un sistema es la organización o estructura de sus partes más relevantes y constituye la pieza clave que permite comprender el sistema, organizar el desarrollo y hacer evolucionar el software. La arquitectura involucra los elementos más significativos del sistema y está influenciada entre otros por plataformas software, sistemas operativos, manejadores de bases de datos, protocolos, consideraciones de desarrollo como sistemas heredados y requerimientos no funcionales.
- Proceso iterativo e incremental: Para hacer más manejable un proyecto se recomienda dividirlo en ciclos, para cada ciclo se establecen fases de referencia, cada una de las cuales debe ser considerada como un mini proyecto cuyo núcleo fundamental está constituido por una o más iteraciones de las actividades principales básicas de cualquier proceso de desarrollo. El desarrollo se plantea de manera progresiva, de tal modo que se atenúen los riesgos y se planteen las cuestiones en el instante en que se está capacitado para resolverlas.

2.6.2 Fases de la metodología RUP

El RUP se repite a lo largo de una serie de ciclos que constituyen la vida de un sistema. Cada ciclo consta de cuatro etapas, como se ve en la *Figura 2-43*:

- **Inicio:** se define el alcance del proyecto y se desarrollan los casos de negocio.
- **Elaboración:** se planifica el proyecto, se especifican en detalle la mayoría de los casos de uso y se diseña la arquitectura del sistema.
- **Construcción:** se construye el producto.
- **Transición:** el producto se convierte en versión beta. Se corrigen problemas y se incorporan mejoras sugeridas en la revisión.

Dentro de cada etapa se puede, a su vez, descomponer el trabajo en iteraciones con sus incrementos resultantes.

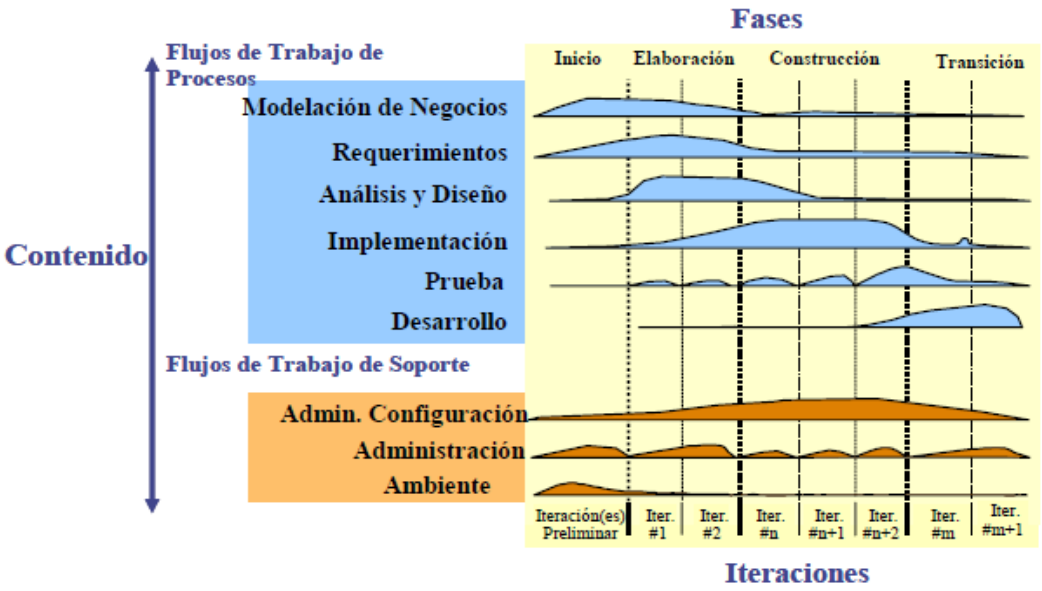


Figura 2-43. *Estructura RUP*

Las actividades que se realizan en las fases se dividen en dos grupos, denominados f**lujos de trabajo de proceso** y **flujo de trabajo de soporte**.

2.6.2.1 Flujos de Trabajo de Soporte

Involucran actividades de administración y planificación de recursos humanos, tecnológicos y financieros.

Gestión del Cambio y Configuraciones: la finalidad de este flujo de trabajo es mantener la integridad de todos los artefactos que se crean en el proceso, así como de mantener información del proceso evolutivo que han seguido.

Gestión del Proyecto: pretende lograr un balance al gestionar objetivos, riesgos y restricciones para desarrollar un producto que sea acorde a los requerimientos de los clientes y los usuarios. La planeación de un proyecto posee dos niveles de abstracción: un plan para las fases y un plan para cada iteración.

Ambiente o Entorno: Ia finalidad de este flujo de trabajo es dar soporte al proyecto con las adecuadas herramientas (selección y configuración), procesos y métodos. Brinda una especificación de las herramientas que se van a necesitar en cada momento, así como definir la instancia concreta del proceso que se va a seguir.

2.6.2.2 Flujos de Trabajo del Proceso

Agrupa las actividades que están asociados a la construcción propiamente dicha del software. Los flujos de trabajos del proceso son la forma de describir significativamente las secuencias de actividades que producen resultados (modelos) y las interacciones. Los modelos recogen diferentes perspectivas del sistema y un sistema posee una colección de modelos y las relaciones entre ellos.

Modelado del Negocio: con este flujo de trabajo se pretende llegar a un mejor entendimiento de la organización donde se va a implantar el producto. El modelo de negocio describe como desarrollar una visión de la nueva organización, basado en esta visión se definen procesos, roles y responsabilidades de la organización por medio de un modelo de Casos de Uso del negocio y un Modelo de Objetos del Negocio. Complementario a estos modelos, se desarrollan otras especificaciones tales como un Glosario.

Requerimientos: el objetivo es describir lo que el sistema bebería hacer y permite a los desarrolladores y clientes ponerse de acuerdo en esa descripción. La captura de los requerimientos resulta en un modelo de casos de uso y algunos requerimientos suplementarios. El modelo de casos de uso es esencial tanto para el cliente, que puede validar lo que espera del sistema, y para los desarrolladores, quienes necesitan el modelo para un mejor entendimiento del sistema. Los requerimientos funcionales representan la funcionalidad del sistema. Se modelan mediante diagramas de Casos de Uso. Los requerimientos no funcionales representan aquellos atributos que debe exhibir el sistema, pero que no son una funcionalidad específica.

Análisis y Diseño El objetivo es enseñar como el sistema será realizado en la fase de implementación. En la fase de análisis se trabaja con abstracciones primarias (clases y objetos) y los mecanismos presentes en el dominio del problema. Se identifican las relaciones entre clases y son descriptas en un diagrama de clases. Por otro lado el diseño es un refinamiento del análisis que tiene en cuenta los requerimientos no funcionales, en definitiva cómo cumple el sistema sus objetivos. El resultado final más importante de este flujo de trabajo será el modelo de diseño. Consiste en colaboraciones de clases, que pueden ser agregadas en paquetes y subsistemas.

Implementación En este flujo de trabajo se implementan las clases y objetos en ficheros fuente, binarios, ejecutables y demás. Además se deben hacer las pruebas de unidad: cada implementador es responsable de probar las unidades que produzca. El resultado final de este flujo de trabajo es un sistema ejecutable. La estructura de todos los elementos implementados forma el modelo de implementación, la integración debe ser incremental, de este modo es más fácil localizar fallos y los componentes se prueban más a fondo.

Pruebas: este flujo de trabajo es el encargado de evaluar la calidad del producto que se desarrolla, pero no para aceptar o rechazar el producto al final del proceso de desarrollo, sino que debe ir integrado en todo el ciclo de vida.

Despliegue: el objetivo de este flujo de trabajo es producir con éxito distribuciones del producto distribuirlo a los usuarios. Este flujo de trabajo se desarrolla con mayor intensidad en la fase de transición, ya que el propósito del flujo es asegurar una aceptación y adaptación sin complicaciones del software por parte de los usuarios. Su ejecución inicia en fases anteriores, para preparar el camino, sobre todo con actividades de planificación, en la elaboración del manual de usuario y tutoriales.

2.6.3 El lenguaje unificado de modelado (UML)

El UML es la creación de Graby Booch, James Rumbugh e Ivar Jacobson, que trabajaban en empresas distintas durante la década de los ochenta y principios de los noventa y cada uno diseñó su propia metodología para el análisis y diseño orientado a objetos. A mediados

de los noventa empezaron a intercambiar ideas entre si y decidieron desarrollar su trabajo en conjunto (Schmuller, 2001).

La primera versión se ofreció a un grupo de trabajo para convertirlo en 1997 en un estándar del *Object Management Group* (OMG). Este grupo, que gestiona estándares relacionados con la tecnología orientada a objetos (metodologías, bases de datos orientadas a objetos, CORBA, etc.), propuso una serie de modificaciones y una nueva versión de UML (la 1.1), que fue adoptada por el OMG como estándar en noviembre de 1997. Desde aquella versión ha habido varias revisiones que gestiona la *OMG Revisión Task Force*.

2.6.3.1 El poder de UML

UML satisface una necesidad importante en el desarrollo de software. Especialmente el modelado de una manera que se comprende fácilmente, permite que el desarrollador se concentre en la imagen global del sistema. Ayuda a ver y resolver los problemas importantes primero, e impide distraerse en detalles que se pueden omitir para más adelante. Al modelar, se construye una abstracción de un sistema existente del mundo real, que permite hacer preguntas del modelo y obtener buenas respuestas sin necesidad de desarrollar ninguna parte del sistema.

2.6.3.2 Diagramas UML

El UML está compuesto por diversos elementos gráficos que se combinan para conformar diagramas. La finalidad de estos diagramas es presentar diversas perspectivas de un sistema, a las cuales se las conoce como *modelo.* Este modelo UML describe lo que supuestamente hará un sistema, pero no dice cómo implementar dicho sistema.

Existen varios tipos de diagramas, a continuación se da un breve esbozo sobre los diagramas utilizados para el desarrollo de este trabajo:

Diagramas de caso de uso: principalmente documentan los macro requerimientos del sistema. Los símbolos principales son el *actor* y *el óvalo del caso de uso Figura 2-44.*

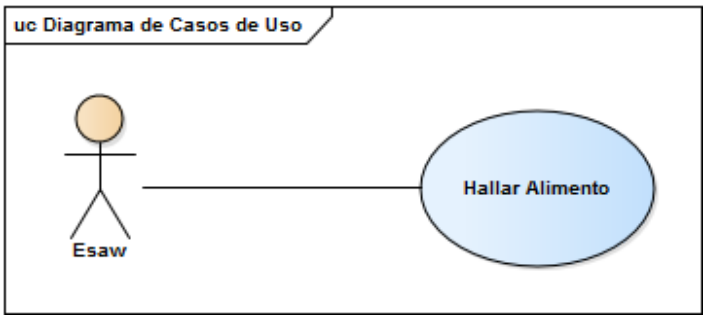


Figura 2-44. *El caso de uso "Hallar alimento".*

Diagrama de secuencia: se usan para destacar la ordenación temporal de los mensajes, se forma colocando en primer lugar los objetos que participan en la interacción en la parte superior del diagrama, a lo largo del eje X. Normalmente, se coloca a la izquierda el objeto que inicia la interacción, y los objetos subordinados a la

derecha. A continuación, se colocan los mensajes que estos objetos envían y reciben a lo largo del eje Y, en orden de sucesión en el tiempo, desde arriba hasta abajo. Esto permite una señal visual clara del flujo de control a lo largo del tiempo. La línea de vida de un objeto, es la línea vertical discontinua que representa la existencia de un objeto a lo largo de un periodo de tiempo. Pueden crearse objetos durante la interacción. Sus líneas de vida aparecen cuando reciben el mensaje estereotipado como <<*create*>>. Los objetos pueden destruirse durante la interacción. Sus líneas de vida acaban con la recepción del mensaje estereotipado como <<*destroy*>> El foco de control que es un rectángulo estrecho situado sobre la línea de vida que representa el período de tiempo durante el cual un objeto ejecuta una acción, bien sea directamente o a través de un procedimiento subordinado *Figura 2-45*.

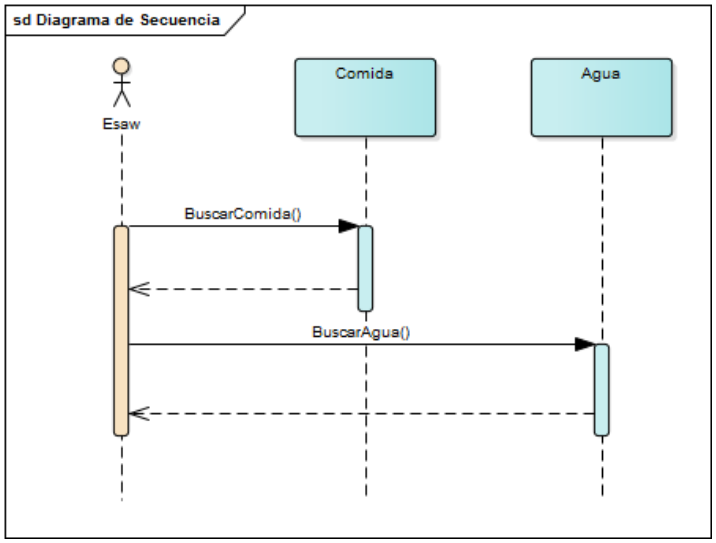


Figura 2-45. *Diagrama de secuencia*

Diagramas de clase: Se usan para mostrar las clases de un sistema y las relaciones entre ellas *Figura 2-46*. Una sola clase puede mostrarse en más de un diagrama de clases y no es necesario mostrar todas las clases en un solo diagrama monolítico de clases. El mayor valor es mostrar las clases y sus relaciones desde varias perspectivas, de una manera que ayudará a transmitir la comprensión más útil.

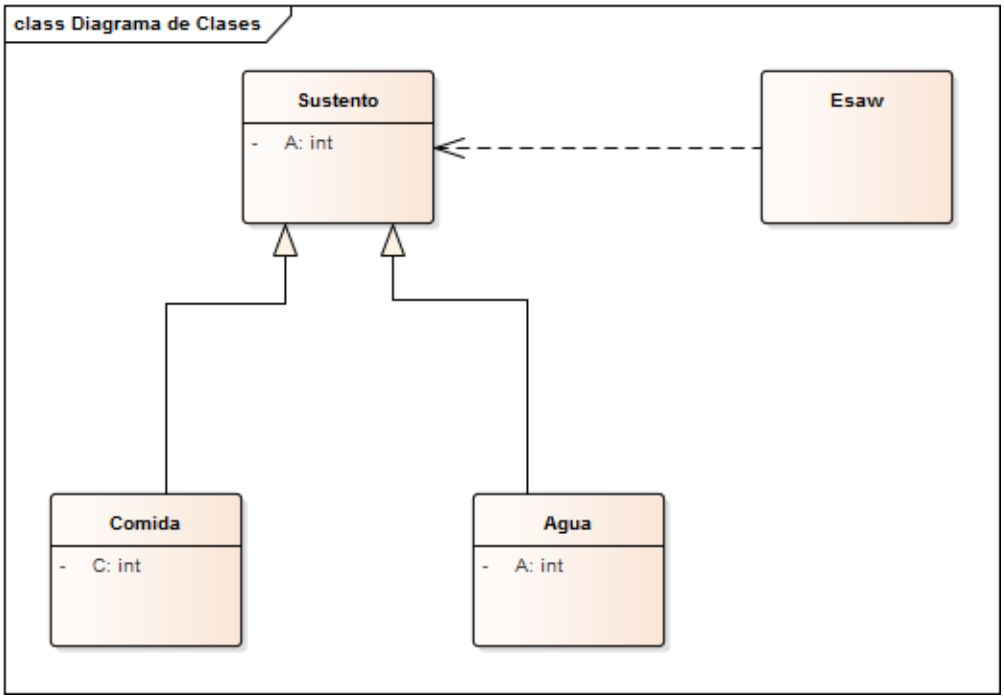


Figura 2-46. *Diagrama de clases*

CAPÍTULO III

Desarrollo de la aplicación de reconocimiento de huellas digitales

3.1 Introducción

Este capítulo muestra la aplicación de Proceso RUP en el desarrollo de la aplicación, se detallan las actividades que se llevaron a cabo en los *Flujos de Trabajo de Soporte* y *Flujos de Trabajo de proceso*, para el desarrollo de la aplicación, mencionando los artefactos que se produjeron como resultado de estas actividades.

3.2 RUP: Flujos de trabajo de soporte

A continuación se muestran los artefactos obtenidos dentro de este Flujo de trabajo de soporte que se realizaron:

- La gestión de cambios y configuraciones
- Configuración del ambiente o entorno

3.2.1 Gestión de cambios y configuraciones

Se llevó a cabo un conjunto de procesos destinados a asegurar la calidad del producto obtenido a través del control de los cambios realizados sobre artefactos para una disponibilidad constante de una versión estable de cada elemento. Esta tarea incluyó el control de cambio de documentos, modelos y cambio en el código fuente.

3.2.1.1 Cambios en los documentos y modelos

Para el almacenamiento, sincronización y soporte de historial de revisiones se utilizó el servicio de alojamiento de archivos en la nube Dropbox[1], para los documentos y los modelos generados en el proceso de desarrollo.

3.2.1.2 Control de cambios de código fuente

Para el control de cambio de código fuente se usó el controlador de versiones Subversión SVN[2], como cliente se utilizó la herramienta TortoiseSVN[3] y se utilizó Assembla[4] como host para el alojamiento.

3.2.2 Ambiente o entorno

En este flujo de trabajo se tuvo en cuenta el ambiente de ejecución, recursos hardware y herramientas necesarias para llevar a cabo el desarrollo. Se realizaron un conjunto de actividades destinadas a determinar el soporte al proyecto con la selección y configuración de las herramientas adecuadas. Se brinda una especificación de las herramientas que se utilizaron en cada momento del desarrollo.

[1] Servicio de alojamiento de archivos multiplataforma en la nube: https://www.dropbox.com/
[2] Subversión SVN es una herramienta de control de versiones open source basada en un repositorio cuyo funcionamiento se asemeja enormemente al de un sistema de ficheros: https://subversion.apache.org/
[3] Cliente del Subversion, implementado como una extensión shell de Windows: https://tortoisesvn.net/
[4] Provee herramientas de colaboración y de seguimiento de errores: https://app.assembla.com/

3.2.2.1 Recursos de hardware

Para el desarrollo de la herramienta se utilizó los siguientes recursos tecnológicos de hardware Tabla 3-1:

Recurso	Especificación	Utilidad
Notebook	Positivo BGH Intel Core i3-3217U	Desarrollo del aplicativo y pruebas de rendimiento
Lector Bioemtrico	Escaner Digital Persona U.areU 4500	Escaner de huella digital

Tabla 3-1. *Recursos de hardware*

3.2.2.2 Herramientas para el desarrollo del aplicativo

- **Herramienta de modelado**

  La herramienta utilizada para el análisis y el diseño es *Enterprise Architect v12.1.1227.*

- **Entorno de Desarrollo Integrado (IDE)**

  El entorno utilizado es *Visual Studio v14.0.23.*

- **Control de versión**

  El sistema de control de versiones utilizado es *Subversion (SVN)*. Se utilizó *TortoiseSVN* como interfaz cliente de SVN y como proveedor de host, se utilizó *Assembla.* https://www.assembla.com/

- **Herramienta para administrar la Base de Datos**

  Para administrar la Base de Datos *FirebirdSQL*, se utilizó la herramienta *IBExpert v2012.02.21.*

- **Herramientas de Gráficos**

  Para generar los gráficos, se utilizó *MATLAB v9.0.0.*

3.3 RUP: Flujos de trabajo de proceso

A continuación se muestra los artefactos obtenidos de los flujos de trabajos de procesos del RUP aplicados, los cuales fueron:

- Modelado del Negocio
- Requerimientos
- Análisis y diseño
- Implementación
- Pruebas
- Despliegue

3.3.1 Modelado del negocio

El modelo del negocio está formado por el Modelo del Dominio y el Modelo de Casos de Uso (CU) que permiten ver el contexto de la aplicación desarrollada.

Las actividades que se realizaron son:

- Identificación de Procesos de Negocio
- Identificación de actores con sus roles del entorno del negocio.
- Descripción de los Casos de Uso del Negocio
- Identificar los objetos del negocio

Artefactos que se obtuvieron son:

- Modelo del Dominio que se compone del diagrama de clases del dominio.
- Modelo de Casos de Uso del Negocio que está compuesto por el diagrama de CU del negocio, descripción de los actores del negocio y descripciones de esos CU.

3.3.1.1 Modelo del dominio

Es un modelo inicial de los objetos que se utilizaron en la aplicación, en primer momento se identificaron los objetos que son componentes del reconocimiento y evaluación de rendimiento del aplicativo de reconocimiento de huellas digitales *Figura 3-1*.

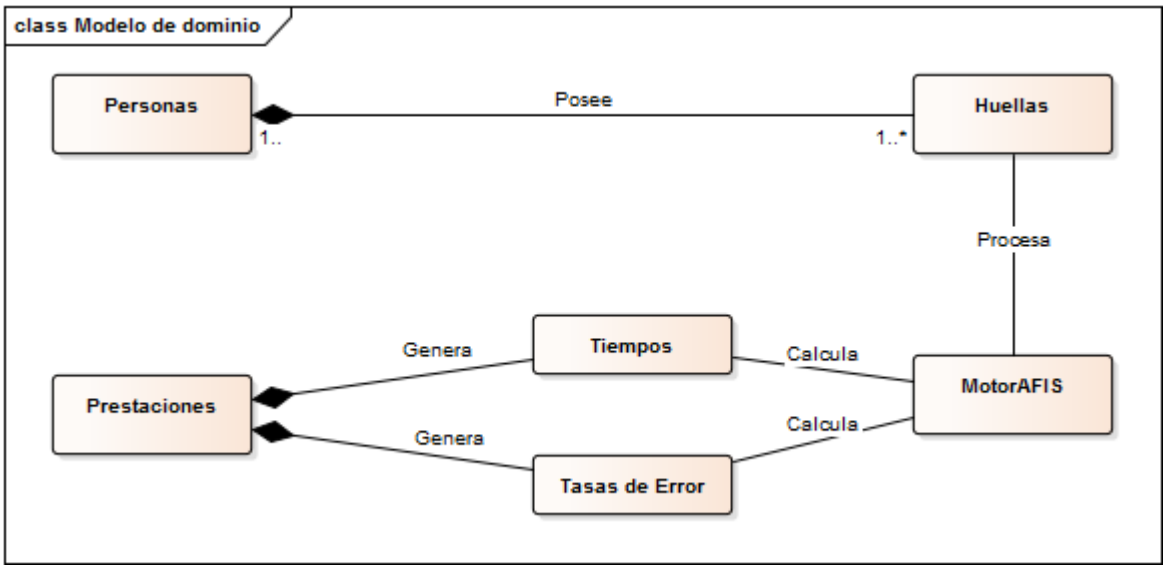


Figura 3-1. *Modelo del Dominio*

3.3.1.2 Modelo de casos de uso del negocio

El modelo de casos de uso del negocio está compuesto por los casos de uso del negocio, actores del negocio y descripciones de esos CU, que muestran las principales funciones del sistema desarrollado.

El modelado del negocio se basa en el diagrama de casos de uso del negocio mostrado en la *Figura 3-2*

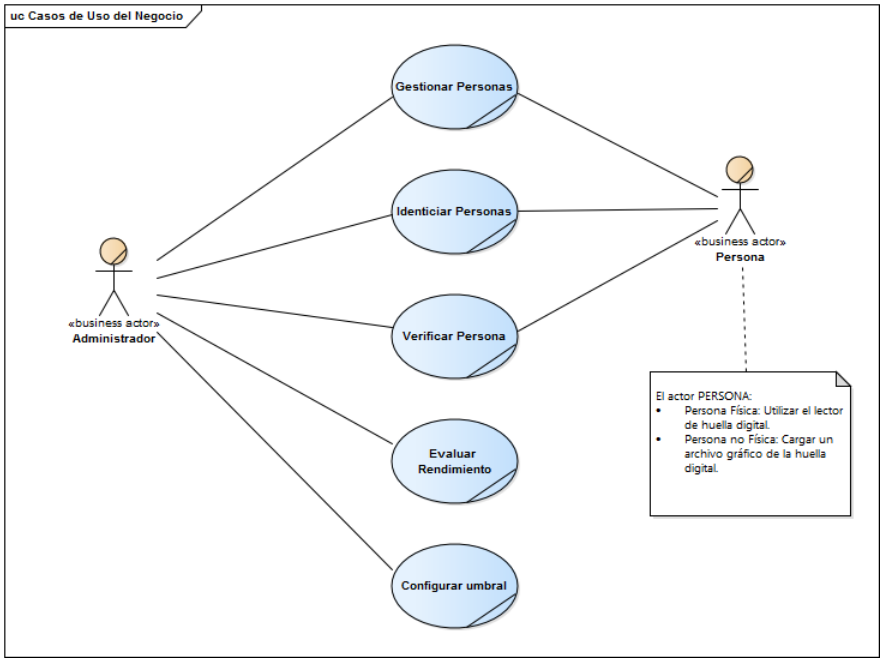


Figura 3-2. *Modelo de caso de uso del negocio.*

3.3.1.3 Actores del negocio

- Administrador: es el responsable del manejo de la aplicación, la cual consiste en acceder al sistema, gestionar los datos de las personas, definir los parámetros para el reconocimiento y obtener los datos para evaluar el rendimiento del módulo de reconocimiento utilizando técnicas de extracción de minucias.
- Persona: es la persona que se pretende reconocer, pude ser una persona física, en tal caso la huella se captura utilizando el lector de huellas digitales.

3.3.1.4 Descripción Textual de Casos de Uso

- Caso de uso Gestionar Personas: este CU brinda la posibilidad capturar los datos de las personas que ingresaran al sistema, además de los datos personales, también se capturan los datos biométricos. El caso de uso además permite modificar y eliminar los datos ingresados.
- Caso de uso Identificar Personas: este CU permite identificar una persona. Se captura la huella digital y se reconoce a la persona realizando N comparaciones en la base de datos

- Caso de uso Verificar Persona: este CU permite reconocer una persona. Se captura la huella digital y se verifica la identidad de la persona realizando una comparación en la base de datos con el PIN o clave suministrado por la persona.
- Caso de uso Evaluar Rendimiento: este CU permite obtener las tasas de reconociendo así como también la velocidad de procesamiento del módulo de reconocimiento.
- Caso de uso Configurar Umbral: este CU permite modificar el umbral del sistema

3.3.2 Requerimientos

Durante este flujo de trabajo de proceso se realizaron las siguientes actividades:

- Identificación de requerimientos funcionales y no funcionales
- Se identificaron restricciones y dependencias.
- Se identificaron los actores y CU
- Se generó el modelo de CU el cual contiene los diagramas de casos de usos.
- Especificación de flujos de sucesos de los CU identificados.

Artefactos que se obtuvieron:

- Especificación de requerimientos funcionales y no funcionales.
- Especificación restricciones y dependencias
- Modelo de casos de usos: compuesto de diagramas de CU y la especificación de los flujos de sucesos

3.3.2.1 Requerimientos funcionales

La aplicación desarrollada debe:

- Permitir gestionar datos personales y biométricos de las personas.
- Permitir identificar una persona por medio de su huella digital.
- Permitir verificar la identidad de una persona con su PIN y su huella digital.
- Permitir modificar los parámetros del módulo de reconocimiento.
- Proveer las tasas de rendimiento y velocidad de ejecución del módulo de reconocimiento.

3.3.2.2 Requerimientos no funcionales

- El desarrollo e implementación de la aplicación está basada en la tecnología .NET.
- La aplicación corre bajo el sistema operativo Windows 7 o superior.
- Para la obtención de las tasas de error y tiempos, se necesitan imágenes de huellas digitales, por ejemplo *NIST Special Database 4* (NIST, 2017).

3.3.2.3 Restricciones

- La aplicación solo aceptara una imagen de huella digital por persona.
- El tamaño de la imagen de huella digital tiene que ser mayor a 100 x 100 pixeles.

3.3.2.4 Modelo de Casos de Uso

El siguiente modelo de Caso de Uso describe los requerimientos funcionales del aplicativo en forma de diagramas de Casos de Uso.

Diagrama de casos de uso GESTIONAR PERSONAS

En este diagrama se presentan las necesidades cubiertas para el actor Administrador, quien es el encargado de gestionar los datos personales y biométricos de los individuos que se cargan en el sistema *Figura 3-3*.

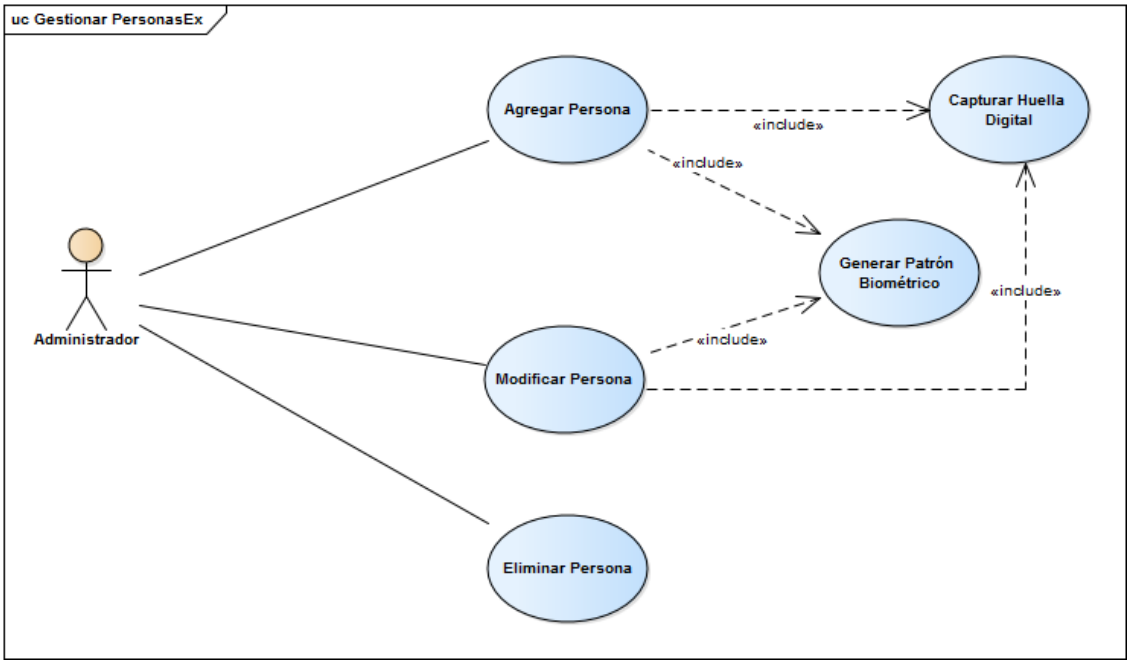


Figura 3-3. *Diagrama de caso de uso –Gestionar Personas.*

Descripción del CU: Agregar Persona

El administrador genera un nuevo registro, almacenando los datos de la persona y sus datos biométricos.

Flujos de Sucesos

Iniciador	Administrador
Precondición	Ninguna
Camino básico	
Actor	**Sistema**
1. Solicita agregar persona	
	2. Habita el campo DNI
3. Carga el DNI de la persona	
	4. Verifica si el DNI no está almacenado. 5. Habilita los campos de edición.

6. Carga datos. 7. Carga Imagen de la Huella digital.	
	8. Genera el patrón biométrico
9. Solicita almacenar datos	
	10. Almacena los datos. 11. Muestra mensaje de operación correcta. 12. El caso de uso finaliza.
Camino alternativo 1	En el **Paso 3** si los datos de la persona ya se encuentran almacenados, envía mensaje solicitando verificar el DNI cargado.
Camino alternativo 2	En el **Paso 7** si la huella no puede ser capturada se vuelve al **Paso 6**.
Camino alternativo 3	Después de **Paso 1**, el Actor puede cancelar cambios y el caso de uso finaliza
Poscondición	Los datos de una persona quedan registrados.

Descripción del CU: Modificar Persona

El administrador edita los datos de una persona que cuyos datos se encuentran almacenados.

Flujos de Sucesos

Iniciador	Administrador
Precondición	Datos de personas almacenados
Camino básico	
Actor	**Sistema**
1. Ingresa datos de persona a buscar.	
	2. Busca los datos de la persona
3. Solicita la modificación de datos	
	4. Habilita los campos de edición 5. Deshabilita el campo DNI.
6. Modifica los datos. 7. Carga Imagen de la Huella digital.	
	8. Genera el patrón biométrico
9. Solicita almacenar datos	
	10. Almacena los datos. 11. Muestra mensaje de operación correcta. 12. El caso de uso finaliza.
Camino alternativo 1	En **Paso 2** si no se encuentra la persona se informa al actor y el caso de uso finaliza

Camino alternativo 2	En **Paso 7** en caso de no modificar el patrón biométrico, se pasa al **Paso 10**.
Camino alternativo 3	En el **Paso 7** si la huella no puede ser capturada se vuelve al **Paso 6**.
Camino alternativo 4	Después de **Paso 1**, el Actor puede cancelar cambios y el caso de uso finaliza.
Poscondición	Los datos de una persona quedan actualizados.

Descripción del CU: Eliminar Persona

El administrador edita los datos de una persona que cuyos datos se encuentran almacenados.

Flujos de Sucesos

Iniciador	Administrador
Precondición	Datos de personas almacenados

Camino básico	
Actor	**Sistema**
1. Ingresa datos de persona a buscar	
	2. Busca los datos de la persona
3. Solicita la eliminación de datos	
	4. Solicita confirmación
5. Confirma eliminación	
	6. Elimina datos almacenados 7. Muestra mensaje de operación correcta. 8. El caso de uso finaliza.

Camino alternativo 1	En el **Paso 2** si no se encuentra la persona se informa al actor y el caso de uso finaliza
Camino alternativo 2	En el **Paso 5** si no el actor no confirma la eliminación, los datos quedan almacenados y el caso de uso finaliza.
Poscondición	Los datos de una persona son eliminados.

Diagrama de casos de uso IDENTIFICAR PERSONAS

En este diagrama se describe la funcionalidad de la identificación de personas *Figura 3-4*. El sistema determina la identidad de una persona a partir de una imagen de su huella digital, buscando en los registros de huellas en la base de datos.

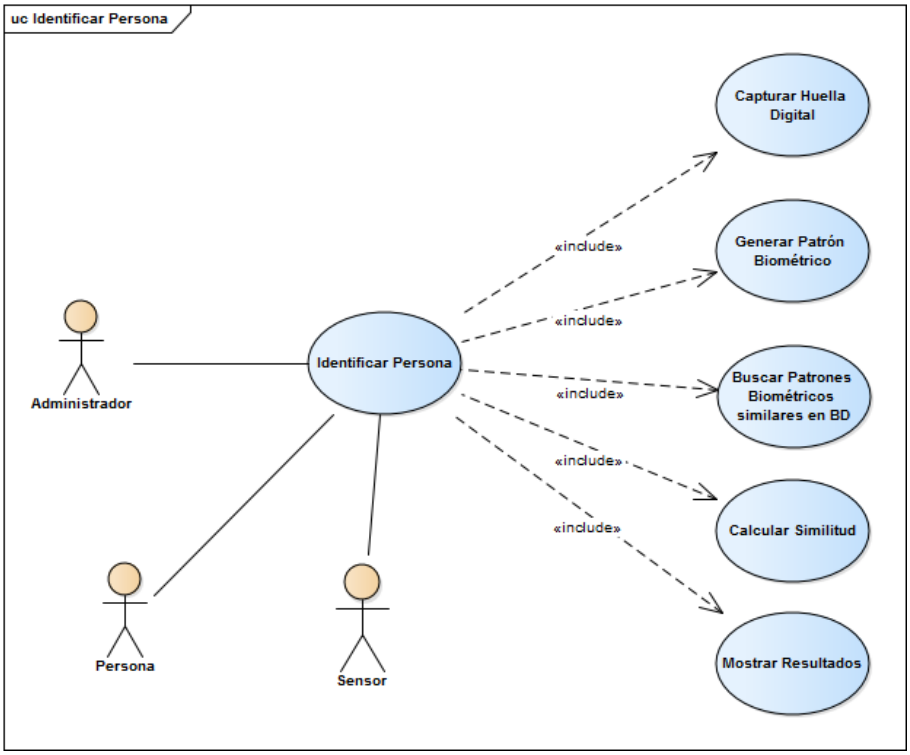


Figura 3-4. *Identificar persona*

Flujo de sucesos

Iniciador	Administrador
Precondición	Personas cargadas en la base de datos.
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Identificación.	
	1. Activa el sensor de captura 2. Espera por imagen
3. Presiona el sensor 4. Envía imagen	

	5. Genera un patrón biométrico de la huella digital capturada. 6. Realiza una comparación entre el patrón biométrico generado y los patrones biométricos almacenados en la base de datos. 7. Obtiene el patrón biométrico con mayor puntuación por encima del umbral establecido. 8. Calcula la similitud entre el patrón biométrico generado en **Paso 6** y el obtenido en **Paso 8**. 9. Obtiene los datos personales relacionados con el patrón similar. 10. Muestra la información de la persona identificada y el grado de similitud con el patrón biométrico obtenido. 11. El caso de uso finaliza.
Camino alternativo 1	**Paso 3**: Se carga la imagen de la huella digital desde un archivo y continúa el CU en el **Paso 6**.
Camino alternativo 2	**Paso 5:** Si no se envía una imagen de la huella digital, no se permite continuar con el CU.
Camino alternativo 3	**Paso 8:** Si no encuentra un patrón biométrico que supere el umbral, se informa esta condición y finaliza el CU.

Diagrama de casos de uso VERIFICAR PERSONAS

En este diagrama se describe la funcionalidad de la velicación de personas *Figura 3-5,* donde el sistema verifica la identidad de una persona a partir de una imagen de su huella digital y un PIN (DNI), comparando el patrón biométrico de la imagen con el patrón biométrico almacenado en la base de datos correspondiente a PIN suministrado.

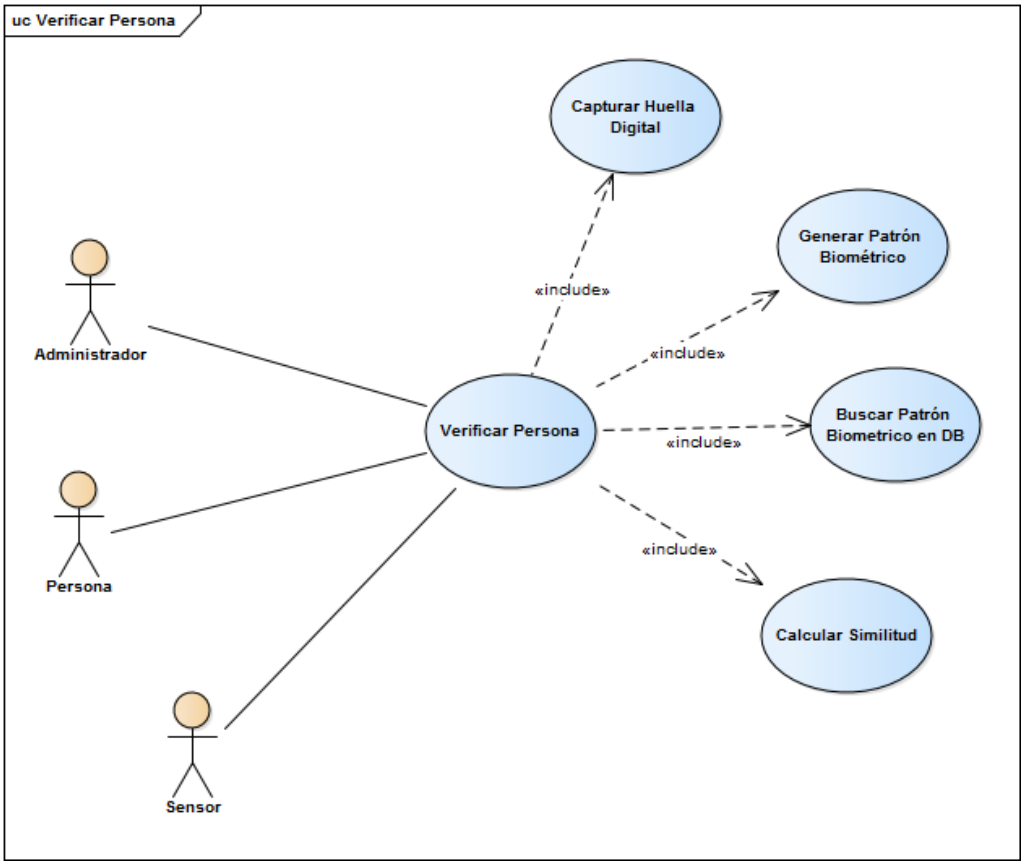


Figura 3-5. *Diagrama de Casos de Uso Verificar Persona*

Flujo de sucesos

Iniciador	Administrador
Precondición	Personas almacenadas.
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Verificación.	
	2. Activa el sensor de captura 3. Espera por imagen

4. Carga el DNI de la persona a verificar. 5. Presiona el sensor 6. Envía imagen	
	7. Genera un patrón biométrico de la huella digital capturada. 8. Obtiene el patrón biométrico almacenado en la base de datos, según DNI ingresado. 9. Calcula la similitud entre el patrón biométrico generado en **Paso 6** y el obtenido en **Paso 7**. 10. Obtiene los datos personales relacionados con el patrón similar. 11. Muestra información de verificación valida o invalida. 12. El caso de uso finaliza.
Camino alternativo 1	**Paso 3**: Se carga la imagen de la huella digital desde un archivo y continúa el CU en el **Paso 6**.
Camino alternativo 2	**Paso 4**: Si no se carga un DNI, no se permite continuar con el CU.
Camino alternativo 3	**Paso 6:** Si no se envía una imagen de la huella digital, no se permite continuar con el CU.

Diagrama de casos de uso DETERMINAR PRESTACIONES

En este diagrama describe la funcionalidad que le permite al administrador calcular, consultar y exportar las prestaciones del sistema *Figura 3-6*.

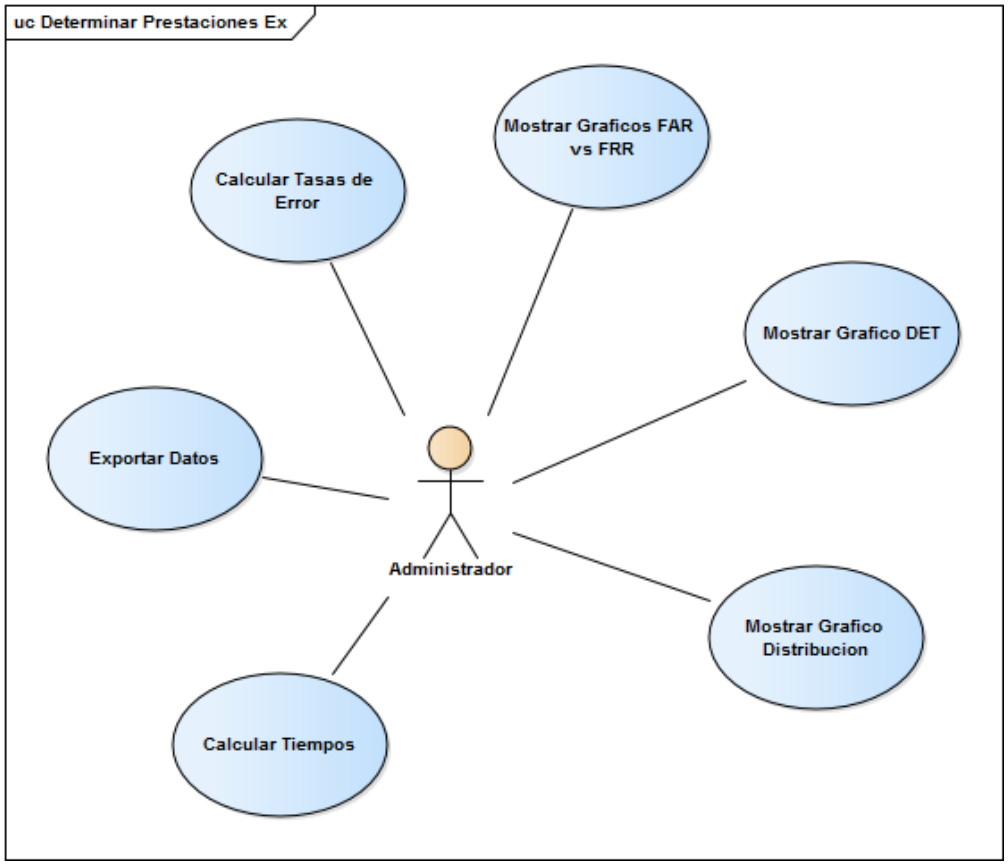


Figura 3-6. *Diagrama de Casos de Uso Determinar Prestaciones*

Descripción del CU Calcular Tasas de Error

Calcula las tasas de Falsa Rechazo, Falsa Aceptación y Tasa de Igual Error para una base de datos de prueba.

Flujo de sucesos

Iniciador	Administrador
Precondición	Bases de Datos de pruebas cargadas
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Calcular Tasas de Error.	
	2. Muestra datos disponibles
3. Selecciona Base de Datos.	

	4. Calcula Tasas de Falso Rechazo. 5. Guarda Tasas. 6. Calcula Tasas de Falsa Aceptación. 7. Guarda Tasas. 8. Calcula Tasa de Igual Error. 9. Guarda Prestaciones 10. El caso de uso finaliza.
Poscondición	Prestaciones Calculadas para la Base de Datos Seleccionada

Descripción del CU Calcular Tiempos

Calcula los tiempos de Registro, Comparación Genuina y Comparación Falsa, para una base de datos de prueba.

Flujo de sucesos

Iniciador	Administrador
Precondición	Bases de Datos de pruebas cargadas
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Calcular Tiempos.	
	2. Muestra Bases de Datos disponibles
3. Selecciona Base de Datos.	
	4. Calcula Tiempo de Registro. 5. Guarda Tiempos. 6. Calcula Tiempo de Comparación Genuina. 7. Guarda Tiempos. 8. Calcula Tiempo de Comparación Falsa. 9. Guarda Tiempos 10. El caso de uso finaliza.
Poscondición	Tiempos Calculados para la Base de Datos Seleccionada

Descripción del CU Mostrar Gráfico de Distribución

Genera y muestra el grafico de distribución, para una base de datos de prueba.

Flujo de sucesos

Iniciador	Administrador
Precondición	Puntuaciones calculadas
Camino básico	
Actor	**Sistema**

1. Solicita Operación de Mostrar Gráfico de distribución.	
	2. Muestra Bases de Datos disponibles
3. Selecciona Base de Datos.	
	4. Obtiene las puntuaciones almacenadas. 5. Genera el gráfico 6. Muestra el gráfico. 7. El caso de uso finaliza.

Descripción del CU Mostrar Gráfico FAR vs FRR

Genera y muestra el grafico FAR vs FRR, para una base de datos de prueba.

Flujo de sucesos

Iniciador	Administrador
Precondición	Tasas de error calculadas
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Mostrar Gráfico FAR vs FRR.	
	2. Muestra datos disponibles
3. Selecciona datos.	
	4. Obtiene las tasas de error de la base de datos. 5. Muestra el grafico. 6. El caso de uso finaliza.

Descripción del CU Mostrar Gráfico DET

Genera y muestra el grafico DET, de todas las base de datos de pruebas.

Flujo de sucesos

Iniciador	Administrador
Precondición	Tasas de error calculadas
Camino básico	
Actor	**Sistema**
1. Solicita Operación de Mostrar Gráfico DET.	
	2. Obtiene las tasas de error de la base de datos. 3. Muestra el grafico. 4. El caso de uso finaliza.

Descripción del CU Exportar Datos

Obtiene los datos almacenados y genera archivos (formato “txt”).

Flujo de sucesos

Iniciador	Administrador	
Precondición	Puntuaciones calculadas Tasas de error calculadas	
Camino básico		
Actor		**Sistema**
5. Solicita Operación Exportar datos.		
		6. Obtiene las puntuaciones de todas las base de datos. 7. Obtiene las tasas de error de todas las bases de datos 8. Genera los archivos de datos. 9. El caso de uso finaliza.

Diagrama de casos de uso CONFIGURAR UMBRAL

Este diagrama presenta la funcionalidad para que el Administrador configure el umbral del sistema *Figura 3-7*.

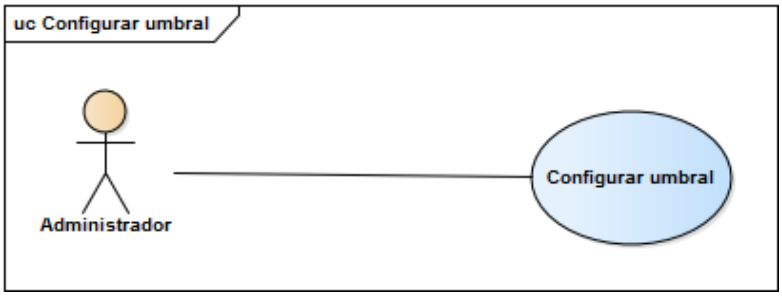


Figura 3-7. *Digrama de Casos de Uso Configurar Umbral*

Flujo de sucesos

Iniciador	Administrador	
Precondición	almacenes de pruebas cargadas	
Camino básico		
Actor		**Sistema**
1. Solicita Configurar Umbral.		
		2. Muestra el valor del umbral actual
3. Modifica el valor del umbral.		
		4. Guarda el nuevo valor del umbral. 5. Muestra mensaje de operación exitosa 6. El caso de uso finaliza.
Poscondición	Nuevo umbral del sistema guardado en Base de Datos	

3.3.3 Análisis y diseño

Se presenta el modelo de análisis y diseño obtenido de este flujo de trabajo de proceso.

Las actividades que se realizaron son:

- Identificación de las clases
- Realización de los CU mediante un diagrama de clases genérico y diagramas de secuencias para cada CU.
- Elección de patrones de diseño
- Definición de las salidas de la aplicación

Artefactos que se obtuvieron:

- Modelo de Análisis y Diseño: compuesto por el diagrama de clases y diagramas de secuencias.
- Especificación de Patrones de diseño utilizados
- Especificación de archivos de salida

3.3.3.1 Diagrama de clases

Para la realización de CU se realizó el diagrama de clases con las clases que se usan para realizar todos los CU: Gestionar Personas, Identificar Persona, Verificar Persona, Evaluar Rendimiento y Configurar Umbral *Figura 3-8*, contenidos en los diagramas CU de los modelos de casos de uso, también se muestra los diagramas de secuencias para el flujo de suceso básico de cada CU.

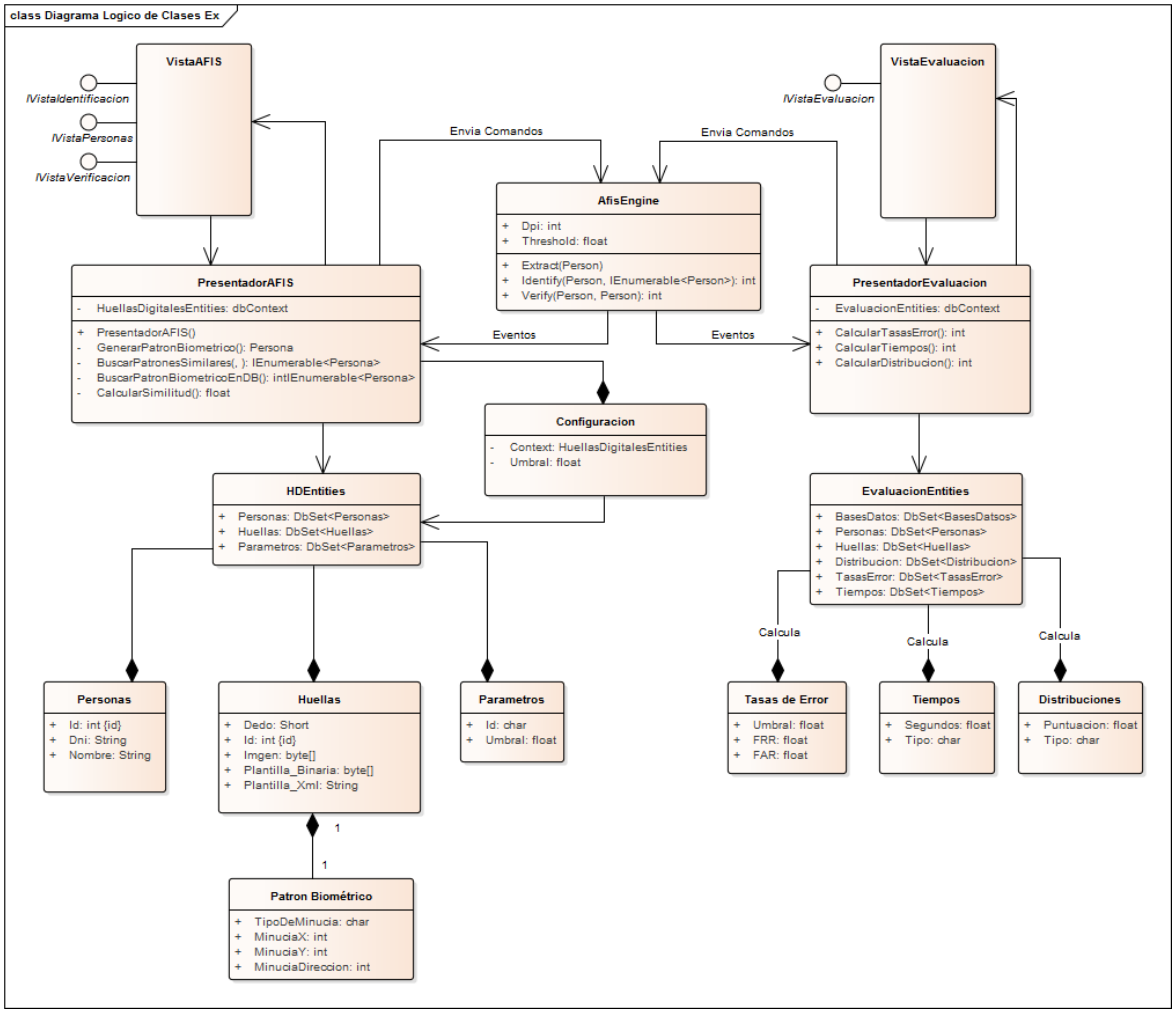


Figura 3-8. *Diagrama de clases General*

3.3.3.2 Diagramas de secuencia

Se presenta la realización de los siguientes CU:

- Alta de persona.
- Modificar persona.
- Eliminar persona.
- Identificar Persona.
- Verificar Persona.
- Calcular puntuaciones.
- Calcular tasas de error.
- Calcular tiempos.
- Mostrar grafico de distribuciones.
- Mostrar grafico de FAR vs FRR.
- Mostrar grafico curvas DET.
- Exportar datos.
- Configurar umbral.

Caso de Uso Agregar Persona

Diagrama de secuencia del suceso básico para dar de alta una persona en el sistema *Figura 3-9*.

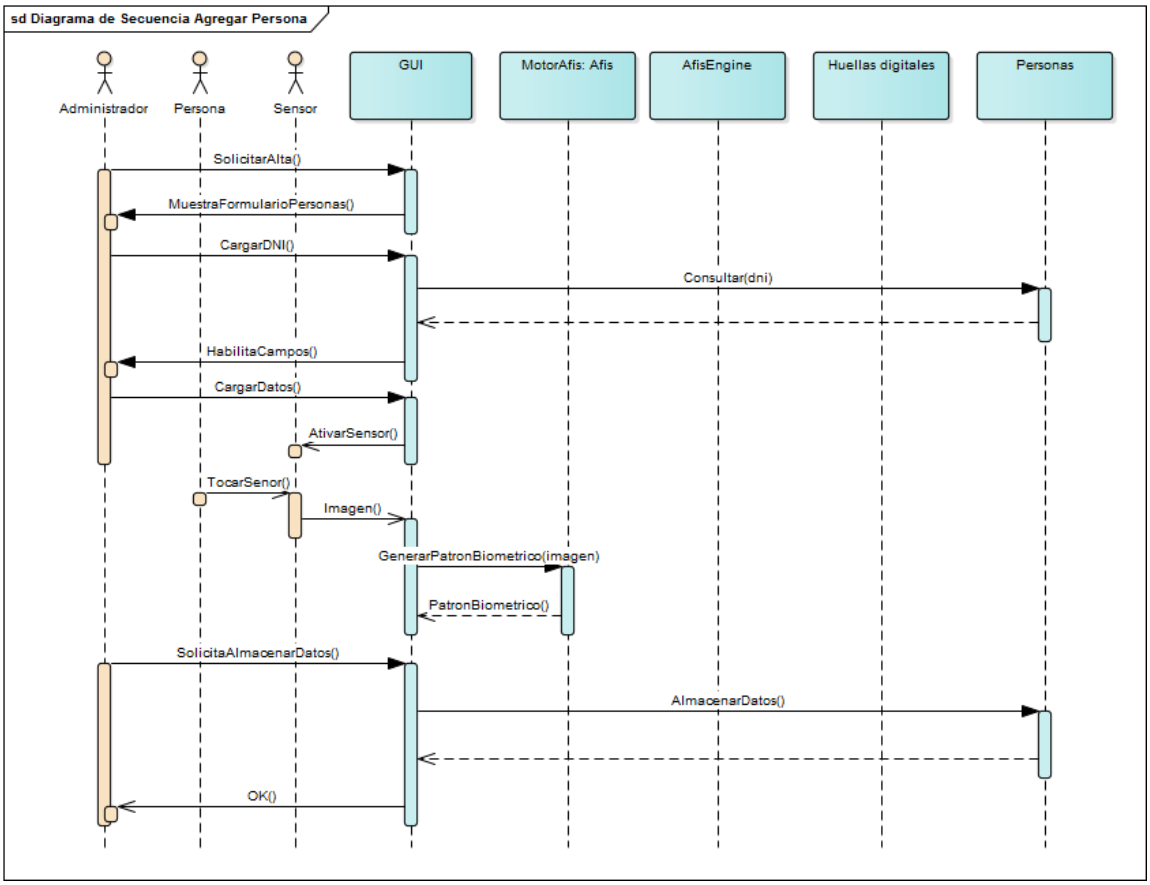


Figura 3-9. *Diagrama de Secuencia CU Agregar Persona*

Caso de Uso Modificar Persona

Diagrama de secuencia del suceso básico para modificar datos personales y biométrico de una persona *Figura 3-10*

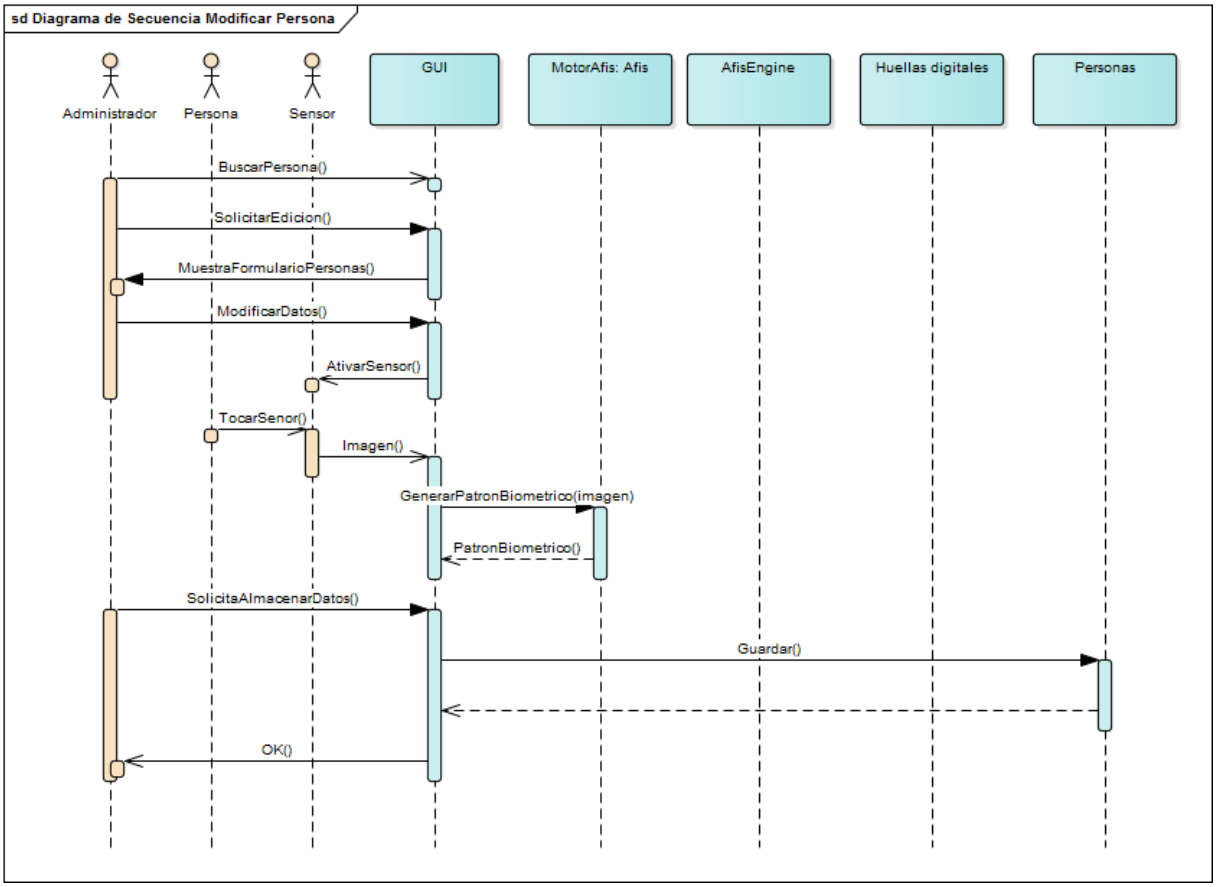


Figura 3-10. *Diagrama de Secuencia CU Modificar Persona*

Caso de Uso Eliminar Persona

Diagrama de secuencia del suceso básico para eliminar una persona en el sistema *Figura 3-11*

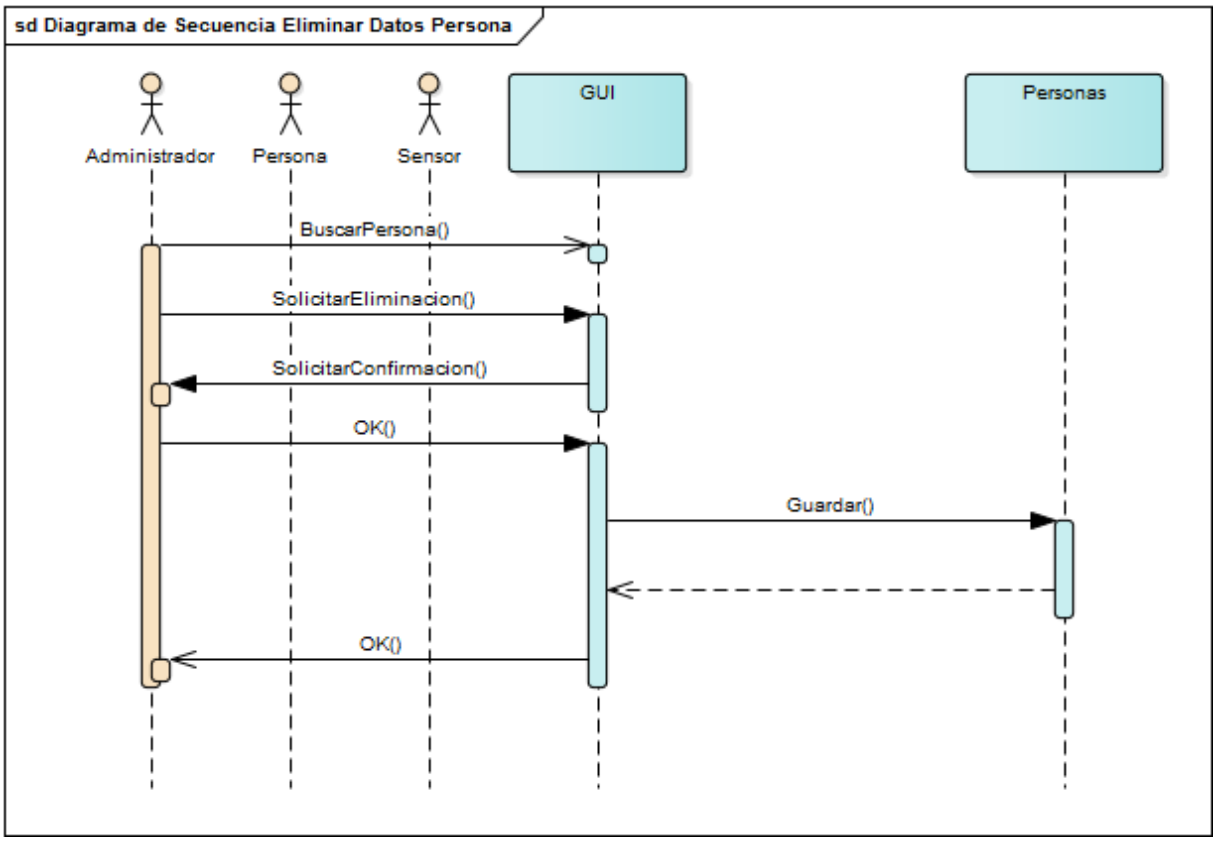


Figura 3-11. *Diagrama de Secuencia CU Eliminar Persona*

Caso de uso: Identificar Persona

Diagrama de secuencia del suceso básico identificar una persona *Figura 3-12*.

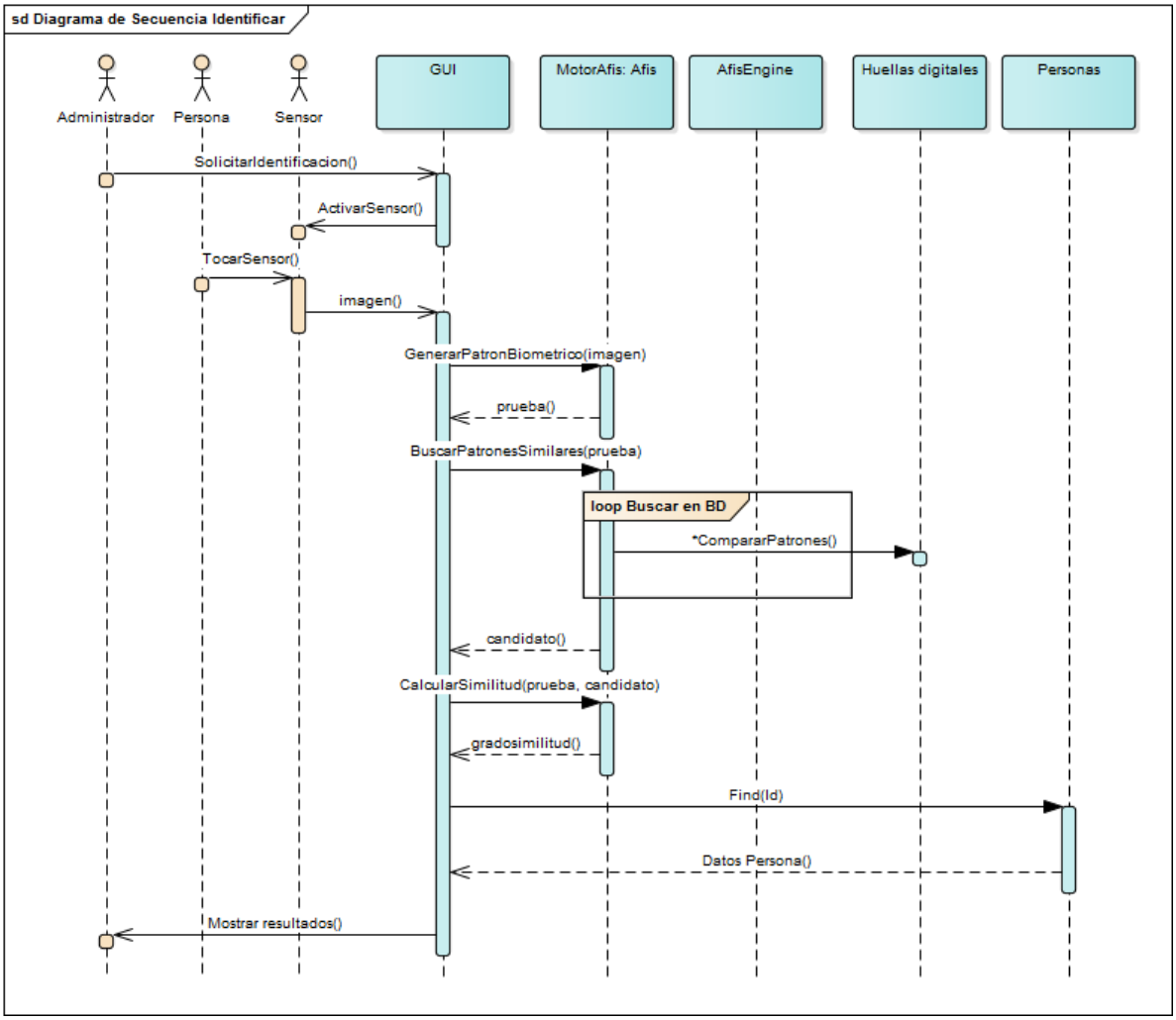


Figura 3-12. *Diagrama de Secuencia CU Identificar Persona*

Caso de uso: Verificar Persona

Diagrama de secuencia del suceso básico para verificar los datos de una persona *Figura 3-13*.

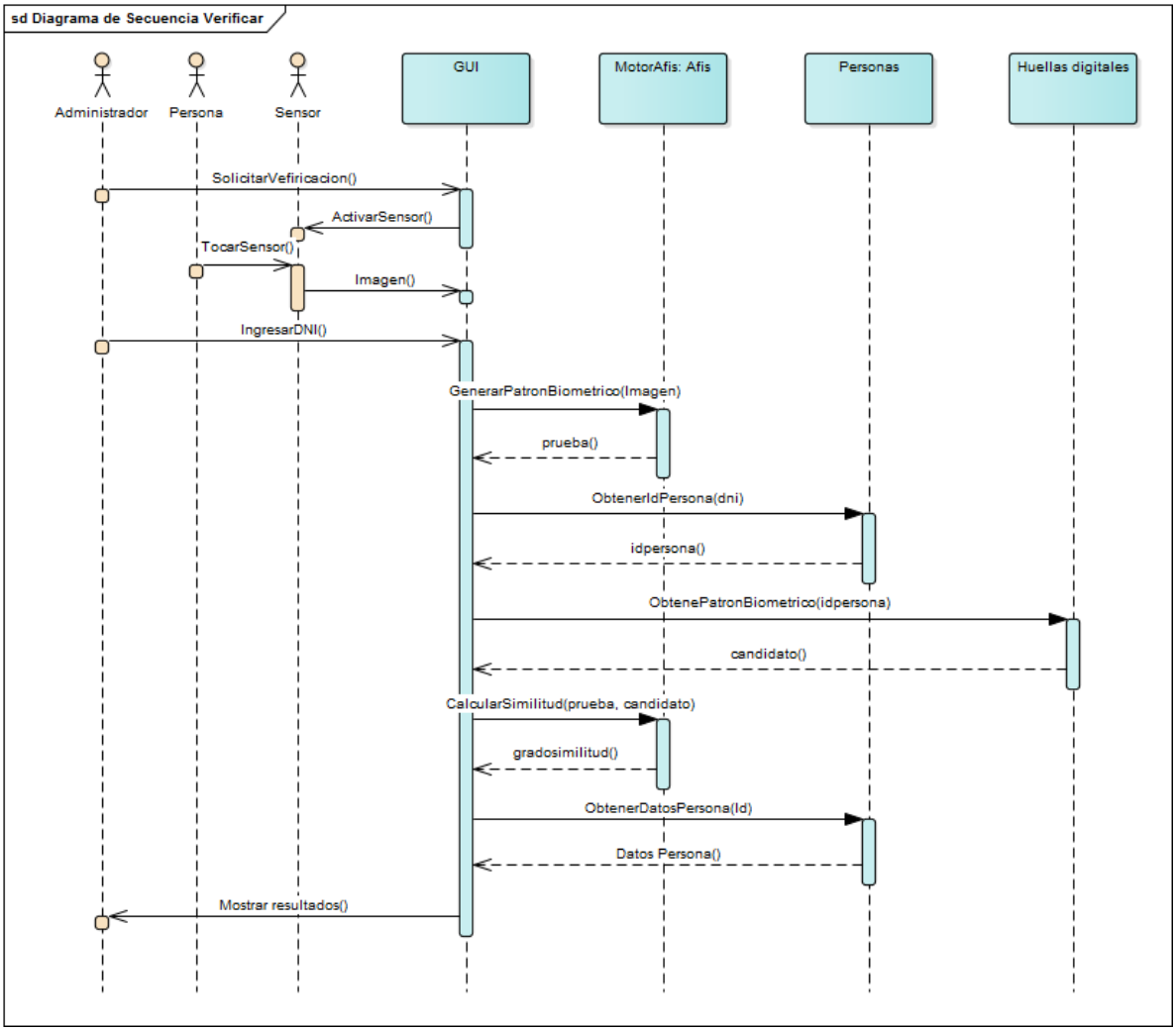


Figura 3-13. *Diagrama de Secuencia CU Verificar Persona*

Caso de uso: Calcular Puntuaciones

Diagrama de secuencia del suceso básico para calcular las puntuaciones de la imágenes de huellas digitales genuinas e impostoras *Figura 3-14*.

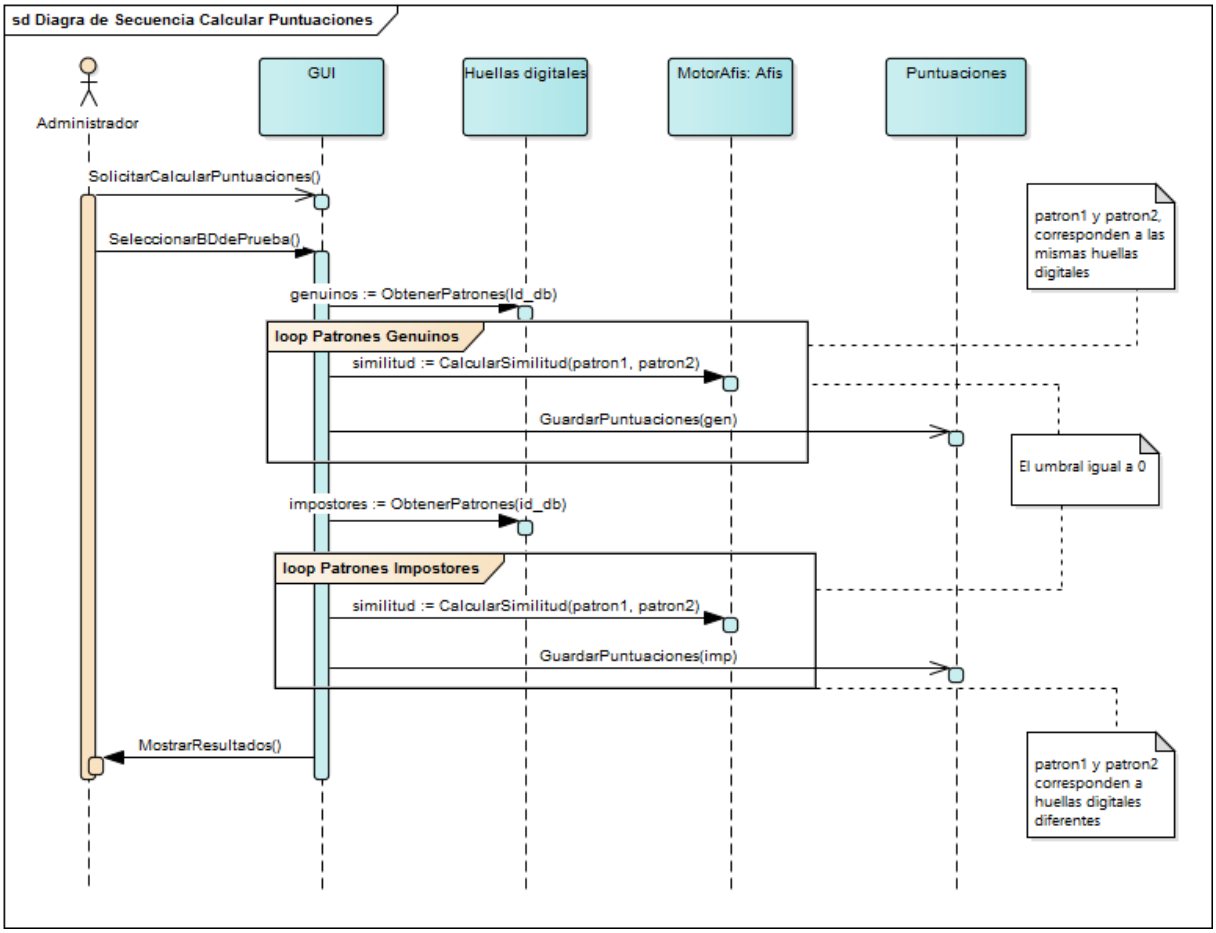


Figura 3-14. *Diagrama de Secuencia CU Calcular Puntuaciones*

Caso de uso: Calcular Tasa de Error

Diagrama de secuencia del suceso básico para calcular la tasas de igual error *Figura 3-15*.

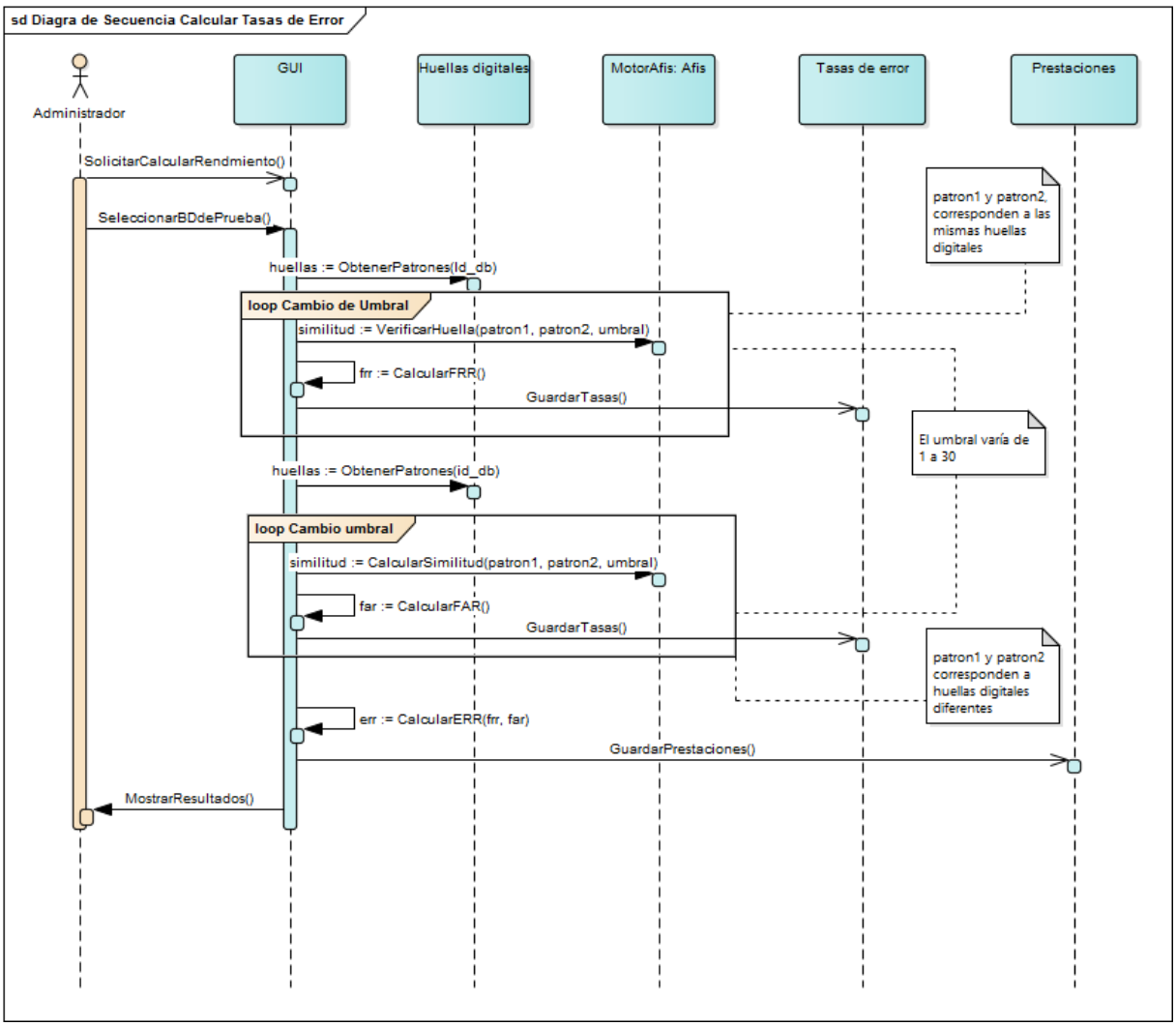


Figura 3-15. *Diagrama de Secuencia CU Calcular Tasa de Error*

Caso de uso: Calcular Tiempos

Diagrama de secuencia del suceso básico para calcular los tiempos de registro, comparación de patrones genuinos y patrones falsos de huellas digitales *Figura 3-16*.

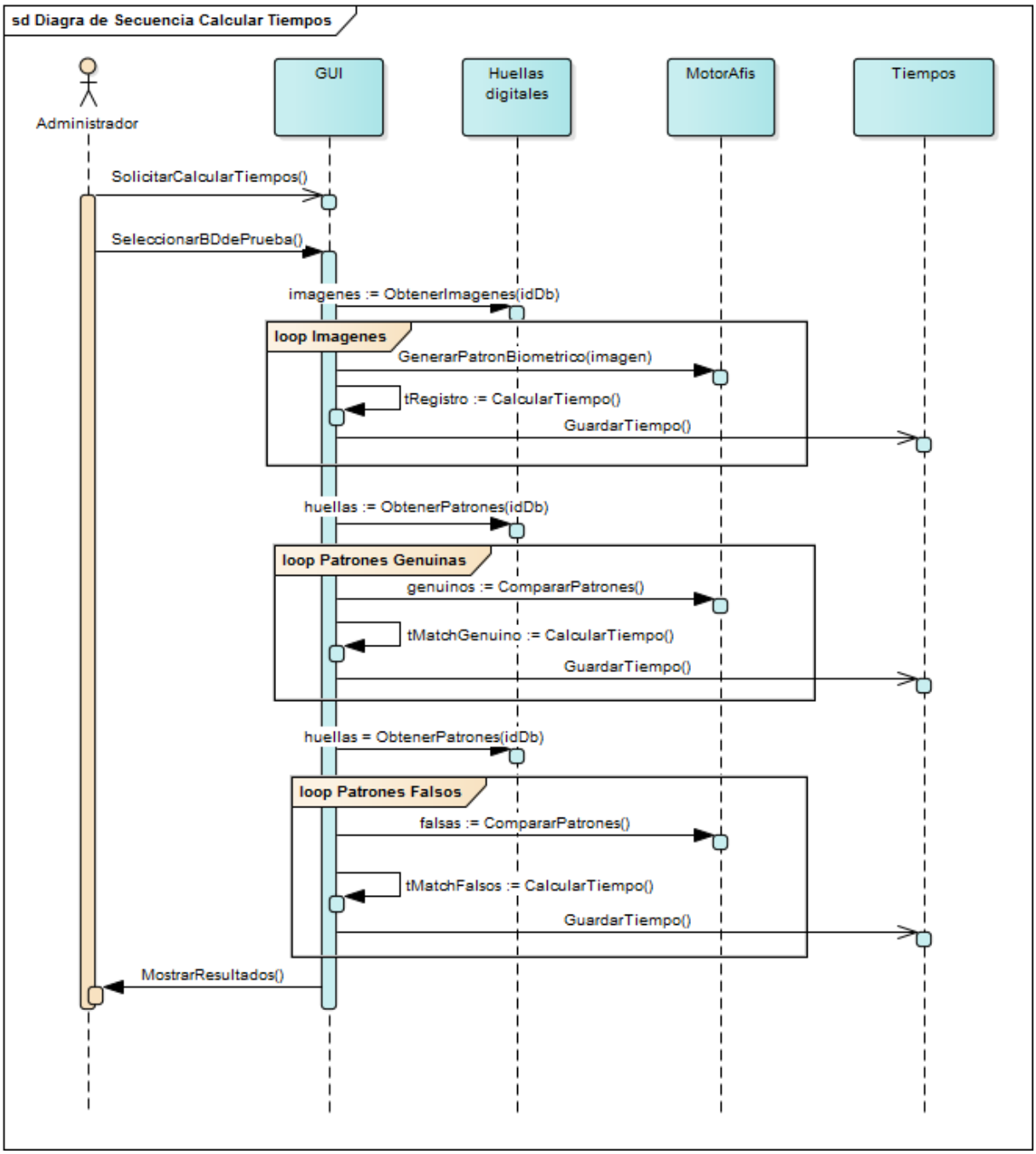


Figura 3-16. *Diagrama de Secuencia CU Calcular Tiempos*

Caso de uso: Mostrar Grafico de Distribución

Diagrama de secuencia del suceso básico para mostrar los gráficos con las curvas de distribuciones *Figura 3-17*.

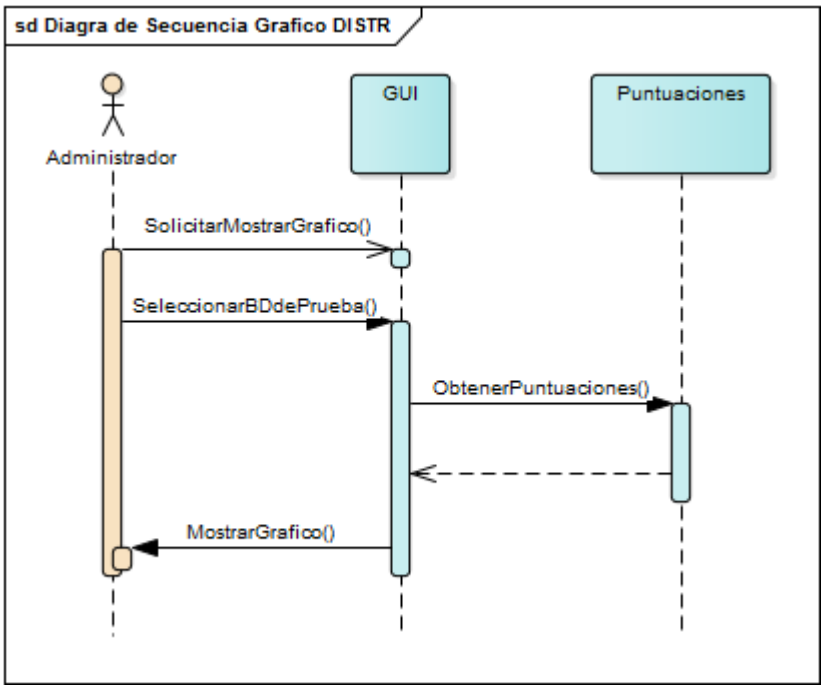


Figura 3-17. *Diagrama de Secuencia CU Mostrar Gráfico de distribución*

Caso de uso: Mostrar FAR vs FRR

Diagrama de secuencia del suceso básico para mostrar los gráficos con las curvas FAR vs FRR *Figura 3-18*.

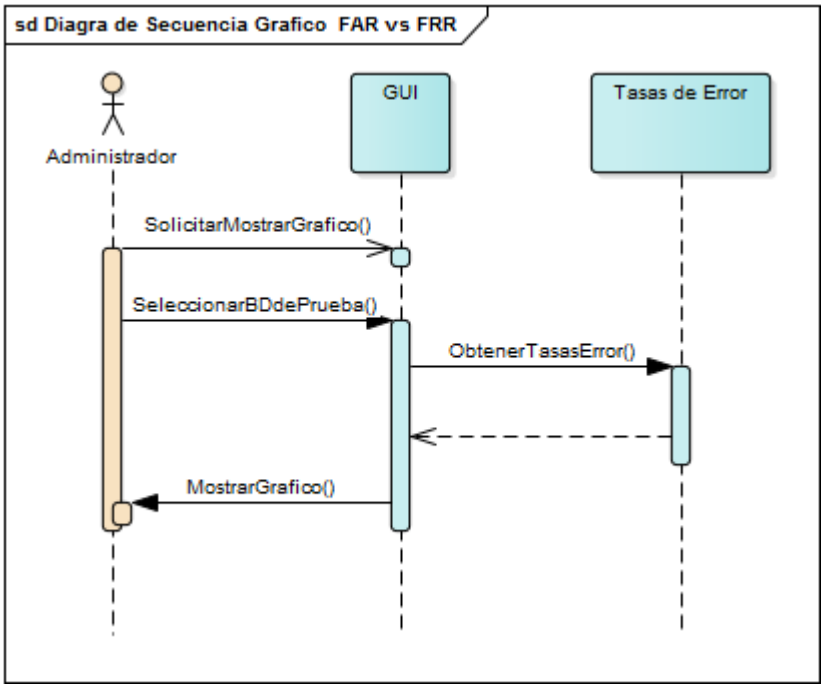


Figura 3-18. *Diagrama de Secuencia CU Mostrar Gráfico FAR vs FRR*

Caso de uso: Mostrar Grafico de *Detection Error Tradeoff* (DET)

Diagrama de secuencia del suceso básico para mostrar los gráficos con las curvas DET de todos las evaluaciones *Figura 3-19*.

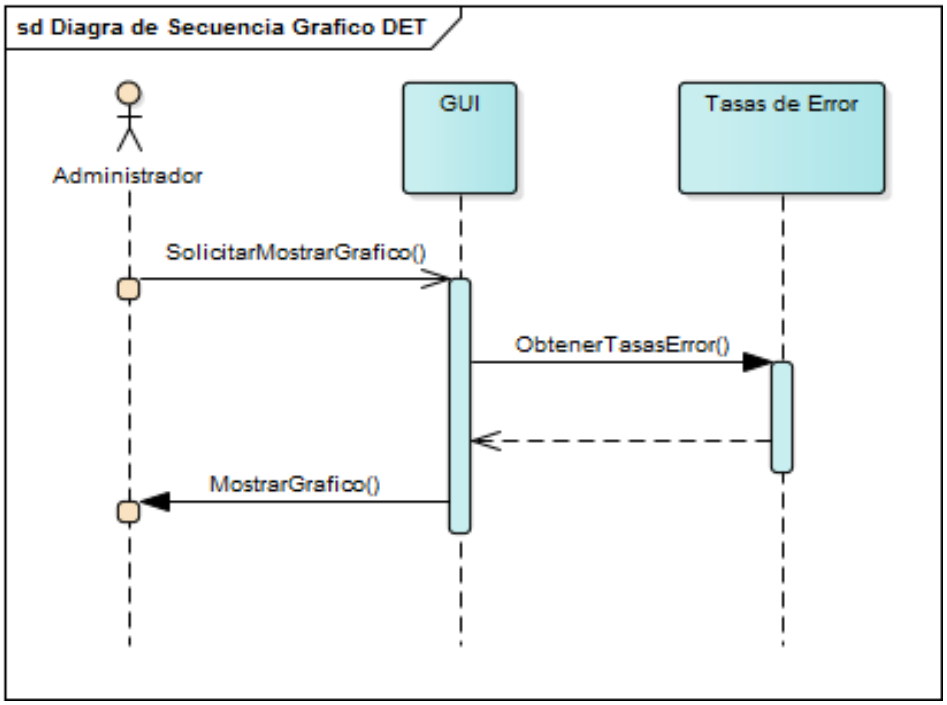


Figura 3-19. *Diagrama de Secuencia CU Mostrar Grafico DET*

Caso de uso: Exportar Datos

Diagrama de secuencia del suceso básico para exportar los de datos de las evaluaciones *Figura 3-20*

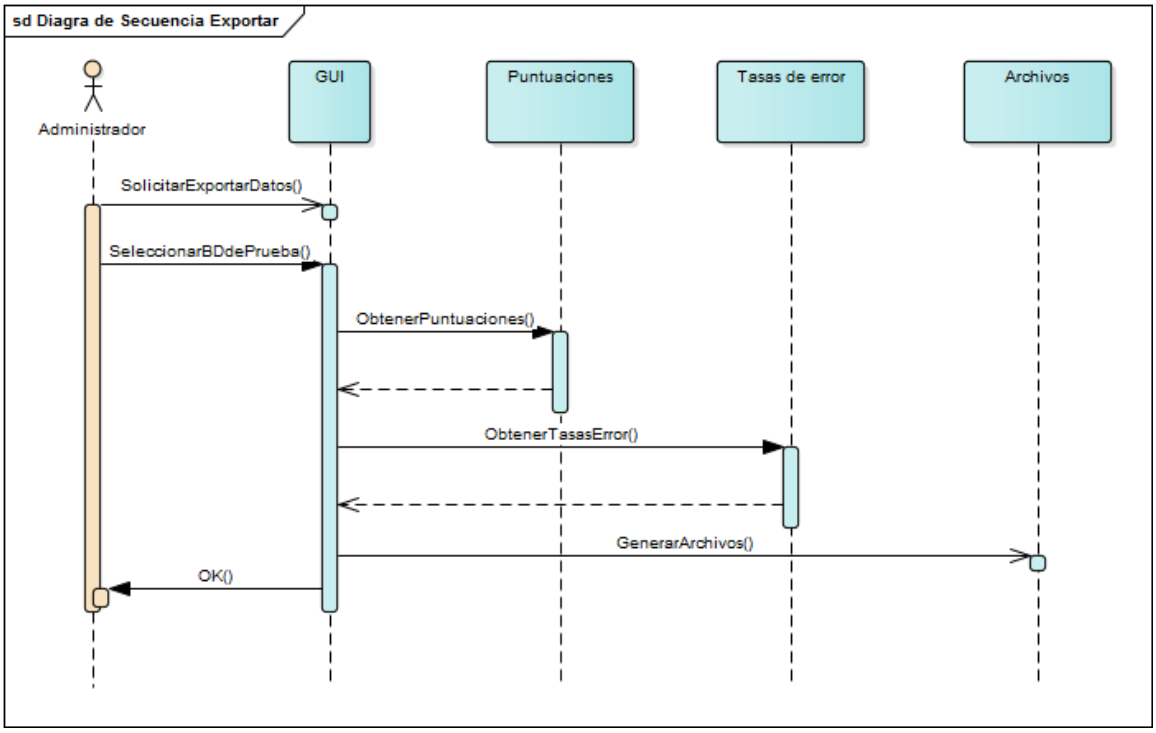


Figura 3-20. *Diagrama de Secuencia CU Exportar Datos*

Caso de uso: Configurar Umbral

Diagrama de secuencia del suceso básico para configurar el umbral del sistema *Figura 3-21*.

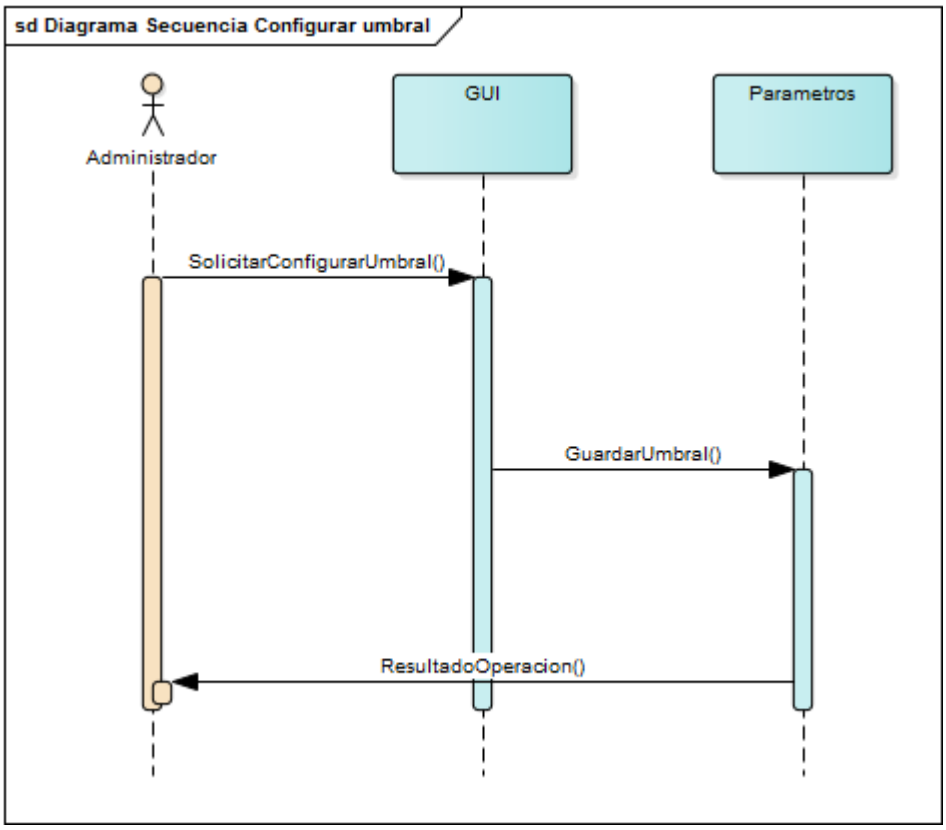


Figura 3-21. *Diagrama de Secuencia CU Configurar Umbral*

3.3.3.3 Patrones de diseño

Para el diseño de la herramienta se usaron dos patrones de diseño (Bishop, 2008):

- Patrón de diseño Singleton (instancia única) para las clases
- Modelo Vista Presentador (MVP) para el diseño de la aplicación.

Patrón de diseño Singleton (instancia única)

Se usó este patrón para todas las clases entidades que se persisten en la base de datos, ya que permite asegurar que de una clase habrá solo una instancia, y proporciona un punto de acceso a ella global a todo el código. El diagrama de clases es muy sencillo, ya que se compone de una única clase *Figura 3-22*

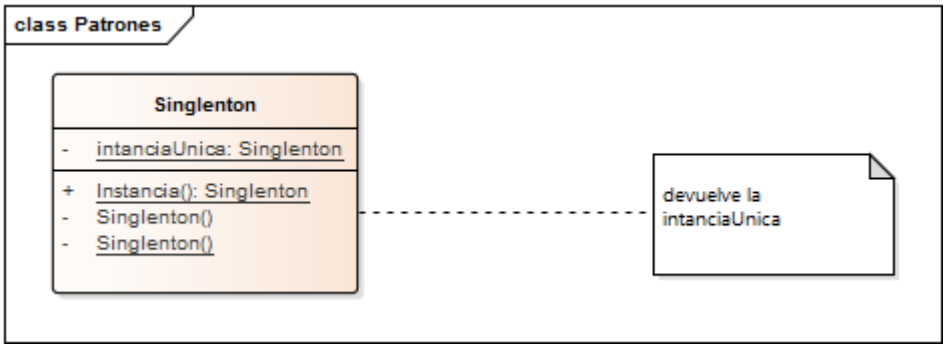


Figura 3-22. *Diagrama UML del patrón Singleton*

Patrón de diseño Modelo Vista Presentador (MVP)

Para la implementación de la aplicación de reconocimiento se utilizó el patrón de diseño MVP *Figura 3-23,* El presentador asume la funcionalidad de "intermediario" y toda la lógica es colocada en este módulo. Al separar la lógica de la interfaz de usuario, se puede cambiar el módulo de reconocimiento de manera sencilla.

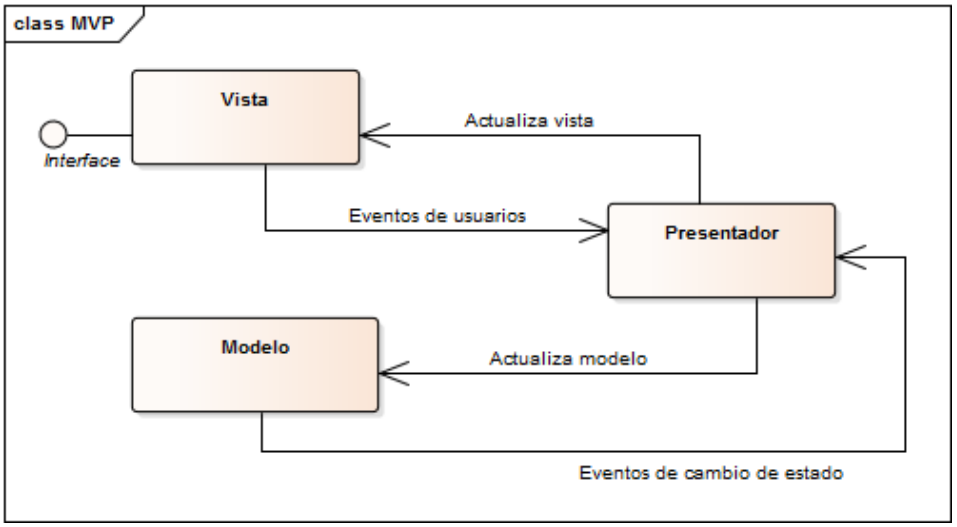


Figura 3-23. *Diagrama UML del patrón de diseño Modelo Vista Presentador*

3.3.3.4 Diseño de archivos de salidas

Se diseñaron las salidas que genera el aplicativo, que permitirá exportar los datos para la generación de las curvas de error y distribución.

Archivo de Curvas de Distribución

Permite generar, por cada base de datos, un archivo de texto con el formado de la *Figura 3-24* para la generación de las curvas de distribución.

CAMPO	NOMBRE	TIPO	LONG
1	Genuinas	Entero	
2	Impostoras	Entero	

Figura 3-24. *Formato de archivo para generación de Curvas de Distribución*

Archivo de Curvas FMR vs FNMR

Permite generar, por cada base de datos, un archivo de texto con el formado de la *Figura 3-25* para la generación de las curvas de FMR y FNMR. Los valores de FMR y FNMR están expresados en porcentajes, con dos pociones decimales.

CAMPO	NOMBRE	TIPO	LONG
1	Umbral	Numérico	5,2
2	FMR	Numérico	5,2
3	FNMR	Numérico	5,2

Figura 3-25. *Formato archivo de salida para generación de Curvas FMR vs FNMR*

Archivo de Curvas DET

Permite generar, por cada base de datos, un archivo de texto con el formado de la *Figura 3-26* para la generación de las curvas de FMR y FNMR. Los valores de FMR y FNMR están expresados en tasas con valores en el rango [0,1] con cuatro posiciones decimales.

CAMPO	NOMBRE	TIPO	LONG
1	FAR	Numérico	5,4
2	FNM	Numérico	5,4

Figura 3-26. *Formato de archivo de salida para generación de Curvas DET*

3.3.4 Implementación

Las actividades que se realizaron en este flujo de trabajo de proceso son:

- Definir la organización del código
- Implementar clases y objetos en forma de componentes (fuente, ejecutables, etc.)
- Generación de paquetes
- Generación de los prototipos de interfaces de usuarios
- Probar las componentes desarrolladas
- Integrar las componentes en un sistema ejecutable

Artefactos que se obtuvieron:

- Especificación de la tecnología usada
- Interfaces de usuarios
- Modelo de implementación compuesto por el diagrama de componentes.
- Prototipo Operacional

3.3.4.1 Tecnología utilizada

En la *Figura 3-27*, se muestra la tecnología y herramientas utilizadas para la implementación del aplicativo.

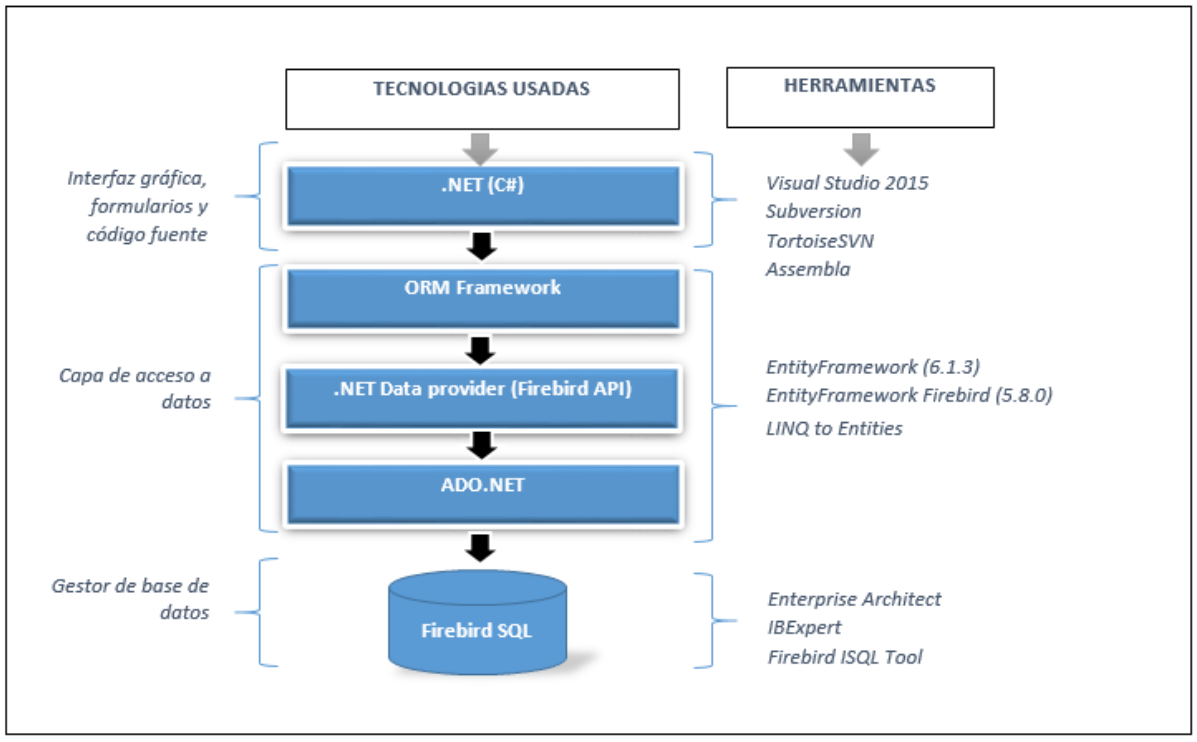


Figura 3-27. *Tecnologías y herramientas usadas para la implementación*

Para la implementación del código fuente se usó el lenguaje de programación *C#* y formularios de la Interfaz gráfica (*WinForms*) se utilizó ***Visual Studio 2015***. El control de versiones del código fuente se realizó con la herramienta ***Subversión***, se utilizó el cliente ***TortoiseSVN*** implementado como Windows Shell Extensión, y ***Assembla*** como hosting SVN.

En la capa de acceso a datos se trabajó con ***EntityFramework***, para la persistencia de las clases en la DB ***FirebirdSQL***, que maneja datos relacionales para no perder las ventajas de la orientación a objetos al interactuar con la DB, siguiendo el patrón de mapeo objeto relacional (ORM). Para realizar las consultas a la base de datos se utilizó ***LINQ to Entities*** que proporciona la capacidad de realizar consultas integradas en lenguajes (LINQ) que permite escribir consultas contra el modelo conceptual de ***EntityFramework*** mediante Visual C#.

Para la administración de bases de datos se usó la herramienta ***IBExpert*** para ***FirebirdSQL*** y la consola de Firebird ***ISQL Tool***. Para poder generar los Diagramas de Entidad Relación del sistema se empleó la herramienta ***Enterprise Architect*.**

3.3.4.2 Interfaces de usuario

Se presentan los prototipos de interfaces gráficas de usuario diseñadas para la aplicación, se presentan únicamente los prototipos de interfaces de usuario de las funciones más importantes.

Ventana principal

La ventana principal del aplicativo de reconocimiento está compuesta por un menú, donde se encuentran las funciones del aplicativo, y una barra de herramientas que tiene las mismas funciones del menú *Figura 3-28*.

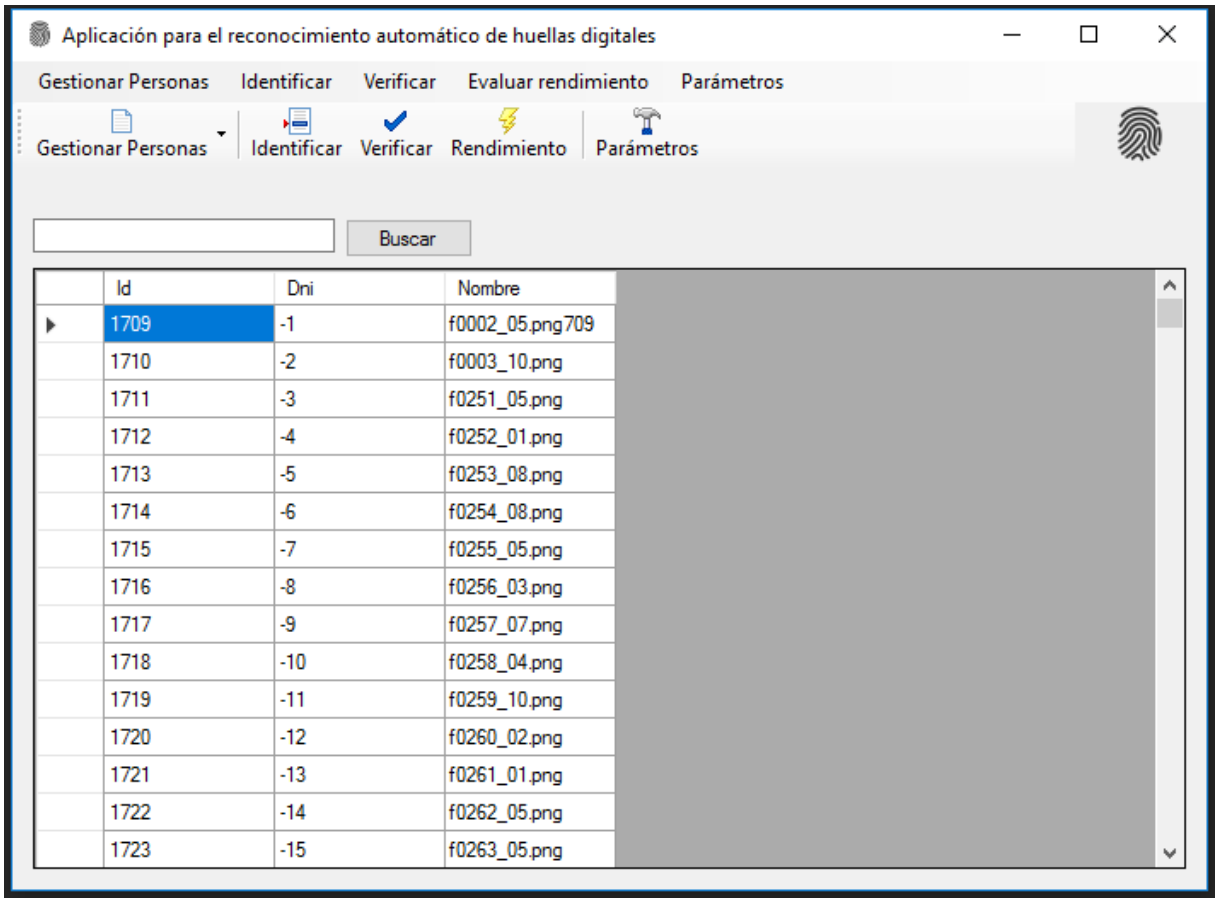


Figura 3-28. *Pantalla principal de la aplicación*

Gestión de datos personales y biométricos:

Permite el alta, baja y modificación de los datos personales *Figura 3-29*.

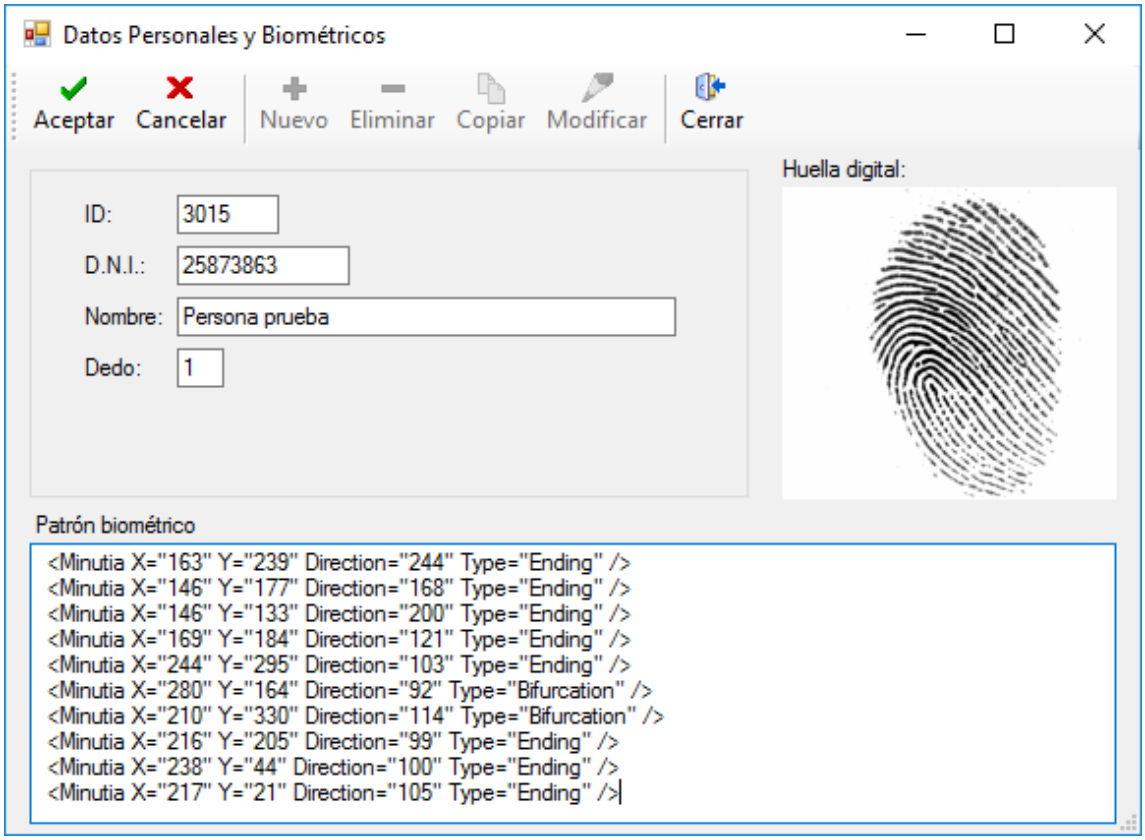


Figura 3-29. *Pantalla de gestión de datos personales y biométricos*

Identificación

Formulario para identificar una persona, comparando el patrón biométrico, de la imagen de huella digital, y los patrones biométricos almacenados *Figura 3-30.*

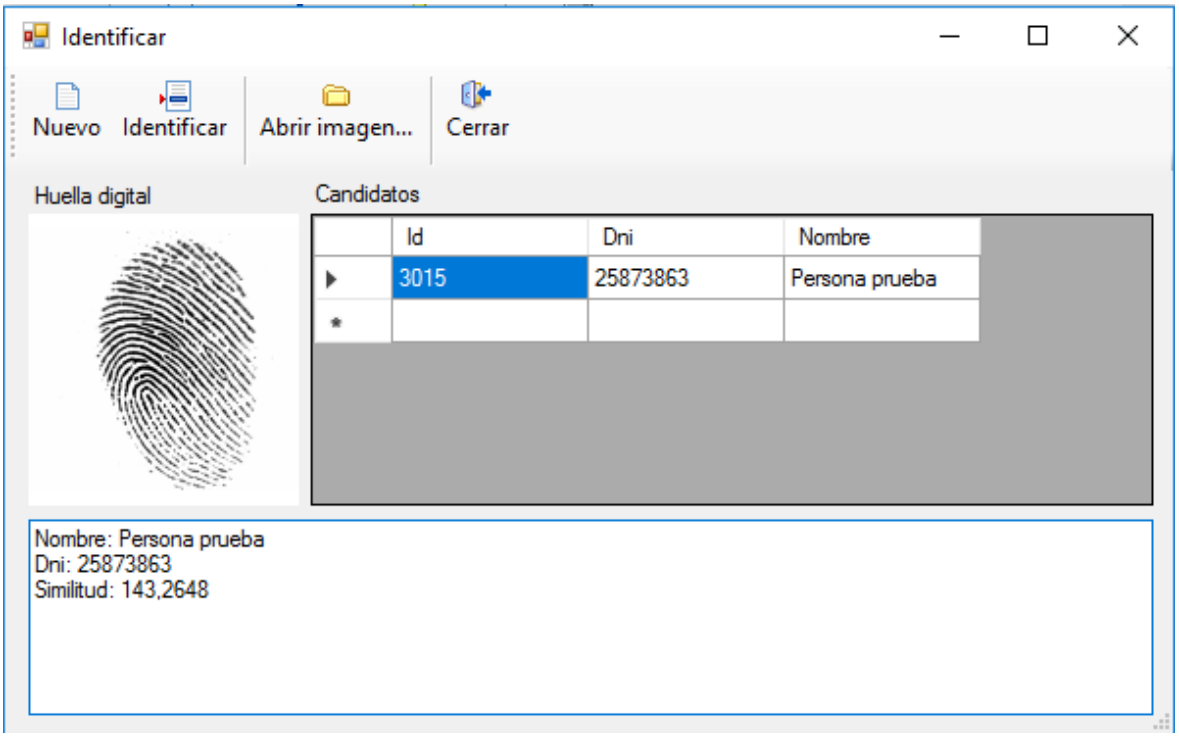


Figura 3-30. *Pantalla de identificación*

Verificación

Formulario para verificar la identidad de una persona, buscando el patrón almacenado correspondiente a la clave ingresada y comparándolo con el patrón biométrico, de la imagen de huella digital, aceptando o rechazando los datos ingresados *Figura 3-31*.

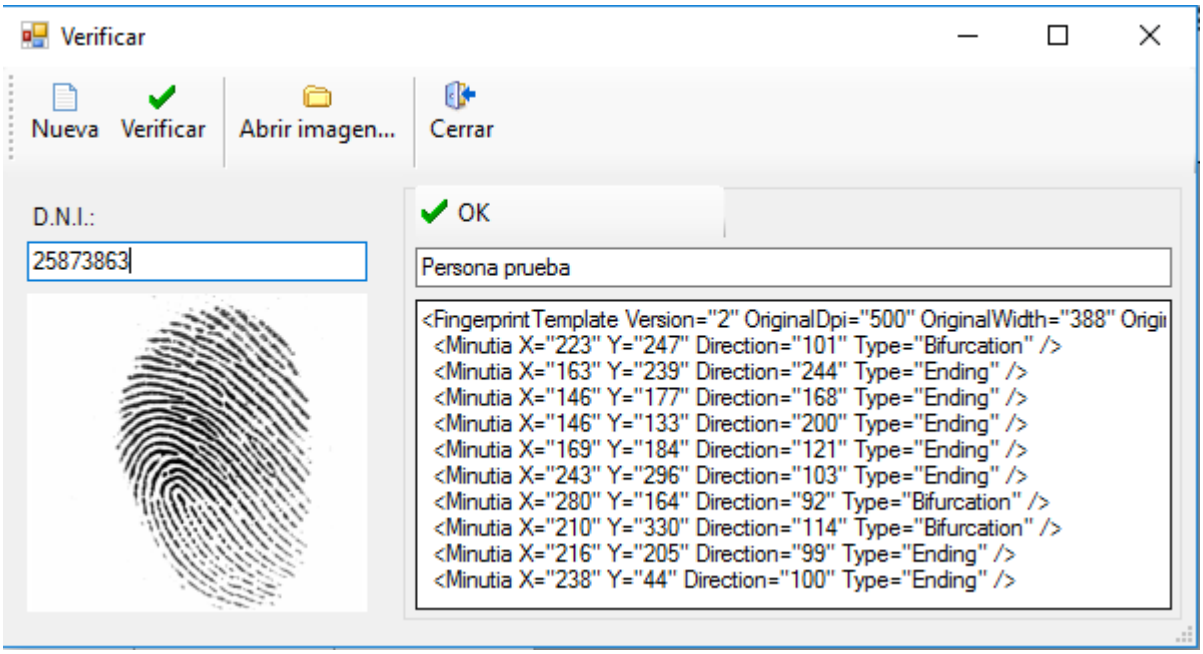


Figura 3-31. *Pantalla de verificación*

Evaluar Rendimiento.

Formulario para la ejecutar la evaluación de rendimiento, caculo de tasas y tiempos de ejecución *Figura 3-32*

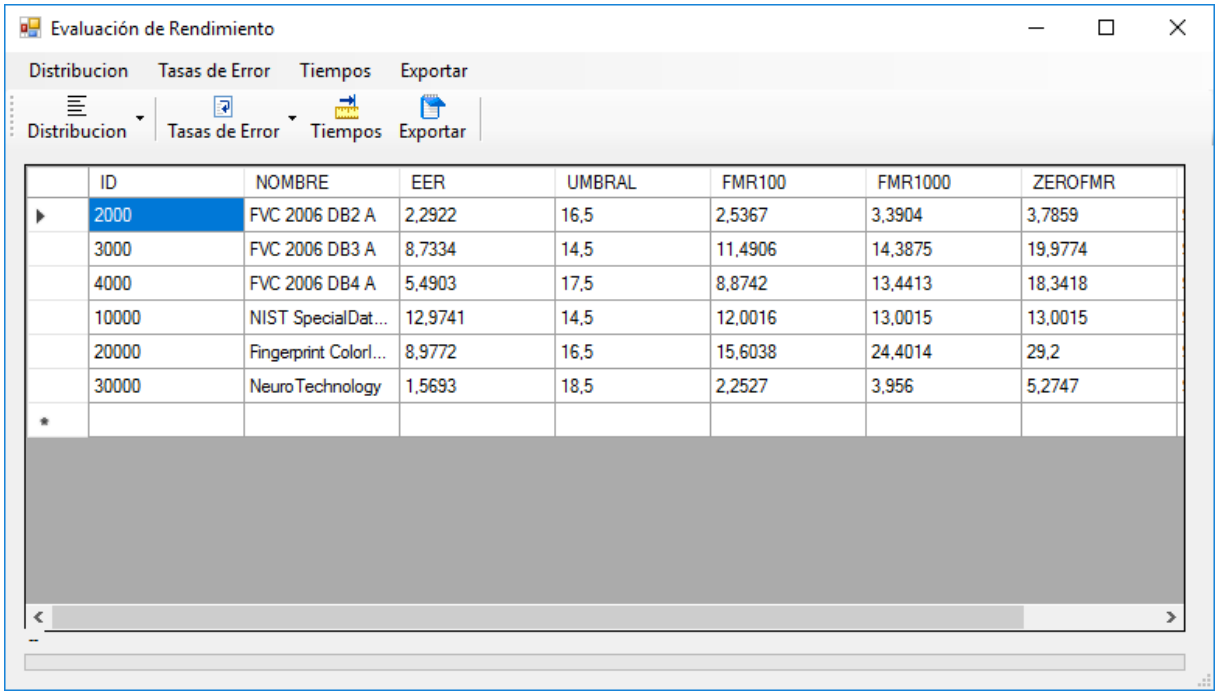


Figura 3-32. *Pantalla evaluar rendimiento*

Configurar umbral

Formulario que permite la modificación del umbral del sistema *Figura 3-33*

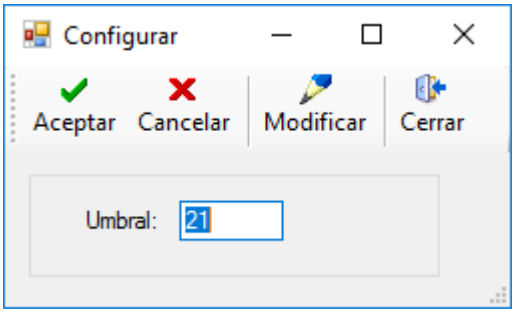


Figura 3-33. *Pantalla configurar*

3.3.4.3 Modelo de implementación

Durante el flujo de trabajo de implementación se desarrolló todo lo necesario para obtener un sistema ejecutable: componentes ejecutables, componentes de ficheros (código fuente, scripts etc.), componentes de tabla (elementos de la base de datos) etc. partiendo del modelo de diseño se implementan los componentes correspondientes *Figura 3-34*.

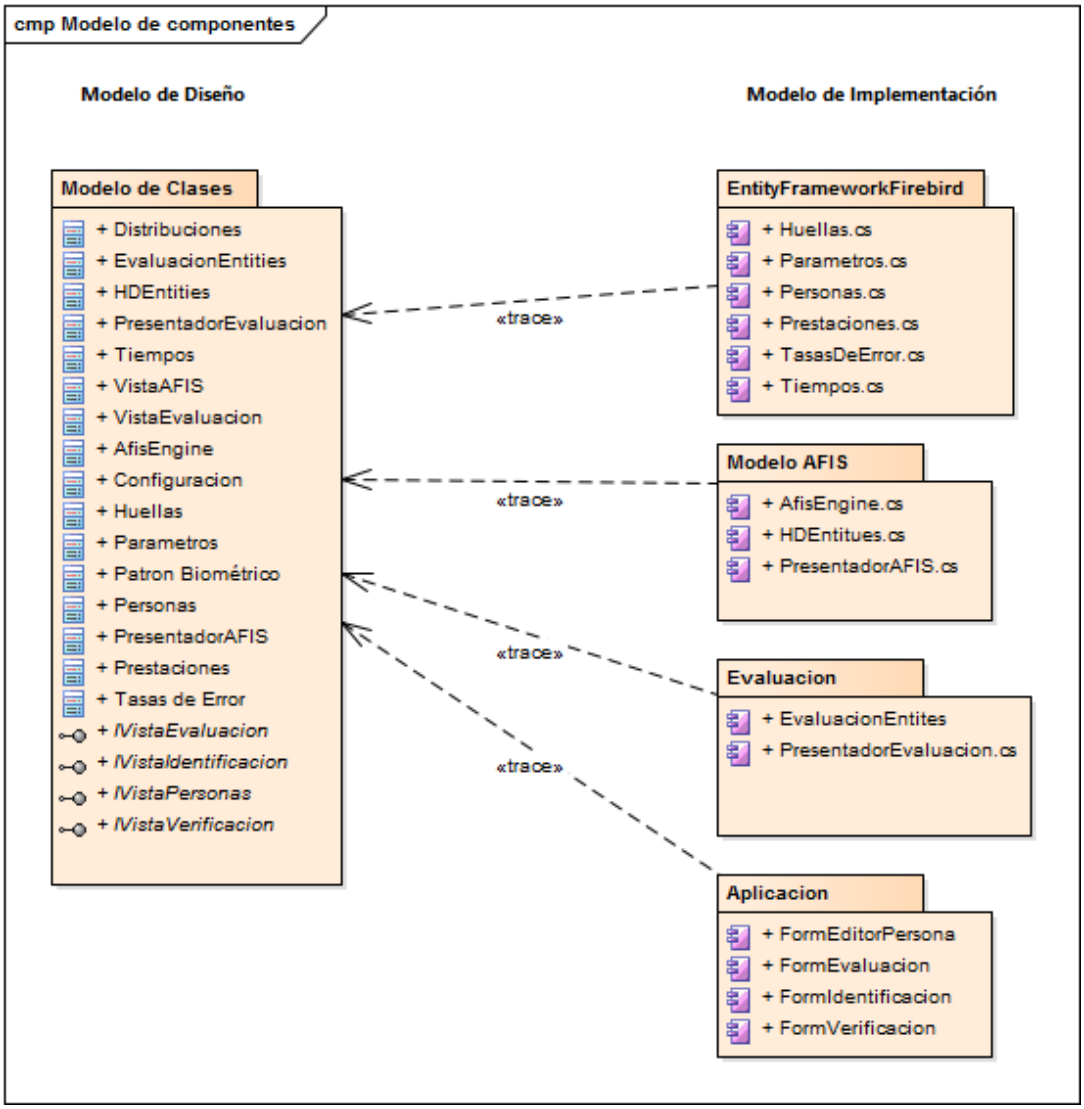


Figura 3-34. *Modelo de componentes implementación*

3.3.5 Pruebas

Las actividades que se realizaron en este flujo de trabajo de proceso son:

- Probar las componentes desarrolladas.
- Generación de la base de datos de prueba.

Artefacto que se produjo:

- Base de datos de prueba.

En paralelo a la implementación de los componentes se realizó la revisión de los mismos mediante las *pruebas*, siendo está una de las maneras en que se llevan a cabo los mecanismos de control de calidad.

Para el trabajo se utilizaron:

- Pruebas unitarias: se realizaron estas pruebas a cada módulo construido para la aplicación.
- Pruebas funcionales: se realizaron este tipo de pruebas para verificar el flujo de interacción de la funcionalidad definida.
- Se generó la base de datos de prueba con las huellas usadas.

3.3.6 Despliegue

Las actividades que se realizaron en este flujo de trabajo de proceso son:

- Se generó el diagrama de despliegue
- Producir un “reléase” o versión.
- Empaquetar el software.

Artefactos Producidos:

- Versión ejecutable de la aplicación.

En la *Figura 3-35* se muestra el diagrama de despliegue de la herramienta.

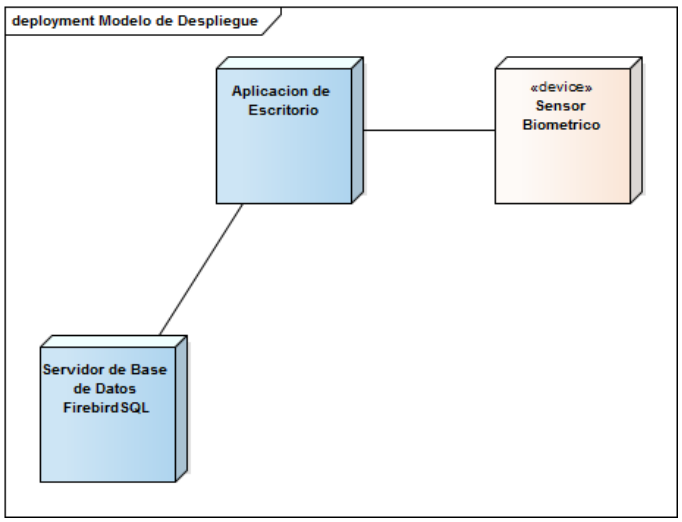


Figura 3-35. *Diagrama de despliegue del Aplicativo*

CAPÍTULO IV

EVALUACION DE RENDIMIENTO

4.1 Introducción

En este capítulo se presentan las pruebas realizadas a la aplicación desarrollada y los resultados obtenidos, tanto en términos de tasas de error y tiempo de ejecución.

El módulo de reconocimiento fue sometido a una serie de pruebas utilizando distintas base de datos. El principal objetivo de estas pruebas fue la identificación del umbral en el cual el funcionamiento del sistema presenta las menores tasas de error, además determinar las tasas de error y tiempos de cálculo. Las evaluaciones se basaron en el estándar ISO/IEC 19795 (ISO JTC1/SC37, 2006) que proporciona un marco de evaluación de sistemas biométricos, además se utilizaron otros indicadores (Ferrara, Franco, & Maltoni, 2007) para reflejar el comportamiento del aplicativo, que no encuentran en el estándar.

4.2 Procedimiento para la evaluación

La evaluación se realizó siguiendo el estándar ISO/IEC 19795 (ISO JTC1/SC37, 2006) y el protocolo de pruebas utilizado en la competencia de algoritmos de reconocimiento de huellas digitales *Fingerprint Verification Competition* (Ferrara, Franco, & Maltoni, 2007), Para lo cual se llevaron a cabo las siguientes actividades:

- **Importar archivos de imágenes:** cada una de las imágenes de bases de datos de imágenes utilizadas para la evaluación, se cargaron al motor base de datos del sistema, utilizando la estructura de tablas de la *Figura 4-1.*

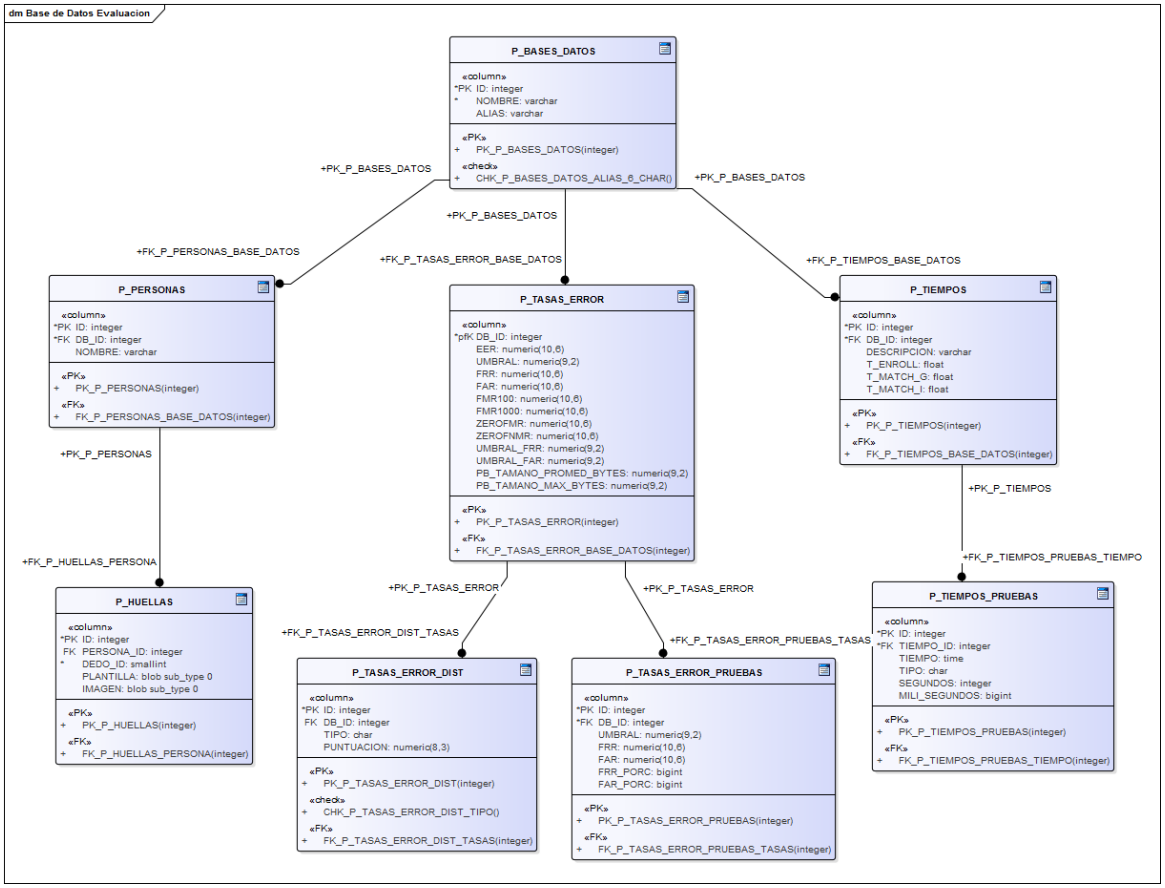


Figura 4-1. *Estructura de tablas para Evaluaciones*

- **Calcular puntuaciones de similitud de intento genuino:** el patrón biométrico de cada imagen es comparado con los restantes patrones del mismo dedo.
- **Calcular puntuaciones de similitud de intento impostor sin esfuerzo:** el patrón biométrico de la primera imagen de cada dedo es comparado con el primer patrón biométrico de los demás dedos.
- **Generar Distribución de huellas genuinas e impostoras**.
- **Calcular Tasa de Falsa Concordancia (FMR) y Tasa de Falsa No Concordancia (FNMR)**.
- **Calcular Tasa de Igual Error (EER).**
- **Determinar indicadores FMR100, FMR1000, ZeroFMR y ZeroFNMR.**
- **Determinar tiempo medio de registro y comparación.**

4.3 Base de datos utilizadas para la evaluación

Uno de los principales inconvenientes a la hora de evaluar el rendimiento de un aplicativo de reconocimiento de huellas digitales es que es prácticamente inviable contar con la cantidad de individuos que permitan capturar sus huellas digitales, además que las capturas se tienen que realizar varias veces y utilizar diferentes sensores a fin de obtener una buena representatividad. Pero se dispone de base de datos públicos de grandes volúmenes de

datos que representen de manera confiable las características biométricas de las huellas de los individuos. Ya que a mayor cantidad de huellas disponibles y a mayor cantidad de muestras de cada huella, se puede representar de manera confiable la población de individuos.

Por lo antes expuesto es que se consideraron bases de datos públicas de libre acceso, en la Tabla 4-1 se presenta un resumen de las características de las bases de datos utilizadas para las pruebas, y en los apartados siguientes se describen con mayor detalle las bases de datos utilizadas.

Base de Datos	Tipo de sensor	Individuos	Capturas por individuos	Tamaño de la imagen	Resolución
FVC 2006 DB1 A	Sensor de campo	140	12	96x96	250 dpi
FVC 2006 DB2 A	Sensor optico	140	12	400x560	569 dpi
FVC 2006 DB3 A	Sensor térmico	140	12	400x500	500 dpi
FVC 2006 DB4 A	SFinGe v3.0	140	12	288x384	500 dpi
NIST Special Database 4	Tintadas	2000	2	512x512	400 dpi
Fingerprint Color Image Database .v1	Digital Persona U.are.U 4500	50	5	200x200	400 dpi
Neurotech Sample Fingerprint Database	Digital Persona U.are.U 4000	65	8	326x357	500 dpi

Tabla 4-1. *Resumen de las características de las base de datos*

4.3.1 Base de datos FVC 2006

Provee cuatro base de datos (DB1 A, DB2 A, DB33, DB4 A), las cuales están disponibles para proyectos de investigación y pueden ser descargadas, previo un acuerdo de licencia, del sitio web de *Biometric Recognition Group – ATVS* http://atvs.ii.uam.es/atvs/fvc2006.html. Estas bases de datos son las utilizadas en la competencia FVC 2006 (Ferrara, Franco, & Maltoni, 2007). Cada base de datos cuenta con 140 huellas, con 12 muestras por huella (formato bmp) *Figura 4-2* (1680 imágenes en total).

4.3.2 Base de datos NIST Special Database 4

Figura 4-2. *Imágenes de cada una de las base de datos FVC 2006*

Esta base de datos puede ser descargada libremente del sitio web de NIST https://www.nist.gov/srd/nist-special-database-4. Cuenta con 2000 pares de imágenes de huellas digitales (formato png), corresponden con huellas tintadas capturadas manualmente (*off-line*) *Figura 4-3,* en escala de grises de 8 bit. Cada imagen tiene 512x512 pixeles con 32 líneas de espacio blanco en el pie de cada imagen, clasificadas de la siguiente forma:

- A=Arco
- L=Bucle izquierdo
- R=Bucle derecho
- T=Arco tendido
- W=Espiral

La base de datos es distribuida uniformemente en cada una de las clasificaciones, con 400 pares imágenes de cada clase.

Figura 4-3. *Dos capturas ("f0001_01.png" y "s0001_01.png") de la misma huella digital de la base de datos NIST*

4.3.3 Base de datos Fingerprint Color Image Database .v1

Esta base de datos puede ser descargada libremente del sitio web de MATHWORKS https://www.mathworks.com/matlabcentral/fileexchange/52507-fingerprint-color-image-database-v1. La base de datos contiene 250 imágenes a color de huellas digitales (formato jpg) *Figura 4-4*, de 200x200 pixeles. Todas las imágenes corresponden a la colección de 50 individuos utilizando el sensor Digital Persona U.are.U 4500. Por cada individuo se cuenta con 5 capturas diferentes de cada dedo.

Figura 4-4. *Ejemplo de dos capturas ("11.jpg" y "12.jpg") de la misma huella digital de la base de datos Fingerprint Color Image*

4.3.4 Base de datos NeuroTechnologic Fingerprint Database

Esta base de datos puede ser descargada libremente del sitio web de NEUROTECHNOLOGIC http://www.neurotechnology.com/download.html. La base de datos contiene 520 imágenes de huellas digitales (formato tif) *Figura 4-5*, de 326x357 pixeles. Todas las imágenes corresponden a la colección de 65 individuos utilizando el sensor Digital Persona U.are.U 4000. Por cada individuo se cuenta con 8 capturas diferentes de cada dedo.

Figura 4-5. *Ejemplo de dos capturas ("012_1_1.tif" y "012_1_2.tif") de la misma huella digital de la base de datos NeuroTechnologic Fingerprint Database*

4.4 Evaluaciones realizadas

Las evaluaciones realizadas consistieron en cálculos de:

- Distribuciones genuinas e impostoras
- Las tasas de error
- Tiempos de ejecución

4.4.1 Distribuciones genuinas e impostoras

Para el cálculo de la distribución genuina, se calcularon las puntuaciones de similitud, para todos los pares de patrones biométricos de un mismo dedo (intento genuino), Ecuación (2.13) Capitulo II apartado 2.5.1.2, y para la distribución impostora, se calcularon los puntajes de los pares de patrones biométricos de diferentes dedos, Ecuación (2.15) Capitulo II apartado 2.5.1.2, en la *Tabla 4-2* se muestran la cantidad de comparaciones realizadas. En base a los puntajes obtenidos se obtiene la distribución normal tanto para las huellas genuinas como impostoras dando como resultado los gráficos de la *Figura 4-6 a Figura 4-11,* para cada una de las base de datos. Donde se observa que en todas las base de datos las puntajes impostores se agrupan en torno a un valor central de umbral entre 15 y 17, mientras que para las distribuciones genuinas el valor central de umbral varía en cada base de datos. Por ejemplo, para la base de datos *FVC2006 DB3 A* Figura 4-7, se tiene un valor central de 119 y para la base de datos *Fingerprint Color Imagen Figura 4-10* el valor central es de 55.

Base de Datos	Comparaciones Genuinas	Comparaciones Impostoras
FVC 2006 DB2 A	9.240	9.730
FVC 2006 DB3 A	9.240	9.730
FVC 2006 DB4 A	9.240	9.730
NIST SpecialDatabase 4 Gray Scale	100	4.950
Fingerprint Color Image Database	500	1.225
NeuroTechnologic	1.820	2.080

Tabla 4-2. *Cantidad de comparaciones genuinas e impostoras de cada una de las base de dato de prueba*

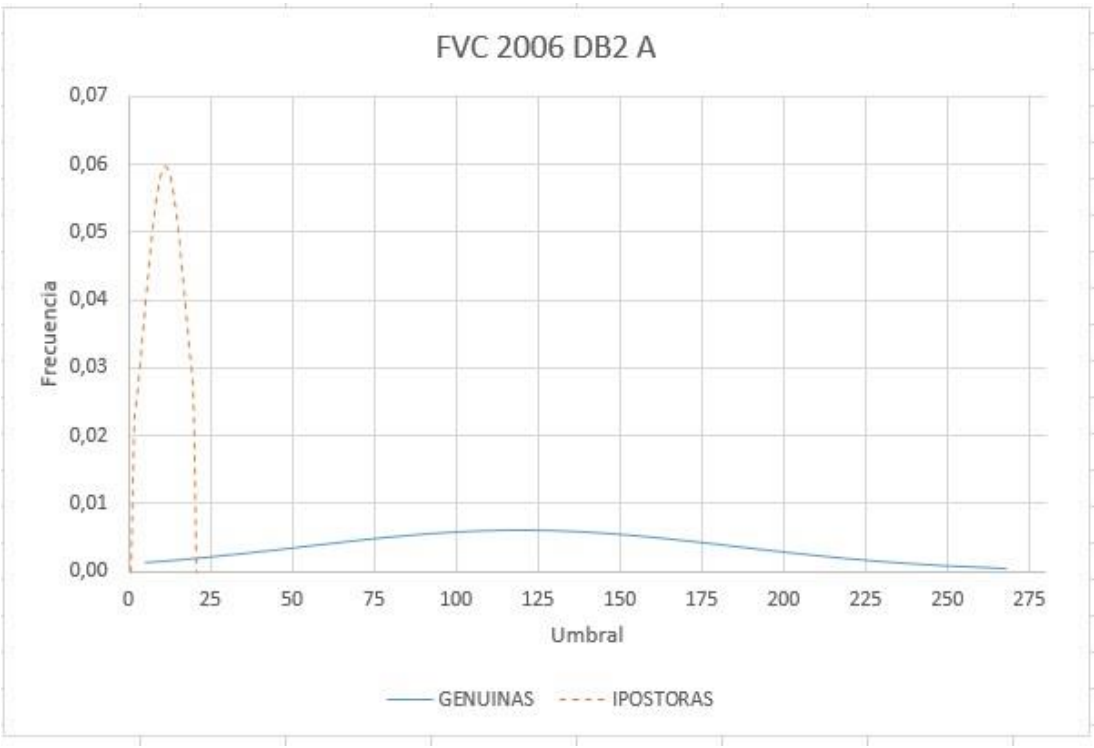


Figura 4-6. *Curvas de Distribuciones BD FVC 2006 DB2 A*

.

.

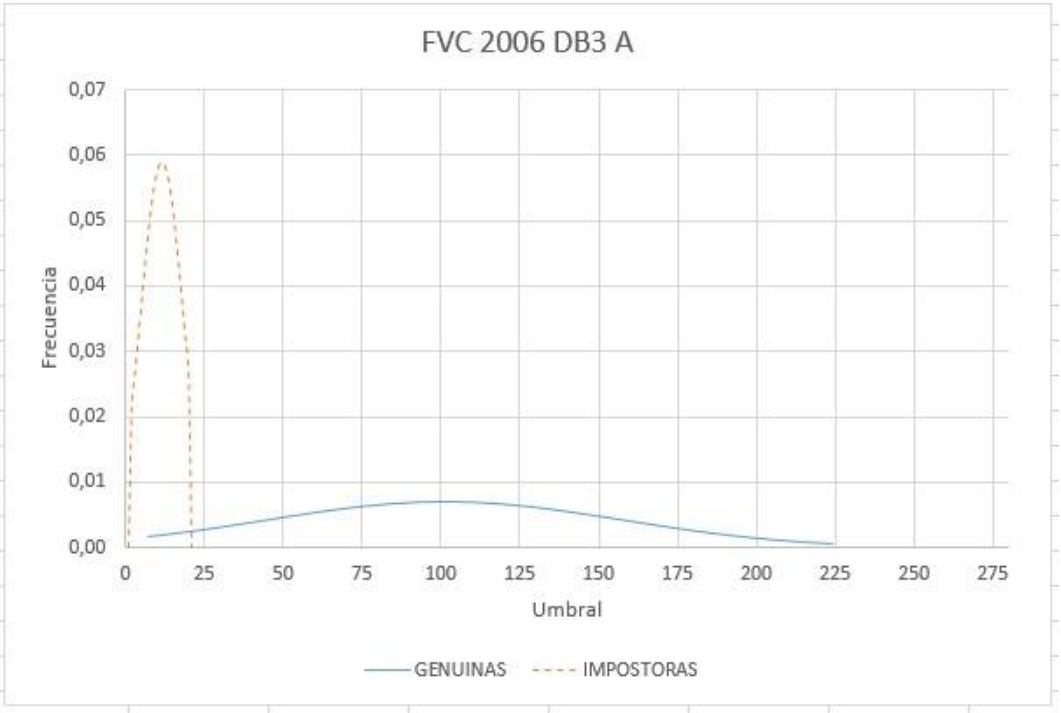


Figura 4-7. *Curvas de Distribuciones BD FVC 2006 DB3 A*

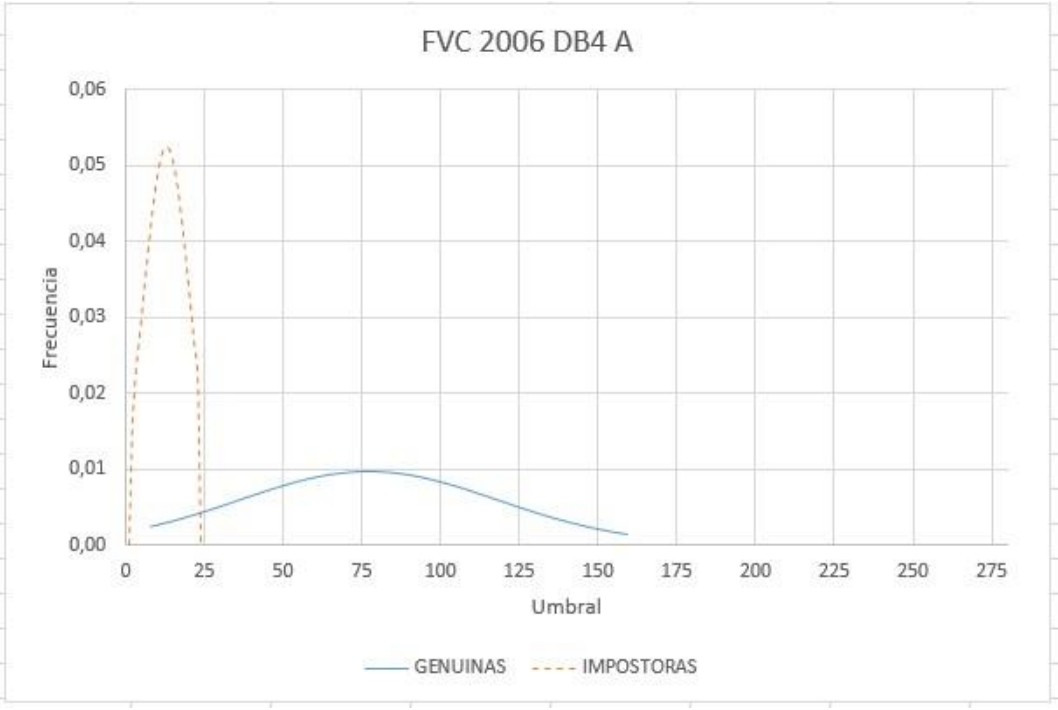


Figura 4-8. *Curvas de Distribuciones BD FVC 2006 DB4 A*

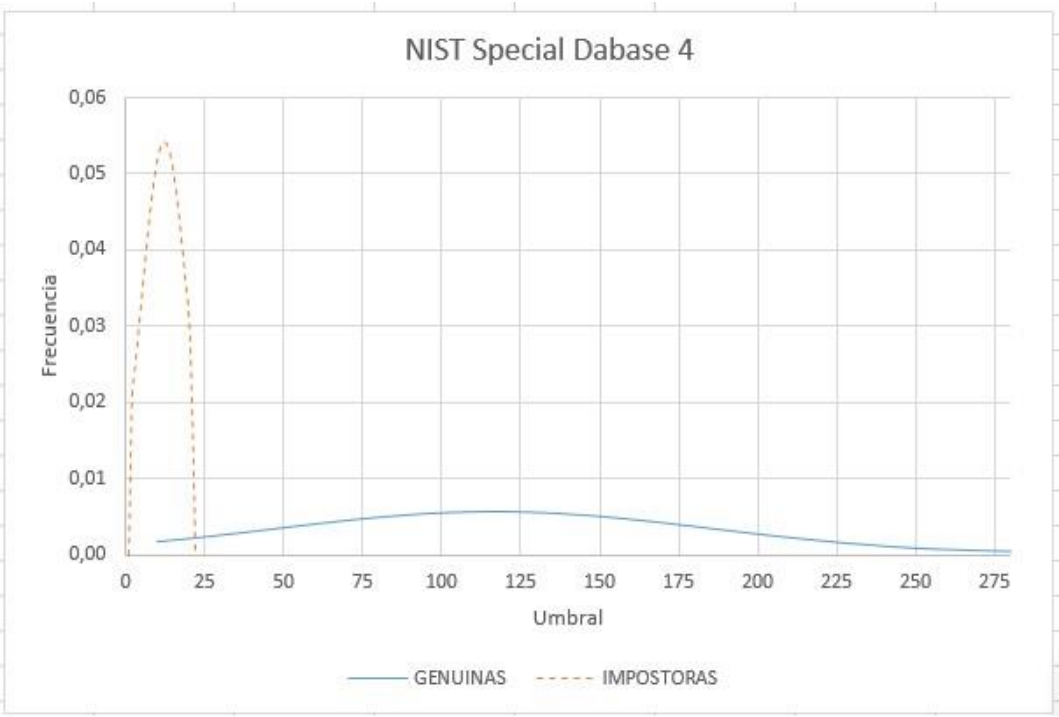


Figura 4-9. *Curvas de Distribuciones NIST Special Database 4*

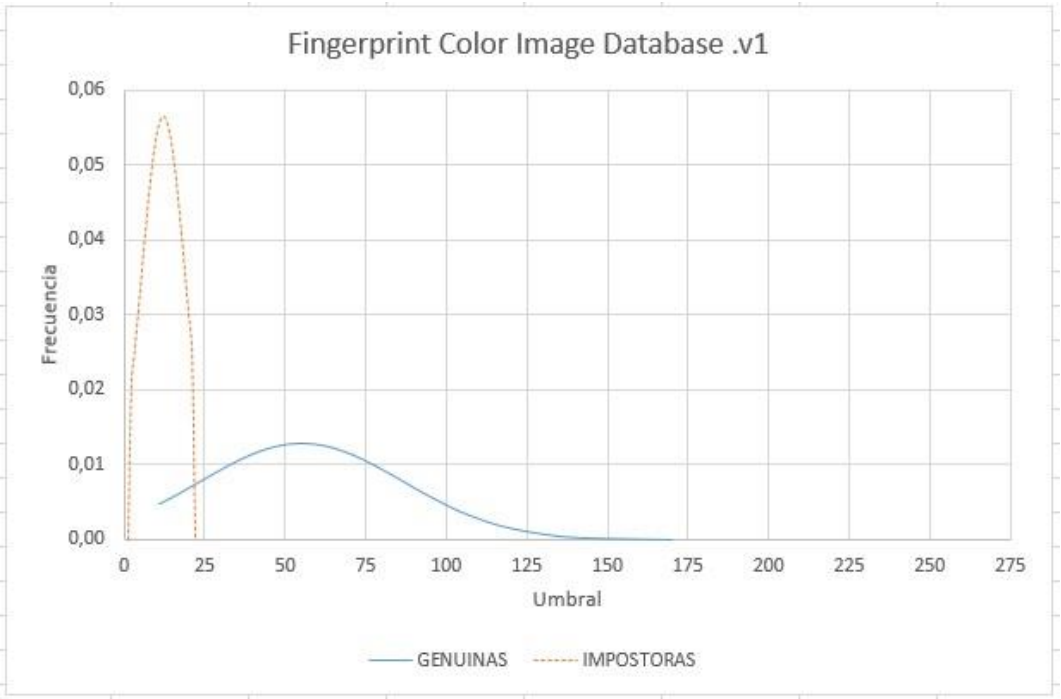


Figura 4-10. *Curvas de Distribuciones Fingerprint Color Image Database*

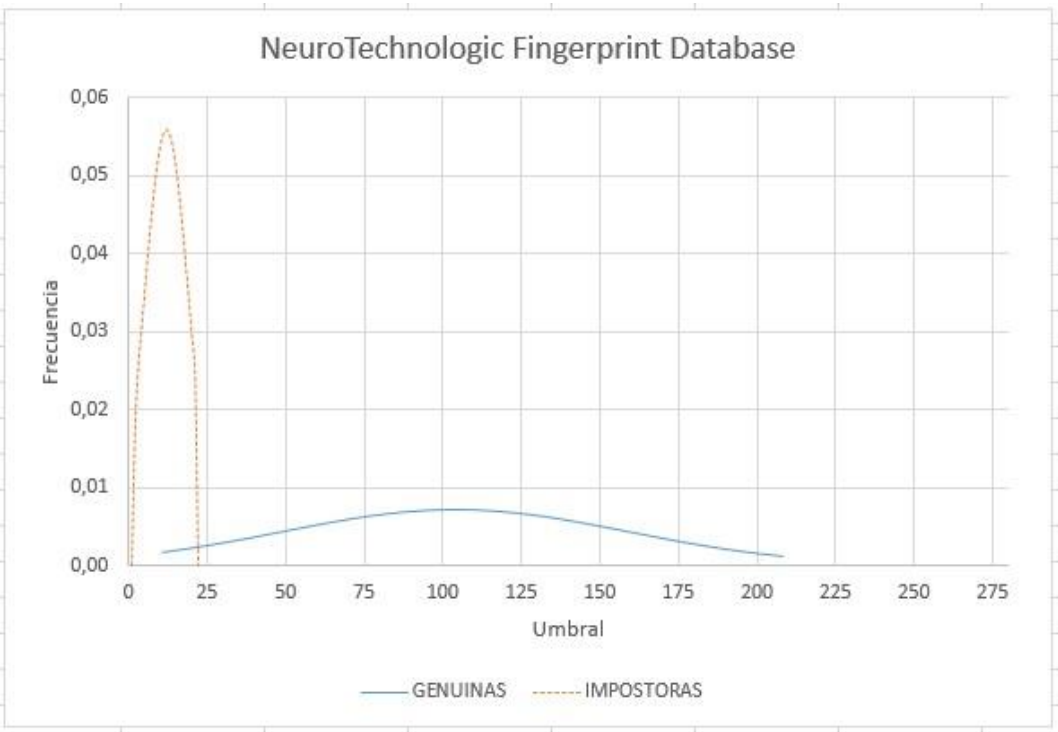


Figura 4-11. *Curvas de Distribuciones NeuroTechnologic Fingerprint Database*

4.4.2 Tasas de error

Para el cálculo de las tasas de error se procedió a calcular los puntajes de intentos genuinos (misma huella digital) e impostores (distintas huellas digitales) de verificación para cada base de datos de imágenes. Una vez obtenidos los puntajes se determinan las tasas de error FNMR, FMR, EER, y los indicadores FMR100, FMR1000, ZeroFMR, ZeroFNMR.

A continuación se describen las tasas de error según la base de datos utilizada.

Base de datos *FVC 2006 DB2 A*

La base de datos tiene 140 huellas de, con 12 muestras por cada una. Para el cálculo de la Tasa de Falsa No Concordancia FNMR, se realizaron 9240 (12x11x140/2) comparaciones, Ecuación (2.13) Capitulo II apartado 2.3.10.1, mientras que para el cálculo de la Tasa de Falsa Concordancia FMR, se realizaron un total de 9730 pruebas (140x139/2) (2.15) Capitulo II apartado 2.3.10.1. En el gráfico de la *Figura 4-12* se muestran los resultados obtenidos, donde puede observarse como las tasas FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 20) mientras que las tasas FNMR lo hacen en un rango mucho mayor (aproximadamente en el rango 10 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 10 y 21) que dan como resultado un EER = 2,29% para un umbral = 16,5; FMR100 = 2,54%; FMR1000 = 3,39%; ZeroFMR = 3,79%; ZeroFNMR = 99,96%.

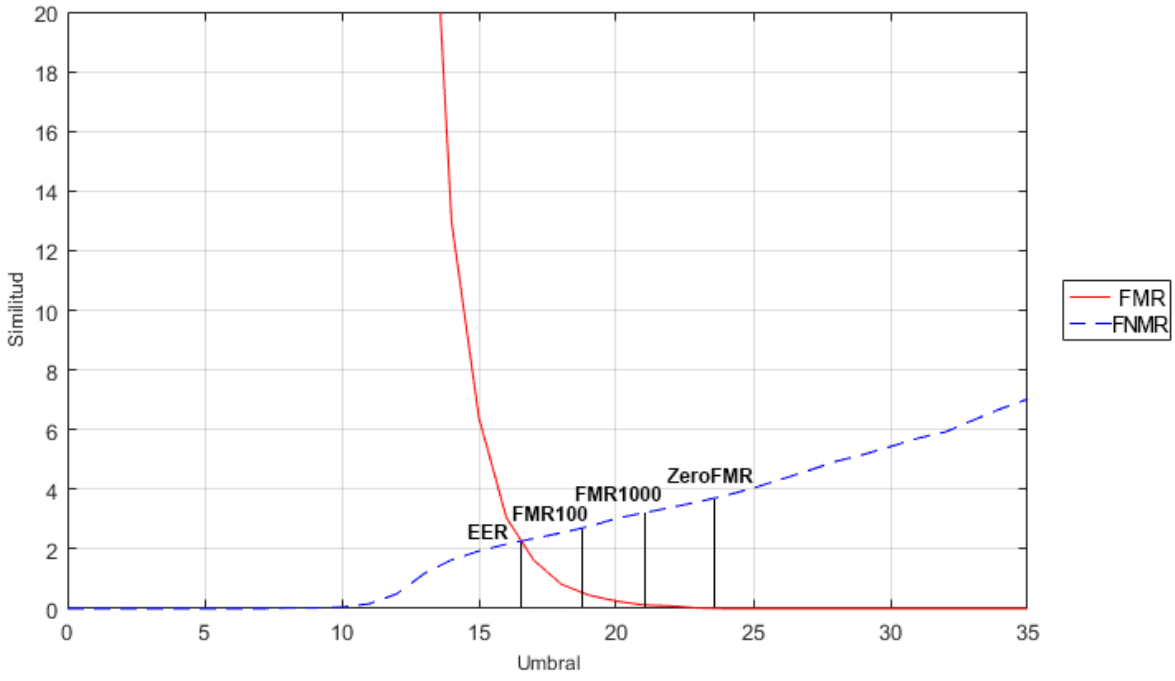


Figura 4-12. *Curvas FMR vs FNMR de FVC 2006 DB2 A*

Base de datos FVC 2006 DB3 A

Para el cálculo de la tasa FNMR se realizaron 9240 (12x11x140/2) comparaciones, mientras que para el cálculo de la tasa de FMR se realizaron un total de 9730 pruebas (140x139/2). En el gráfico de la *Figura 4-13* se muestran los resultados obtenidos. En la figura puede observarse como las tasas de FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 20) mientras que las tasas FNM lo hacen en un rango mucho mayor (aproximadamente en el rango 10 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 10 y 23) que dan como resultado un EER = 8,73% para un umbral = 14,5; FMR100 = 11,49%; FMR1000 = 14,39%; ZeroFMR = 19,98%; ZeroFNMR = 99,91%.

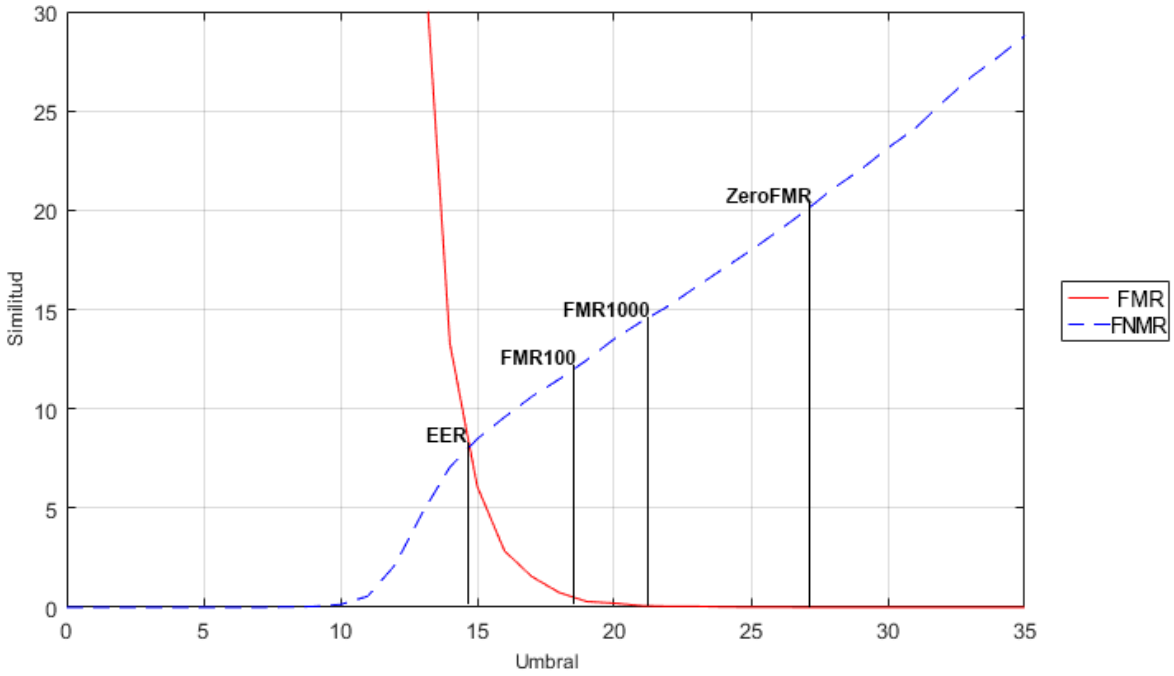


Figura 4-13. *Curvas FMR vs FNMR de FVC 2006 DB3 A*

Base de datos FVC 2006 DB4 A

Para el cálculo de la tasa FNMR se realizaron 9240 (12x11x140/2) comparaciones, mientras que para el cálculo de la tasa FMR se realizaron un total de 9730 pruebas (140x139/2). En el gráfico de la *Figura 4-14* se muestran los resultados obtenidos. En la figura puede observarse como las tasas FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 24) mientras que las tasas FNMR lo hacen en un rango mucho mayor (aproximadamente en el rango 12 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 12 y 24) que dan como resultado un EER = 5,49% para un umbral = 17,5; FMR100 = 8,87%; FMR1000 = 13,44%; ZeroFMR = 18,34%; ZeroFNMR = 99,89%.

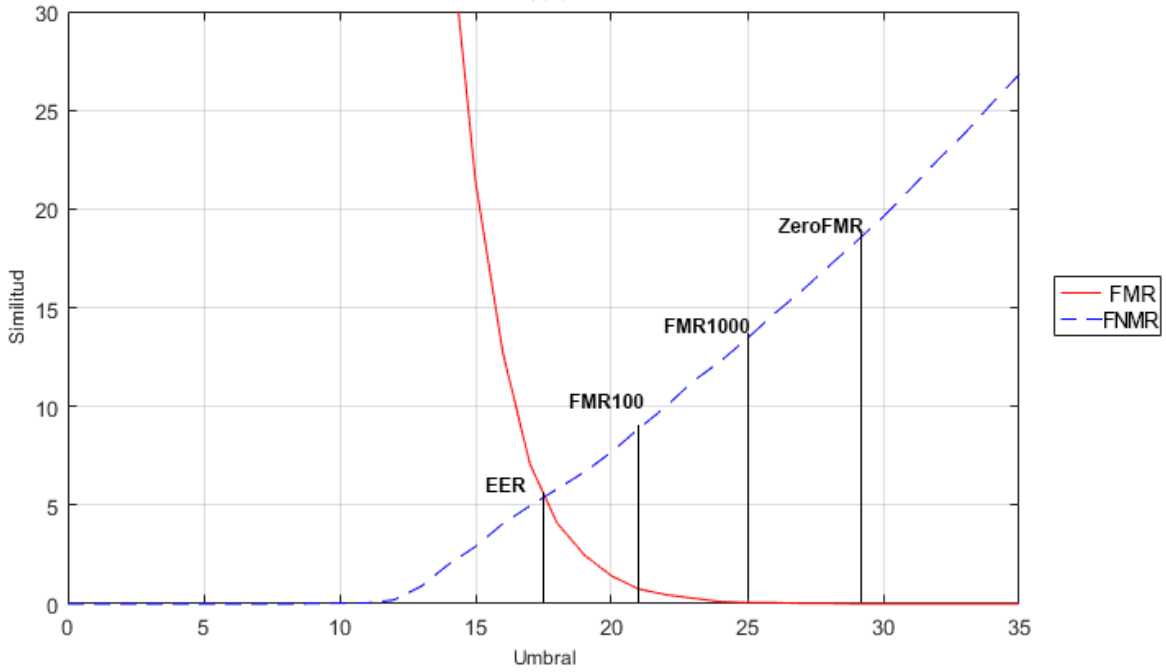


Figura 4-14. *Curvas FMR vs FNMR de FVC 2006 DB4 A*

Base de datos NIST Special Database 4

La base de datos tiene 100 huellas de, con 2 muestras por cada una. En el cálculo de la tasa FNMR se realizaron 100 (2x1x100/2) comparaciones, y el cálculo de la tasa FMR se realizaron un total de 4950 pruebas (100x99/2). En el gráfico de la *Figura 4-15* se muestran los resultados obtenidos. En la figura puede observarse como las tasas FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 24) mientras que las tasas FNMR lo hacen en un rango mucho mayor (aproximadamente en el rango 9 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 9 y 24) que dan como resultado un EER = 10,12% para un umbral = 15,10; FMR100 = 12,00%; FMR1000 = 13,00%; ZeroFMR = 14,00;% ZeroFNMR = 99,76%.

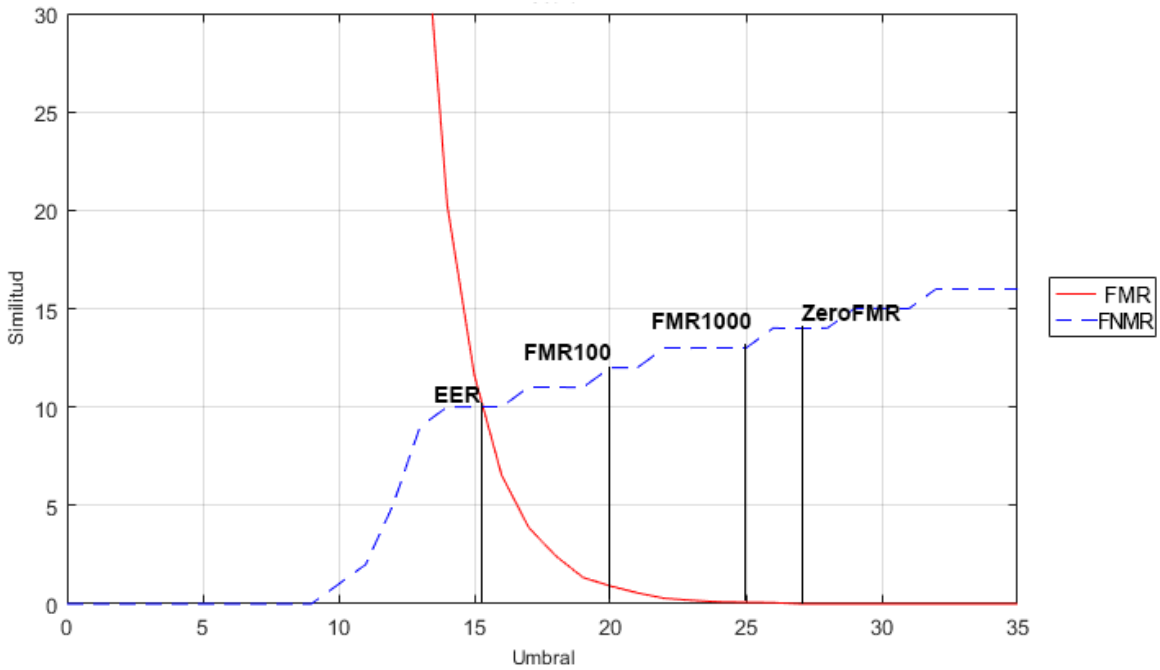


Figura 4-15. *Curvas FMR vs FNMR de NIST Special Database 4*

Base de datos NeuroTechnologic

La base de datos tiene 65 huellas de, con 8 muestras por cada una. Para el cálculo de la tasa FNMR se realizaron 100 (2x1x100/2) comparaciones, mientras que para el cálculo de la tasa FMR se realizaron un total de 4950 pruebas (100x99/2). En el gráfico de la *Figura* 4-16 se muestran los resultados obtenidos. En la figura puede observarse como las tasas FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 24) mientras que las tasas FNMR lo hacen en un rango mucho mayor (aproximadamente en el rango 13 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 13 y 24) que dan como resultado un EER = 1,57% para un umbral = 18,5; FMR100 = 2,25%; FMR1000 = 3,96%; ZeroFMR = 5,27;% ZeroFNMR = 93,08%.

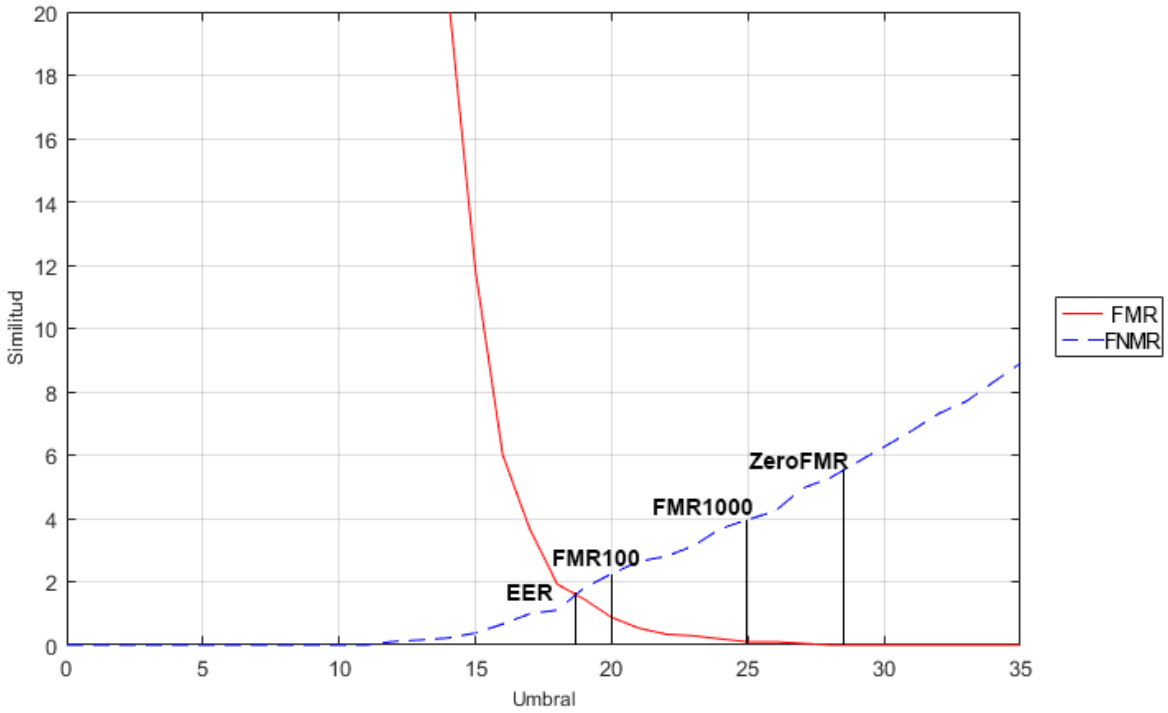


Figura 4-16. *Curvas FMR vs. FNMR de NeuroTechnology Fingerprint Database*

Base de datos Fingerprint Color Image Database .v1

La base de datos tiene 50 huellas de, con 5 muestras por cada una. Para el cálculo de la tasa FNMR se realizaron 500 (5x4x50/2) comparaciones, mientras que para el cálculo de la tasa FMR se realizaron un total de 1225 pruebas (50x49/2). En el gráfico de la *Figura 4-17* se muestran los resultados obtenidos. En la figura puede observarse como las tasas FMR se distribuyen en torno a un reducido valor es de similitud (aproximadamente en el rango de 0 a 26) mientras que las tasas FNMR lo hacen en un rango mucho mayor (aproximadamente en el rango 13 a 100) y la intersección de ambos rangos forman una zona reducida de valores de similitud (aproximadamente entre 13 y 26) que dan como resultado un EER = 8,98% para un umbral = 16,50; FMR100 = 16,50%; FMR1000 = 24,40%; ZeroFMR = 29,20;% ZeroFNMR = 99,76%.

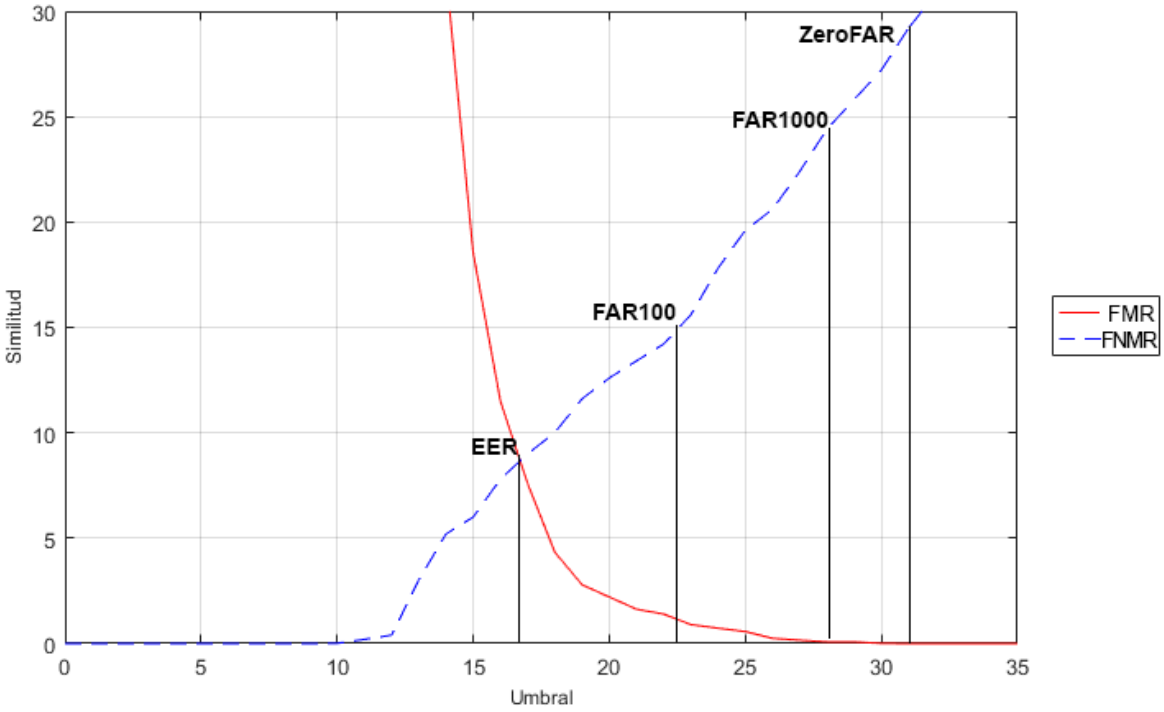


Figura 4-17. *Curvas FMR vs. FNMR de Fingerprint Color Image Database v1*

Resumen

En la *Tabla 4-3* se muestra un resumen de las tasas de error calculadas en las distintas bases de datos ordenadas por Tasa de Igual Error ERR, donde la Tasa de Falsa Concordancia (FMR) es igual a la Tasa de Falsa No Concordancia (FNMR), utilizado frecuentemente para caracterizar con un único número el rendimiento de un sistema biométrico. La caracterización del funcionamiento según lo descripto en el apartado "2.2.5 Caracterización del funcionamiento de un sistema biométrico" del Capítulo II, para las imágenes de la base de datos *NeuroTecnologic* presenta un nivel de funcionamiento alto con una EER = 1,5%. Por otro lado, con las imágenes de la base de datos Base de datos *NIST Special Database 4*, donde la captura de las imágenes se realizó manualmente (off-line) el nivel de rendimiento disminuye con una EER = 10%.

Las curvas DET *Figura 4-18*, donde se representa la Tasa de Falsa No Concordancia (FNMR) en el eje-Y y la Tasa de Falsa Concordancia (FMR) en el eje-X, generadas para cada una de las Base de Datos de prueba, se pude observar que la base de datos *NeuroTecnologic*, presenta el mejor rendimiento biométrico. Destacándose también la tasa FMR1000 de la base de datos *FVC2006 DB2 A*, que muestra un FNMR = 3,39% para un FMR 1/1.000, es decir, 1 de 1.000 intentos impostores es falsamente identificado como genuino y solo el 3.39% de los intentos genuinos fallaran.

Base de Datos	Umbral	EER (%)	FMR100 (%)	FMR1000 (%)	ZEROFMR (%)	ZEROFNMR (%)	Tamaño promed. PB (Bytes)	Tamaño máximo PB (Bytes)
NeuroTechnologic	**18,50**	**1,57**	**2,25**	**3,96**	**5,27**	**93,08**	**223,00**	**387,00**
FVC 2006 DB2 A	16,50	2,29	2,54	3,39	3,79	99,96	348,00	615,00
FVC 2006 DB4 A	17,50	5,49	8,87	13,44	18,34	99,89	208,00	471,00
FVC 2006 DB3 A	14,50	8,73	11,49	14,39	19,98	99,91	287,00	615,00
Fingerprint Color Image Database	16,50	8,98	15,60	24,40	29,20	99,76	153,00	273,00
NIST SpecialDatabase 4	15,10	10,12	12,00	13,00	14,00	99,76	579,00	615,00

Tabla 4-3. *Tasas de error calculadas para cada base de datos*

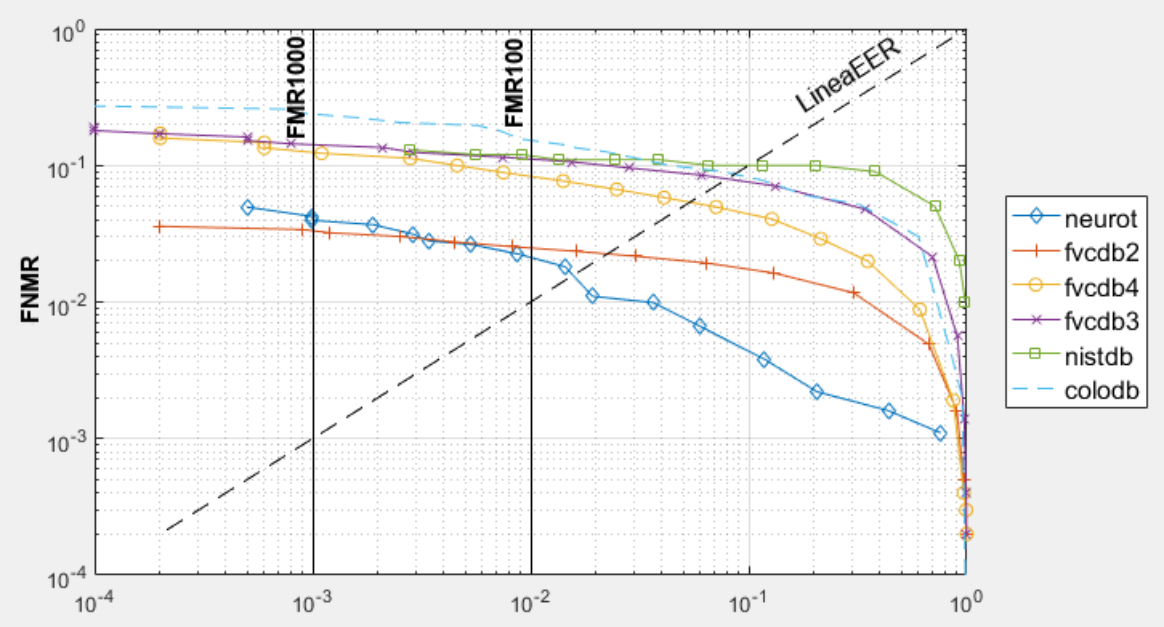


Figura 4-18. *Curva DET para las Bases de Datos de prueba*

4.4.3 Tiempos de ejecución

Los pruebas se realizaron utilizando una notebook Windows 10 Enterprise N2016 LSTB O.S. Intel Core i3-3271U – 1.8 GHz – 4 GB RAM y una PC Windows 10 Pro Intel Core i7 2600K – 3.7 GHz – 8 GB RAM. Los tiempos de ejecución se calcularon mediante la clase ***Stopwatch*** (NET Framewok) que proporciona una serie de métodos y propiedades para medir el tiempo transcurrido con precisión. Los tiempos se calcularon para la generación del patrón biométrico, para la comparación de patrones genuinos y para la comparación de patrones falsos.

Generación del patrón biométrico

Por cada imagen de huellas en la base de datos, se midió el tiempo que se demora en generar el patrón biométrico de una imagen de entrada. El cálculo se realizó exclusivamente en el proceso de generación, sin tener en cuenta el tiempo de adquirir la imagen desde la base de datos *Tabla 4-4*. Por Ejemplo, el tiempo promedio máximo de registro fue de 345 ms (Core i3) y de 83 ms (Core i7) para la Base de Datos *NIST SpecialDatabase 4*(huellas tintadas), mientras que el tiempo promedio mínimo 33 ms (Core i7) para la Base de Datos *NeuroTechnology* (sensor óptico) y 174 ms (Core i3) para la Base de Datos *FVC 2006 DB4 A* (huella artificial).

Comparación de patrones genuinos e impostores

Para cada par de patrones genuinos, (misma huella digital), y cada par de patrones impostores (huellas digitales diferentes), se tomó el tiempo que se demora en calcular la puntuación o similitud, dando como resultado los tiempos de la *Tabla 4-4*. El cálculo se realizó exclusivamente en el proceso de comparación, excluyéndose los tiempos de carga de los patrones biométricos desde la base de datos.

.

Base de Datos	CPU	Tiempo promedio de Registro (ms)	Tiempo promed de Comp. genuina (ms)	Tiempo promed de Comp. impostora (ms)
FVC 2006 DB2 A	i3	279	84	138
	i7	72	53	85
FVC 2006 DB3 A	i3	239	60	62
	i7	63	34	41
FVC 2006 DB4 A	i3	174	15	14
	i7	38	8	5
NIST SpecialDatabase 4	i3	345	108	106
	i7	83	66	73
Fingerprint Color Image Database	i3	94	7	5
	i7	55	3	2
NeuroTechnology	i3	190	17	13
	i7	33	7	5

Tabla 4-4. *Resumen de tiempos calculados*

Como puede observarse en la *Figura 4-19* las imágenes de huellas de la base de datos *NIST Special Database 4* generaran los mayores tiempos de registro de huellas, debido al mayor tamaño de los archivos de imágenes que posee *Figura 4-20*

.

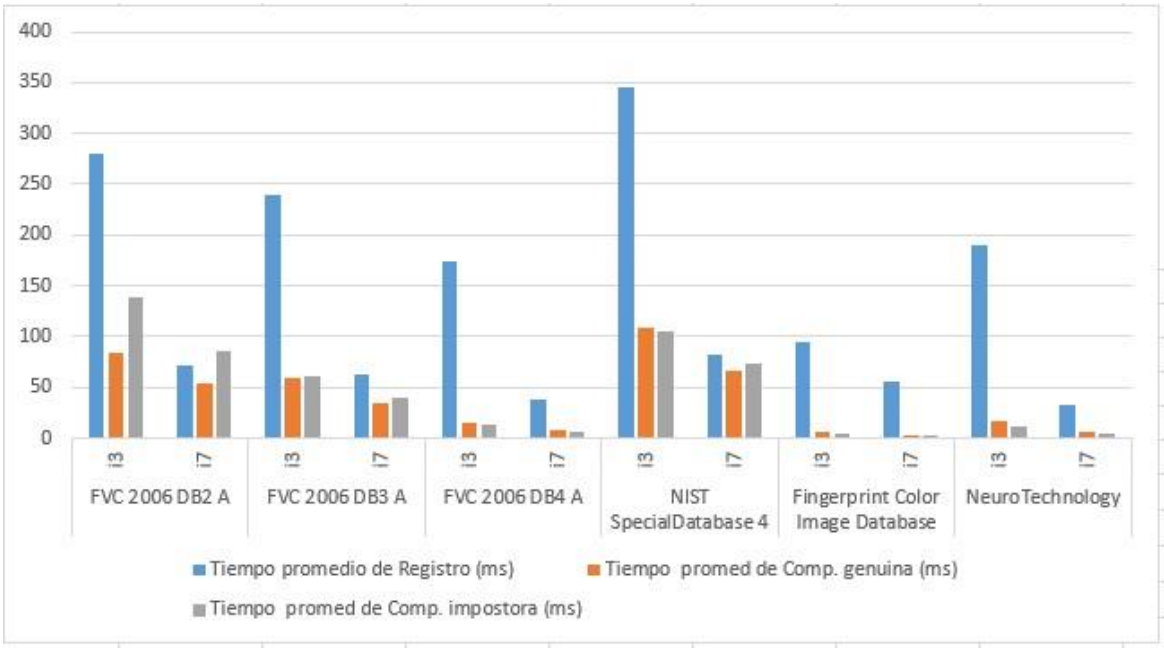


Figura 4-19. *Comparación de tiempos calculados*

.

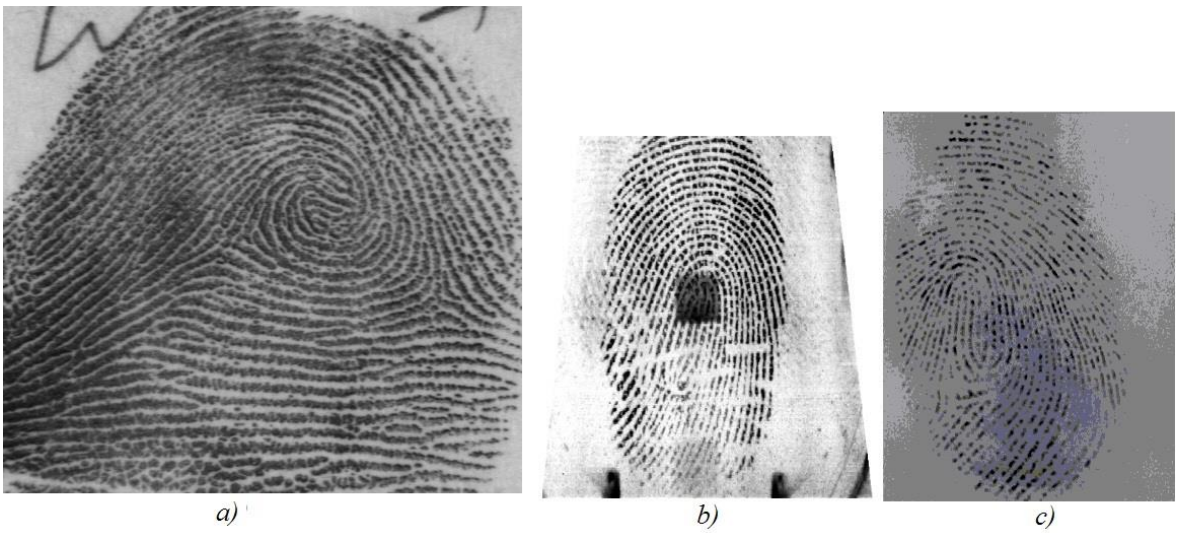


Figura 4-20. *Huellas digitales a escala. a) NIST Special Database b) NeuroTechnology Fingerprint Database c) FVC 2006 DB4 A*

Conclusiones

5.1 Conclusiones

Durante el desarrollo del trabajo final, se realizó un estudio profundo sobre el reconocimiento de huellas digitales utilizando la técnica de minucias. Logrando implementar un aplicativo de reconocimiento automático de huellas digitales, también se llevó a cabo una serie de evaluaciones que permitieron estimar las prestaciones del módulo de reconocimiento.

La elección de un sistema de reconocimiento basado en minucias, depende principalmente de las aplicaciones a las que va destinado. En aquellos casos en los que se desea precisión y fiabilidad, y por tanto, tasas reducidas de FAR y FRR, la comparación de patrones de minucias es el método recomendado por la mayoría de autores. Además, esta técnica no requiere de hardware especializado para su funcionamiento.

La implementación del módulo de reconocimiento, Capitulo 3, utilizando el patrón de diseño Modelo-Vista-Presentador (MVP), abre una amplia gama de posibilidades dentro del campo de evaluación de las prestaciones de módulos de reconocimiento de huellas digitales, permitiendo adaptar de manera sencilla otros módulos de reconocimiento y evaluar las prestaciones de los mismos, lo que deja un punto de partida para nuevas investigaciones.

De las pruebas efectuadas en el punto “4.4.2 Tasas de Error” del Capítulo IV, tras las adquisición de las bases de datos, se comprueba la elevada capacidad del módulo de reconocimiento para reconocer huellas provenientes de un mismo dedo. Las tasas de errores más bajas las encontramos en, ***FVC2006 DB2 A*** con EER 2,29%, ***NEUROTECHNOLOGU*** con EER 1,57%, en donde se observa que las mismas fueron adquiridas con escáneres ópticos. Tasas de errores un poco más elevadas en ***FVC2006 DB3 A*** con EER 8,73%, ***FVC2006 DB4 A*** con EER 5,49%, ***FINGERPRINT COLOR IMAGE DATABASE*** con ERR 8,98%, adquiridas con escáneres térmicos y generador de huellas artificiales. Y la tasa más alta obtenida en ***NIST FINGERPRINT DATABASE*** con EER 10,12% donde las imágenes de huellas tintadas fueron capturadas manualmente (*off- line*).

Se destaca las prestaciones obtenidas de la base de datos ***FVC2006 DB2*** con un rendimiento FRR de 3,39% y FAR 1/1,000, en el que 1 de cada 1000 intentos de huellas impostoras, es falsamente aceptado como genuina, y solo un 3,39% de huellas genuinas fallaron y fueron consideradas falsamente como impostoras.

De las pruebas efectuadas en el punto“4.3.3 Tiempos de Ejecución” del Capítulo IV, en el cálculo de los tiempos de procesamiento y comparación, el modulo ofrece tiempos muy bajos, entre 174 y 279 milisegundos para la generación del patrón biométrico, 15 y 80 milisegundos para la comparación de huellas genuinas y entre 14 y 138 para la comparación de huellas impostoras. Al utilizar un procesador más potente (Intel I7 2600K – 3.7 GHz), los tiempos disminuyeron notablemente, registrando promedios de tiempo entre 38 y 72, 8 y 53 y 5 y 85 milisegundos para el registro, comparación genuina y comparación impostora de patrones biométricos respectivamente. Además, se observó que el tamaño de la imagen afecta directamente los tiempos de procesamiento.

El conjunto de evaluaciones, tuvo como objetivo determinar las prestaciones del módulo de reconocimiento basado en la técnica de minucias, con un volumen mediano de datos, esto permitió evaluar el módulo de manera fiable y precisa, llegando a la conclusión que en dichos volúmenes de datos, una aplicación de reconocimiento automático de huellas

digitales basado en minucias e implementado por medio de software, presenta tasas de errores y tiempos de procesamientos aceptables.

REFERENCIAS

Ballard, D. H. (1981). Generalized Hough Transform to Detect Arbitrary Pattern. *IEEE Trans. Pattern Analysis and Machine Intelligence, 3*(2), 111-122.

Bansal, R., Sehgal, P., & Bedi, P. (2011). *Minutiae Extraction from Fingerprint Images.* New Delhi: IJCSI International Journal of Computer Science Issues.

Bigun J., G. G. (1987). Optimal Orientation Detection of Linear Symmetry. *Proceedings IEEE, 1st Int. Conf. on Computer Vision*, (pp. 433-438).

Bigun, J. G. (1991). Multidimensional Orientation Estimation with Applications to Texture Analysis and Optical Flow. *Trans. Pattern Analysis and Machine Intelligence, 13*(8), 775-790.

Bishop, J. (2008). *C# 3.0 Design Patterns.* Sebastopol: O'Reilly Media.

Cappelli, R., Lumini, A., Maio, D., & Maltoni, D. (1999). Fingerprint Classification by Directional Image Partitioning. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 402-421.

Chellappa, R., Wilson, C., & Sirohey, A. (1995). Human and Machine Recognition of Faces: A Survey. *Proceedings IEEE, 83*(5), 705-740.

Daugman, J. G. (1999). Recognizing Persons by Their Iris Patterns. In *Biometrics - Personal Identification in Networkwed Society* (pp. 103-121). Kluwer Academic Publishers, Chapter 5.

Election, M. (1973). Automatic Fingerprint Identification. *IEEE Spectrum, 10*(9), 36-45.

Ferrara, M., Franco, A., & Maltoni, D. (2007). *Fingerprint verification competition 2006.*

Fitz, P., & Green, R. J. (1996). Fingerprint Classification Using Hexagonal Fast Fourier Transform. *Pattern Recognition, 29*(10), 1587-1597.

Fuenmayor, G. (2004). *Avances en técnicas biometricas y sus aplicaciones en seguridad.*

Garcia Gomar, M. S. (2000). Identificación biométrica mediante comparación de patrones de minucias de huellas dactilares. *Actas XV Simposium Nacional de la Unión Científica Internacional de Radio (URSI).* Zaragoza, 13-15 Septiembre: URSI.

Hill, R. (1999). Retina Identification. In *Biometrics-Personal Identification in Networked Society* (pp. 123-141). Kluwer Academic Publishers.

Hong, L. W. (1998). Fingerprint Image Enhancement: Algorithm and Performance Evaluation. *IEEE Trans. Pattern Analysis and Machine Intelligence, 20*(8), 777-789.

Hong, L., & Jain, A. K. (1998). Integrating Faces and Fingerprints for Personal Identification. *IEEE Trans. Pattern Analysis and Machine Intelligence, 20*(12), 1295-1307.

Hung, D. C. (1993). Enhancement and Feature Purification of Fingerprint Images. *Pattern Recognition, 26*(11), 1661-1671.

Isenor, D. Z. (1986). Fingerprint Identification Using Graph Matching. *Pattern Recognition, 19*, 113-133.

ISO JTC1/SC37. (2006). *Iso 19795: Biometric performance testing and reporting: Part 1 Principles and Framework.* Switzerland: ISO/IEC 2006.

Jain, A. K. (2006). An Introduction to Biometric Recognition . *IEEE Trans. Circuits Syst. Video Techn*, 125-143.

Jain, A. K., & Pankanti, S. (2001). *Automated Fingerprint Identification and Imaging Systems, In Advances in Fingerprint Technology, H. C. Lee and R. E. Gaensslen (editors).* New York: Elsevier Science, 2nd edition.

Jain, A. K., Bolle, R. M., & Pankanti, S. (1999). *Biometrics: Personal Identification in a Networked Society.* Kluwer Academic Publishers.

Jain, A. K., Hong, , L., & Kulkarni, Y. (1999). *A Multimodal Biometric System Using Fingerprint, Face, and Speech.* Washington D.C. March 22-24.

Jain, A. K., Hong, L., Pankanti, S., & Bolle, R. (1997). *An Identity Authentication System Using Fingerprints.* Proceedings of the IEEE Vol. 8, No 9, pp. 1365-1388.

Jain, A. K., Hong, L., Pankanti, Sharath, & Bolle. (1996). *An Identity-Authentication System using Fingerprints.* New York.

Jain, A. K., Ross, A., & Prabhakar, S. (2001). *Fingerprint Matching Using Minutiae and Texture Features.* Thessaloniki, Greece, October 7-10.

Jain, A. K., Ross, A., & Prabhakar, S. (2004). *An Introduction to Biometric Recognition.* IEEE Transactions on Circuits and Systems for Video Technology.

Jain, K. P. (2000). *Fingerprint Classification and Matching, In A. Bovik, editor, Handbook for Image and Video Processing.* .: Academic Press.

Jain, K., Prabhakar, S., & Hong, L. (1999). A Multichannel Approach to Fingerprint Classification. *IEEE Trans. Pattern Analysis and Machine Intelligence, 21*(4), 348-359.

Karen, F. (1989). Encryptions, Smart Cards, and Fingerprint Readers. *IEEE Spectrum, 26*(8), 22.

Karu, K. J. (1996). Fingerprint Classification. *Pattern Recognition, 29*(3), 389-404.

Kawagoe, M., & Tojo, A. (1984). Fingerprint Pattern Classification. *Pattern Recognition, 17*(3), 295-303.

Kittler, J., Hater, M., Duin, R. P., & Matas, J. (1998). On Combining Classifiers. *IEEE Trans. Pattern Analysis and Machine Intelligence, 20*(3), 226-239.

Knutsson, H. E., Wilson, R., & Granlund, G. H. (1983). Anisotropic Nonstationary Image Estimation and its Application: Part-1 - Restoration of Noisy Images. *IEEE Trans. Communications, 31*, 388-397.

Komarinski, P. (2005). In P. Komarinski, *Automated Fingerprint Identification Systems (AFIS)* (p. 29).

Komariski, P. (2005). *Automated Fingerprint Identification Systems.* California: Elsevier Academic Press.

Lee, H. C., & Gaensslen, R. E. (2001). *Advances in Firgerprint Techology.* Now York: CRC Press.

Leiva Muñoz, P., Mayorga, F. J., & Serrano S, J. (2008). In *Extracción de minucias de huellas dactilares en imágenes digitales. Universidad de Sevilla* (p. 8).

Lopez Illescas, D. C., Peña Herrera Aroca, A. M., & Rodriguez Veintimilla, L. I. (2004). Desarrollo de Software utilizando la metodologia RUP. Ecuador.

Lu, G., & Zhang, D. (2002). Smart Card Aplication Based on Palmprint Identification. In *Biometrics Solutions for Authentication in an E-World.* Kluwer Academic Publisher.

Maio, D. M. (1997). *Direct Gray-Scale Minutiae Detection in Fongerprints.* IEEE Trans. Pattern Analysis and Machine Intelligence Vol 19, No. 1, pp. 27-40.

Maltoni, D., & Maio, D. (1996). A Structural Approach to Fingerprint Classification. *Proc. Int. Conf. on Pattern Recognition 13th pp. 578-585.* Vienna.

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* New York: Springer-Verlag.

Maltoni, D., Maio, D., Jain, A., & Prabhakar, S. (2003). *Handbook of Fingerprint Recognition.* Springer-Verlag New.

Marin , M., Rodriguez Uribe, J., & Olivares Morales, J. (2008). *Una mirada a la Biometría.*

Mehtre, B. M., Murthy, N. N., & Kapoor, S. (1987). Segmentation of Fingerprint Images Using the Directional Image. *Pattern Recognition, 20*(4), 429-435.

Miller, B. (1994). *Vital signs of identity.* IEEE Spectrum.

Morosi, P. (2003, Septiembre 04). *LA NACIÓN.* Retrieved 11 3, 2016, from http://www.lanacion.com.ar/524540-ponen-en-marcha-un-novedoso-sistema-de-identificacion-digital

NIST. (2017). *Nationa Institute of Standards and Technology*. Retrieved 03 02, 2017, from NIST Special Database 4: https://www.nist.gov/srd/nist-special-database-4

O´Gorman L., N. J. (1989). An Approach to Fingerprint Filter Design. *Pattern Recognition, 22*(1), 29-38.

Odaidat, M. S., & Sadoun, B. (1999). Keystroke dynamics based authentification. In *Biometrics-Personal Identification in Networked Society* (pp. 213-229). Kluwer Academic Publishers.

O'Gorman, L. (1998). Fingerprint Verification. In *Biometrics: Personal Identification in a Networked Society* (pp. 43-64). Kluwer Academic Publisher.

Ortega-Garcia, J., Bigun, J., Reynolds, D. A., & Gon, J. (2003). *Increasing Security in DRM Systems through Biometric Authentication.*

Plamondon, R., & Srihari, S. N. (2000). On-Line and Off-Line Handwritting Recognition: A Comprehensive Survey. *IEEE Trans. Pattern Anal. and Machine Intell, 22*(1), 63-84.

Prabhakar, S. J. (2000). Miniutae Verification and Classification for Fingerprint Matching. *Proceedings 15th ICPR International Conference On Pattern Recognition* (pp. 25-29). Barcelona, 3-8 Sep.: .

Prokoski, F. J., & Riedel, R. (1999). Infrared Identification of Faces and Body Parts. In *Biometrics-Personal Identification in Networked Society* (pp. 191-212). Kluwer Academic Publishers.

Ranade, S. R. (1983). Point Pattern Matching by Relaxation. *Pattern Recognition, 12*, 269-275.

Rao, A. R. (1990). *A Taxonomy for Texture Description and Identification.* New York: Springer-Verlag.

Ratha, N. C. (1995). Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images. *Pattern Recognition, 28*(11), 1657-1672.

Ratha, N. K., Connell, J., & Bolle, R. (1999). *Secure Biometric Authentication.* Morristown October 28-29, NJ: Proceedings IEEE Workshop on Atomatic Identification Advanced Technologies.

Ratha, N., Karus, K., Chen, S., & Jain, A. K. (1996). A Real-Time Matching System for Large Fingerprint Database. *IEEE Trans. Pattern Analysis and Machine Intelligence, 18*(8), 799-813.

RPP Noticias. (2012, Julio 30). *Noticias.* Retrieved 09 15, 2016, from http://www.rpp.com.pe/2012-07-30-utilizaran-lector-de-huellas-digitales-en-estadios-de-argentina-noticia_506961.html

Sánchez Reillo, R., & Sánchez-Ávila, C. (2001). RBF Neural Networks for Hand-Based Biometric Recognition. *Proceedings 3rd International Conference on Audio and Video-Based Person Authentication.* Halmstad, Sweden.

Schmuller, J. (2001). La concepción del UML. In *Aprendiendo UML 1a ed* (pp. 26,27). Prentice Hall.

Sherlock, B. G. (1993). A Model for Interpreting Fingerprint Topology. *Pattern Recognition, 26*(7), 1047-1055.

Sherlock, D. M. (1994). Fingerprint Enhancement by Directional Fourier Filtering. *IEEE Proceedings Vis. Image Signal Processing, 141*(2), 87-94.

Simon Zorita, D., Ortega Garcia, J., & Cruz Llanas, S. (2001). Minutiae Extraction Scheme for Fingerprint Recognition Systems. *Proceedings ICIP 2001, International Conference on Image Proceesing.* Thessaloniki, October 7-10.

Srinivasan, V. S. (1992). Detection of Singular Points in Fingerprint Images. *Pattern Recognition, 25*(2), 139-153.

Tojo, M., & Kawagoe, A. (1984). *Fingerprint Pattern Classification.* Pattern Recognition, Vol. 17, No. 3.

Tomoyose, G. (2013, Noviembre 07). *LA NACIÓN.* Retrieved septiembre 15, 2016, from SIBIOS: http://www.lanacion.com.ar/1635928-que-es-sibios-el-sistema-que-tiene-bajo-la-lupa-a-40-millones-de-argentinos

Willis, A. J. (2001). A Cost-Effective Fingerprint Recognition System for Use with Low-Quality Prints and Damage Fingertips. *Pattern Recognition, 34*(2), 255-270.

Xia, X., & O'Gorman, L. (2003). Innovations in Fingeprint Capture Devices. *Pattern Recognition, 36*(2), 361-369.

Xiao, Q., & Raafat, H. (1991). Fingerprint Image Postprocessing: A Combined Statistical and Structural Aproach. *Pattern Recognition, 24*(10), 985-992.

Yam, C. Y., Nixon, M. S., & Carter, J. N. (2003). Extended Model-Based Automatic Gait Recognition of Walking and Running. *Proceedings AVBPA'03, 4th International Conference on Audio and Video-Based Person Authentication*, (pp. 278-283). Surrey, London, 9-11 June.

Zhang, D. D. (2000). *Automated Biometrics, Technologies and Systems.* Kluwer Academic Publishers.

Zhang, D. D. (2002). *Biometrics Solutions for Authentication in an E-World.* Kluwer Academic Publishers.

Zhang, T. Y., & Suen, C. Y. (1984). *A Fast Parallel Algorithm for Thinning Digital Patterns.* Chongqing, China;: Communications of the ACM.

Zunkel, R. (1999). Hand Geometry Based Verification. In *Biometrics Personal Identification in Networked Society* (pp. 87-101). Kluwer Academic Publisher.

SITIOS WEB CONSULTADOS

ATVS. “Biometric Recognition Group” - http://atvs.ii.uam.es/atvs/fvc2006.html - Fecha de consulta: el 02 de 03 de 2017.

FVC2006. “Fingerprint Verificacion Competition” - http://bias.csr.unibo.it/fvc2006/ - Fecha de consulta: el 17 de 09 de 2016.

NEUROTECHNOLOGY “Neuro Technology” - http://www.neurotechnology.com/download.html - Fecha de consulta: el 07 de 02 de 2017.

NIST. “Nationa Institute of Standards and Technology” - https://www.nist.gov/srd/nist-special-database-4 - Fecha de consulta: el 02 de 03 de 2017.

MATHWORKS. - https://www.mathworks.com/matlabcentral/fileexchange/52507-fingerprint-color-image-database-v1 - Fecha de consulta: el 07 de 02 de 2017.

RPP Noticias. - http://www.rpp.com.pe/2012-07-30-utilizaran-lector-de-huellas-digitales-en-estadios-de-argentina-noticia_506961.html - Fecha de consulta: el 15 de 09 de 2016.

LA NACIÓN - http://www.lanacion.com.ar/524540-ponen-en-marcha-un-novedoso-sistema-de-identificacion-digital - Fecha de consulta: el 03 de 11 de 2016.

LA NACIÓN. - http://www.lanacion.com.ar/1635928-que-es-sibios-el-sistema-que-tiene-bajo-la-lupa-a-40-millones-de-argentinos - Fecha de consulta: el 15 de 09 de 2016.