UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

PROYECTO FIN DE CARRERA

RECONOCIMIENTO OFF-LINE DE ESCRITURA BASADO EN FUSIÓN DE CARACTERÍSTICAS LOCALES Y GLOBALES

Almudena Gilpérez de la Hera

Septiembre 2010

Reconocimiento off-line de escritura basado en fusión de características locales y globales

AUTOR: Almudena Gilpérez de la Hera

TUTOR: Fernando Alonso Fernández

ATVS Grupo de Reconocimiento Biométrico
(https://atvs.uam.es)
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid

Resumen

En este proyecto se estudian, desarrollan y evalúan distintos sistemas automáticos de identificación de escritor.
Además, se comparan los resultados obtenidos de estos sistemas implementados en el marco de este proyecto fin de carrera y otros sistemas disponibles en el grupo de reconocimiento biométrico ATVS.

Estos sistemas se emplean para el reconocimiento biométrico de personas en el ámbito forense. Por ello, su evaluación se realiza a partir de un conjunto de muestras reales. Es decir, se realiza identificación forense mediante análisis grafístico.
El reconocimiento es realizado a partir de imágenes de caracteres escaneados, esto es, reconocimiento *off-line* de escritura. Además, se busca reconocer al individuo que escribió el texto, sin darle importancia al contenido del mismo. Es decir, la identificación es independiente del contenido del texto.
Por otro lado, en este proyecto se extraen dos tipos de características de las muestras: características locales, las cuales dividen las imágenes de las firmas en regiones y se calcula un vector de características por región; y características globales que son aquellas que obtienen el vector de características a partir de la imagen completa de la muestra de escritura.

Se implementan tres sistemas diferentes en el marco de este proyecto. El primero de ellos, se basa en la extracción de una característica estructural (característica local) para cada muestra. El segundo utiliza para la tarea de reconocimiento un conjunto de características de concavidad (característica local) y, el último sistema está basado en características geométricas (característica global) de la muestra.
Por otro lado, se presentan y evalúan los sistemas disponibles en el grupo: un sistema basado en características de gradiente, un sistema basado en alógrafos y un sistema basado en características de contorno.
Inicialmente, todo ellos devolvían un vector de características para cada muestra. Por ello, como mejora, se propone una normalización a función de densidad de probabilidad en los casos en los que puede ser posible.

Con los resultados obtenidos, comprobamos qué característica proporciona mejor rendimiento. Además, se analiza una fusión de las características y se observa que rendimiento se obtiene.
Tras ello, se presentan las conclusiones y se proponen líneas de trabajo futuras.

Finalmente, como anexo se presenta la descripción de una competición, basada en verificación de firma *off-line*, en la que se participó con parte de los sistemas disponibles en el grupo ATVS y los desarrollados en este proyecto.

Palabras clave: Biometría, Identificación de escritor independiente de texto, Vector de características, Función de densidad de probabilidad.

Abstract

In this project we study, develop and evaluate various automatic writer identification systems. In addition, we compare the results obtained with the systems implemented in this project and other systems available at the ATVS, Biometric Recognition Group.

These systems are used for biometric recognition of people in the forensic field. Therefore, this evaluation was made from a set of real samples. That is, forensic identification is done by graphic analysis.
Recognition is made from scanned images of characters, i.e. *off-line* handwriting recognition.
In addition, it seeks to recognize the individual who wrote the text without giving importance to content. That is, we perform text independent identification.

Three different systems are implemented within the framework of this project. The first of them is based on the development of a structural features for each sample. The second is the implementation of a concavity feature set and the last system is based on geometric features of the sample.
Initially, each of these systems returns an array of features for each sample. As an improvement, we propose a normalization to a probability density function in cases where it is possible.
On the other hand, the already available systems, with which we will compare the ones developed here, are: a system based on gradient features, a system based on allographs and a system based on boundary features.

With these results, we see what feature provides better performance. Similarly, we get to see how it affects the size of the Top N candidates for a proper system performance.
We also analyze a fusion of the implemented features and analyze that performance too.
After that, we present the conclusions and propose future research.

Finally, as an attachment, we present the description of a competition on off-line signature verification in which we participated with part of the available systems and systems developed in this project.

Key Words: Biometrics, text independent writer identification, vector of features, probability density function.

Gracias…

En primer lugar, quiero dar las gracias a mi ponente Javier Ortega por haber confiado en mí, por haberme dado la oportunidad de trabajar en el grupo de investigación ATVS y por seguir dándome oportunidades a día de hoy.

A mis compañeros del ATVS, gracias por estar a mi lado cada mañana y cada tarde.
A Fer, por escucharme, por darme sustos, por hacerme reír…pero sobretodo, por ser mi tutor y ayudarme con el proyecto.
A Julián, por ser capaz de contestarme a esas preguntas que siempre me había parecido que no tenían respuesta.
A María, gracias por ser mi compañera y mi amiga; por reírte con mis chistes, por tus ánimos y por entenderme a pesar de que a veces es muy difícil.
A Ali y Vir, por ser las mejores *babies* del mundo!
Y a todos los demás, mil gracias porque a vuestro lado todo me ha parecido muy fuerte.

A mis amigos de teleco, gracias porque cada vez que me acuerdo de cada uno de vosotros, sonrío al recordar todos esos ratos juntos! GRACIAS!
A Sarita!...gracias por los bancos de la biblioteca, por las tardes de compras, por las llamadas de teléfono, por las historias para no dormir…me ha encantado conocerte!

A Sara, Irene, Elena y Mawi, gracias porque fuisteis, sois y siempre seréis mis niñas. Gracias por las noches en el parque, por las quinielas, por los álbumes de fotos, por las fiestas sin fin...gracias por enseñarme tantas y tantas cosas.
A Sonia, por mostrarme que hacerse mayor puede hacerte regalos maravillosos que te hacen feliz!

A Javi, Micky y Adri, gracias por esos veranos!!!! Sois los mejores!!!!

A Jimena, por llamarme todas las noches durante estos dos años, por los paseos por el barrio, por las cenas en el VIPS, por todos esos viajes. Gracias por saber darme consejos para todo!...alucina vecina!

A mis tíos y primos, gracias porque todas las horas que habéis pasado conmigo han estado llenas de grandísimas anécdotas. A mi abuelo, gracias por cenar a mi lado todas las noches y por reírte conmigo cuando no te apetecía hacerlo.

A mi hermano, por hacerme la comida días y días, por darme la mano cuando me resbalaba por el hielo, por perdonarme lo imperdonable…por contagiarme la risa!

Y como no…a mis padres. Evidentemente, sin vosotros esto no hubiera sido posible!
Millones de gracias por aguantarme tantos malos ratos durante estos años. Gracias por estar SIEMPRE conmigo y por saber cómo me siento en cada momento.
Pero sobretodo, gracias por hacerme la vida más fácil y por demostrarme que mis alegrías también son vuestras alegrías.

Índice de Contenidos

Índice de Figuras

Capítulo 1

INTRODUCCIÓN

La ciencia forense se basa en una hipótesis central: dos marcas indistinguibles deben haber sido producidas por un único objeto o individuo [1].

Tradicionalmente, científicos forenses buscan pruebas para vincular la escena del crimen a una sola persona o un objeto "con exclusión de todos los demás en el mundo". Y lo hacen apoyándose en la hipótesis de la singularidad perceptible, siendo visiblemente diferentes dos marcas producidas por diferentes personas u objetos. Por tanto, los criminalistas pueden concluir si dos marcas fueron hechas, o no, por la misma persona u objeto.

Fuerzas legales y científicos están presionando a las ciencias forenses tradicionales de identificación para que se produzca un cambio fundamental en su paradigma. El motivo por el cual se pretende este cambio es debido a la evidencia de errores en casos reales. Así, los cambios en la legislación, relativos a la admisibilidad de una prueba pericial, junto con la aparición del ADN como un modelo que responde a preguntas de reconocimiento, están impulsando a las ciencias forenses mayores hacia un nuevo paradigma científico.

Por ello, el análisis biométrico de estas muestras cada vez cobra más fuerza, ya que con éste se busca reducir al mínimo la intervención humana en el proceso de identificación del individuo u objeto. El objetivo, en este caso, sería desarrollar herramientas de identificación automáticas que puedan ser un apoyo para evaluar el peso de la evidencia forense.

Los motivos por los cuales el reconocimiento biométrico puede ser una gran ayuda para realizar las evaluaciones forenses se basa en las propiedades ideales de los rasgos biométricos: universalidad (toda persona debe poseer dicho rasgo), unicidad (personas distintas posean rasgos diferenciados y distintos), permanencia (invariante en el tiempo a corto plazo), perennidad (invariante en el tiempo a largo plazo) y mensurabilidad (puede ser caracterizado cuantitativamente de la forma menos molesta e invasiva posible para el usuario).

En este trabajo, nos centramos en el caso del reconocimiento biométrico de personas a partir de su escritura. Este rasgo biométrico cumple la mayoría de las características anteriormente expuestas y, además, suscita un alto interés en la comunidad científica debido a su aceptación social y legal.

En este capítulo, se presenta la motivación que lleva al desarrollo de este proyecto. Además, se detallan los objetivos que se persiguen. Por último, se detalla el contenido de las distintas partes de este proyecto.

1.1 Motivación y Objetivos

Este trabajo aborda el problema de la identificación automática de personas basado en imágenes escaneadas de la escritura. [2]
Se presenta una serie de nuevos y eficaces métodos estadísticos de reconocimiento de patrones para la identificación automática de escritor; y además, se compara el rendimiento de estos sistemas con otros sistemas disponibles por el Grupo de Investigación ATVS.
Nuestros métodos son evaluados experimentalmente utilizando un conjunto de muestras de textos manuscritos escaneados.

Nuestro enfoque muestra dos características relevantes: la intervención humana se reduce al mínimo en el proceso de identificación escritor y la codificación del estilo de escritura individual se realiza a partir de características diseñadas para ser independientes del contenido textual de la muestra manuscrita.

El desarrollo de nuestras técnicas de identificación escritor tiene lugar en un momento en que muchas modalidades biométricas están experimentando una transición que parte de la investigación y llega a su despliegue real a gran escala, es decir, nuestros métodos tienen viabilidad práctica y prometen aplicabilidad concreta.

1.2 Organización de la memoria

Esta memoria consta de los siguientes capítulos:

Capítulo 1. Introducción

En el primer capítulo, se presenta la motivación que nos ha llevado a la realización de este proyecto y los objetivos que se han perseguido durante el desarrollo del mismo. Además, se presenta una introducción del tema a tratar en este trabajo.

Capítulo 2. Estado del arte

Este capítulo empieza con una introducción a la biometría donde se presentan los rasgos biométricos y sus propiedades. A continuación, se expone un apartado sobre sistemas biométricos, sus modos de operación y el rendimiento de los sistemas automáticos de reconocimiento. Finalmente, se presenta un apartado que se centra en la identificación de personas a partir de la escritura. En éste, se presenta una serie de características que tiene nuestro sistema así como los trabajos previos y los algoritmos existentes para el reconocimiento de escritor.

Capítulo 3. Sistemas de reconocimiento de escritor

En el capítulo3, se presentarán los sistemas utilizados en el presente proyecto para el reconocimiento de escritor.
Se exponen tres sistemas desarrollados en el marco de este PFC y otros tres sistemas disponibles por el ATVS y que también han sido evaluados en este proyecto.

Capítulo 4. Experimentos en identificación de escritor

Este capítulo describe la base de datos utilizada para la realización de este proyecto así como el protocolo experimental y los resultados obtenidos.
Se presentan las tasas de identificación obtenidas tanto el TOP1 como en TOPN.

Capítulo 5. Conclusiones y trabajo futuro.

Capítulo 2

INTRODUCCIÓN A LA BIOMETRÍA

2.1 Biometría

El término “Biometría” proviene del griego “bio” (vida) y “metron” (medida) y se refiere a todas aquellas técnicas que permiten identificar y autenticar a las personas a través de sus características fisiológicas o de comportamiento.
Actualmente, el término "Biometría" es utilizado para referirse al campo de tecnología dedicado a la identificación de individuos a partir de sus rasgos biométricos, por ejemplo las huellas dactilares, el iris, la escritura o la geometría de la mano entre otros [3].

Los rasgos biométricos se pueden clasificar en **rasgos biométricos fisiológicos** y **rasgos biométricos de comportamiento o conducta**.
Entre los rasgos biométricos fisiológicos se encuentran el iris, la huella dactilar, la geometría de la mano, la retina y el ADN. Su principal característica es su reducida variabilidad a lo largo del tiempo, pero su adquisición es más invasiva y requiere la cooperación de los sujetos.
Por el contrario, los rasgos biométricos de comportamiento o conducta, como son la voz, la firma o la escritura, son menos invasivos aunque la exactitud de la identificación es menor debido a la variabilidad de los patrones de comportamiento. Asimismo, no se encuentran siempre presentes, sino que es preciso que el individuo lleve a cabo una realización de los mismos, como firmar o hablar.

Todos los rasgos biométricos tienen como ventaja que no pueden ser sustraídos, perdidos, olvidados o descolocados; representando, por tanto, una manifestación tangible de lo que la persona es. Por tanto, mediante el uso del reconocimiento biométrico, es posible establecer la identidad de una persona mediante “algo que se es”, a diferencia de los tradicionales sistemas basados en algo que se posee (como un DNI, una tarjeta de identificación o una llave), que puede perderse o robarse, o en “algo que se sabe”(como una clave), que puede ser olvidado

2.1.1 Características de los rasgos biométricos

Un rasgo personal será válido y un sistema biométrico será capaz de distinguir a las personas a partir de él si cumple las siguientes propiedades [4]:

- **Universalidad:** toda persona debe poseer dicho rasgo biométrico.
- **Unicidad:** personas distintas deben poseer rasgos distintos, lo suficientemente diferentes como para permitir distinguirlas a partir de ese rasgo.
- **Permanencia**: el rasgo debe ser lo suficientemente invariante con el tiempo.
- **Mensurabilidad:** el rasgo debe poder ser caracterizado cuantitativamente.

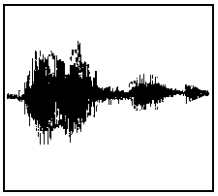
Desde el punto de vista práctico de un sistema basado en reconocimiento a partir de rasgos biométricos, hay otro conjunto de propiedades que deben satisfacerse:

- **Rendimiento**: hace referencia al error cometido en el reconocimiento de individuos, a la velocidad y recursos necesarios para llevarlo a cabo, así como a los factores externos que afecten a las capacidades de reconocimiento del sistema.
- **Aceptabilidad**: los usuarios deben estar dispuestos a emplear ese rasgo en las actividades de su vida cotidiana.
- **Fraude**: los sistemas que usen ese rasgo deben ser suficientemente seguros de forma que resulte difícil atacarlos.

Dependiendo de las características y necesidades del sistema biométrico se debe comprobar que el rasgo elegido cumple la funcionalidad requerida por el sistema. En resumen, un sistema práctico que haga uso del reconocimiento biométrico debe cumplir con los requisitos de precisión, velocidad y utilización de recursos, debe ser aceptado por la población a la que se dirige y debe ser lo suficiente robusto a los intentos de fraude y ataques a los que pueda ser sometido. Cada rasgo biométrico tiene sus ventajas y sus inconvenientes, y no hay ningún rasgo que cumpla con alguna de las propiedades anteriores al 100% o que cumpla con todas a la vez de forma satisfactoria, por lo que ninguno de ellos puede cubrir de forma efectiva las necesidades de todas las aplicaciones y siempre será necesario algún tipo de compromiso.

2.1.2 Ejemplo de rasgos biométricos

A continuación, se presentará una lista de los rasgos biométricos más comunes, sin entrar en un nivel de detalle profundo, pero a la vez destacando sus características más relevantes, así como sus ventajas e inconvenientes [3].



Voz: la voz es una combinación de características físicas y de conducta. Las características físicas del habla de cada individuo permanecen invariantes, pero las características de conducta cambian a lo largo del tiempo y se ven influenciadas por la edad, las afecciones médicas o el estado de ánimo de la persona. Las principales desventajas de este rasgo son su baja distintividad y la facilidad con la que puede ser imitado. Por el contrario, la voz es un rasgo biométrico muy aceptado y fácil de obtener.

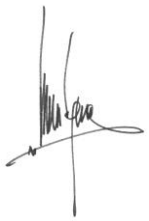
Iris: la estructura del iris de cada ojo muestra un alto grado de unicidad y estabilidad con el tiempo. El patrón se mantiene prácticamente invariante desde la infancia del individuo y la herencia genética sólo determina su estructura y su pigmentación, pero no con gran detalle. Por tanto, es un rasgo altamente distintivo de cada individuo. El mayor problema reside en su adquisición ya que se necesita un alto nivel de detalle pero el sistema no debe ser invasivo como para provocar rechazo por el usuario.

Huella dactilar: una huella consiste en un conjunto de valles y crestas que son capturados al presionar el dedo contra un sensor. Las huellas dactilares son rasgos biométricos perennes, es decir, invariables hasta la descomposición *post-mortem* (excepto por accidentes) y con alta capacidad regenerativa. Además, muestran un alto grado de individualidad ya que son figuras de tal variedad que resultan totalmente características de cada individuo.

Geometría de la mano: a partir de este rasgo biométrico, se mide la forma de la mano, el tamaño de la palma, el grosor y la longitud de los dedos, etc. Es un rasgo con un bajo nivel de distintividad puesto que la mano está expuesta a cambios y agentes externos que modifican su geometría. Por otro lado, su adquisición se realiza a partir de un sencillo scanner y es útil cuando se dispone de poco espacio de almacenamiento de datos.

Forma de andar: rasgo biométrico de comportamiento o conducta que varía a lo largo del tiempo. Su adquisición no es invasiva para el individuo y para su captura únicamente se necesita una cámara de vídeo. Tiene una alta variabilidad a lo largo del tiempo, tanto en el corto como en el largo plazo.

Cara: la cara es el rasgo biométrico más utilizado y aceptado ya que es el utilizado por los humanos para reconocernos de manera natural junto con la voz. Su mayor problema es que no es permanente ya que sufre grandes cambios a lo largo de la vida del individuo. En contrapartida, su adquisición es no intrusiva ya que basta con tomar una imagen del rostro de la persona.



Firma: a lo largo de la historia, la firma ha sido el medio de reconocimiento más aceptado en transacciones de todo tipo (legales, comerciales, etc.). La captura de este rasgo requiere contacto con una superficie y cooperación del usuario. Asimismo, la firma de cada individuo varía significativamente dependiendo de su estado físico, emocional o del paso del tiempo.

Escritura: sistema de representación gráfica de una lengua, por medio de signos grabados o dibujados sobre un soporte plano. Este rasgo biométrico requiere las mismas características de captura que la firma. En cambio, la escritura no varía tanto dependiendo del estado de la persona pero sí que lo hace con el paso del tiempo.

2.2 Sistemas biométricos

Un sistema biométrico se basa en reconocer patrones de rasgos biométricos de forma automática. Su modo de operación se puede dividir en cuatro pasos:

1. Captura del rasgo biométrico mediante un sensor apropiado
2. Extracción de un conjunto de características discriminativas del rasgo
3. Comparación entre patrones almacenados en una base de datos y el patrón anteriormente extraído
4. Decisión de si los datos de entrada pertenecen a un individuo determinado o a un impostor.

Estas cuatro etapas en las que se divide un sistema biométrico se consiguen a partir de la ejecución del esquema de la Figura 1. En general, el usuario sólo tiene acceso al sensor, el cual captura el rasgo biométrico.

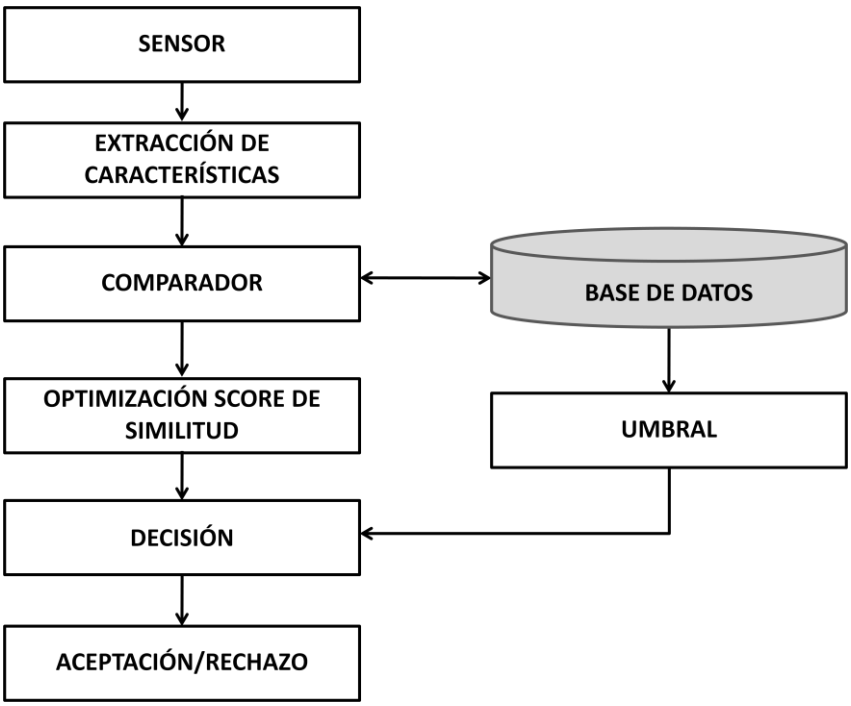


Figura 1. Estructura general de un sistema biométrico

En un primer momento, se deben recoger los datos analógicos a través de un **sensor** y convertirlos a un formato digital. Este proceso es determinante ya que de él depende la cantidad y calidad de la información adquirida, el desarrollo de las siguientes fases y el resultado que se obtiene. En algunos casos es necesario acondicionar la información capturada mediante un preprocesado para eliminar posibles ruidos o distorsiones producidas en la adquisición, o para normalizar la información a unos rangos específicos para tener una mayor efectividad en el reconocimiento posterior.

A continuación, se extraen las **características del rasgo biométrico** en formato digital. En este caso, se elimina la información que no resulte relevante para el proceso de reconocimiento y se adquieren únicamente las características que sean discriminantes entre individuos y que, al mismo tiempo, permanezcan invariantes para un mismo usuario.

Tras la adquisición de las características más significativas, se elabora un modelo representativo de cada usuario. Éste permite la **evaluación de la similitud entre los patrones de entrada y el modelo de un individuo que se encuentre en la base de datos**.
Esta evaluación se realiza teniendo en cuenta un **umbral** que se genera con los datos que tenemos en la base de datos. La comparación entre los datos de entrada y un modelo de identidad extraído de la base de datos está regulada por el umbral. Si la comparación supera cierto umbral de similitud, se considera que los datos de entrada y el modelo corresponden al mismo individuo y en caso contrario, no.

En la **base de datos** del sistema es donde se almacenan los modelos que representan la identidad de cada usuario autorizado del sistema. Dependiendo del tipo de aplicación, los datos usados para generar el modelo de un usuario pueden capturarse bajo supervisión de un operador o no. De la misma manera, la base de datos puede estar almacenada en un lugar único centralizado o cada usuario puede llevar una tarjeta inteligente que almacene únicamente el modelo de su identidad. Asimismo, es usual que con el paso del tiempo, los modelos de cada usuario se actualicen para tomar en consideración posibles variaciones del rasgo biométrico en cuestión.

2.2.1 Modos de operación de un sistema biométrico

Desde el punto de vista del funcionamiento de los sistemas automáticos de reconocimiento de personas mediante rasgos biométricos, se hace necesario clasificar dos perspectivas fundamentales de trabajo de los mismos:

- Sistemas de reconocimiento en **modo verificación**
- Sistemas de reconocimiento en **modo identificación**

Además, para generar la base de datos con los que se compararán los datos de entrada, el sistema de reconocimiento funciona en **modo registro o "enrolment"**. Esto es, los usuarios son dados de alta en el sistema y, para ello, se realiza la adquisición de sus rasgos biométricos, se extraen sus características y se genera un modelo o patrón representativo del individuo. Este modelo queda almacenado en la base de datos de usuarios del sistema. No se realiza por tanto comparación alguna en este modo de trabajo. El esquema de este funcionamiento se puede observar en la Figura 2.

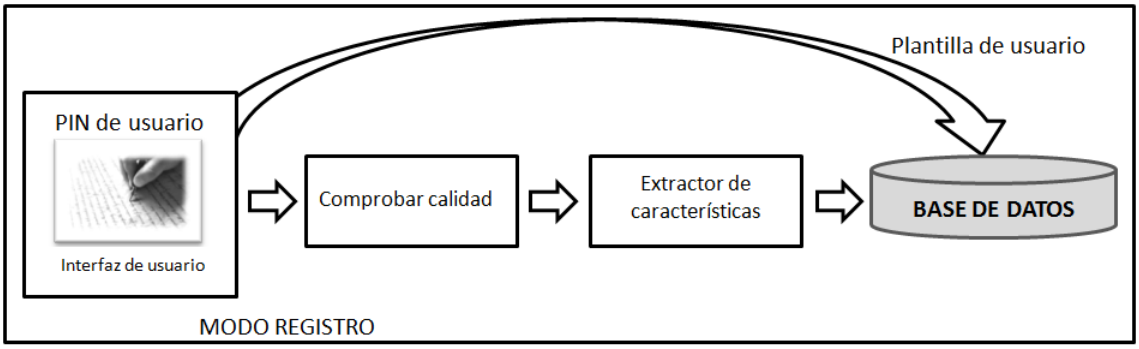


Figura 2. Esquema de funcionamiento en modo registro

Modo Verificación

En el modo verificación, el sistema valida la identidad de una persona comparando el rasgo biométrico, capturado en la entrada, con su propia plantilla biométrica previamente almacenada en la base de datos.

En este caso, el sistema toma dos entradas:

- una realización del rasgo biométrico a verificar
- una solicitud de identidad que puede ser realizada de diversas formas (lectura de una tarjeta magnética individual, introducción mediante teclado o mediante voz de un código locutor, etc.)

El sistema funcionando en este modo pretende responder a la pregunta "¿es esta persona quien dice ser?". De esta manera, las dos únicas salidas o decisiones del sistema son la de aceptación o rechazo del individuo como aquél que pretende ser. Así, el individuo solicitante será catalogado como usuario auténtico o como impostor, respectivamente.

La decisión de aceptar o rechazar al individuo de entrada como correspondiente a la identidad solicitada dependerá de si el valor de parecido o probabilidad obtenida supera o no un determinado umbral de decisión.

El esquema de un sistema de reconocimiento en **modo verificación** se puede observar en la Figura 3.

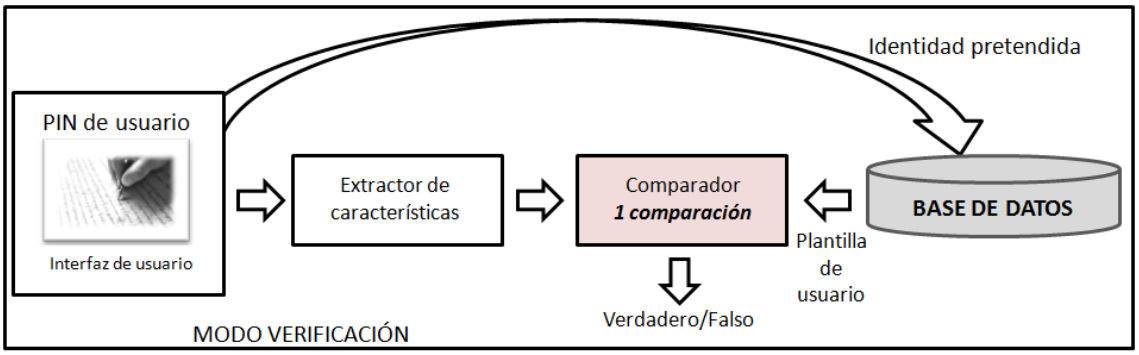


Figura 3. Esquema de funcionamiento de un sistema en modo verificación.

Modo Identificación

En el modo identificación, el sistema tiene como objetivo clasificar una realización determinada de un rasgo biométrico de una identidad desconocida como perteneciente a uno de entre un conjunto de N posibles individuos. En este caso, el sistema pretende responder a la pregunta "¿quién es esta persona?". Como resultado, devolverá el patrón de la base de datos que más se parece a los datos de entrada o una indicación de que el individuo no se encuentra en la base de datos si el parecido no es suficiente. En este caso, el usuario no introduce una identificación pretendida, sino que es el sistema el que determina su identidad de entre todas las almacenadas en la base de datos.
El esquema de un sistema de reconocimiento en **modo identificación** se puede observar en la Figura 4.

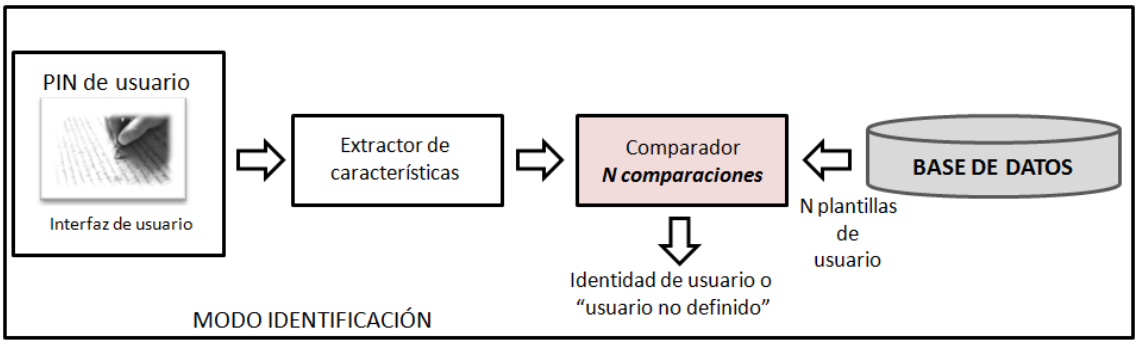


Figura 4. Esquema de funcionamiento de un sistema en modo identificación.

El funcionamiento en modo identificación se utiliza también para realizar "reconocimiento negativo", donde el sistema ha de establecer si una persona es quien (implícita o explícitamente) niega ser. El propósito del reconocimiento negativo es evitar que un único individuo utilice varias identidades. El modo identificación también puede utilizarse en reconocimiento positivo para comodidad del usuario (no se le pide al usuario que solicite ninguna identidad pretendida). Ejemplos de aplicaciones que funcionan en modo identificación son el control de fronteras, la investigación criminal sobre grandes bases de datos, identificación de personas perdidas, etc. Mientras que el reconocimiento positivo puede realizarse también con los métodos tradicionales (llaves, números PIN, etc.), el reconocimiento negativo solamente puede llevarse a cabo mediante el reconocimiento biométrico.

2.2.2 Rendimiento de los sistemas automáticos de reconocimiento

Dos muestras de un mismo rasgo biométrico no son exactamente iguales debido a imperfecciones en las condiciones en las que se captura la imagen, cambios en los rasgos fisiológicos o de comportamiento del usuario, factores ambientales y a la interacción del usuario con el sensor entre otros. Por esto, la respuesta del comparador de un sistema biométrico consiste en una puntuación o *score* que cuantifica la similitud entre la entrada y el patrón de la base de datos con el que se está comparando. Cuanto mayor sea el parecido 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: con los pares de muestras que se obtengan puntuaciones mayores o iguales que el umbral se supondrán correspondientes a la misma persona mientras que con los pares de muestras cuya puntuación sea menor que el umbral se considerarán de personas diferentes.

Ahora, analizaremos formas de evaluación del rendimiento de los sistemas biométricos dependiendo de su modo de funcionamiento.

Criterios de evaluación de sistemas de verificación:

- **Representación mediante curvas FAR y FRR.**
  Las dos posibles salidas en un sistema de verificación dan lugar a la aparición de dos errores distintos:

  - **Falso Rechazo**: se produce si el sistema de verificación devuelve como salida que el usuario en la entrada no se corresponde con la plantilla almacenada, y realmente sí es la misma persona.
  - **Falsa Aceptación**: es complementario al falso rechazo y se produce cuando el sistema indica que la información adquirida del usuario en la entrada sí se corresponde con la plantilla almacenada, cuando realmente se trata de otra persona.

  En un sistema ideal, los rangos de variación de las puntuaciones obtenidas para usuarios impostores y auténticos están separados, de manera que no hay solapamiento entre sus distribuciones, pudiéndose establecer un umbral de decisión que discrimine perfectamente ambas clases. Sin embargo, en un sistema real existe una región en la que se solapan ambas distribuciones, como se muestra en la Figura 5. Como consecuencia, el área bajo la curva de impostores que queda por encima del umbral es la probabilidad de que un impostor sea aceptado y se conoce como la tasa de falsa aceptación (FAR). De igual modo, el área bajo la curva de usuarios válidos que queda por debajo del umbral es la probabilidad de que un usuario registrado no sea aceptado por el sistema y se denomina tasa de falso rechazo (FRR). Según se sitúe el umbral, la FAR y la FRR varían. Si el umbral es bajo, el sistema dará como válido a impostores (aumentará la falsa aceptación) y si el umbral es alto, se rechazarán usuarios validos (aumentará el falso rechazo).

Así, para cada valor que se fije del umbral, se obtiene simultáneamente un valor de FAR y otro de FRR que, como podemos observar, tienen tendencias opuestas según varíe el umbral.

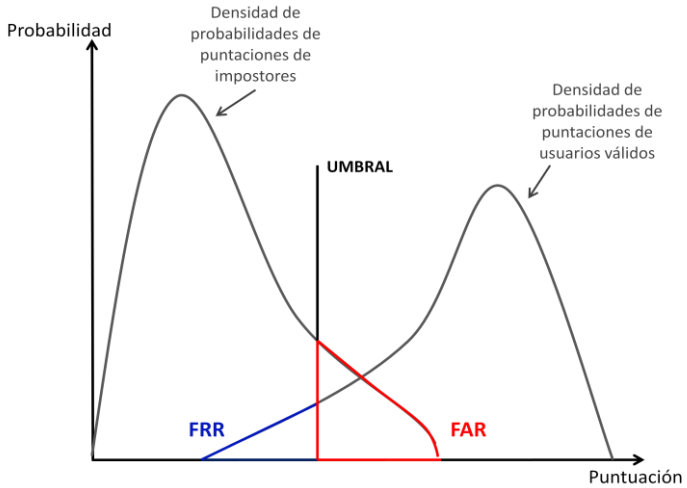


Figura 5. Densidad de probabilidades de usuarios e impostores para todos los posibles umbrales.

- **Tasa de Igual Error: EER** (Equal Error Rate)**.**

  Como medida conjunta de los dos tipos de error anteriormente presentados (FAR y FRR), los sistemas se suelen caracterizar mediante la EER (Equal Error Rate). Esto es, el punto en el que la FAR y la FRR son iguales. Es fácil deducir de las Figuras 5 y 6 que cuanto menor sea el EER, menor es el solape entre las curvas de usuario e impostor.
  Por tanto, como medida comparativa entre varios sistemas, cuanto menor sea el valor de EER, mejor es el sistema.

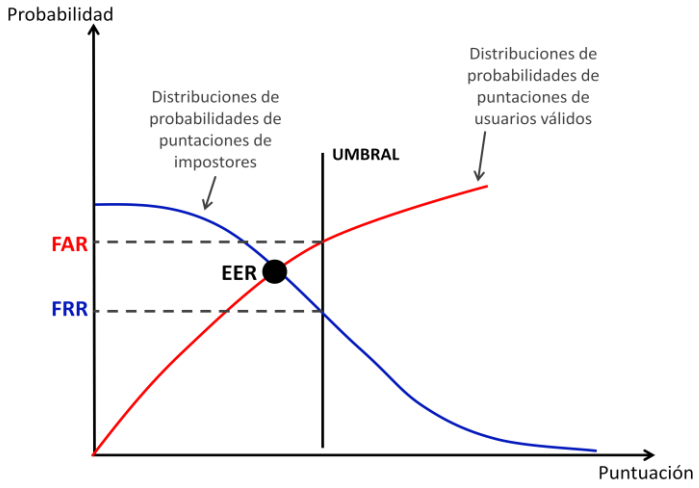


Figura 6. Distribución de probabilidades de usuarios e impostores para todos los posibles umbrales.

- **Representación mediante curvas DET (Detection Error Tradeoff).**

  Aunque el punto de EER corresponde al umbral donde se igualan FAR y FRR, esto no implica que el sistema deba trabajar en ese punto.

  Para establecer este punto de trabajo del sistema, por lo general, se suele emplear la representación en forma de curvas DET, que consiste en la presentación de un error frente al otro en un eje normalizado, obteniéndose así una única curva para ambos tipos de error definida por todos los posibles puntos de trabajo del sistema. En esta curva (ver Figura 7), cualquier punto está dado por un valor de FA y otro de FR, de modo que no es necesario estar manejando varias curvas para determinar el punto de trabajo, pero ya no tenemos la información del umbral. El valor del EER se extrae a partir de la curva DET como el punto en el que ésta corta a la bisectriz de la gráfica.

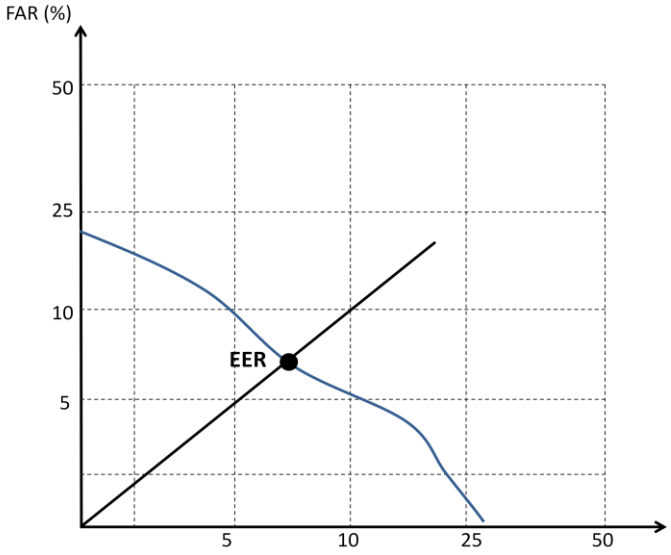


Figura 7. Curva DET

En aplicaciones de alta seguridad (control de accesos), el punto de trabajo suele situarse en valores bajos de FA, para evitar que accedan impostores, a costa de tener alta FR. Por el contrario, en aplicaciones forenses se trabaja en baja FR, para no perder individuos buscados, a costa de una alta FA. Las aplicaciones civiles suelen trabajar en un punto intermedio.

Criterios de evaluación de sistemas de identificación

Para un sistema biométrico que trabaja en modo identificación, se deben comparar todos los datos de entrada con todos los modelos de usuario almacenados en la base de datos. El sistema devolverá el modelo con el que se obtenga un mayor parecido.

En este caso, el rendimiento se indica en términos de tasa de acierto, medida como el porcentaje de veces que el modelo devuelto por el sistema es el correcto. Hay que tener en cuenta que solamente hay un modelo de identidad en la base de datos que se corresponde con los datos de entrada, mientras que hay N - 1 modelos que corresponden a otras identidades. De esto se deduce que si el tamaño de la base de datos es muy grande, la tasa de acierto del sistema puede decrecer considerablemente, ya que hay más modelos de otras identidades con los que comparar y por tanto, mayor probabilidad de cometer un error. Esto

puede suponer un problema por ejemplo en reconocimiento negativo, donde sólo es posible trabajar en modo identificación. Una posible opción es que el sistema no devuelva una sola identidad como resultado, sino una lista de varias, por ejemplo de 10 ó 20 identidades, aumentando así las posibilidades de que la identidad buscada se encuentre dentro de esta lista. A continuación un operador manual efectuará la decisión final a partir de dicha lista. En este caso, a pesar de que tenga que haber intervención humana en la decisión, el sistema nos evita tener que buscar manualmente en un conjunto de N identidades (que pueden ser millones), reduciendo la búsqueda a solamente 10 ó 20.

Cuando disponemos de un sistema de identificación, cuya salida es una lista de candidatos, se utilizan curvas CMC (*Cumulative Match Characteristic*) (Figura 8) para poder analizar de manera visual los resultados obtenidos. Estas curvas no tienen en cuenta los *scores* de salida del sistema, sino la posición del candidato genuino en la lista devuelta por el sistema. En ellas se representa para cada posición de la lista, el porcentaje de identificación del usuario genuino para esa posición y todas las anteriores en todas las búsquedas realizadas para cada tipo de experimento.

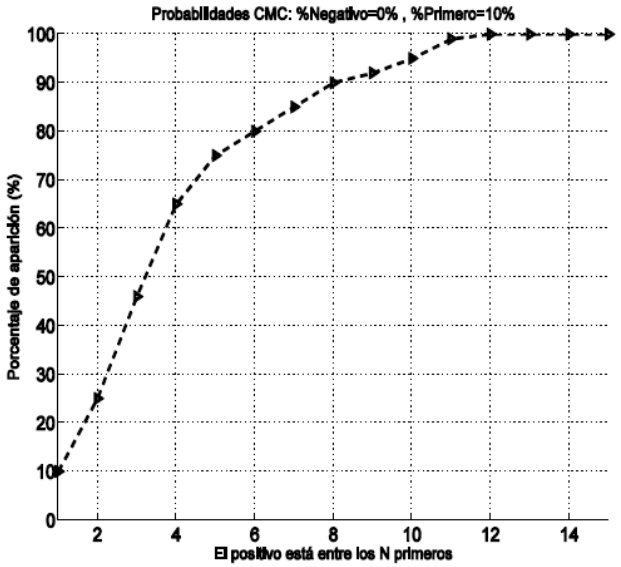


Figura 8. Curva CMC

2.2.3 Limitaciones de los sistemas biométricos

El hecho de que el reconocimiento biométrico esté extendido en múltiples sectores y aplicaciones no significa ni mucho menos que sea un problema totalmente resuelto. Aún hay margen de mejora en los sistemas biométricos, no sólo desde el punto de vista de las tasas de error, sino también de la usabilidad de los sistemas y de su vulnerabilidad frente a ataques. A continuación, detallamos algunas de las limitaciones de los sistemas biométricos que operan usando un solo rasgo. A pesar de que la tecnología va evolucionando y es capaz de aliviar algunos de estos, hay casos en los que resulta muy difícil ponerle solución. Presentaremos algunos de estos casos:

- **Ruido en los datos adquiridos.** Los datos capturados pueden estar perturbados o distorsionados. Un dedo con cortes o quemaduras o la voz de una persona resfriada son un ejemplo. La perturbación también puede proceder de un mal mantenimiento del sensor (acumulación de suciedad) o de condiciones ambientales desfavorables. El resultado es que los datos capturados no podrán ser correctamente comparados con otros datos, produciéndose errores. En ocasiones estos problemas pueden solucionarse tomando las medidas adecuadas (por ejemplo, limpiando el sensor), pero otras veces no es posible hacer nada (quemaduras en el dedo).

- **Variabilidad de los datos adquiridos**. Los datos biométricos de un individuo no suelen ser iguales entre diferentes capturas. A esta diferencia se la conoce como variabilidad intraclase. Esto sucede, por ejemplo, cuando el usuario interactúa de una manera distinta con el sensor cada vez que intenta usarlo. En otros casos, el estado de ánimo o el simple paso del tiempo produce cambios en los rasgos, sobre todo en los rasgos de comportamiento. El rasgo capturado puede ser muy diferente del modelo almacenado de ese usuario, incrementándose así el Falso Rechazo. Una solución a este problema consiste en ir actualizando el modelo almacenado del usuario a medida que pasa el tiempo.

- **Capacidad distintiva de los rasgos biométricos**. De la misma manera que los datos biométricos de un individuo pueden variar con el tiempo, en algún caso, los datos de dos individuos distintos pueden ser lo suficientemente parecidos como para no poder distinguirlos. A este parecido se le conoce como similitud interclase. Este hecho también tiene su efecto en las tasas de error, incrementando la Falsa Aceptación.
  En la práctica no existe un rasgo biométrico para el cual los datos de cualquier par de individuos sean totalmente distintos, por lo que siempre hay un límite en términos de capacidad discriminativa.

- **No universalidad**. Si bien se supone que cualquier individuo posee cualquier rasgo biométrico, en la práctica no es así. Por ejemplo, ciertos colectivos de población pueden no tener huellas adecuadas para el reconocimiento (trabajadores manuales). También puede suceder que por lesiones o accidentes no se posea un rasgo biométrico de modo temporal o permanente. Como consecuencia, no es posible obtener un modelo fiable que represente la identidad del usuario, o directamente no es posible capturar el rasgo.

- **Ataques a sistemas biométricos**. La seguridad de un sistema biométrico puede verse comprometida por ataques. Un impostor puede intentar imitar el rasgo biométrico de un usuario legítimo para sortear el sistema. Los rasgos biométricos de comportamiento son más susceptibles a este tipo de ataques que los fisiológicos (imitadores de firma o voz, etc).

2.2.4 Multimodalidad biométrica

Algunas de las limitaciones de los sistemas biométricos pueden solventarse utilizando más de un rasgo biométrico para el reconocimiento, lo que da lugar a los llamados sistemas multimodales. Estos sistemas biométricos:

- son más precisos al combinar varios frentes de información,
- son más difíciles de suplantar al tener que atacar a varios rasgos,
- permiten cubrir mayor población que un sistema unimodal, puesto que es más difícil que un individuo no posea varios rasgos a la vez.

Un sistema multimodal puede operar de diferentes **modos,** según el orden en el que se combinan las distintas fuentes de información, afectando de diferente manera al tiempo de respuesta y a la forma de interacción con el usuario:

- **Modo serie**: las salidas del análisis de un rasgo biométrico se usan como entrada para análisis del siguiente rasgo, reduciendo así en cada paso el número de identidades posibles antes de emplear la siguiente característica. Este modo se usa, por ejemplo, poniendo en primer lugar un sistema poco preciso pero de rápido procesado para después, una vez reducidas rápidamente las posibles identidades, emplear un sistema más preciso (Ver Figura 9).

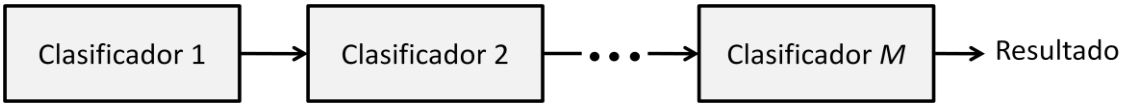


Figura 9. Sistema multimodal en modo serie.

- **Modo paralelo**: la información de múltiples rasgos biométricos se emplea simultáneamente en el proceso de reconocimiento. En contraste al caso anterior, siempre se utilizan todos los sistemas fusionados, por ello, lo requiere capturar todos los rasgos antes de decidir (Ver Figura 10)

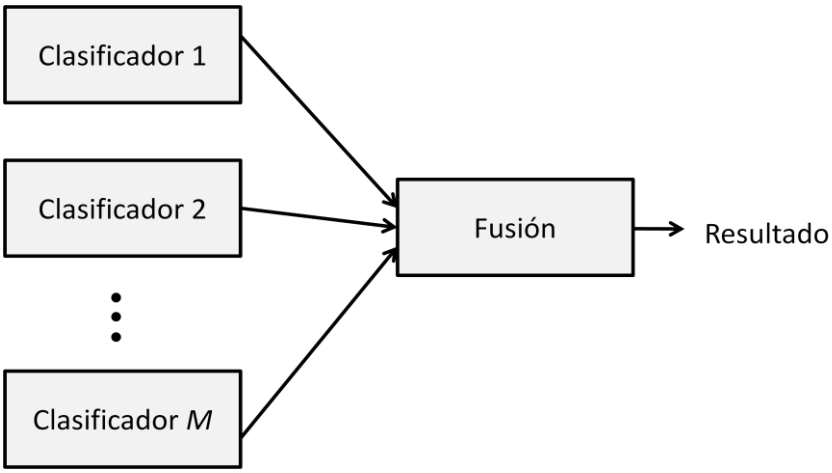


Figura 10. Sistema multimodal en modo paralelo.

A su vez, existen varios **niveles** donde se puede combinar la información de múltiples sistemas:

- **A nivel de extracción de características**: combinando las diferentes características extraídas (Ver Figura 11).

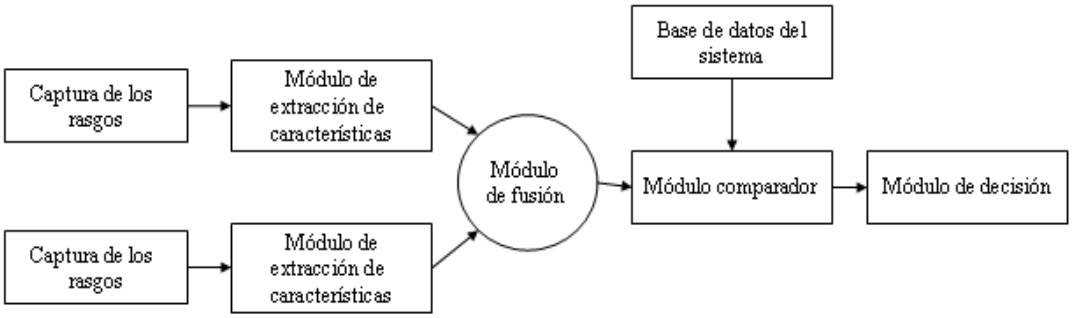


Figura 11. Fusión a nivel de extracción de características.

- **A nivel de score**: combinando los diferentes scores de similitud, por ejemplo un promedio (Ver Figura 12).

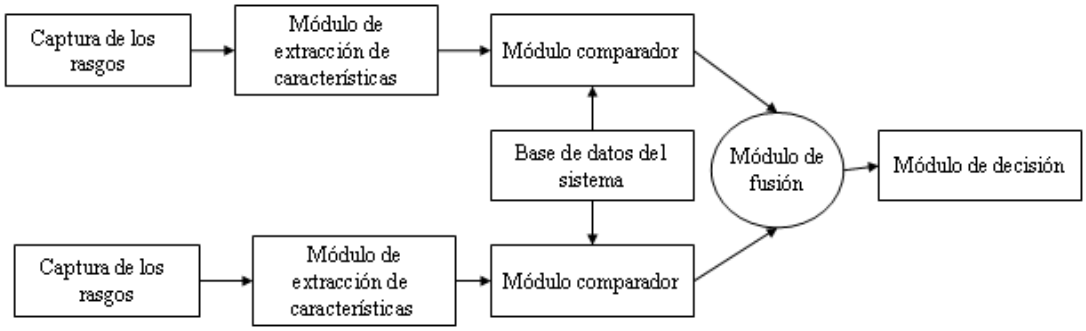


Figura 12. Fusión a nivel de score.

- **A nivel de decisión**: a partir de las distintas decisiones de aceptado/rechazado, por ejemplo por mayoría (Ver Figura 13).

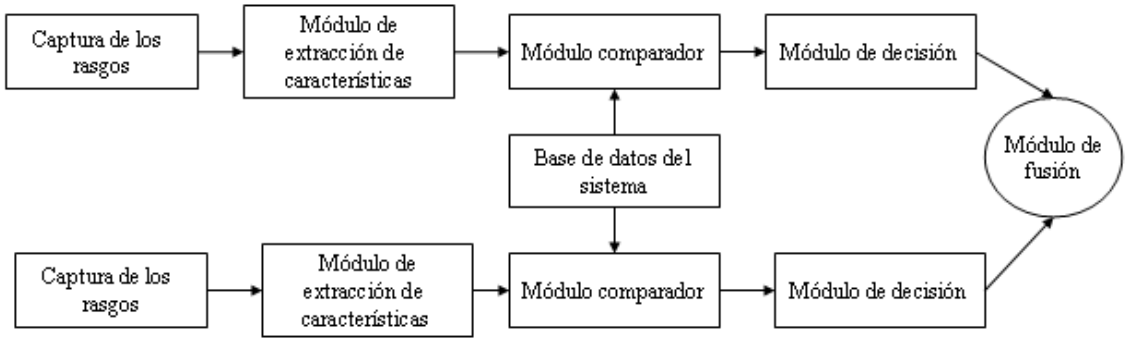


Figura 13. Fusión a nivel de decisión.

En este PFC, se estudian diferentes características extraídas a partir de datos manuscritos y, como se verá más adelante, también se estudia la fusión a nivel de score a partir de las puntuaciones individuales de cada característica.

Por último, un sistema multimodal puede combinar información de múltiples fuentes según los siguientes **escenarios**:

- **Múltiples sensores**: se combina la información obtenida de diferentes sensores (con distinta tecnología o mecanismo de captura) para el mismo rasgo biométrico.

- **Múltiples rasgos**: se combinan diferentes rasgos biométricos como pueden ser la cara y la huella dactilar. Estos sistemas contendrán necesariamente más de un sensor, cada uno para un rasgo biométrico distinto.

- **Múltiples instancias de un mismo rasgo**: permite combinar las huellas dactilares de dos o más dedos de una persona, o una imagen de cada uno de los dos iris de un sujeto.

- **Múltiples capturas de un mismo rasgo**: se emplea más de una captura del mismo rasgo biométrico. Por ejemplo, se combinan múltiples impresiones del mismo dedo, múltiples muestras de voz o múltiples imágenes de la cara.

- **Múltiples representaciones/comparaciones para un mismo rasgo**: implica combinar diferentes enfoques para la extracción y comparación de las características biométricas.

En este proyecto, se hará uso del último escenario (múltiples representaciones/comparaciones para un mismo rasgo) cuando se fusionen diferentes características extraídas a partir de un mismo material manuscrito.

2.2.5 Aplicaciones de los sistemas biométricos

Al igual que los rasgos biométricos difieren en aspectos importantes, lo mismo sucede con las aplicaciones biométricas [5]. Éstas pueden diferir sustancialmente en factores como el nivel de seguridad requerido, la conveniencia para el usuario, el proceso de registro en el sistema o en el proceso de verificación de identidad. De la misma manera, junto con la variedad de aplicaciones de reconocimiento biométrico, existen distintos mercados.

Se pueden establecer los siguientes tipos de **aplicaciones** del reconocimiento biométrico:

Aplicaciones de **cara al ciudadano**, dentro las cuales se engloban:

- Identificación criminal de un sospechoso o detenido.
- Verificación de la identidad en la interacción del ciudadano con servicios públicos como salud, voto, seguridad social, etc.
- Vigilancia de individuos presentes en un lugar en un momento determinado, por ejemplo en eventos públicos.

Aplicaciones de **cara al empleado**, dentro las cuales se engloban:

- Acceso a equipos o redes, sustituyendo o complementando los mecanismos tradicionales mediante clave.
- Acceso físico a instalaciones, típicamente a un edificio, en complemento o sustitución de llaves, tarjetas magnéticas, etc.

Aplicaciones de **cara al cliente**, dentro las cuales se engloban:

- Comercio electrónico y transacciones remotas telefónicas.
- Terminales de punto de venta, complementando o sustituyendo las tradicionales tarjetas con número PIN.

Igualmente, se establecen una serie de **mercados** dentro de los cuales se engloban la mayor parte de las aplicaciones biométricas. Estos mercados hacen uso de diversas aplicaciones, sin que una misma aplicación sufra importantes variaciones en los diferentes mercados. Por ejemplo, un control de acceso físico que haga uso de la mano funciona de modo más o menos parecido si se usa en un banco o en un aeropuerto. Los distintos mercados son:

- **Legal (forense),** que hace uso del reconocimiento biométrico para identificar a individuos sospechosos, detenidos, bajo situación de arresto o con restricciones de libertad (arresto domiciliario, etc.).

- **Gubernamental**, donde el reconocimiento biométrico se utiliza para controlar la interacción del ciudadano con entidades públicas y para la propia administración del sistema público.

- **Financiero**, al igual que en el sector gubernamental, el reconocimiento biométrico controla la interacción del ciudadano con el sistema financiero (acceso a cuentas o transacciones comerciales) y la propia administración del sector, por ejemplo el acceso de empleados a redes protegidas.

- **Salud**, donde al igual que los dos casos anteriores, por un lado se controla la interacción del usuario (utilización de servicios sanitarios) y por otro lado se asegura el correcto funcionamiento del sistema (manejo de información médica por parte de empleados).

- **Inmigración**, donde el reconocimiento biométrico se usa para el control de movimientos a través de fronteras y para el control interno de los propios empleados dentro de las áreas restringidas de acceso.

2.2.6 Aceptación social y privacidad

La actual aportación tecnológica de los sistemas de reconocimiento biométrico ha de venir sin duda acompañada de una evolución paralela en el ámbito de los derechos fundamentales de los usuarios en cuanto a temas de privacidad se refiere. Cabe destacar que el aspecto de desarrollo tecnológico que se produce en el diseño y desarrollo de los sistemas de reconocimiento biométrico es un pilar fundamental para la integración de los mismos de manera efectiva dentro de los actuales sistemas de seguridad, pero no se puede olvidar por otro lado la necesidad de desarrollar otros aspectos "no técnicos".

La sociedad es la que determina el éxito de los sistemas de identificación basados en rasgos biométricos. La facilidad y comodidad en la interacción con el sistema contribuye a su aceptación. Si un sistema biométrico permite medir una característica de un individuo sin necesidad de contacto directo, se percibe como mejor. Además, las tecnologías que requieren muy poca cooperación o participación de los usuarios suelen ser percibidas como más convenientes. Por otro lado, los rasgos biométricos que no requieren la participación del usuario en su adquisición pueden ser capturados sin que el individuo se dé cuenta y esto es percibido como una amenaza a la privacidad por parte de muchos usuarios. El tema de la privacidad adquiere gran relevancia con los sistemas de reconocimiento biométrico porque los rasgos biométricos pueden proporcionar información muy personal de un individuo, como afecciones médicas, y esta información puede ser utilizada de forma poco ética.

Por otro lado, los sistemas biométricos pueden ser empleados como uno de los medios más efectivos para la protección de la privacidad individual. Si un individuo extravía su tarjeta de crédito y otra persona la encuentra podría hacer un uso fraudulento de ella. Pero si la tarjeta de crédito únicamente pudiese ser utilizada si el impostor suplantase los rasgos biométricos del usuario, éste estaría protegido. Otra ventaja del uso de los rasgos biométricos consiste en limitar el acceso a información personal.

La mayoría de los sistemas biométricos comerciales disponibles hoy en día no almacenan las características físicas capturadas en su forma original, sino que almacenan una representación digital en un formato encriptado. Esto tiene dos propósitos: el primero consiste en que la característica física real no pueda ser recuperada a partir de su representación digital, lo que asegura privacidad, y el segundo se basa en que el encriptado asegura que sólo la aplicación designada puede usar dicha representación digital.

Capítulo 3

ESTADO DEL ARTE SOBRE IDENTIFICACIÓN DE PERSONAS A PARTIR DE LA ESCRITURA Y LA FIRMA

La identificación de los autores de manuscritos es el objetivo de una importante disciplina forense, la *grafística*. Ésta se centra en el análisis de documentos escritos a mano por el individuo utilizando algún tipo de utensilio de escritura (lápiz, bolígrafo, pluma,…). La identificación de escritor a partir de muestras digitales de la escritura o la firma tiene como objetivo el desarrollo de sistemas informáticos que puedan desempeñar esta tarea de manera automática.

3.1 Reconocimiento de escritor vs. Reconocimiento de escritura

En el ***reconocimiento de escritura*** se buscan representaciones capaces de eliminar variaciones entre diferentes escrituras con el objetivo de clasificar la forma de los caracteres y de las palabras de manera robusta. Su objetivo es averiguar el texto escrito independientemente de la fuente. Por el contrario, el ***reconocimiento de escritor*** requiere representaciones realzadas de estas variaciones ya que son características de cada escritor, siendo su objetivo distinguir o averiguar la fuente que ha producido el texto.

Debido a sus múltiples aplicaciones, el reconocimiento de escritura siempre ha tenido más peso en las investigaciones del área de análisis de la escritura [6]. Pero en los últimos años, el reconocimiento de escritor ha empezado a cobrar importancia como consecuencia de sus aplicaciones en el campo forense y en el análisis de documentos históricos. La meta del reconocimiento de escritura consiste en obtener generalizaciones y eliminar las variaciones, mientras que en el reconocimiento de escritor lo que se pretende es maximizar las características específicas del estilo de escritura individual para poder discriminar entre escritores.

Es importante destacar que el reconocimiento de escritor podría reducir ciertas ambigüedades en el proceso de reconocimiento de patrones si la información de los hábitos de escritura generales del escritor estuviese disponible en el sistema de reconocimiento de escritura. Así pues, se bien su objetivo es contrapuesto, ambas podrían complementarse para un único fin.

3.2 Identificación de escritor vs. Verificación de escritor

La identificación grafística es un método comúnmente utilizado por los cuerpos policiales y fuerzas del orden público. La escritura manuscrita, y en concreto la identificación de los autores de documentos dubitados (esto es, de autoría desconocida), tiene una gran relevancia e interés para el sistema judicial y policial desde dos puntos de vista: *verificación* e *identificación*. Ambos mecanismos, descritos a continuación, se representan en la Figura 14.

La ***verificación*** se refiere a los casos en los que los científicos forenses tienen que trabajar con pruebas en forma de documentos manuscritos que deben comparar uno frente a otro para contrastar su autenticidad. Típicamente se toma una muestra, validada por un agente de policía o judicial al sujeto en cuestión, que se compone de diferentes elementos de escritura: firma, nombre y apellidos, escritura natural en mayúsculas, en minúsculas y distintos números. Dicha muestra validada (también llamada indubitada) se contrasta con el documento cuya autoría se desconoce y que se pretende atribuir o no al sujeto. Un ejemplo típico de esto podría ser la autenticación de un contrato o un testamento. Para la muestra validada, tradicionalmente suele utilizarse como referencia algún texto o párrafo con una distribución uniforme de las letras más representativas desde el punto de vista de autentificación. Generalmente, el objetivo de esta actividad por los expertos forenses es el generar un informe judicial, de forma que el juez o el jurado pueda tomar una decisión sobre la culpabilidad o inocencia de un posible inculpado de delito. Estamos pues en un caso de comparación de documentos de uno versus uno (dubitado vs. indubitado).

Por otro lado, la ***identificación*** se refiere a comparar un documento de autoría desconocida (dubitado) frente a N documentos de autoría conocida (indubitados), siendo N un número elevado, típicamente un grupo de individuos sobre el que queremos identificar al individuo dubitado. Este podría ser el caso de intentar identificar a un delincuente entre un grupo de sospechosos, siempre y cuando dispusiéramos de muestras indubitadas de escritura de los mismos.

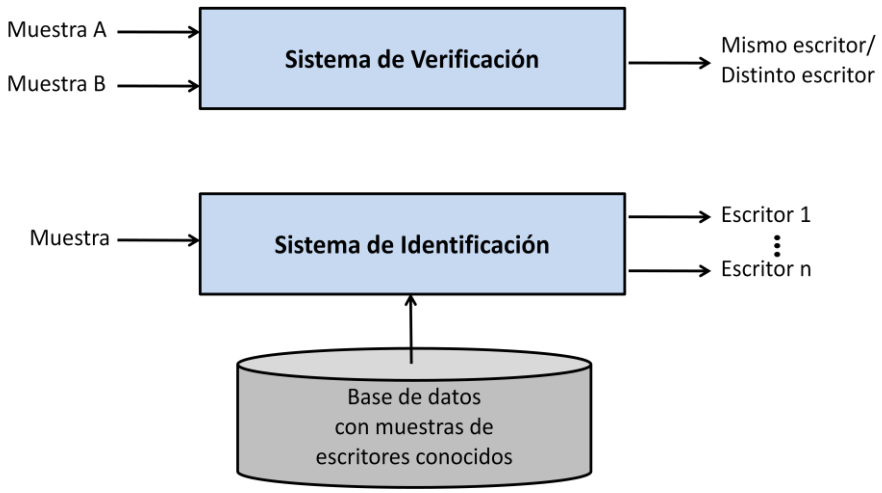


Figura 14. Sistema de verificación de escritor. Sistema de identificación de escritor.

3.3 Escritura *off-line* vs. Escritura *on-line*

Las técnicas de reconocimiento de escritor tienen como objetivo el transformar texto de su forma gráfica manuscrita (en dos dimensiones, en papel) a un formato simbólico útil para la computadora para poder ser procesado. En general, los sistemas de reconocimiento de escritor se dividen en dos clases principales según los dispositivos de adquisición de datos: la clase de los dispositivos ***off-line*** (Ver Figura 15) y la clase de los dispositivos ***on-line*** (Ver Figura 16) [7].

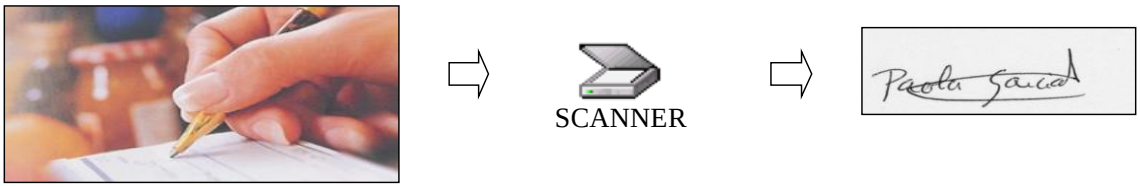


Figura 15. Ejemplo de un sistema de adquisición de escritura off-line.

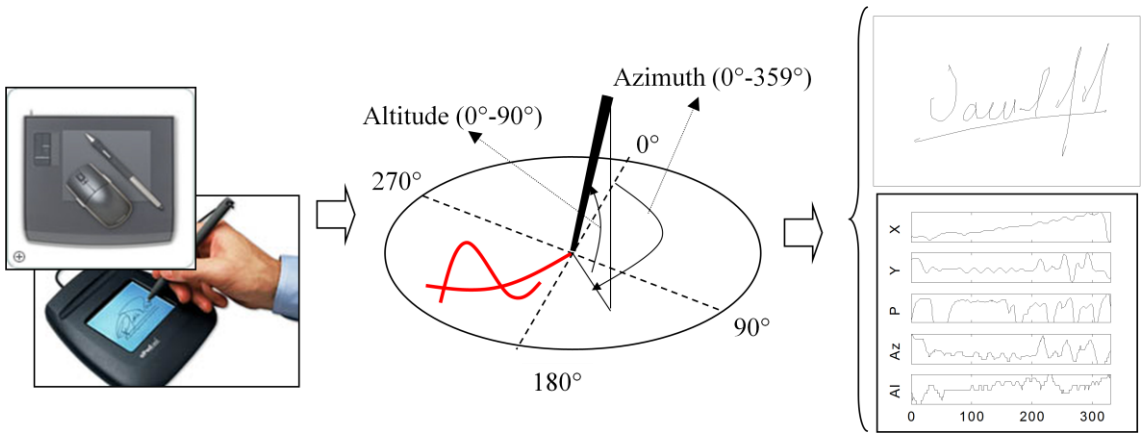


Figura 16. Ejemplo de un sistema de adquisición de escritura on-line.

Los dispositivos on-line normalmente son tabletas digitalizadoras que son sensibles a la presión. Estos dispositivos especiales permiten registrar información dinámica sobre la velocidad de escritura, presión, ángulo y posición del lápiz, aceleración etc. mejorando así mucho la capacidad de reconocimiento al capturar mucha información durante el proceso de escritura manual por parte del individuo. Por otro lado, los dispositivos off-line utilizan una información más limitada, normalmente se basan en usar algún tipo de escáner, simplemente para capturar una imagen del texto manuscrito. En la mayoría de los casos, esta es la única información disponible si el escritor no ha utilizado uno de estos dispositivos especiales de escritura. Este proyecto se basa en el análisis de escritura manuscrita *off-line*.

3.4 Características locales vs. Características globales

En este proyecto, se presentan varios tipos de sistemas de reconocimiento off-line de escritura. Cada uno de estos sistemas calculan una serie de características distintivas de cada muestra de escritura. Estas características se pueden clasificar de dos formas diferentes: características locales y características globales.

Las ***características globales*** son aquellas que obtienen el vector de características a partir de la imagen completa de la muestra de escritura.

Las ***características locales*** son aquellas que dividen las imágenes de las muestras de escritura en regiones y se calcula un vector de características por cada región.

3.5 Reconocimiento independiente de texto vs. Reconocimiento dependiente de texto

La identificación y verificación de escritor pueden a su vez estar dentro de dos categorías: métodos dependientes de texto y métodos independientes de texto.

Los métodos ***independientes de texto*** utilizan características extraídas de la imagen entera de un bloque de datos manuscritos, proporcionando una descripción global de la región escrita. Se necesita una cantidad suficiente de escritura, como por ejemplo un párrafo o unas cuantas líneas, para poder obtener características estables insensibles al contenido del texto de las muestras. Desde el punto de vista de la aplicación, el gran avance consiste en que la intervención humana y la complejidad se reducen, dado que se hace uso del material manuscrito existente cualesquiera que sea su contenido. Por otro lado, en entornos forenses como los evaluados en este Proyecto, no hay posibilidad de elección acerca del material manuscrito. En este caso, los datos dubitados suelen corresponder a muestras intervenidas o requisadas, sin ningún control sobre su captura ni sobre su contenido.

Otros métodos, llamados ***dependientes de texto***, hacen uso de caracteres o palabras individuales de contenido semántico conocido. Estos métodos requieren en primer lugar localizar y segmentar la información relevante, lo que los hace más complejos. Su ventaja consiste en que permiten alcanzar un alto rendimiento incluso con pequeñas cantidades de material escrito disponible, pero tienen limitada su aplicabilidad debido a que suponen un texto fijo o a la necesidad de intervención humana para localizar los objetos de interés.

En este trabajo abordamos la identificación de escritor *independiente* del texto escrito; capturado sin utilizar dispositivos especiales, por lo que serán casos de identificación de escritura *off-line*.

3.6 Variabilidad en la escritura

La escritura es un sistema de representación gráfica de una lengua, por medio de signos grabados o dibujados sobre un soporte plano, normalmente, sobre un papel. Cada individuo presenta, por lo general, su estilo de escritura en cada texto pero se ve afectado por una serie de condiciones reales:

- todo tipo de condiciones de apoyo
- iluminación
- entorno
- utensilios de escritura
- suciedad del documento
- distintos tipos/tamaños de hojas (blanco, cuadrícula,...)
- etcétera.

Por otro lado, dependiendo del estado del escritor, su estilo de escritura también puede variar. Por ello, presentamos cuatro factores que pueden producir variabilidad en la [6], ver Figura 17:

- **Transformaciones afines:** pueden ser controladas voluntariamente por el escritor. Entre ellas se encuentran los cambios en el tamaño y la inclinación de la escritura, las traslaciones y las rotaciones. Son una molestia en la identificación de escritor pero no suponen un obstáculo importante.

- **Variabilidad neuro-biomecánica:** hace referencia al contexto local y el estado fisiológico del individuo. Pueden determinar la legibilidad de una muestra escrita y la cantidad de esfuerzo que supone hacer la forma de un carácter. Este factor está más relacionado con el estado del escritor que con la identidad del mismo.

- **Variabilidad de la secuencia u orden de los trazos:** este factor tiene una gran dependencia con el estado del escritor durante el proceso de escritura. El orden de los trazos puede variar estocásticamente. Generalmente, este problema afecta más al proceso de identificación de escritor a partir de escritura *on-line*, que en este proyecto no se trata.

- **Variación alográfica:** hace referencia a la forma específica con la que cada individuo escribe un carácter. Proporciona información esencial para el reconocimiento automático de escritor.

Las transformaciones afines y la variación alográfica son las fuentes de información más útiles en la identificación y verificación de escritor. La escritura de una persona también cambia con la edad y constituye un factor de variabilidad importante que hay que considerar. Al crecer, la escritura de una persona se vuelve más rápida, continua, rítmica y suave, y en las personas mayores puede verse afectada por las condiciones médicas que influyen en la fuerza y la destreza de la mano.

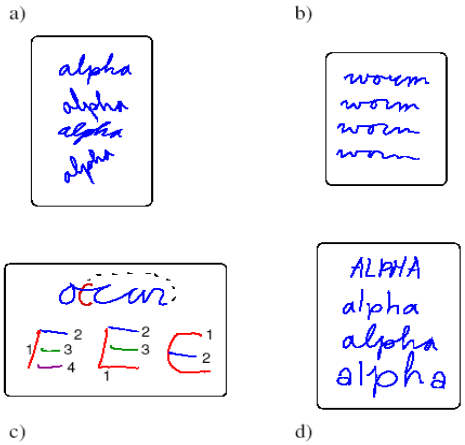


Figura 17. Factores que producen variabilidad en la escritura. (a) Transformaciones afines. (b) Variabilidad neuro-biomecánica. (c) Variabilidad de la secuencia de trazos. (d) Variación alográfica.

3.7 Individualidad de la escritura

A pesar de los cambios en el estilo de escritura de cada persona, este rasgo biométrico suele mostrar características distintivas. A medida que una persona va madurando, su estilo de escritura se va desviando del aprendido en el colegio y progresivamente va incorporando características suyas propias. Apuntaremos dos factores que definen la individualidad de este rasgo biométrico:

- **Factores genéticos:** también llamados factores biológicos. Son los siguientes:
  - Estructura biomecánica de la mano, es decir, tamaño relativo de los huesos de la muñeca y su influencia sobre el bolígrafo.
  - Ser zurdo o diestro.
  - Fuerza muscular.
  - Características del sistema nervioso central.

- **Factores miméticos:** también conocidos como factores culturales, influyen en la manera de coger el bolígrafo y en la forma de los caracteres. La idoneidad de la forma de una letra para su reconocimiento está influenciada por la legibilidad y la facilidad de escribir con las herramientas de escritura disponibles.

En conjunto, los factores genéticos y los miméticos determinan el proceso habitual de escritura de un individuo.
Escribir consiste en movimientos rápidos de los dedos y la mano, y un movimiento horizontal progresivo y lento del extremo inferior del brazo [8].
Por último, cabe mencionar que el proceso de escritura es un proceso psicomotor jerárquico. Éste procede de la memoria a largo plazo, después se especifican los parámetros para este programa motor, tales como el tamaño y la forma, y finalmente se generan comandos para el movimiento de los músculos.

3.8 Trabajos previos y algoritmos existentes para reconocimiento de escritor

Desde el punto de vista de automatizar el análisis de la escritura con el objetivo de identificar al autor, se pueden distinguir el área específica de reconocimiento a partir de la **firma** manuscrita y el área global de reconocimiento a partir de **textos** manuscritos de forma libre.

La firma constituye una parte muy especializada y particular del acto de escritura de un individuo, tan repetida y asimilada que se convierte en un acto pseudo-reflejo que este repite de forma mecánica. Aunque sea para un caso muy particular de escritura, la firma también utiliza técnicas de extracción de características y de reconocimiento de patrones muy similares a las del reconocimiento a partir de textos. Pero por otro lado, no busca en general un análisis de la imagen con vistas a entender su significado o descomponerla en letras (de hecho hay firmas donde esto no es posible debido a que son sólo un grafismo personalizado por el individuo que no refleja caracteres concretos), sino que busca el análisis de características gráficas locales o globales que permitan verificar que una nueva firma presentada al sistema es igual a alguna otra. El tipo de características que se usan en estos sistemas pueden ser útiles o servir de base e inspiración para características de un sistema de identificación a partir de textos, pero no siempre aplicables en general.

Por estas razones, resumimos aquí separadamente los trabajos más relevantes sobre las áreas de reconocimiento a partir de firma y a partir de textos. El resumen aquí presentado se refiere solamente al análisis *off-line*, que es el caso particular que se estudia en la sección experimental de este Proyecto.

3.8.1 Algoritmos para reconocimiento a partir de textos

Un resumen de los primeros trabajos sobre reconocimiento automático de escritor se hace en [9]. Los algoritmos de identificación de escritor de trabajos trabajan con características o representaciones en el dominio *espacial*, en el dominio de *frecuencias*, o con representaciones *vectoriales* entre otras.

Entre los métodos que hacen uso de representaciones en el dominio espacial y que se han estudiado a partir de [10], encontramos:

- El de [11] sobre identificación basada en medidas de run-length i.e. secuencias continuas de puntos negros en horizontal o vertical.
- Los trabajos de [12] y [13] basados en transformadas de patrón de arco y los generales sobre características off-line de caracteres.
- Los perfiles de proyección horizontal y operadores morfológicos propuestos en [14].
- Los trabajos de [15] sobre características basadas en la línea de texto.
- Los de [16] sobre macro y micro características.

- Los de [17] sobre trasformadas lineales y elementos direccionales para caracteres chinos.
- El conjunto de 21 características computacionales extraídas a los niveles de documento, párrafo, palabra y carácter por [18], siendo el más amplio estudio sobre la individualidad de la escritura manuscrita realizado en el área. Se incluyen características como número de píxeles de tinta, número de contornos externos/internos, inclinación media y longitud de las palabras, de gradiente, estructurales y de concavidad.
- Las características direccionales de los bordes presentadas en [2].

Otra alternativa es la representación *frecuencial*, consistente en aplicar de alguna forma la teoría de Fourier, de manera que la imagen espacial de la escritura se descompone en un espectro de frecuencias componentes de la misma. Una investigación importante en este sentido fue desarrollada por Said et al. [2000]. El algoritmo propuesto se basa en características de textura, filtros de Gabor multicanal y matrices de co-ocurrencia en escala de gris.

Por último, tenemos los métodos de representación *vectorial*. Consiste en la utilización de "splines" para representar las letras (Hearn y Baker, 1994), que intuitivamente se pueden definir como bandas flexibles que se utilizan para producir una curva suave a través de un conjunto de puntos prefijados. Así la idea es que se definen para la forma de las letras una serie de puntos críticos y parámetros que permiten a curvas paramétricas aproximar la forma de las mismas. Un trabajo especialmente destacado que utiliza este enfoque es el de Cohen et al. (1995).

3.8.2 Algoritmos para reconocimiento a partir de firmas

Estos algoritmos se han estudiado a partir de [19].
En los últimos años, una gran cantidad de técnicas basadas en este tema han sido propuestas. La mayoría de ellas, se han resumido por DiMauro et al. (2004); Hou et al. (2004); Leclerc y Plamondon (1994); Plamondon y Lorette (1989); Sabourin (1992) .

Estas técnicas se basan en extracción de características de las firmas y se pueden clasificar dando dos enfoques diferentes: enfoques globales y enfoques locales.

Las técnicas basadas en **enfoques globales** obtienen el vector de características a partir de la imagen completa de la firma. Los primeros trabajos sobre este tema utilizaban diferentes técnicas fundamentadas en el análisis de la forma de la imagen, como por ejemplo descriptores de Fourier, Hadamard transforma, etc (Ammar et al., 1988).

Ahora, presentamos algunos estudios recientes basados en este enfoque:

- Técnicas basadas en funciones de densidad de probabilidad direccionales que calculan la dirección de los trazos de la firma (Sabourin and Drouhard, 1992).
- Cálculo de momentos basados en proyecciones verticales y horizontales. En este caso, se calcula la cantidad de píxeles de cada fila y cada columna de la imagen (Bajaj and Chaudhury, 1997).
- Obtención de matrices de forma calculadas sobre una cubierta psuedo-convexa de la imagen de la firma (Sabourin et al., 1997) .
- Desarrollo de características basadas en la inclinación y dirección de las firmas; usando procesado morfológico de la imagen (Lee and Lizarraga, 1996).
- Técnicas basadas en densidades de píxeles que dividen la imagen de la firma en celdas y calculan la cantidad de píxeles de la firma en cada una de estas celdas (Justino et al., 2000; Rigoll and Kosmala, 1998).
- Métodos que calculan características geométricas a partir de medidas del contorno de la firma basadas en las coordenadas polares y cartesianas (Ferrer et al., 2005).
- Cálculo de características grafométricas como pueden ser la proporción de la firma, el espacio entre los bloques de la firma, el ángulo de la imagen, el área de la imagen, el número de bucles cerrados, el número de cruces, el número máximo de proyecciones verticales y horizontales, el ángulo de inclinación global, el número de puntos de borde, etc. (Baltzakis and Papamarkos, 2001; Justino et al., 2000).

Por otro lado, las técnicas basadas en **enfoques locales** dividen las imágenes de las firmas en regiones y se calcula un vector de características por región.
Algunos trabajos recientes basados en este enfoque se presentan a continuación:

- Técnicas basadas en descriptores estructurales que consideran la firma completa como un conjunto de símbolos jerárquicos que pueden ser descritos a diferentes niveles en estructuras tipo árbol (Ammar et al., 1990).
- En Sabourin et al. (1993) se proponen códigos de sombra como características. Esta técnica divide la imagen de la firma en celdas y luego se calcula la proyección de los píxeles en cada una de las celdas en distintas direcciones.
- Un método basado en distribuciones granulométricas se propusieron por Sabourin et al. (1996). Esta técnica divide la imagen de la firma en celdas, que son llamadas retinas, y calcula el espectro de patrones de los píxeles de cada retina basándose en diferentes operadores morfológicos.
- Obtención de características simples como pueden ser la curvatura, el ángulo y el tamaño de trazos aislados (Guo et al., 1997).
- Técnicas que calculan un índice de suavidad que permite comparar la individualidad entre las curvas de los trazos individuales basados en su suavidad (Fang et al., 1999).
- Métodos de extracción de características basados en la inclinación y la dirección de las firmas. Se calculan a partir de regiones locales de la imagen usando procesado morfológico de imágenes (Lee and Lizarraga, 1996).

Además, existen enfoques que combinan características locales y globales como los trabajos presentados por Fierrez-Aguilar et al. (2004); Huang y Yan (1997); Sabourin et al. (1994).

Por otro lado, las características también pueden ser clasificadas como características estáticas y características pseudo-dinámicas. Las características presentadas en esta sección son características estáticas.
Las características pseudo-dinámicas tratan de extraer información dinámica de la imagen de la firma; esto es, información muy valiosa para detectar falsificaciones entrenadas. Algunos trabajos que estudian este tipo de características son:

- El método propuesto por Ammar y Fukumura (1986). La información de presión se recupera a partir de los trazos de la estructura.
- En Lee y Pan (1992) calculan el movimiento direccional de los trazos de las imágenes de la firma.
- Pan y Lee (1991) reescriben la firma con un algoritmo heurístico, emulando el modo en que una persona podría firmar.

Capítulo 4

SISTEMAS DE RECONOCIMIENTO DE ESCRITOR

4.1 Descripción general de los sistemas

En este proyecto, se han desarrollado tres sistemas de reconocimiento de escritor basados en las características estructurales, de concavidad y geométricas presentadas por [18] en su amplio estudio sobre características de escritura. Asimismo, en las pruebas experimentales llevadas a cabo, se ha contado con tres sistemas adicionales disponibles en el grupo ATVS, basados en características de gradiente, alográficas y de contorno. La primera se presenta también en [13], mientras que las alográficas y de contorno se presentan en [2].
La clasificación de estos sistemas se detalla en la tabla de la Figura 18.

De los sistemas desarrollados en el marco de este PFC, el sistema basado en característica estructural y el sistema basado en características de concavidad tienen como objetivo detectar propiedades "multi-resolución". Esto es, se fijan en un pixel (x,y) de un trazo escrito y buscan las relaciones de éste con sus vecinos de menor a mayor proximidad. Por otro lado, el sistema basado en características geométricas pretende dar una representación de la forma de la letra o de la firma.

En el caso de los sistemas disponibles, el sistema basado en características de gradiente y de contorno analizan la orientación de los trazos manuscritos, así como otras magnitudes derivadas de la misma. Por último, las características alográficas y de contorno buscan caracterizar la preferencia de uso por parte del escritor de un conjunto de formas de referencia de un catálogo común.

En este Capítulo se incluye una descripción de estos sistemas. En el Capítulo de experimentos se describen las muestras de escritura disponibles para su evaluación. Éstas se componen de imágenes de letras individuales segmentadas a partir de textos escritos o bien de imágenes de la firma de un sujeto (se realizan experimentos separados para cada caso). Toda imagen de carácter o de firma utilizada en los experimentos pasa por un proceso inicial de preprocesamiento consistente en la binarización de la imagen según el método de Otsu [20] seguido de la eliminación de los márgenes blancos del carácter o la firma (Ver Figura 19).

	CARACTERÍSTICA LOCAL	CARACTERÍSTICA GLOBAL
DISPONIBLES	SISTEMA BASADO EN CARACTERÍSTICAS DE GRADIENTE	
		SISTEMA BASADO EN ALÓGRAFOS
	SISTEMA BASADO EN CARACTERÍSTICAS DE CONTORNO	
DESARROLLADOS	SISTEMA BASADO EN CARACTERÍSTICA ESTRUCTURAL	
	SISTEMA BASADO EN CARACTERÍSTICAS DE CONCAVIDAD	
		SISTEMA BASADO EN CARACTERÍSTICAS GEOMÉTRICAS

Figura 18. Clasificación de los sistemas.

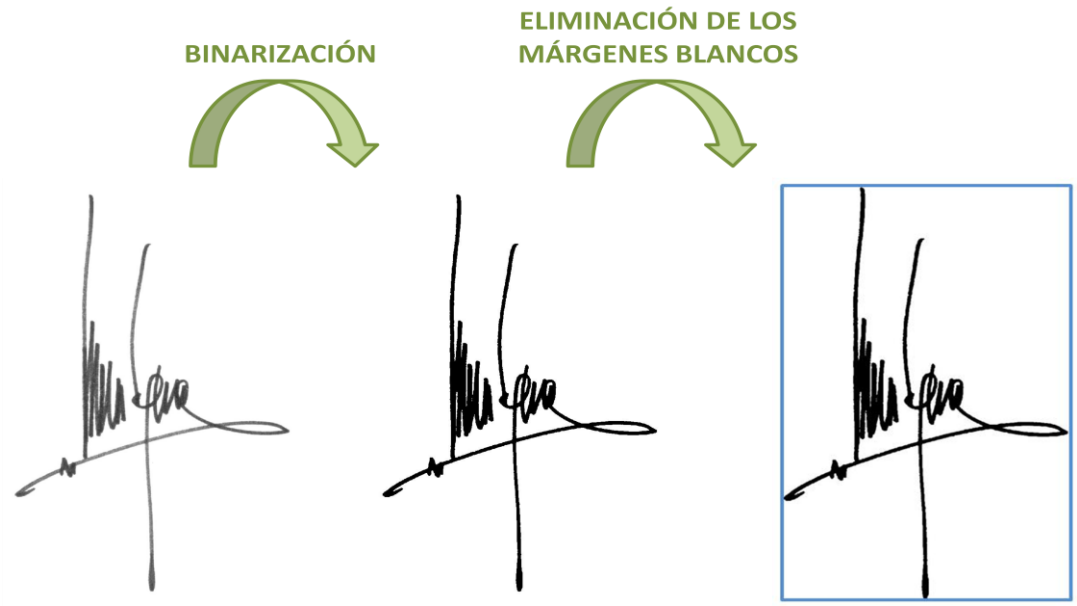


Figura 19. Preporcesamiento del carácter o firma.

Hay que destacar que todos los sistemas de este Proyecto han sido evaluados en sus respectivas publicaciones usando textos de hojas completas manuscritas. En este sentido, tanto la evaluación de estos sistemas sobre imágenes de letras segmentadas individuales como de firmas es una contribución de los trabajos en los cuales se ha enmarcado este Proyecto. Asimismo, durante la implementación y/o adaptación de estos sistemas, se incluyen también algunas aportaciones originales en las distintas fases de procesado, no contempladas en la descripción original de los mismos. Parte de la evaluación llevada a cabo durante estos trabajos fue publicado por la autora en [21]. Igualmente, los desarrollos llevados a cabo dentro de este Proyecto dieron lugar a las publicaciones [22] y [23] colaboradas por la autora.

4.2 Sistemas disponibles evaluados

4.2.1 Sistema basado en características de gradiente

Este sistema obtiene características locales de las muestras. Es decir, divide las imágenes de las muestras de escritura en regiones y calcula un vector de características por región.
Las características de gradiente se basan en calcular el gradiente (derivada) en la imagen de la letra. Para cada punto (x,y) de la imagen con un valor de gris f(x,y), el vector gradiente en ese punto será un vector cuyas componentes serán las derivadas parciales de f(x,y) respecto de cada componente x e y. El gradiente se puede obtener tanto de la imagen en escala de gris como de una imagen binarizada. En este proyecto, se comparará el uso de imágenes escaneadas en escala de gris con el uso de estas imágenes binarizadas según el método de Otsu [20].

Para la extracción de estas características, se utilizará una aproximación del cálculo del gradiente mediante operadores de Sobel [24]. Para ello, se convolucionan dos operadores de Sobel de 3x3, los cuales aproximarán las derivadas parciales de x e y en la posición del píxel en la imagen (esto es, derivada vertical y horizontal). Los operadores de Sobel son filtros que se realizan aplicando máscaras de coeficientes sobre pixeles y sus vecinos. En concreto, se refieren a filtros lineales, siendo su resultado una combinación lineal de los valores de los pixeles y los coeficientes de la máscara espacial, esto es:

$$\begin{matrix} w_1\ w_2\ w_3 \\ w_4\ w_5\ w_6 \\ w_7\ w_8\ w_9 \end{matrix} \quad + \quad \begin{matrix} z_1\ z_2\ z_3 \\ z_4\ z_5\ z_6 \\ z_7\ z_8\ z_9 \end{matrix}$$

con w_i los coeficientes de la máscara espacial a aplicar y z_i los valores de los pixeles, dando como resultado $c= \Sigma^{9}_{i=1} (w_i z_i)$.

Así, considerando la matriz de pixeles z_i tendremos que aplicar dos máscaras, primero una para obtener la componente x del vector gradiente y luego otra para la y. Su objetivo será tomar una medida cuantitativa de cómo varía la imagen respecto de la dirección vertical y respecto de la horizontal.

La máscara de Sobel utilizada para la componente x es:

$$\begin{matrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{matrix}$$

La máscara de Sobel utilizada para la componente y es:

$$\begin{matrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{matrix}$$

De manera que si el vector gradiente en un punto (x,y) es **c** = (c_x,c_y), tendremos que

$$c_x = |c| \cdot \text{sen}(\alpha)$$

$$c_y = |c| \cdot \cos(\alpha)$$

Siendo,

$$\tan(\alpha) = c_x / c_y$$

$$\alpha = \tan^{-1}(c_x / c_y)$$

donde tenemos sobre la matriz de píxeles que

$$c_x = (z_7 + 2\, z_8 + z_9) - (z_1 + 2\, z_2 + z_3)$$

$$c_y = (z_3 + 2\, z_6 + z_9) - (z_1 + 2\, z_4 + z_7)$$

Nota: cuidado con el hecho de que la arctg(α) = $\tan^{-1}$(α) asociado a la *tangente* que tiene periodo π radianes, ya que esto hace que haya dos soluciones posibles para el ángulo α. Habrá que usar los signos de c_x, y de c_y para saber exactamente en qué cuadrante estamos, es decir, qué dirección considerar.

El vector gradiente tiene dirección y módulo. Aquí solo usaremos la dirección, la cual puede variar entre 0 y 2π radianes. Se considerarán sólo los valores múltiplos de π/6, de tal manera que se particiona el espacio de direcciones en 12 regiones, como se muestra a continuación en la Figura 20.

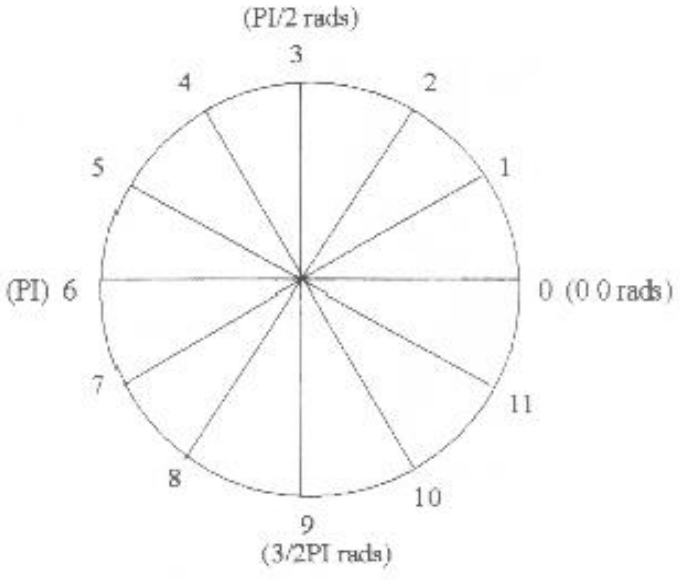


Figura 20. Partición del espacio de direcciones del gradiente.

Para generar la característica de gradiente de una imagen dada, ésta se divide en una malla de 4x4 celdas (ver Figura 21). El gradiente se calculará por separado en cada celda, haciéndose un histograma de cuántas veces se da en cada región cada dirección posible. Para cada celda se generará un histograma de 12 posiciones asociadas a las 12 direcciones posibles. De esta manera tenemos un vector de características total de 12x4x4 = 192 componentes.

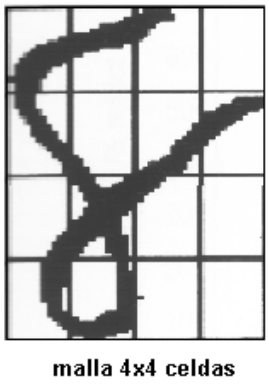


Figura 21. Malla de 4x4 celdas.

En la descripción original de esta característica [18], sobre el histograma de direcciones de la celda se calcula un umbral para la binarización (la media de valores del histograma), de manera que se decide si la dirección en la celda está (bit=1) o no (bit=0). De esta manera tenemos un vector binario de 192 componentes. Como una de las mejoras a esta parte del sistema, en lugar de binarizar los histogramas de direcciones, en este Proyecto se propone normalizarlos a una función densidad de probabilidad. Con un vector binario, concedemos la misma "importancia" a todas las direcciones con tal de que el histograma supere el umbral fijado. Por el contrario, con una función densidad de probabilidad (fdp), mantenemos el peso relativo de cada una de las direcciones dentro de la celda (esto es, su probabilidad). La Figura 22 muestra un ejemplo de las diferencias entre uno y otro método. Como veremos en la sección de resultados, el uso de funciones densidad de probabilidad produce una mejora de los resultados obtenidos con el método del gradiente y en general con el resto de sistemas evaluados en los que incorporamos esta funcionalidad.

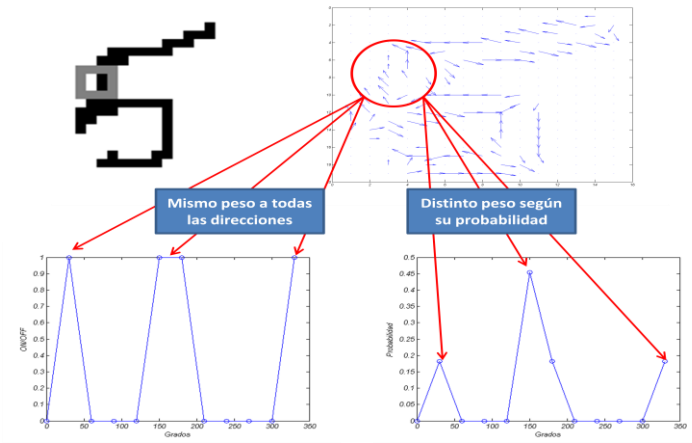


Figura 22. Comparación entre binarización y conversión a fdp de un histograma.

Para el cálculo de similitud entre dos muestras manuscritas de dos usuarios dados, para el caso de histogramas de direcciones binarizados, se utiliza la distancia Euclídea. Dados dos vectores binarios de características a y b con n componentes (n=192 en el caso del gradiente), su medida de distancia es:

$$d_{euclidea} = \sqrt{\sum_{i=1}^{n} a_i^2 - b_i^2}$$

Por otro lado, para el cálculo de distancias entre histogramas normalizados a función densidad de probabilidad, utilizaremos la distancia conocida como χ^2, la cual se ha demostrado que funciona mejor con este tipo de funciones [2]:

$$d_{X^2} = \sum_{i=1}^{n} \frac{(a_i - b_i)^2}{a_i + b_i}$$

4.2.2 Sistema basado en alógrafos

Este sistema obtiene características globales de las muestras. Es decir, obtiene el vector de características a partir de la imagen completa.
Este sistema de reconocimiento de escritor utiliza características a nivel de alógrafo [2]. Su funcionamiento está basado en la utilización de un catálogo común de imágenes de alógrafos (*codebook*), el cual contenga representaciones de las diversas formas de escritura (en nuestro caso, caracteres individuales o trazos de firma).
Cada escritor es considerado como un generador aleatorio de alógrafos, de manera que distintos escritores "hacen uso" de distintos alógrafos del *codebook*. Este distinto uso se cuantificará a partir de una función densidad de probabilidad (fdp) particular de cada escritor, que refleje con qué probabilidad se hace uso de cada uno de los alógrafos, siendo necesario, por tanto, el adecuado diseño del *codebook*. Para ello, el proceso se divide en dos grandes partes:

1. Generación de un catálogo representativo de grafemas o alógrafos.
2. Cálculo de la FDP de cada escritor, a partir de dicho catálogo. Esta función densidad de probabilidad nos indicará cuáles de los grafemas del catálogo son más utilizados por cada escritor, permitiendo discriminar entre diversos escritores y calcular tasas de acierto del sistema.

El catálogo representativo de alógrafos se genera mediante técnicas de agrupamiento (*clustering*). A grandes rasgos, el *clustering* nos permite, a partir de una gran cantidad de datos, obtener un conjunto reducido de elementos (llamados centroides o *clusters*) que sea una buena representación del conjunto inicial. En nuestro caso, este procedimiento nos permitirá obtener una reducida lista de alógrafos que serán utilizados como catálogo representativo de formas alográficas.

Los experimentos llevados a cabo con textos manuscritos, en este proyecto, se realizan utilizando caracteres individuales segmentados del texto de un sujeto dado. En este caso, la unidad alográfica de trabajo son los caracteres del alfabeto, esto es, los dígitos 0-9 y las letras a-z (minúsculas) y A-Z (mayúsculas). Para la generación del catálogo o *codebook*, haremos uso de una base de datos externa de caracteres, distinta de la base de datos que se usa para el reconocimiento. En la Figura 23, se muestra un ejemplo de *codebook* generado según este procedimiento.

Figura 23. Ejemplo de catálogo de alógrafos generado a partir de una base de datos de caracteres individuales manuscritos (tamaño 100 clusters).

Por otro lado, para los experimentos llevados a cabo con imágenes de firma, la unidad alógrafica de trabajo se calcula como sigue. Dada una imagen de firma (en su caja limítrofe), se aplica una ventana deslizante que vaya recorriendo la firma horizontal y verticalmente, permitiendo cierto solape a medida que se va moviendo. El proceso se muestra en la Figura 24. La unidad alográfica de trabajo en este caso serán los bloques extraídos siguiendo este procedimiento, descartando los que no tengan ningún trazo (esto es, bloques blancos).

Figura 24. Ejemplo de aplicación de una ventana deslizante a una firma (firma de 512x218, ventana de 32x32 con solape del 50%).

En la Figura 25, se muestra un ejemplo de codebook generado con este mecanismo a partir de una base de datos de imágenes de firma.

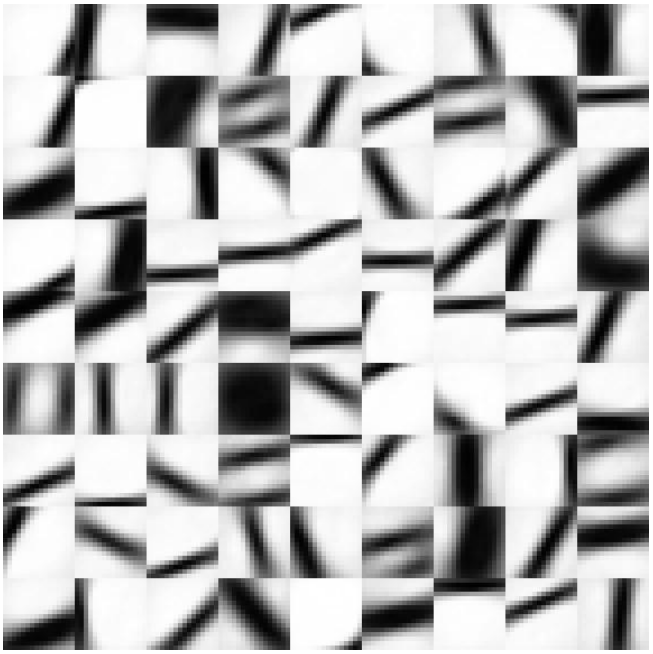


Figura 25. Ejemplo de catálogo de alógrafos generado a partir de una base de datos de imágenes de firma (tamaño 81 clusters, ventana deslizante de 16x16 con solape del 50%).

En este sistema, la característica identificativa de cada escritor será una función densidad de probabilidad construida a partir de la probabilidad de emisión de cada prototipo (*cluster*) del catálogo (*codebook*). Esta función densidad de probabilidad se generará a partir de un histograma en el que cada caja se corresponde con cada uno de los prototipos del catálogo. Para cada elemento alográfico extraído de una muestra manuscrita de un individuo, se busca el prototipo más cercano del catálogo (el ganador) utilizando la distancia euclídea entre las imágenes y esta distancia se acumula en la correspondiente caja del histograma. Finalmente, hecho esto para todos los elementos de un mismo usuario, el histograma se normaliza a una función densidad de probabilidad, siendo esta fdp la característica utilizada por el sistema de reconocimiento. Dadas las fdp de dos caracteres cualesquiera a comparar, la distancia entre dichos caracteres se calcula utilizando la distancia χ^2.

4.2.3 Sistema basado en características de contorno (*f*1, *f*2)

Este sistema obtiene características locales de las muestras. Es decir, divide las imágenes de las muestras de escritura en regiones y calcula un vector de características por región.
Este sistema opera en el nivel de análisis de textura de las imágenes. Las características de este sistema proporcionan información referente a la forma habitual de cada individuo de coger el bolígrafo y la inclinación preferente del trazo a la hora de escribir, junto con su curvatura. Asumimos que el escritor tiende a mantener estas características a lo largo del texto manuscrito independientemente del movimiento progresivo horizontal. A continuación se describen las fases de pre-procesado de la imagen y de extracción de estas características.

1. Preprocesado

Para los datos consistentes en imágenes de caracteres individuales, se realiza una interpolación de las imágenes escaneadas en escala de gris (caracteres con caja limítrofe) para convertirlas a una altura constante de 120 píxeles. Este paso es importante, ya que las imágenes originales de caracteres escaneadas en los experimentos de este Proyecto no poseen el tamaño suficiente para el correcto funcionamiento de este algoritmo [2]. No sucede lo mismo con las imágenes de firma utilizadas, puesto que están escaneadas a resolución suficiente.

A continuación, se realiza una binarización utilizando el método de Otsu [20], seguida de un proceso de apertura y otro de cierre. Los procesos de apertura y cierre consisten en realizar un ensanchado y un adelgazamiento de los trazos, respectivamente, y el objetivo de combinar ambos es el de eliminar el ruido presente en la imagen, así como rellenar los pequeños huecos a lo largo de los trazos con el fin de facilitar la posterior extracción del contorno. En la Figura 26, se puede observar este hecho.

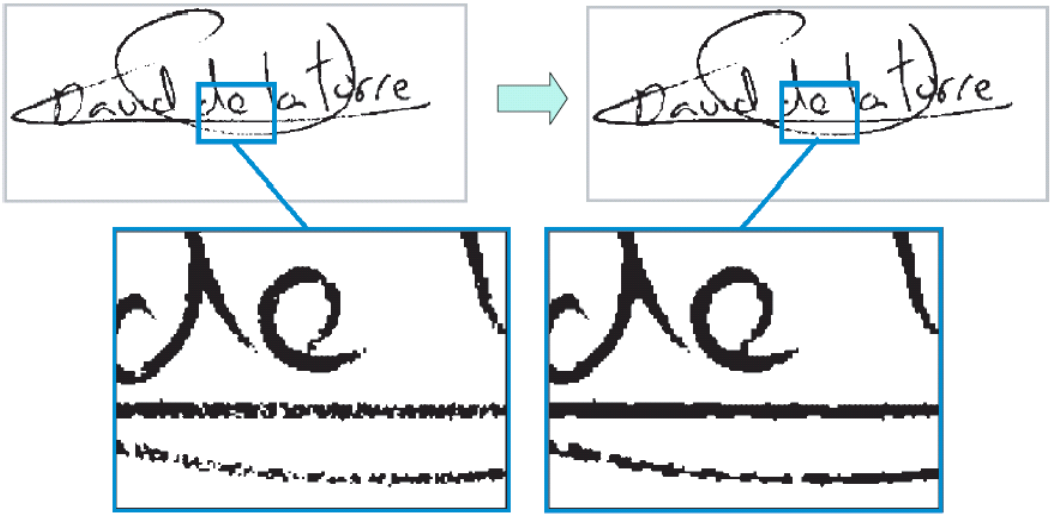


Figura 26. Eliminación de ruido tras efectuar una apertura seguida de cierre.

Por último, se extraen todos los contornos internos y externos de las componentes conectadas de la imagen. Para ello, se usa el algoritmo de seguimiento de contornos de Moore (Ver Figura 27). En este algoritmo se va recorriendo la imagen hasta encontrar un primer píxel del contorno, que se toma como punto de partida. Una vez encontrado este píxel, se busca un píxel de contorno a su alrededor siguiendo el sentido de las agujas del reloj y se repite este proceso hasta llegar de nuevo al píxel de partida por la misma posición desde la que se accedió a él al comenzar el algoritmo. El resultado es una secuencia ordenada con las coordenadas de todos los píxeles situados en el borde de los trazos. Esta representación vectorial, donde las coordenadas de los píxeles se almacenan seguidas en un vector, es muy efectiva, ya que permite un rápido procesamiento computacional de las características usadas en este apartado.

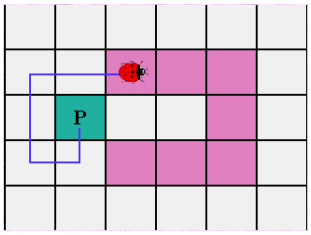


Figura 27. Funcionamiento del algoritmo de Moore.

2. Extracción de características

Para la extracción de características, se utilizará el vector con el contorno de los trazos obtenido de la sección anterior. En la Figura 28, muestra una tabla con un resumen de las mismas.

Característica	Nombre	Dimensiones (Ndims)	Calculada a partir de
f1	Dirección del contorno	12	Contornos
f2	Curvatura del contorno	300	Contornos

Figura 28. Tabla de las características de textura o de contorno.

Dirección del contorno (*f*1)

Una característica visual importante de los textos escritos que revela el estilo de escritura de cada individuo es la inclinación de los trazos. La distribución de probabilidad de las direcciones en la escritura proporciona información muy útil para el reconocimiento de escritor y puede ser calculada rápidamente utilizando el vector del contorno. La ventaja adicional de calcular la inclinación de los trazos usando este método es que se elimina la influencia del grosor del trazo de tinta.
Para extraer la distribución de esta característica, se utiliza la orientación de fragmentos locales del contorno. Cada fragmento se determina mediante dos píxeles del contorno situados a una cierta distancia ε uno del otro (Ver Figura 29). El ángulo que el fragmento forma con la horizontal se calcula mediante la siguiente expresión:

$$\phi = \arctan\left(\frac{y_{k+\varepsilon} - y_k}{x_{k+\varepsilon} - x_k}\right)$$

Mientras el algoritmo recorre el contorno, se va calculando la orientación de los fragmentos locales de contorno y simultáneamente se construye un histograma de ángulos. Más tarde dicho histograma se normaliza a una distribución de probabilidad, que indica la probabilidad de encontrar en una imagen un fragmento del contorno orientado con cada ángulo. Esta característica codifica información similar a la del gradiente, no obstante cada una utiliza una fuente diferente para extraer los datos de orientación de los trazos. Asimismo, el gradiente se aplica a la malla 4x4 de la imagen, mientras que esta característica *f*1 se calcula sobre la imagen completa. Para el cálculo de distancias entre vectores normalizados a función densidad de probabilidad, utilizaremos la distancia χ^2. En la Figura 30, se muestran algunos ejemplos de caracteres con su histograma calculado.

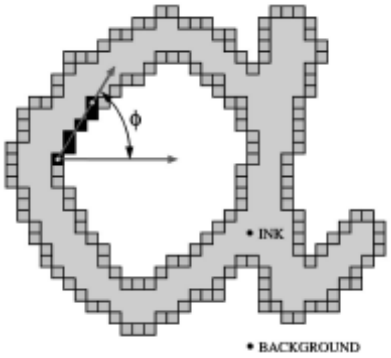


Figura 29. Extracción de la característica de dirección del contorno (f1).

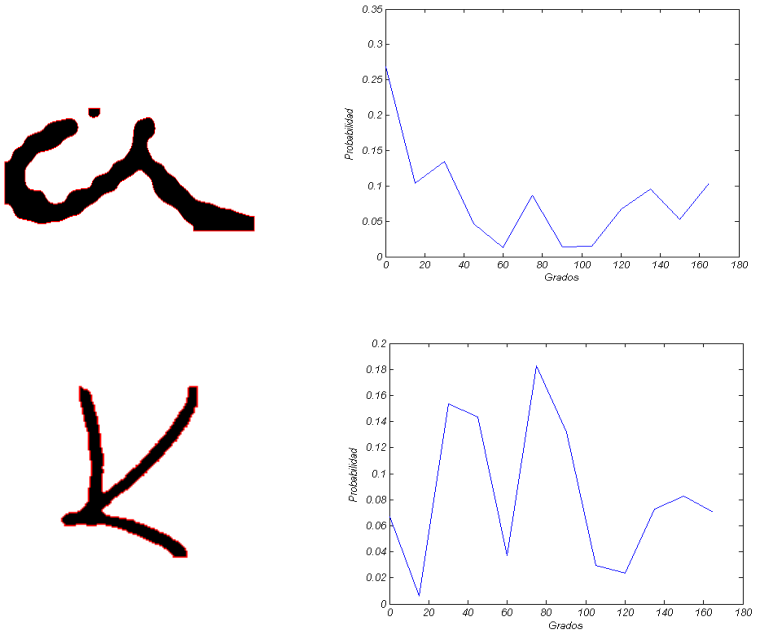


Figura 30. Ejemplos de extracción de la característica de dirección del contorno (f1) para dos caracteres.

Con el fin de controlar la longitud de los fragmentos de contorno analizados, se establece el parámetro ε, cuyo valor se ha fijado a ε=5 (a partir de recomendaciones de la literatura). Se considera que el ángulo reside en los dos primeros cuadrantes porque al no disponer de información dinámica acerca de la escritura, no se puede conocer la forma en la que el escritor trazó el contorno que se está analizando. Como consecuencia, el histograma se extiende dentro del intervalo de 0º a 180º, el cual se divide en *n*=12 secciones, con lo que cada una de ellas abarca un rango de 15º. Este rango proporciona una descripción suficientemente detallada y al mismo tiempo robusta de la escritura para el proceso de identificación del escritor. Estos valores también serán utilizados en la característica de dirección siguiente.

Curvatura del contorno (*f*2)

En esta característica, además de la orientación (característica *f1*), se captura la curvatura del trazo de tinta. La idea principal consiste en considerar dos fragmentos de contorno sujetos al mismo píxel en lugar de uno (Ver Figura 31), y calcular la distribución de probabilidad conjunta de las orientaciones de las dos ramas del contorno obtenido. Por tanto, por cada píxel del contorno se miden dos ángulos respecto a la horizontal y los resultados se van almacenando en un histograma bidimensional. Después se normaliza el histograma y se obtiene la función de distribución de probabilidad conjunta que cuantifica la posibilidad de encontrar en la imagen del carácter dos fragmentos orientados según los ángulos medidos y sujetos al mismo píxel. Para el cálculo de distancias entre vectores normalizados a función densidad de probabilidad, utilizaremos la distancia χ^2.

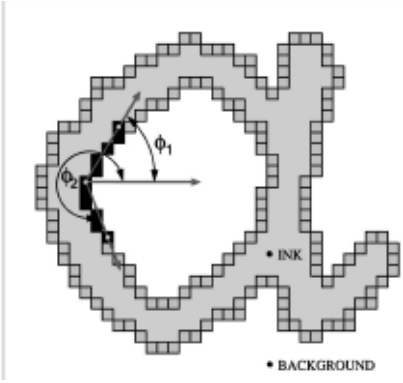


Figura 31. Extracción de la característica de curvatura del contorno (f2).

En este caso, es necesario extenderse por los cuatro cuadrantes (360º) alrededor del píxel de unión para calcular los ángulos de los dos fragmentos considerados. Como consecuencia, la orientación es cuantificada en *2n* direcciones por cada rama. Del total de combinaciones de los dos ángulos sólo se consideran aquellas no redundantes, es decir, las que cumplen la condición Ø1≤ Ø2. El resultado es un vector de características de 300 dimensiones.

4.3 Sistemas desarrollados en el marco de este PFC

Se presentan:

- Característica estructural: Obtiene la trayectoria de los trazos, medida a partir de los vecinos inmediatamente cercanos a un píxel.

- Características de concavidad: Obtienen la relación entre trazos, medida a partir de todos los píxeles de una celda 4x4 o de la imagen completa.

- Características geométricas: Obtiene un valor numérico calculado a partir de la imagen completa de la muestra.

4.3.1 Sistema basado en característica estructural

Este sistema obtiene características locales de las muestras. Es decir, dividen la imagen en regiones y calcula un vector de características por región.
Con este sistema, se intenta obtener la trayectoria de los trazos medida a partir de los vecinos inmediatamente cercanos a un píxel.

Las características desarrolladas en este caso revelan patrones en el mapa de gradiente de la imagen en forma de "mini-trazos". Estas características se calculan aplicando a cada pixel un conjunto de 12 reglas que operan sobre los 8 píxeles próximos (vecinos) (Figura 33). Cada regla busca un patrón determinado en los vecinos respecto a su gradiente extraído según se detalla en la Sección 3.2.1. Estas reglas se muestran en una tabla en la Figura 33. Como unidad de trabajo para estas características se utiliza cada una de las 4x4 celdas en las que se divide cada imagen (Ver Figura 32).

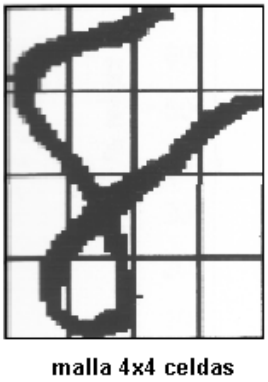


Figura 32. Malla de 4x4 para cálculo de características.

Regla	Descripción	Rango del Vecino 1		Rango del Vecino 2	
		Vecino	Direcciones	Vecino	Direcciones
1	Línea Horizontal, tipo 1	1	2,3,4	5	2,3,4
2	Línea Horizontal, tipo 2	1	8,9,10	5	8,9,10
3	Línea Vertical, tipo 1	3	5,6,7	7	5,6,7
4	Línea Vertical, tipo 2	3	1,0,11	7	1,0,11
5	Subida Diagonal, tipo 1	6	4,5,6	2	4,5,6
6	Subida Diagonal, tipo 2	6	10,11,0	2	10,11,0
7	Caida Diagonal, tipo 1	4	1,2,3	8	1,2,3
8	Caida Diagonal, tipo 2	4	7,8,9	8	7,8,9
9	Esquina 1	3	5,6,7	1	8,9,10
10	Esquina 2	7	5,6,7	1	2,3,4
11	Esquina 3	5	8,9,10	3	1,0,11
12	Esquina 4	7	1,0,11	5	2,3,4

Figura 33. Reglas para las características estructurales.

Para que se cumpla una regla, debe verificarse el rango del vecino 1 y el rango del vecino 2. Para que se verifique un rango debe cumplirse que el gradiente del vecino indicado tenga una de las direcciones indicadas.

Por ejemplo, fijándonos en la Figura 34, los vecinos 1 y 5 del píxel central cumplirán la regla 1. Esto es, la línea que pasa por el píxel será horizontal ya que los valores del gradiente por éste y por sus vecinos serán perpendiculares y, por tanto, tendrán dirección vertical (3), o casi (2,4).

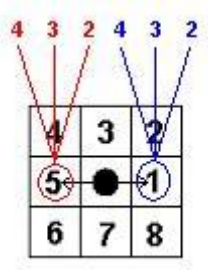


Figura 34. Cálculo de características estructurales en los 8 vecinos de un píxel.

Cada regla se cumplirá o no en cada píxel. Por cada celda, se generará un histograma de 12 elementos que indica cuántos píxeles de la celda de la malla 4x4 cumplen cada una de las 12 reglas. De nuevo, se hará un histograma por cada celda que se binarizará utilizando un umbral, de manera que se decide si cada regla se cumple (bit=1) o no (bit=0) en la celda. Como resultado, tendremos un vector de 12x4x4=192 componentes.

Para el cálculo del umbral de binarización, se proponen dos métodos en este proyecto:

- Un umbral diferente para cada celda, que se calcula como la media de los valores del histograma de esa celda.
- Un umbral global único para toda la imagen, que se calcula como la media de los valores de todos los histogramas juntos.

Como mejora a esta parte del sistema (no propuesta en la descripción original), se propone normalizar los histogramas a una función densidad de probabilidad en lugar de binarizarlos. Con un vector binario, concedemos la misma "importancia" a todas las direcciones (bit=1) con tal de que el histograma supere el umbral fijado. Por contra, con una función densidad de probabilidad, mantenemos el peso relativo de cada una de las reglas dentro de la celda (esto es, su probabilidad). Como ya se ha apuntado anteriormente, el uso de funciones densidad de probabilidad produce una mejora de los resultados obtenidos, mejora que se puede ver en el Capítulo de resultados.

4.3.2 Sistema basado en características de concavidad

Este sistema obtiene características locales de las muestras. Es decir, dividen la imagen en regiones y calcula un vector de características por región.
Con este sistema, se pretende obtener la relación entre trazos, medida a partir de todos los píxeles de una celda o de la imagen completa.
De la misma manera que con el sistema anterior, como unidad de trabajo para estas características se utiliza cada una de las 4x4 celdas en las que se divide cada imagen (Ver Figura 32).
Para este sistema, los datos se extraen a partir de la imagen binaria.
En este caso, se han implementado las siguientes características:

Característica de “Densidad de Punto Grueso”

Esta característica captura las agrupaciones de píxeles en la imagen. Para ello, se mide el número de píxeles negros en cada celda y se hace el histograma de la malla 4x4 completa. A continuación, se aplica un umbral de binarización que indique si en cada celda predominan (bit=1) o no (bit=0) los píxeles negros. Queda así un vector de características de 4x4 = 16 bits. En este caso, al tener un solo histograma, la única forma de binarización posible en la de usar la media de valores del histograma.

Al igual que antes, en este Proyecto, se propone comparar esta binarización con la aproximación del histograma a una función densidad de probabilidad, de manera que se cuantifique la relación relativa de píxeles negros entre cada celda.

Característica de “Trazo Largo”

Esta característica detecta trazos largos en horizontal o en vertical en la imagen. Para esto, se computan las longitudes de segmentos continuos sobre filas –trazos horizontales- o columnas –trazos verticales-. La idea es formular cada fila y columna en términos de secuencias de píxeles negros. Se hace así un histograma sobre toda la imagen de los posibles valores de longitud de los trazos y se fija un umbral óptimo. Si en una celda hay trazos horizontales de longitud mayor del umbral, determinaremos que en la celda hay trazos largos horizontales (bit=1), y lo mismo en la celda para el caso vertical. Estos dos indicadores sobre la malla 4x4 nos da un vector total de 4x4x2 = 32 elementos.
Para el cálculo del umbral de binarización, se proponen dos métodos al igual que en las características estructurales:

- Un umbral diferente para cada celda, que se calcula como la media de longitudes de los segmentos de esa celda.
- Un umbral global único para toda la imagen, que se calcula como la media de longitudes de todos los segmentos de la imagen.

La característica de trazo largo mide longitudes de segmentos y al ser variable el tamaño de las imágenes de caracteres y firmas, también lo sería el rango de los histogramas, de manera que para este trabajo no se ha abordado la conversión del histograma a función densidad de probabilidad.

4.3.3 Sistema basado en características geométricas

Este sistema obtiene características globales de las muestras. Es decir, obtiene el vector de características a partir de la imagen completa.
Para el desarrollo de este sistema se han implementado 5 características (*f1, f2, f3, f4,* y *f5*) que miden propiedades geométricas de la letra.
Estas características se obtienen a partir de la imagen completa (también binarizada), al contrario que las anteriores características que se calculaban por celda.

Además, este tipo de características se han evaluado solamente con datos de caracteres individuales, no así con imágenes de firmas.

Denotamos cada pixel de la imagen binarizada como B(i,j), siendo:

- $B(i,j) = 0$ white pixel (fondo).
- $B(i,j) = 1$ black pixel (trazo).

La primera de estas características es el porcentaje de píxeles negros de la imagen:

$$f1(\#black\ pixels) = 100 \times [\sum_i \sum_j B(i,j)\ ] /tamaño\ imagen$$

Ahora, siendo l(left), r (right), t (top) y b (bottom) los pixels negros extremos por las cuatro direcciones que sus nombres indican (ver Figura 35) se definen las siguientes características.

La segunda característica geométrica nos mide la relación de aspecto de la imagen:

$$f2\ (height - width\ ratio) = \frac{r-l+1}{b-t+1} = \frac{ancho\ imagen}{alto\ imagen}$$

Para obtener la tercera y la cuarta característica, se define el centroide de la imagen como *centroid(m_i ,mj)*:

$$m_i = \frac{\sum_i \sum_j i\ B(i,j)}{\sum_i \sum_j B(i,j)}$$

$$m_j = \frac{\sum_i \sum_j j\ B(i,j)}{\sum_i \sum_j B(i,j)}$$

Así, obtenemos:

$$f3\ (centroid\ height\ ratio) = \frac{m_i - l + 1}{b-t+1} = \frac{ancho\ centroide}{alto\ imagen}$$

$$f4\ (centroid\ width\ ratio) = \frac{m_j - l + 1}{r-t+1} = \frac{alto\ centroide}{ancho\ imagen}$$

Por otro lado, se forma un sensor espacial en la forma de una rejilla de 3x3 puntos equidistantes sobre la imagen como se muestra en la Figura 35, y centrado en

$$center\ (c_i, c_j) = (\frac{b-t+1}{2}, \frac{r-l+1}{2})$$

Así, la quinta característica mide la distancia entre el pixel negro más cercano y los 9 puntos del sensor (Ver Figura 35):

$$f5\ (9\ spatial\ sensor\ distance) = \sum_{S1}^{S9} d(S_x\ , B(i,j))$$

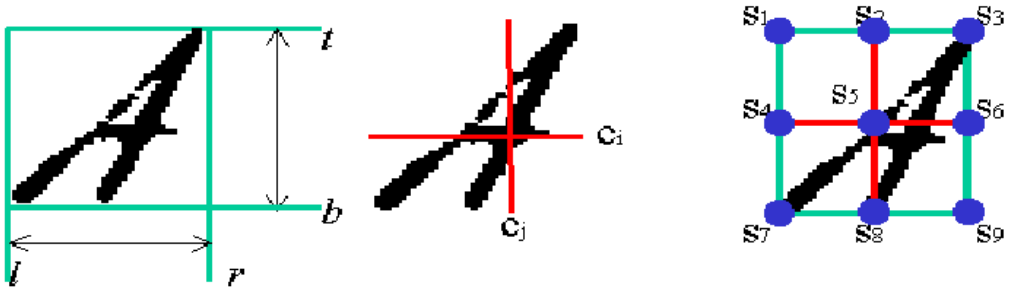


Figura 35. Ejemplos de características geométricas.

Para este sistema, es imposible la conversión de los resultados a función densidad de probabilidad puesto que los valores obtenidos no se pueden expresar de esta manera debido a que no son distribuciones de valores sino un valor numérico concreto.

Capítulo 5

EXPERIMENTOS EN IDENTIFICACIÓN DE ESCRITURA

5.1 Base de datos

Para el reconocimiento de individuos a partir de textos escritos, se ha hecho uso de una base de datos de documentos forenses reales del Laboratorio de Grafística de la Dirección General de la Guardia Civil (DGGC), proporcionada como parte de las actividades de investigación del grupo ATVS en las cuales se ha desarrollado este Proyecto.

Para cada individuo de la base de datos, se escanean los documentos manuscritos disponibles del mismo a 300 dpi y se extraen manualmente un conjunto de muestras representativas de cada uno de los caracteres del alfabeto haciendo uso de una herramienta software disponible en la DGGC (Ver Figura 36). Se definen un total de 62 caracteres posibles: mayúsculas A-Z, minúsculas a-z y los dígitos 0-9.

Por cada tipo de letra para un individuo dado, el operador intenta capturar una media de unas 3-5 muestras lo más limpias posibles, evitando ruido de fondo (cuadrículas del papel, manchas, sellos, otras tipografías automáticas o manuales, etc.). Hay que tener en cuenta que, dada la naturaleza de los manuscritos de la base de datos, no siempre será posible extraer este número, e incluso en algún caso puede que no haya muestras de algún tipo de letra. Una vez se tiene la imagen de la letra, se aplica una binarización usando el algoritmo de Otsu [20]. Finalmente los márgenes en blanco se suprimen en torno a la letra calculando su caja limítrofe. La Figura 37 muestra un ejemplo del conjunto de letras y números de un individuo registrado en la base de datos siguiendo este procedimiento. Dicho procedimiento, junto con el protocolo experimental de la Sección 4.2 forma parte de la operativa de trabajo del Laboratorio de Grafística de la DGGC. Entre las contribuciones de este Proyecto está la evaluación de un conjunto de sistemas bajo estas condiciones de operación, así como de su fusión.

La base de datos completa usada en este Proyecto contiene 9297 muestras de caracteres de 30 escritores distintos, con unas 300 muestras de media por escritor separadas en datos de entrenamiento y de test. Para cada escritor, los datos de entrenamiento y de test se han extraído de documentos diferentes, lo que quiere decir que se “capturaron” en diferentes momentos. Los datos de entrenamiento de cada escritor se almacenan en la base de datos del sistema, siendo los datos de identidades conocidas por el sistema. Por otro lado, los datos de test se utilizarán para simular búsquedas en la base de datos, con el fin de evaluar el rendimiento del sistema a la hora de asignarles la identidad correcta.

Por su naturaleza, la base de datos no contiene un número uniforme de muestras por carácter o por usuario, ni el tiempo entre los datos de entrenamiento y test es constante para cada escritor. La Figura 38 muestra la distribución de caracteres por usuario y por muestra de la base de datos.

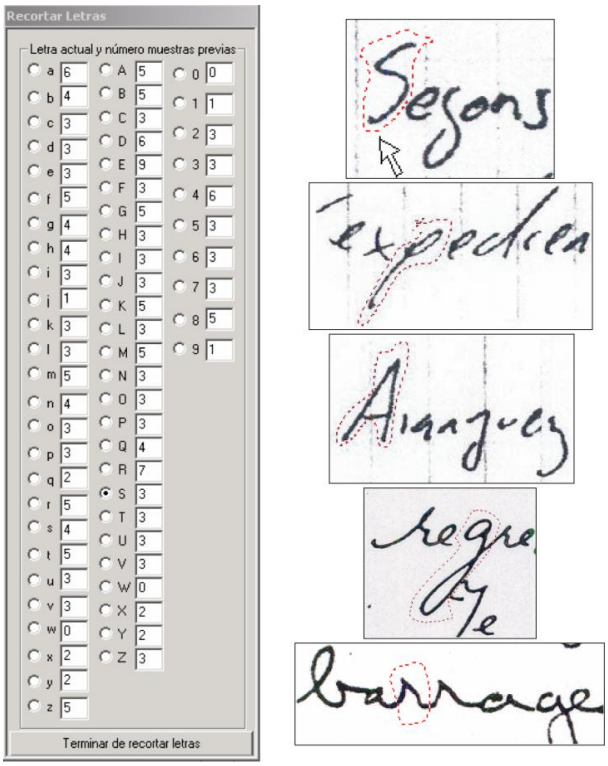


Figura 36. Izquierda: las 62 clases de caracteres definidas en la base de datos forense de textos manuscritos usada en este Proyecto (mayúsculas A-Z, minúsculas a-z, dígitos 0-9). Derecha: selección manual de caracteres individuales con la herramienta software dedicada.

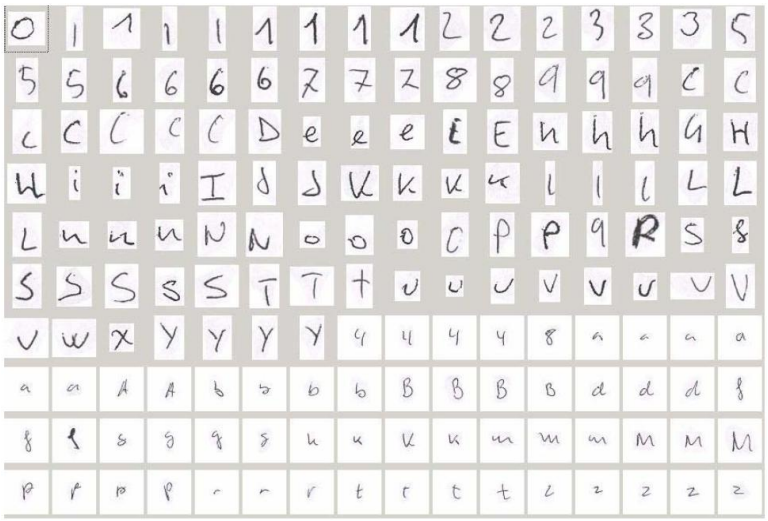


Figura 37. Ejemplo de muestras (letras y números) de un individuo de la base de datos forense de textos manuscritos usada en este Proyecto.

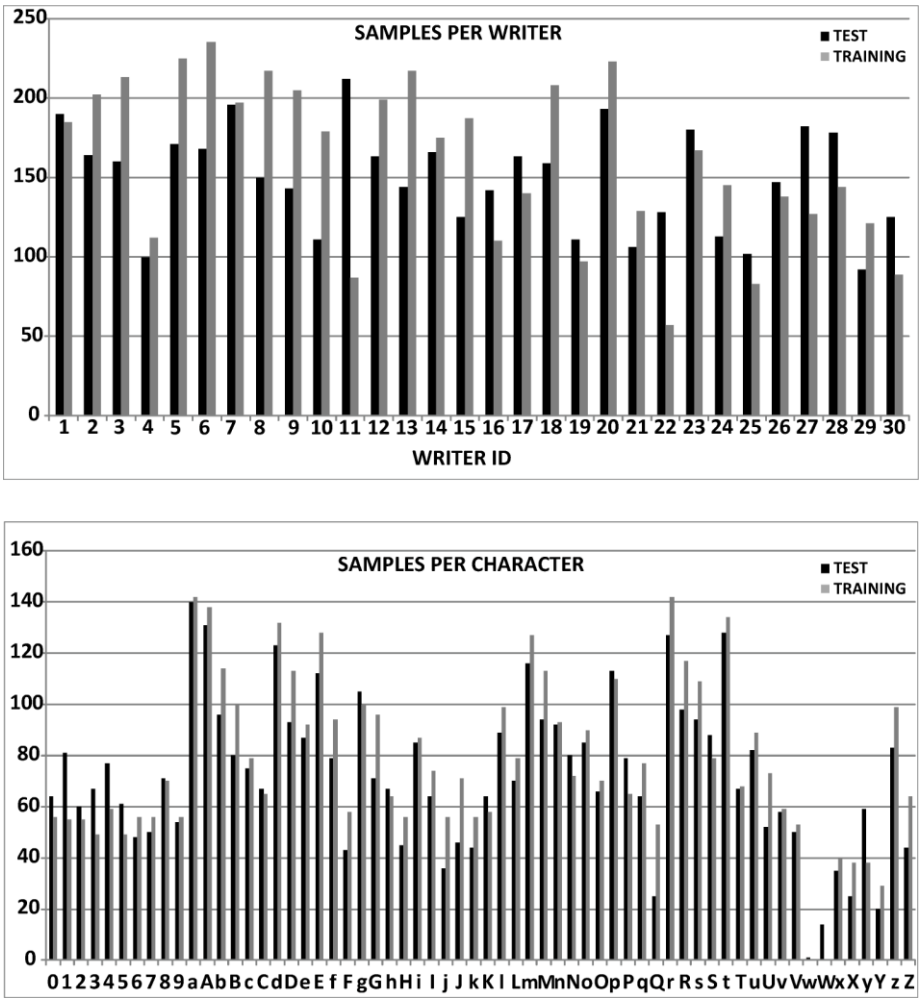


Figura 38. Distribución de muestras por escritor (arriba) y por carácter (abajo) de la base de datos forense de textos manuscritos usada en este Proyecto.

5.2 Protocolo experimental

Para los experimentos de reconocimiento a partir de textos manuscritos usando la mencionada base de datos forense, se han evaluado los sistemas funcionando en modo identificación. Así, para reconocer a un individuo, se comparan sus datos de test con todos los datos de entrenamiento de los sujetos existentes en la base de datos. Como resultado, se devuelve una lista ordenada de identidades de la base de datos de tamaño *N*. Idealmente, la primera posición (Top 1 ó *N*=1) debe corresponder con la identidad correcta, pero es posible considerar una lista mayor (por ejemplo, Top 10 ó *N*=10) para aumentar la probabilidad de que la identidad correcta se encuentre en ella. Se considerará que una identificación es exitosa si la identidad correcta se encuentra entre las *N* devueltas. Esta es la operativa habitual de funcionamiento en sistemas forenses, puesto que normalmente el individuo de identidad desconocida no solicita una identidad pretendida (esto es, no desea ser reconocido), de modo que hay que hacer una búsqueda sobre toda la base de datos.
El beneficio de los sistemas biométricos automáticos en este caso consiste en acotar la búsqueda de la identidad desconocida entre una lista reducida de tamaño *N* devuelta por el sistema. A continuación, el experto forense se centra solamente entre las *N* identidades para efectuar el cotejo manual, en lugar de tener que hacerlo sobre la base de datos completa.

Para la identificación con un sistema dado, se realiza una identificación parcial para cada uno de los 62 canales (esto es, caracteres) en que se separan las muestras de cada individuo, tomando una decisión para cada uno de ellos. Para cada canal, por tanto, se obtiene una decisión de cuál es la identidad correcta de la base de datos. A continuación, se aplica una fusión de datos a nivel de decisión utilizando una estrategia de votación por mayoría, de manera que el primer candidato de la base de datos será el que ha resultado ganador de la decisión parcial en el mayor número de canales, el segundo el que siguiendo el mismo criterio ha quedado en segundo lugar, y así sucesivamente.

Para la identificación parcial de cada uno de los 62 canales, se aplica también una decisión por mayoría entre todas las muestras disponibles en el canal en cuestión. Dado el número de muestras por canal (idealmente entre 3 y 5 por usuario) es posible que sucedan empates en la votación (por ejemplo, si hay cuatro muestras, en dos de ellas “gana” una identidad y en las otras dos “gana” otra). Cuando esto sucede, se calcula la distancia media entre muestras para cada una de las identidades ganadoras, asignando la de menor distancia media. Por ejemplo:

Muestra	Identidad ganadora por el sistema	Distancia asignada
1	A	0.1
2	B	0.2
3	B	0.2
4	A	0.12

En este caso, para la identidad A tenemos una distancia media de (0.1+0.12)/2=0.11, mientras que para la B tenemos (0.2+0.2)/2=0.2, resultando que la identidad de menor distancia media es la A. Por tanto, asignaremos la identidad A como ganadora del canal en cuestión.

5.3 Resultados

El objetivo que se persigue consiste en comprobar qué sistema proporciona mejor rendimiento en el escenario forense propuesto. Dentro de cada sistema, se han evaluado también una serie de mejoras no contempladas en la descripción original de los mismos. Por último, se ha evaluado también la fusión de los sistemas evaluados, a fin de valorar en beneficio obtenido con dicha combinación.

5.3.1 Resultados de los sistemas disponibles evaluados

5.3.1.1 Sistema basado en características de gradiente

Para el gradiente, se propuso la evaluación de las siguientes alternativas, cuyos resultados se muestran en la Figura 38:

- sin binarizar/binarizando la imagen para calcular el gradiente
- usando histogramas binarizados por umbralización vs. normalizados a función densidad de probabilidad (FDP)

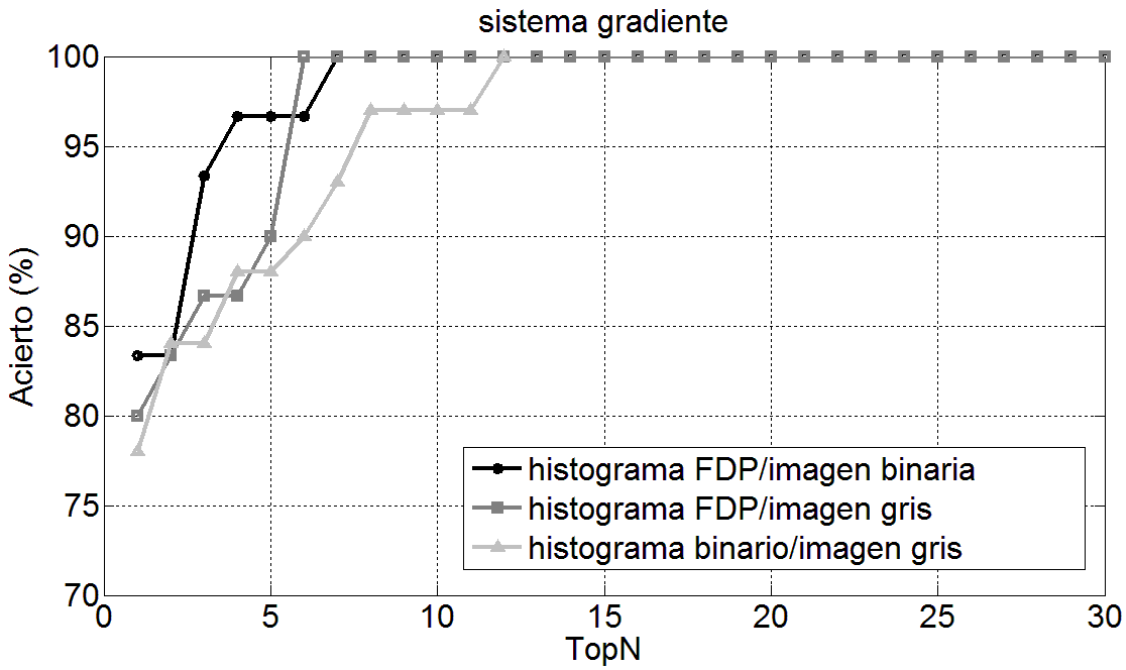


Figura 39. Resultados del sistema basado en características de gradiente.

En la Figura 39, observamos que el uso de histogramas normalizados a función densidad de probabilidad (FDP) mejora las tasas de identificación (curva gris clara frente a curva gris oscura). Asimismo, utilizar imágenes binarias para la extracción del gradiente supone una mejora extra en los resultados, acercándonos al 94% de tasa de acierto con una lista de tan solo tres candidatos (Top 3, curva negra). La binarización produce un realce en los bordes del carácter, por lo que la magnitud del gradiente (esto es, su "fuerza") es mayor, siendo su extracción por tanto más fiable. Por último, notar que con este sistema obtenemos una tasa de acierto del 100% con una lista de 6-7 candidatos.

5.3.1.2 Sistema basado en alógrafos

La configuración utilizada en el sistema de alógrafos procede de un ajuste realizado en otro Proyecto dentro del grupo ATVS. En el presente Proyecto solamente mostraremos la configuración óptima encontrada, la cual se usará para su comparación con el resto de características y para la fusión.

El catálogo o codebook representativo de caracteres individuales se ha generado a partir de muestras de la base de datos CEDAR [25], de acceso público. Las imágenes de dicha base de datos se extrajeron de un conjunto de direcciones y códigos postales recogidos en la Oficina Postal de Buffalo (EE.UU.) a partir de escaneos de envíos reales del servicio postal de dicha oficina, conteniendo muestras de caracteres alfanuméricos y dígitos segmentados de forma manual a partir de las direcciones y códigos postales. De esta manera, la base de datos utilizada para generar el codebook es independiente de la base de datos de evaluación del sistema, mientras que por otro lado, procede también de muestras representativas de documentos reales, no adquiridos bajo condiciones de laboratorio. El conjunto de caracteres segmentados usado en este Proyecto consiste en 27837 caracteres alfanuméricos sacados de bloques de dirección postal y 21179 caracteres numéricos sacados de códigos postales.

A grandes rasgos, para optimizar este sistema, se ha buscado un codebook óptimo para cada uno de los 62 canales alfanuméricos, de manera que en realidad se tendrán 62 sub-codebooks. Cada sub-codebook se ha optimizado variando el número de clusters y obteniendo las tasas de acierto de cada canal para una lista de tamaño *N*=1 (Top 1). El número de clusters óptimo será el que produzca la mayor tasa de acierto en cada canal. En la Figura 40, se muestran ejemplos de sub-codebooks óptimos para algunos de los caracteres. Finalmente, se efectúa la combinación de los 62 canales. Los resultados obtenidos siguiendo este procedimiento se muestran en la Figura 41. Observamos que los resultados obtenidos con este sistema son algo peores que con el gradiente (tasa de acierto del 90% para Top3 y tasa de acierto del 100% para una lista de 10 candidatos).

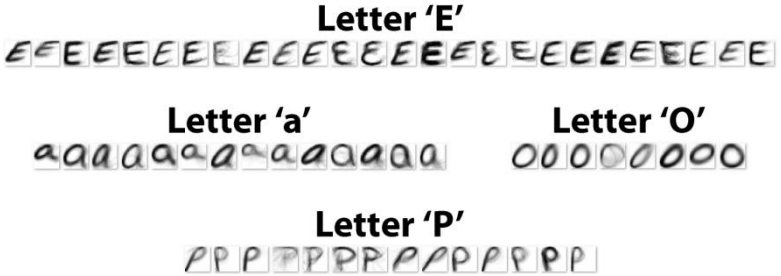


Figura 40. Ejemplos de sub-codebooks óptimos para algunos caracteres de escritura.

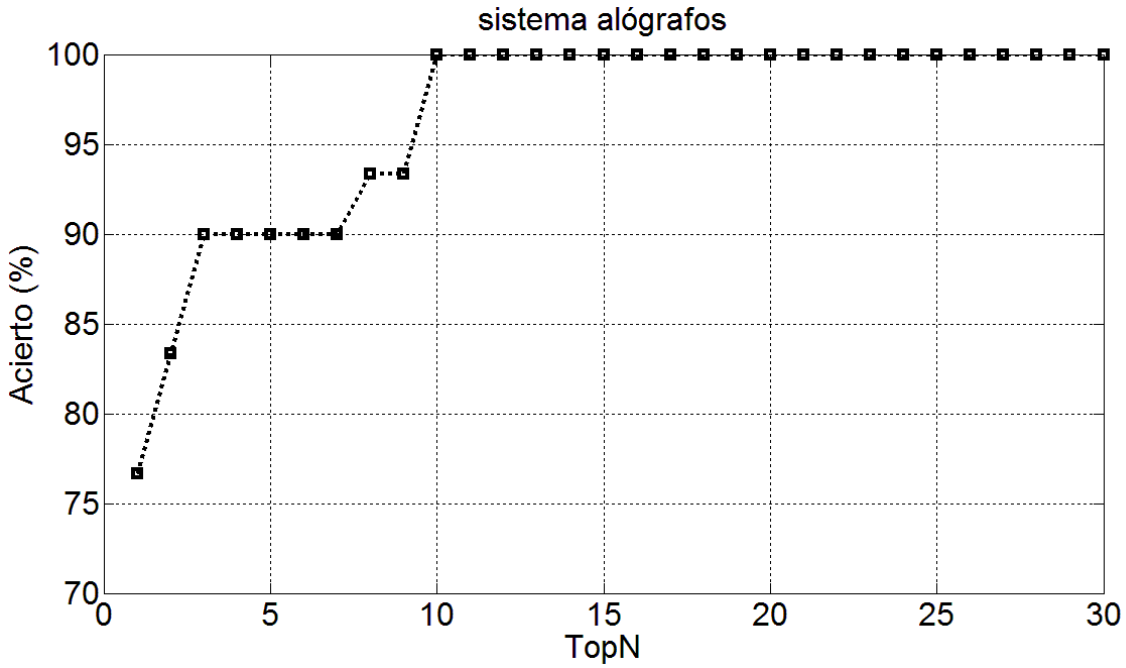


Figura 41. Resultados del sistema basado en alógrafos.

En este caso, se observa que se obtiene un 100 % de acierto con una la lista de candidatos de 10. Esto implica que este sistema funciona peor que el sistema basado en características de gradiente, pero aún así, los resultados son relativamente buenos. Esto es así debido a que la optimización de de los *sub-codebooks* variando el número de *clusters*, así como la combinación de los 62 canales, consigue una correcta caracterización de cada usuario indubitado.

5.3.1.3 Sistema basado en características de contorno

En la Figura 42, se muestra el rendimiento de estas dos características ($f1$ y $f2$). Se observa una clara superioridad de la característica $f2$, la cual, adicionalmente a la orientación del contorno codificada por $f1$, captura también su curvatura. El rendimiento, en cualquier caso, es sensiblemente peor que las dos características anteriores (gradiente y alógrafos).

Se observa asimismo un efecto importante con ambas características: no se consigue una tasa de acierto del 100% ni cuando la lista de candidatos devuelta es del tamaño de la base de datos completa (Top 30), sino que el máximo acierto es del 96.67%. Eso significa que hay un usuario de test para el cual no se asigna su usuario de la base de datos en ninguno de los 62 canales. La menor capacidad identificativa observada en general para estas características con nuestra base de datos puede ser una explicación para este hecho, sugiriendo la exploración de mejoras que conduzcan a un mayor rendimiento de las mismas.

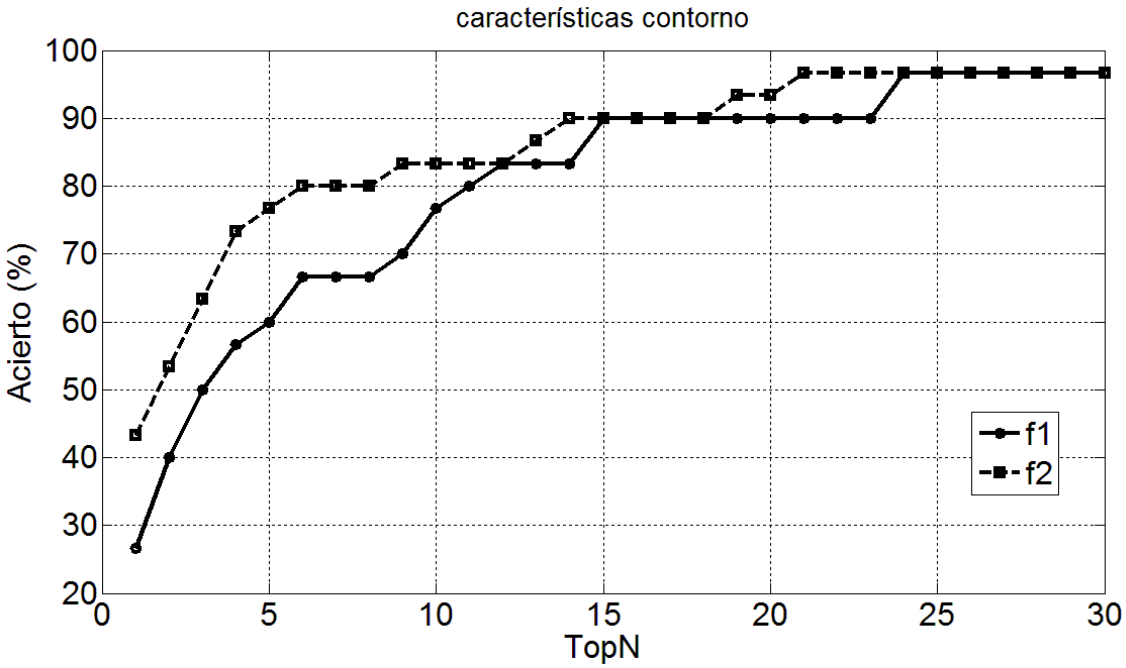


Figura 42. Resultados del sistema basado en características de contorno.

Como se observa en los resultados, la característica *f*2 funciona mejor que *f*1. Esto es debido a que *f*2 calcula la orientación del contorno y la curvatura, a diferencia de *f*1 que únicamente calcula la orientación del contorno. Por tanto, esta superioridad en los resultados por parte de *f*2 se debe a que ésta es más completa.

Por otro lado, se observa que los resultados obtenidos con estas características en ningún caso llegan a un 100 % de tasa de acierto. Esto implica que a algún usuario dubitado no es identificado, es decir, no se le asigna ninguno de los usuarios dubitados en ninguno de los 62 canales. Este efecto no se observa por ejemplo en el trabajo donde se propusieron estas características [2] en el cual la evaluación se efectúa usando una base de datos de laboratorio donde se pide a los usuarios que contribuyan con escritos formados por varias líneas de texto. Por tanto, la limitación en la cantidad de datos del escenario forense real de operación de este Proyecto, donde no es posible controlar la extensión de texto disponible de cada usuario, es una característica importante a la hora de obtener el rendimiento de los sistemas.

5.3.2 Resultados de los sistemas desarrollados en el marco de este PFC

5.3.2.1 Sistemas basados en características estructural, de concavidad y geométricas

Dentro de estas características tenemos la característica estructural, la de punto grueso, la de trazo largo y las geométricas. Para algunas de ellas se han propuesto varias alternativas que se indican en la tabla de la Figura 43. En las Figuras 44 – 46, se muestran los resultados para las distintas condiciones propuestas. Las características etiquetadas "estructural1" y "trazo largo1" se refieren a la umbralización de histograma por celda, mientras que "estructural2" y "trazo largo2" se refieren a la umbralización de histograma por imagen completa.

Al igual que observamos con el gradiente, el uso de histogramas normalizados a función densidad de probabilidad (FDP) mejora las tasas de identificación de las características que lo implementan aquí (estructural y punto grueso, comparar Figura 44 respecto a 46). De hecho, en todas las características que hacen uso de histogramas binarizados (Ver Figura 44), se observa también que no se alcanza una tasa de acierto del 100% ni para el Top 30. En este caso, el uso de histogramas normalizados a FDP proporciona la mejora adicional necesaria para solventar este efecto que no se obtenía en las características de contorno de la Sección 4.3.1.3 anterior.

En cuanto a la umbralización de histograma llevada a cabo en las características estructural y trazo largo, en esta última resulta claramente superior la umbralización por imagen completa (curva "trazo largo2" en la Figura 44). En la característica estructural sucede lo contrario, funciona mejor la umbralización por celda. Por otro lado, destacar el bajo rendimiento de las características geométricas. Solo la combinación de las mismas permite alcanzar un rendimiento parecido a alguna de las otras características GSC de este apartado, aunque en ningún caso se acerca al de las mejores. El entorno forense de escasez de datos mencionado, junto con el reducido tamaño del vector de datos de características geométricas (5 elementos por letra), hacen que su rendimiento esté muy por debajo de otras características con vectores de datos mayores.

Característica	Opciones evaluadas
Estructural	• para histograma binarizado: umbral de binarización global vs. umbral de binarización por celda 4x4 • uso de histograma binarizado por umbralización vs. normalizado a función densidad de probabilidad
punto grueso	• uso de histograma binarizado por umbralización vs. normalizado a función densidad de probabilidad
trazo largo	• para histograma binarizado: umbral de binarización global vs. umbral de binarización por celda 4x4

Figura 43. Opciones evaluadas en las características GSC desarrolladas en este Proyecto.

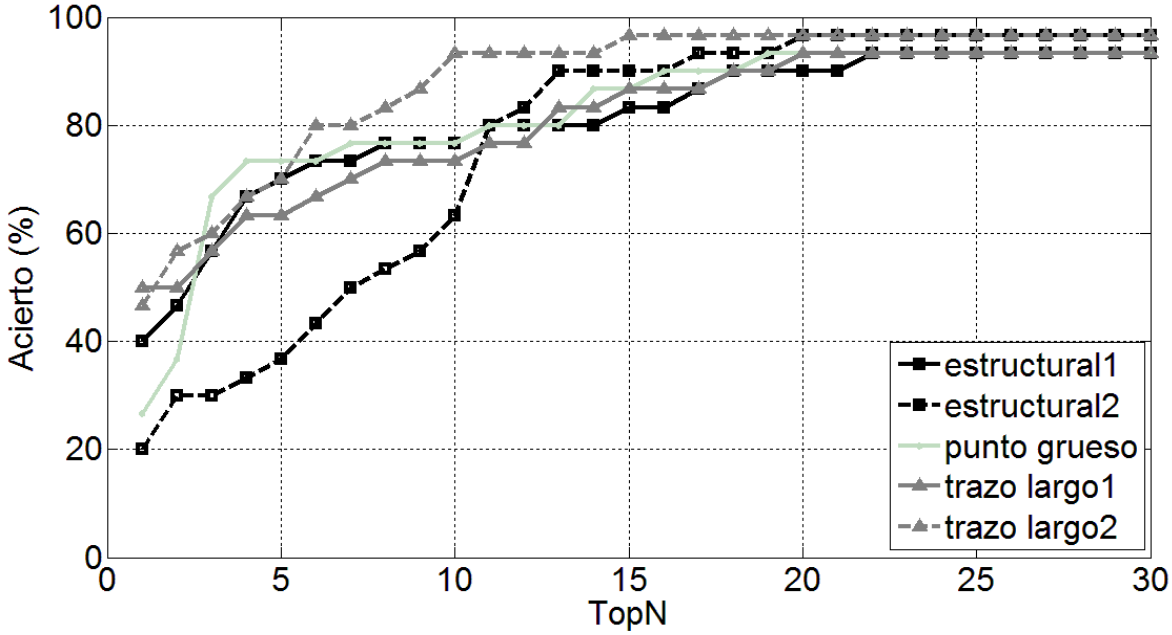


Figura 44. Resultado características (vectores binarios).

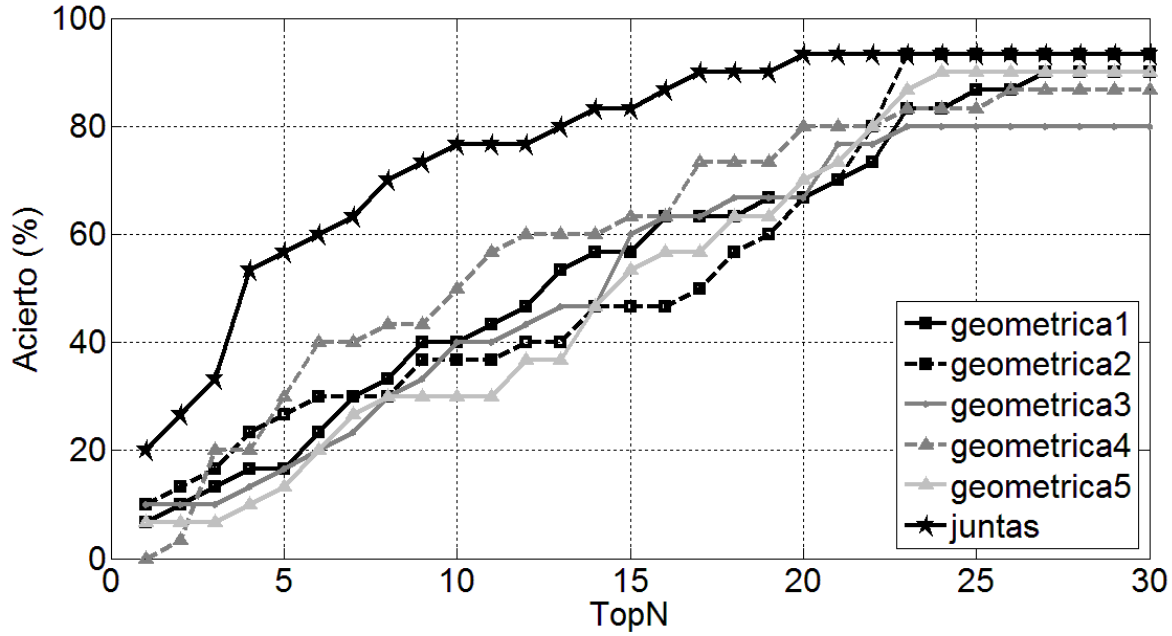


Figura 45. Resultado características (vectores binarios).

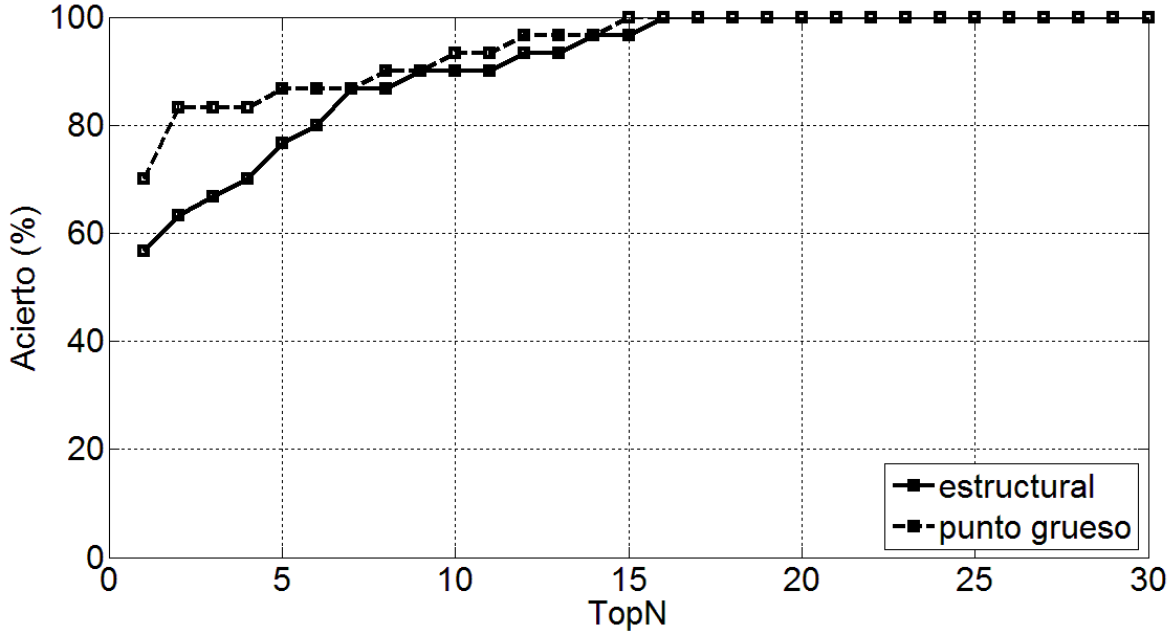


Figura 46. Resultado características (vectores densidad de probabilidad).

5.3.3 Fusión de características

En este apartado evaluaremos la fusión de los sistemas anteriores. La Figura 47 muestra la mejor configuración encontrada para los mismos en los apartados anteriores, esto es:

- GRADIENTE: con binarización de imagen e histograma FDP
- ALÓGRAFOS: optimización externa
- DE CONTORNO: característica *f*2.
- ESTRUCTURAL: con histograma FDP
- PUNTO GRUESO: con histograma FDP
- TRAZO LARGO: con histograma binario y umbralización por imagen completa ("trazo largo 2")
- GEOMÉTRICAS: combinación de todas las características

La Figura 47 nos permite comparar mejor el rendimiento relativo entre cada uno de los sistemas individuales. Así, por ejemplo, el mejor rendimiento se observa con el sistema del gradiente, seguido por el de alógrafos y el de punto grueso. Alejados de estos sistemas, con un rendimiento parecido, tenemos a continuación el estructural, el de trazo largo y el de contorno *f*2. Por último, con un rendimiento mucho peor que los demás, se sitúan las características geométricas.

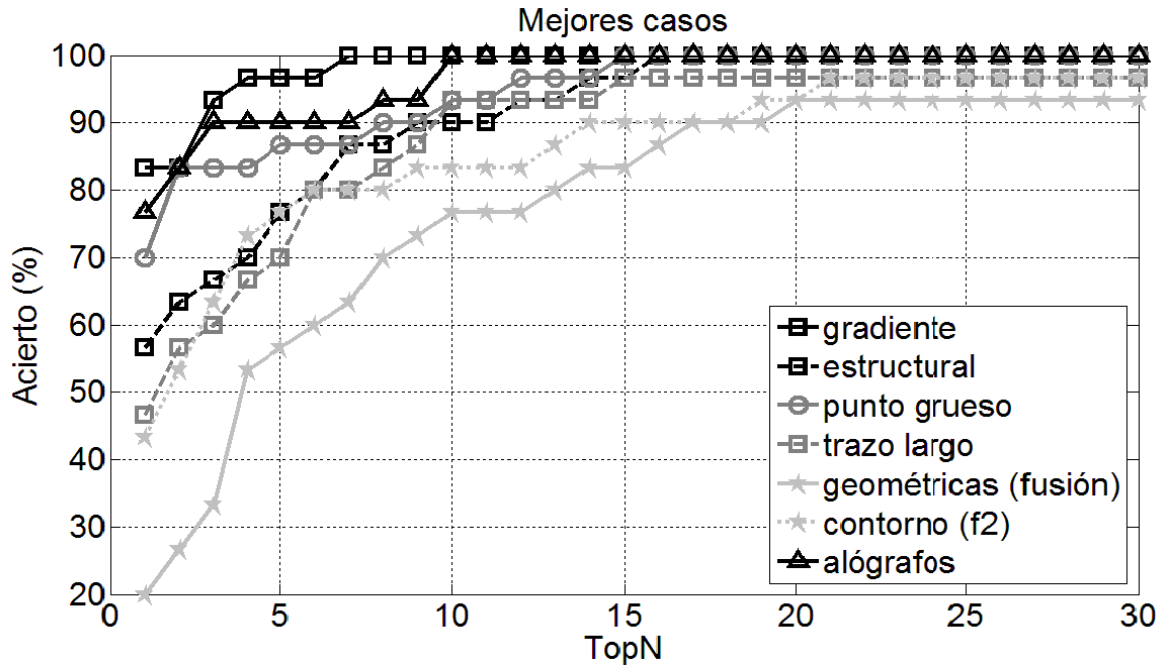


Figura 47. Rendimiento de los sistemas individuales para la mejor configuración de los mismos.

Las pruebas de fusión se han efectuado a nivel del número de canales asignados a cada usuario de la base de datos. Dado un usuario de entrada (de identidad desconocida), para cada usuario registrado en la base de datos del sistema se obtiene un número de canales ganadores, siendo el primer candidato el que resulte ganador en la mayoría de canales, el segundo candidato el que resulte en segundo lugar y así sucesivamente.

Cuando disponemos de más de un sistema, cada uno nos proporciona un número de canales ganadores a cada usuario de la base de datos. La fusión aplicada en este proyecto consiste en:

Si en algún sistema se asignan 0 canales a un usuario	➔	se asigna cero
En caso contrario	➔	se asigna la media

Con este esquema de fusión propuesto, si un sistema "opina" que un usuario de la base de datos tiene cero canales ganadores, se descarta la información del resto de sistemas. En caso contrario, se promedia por igual la opinión de cada sistema. En la Figura 46, se muestra el rendimiento fusionando el sistema del gradiente (el de mejor rendimiento individual) con el resto de sistemas. Asimismo, en la Figura 47 se muestra el rendimiento fusionando los sistemas del gradiente y alógrafos (los dos de mejor rendimiento individual) con el resto.

En la Figura 48, observamos que la fusión mejora sustancialmente al sistema del gradiente, mostrando los beneficios de la misma. En particular, la fusión del sistema del gradiente con alógrafos obtiene una tasa de acierto del 100% solamente con 3 usuarios. Asimismo, la fusión del gradiente con punto grueso también supone una mejora sustancial en Top1 y Top2, teniendo el mismo rendimiento que el gradiente para el resto de valores de Top. En este sentido, la fusión nos está permitiendo asegurar que el usuario correcto se sitúa con muy alta probabilidad en las dos o tres primeras posiciones del Top.

Si nos fijamos en una fusión de un mayor número de sistemas (Ver Figura 49), el rendimiento no mejora especialmente (incluso se alcanza el 100% en Top4 en lugar de Top3). Es importante resaltar no obstante que en Top1 obtenemos ya un rendimiento cercano al 94% cuando fusionamos los sistemas de gradiente, alógrafos y punto grueso, mejorando en este caso la fusión de solo dos sistemas. En definitiva, observamos que con la fusión de sistemas podemos alcanzar unas tasas de acierto muy elevadas para un tamaño de Top pequeño.

A la hora de analizar estos resultados, hay que considerar el reducido tamaño de la base de datos (30 usuarios), de modo que una diferencia pequeña en los porcentajes de acierto no resulta significativa. No obstante, permite observar tendencias de mejora tanto con la implementación de nuevas técnicas dentro de cada sistema individual así como con la fusión de los mismos.

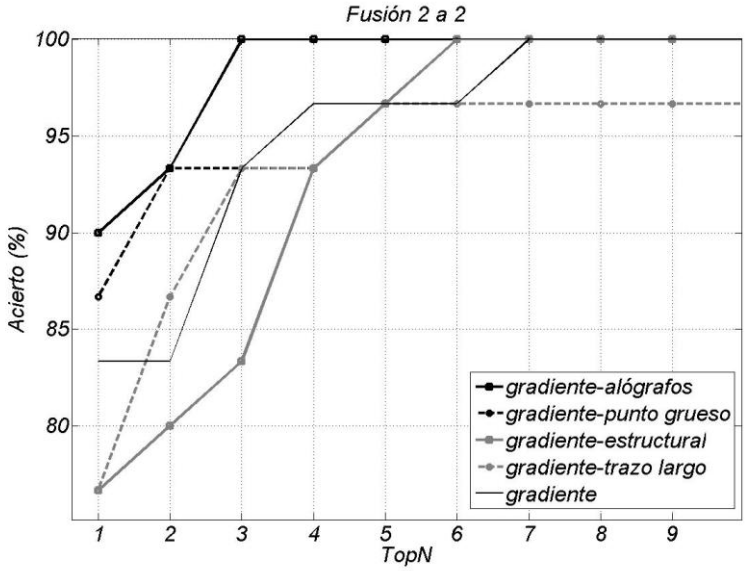


Figura 48. Rendimiento de la fusión del sistema de gradiente (el de mejor rendimiento individual) con el resto de sistemas.

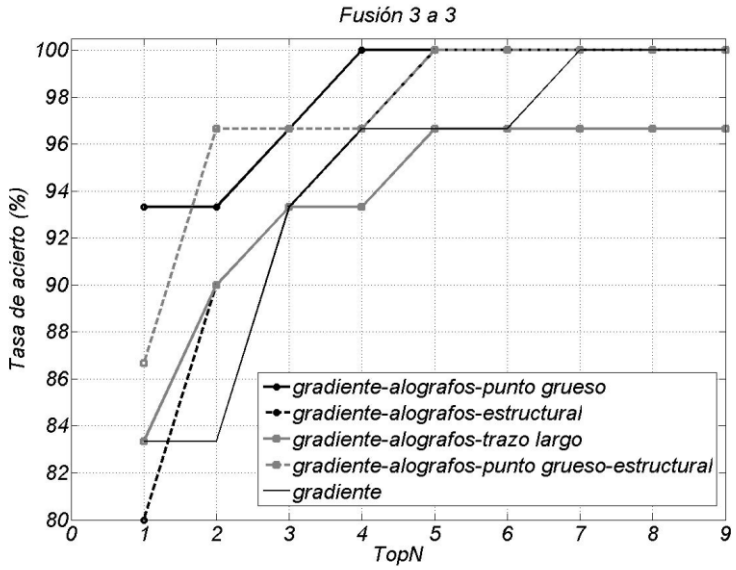


Figura 49. Rendimiento de la fusión del sistema de gradiente y alógrafos (los dos de mejor rendimiento individual) con el resto de sistemas.

Capítulo 6

CONCLUSIONES Y TRABAJO FUTURO

6.1 Conclusiones

Las conclusiones que pueden extraerse a partir de los resultados, así como el trabajo futuro, se presentan a continuación.

Conclusiones de los resultados obtenidos a partir de los sistemas disponibles evaluados en este PFC:

Sistema basado en características de gradiente

En primer lugar, observamos que el uso de histogramas normalizados a función densidad de probabilidad (FDP) mejora las tasas de identificación. Asimismo, utilizar imágenes binarias para la extracción del gradiente supone una mejora extra en los resultados, acercándonos al 94% de tasa de acierto con una lista de tan solo tres candidato. La binarización produce un realce en los bordes del carácter, por lo que la magnitud del gradiente (esto es, su "fuerza") es mayor, siendo su extracción por tanto más fiable. Por último, notar que con este sistema obtenemos una tasa de acierto del 100% con una lista de 6-7 candidatos.

Sistema basado en alógrafos

En este caso, se observa que se obtiene un 100 % de acierto con una la lista de candidatos de 10. Esto implica que este sistema funciona peor que el sistema basado en características de gradiente, pero aún así, los resultados son relativamente buenos. Esto es así debido a que la optimización de los sub-codebooks variando el número de clusters, así como la combinación de los 62 canales, consigue una correcta caracterización de cada usuario indubitado.

Sistema basado en características de contorno

Como se observa en los resultados del apartado anterior, la característica $f2$ funciona mejor que $f1$. Esto es debido a que $f2$ calcula la orientación del contorno y la curvatura, a diferencia de $f1$ que únicamente calcula la orientación del contorno. Por tanto, esta superioridad en los resultados por parte de $f2$ se debe a que ésta es más completa.

Por otro lado, se observa que los resultados obtenidos con estas características en ningún caso llegan a un 100 % de tasa de acierto. Esto implica que a algún usuario dubitado no es identificado, es decir, no se le asigna ninguno de los usuarios dubitados en ninguno de los 62 canales. Este efecto no se observa por ejemplo en el trabajo donde se propusieron estas

características [2] en el cual la evaluación se efectúa usando una base de datos de laboratorio donde se pide a los usuarios que contribuyan con escritos formados por varias líneas de texto. Por tanto, la limitación en la cantidad de datos del escenario forense real de operación de este Proyecto, donde no es posible controlar la extensión de texto disponible de cada usuario, es una característica importante a la hora de obtener el rendimiento de los sistemas.

Conclusiones de los resultados obtenidos a partir de los sistemas desarrollados en el marco de este PFC:

Sistema basado en característica estructural

Con este sistema se proponen dos métodos para el cálculo de umbral de binarización.
El primero de ellos, sería un umbral diferente para cada celda. Este se calcula como la media de los valores del histograma de esa celda.
Por otro lado, se calcula un umbral único para toda la imagen que se calcula como la media de los valores de todos los histogramas juntos.
Se observa que funciona mejor la umbralización por celda, aunque para una lista de entre 1 y 10 candidatos es al contrario. Además, se observa que con el uso de histogramas binarizados no obtenemos una tasa de acierto del 100 %.

También se propuso el uso de histogramas normalizados a función de densidad de probabilidad. El uso de esta propuesta implica una mejora considerable, llegando a alcanzar el 100 % de acierto con una lista de 15 candidatos.
El motivo de esta mejora es debido a que con una función densidad de probabilidad mantenemos el peso relativo de cada una de las reglas dentro de cada celda donde se calcula la característica; en cambio, con un vector binario, se concede la misma importancia a todas las reglas.

Sistema basado en características de concavidad

Con la característica de trazo largo también se proponen dos métodos para el cálculo de umbral de binarización, igual que en el sistema anterior. En este caso, funciona mejor la umbralización por imagen completa.

Con la característica de densidad de punto grueso, se obtienen dos resultados diferentes. En un primer lugar, se obtienen los resultados a partir de histogramas binarizados. Por otro lado, se propuso el uso de histogramas normalizados a función densidad de probabilidad, observándose que esta propuesta funciona mejor, llegando a obtener una tasa de acierto del 100 %.

Sistema basado en características geométricas

En este caso, cabe destacar el bajo rendimiento de las características geométricas. Sólo la combinación de las mismas permite alcanzar un rendimiento parecido a alguna de las otras características desarrolladas en el marco de este PFC, aunque en ningún caso se acerca al de las mejores.

El entorno forense de escasez de datos mencionado, junto con el reducido tamaño del vector de datos de características geométricas (5 elementos por letra), hacen que su rendimiento esté muy por debajo de otras características con vectores de datos mayores.

Fusión de características

Inicialmente, observamos que la fusión con el sistema del gradiente mejora sustancialmente al sistema del gradiente. En particular, la fusión del sistema del gradiente con alógrafos obtiene una tasa de acierto del 100% solamente con 3 usuarios. Asimismo, la fusión del gradiente con punto grueso también supone una mejora sustancial en Top1 y Top2, teniendo el mismo rendimiento que el gradiente para el resto de valores de Top. En este sentido, la fusión nos está permitiendo asegurar que el usuario correcto se sitúa con muy alta probabilidad en las dos o tres primeras posiciones del Top.

Si nos fijamos en una fusión de un mayor número de sistemas (Figura 49), el rendimiento no mejora especialmente (incluso se alcanza el 100% en Top4 en lugar de Top3). Es importante resaltar no obstante que en Top1 obtenemos ya un rendimiento cercano al 94% cuando fusionamos los sistemas de gradiente, alógrafos y punto grueso, mejorando en este caso la fusión de solo dos sistemas. En definitiva, observamos que con la fusión de sistemas podemos alcanzar unas tasas de acierto muy elevadas para un tamaño de Top pequeño.

A la hora de analizar estos resultados, hay que considerar el reducido tamaño de la base de datos (30 usuarios), de modo que una diferencia pequeña en los porcentajes de acierto no resulta significativa. No obstante, permite observar tendencias de mejora tanto con la implementación de nuevas técnicas dentro de cada sistema individual así como con la fusión de los mismos.

6.2 Trabajo futuro

A partir de este trabajo se abren nuevas líneas de investigación. Las más interesantes se detallan a continuación:

Repetición de los experimentos con un nuevo y más rico conjunto experimental: como se ha observado, la fiabilidad de los resultados obtenidos en este proyecto es pobre. Se propone la repetición de los experimentos con un conjunto de muestras mayores. Esto es, realizar los experimentos con listas de candidatos mayores.

Medida de la robustez y confianza estadística: aun disponiendo de un conjunto experimental pequeño, como del que se dispone en este proyecto, existen medidas para comprobar la robustez estadística de los resultados con el objetivo de medir la fiabilidad de los mismos. Se propone la utilización de métodos de medida de la confianza estadística con los resultados obtenidos en este proyecto.

Integración de estas técnicas a una aplicación práctica: se plantea la realización de una aplicación que devuelva la lista de candidatos dubitados con sus respectivos usuarios indubitados, así como la tasa de acierto de los sistemas que muestran en este proyecto. Además, sería semi-automática ya que consideraría la experiencia del experto forense.

Bibliografía

1. **Saks, M.J. y Koehler, J.J.** The coming Paradigm Shift in Forensic Identification Science. *Science.* 2005, Vol. 309, págs. 892-895.

2. **M. Bulacu, L. Schomaker.** *Text-Independent Writer Identification and Verification Using Textural and Allographic Features.* s.l. : IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 4, 2007.

3. **A.K. Jain, P. Flynn, A.A. Ross, editors.** *Handbook of biometrics.* s.l. : Springer, 2007.

4. **A.K. Jain, A. Ross and S. Prabhakar.** *An Introduction to Biometric Recognition.* s.l. : IEEE Transactions on Circuits and Systems for Video Tecnology, Special Issue on Image and Video Based Biometrics, Vol.14, No.1, pp. 4-20, 2004.

5. **S. Nanavati, M. Thieme and R. Nanavati, editors.** *Biometrics: Identity, Verification in Networked World.* s.l. : Wiley, 2002.

6. **Bulacu, M.** *Statistical Pattern Recognition for Automatic Writer Identifiaction and Verification.* University of Groningen : PhD Thesis, 2006.

7. **S. Impedovo, editor.** *Fundamentals in Handwriting Recognition.* s.l. : Springer Verlag, 1994.

8. **Andreas Schlapbach, Horst Bunke.** *Fusing Asynchronous Feature Streams for On-line Writer Identification.* s.l. : ICDAR, 2007.

9. **R. Plamodon, G. Lorette.** *Automatic Signature Verification and Writer Identification - The State of the Art.* s.l. : Pattern Recognition, Vol 22, No. 2, pp. 107-131, 1989.

10. **Tapiador, Marino.** *Análisis de las Características de Identificación Biométrica de la Escritura Manuscrita y Mecanográfica.* s.l. : PhD. Thesis, 2006.

11. **Arazi, B.** *Handwriting identification by means of run-length measurements.* s.l. : IEEE Trans. Syst., Manand Cybernetics, no. 7, vol. 12, pp.878-881, 1997, 1997.

12. **I.Yoshimura, M. Yoshimura.** *Writer identification based on the arc pattern transform.* s.l. : 9th International Conference on Pattern Recognition, Editorial Computer Society Press, 1988.

13. **I. Yoshimura, M. Yoshimura.** *Off-line writer verification using ordinary characters as the object.* s.l. : Pattern Recognition, vol. 24, no. 9, pp.909-915, 1991.

14. **E. Zois, V. Anastossopoulus.** *Morphological Waveform Coding for Writer Identification.* s.l. : Pattern Recognition, Vol. 33, No. 3, pp. 385-398, 2000.

15. **U.V. Marti, R. Messerli, H. Bunke.** *Writer identification using text line based features.* s.l. : ICDAR, 2001.

16. **S.H. Lee, S.N. Cha, Srihari.** *Combining macro and micro features for writer identification.* s.l. : SPIE, Document Recognition and retrieval IX, San Jose, CA, pp. 129-142, 2002.

17. **X. Wang, X. Ding, H. Liu.** *Writer identification using directional element features and linear transform.* s.l. : ICDAR, 2003.

18. **S.N. Srihari, S. H. Cha, H. Arora, S. Lee.** *Individuality of Handwriting.* s.l. : Journal of Forensic Sciences, 47(4), pp. 1-17, 2002.

19. **Alonso-Fernandez, Fernando.** *Biometric Sample Quality and its Application to Multimodal Authentication Systems.* s.l. : PhD. Thesis, 2008.

20. **Otsu.** *A threshold selection method from gray-scale histogram.* s.l. : IEEE Transactions System, Man and Cybernetics, vol. 9, pp. 62-66, 1979.

21. **A. Gilperez, F. Alonso-Fernandez, S. Pecharroman, J. Fierrez, J. Ortega-Garcia.** *Off-line signature verification using contour features.* s.l. : ICFHR, 2008.

22. **F. Alonso-Fernandez, J. Fierrez, A. Gilperez, J. Galbally, J. Ortega-Garcia.** *Robustness of signature verification systems to imitators with increasing skills.* s.l. : ICDAR, 2009.

23. **F. Alonso-Fernandez, J. Fierrez-Aguilar, A. Gilperez, J. Ortega-Garcia.** *Impact of time variability in off-line writer identification and verification.* s.l. : ISPA, Spec. Session on Signal Image Processing for Biometrics (invited paper), 2009.

24. **R.C. González, R.E. Woods.** *Digital Image Processing.* s.l. : Editorial Addison-Wesley, 1992.

25. **Hull, Jonathan J.** *A Database for Handwritten Text Recognition Research.* s.l. : IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993.

26. **2010, Signature Competition ICFHR.** *http://www.isical.ac.in/~icfhr2010/CallforParticipation4NSigComp2010.html].*

27. **Francisco Vargas, Miguel A. Ferrer, Carlos M. Travieso, Jesús B.Alonso.** *Off-line Handwritten Signature GPDS-960 Corpus.* s.l. : IAPR 9th International Conference on Document Analysis and Recognition, ISBN: 978-0-7695-2822.9, pp.764-768, 2007.

28. **J. Fierrez, J. Galbally, J. Ortega-Garcia, M. R. Freire, F. Alonso-Fernandez, D. Ramos, D. T. Toledano, J. Gonzalez-Rodriguez, J. A. Siguenza, J. Garrido-Salas, E. Anguiano, G. Gonzalez-de-Rivera, R. Ribalda, M. Faundez-Zanuy, J. A. Ortega et. al.** *BiosecurID: A Multimodal Biometric Database.* s.l. : Pattern Analysis and Applications, Vol.13, n.2, pp. 235-246, 2010.

29. **Brummer, N.** *"Focal toolkit," Available in http://www.dsp.sun.ac.za/ nbrummer/focal.*

30. **F. Alonso-Fernandez, J. Fierrez, D. Ramos, J. Gonzalez-Rodriguez,.** *Quality-Based Conditional Processing in Multi-Biometrics: application to Sensor Interoperability.* s.l. : IEEE Tansactions on Systems, Man and Cybernetics Part A, (article in press), 2010.

31. **G. Dimauro, S. Impedovo, M.G. Lucchese, R. Modugno, G. Pirlo.** *Recent Advancements in Automatic Signature Verification.* s.l. : IWFHR-9, 2004.

32. **R. Sabourin, J.P. Drouhard.** *Off-Line Signature Verification Using Directional PDF and Neural Networks.* s.l. : Proc. of the Intl. Conf. on Pattern Recognition, vol. 2, pp. 321-325, 1992.

33. **W. Hou, X. Ye, K. Wang.** *A survey of off-line signature verification.* s.l. : Proceedings of the 2004 International Conference on Intelligent Mechatronics and Automation, pp. 536–541, 2004.

ANEXO A: Presupuesto

1. Material

- Compra de ordenador personal 2000 €
- Material de oficina 150 €
- Total de ejecución material 2150 €

2. Gastos generales

- 18 % sobre Ejecución Material 387 €

3. Beneficio Industrial

- 6 % sobre Ejecución Material 129 €

4. Honorarios Proyecto

- 700 horas a 15 € / hora 10.500 €

5. Material fungible

- Gastos de impresión 160 €
- Encuadernación 20 €
- Total de Material fungible 180 €

6. Subtotal del presupuesto

- Subtotal Presupuesto 13.346 €

7. Total presupuesto

- 18% Subtotal Presupuesto 2402,28 €
- Total Presupuesto 15748,28 €

Madrid, Septiembre de 2010
La Ingeniera Jefa del Proyecto

Fdo.: Almudena Gilpérez de la Hera
Ingeniera Superior de Telecomunicación

ANEXO B: Pliego de Condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de *Reconocimiento off-line de escritura basado en fusión de características locales y globales*. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.
Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales

1. La modalidad de contratación será el concurso. La adjudicación se hará, por tanto, a la proposición más favorable sin atender exclusivamente al valor económico, dependiendo de las mayores garantías ofrecidas. La empresa que somete el proyecto a concurso se reserva el derecho a declararlo desierto.

2. El montaje y mecanización completa de los equipos que intervengan será realizado totalmente por la empresa licitadora.

3. En la oferta, se hará constar el precio total por el que se compromete a realizar la obra y el tanto por ciento de baja que supone este precio en relación con un importe límite si este se hubiera fijado.

4. La obra se realizará bajo la dirección técnica de un Ingeniero Superior de Telecomunicación, auxiliado por el número de Ingenieros Técnicos y Programadores que se estime preciso para el desarrollo de la misma.

5. Aparte del Ingeniero Director, el contratista tendrá derecho a contratar al resto del personal, pudiendo ceder esta prerrogativa a favor del Ingeniero Director, quien no estará obligado a aceptarla.

6. El contratista tiene derecho a sacar copias a su costa de los planos, pliego de condiciones y presupuestos. El Ingeniero autor del proyecto autorizará con su firma las copias solicitadas por el contratista después de confrontarlas.

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los

preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

8. Tanto en las certificaciones de obras como en la liquidación final, se abonarán los trabajos realizados por el contratista a los precios de ejecución material que figuran en el presupuesto para cada unidad de la obra.

9. Si excepcionalmente se hubiera ejecutado algún trabajo que no se ajustase a las condiciones de la contrata pero que sin embargo es admisible a juicio del Ingeniero Director de obras, se dará conocimiento a la Dirección, proponiendo a la vez la rebaja de precios que el Ingeniero estime justa y si la Dirección resolviera aceptar la obra, quedará el contratista obligado a conformarse con la rebaja acordada.

10. Cuando se juzgue necesario emplear materiales o ejecutar obras que no figuren en el presupuesto de la contrata, se evaluará su importe a los precios asignados a otras obras o materiales análogos si los hubiere y cuando no, se discutirán entre el Ingeniero Director y el contratista, sometiéndolos a la aprobación de la Dirección. Los nuevos precios convenidos por uno u otro procedimiento, se sujetarán siempre al establecido en el punto anterior.

11. Cuando el contratista, con autorización del Ingeniero Director de obras, emplee materiales de calidad más elevada o de mayores dimensiones de lo estipulado en el proyecto, o sustituya una clase de fabricación por otra que tenga asignado mayor precio o ejecute con mayores dimensiones cualquier otra parte de las obras, o en general, introduzca en ellas cualquier modificación que sea beneficiosa a juicio del Ingeniero Director de obras, no tendrá derecho sin embargo, sino a lo que le correspondería si hubiera realizado la obra con estricta sujeción a lo proyectado y contratado.

12. Las cantidades calculadas para obras accesorias, aunque figuren por partida alzada en el presupuesto final (general), no serán abonadas sino a los precios de la contrata, según las condiciones de la misma y los proyectos particulares que para ellas se formen, o en su defecto, por lo que resulte de su medición final.

13. El contratista queda obligado a abonar al Ingeniero autor del proyecto y director de obras así como a los Ingenieros Técnicos, el importe de sus respectivos honorarios facultativos por formación del proyecto, dirección técnica y administración en su caso, con arreglo a las tarifas y honorarios vigentes.

14. Concluida la ejecución de la obra, será reconocida por el Ingeniero Director que a tal efecto designe la empresa.

15. La garantía definitiva será del 4% del presupuesto y la provisional del 2%.
16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

17. La fecha de comienzo de las obras será a partir de los 15 días naturales del replanteo oficial de las mismas y la definitiva, al año de haber ejecutado la provisional, procediéndose si no existe reclamación alguna, a la reclamación de la fianza.

18. Si el contratista al efectuar el replanteo, observase algún error en el proyecto, deberá comunicarlo en el plazo de quince días al Ingeniero Director de obras, pues transcurrido ese plazo será responsable de la exactitud del proyecto.

19. El contratista está obligado a designar una persona responsable que se entenderá con el Ingeniero Director de obras, o con el delegado que éste designe, para todo relacionado con ella. Al ser el Ingeniero Director de obras el que interpreta el proyecto, el contratista deberá consultarle cualquier duda que surja en su realización.

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

21. El contratista, deberá realizar la obra en el plazo mencionado a partir de la fecha del contrato, incurriendo en multa, por retraso de la ejecución siempre que éste no sea debido a causas de fuerza mayor. A la terminación de la obra, se hará una recepción provisional previo reconocimiento y examen por la dirección técnica, el depositario de efectos, el interventor y el jefe de servicio o un representante, estampando su conformidad el contratista.

22. Hecha la recepción provisional, se certificará al contratista el resto de la obra, reservándose la administración el importe de los gastos de conservación de la misma hasta su recepción definitiva y la fianza durante el tiempo señalado como plazo de garantía. La recepción definitiva se hará en las mismas condiciones que la provisional, extendiéndose el acta correspondiente. El Director Técnico propondrá a la Junta Económica la devolución de la fianza al contratista de acuerdo con las condiciones económicas legales establecidas.

23. Las tarifas para la determinación de honorarios, reguladas por orden de la Presidencia del Gobierno el 19 de Octubre de 1961, se aplicarán sobre el denominado en la actualidad “Presupuesto de Ejecución de Contrata” y anteriormente llamado ”Presupuesto de Ejecución Material” que hoy designa otro concepto.

Condiciones particulares

La empresa consultora, que ha desarrollado el presente proyecto, lo entregará a la empresa cliente bajo las condiciones generales ya formuladas, debiendo añadirse las siguientes condiciones particulares:

1. La propiedad intelectual de los procesos descritos y analizados en el presente trabajo, pertenece por entero a la empresa consultora representada por el Ingeniero Director del Proyecto.

2. La empresa consultora se reserva el derecho a la utilización total o parcial de los resultados de la investigación realizada para desarrollar el siguiente proyecto, bien para su publicación o bien para su uso en trabajos o proyectos posteriores, para la misma empresa cliente o para otra.

3. Cualquier tipo de reproducción aparte de las reseñadas en las condiciones generales, bien sea para uso particular de la empresa cliente, o para cualquier otra aplicación, contará con autorización expresa y por escrito del Ingeniero Director del Proyecto, que actuará en representación de la empresa consultora.

4. En la autorización se ha de hacer constar la aplicación a que se destinan sus reproducciones así como su cantidad.

5. En todas las reproducciones se indicará su procedencia, explicitando el nombre del proyecto, nombre del Ingeniero Director y de la empresa consultora.

6. Si el proyecto pasa la etapa de desarrollo, cualquier modificación que se realice sobre él, deberá ser notificada al Ingeniero Director del Proyecto y a criterio de éste, la empresa consultora decidirá aceptar o no la modificación propuesta.

7. Si la modificación se acepta, la empresa consultora se hará responsable al mismo nivel que el proyecto inicial del que resulta el añadirla.

8. Si la modificación no es aceptada, por el contrario, la empresa consultora declinará toda responsabilidad que se derive de la aplicación o influencia de la misma.

9. Si la empresa cliente decide desarrollar industrialmente uno o varios productos en los que resulte parcial o totalmente aplicable el estudio de este proyecto, deberá comunicarlo a la empresa consultora.

10. La empresa consultora no se responsabiliza de los efectos laterales que se puedan producir en el momento en que se utilice la herramienta objeto del presente proyecto para la realización de otras aplicaciones.

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial,

siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

12. El Ingeniero Director del presente proyecto, será el responsable de la dirección de la aplicación industrial siempre que la empresa consultora lo estime oportuno. En caso contrario, la persona designada deberá contar con la autorización del mismo, quien delegará en él las responsabilidades que ostente.

ANEXO C: Competición

COMPETICIÓN 4NSigComp2010

A partir de este proyecto, se planteó la posibilidad de que el grupo utilizará los sistemas desarrollados en el marco de este PFC, así como los sistemas que ya se encontraban disponibles, para realizar la competición sobre Verificación de Firma Off-Line que 4NSigComp2010 - Forensic Signature Verification Competition [26]. En particular el escenario 2 de dicha competición. Ésta se organiza en conjunción con la International Conference in Frontiers of Handwritting Recognition – ICFHR2010.
Por ello, los experimentos de reconocimiento de individuos a partir de firmas que se presentan, se han enmarcado en la participación del grupo ATVS en la evaluación de firma de esta competición.

Al tratarse de un trabajo en equipo, la descripción de esta tarea no se presenta como material principal de este proyecto fin de carrera, sino como un anexo.

C.1 Base de datos

Los datos usados en esta evaluación proceden de la base de datos GPDS [27] capturada en el Grupo de Procesado Digital de Señales, Universidad De Las Palmas De Gran Canaria, co-organizador de la evaluación. Para el entrenamiento de los sistemas participantes, se ha distribuido un conjunto de firmas de 300 individuos, con 24 firmas genuinas por cada individuo (capturadas en una única sesión) y 30 imitaciones de su firma, resultando en 16200 imágenes de firmas. Las imitaciones se realizaron mostrando al imitador la imagen de la firma a imitar y permitiéndole practicar antes. Cada imitador produjo 3 imitaciones de 5 individuos distintos de la base de datos, de modo que la firma de un individuo ha sido imitada por 10 imitadores distintos. Los datos de test (no distribuidos a los participantes) consisten en un conjunto de firmas de 400 individuos de similares características. A cada persona firmante se le permitió usar su propio bolígrafo y las imágenes de firma fueron escaneadas a 300 dpi. La Figura 50 muestra algunos ejemplos de firmas genuinas e imitadas del conjunto de datos de entrenamiento.

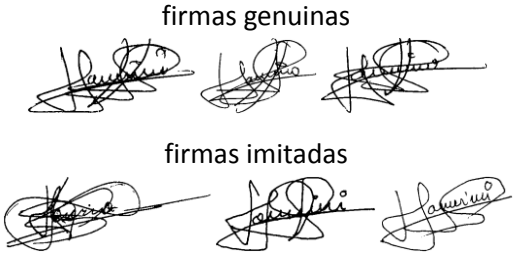


Figura 50. Ejemplo de firmas genuinas e imitadas de un usuario del conjunto de datos de entrenamiento de la competición de firma 4NSigComp2010.

C.2 Protocolo experimental

Para los experimentos de reconocimiento a partir de firma manuscrita, seguimos el protocolo de la citada competición, donde se evalúan los sistemas funcionando en modo verificación. Para generar el modelo de identidad de un individuo, se usan 4 firmas genuinas. El resto de sus firmas genuinas se utilizan para generar intentos de acceso de usuario genuino, mientras que las imitaciones se usan para generar intentos de acceso de impostor *entrenado* (también llamado *skilled*). Esto resulta en 24-4=20 *scores* de acceso genuino y 30 *scores* de acceso de impostor entrenado por cada individuo de la base de datos. Asimismo, para un individuo específico, calculamos *scores* de impostor casual (también llamados *random*) usando una firma genuina del resto de individuos de la base de datos. Con el conjunto de 300 usuarios de entrenamiento, esto resulta en 299 *scores* de acceso de impostor casual por cada individuo de la base de datos. Los intentos de acceso casuales simulan el hecho de intentar hacerse pasar por un usuario proporcionando al sistema una firma aleatoria cualquiera, sin parecido y/o conocimiento de la firma del usuario por el que el impostor pretende hacerse pasar.

En un contexto de verificación, son posibles dos situaciones de error: un impostor es aceptado (Falsa Aceptación, FA) o un usuario correcto es rechazado (Falso Rechazo, FR). Como resultado del proceso de verificación, se genera un *score* que se compara con un umbral, resultando en una decisión de aceptación o rechazo. El rendimiento en la competición mencionada se calcula en términos de un error global "OE" (Overall Error) que se obtiene a partir de los errores de Falsa Aceptación y Falso Rechazo como sigue:

$$OE = 0.5 \times \frac{nGFR}{nG} + 0.25 \times \left(\frac{nSFA}{nSF} + \frac{nRFA}{nRF} \right)$$

donde:

nG: número total de accesos de usuario genuino
nSF: número total de accesos de impostor entrenado
nRF: número total de accesos de impostor casual

nGFR: número de accesos de usuario genuino incorrectamente rechazados
nSFA: número de accesos de impostor entrenado incorrectamente aceptados
nRFA: número de accesos de impostor casual incorrectamente aceptados

C.3 Resultados

A continuación se muestran los resultados de los sistemas individuales sobre los datos de entrenamiento distribuidos por los organizadores de la competición, así como los experimentos de fusión llevados a cabo para optimizar el sistema enviado. También se muestran los resultados publicados por los organizadores sobre los datos de test.

En esta parte de experimentos sobre firmas manuscritas solamente se han evaluado los siguientes sistemas, aplicando cuando proceden las mejoras desarrolladas en la parte de textos manuscritos (i.e. histograma normalizado a FDP en todos los casos):

- Sistema basado en características de gradiente (sobre imagen binaria)
- Sistema basado en alógrafos
- Sistema basado en características de contorno
- Sistema basado en característica GCS estructural

El catálogo o codebook representativo de firmas del sistema basado en alógrafos se ha generado a partir de muestras de la base de datos BIOSECUR-ID [28], capturada en el grupo ATVS. Dicha base de datos contiene firmas de 133 individuos capturados en 4 sesiones diferentes. Cada usuario tiene 4 firmas genuinas y 3 imitaciones entrenadas por sesión hechas por otro 3 imitadores. A cada persona se le pidió que firmara en una hoja de papel sobre una tableta digitalizadora (mismo bolígrafo para todas las personas) y las firmas se escanearon a 600 dpi. Para la generación del codebook, se ha hecho uso de una firma genuina de cada usuario, en total 133 firmas, a las cuales se aplicó el método de extracción de bloques descrito en la Sección 3.2.2. (ventana deslizante de 16x16 con solape del 50%). Ello resulta en 93735 bloques de firma (no blancos) disponibles para el clustering. En este caso, existe un único canal de datos (esto es, firmas) y el número de clusters óptimo será el que minimice la Tasa de Igual Error (EER). La configuración de este sistema procede de un ajuste realizado en otro Proyecto dentro del grupo ATVS. En el presente Proyecto solamente mostraremos la configuración óptima encontrada, la cual se usará para su comparación con el resto de características y para la fusión. Para el caso de firma, consiste en un codebook de formas alográficas de 49 clusters.

C.3.1 Sistemas individuales

La Figura 51 muestra el rendimiento mediante curvas DET de los sistemas individuales sobre los datos de entrenamiento de la competición. Las tasas de EER correspondientes se detallan en la tabla de la Figura 52.

En primer lugar, como cabe esperar, el rendimiento con intentos de acceso de impostor casual es sensiblemente mejor que con intentos de acceso de impostor entrenado (tasa EER por lo general entre 2 y 3 veces más baja). Destacar también los valores aparentemente “elevados” de las tasas de EER, sobre todo para impostores entrenados (25% o mayores). Mencionar que las firmas de la base de datos de la evaluación están escaneadas solamente a 300 dpi, lo cual es una fuente de empeoramiento de los resultados. Los resultados de la evaluación publicados

por los organizadores (ver Sección C.3.3) corroboran este hecho. En otros trabajos, como el de la autora de este proyecto en [21] donde se evalúan las características de contorno sobre un base de datos a 600 dpi, las tasas EER son aproximadamente la mitad para impostores entrenados y un tercio para impostores casuales.

En cuanto al rendimiento relativo entre los sistemas, observamos que con impostores entrenados, el mejor con diferencia es el de característica de contorno *f*2 para todos los rangos de FAR y FRR. Con impostores casuales, el mejor sistema para baja FAR es el de característica de contorno *f*2, mientras que para baja FRR es el de alógrafos. Por otro lado, los sistemas con peor rendimiento en general son el de característica de gradiente y el de característica estructural. Estos resultados contrastan con los experimentos usando textos manuscritos del Capítulo 4, donde el mejor sistema era el del gradiente, mientras que la característica de contorno *f*2 no se encontraba entre los mejores.

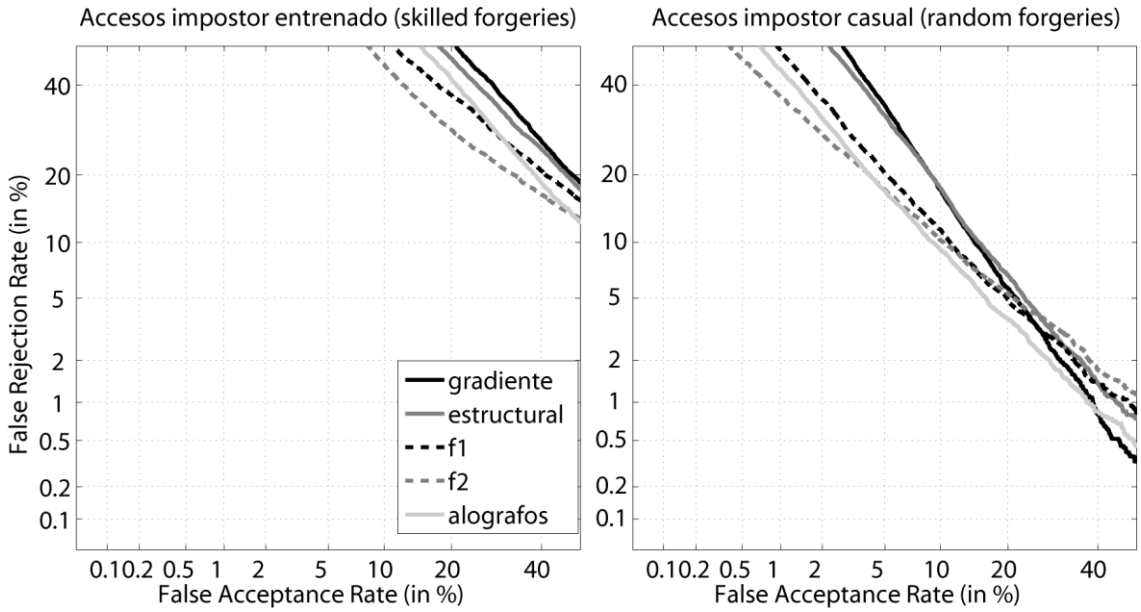


Figura 51. Rendimiento de los sistemas individuales sobre los datos de entrenamiento de la competición de firma 4NSigComp2010 (curvas DET).

	EER impostor entrenado (skilled forgeries)	**EER impostor casual (random forgeries)**
Gradiente	33,58%	12,54%
Estructural	31,93%	12,68%
Contorno *f*1	28,75%	10,63%
Contorno *f*2	24,92%	10,14%
Alógrafos	29,01%	9,60%

Figura 52. Rendimiento de los sistemas individuales sobre los datos de entrenamiento de la competición de firma 4NSigComp2010 (valores de EER).

C.3.2 Fusión de características

El sistema enviado a la competición de firma 4NSigComp2010 por el grupo ATVS ha consistido en una fusión de los sistemas anteriores. Se han realizado pruebas con diversas combinaciones de los mismos, eligiéndose la óptima en términos del criterio de menor error global "OE" utilizado por los organizadores. En esta Sección se muestran los resultados de dichas pruebas.

Para cada acceso al sistema utilizando una imagen de firma, éste devolverá *N* scores correspondientes al enfrentamiento del modelo de la firma de entrada con el modelo de identidad pretendida usando los *N* sistemas individuales disponibles. Dados *N* sistemas que producen un conjunto de scores $\left(s_{1j}, s_{2j}, \ldots, s_{Nj}\right)$ para una firma de entrada *j*, en las pruebas de este Proyecto se ha efectuado una fusión lineal de los mismos:

$$f_j = a_0 + a_1 \cdot s_{1j} + a_2 \cdot s_{2j} + \ldots + a_N \cdot s_{Nj}$$

El conjunto de pesos $\left(a_0, a_1, \ldots, a_N\right)$ se entrena por regresión logística lineal de tal manera que el score fusionado f_j tienda a una log-relación de verosimilitud (LLR por sus siglas en inglés "Log-Likelihood Ratio") entre las dos posibles hipótesis de decisión, esto es, el logaritmo de la probabilidad de que los modelos bajo comparación pertenezcan al mismo sujeto frente a la probabilidad de que los modelos bajo comparación no pertenezcan al mismo sujeto. Idealmente, de acuerdo con la definición de LLR, los accesos de usuario genuino deberían producir un score fusionado con valor positivo (probabilidad de que los modelos bajo comparación pertenezcan al mismo sujeto mayor que la probabilidad de que los modelos bajo comparación no pertenezcan al mismo sujeto). Análogamente, los accesos de usuario impostor deberían producir un score fusionado con valor negativo. Un LLR de valor cero significa que no hay apoyo a ninguna de las dos hipótesis.

El entrenamiento de los pesos se hace usando todos los *scores* disponibles obtenidos a partir los datos de entrenamiento de la competición, incluyendo los de acceso de usuario genuino y los de impostor entrenado. Solamente utilizamos los accesos de impostor entrenado aquí ya que, por su propia naturaleza, producirán valores de LLR negativos más cercanos a cero que los accesos de impostor casual. Cuando se produzca un acceso de impostor casual, donde se intenta acceder usando una firma con forma aleatoria sin ninguna relación con la del usuario verdadero, se obtendrá un valor de LLR negativo más alejado de cero. Esto se refleja por ejemplo en que las tasas de error EER con impostores entrenados son mayores que con impostores casuales (ver Figura 51 de la Sección anterior).

El entrenamiento de la fusión ha efectuado con las herramientas del toolbox FoCal, de libre disposición [29]. Los detalles sobre el procedimiento de entrenamiento de la fusión pueden encontrarse en el trabajo [30] y en las referencias indicadas dentro del mismo.

Se han probado combinaciones de fusión de dos, tres, cuatro y todos los sistemas individuales, calculándose sus tasas EER y OE. Para cada caso, se ha calculado el umbral de decisión óptimo que resulta en el menor valor de error global "OE" de acuerdo a la fórmula indicada en la Sección C.2. En la tabla de la Figura 53, se muestran los resultados de todas las combinaciones posibles, recuadrándose la mejor de todas ellas en términos de "OE", que es la enviada por el grupo ATVS a la competición 4NSigComp2010. La mejor combinación en términos de "OE" es aquella que fusiona los sistemas de gradiente, estructurales $f1$, $f2$ y el sistema de alógrafos. El umbral óptimo de decisión obtenido en todos los casos es próximo a cero, lo que en términos de un LLR significa que se sitúa en torno al valor donde no hay apoyo a ninguna de las hipótesis de aceptación o rechazo. También mostramos en la Figura 54 el rendimiento de la combinación de dos, tres, cuatro y todos los sistemas que resulta en el menor "OE" (indicados en negrita en la columna "OE" de la tabla de la Figura 53).

Se observa en las curvas DET de la Figura 53 que la fusión de sistemas produce una mejora adicional sobre el mejor de los sistemas individuales. La mejor combinación en términos de EER para el caso de impostores entrenados (fusión de $f1$, $f2$ y alógrafos) produce un EER del 23.21%, lo que supone una mejora cercana al 7% respecto al mejor sistema individual. Por otro lado, la mejor combinación para el caso de impostores casuales (fusión de $f2$ y alógrafos) produce un EER del 7.77%, una mejora del 19% respecto al mejor sistema individual. Resulta por tanto evidente el beneficio de la de combinación de sistemas para el reconocimiento. En ambas casos, se encuentran implicados los dos mejores sistemas individuales de la Sección C.3.1, esto es, los sistemas $f2$ y alógrafos.

A pesar de que la mejor combinación obtenida según el criterio de "OE" fusiona cuatro sistemas, se observan otras combinaciones donde el rendimiento es parecido, como sugiere el hecho de que en muchos casos de la tabla de la Figura 53 haya una diferencia de decimales respecto al mejor valor de "OE". De hecho, para el caso de impostores entrenados (Figura 54, izquierda), a partir de tres sistemas fusionados no hay diferencia de rendimiento apreciable si añadimos un cuarto o un quinto. Aun más, para el caso de impostores casuales (Figura 54, izquierda), la mejor combinación es la que combina dos sistemas, empeorando cuando se combinan tres o más. Esto indica también que la combinación óptima no siempre es aquella que hace uso de todos los sistemas disponibles, ni necesariamente de los mejores sistemas individuales.

DOS SISTEMAS

	EER skilled	EER random	OE	umbral optimo
grad-estr	32,50	**12,27**	23,51	0,00
grad-f1	28,78	10,63	21,71	0,10
grad-f2	**24,89**	10,17	19,18	0,10
grad-alogr	**27,71**	**8,07**	19,36	-0,10
estr-f1	29,19	**10,58**	21,71	0,10
estr-f2	**24,86**	10,14	19,16	0,10
estr-alogr	**27,42**	**8,16**	19,23	-0,10
f1-f2	25,01	10,90	19,04	0,00
f1-alogr	**26,51**	**7,84**	18,93	-0,20
f2-alogr	**24,11**	**7,77**	**17,82**	-0,20

TRES SISTEMAS

	EER skilled	EER random	OE	umbral optimo
grad-estr-f1	**28,71**	**10,55**	21,64	0,10
grad-estr-f2	**24,88**	10,15	19,16	0,10
grad-estr-alogr	**27,64**	**8,03**	19,21	-0,30
grad-f1-f2	25,57	11,08	19,28	0,00
grad-f1-alogr	**26,41**	**7,88**	18,93	-0,20
grad-f2-alogr	**23,69**	**8,03**	17,70	-0,10
estr-f1-f2	25,01	10,73	18,91	0,10
estr-f1-alogr	**26,48**	**7,82**	18,93	-0,20
estr-f2-alogr	**23,89**	**7,86**	17,84	-0,10
f1-f2-alogr	**23,21**	**8,43**	**17,43**	-0,10

CUATRO SISTEMAS

	EER skilled	EER random	OE	umbral optimo
grad-estr-f1-f2	25,50	11,15	19,31	0,00
grad-estr-f1-alogr	**26,29**	**7,82**	18,85	-0,20
grad-estr-f2-alogr	**23,79**	**8,04**	17,75	0,10
grad-f1-f2-alogr	**23,64**	**8,35**	17,38	-0,10
estr-f1-f2-alogr	**23,28**	**8,37**	**17,29**	-0,10

	EER skilled	EER random	OE	umbral optimo
TODOS	**23,63**	**8,35**	**17,31**	-0,10

Figura 53. Rendimiento de la fusión de sistemas individuales sobre los datos de entrenamiento de la competición de firma 4NSigComp2010 (valores de EER y de OE). Se recuadra la mejor de todas ellas en términos de "OE". Asimismo, se indican en negrita las combinaciones cuyo EER es mejor que cualquiera de los sistemas individuales combinados.

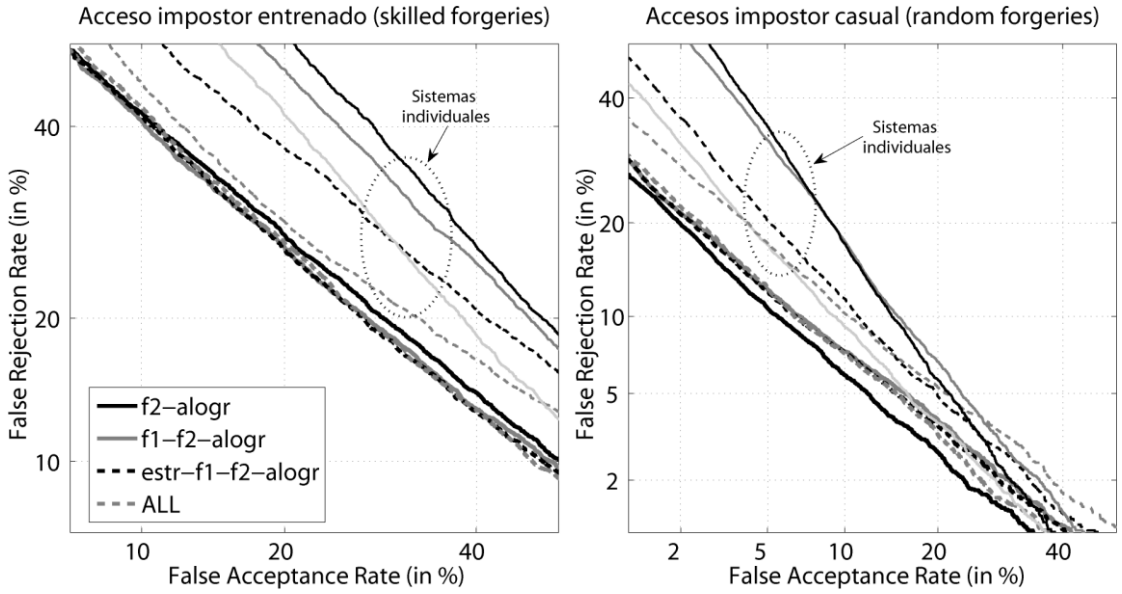


Figura 54. Rendimiento de la combinación de dos, tres, cuatro y todos los sistemas que resulta en el menor "OE" sobre los datos de entrenamiento de la competición de firma 4NSigComp2010 (curvas DET).

C.3.3 Resultados de la competición 4NSigComp2010

En la tabla de la Figura 55 se muestran los resultados de la competición 4NSigComp2010 proporcionados por los organizadores, los cuales se harán públicos en la International Conference in Frontiers of Handwritting Recognition – ICFHR2010 (a fecha de realización de este Proyecto, solamente se habían dado a conocer entre los participantes). Estos resultados han sido calculados sobre los datos de evaluación de la competición, i.e. no distribuidos a los participantes antes de la misma. El Id del grupo ATVS es el 8 (segunda posición del ranking de OE). Las siglas de la primera columna indican tasa de Falso Rechazo (FRR), tasa de Falsa Aceptación de impostor entrenado o "skilled" (FARS) y tasa de Falsa Aceptación de impostor casual o "random" (FARR) junto con el error global OE. Hay que notar que según el protocolo de la competición, solo había que proporcionar una decisión de aceptación o rechazo respecto de la firma de entrada en cuestión. Es por ello que los organizadores solamente son capaces de proporcionar resultados de Falsa Aceptación y Falso Rechazo, pero no de curvas DET o tasas EER.

Destacar los excelentes resultados del grupo ATVS en la evaluación, con una tasa de error OE incluso menor que los obtenidos con los datos de entrenamiento (OE=17,29). Si bien la tasa de Falsa Aceptación de impostor casual (FARR) es la más alta de todos los participantes, se ve compensada por unas tasas FRR y FARS menores que la mayoría de participantes. Estos resultados son una excelente validación de los desarrollos y experimentos llevados a cabo para esta competición.

Id	*FRR (%)*	*FARR (%)*	*FARS (%)*	*OE (%)*	*Rank*
6	13,96	0,01	7,81	8,94	1st
8	**18**	**4,31**	**25,38**	**16,42**	**2nd**
9	21,49	1,22	22,84	16,76	3rd
1	10,43	9,18	39,18	17,31	4th
10	11,19	0,96	47,8	17,79	5th
2	22,06	0,07	46,27	22,62	6th
3	37,86	0,15	28,4	26,07	7th
4	40,83	0,09	28,36	27,53	8th
5	41,84	0,09	29,35	28,28	9th
7	46,08	0,24	29,73	30,53	10th

Figura 55. Resultados de la competición de firma 4NSigComp2010 sobre los datos de evaluación publicados por los organizadores.

ANEXO D: Publicaciones

D1. ICFHR 2008:

Off-line Signature Verification Using Contour Features

Almudena Gilperez, Fernando Alonso-Fernandez, Susana Pecharroman, Julian Fierrez, Javier Ortega-Garcia
Biometric Recognition Group - ATVS
Escuela Politecnica Superior - Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - 28049 Madrid, Spain
{almudena.gilperez, fernando.alonso, julian.fierrez, javier.ortega}@uam.es
http://atvs.ii.uam.es

Abstract

An off-line signature verification system based on contour features is presented. It works at the local image level, and encodes directional properties of signature contours and the length of regions enclosed inside letters. Results obtained on a sub-corpus of the MCYT signature database shows that directional-based features work much better than length-based features. Results are comparable to existing approaches based on different features. It is also observed that combination of the proposed features does not provide improvements in performance, maybe to some existing correlation among them.

1. Introduction

The increasing interest on biometrics is related to the number of important applications where a correct assessment of identity is a crucial point [1]. In this paper, we address the problem of automatic verification of writers on scanned images of signatures, known as off-line signature verification. This is a long-established pattern classification problem [2], since signature is one of the most widely used authentication methods due to its acceptance in government, legal, financial and commercial transactions [3]. It is worth noting that even professional forensic examiners perform at about 70% of correct classification rate, and thus this is a challenging research area [4].

A machine expert for off-line signature verification has been built in this work. It is based on features proposed for writer identification and verification using images of handwriting documents [5]. We have selected and adapted a number of features to be used with handwritten signatures which are based on local image analysis. The features implemented work at the analysis of the contour level. The signature is seen as a texture described by some probability distributions computed from the image and capturing the distinctive visual appearance of the samples. User individuality is therefore encoded using probability distributions (PDF) extracted from signature images. The term "feature" is used to denote such a complete PDF, so we will obtain an entire vector of probabilities capturing the signature uniqueness.

The rest of this paper is organized as follows. A description of the machine expert implemented in this work is given in Section 2. The experimental framework used, including the database, protocol and results, is described in Section 3. Conclusions are finally drawn in Section 4.

2. Machine expert based on contour features

The signature verification system includes three main stages: i) signature preprocessing, ii) feature extraction, and iii) feature matching. These stages are described next.

2.1. Pre-processing Stage

The objective of this stage is to enhance the signature image and to adapt it to the feature extraction stage. The preprocessing stage is divided in four parts, as shown in Figure 1: binarization, noise removal, component detection and contour extraction.

In the first place, the scanned image is binarized using the Otsu's method [6]. This method consists in a histogram thresholding. It performs well when the image is characterized by a uniform background and similar objects, as it is the case of signature images, and it does not need human supervision or prior information before its execution. The next step is the elimination of noise of the binary image, which is done through a morphological opening plus a closing operation [7]. Then a connected component detection, using 8-connectivity, is carried out. In the last step, internal and external contours of the connected components are extracted using the Moore's algorithm [7]. Beginning from a contour pixel of a connected component, which is set as the starting pixel,

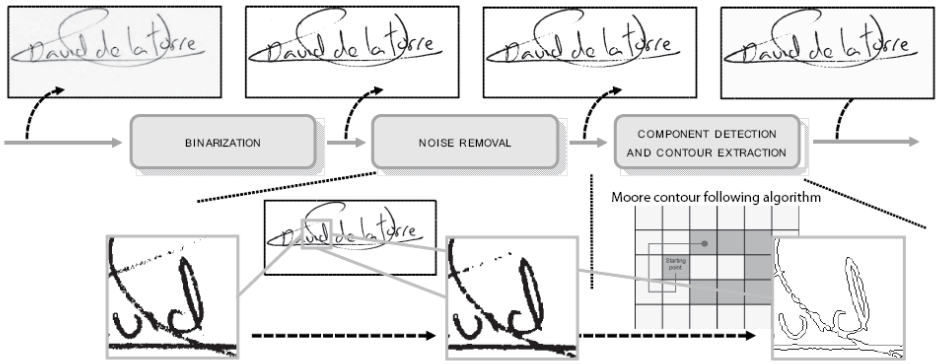


Figure 1. Preprocessing stage performed by the verification system.

this algorithm seeks a pixel boundary around it following the meaning clockwise, and repeats this process until the starting pixel is reached for the same position from which it was agreed to begin the algorithm. The result is a sequence with the pixels coordinates of the boundary of the component. This vectorial representation is very effective because it allows a rapid extraction of many of the features used later.

2.2. Feature Extraction Stage

Features are calculated from two representations of the signature extracted during the preprocessing stage: the binary image without noise and the contours of the connected components. The features used in this work are summarized in Table 1, including the signature representation used by each one. The signature is shaped like a texture that is described with probability distribution functions (PDFs). Probability distribution functions used here are grouped in two different categories: direction PDFs (features f1, f2, f3h, f3v) and length PDFs (features f5h, f5v). A graphical description of the extraction of direction PDFs is depicted in Figure 2. To be consistent with the work in which these features where proposed [5], we follow the same nomenclature used in it.

Contour-Direction PDF (f1)

This directional distribution is computed very fastly using the contour representation, with the additional advantage that the influence of the ink-trace width is eliminated. The contour-direction distribution f1 is extracted by considering the orientation of local contour fragments. A fragment is determined by two contour pixels (x_k,y_k) and $(x_{k+\epsilon},y_{k+\epsilon})$ taken a certain distance ϵ apart. The angle that the fragment makes with the horizontal is computed using

$$\phi = \arctan(\frac{y_{k+\epsilon} - y_k}{x_{k+\epsilon} - x_k}) \quad (1)$$

As the algorithm runs over the contour, the histogram of angles is built. This angle histogram is then normalized to a probability distribution f1 which gives the probability of finding in the signature image a contour fragment oriented with each ϕ. The angle ϕ resides in the first two quadrants because, without online information, we do not know which inclination the writer signed with. The histogram is spanned in the interval 0°-180°, and is divided in $n = 12$ sections (bins). Therefore, each section spans 15°, which is a sufficiently detailed and robust description [5]. We also set $\epsilon = 5$. These settings will be used for all of the directional features presented in this paper.

Contour-Hinge PDF (f2)

In order to capture the curvature of the contour, as well as its orientation, the "hinge" feature f2 is used. The main idea is to consider two contour fragments attached at a common end pixel and compute the joint probability distribution of the orientations ϕ_1 and ϕ_2 of the two sides. A joint density function is obtained, which quantifies the chance of finding two "hinged" contour fragments with angles ϕ_1 and ϕ_2, respectively. It is spanned in the four quadrants (360°) and there are $2n$ sections for every side of the "contour-hinge", but only non-redundant combinations are considered (i.e. $\phi_2 \geq \phi_1$). For $n = 12$, the resulting contour-hinge feature vector has 300 dimensions [5].

Direction Co-Occurrence PDFs (f3h, f3v)

Table 1. Features used in this work.

	Feature	Explanation	Dimensions	Source
f1	$p(\phi)$	Contour-direction PDF	12	contours
f2	$p(\phi_1, \phi_2)$	Contour-hinge PDF	300	contours
f3h	$p(\phi_1, \phi_3)_h$	Direction co-occurrence PDF, horizontal run	144	contours
f3v	$p(\phi_1, \phi_3)_v$	Direction co-occurrence PDF, vertical run	144	contours
f5h	$p(rl)_h$	Run-length on background PDF, horizontal run	60	binary image
f5v	$p(rl)_v$	Run-length on background PDF, vertical run	60	binary image

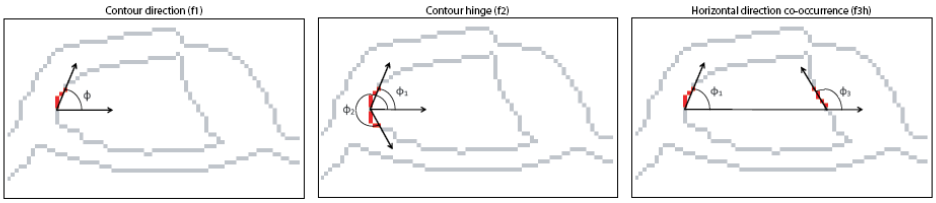


Figure 2. Graphical description of the feature extraction. From left to right: contour direction (f1), contour hinge (f2) and horizontal direction co-occurrence (f3h).

Based on the same idea of combining oriented contour fragments, the directional co-occurrence is used. For this feature, the combination of contour-angles occurring at the ends of run-lengths on the background are used, see Figure 2. Horizontal runs along the rows of the image generate f3h and vertical runs along the columns generate f3v. They are also joint density functions, spanned in the two first quadrants, and divided into n^2 sections. These features give a measure of a roundness of the written characters and/or strokes.

Run-Length PDFs (f5h, f5v)

These features are computed from the binary image of the signature taking into consideration the pixels corresponding to the background. They capture the regions enclosed inside the letters and strokes and also the empty spaces between them. The probability distributions of horizontal and vertical lengths are used.

2.3. Feature Matching Stage

Each client of the system (enrolee) is represented by a PDF that is computed using an enrolment set of K signatures. For each feature, the histogram of the K signatures together is computed and then normalized to a probability distribution.

To compute the similarity between a claimed identity q and a given signature i, the χ^2 distance is used [5]:

$$\chi^2_{qi} = \sum_{n=1}^{N} \frac{(p_q[n] - p_i[n])^2}{p_q[n] + p_i[n]} \quad (2)$$

where p are entries in the PDF, n is the bin index, and N is the number of bins in the PDF (the dimensionality)

We also perform experiments combining the different features. The final distance in this case is computed as the mean value of the Hamming distances due to the individual features:

$$H_{qi} = \sum_{n=1}^{N} |p_q[n] - p_i[n]| \quad (3)$$

The χ^2 distance, due to the denominator, gives more weight to the low probability regions of the PDF and maximizes the performance of each individual feature. On the other hand, the Hamming distance provides comparable distance values for the individual features [5].

3. Experiments

3.1. Database and Experimental Protocol

We have used for the experiments a subcorpus of the MCYT database [8] which includes fingerprint and on-line signature data of 330 contributors from 4 different Spanish sites. Skilled forgeries are also available in the case of signature data. Forgers are provided the signature images of clients to be forged and, after training with them

Figure 3. Signature examples of the four types encountered in the MCYT corpus.

several times, they are asked to imitate the shape. Signature data were acquired with an inking pen and paper templates over a pen tablet. Therefore, signature images are also available on paper. Paper templates of 75 signers (and their associated skilled forgeries) have been digitized with a scanner at 600 dpi. The resulting subcorpus has 2250 images of signatures, with 15 genuine signatures and 15 forgeries per user (see Figure 3)[1].

The training set comprises either $K = 5$ or $K = 10$ genuine signatures (depending on the experiment under consideration). The remaining genuine signatures are used for testing. For a specific target user, casual impostor test scores are computed by using the genuine samples available from all the remaining targets. Real impostor test scores are computed by using the skilled forgeries of each target. As a result, we have $75 \times 10 = 750$ or $75 \times 5 = 375$ client similarity scores, $75 \times 15 = 1,125$ impostor scores from skilled forgeries, and $75 \times 74 \times 10 = 55,500$ or $75 \times 74 \times 5 = 27,750$ impostor scores from random forgeries.

In a verification context, two situations of error are possible: an impostor is accepted (false acceptance, FA) or the correct user is rejected (false rejection, FR). For error reporting, we use the graphical representations of Detection Error Trade-off (DET), which represent FA vs. FR rate. In order to have an indication of the level of performance with an ideal score alignment between users, we also report the EER when using *a posteriori* user-dependent score normalization [9]. The score normalization function is as follows $s' = s - s_\lambda$, where s is the raw similarity score computed by the signature matcher, s' is the normalized similarity score and s_λ is the user-dependent decision threshold at the EER obtained from a set of genuine and impostor scores of the user λ.

[1] This signature corpus is publicly available at http://atvs.ii.uam.es

3.2. Results

The system performance for *a posteriori* user-dependent score normalization is given in Table 2 (individual features) and Table 3 (combination of features). DET curves for the individual features without score normalization are plotted in Figure 4.

It is observed that the best individual feature is always the Contour-Hinge PDF f2, independently of the number of signatures used for training and both for random and skilled forgeries. This feature encodes simultaneously curvature and orientation of the signature contours. It is remarkable that the other features using two angles (f3h, f3v) perform worse than f2. Also worth noting, the feature using only one angle (f1) exhibits comparable performance to f3h and f3v, even outperforming them in some regions of the DET. It is interesting to point out the bad result obtained by the length PDFs (f5h and f5v). This suggests that the length of the regions enclosed inside the letters and strokes is not a good distinctive feature in offline signature verification (given a preprocessing stage similar to ours).

An important result also is that the combination of features does not result in performance improvement, as can be observed in Table 3, even for combinations that involve features of different categories (direction and length). Only the combination of f5h and f5v features has a significant improvement. An explanation is as follows. Although paired differently, the features based on directions involve the same set of angle values. As can be observed in Figure 2, the three examples depicted include the same value in one of the angles. As a result, there is some correlation between the features and therefore its combination does not result in improvement. For the features based on length, their bad performance could explain why they do not provide benefits in the fusion.

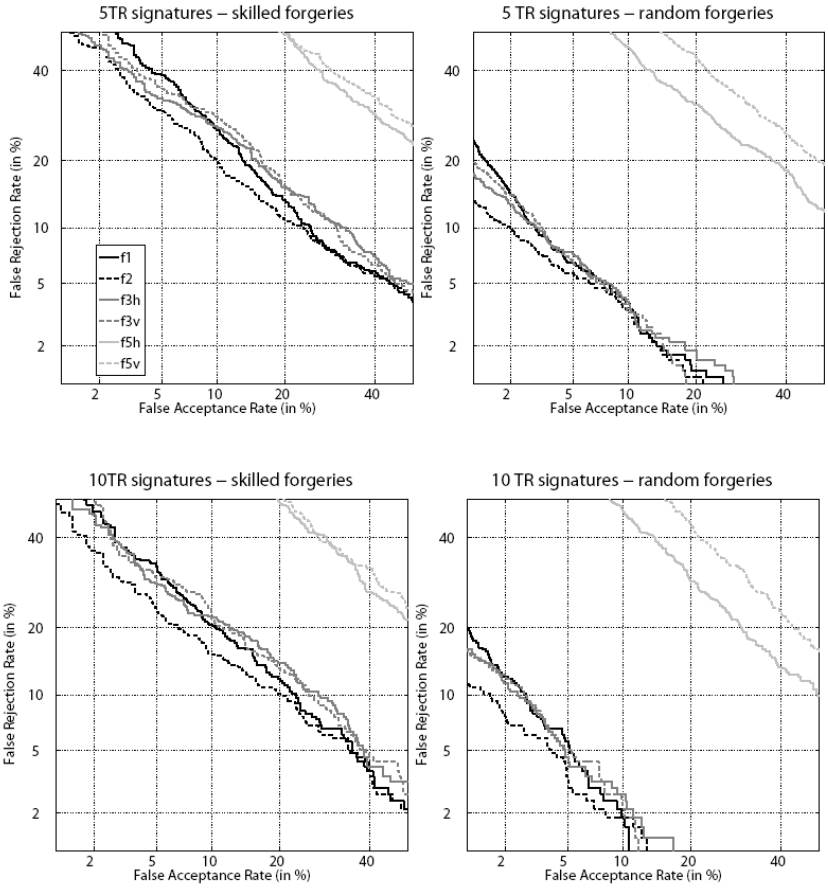


Figure 4. Verification performance without score normalization (user-independent decision thresholds).

4. Conclusions

A machine expert for off-line signature verification based on contour features has been presented. Writer individuality has been encoded using probability density functions (PDFs), grouped in two categories: direction PDFs and length PDFs. They work at the local level and encode several directional properties of contour fragments of the signature as well as the length of the regions enclosed inside letters.

Experimental results are given using 2250 different signature images of 75 contributors extracted from the MCYT signature database. Verification performance is reported for user-dependent and user-independent decision thresholds. Features based on direction work much better that those based on lengths, with best EERs of 6.44% and 1.18% for skilled and random forgeries, respectively (contour-hinge PDF, 10 training signatures, *a posteriori* score normalization). It is also remarkable that the combination of features does not result in performance improvement, maybe due to the correlation among them.

Verification results are comparable to other existing approaches for off-line signature verification based on different features using the same experimental framework [10]. This encourages us to exploit their complementary information using different fusion strategies [11]. Another source of future work is to better analyze the information content in signature images in order to devise quality measures related to their utility for identity verification [12].

5. Acknowledgements

This work has been supported by Spanish project TEC2006-13141-C03-03, and by European Commission

Table 2. System Performance in terms of EER (in %) of the **individual features** with *a posteriori* user-dependent score normalization.

	SKILLED FORGERIES						RANDOM FORGERIES					
	Direction PDFs				Length PDFs		Direction PDFs				Length PDFs	
	f1	**f2**	**f3h**	**f3v**	**f5h**	**f5v**	**f1**	**f2**	**f3h**	**f3v**	**f5h**	**f5v**
5 TR Samples	12.71	10.18	11.40	12.31	30.33	31.78	3.31	2.18	3.09	3.21	22.18	28.03
10 TR Samples	10.00	6.44	7.78	9.16	28.89	33.78	1.96	1.18	1.40	1.49	20.46	28.58

Table 3. System Performance in terms of EER (in %) of the **combination of features** with *a posteriori* user-dependent score normalization. They are marked in bold the cases in which there is a performance improvement with respect to the best individual feature involved.

SKILLED FORGERIES

	f3=f3h+f3v	**f5=f5h+f5v**	**f1 & f5**	**f2 & f5**	**f3 & f5**	**f1 & f2**	**f1 & f3**	**f2 & f3**
5 TR Samples	12.40	**27.56**	16.69	15.56	13.33	13.11	12.38	11.40
10 TR Samples	8.93	**25.60**	13.64	12.13	9.64	9.87	9.16	8.40

RANDOM FORGERIES

	f3=f3h+f3v	**f5=f5h+f5v**	**f1 & f5**	**f2 & f5**	**f3 & f5**	**f1 & f2**	**f1 & f3**	**f2 & f3**
5 TR Samples	3.08	**21.00**	6.40	5.86	4.13	2.87	**2.95**	2.45
10 TR Samples	1.63	**17.86**	4.27	3.73	2.23	1.87	**1.43**	**1.06**

IST-2002-507634 Biosecure NoE. Author F. A.-F. thanks Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting his PhD studies. Author J. F. is supported by a Marie Curie Fellowship from the European Commission.

References

[1] A. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Trans. on Information Forensics and Security*, 1:125–143, 2006.

[2] R. Plamondon and S. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(1):63–84, 2000.

[3] M. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", *Electronics and Communication Engineering Journal*, 9:273–280, December 1997.

[4] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of signature legibility and signature type in off-line signature verification", *Proceedings of Biometric Symposium, Biometric Consortium Conference*, Baltimore, Maryland (USA), 1:1-6, September 2007.

[5] M. Bulacu and L. Schomaker, "Text-Independent Writer Identification and Verification Using Textural and Allographic Features", *IEEE Trans. on Pattern Analysis and Machine Inteligence*, 29(4):701–717, April 2007.

[6] N. Otsu, "A threshold selection method for gray-level histograms", *IEEE Trans. on Systems, Man and Cibernetics*, 9:62–66, December 1979.

[7] R. Gonzalez and R. Woods, *Digital Image Processing*, Addison-Wesley, 2002.

[8] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. Igarza, C. Vivaracho, D. Escudero and Q. Moro, "MCYT baseline corpus: a bimodal biometric database", *IEE Proceedings on Vision, Image and Signal Processing*, 150(6):395–401, December 2003.

[9] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Target Dependent Score Normalization Techniques and Their Application to Signature Verification", *IEEE Trans. on Systems, Man and Cybernetics-Part C*, 35(3), 2005.

[10] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information", *Proc. Workshop on Biometric Authentication, BIOAW*, Springer LNCS-3087:295–306, 2004.

[11] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez and J. Bigun, "Discriminative multimodal biometric authentication based on quality measures", *Pattern Recognition*, 38(5):777–779, 2005.

[12] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Automatic measures for predicting performance in off-line signature", *Proc. International Conference on Image Processing, ICIP*, 1:369-372, San Antonio TX, USA, September 2007.

Robustness of signature verification systems to imitators with increasing skills

Fernando Alonso-Fernandez, Julian Fierrez, Almudena Gilperez, Javier Galbally, Javier Ortega-Garcia
Biometric Recognition Group - ATVS, Escuela Politecnica Superior, Universidad Autonoma de Madrid
C/ Francisco Tomas y Valiente 11, 28049 Madrid SPAIN
{fernando.alonso, julian.fierrez, almudena.gilperez, javier.galbally, javier.ortega}@uam.es

Abstract

In this paper, we study the impact of an incremental level of skill in the forgeries against signature verification systems. Experiments are carried out using both off-line systems, involving the discrimination of signatures written on a piece of paper, and on-line systems, in which dynamic information of the signing process (such as velocity and acceleration) is also available. We use for our experiments the BiosecurID database, which contains both on-line and off-line versions of signatures, acquired in four sessions across a 4 month time span with incremental level of skill in the forgeries for different sessions. We compare several scenarios with different size and variability of the enrolment set, showing that the problem of skilled forgeries can be alleviated as we consider more signatures for enrolment.

1. Introduction

Nowadays, due to the expansion of the networked society, an automatic correct assessment of identity is a crucial point. This has resulted in the establishment of a new research and technology area known as *biometrics* [1], which refers to automatic recognition of an individual based on behavioral and/or anatomical characteristics (e.g., fingerprints, face, iris, voice, signature, etc.).

The handwritten signature is one of the most widely used individual authentication methods due to its acceptance in government, legal and commercial transactions [2]. There are two main signature recognition approaches [3, 4]: off-line and on-line. Off-line methods consider only the signature image, so only static information is available for the recognition task. On-line systems use pen tablets or digitizers which capture dynamic information such as velocity and acceleration of the signing process, providing a richer source of information and more reliability [3].

Despite the evident advantages of biometric systems, they are not free from external attacks which can decrease their level of security. Thus, it is of utmost importance to analyze the vulnerabilities of biometric systems, in order to find their limitations and to develop useful countermeasures for foreseeable attacks [5]. Like other biometric systems, signature verification systems are exposed to forgeries, which can be easily performed by direct observation and learning of the signature by the forger. Signature verification systems are usually evaluated by analyzing their ability to accept genuine signatures and to reject forgeries.

In this paper, we evaluate the robustness of signature verification systems to forgeries created with an increasing level of skill. For this purpose, we use the BiosecurID database [6], which contains both on-line and off-line versions of signatures acquired in several sessions with an incremental level of skill in the forgeries. For the verification experiments, three machine experts exploiting information at different levels have been used (one on-line [7] and two off-line [8, 9]). Several enrolment strategies with different size and variability of the enrolment set are studied.

The rest of this paper is organized as follows. The problem of forgeries with different level of skill is briefly addressed in Section 2. The three machine experts used are described in Section 3. The experimental framework used, including the database and protocol, is described in Section 4. The results obtained are presented in Section 5, and conclusions are finally drawn in Section 6.

2. Types of forgeries in signature recognition

When considering forgeries, five categories can be defined depending on the level of attack [10].

- **Random forgeries**, simulated by using signatures from other users as input, so no knowledge about the signature being attacked is exploited. This case does not represent intentional forgeries, but accidental accesses by impostors without information to help them in their attack to the system.

- **Blind forgeries**, which are signature samples generated by intentional impostors that have access to a de-

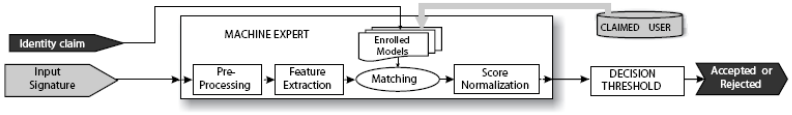


Figure 1. System model for person authentication based on handwritten signature.

scriptive or textual knowledge of the original signatures (e.g. the name of the person).

- **Static forgeries** (low-force in [10]), where the forger has access to a visual static image of the signature. There are two ways to generate the forgeries. In the first one, the forger can use a blueprint to copy the signature, leading to static **blueprint** forgeries. In the second one, the forger can train to imitate the signature, with or without a blueprint, for a limited or unlimited amount of time. The forger then generate the imitated signature, without the help of the blueprint, leading to static **trained** forgeries.

- **Dynamic forgeries** (brute-force in [10]), where the forger has access to a visual static image and to the whole writing process (i.e. the dynamics). The dynamics can be obtained in the presence of the original writer, or through a video-recording, or also through the obtention of the on-line version of the signature. In a similar way as the previous category, the forger can then generate two types of forgeries. Dynamic **blueprint** forgeries are generated by projecting on the acquisition area a real-time pointer that the forger needs to follow. Dynamic **trained** forgeries are produced after a training period where the forger can use dedicated tools to analyze and train to reproduce the genuine signature.

- **Regained forgeries**, where the forger has only access to the static image of the signature and makes use of a dedicated software to regain its dynamics, which are later analyzed and used to create dynamic forgeries.

3. Signature verification systems

This section describes the basics of the three machine experts used in this paper. They exploit information at two different levels. The on-line signature system is based on local image analysis and left-to-right Hidden Markov Models [7]. For off-line analysis, we use an approach based on global analysis of the image [9] and a second approach based on local analysis [8]. In Figure 1, the overall system model of a signature machine expert is depicted.

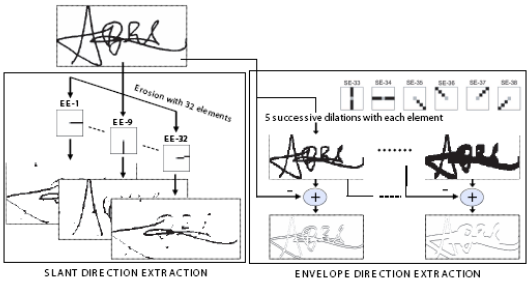


Figure 2. Feature extraction stage performed in the global off-line system.

3.1. On-line system based on HMM

The on-line signature verification system [7] is based on the recognition algorithm from ATVS presented at the First International Signature Verification Competition (SVC 2004)[1]. Coordinate trajectories and the pressure signal are considered. Signature trajectories are first preprocessed by subtracting the center of mass followed by a rotation alignment based on the average path tangent angle. An extended set of 14 discrete-time functions are then derived from the preprocessed trajectories. Given an enrolment set of K signatures of a client, a left-to-right Hidden Markov Model (HMM) is estimated and used for characterizing the client identity (2 states, 32 Gaussian mixtures per state). This HMM is used to compute the similarity matching score between a given test signature and a claimed identity.

3.2. Global off-line system

This system is based on global image analysis and a minimum distance classifier [9]. In this matcher, slant directions of the signature strokes and those of the envelopes of the dilated signature images are extracted with mathematical morphology operators. For slant direction extraction, the preprocessed signature image is eroded with 32 structuring elements as those shown in Figure 2 (left). A slant direction feature sub-vector of 32 components is then generated, where each component is computed as the signature

[1] www.cs.ust.hk/svc2004

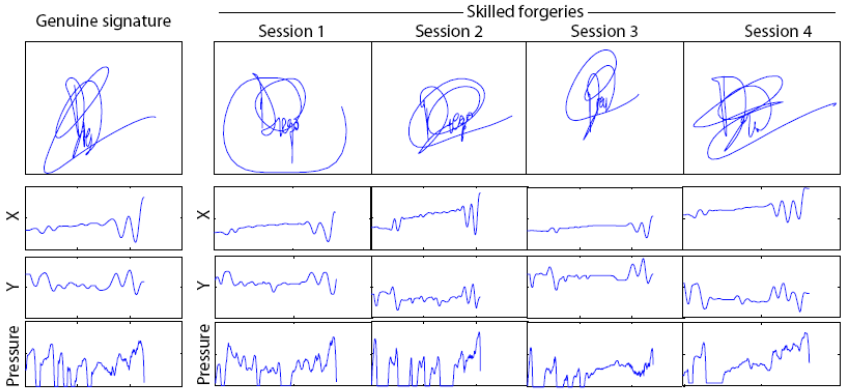


Figure 4. Signature examples from the BiosecurID Database. The left sample is a genuine signature and the remaining ones are forgeries with incremental level of skill. In each case, plots below each signature correspond to the on-line information stored in the database.

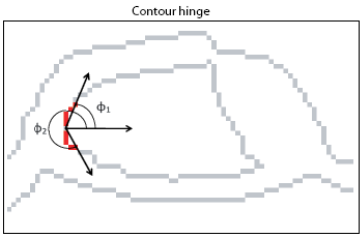


Figure 3. Graphical example of the contour curvature (local off-line system).

pixel count in each eroded image. For envelope direction extraction, the preprocessed signature image is successively dilated 5 times with the 6 structuring elements shown in Figure 2 (right). An envelope direction feature sub-vector of 5×6 components is then generated, where each component is computed as the signature pixel count in the difference image between successive dilations. The preprocessed signature is parameterized by concatenating the slant and envelope feature sub-vectors. Each client (enrolee) of the system is modeled by the mean and standard deviation vectors of an enrolment set of K parameterized signatures. To compute the similarity score between a claimed model and a parameterized test signature, the inverse of the Mahalanobis distance is used.

3.3. Local off-line system

This matcher uses contour level features [8]. Curvature of the contour is computed as follows. We consider two contour fragments attached at a common end pixel and compute the joint probability distribution of the orientations ϕ_1 and ϕ_2 of the two sides, see Figure 3. A joint density function (PDF) is obtained, which quantifies the chance of finding two "hinged" contour fragments with angles ϕ_1 and ϕ_2, respectively. Each client of the system (enrolee) is represented by a PDF that is computed using an enrolment set of K signatures. To compute the similarity between a claimed identity and a given signature, the χ^2 distance is used.

4 Database and experimental protocol

4.1 Database

We have used for our experiments a sub-corpus of the BiosecurID multimodal database [6], containing signatures from 133 users acquired in 4 different sessions distributed in a 4 months time span. Each user has 4 genuine signatures and 3 forgery signatures per session (from 3 different forgers, the same for the 4 sessions). The resulting sub-corpus has $133 \times 4 \times (4+3) = 3,724$ signatures.

An incremental level of skill in the forgeries was considered during the acquisition of each session, resulting in four different scenarios (see Figure 4): **Skill level 1** in session 1, where the forger only sees the signature image once (off-line information) and tries to imitate it; **Skill level 2** in session 2, where the forger sees the signature image once (off-

Figure 5. Enrolment strategies considered.

line information), trains for a minute in a piece of paper, and then imitates the signature; **Skill level 3** in session 3, where the forger sees the dynamic signature process 3 times using a dedicated software (on-line information), trains for a minute in a piece of paper, and then imitates the signature; and **Skill level 4** in session 4, where the forger sees the dynamic signature (on-line information) as many times as he/she requests, trains for a minute in a piece of paper and then imitates the signature. Following the nomenclature of Section 2, forgeries of sessions 1 and 2 are static forgeries, and those of sessions 3 and 4 are dynamic forgeries.

4.2 Experimental Protocol

Several enrolment strategies are considered in this paper using genuine signatures from sessions 1 to 3, see Figure 5: **Scenario 1**: using K=4 genuine signatures from the first session (mono-session). This scenario models the situation where users are enrolled in the system by providing 4 signatures consecutively (i.e. in the same session). **Scenario 2**: using K=4 genuine signatures, but considering also signatures from the second and third sessions (multi-session), capturing more user variability. **Scenario 3**: increasing the size of the enrolment set to K=12 signatures by taking all signatures from sessions 1 to 3 (multi-session).

For each scenario, the four genuine signatures of session 4 are used for testing. Real impostor test scores are computed by using the 3 skilled forgeries of each session. As a result, we have 133$\times$4=532 genuine similarity scores for each scenario, and four sets of 133$\times$3=399 scores from skilled forgeries for each scenario.

5 Results

Figure 6 shows the system performance based on the level of skill in the forgeries for the three machine experts used in this paper. We also report the results when fusing the two off-line systems available using the TANH normalization proposed in [11] and the SUM fusion rule.

Concerning the off-line systems, Figure 6 shows that a significant degradation in the verification performance is only observed for the maximum level of skill in the forgeries (level 4). For the other levels (1 to 3), there is no clear degradation in the performance. On the contrary, the on-line system exhibits a progressive degradation from level 1 to 4. These results suggest that the progressive level of skill in the forgeries that are introduced from level 1 to 4 mainly affects to the dynamic information of signatures, which are analyzed solely by the on-line system. Off-line systems, which analyze static information, are not as heavily affected (only in level 4).

Regarding the three enrolment scenarios considered, we observe that the performance is progressively improved from scenario 1 (K=4 genuine signatures from one session) to scenario 3 (K=12 signatures from three sessions). The only exception is the global off-line system, which does not show significant differences between scenario 1 and 2. Worth noting, the on-line system is quite robust to the level of skill in the forgeries in the scenario 3, resulting in similar performance in levels 2 to 4.

It is also worth noting that the on-line system results in the highest relative performance improvement in the multi-session enrolment scenarios. Since it exploits the dynamic information available in on-line signatures, it is more benefited by the incorporation of user variability and/or additional signatures in the enrolment set. In this sense, we also observe that the biggest improvement in the on-line system is from the enrolment scenario 1 to 2 (i.e., mono- vs multi-session training for the same number of enrolment signatures), which is much higher than from scenario 2 to 3 (i.e., from 4 to 16 multi-session training signatures). This result highlights the importance of an adequate enrolment representative of the natural multi-session signer variability, which can be obtained even with a reduced number of training signatures. The fusion of the two off-line systems also increases the relative improvement figures when considering better enrolment scenarios with respect to the two systems alone. In this case, the improvement from enrolment scenario 1 to 2 is similar to the one observed from scenario 2 to 3. This means that for different enrolment strategies in off-line recognition the performance improvement mainly comes from larger training sets, not from the multi-session aspect in the enrolment data, which was crucial in the online case.

6 Conclusions

The robustness of signature verification systems to forgeries with increasing level of skill has been studied. For this purpose, a database containing forgeries with incremental level of skill has been used. Three machine experts exploiting information at different levels have been used in the experiments: one off-line system based on local information that uses contour level features, one off-line system based

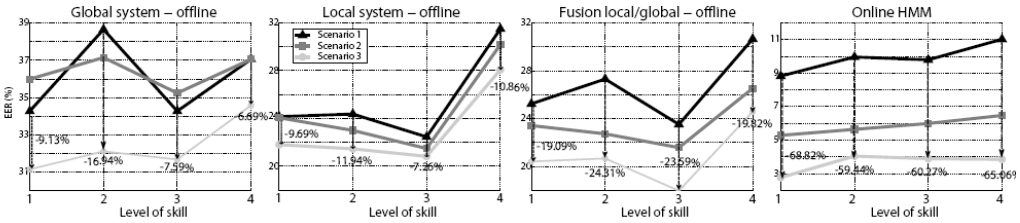


Figure 6. Verification performance based on the level of skill in the forgeries for the different scenarios presented in Section 4.2. Results are given in terms of Equal Error Rates (in %). For each level of skill, it is also given the relative gain of performance of the scenario 3 with respect to the scenario 1.

on global image analysis that computes slant directions of the signature strokes and those of the envelopes of the dilated signature images, and one on-line system based on HMM. Several enrolment strategies with different size and variability of the enrolment set have been also compared.

Our experiments show that the performance of the off-line systems is only degraded with the highest level of skill in the forgeries. On the contrary, the on-line system exhibits a progressive degradation with the level of skill, suggesting that the dynamic information of signatures is the one more affected by the considered increasing skills of the forgers.

Concerning the three enrolment scenarios proposed, it is observed that the performance of the three machine experts is improved as we increase the size and the variability of the enrolment set. It is worthy to remark that the on-line system becomes nearly insensitive to the level of skill in the forgeries for the third scenario (i.e. the one which has the maximum size and variability in the enrolment set). This results stresses the importance of having enrolment models generated with enough data, and acquired at different moments. The scarcity of available templates when a user is enrolled in a system is precisely one of the problems of signature systems. As can be observed from our results, several templates are needed and template signatures should be captured in different sessions in order to obtain a robust model that can deal with the natural user intra-variability, but this is not always possible due to application and user convenience constraints. One solution to this problem could be the generation of synthetic signatures from a user, in order to obtain more signatures for enrolment [12]. This will be a source of future work.

7 Acknowledgments

This work has been supported by the TEC2006-13141-C03-03 project of the Spanish Ministry of Science and Technology. Author F. A.-F. thanks Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting his PhD studies. Author F. A.-F. is supported by a Juan de la Cierva Fellowship from the Spanish MICINN. Author J. F. is supported by a Marie Curie Fellowship from the European Commission. Author J. G. is supported by a FPU Fellowship from the Spanish MEC.

References

[1] A. Jain *et al*. Biometrics: A tool for information security. *IEEE Trans. Inf. Forensics and Sec.*, 1:125–143, 2006.

[2] M. Fairhurst. Signature verification revisited: promoting practical exploitation of biometric technology. *Electronics and Communication Engineering J.*, 9:273–280, Dec. 1997.

[3] R. Plamondon and S. Srihari. On-line and off-line handwriting recognition: A comprehensive survey. *IEEE Trans. Pattern Analysis and Machine Intelligence*, 22(1):63–84, 2000.

[4] J. Fierrez, J. Ortega-Garcia. *Handbook of Biometrics*, ch. 10. On-line signature verification, pp. 189–210. Springer, 2008.

[5] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. *Proc. ICB*, Springer LNCS-4642:386–395, 2007.

[6] J. Fierrez *et al*. BiosecurID: A multimodal biometric database. *Pattern Analysis and Applications (accepted)*, 2009.

[7] J. Fierrez *et al*. HMM-based on-line signature verification: Feature extraction and signature modeling. *Pattern Recognition Letters*, 28:2325–2334, 2007.

[8] A. Gilperez *et al*. Off-line signature verification using contour features. *Proc. ICFHR*, 2008.

[9] J. Fierrez-Aguilar *et al*. An off-line signature verification system based on fusion of local and global information. *Proc. BIOAW*, Springer LNCS-3087:295–306, 2004.

[10] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold. A new forgery scenario based on regaining dynamics of signature. *Proc. ICB*, Springer LNCS-4642:366–375, 2007.

[11] A. Jain, K. Nandakumar, and A. Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 38(12):2270–2285, December 2005.

[12] J. Galbally *et al*. Synthetic generation of handwritten signatures based on spectral analysis. *Defense and Security Symposium, Proc. SPIE (to appear)*, 2009.

Impact of Time Variability in Off-line Writer Identification and Verification

Fernando Alonso-Fernandez, Julian Fierrez, Almudena Gilperez, Javier Ortega-Garcia
Biometric Recognition Group - ATVS - http://atvs.ii.uam.es
Escuela Politecnica Superior - Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - 28049 Madrid, Spain
{fernando.alonso, julian.fierrez, almudena.gilperez, javier.ortega}@uam.es

Abstract

One of the biggest challenges in person recognition using biometric systems is the variability in the acquired data. In this paper, we evaluate the effects of an increasing time lapse between reference and test biometric data consisting of static images of handwritten signatures and texts. We use for our experiments two recognition approaches exploiting information at the global and local levels, and the BiosecurID database, containing 3,724 signature images and 532 texts of 133 individuals acquired in four acquisition sessions distributed along a 4 months time span. We report results of the recognition systems working both in verification (one-to-one) and identification (one-to-many) mode. The results show the extent of the impact that the time separation between samples under comparison has on the recognition rates, being the local approach more robust to the time lapse than the global one. We also observe in our experiments that recognition based on handwritten texts provides higher accuracy than recognition based on signatures.

1 Introduction

A wide variety of applications require reliable person recognition schemes to either confirm or to determine the identity of an individual. Biometrics refer to the automatic recognition of people based on their physiological or behavioral characteristics [1]. *Physiological biometrics* (e.g. fingerprint, face, iris, etc.) are strong modalities for recognition due to its distinctiveness and reduced subject-specific intra-variability. However, these modalities are usually more invasive and require cooperating subjects. On the other hand, *behavioral biometrics* (e.g. signature, gait, handwritting, keystroking, etc.) are less invasive, but they achieve less recognition accuracy, mainly because lower distinctiveness and larger variability across time.

The problem of writer recognition, which pertains to the category of behavioral biometrics, has received significant interest in recent years. Handwritten signatures as person verification means are widely accepted socially and legally, and are used for that purpose in many transactions daily [2]. On the other hand, the use of handwritten text to identify a person has also received significant interest, mainly due to its application in forensic casework (e.g. crimson notes) [3] and historic document authorship analysis.

There are two main automatic recognition approaches of handwritten material [4]: off-line and on-line. Off-line methods consider uniquely the signature or text image, so only static information is available for the recognition task, which is commonly acquired by document scanning [5]. On the other hand, on-line systems use pen tablets or digitizers which capture dynamic information such as velocity and acceleration of the signing and writing process, providing a richer source of information [6]. On-line recognition systems have traditionally shown to be more reliable as dynamic features are more discriminative between subjects and they are harder to imitate [7]. But in spite of its advantages, there are many cases in which online recognition cannot be used because the handwritten material is collected off-line. This is the case of many government/legal/financial transactions that are performed daily. Also, off-line examination is the common type of criminal casework for forensic experts worldwide [3].

This paper addresses the problem of time separation between acquisitions in automatic person authentication based on scanned images of handwritten signatures and texts. The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the reference model, thereby affecting the comparison. Our goal is to determine to what extent recognition rates are degraded when time between sample acquisitions is increased. For this purpose, we use the BiosecurID database [8], which contains handwritten signatures and texts from 133 subjects acquired in 4 different sessions along a 4 months time span. For our recognition experiments, we use two off-line systems based on global [9], and local [10] image analysis. The two systems are evaluated in both verification and identification mode. In verification mode, a one-to-one comparison between two samples is done, with a decision on whether or not the two samples are from the same person. On the other hand, in identification mode, the system identifies an individual by searching the reference models of all the subjects in the database for a match (one-to-many). As a result, the system returns a ranked list of candidates. Ideally, the first ranked candidate

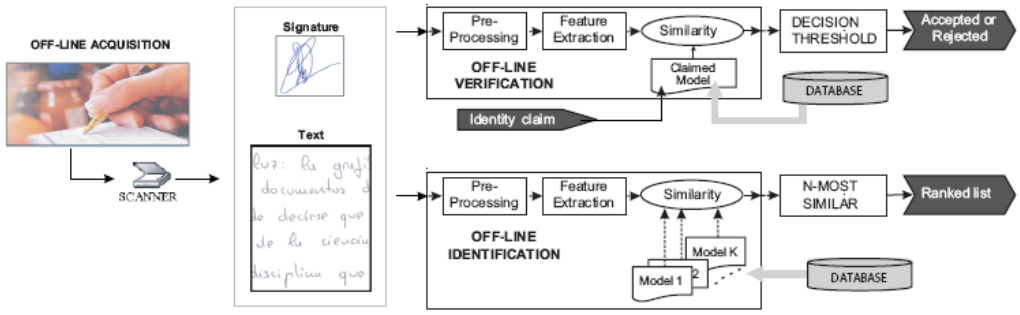


Figure 1. System model for person verification/identification based on handwritten signature and text images.

(Top 1) should correspond with the correct identity of the individual, but one can choose to consider a longer list (e.g. Top 10) to increase the chances of finding the correct identity. Identification is a critical component in *negative* recognition applications (or watchlists) where the aim is checking if the person is who he/she (implicitly or explicitly) denies to be, which is a typical situation in forensic/criminal cases [11]. Experiments reported here show the extent of the impact that the time separation between samples being compared has on the recognition rates, both in verification and identification mode. It is also observed in our experiments that using handwritten text images provides higher recognition accuracy than signature images, and that the local system always works better than the global one.

The rest of the paper is organized as follows. The two systems used are described in Section 2. The experimental framework used, including the database and protocol, is described in Section 3. The results obtained are presented in Section 4, and conclusions are finally drawn in Section 5.

2 Off-line recognition systems

This section describes the basics of the two recognition systems used in this paper. They exploit information at two different levels. We use an approach based on global analysis, which extracts features from the whole preprocessed image [9], and a second approach based on local image analysis [10]. In Figure 1, the overall model of a verification/identification system is depicted.

2.1 Global system

In the global system, input images are first *preprocessed* according to the following consecutive steps (see Table 1): binarization by global thresholding of the histogram [12], and noise removal by morphological closing operation on the binarized image [13]. For the case of signature images, a segmentation of the signature outer traces, and a normalization of the image size to a fixed width of 512 pixels while maintaining the aspect ratio are also carried out. Normalization of signature size is used to make the proportions of different signature realizations of an individual to be the same, whereas segmentation of the outer traces is carried out because a signature boundary typically corresponds to a flourish, which has high intra-user variability [9].

COMMON PREPROCESSING
- Binarization
- Noise removal
GLOBAL SYSTEM (signature only)
- Segmentation
- Size normalization
LOCAL SYSTEM
- Component detection
- Contour extraction

Table 1. Preprocessing stage performed in the global and local systems.

A *feature extraction stage* is then performed, in which slant directions of the strokes and those of the envelopes of various dilated images are extracted using mathematical morphology operators [13], see Figure 2. These descriptors are used as features for recognition as proposed in [14]. For slant direction extraction, the preprocessed image is eroded with 32 structuring elements (EE) like the ones presented in the left column of Figure 2, each one having a different orientation regularly distributed between 0 and 360 degrees [9], thus generating 32 eroded images. A slant direction feature sub-vector of 32 components is then generated, where each component is computed as the signature pixel count in each eroded image. For envelope direction extraction, the preprocessed image is successively dilated 5 times with each one of 6 linear structuring elements, whose orientation is also regularly distributed, thus generating 5×6 di-

lated images. An envelope direction feature sub-vector of 5×6 components is then generated, where each component is computed as the signature pixel count in the difference image between successive dilations. The preprocessed signature or text image is finally parameterized as a vector $\mathbf{o} = [o_1, ...o_{62}]$ with 62 components by concatenating the slant and envelope feature sub-vectors. Each client of the system is represented by a statistical model $\boldsymbol{\mu} = [\mu_1, ...\mu_{62}]$ which is estimated by using a reference set of K parameterized images $\{\mathbf{o}_1, ..., \mathbf{o}_K\}$. The parameter $\boldsymbol{\mu}$ denotes the mean vector of the K vectors $\{\mathbf{o}_1, ..., \mathbf{o}_K\}$. In the *similarity computation stage*, to compute the similarity between a claimed model $\boldsymbol{\mu}$ and a parameterized test image $\mathbf{o}$, the χ^2 distance is used:

$$\chi^2_{\mathbf{o}\boldsymbol{\mu}} = \sum_{i=1}^{N} \frac{(o_i - \mu_i)^2}{o_i + \mu_i} \quad (1)$$

where $N = 62$ is the dimensionality of the vectors $\mathbf{o}$ and $\boldsymbol{\mu}$. Prior to the computation of the χ^2 distance, the vectors $\boldsymbol{\mu}$ and $\mathbf{o}$ are normalized to unit length.

2.2 Local system

The *preprocessing stage* of the local system is divided in four parts, as shown in Table 1: binarization by global thresholding of the histogram [12], noise removal by morphological closing operation on the binarized image [13], connected component detection using 8-connectivity, and contour extraction using the Moore's algorithm [13].

In the *feature extraction stage*, curvature of the contour is computed as follows. We consider two contour fragments attached at a common end pixel and compute the directions ϕ_1 and ϕ_2 between that pixel and both fragments, see Figure 3. As the algorithm runs over the contour, a joint density function (pdf) $p(\phi_1, \phi_2)$ is then obtained by analyzing in this way the whole processed image, which quantifies the chance of finding two "hinged" contour fragments in the image with angles ϕ_1 and ϕ_2, respectively. Each client of the system is represented by a joint pdf that is computed using a reference set of K images. To compute the similarity between a reference model and a given image, the χ^2 distance (Equation 1) is used.

3 Database and protocol

We have used for our experiments a sub-corpus of the BiosecurID multimodal database [8], containing handwritten signatures and text from 133 subjects acquired in 4 different sessions distributed along a 4 months time span. Each subject has 4 genuine signatures and 3 forgery signatures per session (from 3 different forgers, the same for the 4 sessions). A Spanish text was also acquired in each session (the same for all subjects and sessions), handwritten in lowercase with no corrections or crossing outs permitted. The resulting sub-corpus has 133×4×(4+3)=3,724 signatures and 133×4=532 texts. All the handwritten data was captured

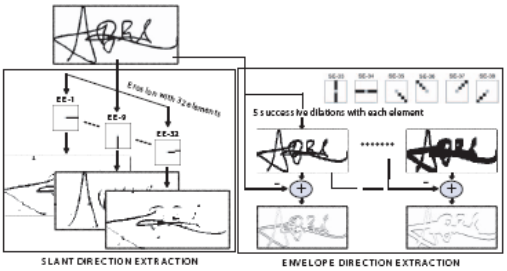


Figure 2. Feature extraction stage performed in the global off-line system.

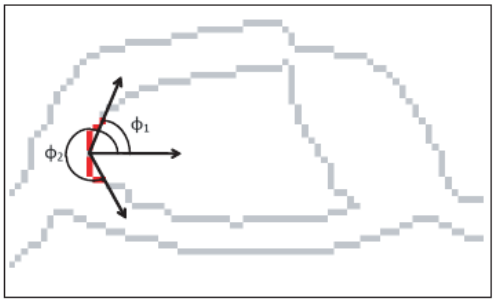


Figure 3. Graphical example of the contour curvature (local off-line system).

using an inking pen over a Wacom pen tablet so that both on-line dynamic signals and off-line versions (scanned images at 600 dpi) of the data are available. Each signature is written within a 2.5×15 cm^2 frame, and the texts were collected in a different sheet of paper with no guiding lines, just a square frame of 17×16 cm^2 highlighting the writing area. The average amount of text per written sheet is around 9-10 lines in a half A4 page. Some signature and text examples are given in Figure 4. Subjects are modeled for reference using K=4 genuine signatures from the first session and K=1 page of handwritten text, also from the first session. The remaining signatures and texts are used for testing.

Verification experiments with the signature modality are done as follows. Genuine test scores are computed by using the 4 genuine signatures of sessions 2 to 4, and real impostor test scores are computed by using all the available skilled forgeries. As a result, we have 133×4×3=1,596 scores from skilled forgeries and three sets of 133×4=532 genuine similarity scores. For the *identification experiments*, we use for testing the 4 genuine signatures of sessions 2 to 4. For each signature, the distances to all the 133 reference models are computed, outputting the N closest identities. An identification is considered successful if the correct identity is

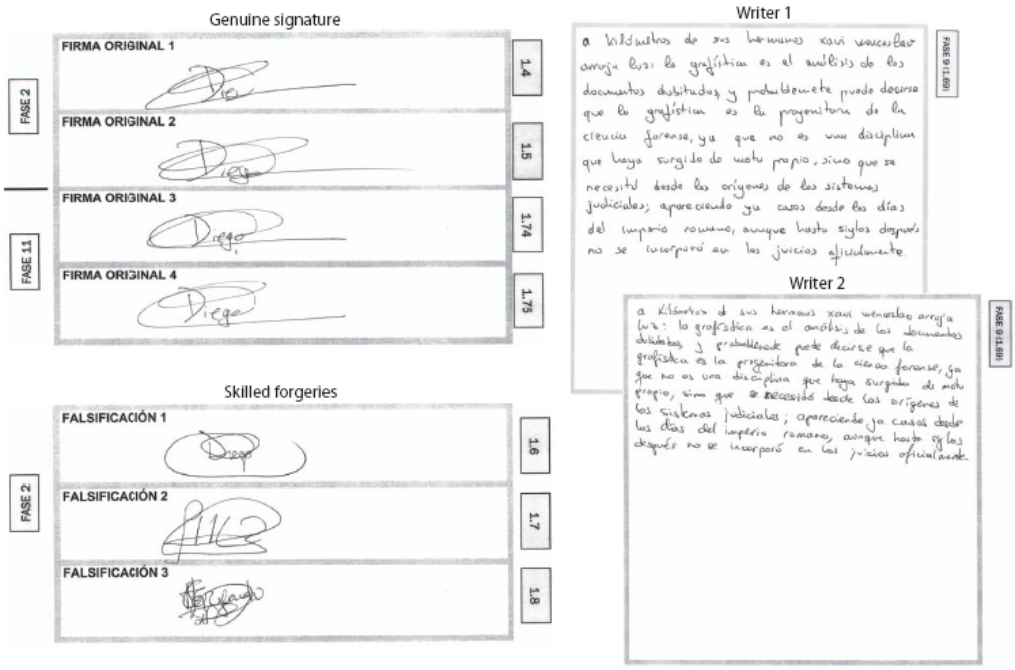


Figure 4. Signature and text examples from the BiosecurID database [8]. Left: four genuine signatures (top) and three forgeries (bottom). Right: one text example of two different writers.

among the N outputted ones. As a result, for the identification experiments we have three sets of 133×4×133=70,756 similarity scores.

Verification experiments with the handwritten texts are as follows. Genuine test scores are computed by using each text page of sessions 2 to 4, and impostor test scores are computed by using all the test pages from the remaining subjects. As a result, we have 133×132×3=52,668 scores from impostors and three sets of 133×1=133 genuine similarity scores. For the *identification experiments*, we use the genuine text page of sessions 2 to 4. For each page, the distances to all the reference models are computed, outputting the N closest identities. An identification is considered successful if the correct identity is among the N outputted ones. As a result, we have three sets of 133×133=17,689 similarity scores.

4 Results

In Figure 5, we show the results for the verification experiments comparing genuine samples from sessions with increasing separation in time. Results are given using either images of handwritten signatures or texts for the same 133 subjects. Verification results in terms of EER (where False Acceptance = False Rejection Rate) are also given in Figure 7 (left). Similarly, results for the identification experiments are given in Figure 6 and Figure 7 (right).

It is observed from our experiments that the time separation between samples being compared has impact on the recognition rates, both in verification and identification mode. Interestingly enough, we observe however, that once that a minimum time between samples has passed, error rates are not apparently increased. This is observed in Figures 5 and 6, where an small separation between lines marked "Session 1 vs. Session 3" and "Session 1 vs. Session 4" can be seen.

Concerning the two modalities evaluated, signature and handwriting, we observe that the latter always provides the highest recognition accuracy. In the verification experiments, the EER using handwritten texts is always below 10% (with an EER of 3% in the best case, see Figure 7). On the contrary, using handwritten signatures, the EER is in the 20-30% range. The explanation is that the texts in our database are written in around half A4 paper sheets, which contain much more discriminative information than signature images, which are done on a 2.5×15 cm^2 frame. Although we are using four signature images for reference, their discriminative information is still much less than the information contained in half page of handwritten text. Similar remarks can be done for the identi-

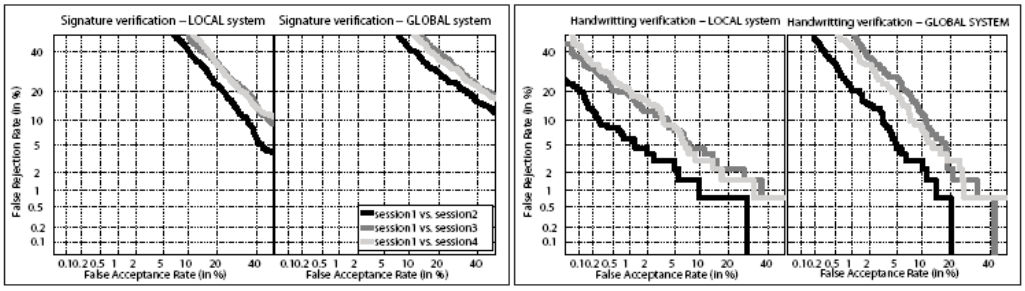


Figure 5. Performance of the verification experiments.

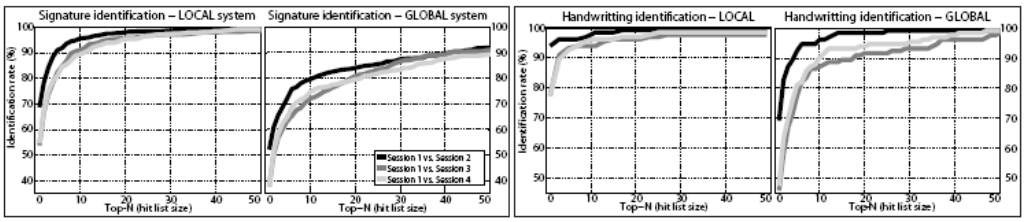


Figure 6. Performance of the identification experiments.

fication experiments. For a hit list size of 10, for instance (see Figure 7), identification rates are mostly above 90% using handwritten texts (with an identification rate of 98.5% in the best case); but using signature images, identification rates are in the 70-90% range in most cases.

Concerning the two recognition algorithms evaluated, we observe from Figures 5 and 6 that the local approach always works better than the global one, either using signatures or texts. This is because the local algorithm processes images locally, thus being able to capture finer details of the image. The global algorithm, on the contrary, processes images as a whole. As a result, it can be seen in Figure 7 that the local approach is less degraded than the global one when time separation between samples is increased (the only exception is the signature verification case). This effect is more evident in the identification case, where the performance of the local approach is only degraded 4.5%, but the global one is degraded 9.5% (when comparing "s1 vs. s2" to "s1 vs. s3").

5 Conclusion

This paper has studied the extent of the impact that the time separation between reference and test samples has on the verification and identification of handwritten signatures and text.

Two off-line recognition approaches exploiting information at the global and local levels and the BiosecurID database have been used in our experiments. This database contains scanned signature and text images of 133 individuals acquired in 4 sessions distributed along a 4 months time span, thus allowing to evaluate time variability. We have carried out experiments both in verification (one-to-one) and identification (one-to-many) mode. We have observed that the time separation between samples being compared has impact on the recognition rates, but once that a specific minimum time between samples has passed (about 2 months), error rates are not apparently worsened with an increased time span between reference and test samples (up to 4 months). This is of course a data-driven statement that should be also studied and validated for longer periods of time (interestingly, new efforts in multimodal database collection have recently enabled this kind of studies for time spans up to a couple of years [15]). The local recognition approach always works better than the global one, both using signatures and texts, and it is less degraded than the global one when time separation between samples is increased. This effect is more evident working in identification mode. We have also observed that recognition based on handwritten text images provides higher accuracy than based on signature images.

Existing technology evaluations have not been aimed to study the effects of time variability in signature and writer recognition [16, 17]. The results of this paper highlight the importance of this phenomenon and encourage its consideration in future technology benchmarks, e.g. [18, 19]. Finally, the results of this paper motivates us to study the individual factors that make some signatures and writers to be more consistent in time than others, in order to develop quality measures that can predict the verification/identification performance [20]. These quality measures can be very useful to compensate the performance

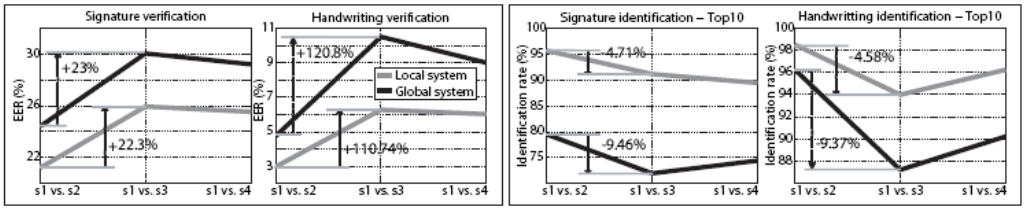


Figure 7. Verification and identification performance of the signature and handwriting modalities when matching genuine samples from different sessions. Verification results are given in terms of EER (%), while identification experiments are given in terms of success rate (%) for a hit list size of 10. The relative variation of performance is also given. The terms "s1", "s2" and "s3" stand for "session 1", "session 2" and "session 3" respectively.

drop encountered with increased time spans between reference and test, e.g., using quality-activated template update techniques [21], or quality-based information fusion [22].

6 Acknowledgements

This work has been supported by Spanish MCYT TEC2006-13141-C03-03 project. Author F. A.-F. is supported by a Juan de la Cierva Fellowship from the Spanish MICINN. Author J. F. is supported by a Marie Curie Fellowship from the European Commission.

References

[1] A. Jain, A. Ross, S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Trans. IFS*, 1, 2006, pp. 125–143.

[2] M. Fairhurst, "Signature Verification Revisited: Promoting Practical Exploitation of Biometric Technology", *Electronics & Communication Engineering J.*, 9, 997, pp. 273–280.

[3] S. Srihari, C. Huang, H. Srinivasan, V. Shah, *Digital Document Processing*, ch. 17. Biometric and Forensic Aspects of Digital Document Processing, pp. 379–406. Springer, 2007.

[4] R. Plamondon, S. Srihari, "On-line and Off-line Handwriting Recognition: A Comprehensive Survey", *IEEE Trans. on PAMI*, 22(1), 2000, pp. 63–84.

[5] D. Impedovo and G. Pirlo, "Automatic Signature Verification: The State of the Art", *IEEE Trans. on SMC-C*, 38(5), 2008, pp. 609–635.

[6] J. Fierrez and J. Ortega-Garcia, *Handbook of Biometrics*, chapter 10. On-line Signature Verification, pp. 189–210. Springer, 2008.

[7] G. Rigoll and A. Kosmala, "A Systematic Comparison Between On-line and Off-line Methods for Signature Verification with Hidden Markov Models", *Proc. ICPR*, 2, 1998, pp. 1755–1757.

[8] J. Fierrez, *et al.*, "BiosecurID: A Multimodal Biometric Database", *Pattern Analysis and Applications (accepted)*, 2009.

[9] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, J. Ortega-Garcia, "An Off-line Signature Verification System Based on Fusion of Local and Global Information", *Proc. BIOAW*, Springer LNCS-3087, 2004, pp.295–306.

[10] A. Gilperez, F. Alonso-Fernandez, S. Pecharroman, J. Fierrez, and J. Ortega-Garcia, "Off-line Signature Verification Using Contour Features", *Proc. ICFHR*, 2008.

[11] A. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition", *IEEE Trans. on CSVT*, 14(1), January 2004, pp. 4–20.

[12] N. Otsu, "A Threshold Selection Method for Gray-level Histograms", *IEEE Trans. SMC*, 9, December 1979, pp. 62–66.

[13] R. Gonzalez and R. Woods, *Digital Image Processing*, Addison-Wesley, 2002.

[14] L. Lee and M. Lizarraga, "An Off-line Method for Human Signature Verification", In *Proc. ICPR*, pp. 195–198, 1996.

[15] J. Ortega-Garcia, *et al.*, "The Multi-scenario Multi-environment BioSecure Multimodal Database (BMDB)", *IEEE Trans. on PAMI (to appear)*, 2009.

[16] D. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "SVC2004: First International Signature Verification Competition", *Proc. ICBA*, Springer LNCS-3072, July 2004, pp. 15–17.

[17] N. Poh, T. Bourlai, J. Kittler, L. Allano, F. Alonso-Fernandez, O. Ambekar, J. Baker, B. Dorizzi, O. Fatukasi, J. Fierrez, H. Ganster, J. Ortega-Garcia, D. Maurer, A. Salah, T. Scheidat, and C. Vielhauer, "Benchmarking Quality-Dependent and Cost-Sensitive Score-Level Multimodal Biometric Fusion Algorithms", *IEEE Trans. IFS (to appear)*, 2009.

[18] B. Dorizzi, R. Cappelli, M. Ferrara, D. Maio, D. Maltoni, N. Houmani, S. Garcia-Salicetti, and A. Mayoue, "Fingerprint and On-line Signature Verification Competitions at ICB 2009", *Proc. ICB*, LNCS-5558, 2009, pp. 725–732.

[19] SigComp09, "Signature Verification Competition - http://sigcomp09.arsforensica.org", 2009.

[20] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez, J. Ortega-Garcia, "Automatic Measures for Predicting Performance in Off-line Signature", *Proc. ICIP*, 1, September 2007, pp. 369–372.

[21] F. Roli, L. Didaci, and G. Marcialis, "Template Co-update in Multimodal Biometric Systems", *Proc. ICB*, Springer LNCS-4642, 2007, pp. 1194–1202.

[22] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, and J. Bigun, "Discriminative Multimodal Biometric Authentication Based on Quality Measures", *Pattern Recognition*, 38(5), 2005, pp. 777–779.