



INSTITUTO POLITÉCNICO NACIONAL
CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN



La firma como un método biométrico de identificación

David Suárez Hernández¹
Edith Cristina Herrera Luna²
Edgardo Manuel Felipe Riverón³

RESUMEN

En este informe técnico se expone someramente lo que es la biometría, una breve descripción de los sistemas biométricos fundamentales desarrollados hasta el momento, así como las principales consideraciones que se deben tener en cuenta para el desarrollo de un sistema biométrico en particular. El rasgo biométrico que se considera más a fondo es la firma manuscrita, para el que se enlistan sus características globales y locales más usadas para su eventual reconocimiento, así como la forma en que se obtienen. De igual forma se presenta el análisis de varios trabajos que se han realizado en relación con la firma manuscrita, las técnicas que se han utilizado para la extracción de rasgos y los resultados obtenidos.

Palabras clave. Análisis de firmas; Biometría; Autenticación; Reconocimiento de patrones.

¹ Estudiante del Programa de la Maestría en Ciencias de la Computación, CIC.

² Estudiante del Programa de la Maestría en Ciencias de la Computación, CIC.

³ Profesor Investigador del Centro de Investigación en Computación (CIC).

“Este reporte contiene información desarrollada por el Centro de Investigación en Computación del Instituto Politécnico Nacional a partir de datos y documentos con derechos de propiedad y por lo tanto su uso queda restringido a las aplicaciones que explícitamente se convenga.

La aplicación no convenida exime al Centro de su responsabilidad técnica y da lugar a las consecuencias legales que para tal efecto se determinen.

Información adicional sobre este reporte podrá obtenerse recurriendo a la Unidad de Publicaciones y Reportes Técnicos del Centro de Investigación en Computación del I.P.N., Av. Juan de Dios Bátiz s/n, teléfono 5729-6000 ext. 56403, 56608 y 56610”.

Índice

| | |
|---|-----------|
| 1. INTRODUCCIÓN | 4 |
| 2. BIOMETRÍA | 5 |
| 2.1 ¿QUÉ ES? | 5 |
| 2.2 BIOMETRÍA ESTÁTICA | 7 |
| 2.3 BIOMETRÍA DINÁMICA | 10 |
| 2.4 PROCEDIMIENTO BIOMÉTRICO | 12 |
| 2.4.1 Recopilación de datos | 13 |
| 2.4.2 Transmisión de datos | 14 |
| 2.4.3 Procesamiento de señales | 14 |
| 2.4.4 Almacenamiento de datos | 14 |
| 2.4.5 Proceso de decisión | 14 |
| 2.5 EVALUACIÓN DE LOS SISTEMAS BIOMÉTRICOS | 14 |
| 2.6 FUSIÓN DE INFORMACIÓN | 15 |
| 2.7 BIOMETRÍA FORENSE | 17 |
| 3. FIRMA MANUSCRITA | 17 |
| 3.1 DEFINICIONES | 18 |
| 3.2 PROCESO DE OBTENCIÓN DE LA FIRMA MANUSCRITA | 18 |
| 3.3 ACONDICIONAMIENTO DE LA SEÑAL DE LA FIRMA | 19 |
| 3.3.1 Acondicionamiento para la firma obtenida fuera de línea (off-line) | 20 |
| 3.3.2 Acondicionamiento para la firma obtenida en línea (on-line) | 20 |
| 3.4 CARACTERÍSTICAS DE LAS FIRMAS | 20 |
| 3.4.1 Características dinámicas | 20 |
| 3.4.2 Características estáticas | 21 |
| 3.4.3 Características globales | 21 |
| 3.4.4 Características locales | 21 |
| 3.5 REPRESENTACIÓN DE LAS FIRMAS | 22 |
| 3.5.1 Representación paramétrica | 22 |
| 3.5.2 Representación mediante funciones | 22 |
| 4. ALGUNOS TRABAJOS REALIZADOS DE IDENTIFICACIÓN DE FIRMAS MANUSCRITAS | 23 |
| 4.1 VISUAL IDENTIFICATION BY SIGNATURE TRACKING (IDENTIFICACIÓN VISUAL POR SEGUIMIENTO DE LA FIRMA) | 23 |
| 4.2 STATIC SIGNATURE RECOGNITION BASED ON LEFT-TO-RIGHT HIDDEN MARKOV MODELS (RECONOCIMIENTO ESTÁTICO DE LA FIRMA BASADO EN LOS MODELOS DE IZQUIERDA A DERECHA OCULTOS DE MARKOV) | 24 |
| 4.3 VERIFICACIÓN DE LA FIRMA ESCRITA ESTÁTICA BASADA EN FUSIÓN DE CARACTERÍSTICAS LOCALES Y GLOBALES | 24 |
| 4.4 VERIFICACIÓN OFF-LINE DE FIRMAS MANUSCRITAS: UNA PROPUESTA BASADA EN SNAKES Y CLASIFICADORES FUZZY | 26 |
| 5. OBJETIVOS | 26 |
| 5.1 OBJETIVO GENERAL | 27 |
| 5.2 OBJETIVOS ESPECÍFICOS | 27 |
| 6. CONCLUSIONES | 27 |
| REFERENCIAS | 28 |

1. Introducción

La verificación y autenticación (o autenticación) de las personas es un tema de actualidad, en los ámbitos donde la seguridad es primordial para evitar fraudes y la usurpación de la personalidad de los individuos. Se han venido realizando investigaciones sobre cómo poder identificar o autenticar a una persona de manera robusta, eficiente y confiable. La biometría se encarga del estudio de los rasgos únicos propios de cada individuo que los diferencia de los demás individuos.

Entre los rasgos que estudia la biometría se pueden mencionar los que provienen de la huella dactilar, de la voz, de la estructura del Ácido Desoxirribonucleico (ADN) humano, de la firma y la escritura manuscrita, de la forma de andar, del iris y las características de la red vascular de la retina del ojo humano, entre otras. En cada uno de estos rasgos se obtienen características que los hacen únicos, con cuya ayuda es posible poder diferenciar unos individuos de otros. Debido a que la identificación y la verificación deben ser de forma rápida y precisa para que puedan utilizarse en los sistemas de seguridad, se han creado los sistemas biométricos automatizados, en los que hay dos maneras de obtener los rasgos, a saber: en línea (*on-line*) que agrupa a los sistemas dinámicos, y fuera de línea (*off-line*) que agrupa a los sistemas estáticos. Algunos sistemas permiten obtener los rasgos de ambas maneras, como por ejemplo, en los relacionados con la firma manuscrita.

La firma manuscrita es el medio más cotidiano que se usa para la verificación de la identidad de una persona, ya sea para indicar la autoría de un documento por una persona en particular, o para la certificación de la conformidad de una persona en cualquier tipo de transacción. Por ello, a la firma se le considera como una característica biométrica confiable para la identificación de una persona o para la verificación de su personalidad; sin embargo, la frecuencia de los intentos de falsificación de la firma en la actualidad es relativamente grande.

El presente reporte técnico consta de tres partes: en la primera se explica someramente lo que es la biometría y su campo de estudio; la segunda parte se dedica a la firma manuscrita como rasgo biométrico, sus características fundamentales y su forma de obtención; la tercera parte consta del análisis de algunos trabajos realizados en torno al reconocimiento e identificación de la firma manuscrita, su forma de obtención, las técnicas más frecuentemente utilizadas para la extracción de sus rasgos y la forma de compararlos.

Este reporte está relacionado con la temática del tema de tesis intitulado “**Nivel de compatibilidad de un texto manuscrito con la firma**”, el cual a grandes rasgos trata, a partir de un texto manuscrito con firma dado, determinar si dicha firma y texto son del mismo autor a partir de una base de datos compuesta previamente confeccionada.

2. Biometría

2.1 ¿Qué es?

La biometría es una tecnología que reconoce a una persona sobre la base de *quién* es la persona, sin interesar lo que ésta lleve o conozca, sino de características humanas propias, inalterables y únicas, las cuales no pueden ser olvidadas, sustraídas o duplicadas. Algunas definiciones de la biometría son las siguientes:

1. El término biometría clásicamente se aplica de forma general a la ciencia que se dedica al estudio estadístico de las características cuantitativas de los seres vivos; en épocas recientes este término se utiliza también para referirse a los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas [1].
2. La biometría es una medida de las características físicas o rasgos personales de un individuo, las cuales son usadas para reconocer o verificar la identidad que se reclama del mismo [2].

En ambas definiciones se observa que la biometría se basa en el reconocimiento de rasgos o características únicos de los seres vivos, las que por las diferencias que ocurren entre sí, permiten una correcta autenticación (o autenticación).

En función de las características usadas para la identificación, se pueden establecer dos tipos de biometrías: *la estática*, la cual se refiere al estudio de características físicas y *la dinámica* para el conjunto de características conductuales [1].

Tanto las características físicas como las conductuales deben cumplir con unos requisitos básicos para que puedan ser utilizadas como elementos de identificación. Entre estos se pueden mencionar [1]:

- **Universalidad.** Toda persona debe presentar la característica.
- **Singularidad.** La característica seleccionada para la autenticación tiene que ser única para cada persona, de tal forma que se puedan distinguir dos personas cualesquiera basándose en ésta.
- **Estabilidad.** Tiene que ser estable a lo largo del tiempo y en condiciones ambientales diversas.
- **Cuantificable.** Tiene que ser mensurable cuantitativamente.
- **Aceptabilidad.** Su nivel de aceptación debe ser suficiente para ser considerada parte de un sistema de identificación biométrico.
- **Rendimiento.** El nivel de exactitud requerido debe ser elevado para que la característica sea considerada como aceptable.
- **Usurpación.** Permite establecer el nivel al que el sistema es capaz de resistir a técnicas fraudulentas.

La finalidad de la biometría, en base de las características seleccionadas, es la de poseer un conjunto de herramientas que permitan la identificación o verificación de la identidad de una persona. Se puede definir identificación y verificación bajo los siguientes términos [1]:

Identificación

Se trata de responder a la pregunta: ¿Quién es la persona X? En este caso se trata de una persona de la cual se desconoce su identidad. Para ello es preciso contar con un sistema que contenga los siguientes elementos:

1. Una base de datos que contenga las características almacenadas de un amplio grupo de personas.
2. Un mecanismo (sensor) para capturar y procesar las características de la persona a identificar.
3. Un procedimiento para comparar las características de la persona a identificar con las almacenadas en la base de datos.

El proceso de identificación es una combinación de uno a muchos (1: N).

Verificación

Se trata de responder a la pregunta: ¿Es esta persona X? En este caso una persona reclama tener cierta identidad y el sistema trata de confirmar si ésta es correcta. Es preciso contar con los siguientes elementos en el sistema:

1. Un sistema de identificación tipo usuario más palabra clave (*password*).
2. Un mecanismo para capturar y procesar las características de la persona a identificar.
3. Un procedimiento para comparar las características de la persona a identificar con las almacenadas en la base de datos.

El proceso de verificación es una combinación de uno a uno (1:1).

En el ámbito de la biometría, se establecen las siguientes métricas que controlan el funcionamiento de los sistemas [9]:

- **Proporción de falsas aceptaciones** (*False Accept Rate*, FAR). Probabilidad de que el sistema declare erróneamente como un éxito el emparejamiento de un patrón de entrada y un patrón de la base de datos que no coinciden.
- **Proporción de falsos rechazos** (*False Reject Rate*, FRR). Probabilidad de que el sistema declare erróneamente como un fallo el emparejamiento de un patrón de entrada y un patrón de la base de datos que sí coinciden.
- **Característica de operación relativa** (*Relative Operating Characteristic*, ROC). Es el algoritmo que compara los patrones de la base de datos y los nuevos introducidos, y toma sus decisiones en función de varios parámetros.
- **Proporción de error igual** (*Equal Error Rate*, EER). Es la proporción para la cual los errores de aceptación y rechazo se hacen iguales.

- **Proporción de fallos al inscribirse** (*Failure to Enroll Rate*, FER). Porcentaje de individuos que falla al registrarse en el sistema.
- **Proporción de fallos al capturar** (*Failure to Capture Rate*, FCR). Probabilidad de que el sistema falle al detectar una característica biométrica que le ha sido presentada correctamente.
- **Capacidad de plantillas** (*Template Capacity*). Máximo número de personas que un sistema en concreto es capaz de distinguir.

2.2 Biometría estática

Dentro de la biometría estática se consideran útiles las siguientes características:

- **Huella dactilar.** La identificación de personas a través del estudio analítico de la huella dactilar (Fig. 2.1), denominada técnica de dactiloscopia, responde al método de identificación biométrica por excelencia, ya que cumple con las dos leyes básicas que regulan el nivel de viabilidad de todo el sistema de identificación: la invariabilidad temporal y la variedad infinita del autenticador [1].



Figura 2.1 Huella dactilar

- **Características del ojo: retina e iris.** Hay dos técnicas biométricas diferentes basadas en el reconocimiento de personas a través del ojo humano: una basada en las características del iris ocular y la otra que utiliza características distintivas de la retina (Fig. 2.2). En ocasiones se suele confundir una con otra con lo que a ambas se les suele considerar como una única técnica denominada biometría del ojo. Sin embargo, el iris y la retina oculares dan lugar a dos sistemas biométricos completamente diferentes, tanto en los métodos de captura de la imagen y las técnicas de extracción de características como en los métodos de comparación.



Figura 2.2 Retina e iris del ojo humano

- **Geometría de la mano.** El uso de la geometría de diversas partes del cuerpo para identificar a las personas, se inició en época de los antiguos egipcios. No se ha avanzado mucho en esta técnica biométrica, aunque diversos expertos sostienen que la fiabilidad de la mano es lo suficientemente alta como para identificar a una persona; incluso existe un sistema comercial de identificación automática mediante la geometría de la mano (Fig. 2.3) [8].



Figura 2.3 Mano humana

- **Características del rostro.** Los problemas y técnicas de reconocimiento del rostro (Fig. 2.4), pueden ser separados ampliamente en dos grupos: dinámica (video) y estática (no video). El modo dinámico se usa cuando se dispone de una secuencia de video; el modo estático usa imágenes con iluminación controlada, fondo, resolución y una distancia conocida promedio entre la cámara y la persona [3].



Figura 2.4 Rostro

- **Reconocimiento por las venas de la palma de la mano.** El reconocimiento por medio de las venas de las manos es una de las últimas novedades en lo que a biometría se refiere (Fig. 2.5). Se captura una imagen del tramado de las venas de la palma de la mano a través del reflejo de rayos casi infrarrojos emitidos. Las venas son elementos internos del cuerpo humano, y tienen gran abundancia de características que las hacen diferente de una persona a otras, más aún si se tiene en cuenta que la sangre ha de estar fluyendo para registrar la imagen o patrón que sirve de identificación [9].



Figura 2.5 Captura de la imagen de las venas de la palma de la mano

- **Reconocimiento de la palma de la mano.** El reconocimiento de la palma de la mano está basada en la información presentada por la fricción de las crestas con una superficie (Fig. 2.6). Esta información incluye el sentido de las crestas y la presencia (o ausencia) de minucias en la huella palmar [9]

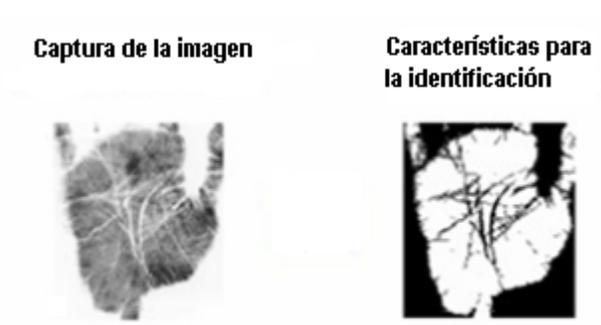


Figura 2.6 Captura de la imagen de la palma de la mano

- **Reconocimiento de la huella del pabellón auricular (Fig. 2.7).** Esta tecnología biométrica se ha desarrollado especialmente para la medicina legal y forense. Se basa en una reproducción bidimensional del pabellón auricular y se maneja de manera similar a la huella digital o a la huella palmar [9].

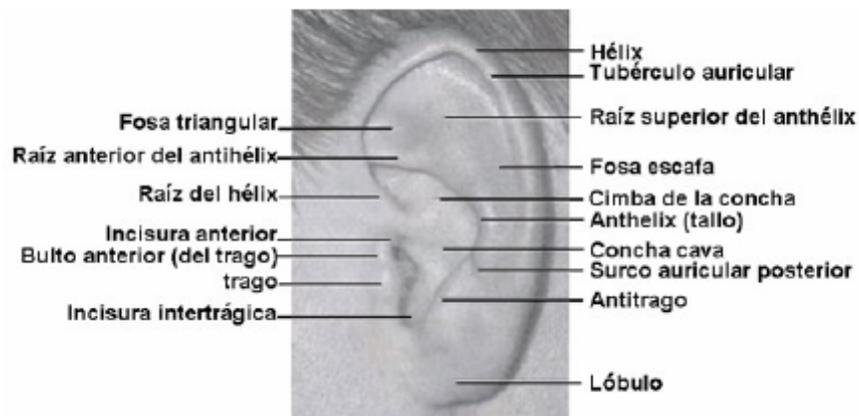


Figura 2.7 Partes del pabellón auricular

- **Reconocimiento de ADN (Fig. 2.8).** Es un sistema biométrico que se puede obtener de un pelo, de la saliva, sangre, etc., que requiere de una muestra física y de su comparación. Actualmente no se puede realizar en tiempo real. La comparación de las estructuras del ADN no utiliza plantillas o extracción de rasgos [9].



Figura 2.8 Cadena de ADN

2.3 Biometría dinámica

Dentro de la biometría dinámica se pueden considerar las siguientes características [1]:

- **Escritura manuscrita.** La grafística es la disciplina forense que tiene como objetivo la identificación o autenticación de los autores de manuscritos. Se centra por tanto en el análisis de documentos escritos a mano (Fig. 2.9). La biometría de la escritura o identificación del escritor tiene como objetivo el desarrollo de sistemas informáticos que puedan desempeñar esta tarea de manera automática [1].

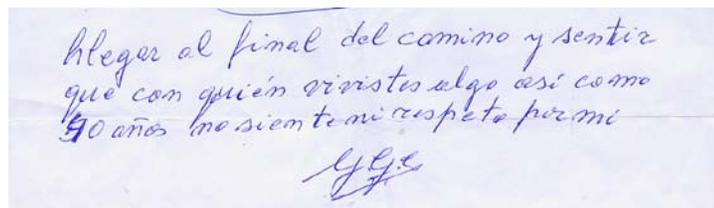


Figura 2.9 Muestra de texto y firma

- **Voz.** Los sistemas de reconocimiento del locutor tienen por objeto discriminar locutores a partir de características diferenciadoras obtenidas mediante el análisis y el tratamiento de la señal de voz (Fig. 2.10). El estudio de los mecanismos de producción de ésta se incluyen dentro de disciplinas tales como la acústica de cavidades, la anatomía humana, la física de los fluidos o la propagación de las ondas acústicas [1].



Figura 2.10 Muestra de una señal de voz

- **Reconocimiento de patrones de tipeo.** Verifica la identidad de un individuo examinando sus patrones de tipeo en un teclado (Fig. 2.11). Usan la duración entre tipeo como característica de verificación del usuario; otros utilizan el tiempo que permanece la tecla presionada. Esta tecnología utiliza clasificadores bayesianos, redes neuronales y sistemas difusos (*fuzzy systems*) [9].



Figura 2.11 Tipeo de usuarios

- **Reconocimiento de la marcha (pasos de una persona).** Verifica la identidad de un individuo examinando su patrón de marcha (Fig. 2.12). La ventaja de este sistema es que el reconocimiento se puede realizar potencialmente a distancia [9].



Figura 2.12 Reconocimiento del modo de andar de una persona

- **Termografía facial.** Mide los patrones infrarrojos de emisión de la cara producidos por el flujo de sangre bajo la piel (Fig. 2.13). Es una tecnología no invasiva que no requiere de contacto físico, es continua y accesible a la mayoría de los usuarios. La verificación o identificación puede ser lograda a dos o más pies de distancia y sin que el usuario tenga que esperar largos periodos de tiempo [9].

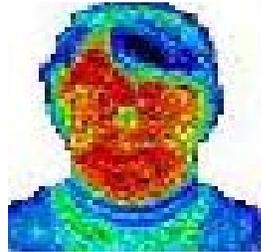


Figura 2.13 Termografía facial

- **Reconocimiento de los labios.** Esta tecnología biométrica se divide en tres subcategorías: huella de los labios, movimiento de los labios y forma de los labios. La huella de los labios es conocida en la ciencia forense por ser diferentes para cada individuo. El movimiento de los labios ayuda a la identificación asociada con el reconocimiento de la voz (Fig. 2.14). La forma de los labios puede ser usada como una característica o rasgo individual para lograr la autenticación [9].

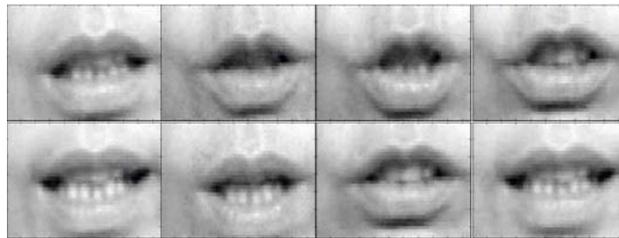


Figura 2.14 Muestras de los movimientos de labios de una persona

2.4 Procedimiento biométrico

Una de las aproximaciones del procedimiento biométrico ha sido elaborada por James L. Wayman [4], la cual establece el modelo de un sistema general de identificación biométrica. El modelo propuesto por Wayman se compone de cinco subsistemas [1]:

- Recopilación de datos.
- Transmisión de datos.
- Procesamiento de señales.
- Almacenamiento de datos.
- Proceso de decisión.

De manera esquemática se muestra en la figura 2.15.

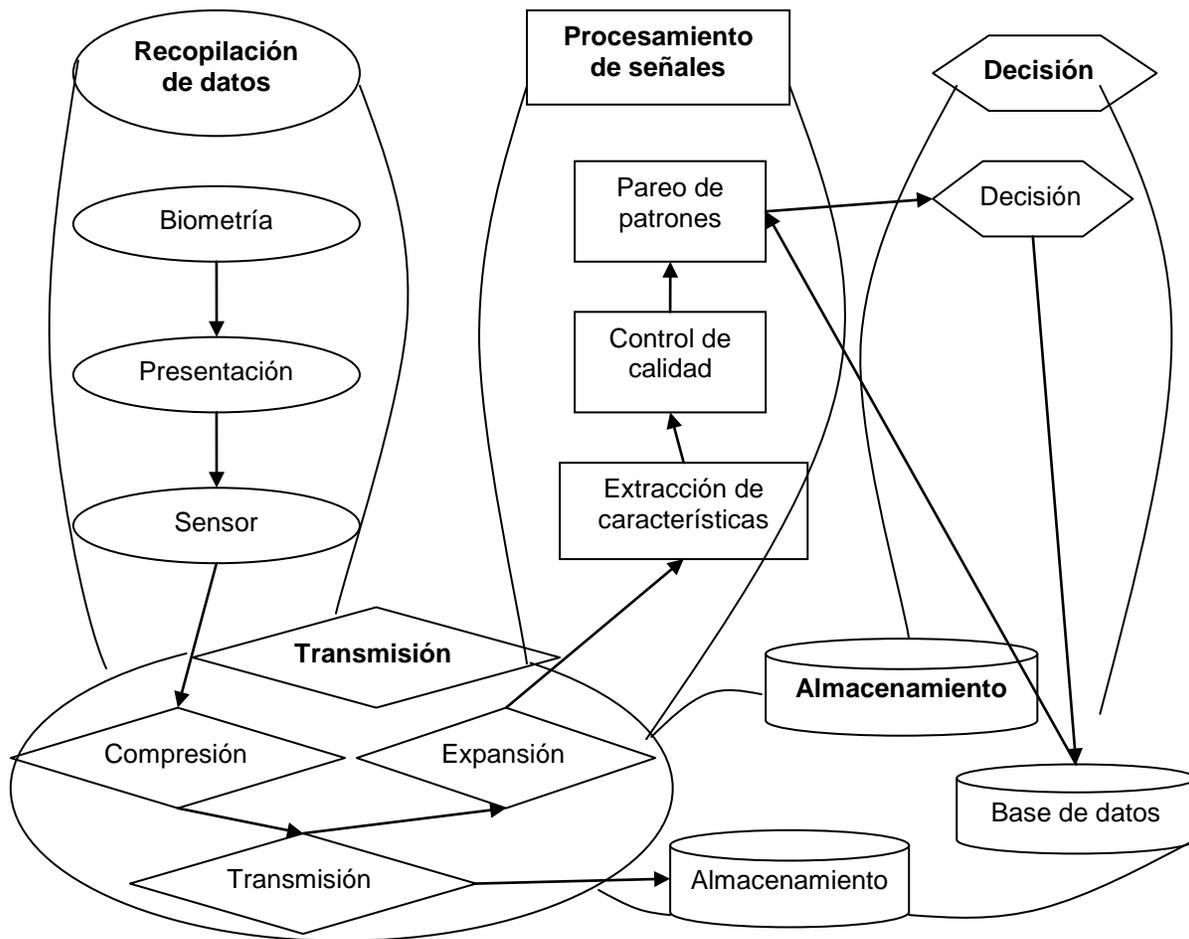


Figura 2.15 Esquema general del procedimiento biométrico

2.4.1 Recopilación de datos

Abarca todos los aspectos relacionados tanto con la fase de darse de alta en el sistema, como con los procedimientos de identificación y verificación que se llevan a cabo cuando un usuario pretende acceder a un sistema controlado mediante técnicas biométricas.

Uno de los problemas que puede encontrarse en la recopilación de datos es que como se trata de medidas biológicas, éstas están sujetas al deterioro causado por la edad y por daños causados por traumas, heridas, etc.; otra problemática tiene que ver con los dispositivos físicos que se encargan de la captura de la información biométrica (sensores), ya que estos precisan que la información a capturar se haga de la forma más estandarizada posible. Esta variabilidad presenta efectos contraproducentes para considerar la confiabilidad de las técnicas biométricas para la identificación y la verificación de los usuarios.

2.4.2 Transmisión de datos

La captura de datos biométricos suele localizarse lejos del lugar donde se almacenarán y procesarán posteriormente. En la mayoría de los casos los datos biométricos sin procesar ocupan un espacio en bytes bastante considerable debido a la naturaleza de su origen y la cantidad de información que contienen.

Debido al gran volumen de información que manejan estos sistemas se hace preciso utilizar técnicas de compresión digital de información. Un aspecto que se debe tomar en cuenta es la pérdida de información que tiene lugar al comprimir y descomprimir la información, por lo que puede suceder que los datos que se recuperan no sean exactamente iguales a los datos que se almacenaron en forma comprimida.

2.4.3 Procesamiento de señales

En esta etapa se extraen determinadas características biométricas presentes en la señal original, las que debido a sus propiedades invariantes en el tiempo, a la forma de presentación, al tipo de sensor, al método de compresión y al sistema de transmisión, se han de considerar como las más relevantes a efectos de la comparación entre las diferentes muestras.

Con la información extraída se genera un “vector de características”, el cual es la unidad de información para ulteriores comparaciones y para el subsistema de toma de decisiones.

2.4.4 Almacenamiento de datos

La información obtenida durante la fase de inscripción debe ser almacenada en forma estructurada para facilitar el procedimiento de identificación y verificación. La estructura debe tener una organización flexible que incluya no solamente los vectores de las plantillas biométricas, sino también aquellas etiquetas de identificación del usuario del que provienen.

2.4.5 Proceso de decisión

El proceso de identificación y verificación culmina con la medida de un índice de comparación entre las plantillas almacenadas (vector de características, p. e.) y los datos introducidos relacionados con un usuario; este índice permitirá tomar una decisión acerca de si la verificación o identificación es correcta o no lo es.

2.5 Evaluación de los sistemas biométricos

Una evaluación completa de un sistema biométrico debería prestar igual atención a todos los aspectos, desde la captura de los datos, hasta la integración total del sistema.

Se pueden destacar los siguientes puntos a analizar:

- El rendimiento con respecto a su función.
- La seguridad, integridad y confidencialidad de los datos que maneje el sistema.
- La fiabilidad, disponibilidad y mantenimiento de la aplicación informática.

- Todo lo referente a la comercialización del producto.
- La aceptación y/o facilidad de manejo por parte del usuario.
- Las cuestiones legales.

El protocolo de evaluación reflejará las decisiones tomadas en este punto, e indicará qué aspectos son impuestos por el sistema, el entorno de aplicación o el fabricante, cuáles son definidos para delimitar el ámbito del estudio, y para cuáles se plantea analizar su influencia en el rendimiento del sistema.

2.6 Fusión de información

El concepto de fusión de información sucede cuando se utiliza una combinación de información proveniente de diferentes fuentes u orígenes. Su finalidad es la de alcanzar una decisión más fiable, sacando provecho de toda la información disponible [1].

Algunos ejemplos de fusión de información son:

- Captación de señales con más de un sensor. Se obtienen las señales de muestra con más de un tipo de sensor.
- Combinación de dos tipos distintos de información. Estos mecanismos contribuyen a tener un conocimiento más profundo del mundo exterior.
- Combinación de opiniones. Con la finalidad de obtener una decisión más objetiva, se valoran las opiniones de varias personas.
- Combinación de decisiones. Cada participante decide una opción y el resultado final es la combinación de las opiniones expresadas por todos los participantes.

En aplicaciones de reconocimientos de personas son posibles estos mismos niveles. Atendiendo a la procedencia de las informaciones se puede establecer la clasificación en dos grandes grupos:

- Fusión unimodal. Trata con un único tipo de dato biométrico.
- Fusión multimodal. Utiliza dos o más tipos de datos biométricos.

La idea principal de utilizar la fusión de información es la de reducir las limitaciones de los sistemas unimodales, entre las cuales se pueden mencionar las siguientes:

- **Ruido en la captura.** Creado por sensores defectuosos o por malas condiciones durante la captura de los datos.
- **Variabilidad intra-usuario.** Dada por la interacción incorrecta del usuario con el sensor, variación de las características del sensor, o variación de las características del usuario.
- **Poder discriminante.** Información limitada en cada rasgo.
- **No universalidad.** Fallo al registrar a determinados usuarios.
- **Ataques al sistema.** Uso de rasgos artificiales.

Para minimizar estas limitaciones es que se utilizan los sistemas multibiométricos, donde se combinan varias fuentes de información biométrica para mejorar el rendimiento de un determinado sistema; se aumenta la cobertura de la población reduciendo el fallo en el registro y se mejora la seguridad del sistema al aumentar la dificultad de imitar o falsificar varios rasgos simultáneamente (Figura 2.16).

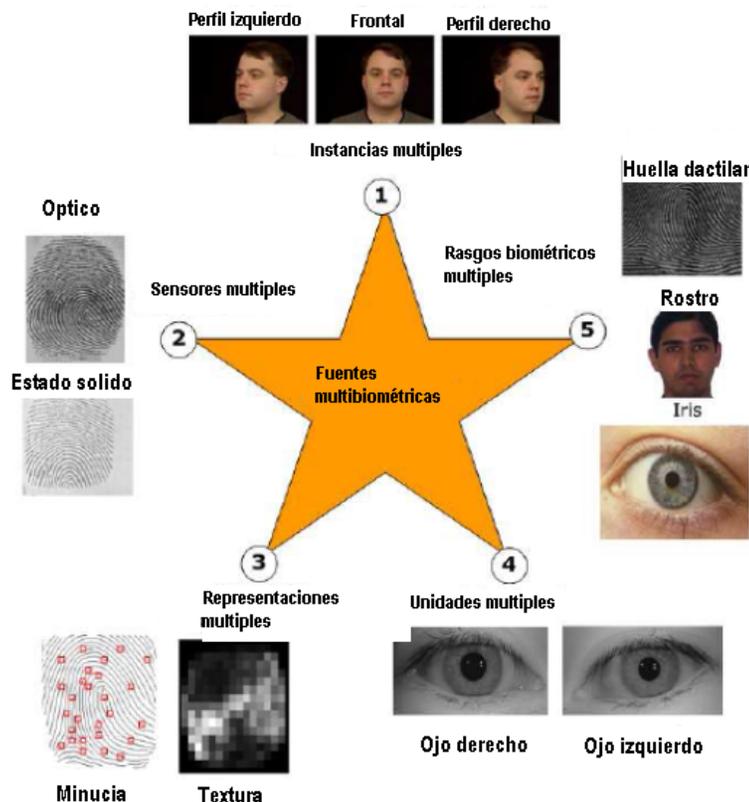


Figura 2.16 Esquemas de fusión

Uno de los trabajos realizados sobre biometría multimodal es la realización de una tesis doctoral titulada “Esquemas adaptados de fusión para autenticación biométrica multimodal”. Esta tesis se centra en la combinación de varios rasgos biométricos para superar algunas de las limitaciones de los rasgos individuales. Los rasgos que toman en cuenta son: firma escrita, voz y huella dactilar. La arquitectura propuesta se muestra en la Figura 2.17 [10].

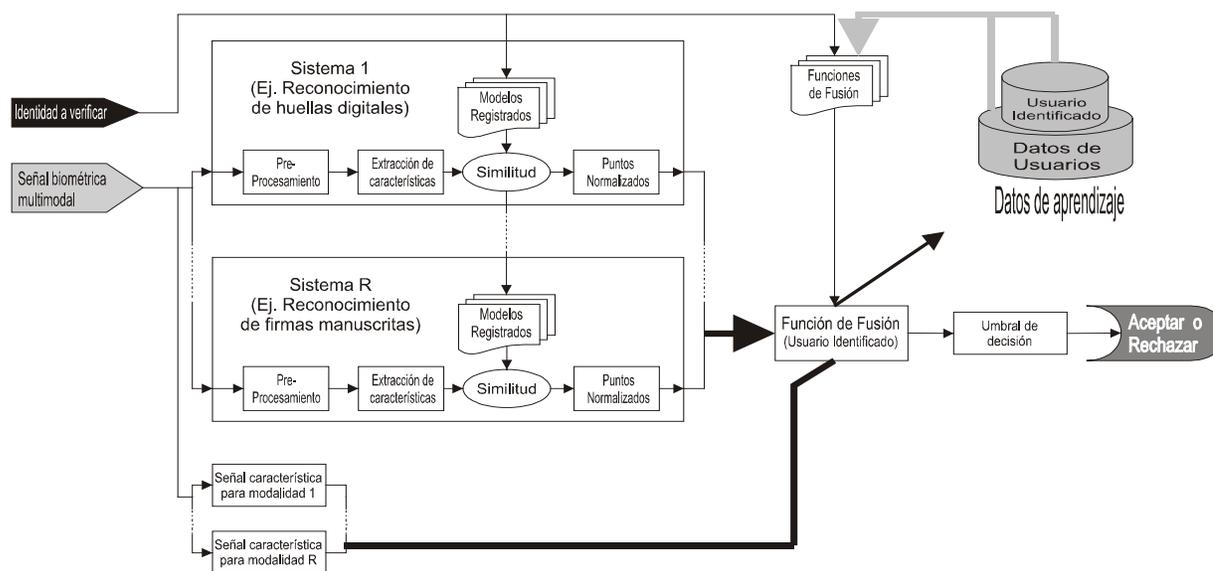


Figura 2.17 Arquitectura propuesta en la tesis doctoral

2.7 Biometría forense

El científico forense debe informar al juez o al jurado acerca de sus conclusiones cuando se utilizan técnicas de análisis biométrico. En este sentido se pone de manifiesto la diferencia entre la caracterización del sistema de reconocimiento biométrico, es decir, las capacidades de identificación de la técnica utilizada, y la caracterización del sistema forense, cuya función será aportar resultados objetivos al tribunal. Los científicos no deben asumir el papel de juez o de jurado en la toma de decisiones, sino sólo deben saber cómo informar al tribunal para cumplir con todas las condiciones de los procesos judiciales, convirtiendo los resultados obtenidos a partir del sistema biométrico en cuestión en datos útiles para el juez y el jurado.

3. Firma manuscrita

La firma manuscrita es el medio más cotidiano para la verificación de la identidad de las personas. Se emplea en la sociedad en todos los niveles, desde la indicación de la autoría de un documento por un individuo en particular, hasta la certificación de la conformidad de una persona en cualquier tipo de transacción, bien sean bancarias, administrativas, o laborales [1].

La firma es la síntesis de la personalidad y se le puede definir como una biografía abreviada. En este sentido, constituye el sello personal que nos representa ante nosotros mismos y ante los demás [5]. Las firmas manuscritas constituyen uno de los principales métodos de justificación de autoría que se manejan para las personas [6].

Estas son ideas generales de diversos autores acerca de la firma, con las cuales se puede concluir que la firma es un rasgo con características que diferencian a las personas entre sí de forma única, por lo que es una de las formas más aceptadas en cuestiones legales para la aceptación de conformidad del firmante con respecto a un documento o a su autoría por dicho firmante. De aquí

que a la firma se le considere como una característica biométrica confiable para la identificación de una persona o para la verificación de su personalidad.

Debido a su carácter legal, también es una de las medidas biométricas más tratadas de falsificar. Por ello es que se han hecho sistemas de autenticación robustos para evitar las falsificaciones extrayendo características de ésta de tal forma que sean únicas para cada persona. Estas características están sujetas a:

- Variaciones intrapersonales (Fig. 3.1), es decir, por regla general una persona no puede realizar idénticamente dos veces su misma firma, con lo que si se encontraran dos firmas idénticas, seguramente se trataría de una falsificación.



Figura 3.1 Ejemplo de variaciones intrapersonales

- Diferencias interpersonales (Fig. 3.2), es decir, las diferencias entre firmas de personas diferentes es suficiente como para considerarla como un rasgo único para cada persona.



Figura 3.2 Ejemplo de diferencias interpersonales

Las variaciones intrapersonales de la firma complican de alguna forma la extracción de sus características para una correcta verificación.

3.1 Definiciones

Firma. Trazo que identifica a una persona; generalmente es un nombre que va acompañado de una rúbrica. Es común que se encuentre al pie de un escrito para atestiguar que se es autor o que el firmante aprueba o respalda su contenido.

Rúbrica. Rasgo o rasgos de una figura que se añade a una firma. Puede estar diseñada por varios cortes de líneas, signos que carecen de algún sentido general, etc. También puede ser definida como una firma corta, o como el rasgo o rasgos de formas determinadas, que como parte de la firma pone cada quien después de su nombre o título, y que a veces va sola, es decir, no precedida del nombre o título de la persona que rubrica.

3.2 Proceso de obtención de la firma manuscrita

El medio de realización de la firma manuscrita es sencillo, ya que solo se requiere un útil de escritura (lápiz, bolígrafo, pluma eléctrica, etc.) y una superficie en donde realizarla.

Se conocen dos formas para la obtención de la muestra de una firma:

- Obtención en línea (*on-line*) (dinámica). La firma se obtiene al momento en el que se está firmando, ya sea por medios electrónicos (tabletas digitales) o por medio de visión (cámaras de video) (Fig. 3.3). De esta forma de obtención de la firma se pueden extraer características tales como: la velocidad, punto de inicio y punto final, presión, entre otras, así como su digitalización.



Figura 3.3 Obtención de firmas en forma dinámica

- Obtención fuera de línea (*off-line*) (estática). La firma es obtenida mediante dispositivos digitalizadores de documentos (escáneres) a partir de un documento en el cual está contenida (Fig. 3.4). Con este medio nada más se cuenta con la imagen digitalizada.



Figura 3.4 Obtención de firmas en forma estática

El modo de captura afectará significativamente al resto de los procesos que realiza el sistema de reconocimiento.

Como se puede observar, la principal diferencia entre los sistemas de captura en línea y fuera de línea es la simultaneidad entre la realización de la firma y la extracción de las características de la misma.

3.3 Acondicionamiento de la señal de la firma

La etapa de acondicionamiento de la señal de la firma tiene básicamente tres objetivos [1]:

- Eliminación de toda la información irrelevante para el reconocimiento.
- Corrección de la información degradada durante la captura.
- Reducción de la variabilidad entre distintas realizaciones de una misma firma.

3.3.1 Acondicionamiento para la firma obtenida fuera de línea (off-line)

Las técnicas que se emplean en el preprocesado de la información son básicamente técnicas de procesamiento digital de la imagen:

- Umbralado.
- Eliminación de ruido.
- Segmentación.
- Normalización en posición y tamaño.
- División en celdas.
- Otras operaciones morfológicas.

3.3.2 Acondicionamiento para la firma obtenida en línea (on-line)

Se busca obtener una representación robusta respecto a las tres variaciones geométricas básicas: rotación, traslación y escalado de las diferentes realizaciones de las firmas. Ejemplos de procesamientos aplicados a la firma en línea son los siguientes:

- Alineamiento respecto a la posición.
- Normalización de la rotación.
- Normalización del tamaño.

3.4 Características de las firmas

Una vez que se ha obtenido y procesado la firma, es necesario seleccionar las características idóneas que faciliten el reconocimiento.

Al seleccionar las características para que representen de forma óptima a la firma, se deben cumplir dos requisitos [1]:

- Ser discriminantes entre firmas verdaderas y las falsificaciones.
- Ser estables ante las variaciones típicas de las firmas verdaderas.

Las características extraídas de la firma se pueden clasificar atendiendo a varios criterios. Dos posibilidades son [1]:

- En función de su naturaleza. Características dinámicas y estáticas.
- En función del ámbito de la representación. Características globales y locales.

3.4.1 Características dinámicas

Toman información temporal del proceso de realización de la firma. Entre otras se pueden mencionar:

- Duraciones totales o parciales (de levantamientos, de trazos).
- Posiciones, velocidades y aceleraciones instantáneas.

- Posiciones, velocidades y aceleraciones máximas, mínimas y medias.
- Posiciones relativas entre levantamientos o contactos con el papel.

Estas características son fáciles de obtener en los métodos de registro en línea, pero muy difíciles de conseguir a partir del análisis estático de las firmas.

3.4.2 Características estáticas

Toman información de tipo geométrico de la firma:

- Aproximaciones de la geometría de la firma mediante polígonos.
- Relación de aspecto (longitud/altura).
- Localizaciones relativas de los inicios y finales de los trazos.
- Concavidad de los trazos.
- Inclinación de los trazos verticales.

Cabe hacer notar que como en la obtención de firmas en línea también se dispone de la imagen digitalizada, entonces las características mencionadas anteriormente también son válidas para éstas. Por lo tanto, con las firmas obtenidas en línea se cuenta con más información que con las obtenidas fuera de línea.

3.4.3 Características globales

Son aquellas que toman información de la firma en su totalidad, considerándola como una unidad inseparable. Entre otras pueden mencionarse las siguientes:

- Duración total.
- Densidad global.
- Relación de aspecto de la firma.
- Medias y desviaciones típicas (sobre cada parámetro extraído).
- Centro geométrico.

3.4.4 Características locales

Son aquellas que toman información de puntos o zonas específicas de la firma, ya sea en el dominio temporal o en el espacial. Entre otras:

- Valores instantáneos de los diferentes parámetros como son: velocidad de escritura, relación de aspecto, duraciones de los trazos, etc.
- Puntos máximos y mínimos (superiores e inferiores).
- Densidades por celdas.
- Medidas locales de orientación de los trazos.
- Cuestiones relacionadas con la rúbrica.

3.5 Representación de las firmas

La fase de extracción de las características de la firma va a influir en la forma final de estructurar el modelo o patrón de la misma.

3.5.1 Representación paramétrica

Las características consisten en un conjunto de parámetros o valores individuales calculados a partir de la información capturada y procesada. Los valores se suelen agrupar en un vector representativo de la firma.

Algunos parámetros típicos son [1]:

- Velocidad de escritura máxima, mínima y media.
- Velocidades de escrituras en los diferentes ejes cartesianos x e y .
- Duraciones globales y locales (total, de contacto bolígrafo – papel, etc.).
- Relación de aspecto.
- Porcentajes de píxeles con una orientación determinada.
- Densidades de probabilidad de píxeles en distintas direcciones.

3.5.2 Representación mediante funciones

La firma puede representarse como una función temporal o espacial que refleja la evolución de ciertos parámetros a lo largo de su realización. Las representaciones temporales solamente se pueden aplicar sobre firmas capturadas en línea y consisten en el muestreo de los parámetros capturados mediante el dispositivo a una cierta frecuencia de muestreo, y la extracción de parámetros adicionales. Algunas funciones temporales son [1]:

- Posición.
- Presión.
- Fuerza y ángulos instantáneos del bolígrafo.
- Velocidades y aceleraciones de los parámetros anteriores.
- Aceleraciones centrípeta y tangencial.
- Curvatura instantánea.

Si la firma se adquiere fuera de línea, la imagen resultante suele dividirse en celdas, filas o columnas, de manera que se extraen los parámetros por separado para cada una de ellas dando lugar a una función o un conjunto de funciones espaciales de la firma. Algunos parámetros son [1]:

- Densidad de píxeles global o por celda.
- Proyecciones de los trazos por celda.
- Medidas locales de orientación.

4. Algunos trabajos sobre identificación de firmas manuscritas

Se han realizado varios trabajos respecto a la identificación y verificación de firmas manuscritas, utilizando y desarrollando varias metodologías o técnicas para la interpretación de las mismas.

En este capítulo se enumeran varios de estos trabajos para comparativamente tener una clara idea de las diversas formas que hay para la identificación y verificación de las firmas manuscritas.

4.1 Visual Identification by Signature Tracking (Identificación visual por seguimiento de la firma)

La firma es capturada por medio de una cámara. En la figura 4.1 se muestra el diagrama de bloques del sistema [11].

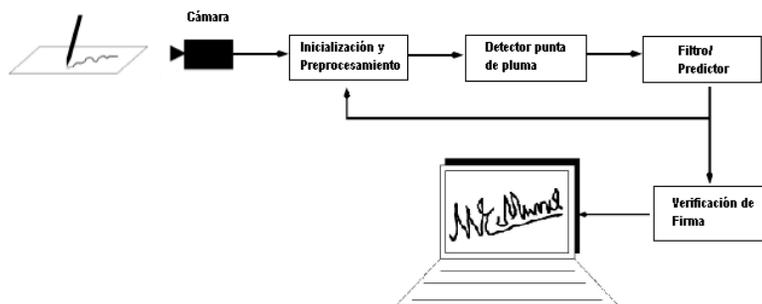


Figura 4.1 Diagrama de bloques del sistema

El sistema fue implementado en tiempo real; las firmas fueron capturadas con una resolución de 480 x 640 píxeles por imagen entrelazada.

Se capturaron dos conjuntos consecutivos de firmas con la cámara de la interfaz, con el fin de evaluar el desempeño de la verificación del sistema.

Para la comparación de la firma se utilizó la técnica DPM (*Dynamic Programming Matching*), la cual es una técnica que busca la correspondencia entre los puntos de las muestras de la firma. Una vez dada esta correspondencia es posible calcular una distancia entre las firmas. La interpretación para la clasificación se basó en tres medidas: la distancia residual entre las formas después de una alineación de la firma, la distancia residual entre funciones de presión y la distancia entre movimientos de la escritura.

La tasa de error del reconocimiento de la firma por este método fue del uno por ciento, valor que indica que el algoritmo es lo bastante aceptable para la clasificación de las firmas.

4.2 Static signature recognition based on left-to-right hidden Markov models (Reconocimiento estático de la firma basado en los modelos de izquierda a derecha ocultos de Markov)

La captura de la firma manuscrita se realiza de manera dinámica mediante una tarjeta digitalizadora Intous A6 de MACOM y el lápiz *Intous Inking Pen* [12]. El lápiz permite firmar igual que un bolígrafo convencional, con lo cual se dispone de una versión en papel de todas las firmas manuscritas digitalizadas que están en la base de datos.

El proceso de escaneo óptico a 600 puntos por pulgada, no interpolados, genera el gráfico estático u *off-line* de las firmas.

Partiendo de la imagen de la firma ya procesada, a través del estudio de la conectividad se analizan las estructuras cerradas (*blobs*) que conforman la imagen de la firma. Un *blob* representa una estructura continua identificable en una imagen la que se establece de un color distintivo al de su fondo y al del resto de la firma; en la Fig. 4.2 se muestra en azul (gris oscuro) las partes o *blobs* que son hijos del fondo de la imagen y en rojo (gris claro) los *blobs* que dependen de estos.

El conjunto de *blobs*, resultado de la conectividad, incluye información de los ejes de inercia, del centro de gravedad, de los puntos del perímetro, etc. de cada *blob*.



Figura 4.2 Ejemplo de firma estática y *blobs* obtenidos

Las cadenas de puntos (x, y) de los perímetros de los *blobs* que conforman la imagen constituyen la información biométrica relevante en este trabajo.

Los modelos utilizados en este trabajo se denominan modelos ocultos de Markov o HMM (*Hidden Markov Models*). Un HMM es por definición un autómata de estados finitos estocástico, a través del cual se representa a una señal estocástica cuyas características estadísticas varían a lo largo del tiempo, mediante una secuencia de estados.

En este trabajo se utiliza como secuencia de muestras para el entrenamiento de los modelos, la cadena de puntos del perímetro (x, y) de los *blobs* que conforman la imagen de la firma.

En este trabajo se obtienen mejores resultados con modelos en los cuales los *blobs* se ordenan de arriba-abajo e izquierda-derecha que con modelos de *blobs* ordenados por tamaño, de mayor a menor.

4.3 Verificación de la firma escrita estática basada en fusión de características locales y globales

El trabajo se ha centrado en la verificación de firmas estáticas u *off-line*, en donde tan sólo se dispone de la imagen de la firma escrita y no se conocen datos dinámicos de la realización de la misma. Se han implementado dos sistemas: uno basado en un análisis global de las imágenes de

firma y medida de distancias; y otro basado en un análisis localizado y Modelos Ocultos de Markov (HMM) [13].

Algunos estudios han demostrado que el funcionamiento de un sistema de verificación a partir de un único rasgo puede mejorarse mediante la fusión unimodal, es decir, mediante la combinación de varios métodos de verificación aplicados a los mismos datos de entrada, por lo que se implementó un tercer sistema fusionando los dos anteriores mediante dos técnicas: Regla de la Suma y clasificación basada en Máquinas de Soporte Vectorial (*Support Vector Machines*, SVM).

Las características elegidas para representar a las firmas son las direcciones de los trazos y de la envolvente, extraídas mediante operadores morfológicos.

Para las direcciones de los trazos se erosiona la imagen procesada con treinta y dos elementos de estructura diferentes (fig. 4.3). Para el caso de la envolvente se realizan cinco dilataciones sucesivas de la imagen con cada uno de seis elementos de estructura (fig. 4.4) diferentes (30 operaciones en total) y se sustrae la imagen obtenida de la dilatación anterior, o la imagen de partida en el caso de la primera dilatación.

Para cada firma se obtiene un vector de parámetros formado por sesenta y dos componentes; para los primeros treinta y dos, éstas son las imágenes obtenidas en cada una de las erosiones; y para los treinta últimos, las imágenes de diferencia entre dilataciones consecutivas para cada elemento de estructura utilizado.

Ambas técnicas han logrado una reducción considerable de los valores de la Tasa o Proporción de Error Igual o EER (*Equal Error Rate*) de los sistemas individuales.

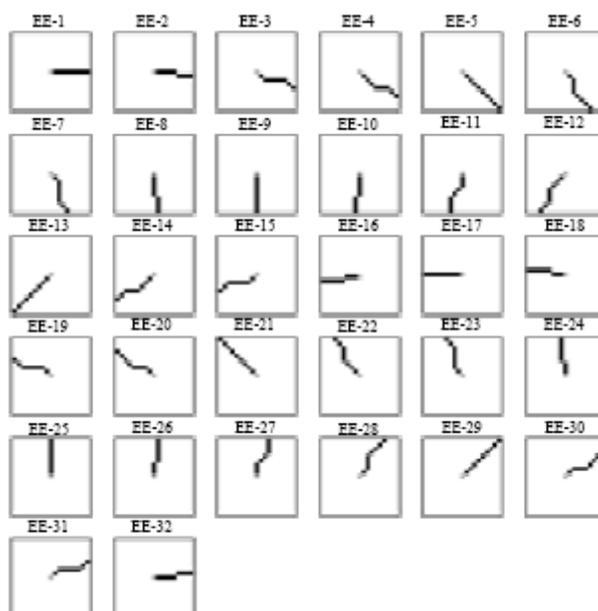


Figura 4.3 Elementos de estructura empleados en el análisis de las direcciones de los trazos

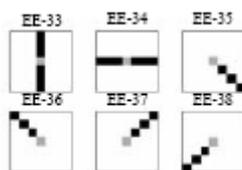


Figura 4.4 Elementos de estructuras empleados en el análisis de las direcciones de la envolvente

4.4 Verificación off-line de firmas manuscritas: una propuesta basada en snakes y clasificadores fuzzy

La base de datos con la que se trabajó fue realizada con cincuenta y seis individuos de los cuales se obtuvieron seis firmas de cada uno. Han sido escaneadas como imágenes binarias a trescientos puntos por pulgada y almacenadas en formato BMP [14].

Se utilizaron en este trabajo algoritmos basados en las culebras (*snakes*), los cuales son un tipo de modelos de contornos activos que se basan en el estudio del movimiento de un contorno abierto o cerrado sobre una imagen a la que trata de adaptarse. Asociado a este contorno se define una función de energía que tiene una componente interna y otra externa.

El problema de verificar una firma consiste en minimizar la energía de ajuste del *snake* asociado a la firma, a comprobar con respecto a la firma original (Fig. 4.5).



Figura 4.5 Ajuste del *snake*

Para el clasificador difuso (*fuzzy*) se utiliza el modelo de Takagi- Sugeno (TS) [15].

Tras iterar cada firma con el *snake*, calcular sus características y compararlas utilizando el modelo TS se obtiene un valor numérico entre 0 y 1. Este valor indica la pertenencia de la firma a la clase de las genuinas o de los falsificadores. Solo queda elegir el valor umbral que defina si el patrón presentado se considera genuino o es una falsificación.

5. Objetivos

Tras los análisis hechos en este reporte, podemos enunciar el objetivo general y los específicos del trabajo de tesis que nos proponemos desarrollar, a saber: **Nivel de compatibilidad de un texto manuscrito con la firma.**

5.1 Objetivo general

Determinar, a partir de un texto manuscrito firmado, el nivel de compatibilidad en relación a la autoría sobre la base de las características previamente extraídas y almacenadas en una base de datos de textos y firmas manuscritos.

5.2 Objetivos específicos

- Diseñar y crear la base de datos compuesta de textos manuscritos y firmas.
- Extraer de forma automática la información de la base de datos a partir del texto escaneado.
- Preprocesar las imágenes de textos manuscritos y firmas.
- Extraer de forma no supervisada las características locales y globales de los textos manuscritos y las firmas ya preprocesadas.
- Clasificar independientemente los textos manuscritos y las firmas sobre la base de las características previamente extraídas.
- Determinar si dados un texto manuscrito y la firma que lo acompaña, ambos proceden del mismo autor.

6. Conclusiones

Actualmente la biometría se ha vuelto una herramienta poderosa para la autenticación de las personas sobre la base del reconocimiento de los rasgos que son únicos en éstas. El hecho de que cada vez son más frecuentes los intentos de falsificación y fraude, al querer una persona de pocos valores morales hacerse pasar por otra persona, hace que los sistemas biométricos sean indispensables para garantizar una cierta seguridad para diversas transacciones monetarias, para la entrada a zonas restringidas, y otras aplicaciones no menos importantes. Debido a que los sistemas biométricos se basan en rasgos intrínsecos y únicos de las personas, entre los que podemos citar, la huella dactilar, la voz, la firma, la escritura manuscrita, etc., hacen de estos sistemas una eficiente y robusta herramienta para la verificación y autenticación de las personas.

La firma manuscrita es uno de los rasgos de mayor aceptación para la identificación de las personas, ya sea de manera legal, como por ejemplo en los cheques de banco, o de forma oficial como en los carnés de identidad y los pasaportes. Se han diseñado sistemas biométricos con el fin de poder decidir confiablemente la autenticidad de las mismas, de los cuales se hace referencia de algunos trabajos realizados en la Sección cuatro.

En los sistemas biométricos se debe tomar en consideración, fundamentalmente en el caso de la firma manuscrita, los cambios que ésta pueda sufrir con el paso del tiempo; para evitar que debido a esto la confiabilidad de estos sistemas disminuya, se requiere una actualización periódica de la base de datos de las personas que la conforman. En este sentido se han creado también los sistemas multibiométricos (o multimodales) que fusionan dos o más características biométricas del mismo individuo.

Referencias

- [1] Tapiador Mateos, Marino., Sigüenza Pizarro, Juan A., et. al. *Tecnologías biométricas aplicadas a la seguridad*. 1ª Edición. Alfaomega Grupo Editor. México. D. F., ISBN 970-15-1128-X, 2005.
- [2] Association for Biometrics and International Computer Security Association. *Glossary of Biometrics Terms*, 1999.
- [3] Lonkaric, S. and Dhawan A. P., Near optimal MST – based shape description using genetic algorithm. *Patt. Recog.*, vol. 28, 1995.
- [4] Wayman James L., A generalized biometric identification System model. *Proc. IEEE Asimolar Conference on signals, and computers*, 1997.
- [5] Tesouro de Grosso, Susana, *Grafología: análisis e interpretación científica de la escritura*, 1ª Edición. Editorial Kier. Buenos Aires, Argentina. ISBN 950-17-7011-7, 2006.
- [6] B. Fang., Off-line signature verification with generated training samples. *IEEE Proc. – Vis. Image and Signal Processing*, Vol. 149, no. 2, 2002.
- [7] *Diccionario de la Real Academia Española*. 22ª Edición, 2001.
- [8] H. C. Lee, R. E. Gaensslen, et al., *Advances in Fingerprint Technology*. Elsevier, Nueva York (EE. UU.). 1991. CRC Press LLC. EE. UU, 1994.
- [9] Jacobo Aragunde Pérez, José Carlos Toucedo Alonso, et al. Reconocimiento de Personas, Visión artificial. Tema 7 – 2006/07.
<http://varpa.lfcia.org/Docencia/VAFiles/Curso0607/tema7.pdf>
- [10] Julián Fierrez Aguilar. Esquemas Adaptados de Fusión para Autenticación Biométrica Multimodal. Tesis Doctoral. ATVS Grupo de Reconocimiento Biométrico – Escuela Politécnica Superior, Universidad Autónoma de Madrid, 2006.
- [11] Mario E. Munich, Pietro Perona, Visual Identification by Signature Tracking. *IEEE Transaction on Pattern Analysis and Machine Intelligence*, vol. 25, No. 2, February 2003.
- [12] Juan J. Igarza, Inmaculada Hernández, Iñiqui Goirizelaia. Static signature reconignion based on left-to-right hidden Markov models. *Journal of Electronic Imaging* 14 (4), 043015, Oct-Dec 2005.
- [13] G. Moreno Márquez, N. Alonso Hermira, et al., Verificación de firma escrita estática basada en fusión de características locales y globales. Laboratorio de Identificación Biométrica, Área de tratamiento de Voz y Señales EUIT de Telecomunicación, Universidad Politécnica de Madrid, 2005.
- [14] José F. Vélez, Ángel Sánchez, et al., Verificación Off-Line de Firmas Manuscritas: una Propuesta basada en Snakes y clasificadores Fuzzy, 2006
- [15] A. Abreu, L. Custodio and C. Pinto. Fuzzy Modeling: a Rule Based Approach. Fifth IEEE International Conference on Fuzzy Systems (FUZZ – IEEE 96), 1996.