

UNIVERSIDAD AUTÓNOMA DE MADRID

ESCUELA POLITÉCNICA SUPERIOR



PROYECTO FIN DE CARRERA

**ESTUDIO DE INTEROPERABILIDAD EN
SISTEMAS BIOMÉTRICOS DE FIRMA
MANUSCRITA DINÁMICA**

Ingeniería de Telecomunicación

Rubén Tolosana Moranchel
Octubre 2014

ESTUDIO DE INTEROPERABILIDAD EN SISTEMAS BIOMÉTRICOS DE FIRMA MANUSCRITA DINÁMICA

AUTOR: Rubén Tolosana Moranchel
TUTOR: Rubén Vera Rodríguez



ATVS Grupo de Reconocimiento Biométrico
Dpto. de Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Octubre 2014

Resumen

En este proyecto se estudian, implementan y evalúan sistemas de reconocimiento biométrico de firma dinámica en presencia de firmas procedentes de distintos dispositivos de captura. Para llevarlo a cabo se han utilizado y comparado diversas técnicas del estado del arte en reconocimiento de firma. A su vez se ha realizado un estudio de las diversas técnicas de normalización de datos usadas en el ámbito de reconocimiento biométrico para conseguir un sistema robusto independientemente del dispositivo de captura utilizado para entrenar o testear el sistema.

Como punto de partida del proyecto se ha realizado un estudio de las diferentes técnicas que han ido marcando el estado del arte, haciendo especial hincapié en los sistemas basados en características globales y en los sistemas basados en características locales o funciones temporales.

Una vez entendido el estado del arte desde el punto de vista teórico, el siguiente paso ha sido definir la tarea sobre la que se han evaluado las diferentes técnicas. Históricamente, la tarea principal en evaluaciones de firma dinámica ha consistido en entrenar y testear el sistema con firmas obtenidas de un mismo dispositivo de captura (sin interoperabilidad). En la tarea que hemos llevado a cabo para la realización de este proyecto disponemos de firmas de un mismo usuario obtenidas con distintos dispositivos de captura.

Para la parte experimental se han llevado a cabo tres etapas. Durante la primera etapa el objetivo fue evaluar el rendimiento del sistema de verificación de firma dinámica con y sin interoperabilidad siguiendo el protocolo de las evaluaciones Biosecure Multimodal Evaluation Campaign (*BMEC*). En la segunda etapa se estudió y se aplicó al sistema con interoperabilidad técnicas de normalización presentes en el ámbito de reconocimiento biométrico con el objetivo de conseguir un rendimiento lo más parecido posible al sistema sin interoperabilidad. En la última etapa se ha aplicado técnicas de selección y fusión de características para obtener un sistema global robusto ante firmas de test provenientes de distintos dispositivos de captura.

Finalmente, se presentan las conclusiones extraídas a lo largo de este trabajo, así como las posibles líneas de trabajo futuro.

Palabras Clave

Sistema biométrico, reconocimiento de firma, interoperabilidad, firma On-line, DTW.

Abstract

This thesis is focused on the development of a robust dynamic signature verification system dealing with interoperability (e.g. PDA, pen tablet). The goal of this project is to obtain an acceptable recognition performance when it is trained and tested with signatures coming from different capturing devices.

As an starting point, an exhaustive study of the state-of-the-art on dynamic signature verification techniques has been conducted. In this sense, particular attention was paid on recognition systems but also on feature selection algorithms (*SFFS*), data normalization, score normalization techniques and fusion of global and local systems. It is worth noting that little attention has been paid in the literature to the problem of interoperability in the field of dynamic signature recognition.

In order to carry out an evaluation of the recognition systems, we use the data and experimental protocols defined in Biosecure Multimodal Evaluation Campaign (*BMEC*). The experiments conducted were divided in three phases. First we evaluated the recognition of the systems with and without interoperability. Secondly we studied data normalization methods in order to improve the similarity among signatures from different devices. Finally the goal was to obtain a global robust system with acceptable performance in scenario with signatures coming from different devices. To achieve this, feature selection algorithms and fusion methods were used.

Key words

Biometric system, signature recognition, interoperability, On-line signature, DTW.

Agradecimientos

En primer lugar, quiero dar mi más sincero agradecimiento a mi tutor Rubén por haberme dado la oportunidad de realizar este proyecto. Por su atención y constante apoyo, siempre dispuesto a atenderme con buen humor para resolver dudas y comentar soluciones que hiciesen el trabajo más gratificante.

También, a cada uno de los componentes del ATVS que de una forma u otra me han ayudado a realizar este trabajo y que desde un primer momento me han integrado en esta gran familia. Es un placer estar con estos grandes profesionales y sobre todo grandes personas y adquirir tantos y tan buenos conocimientos.

Me gustaría dedicar unas líneas de estos agradecimientos a mis compañeros de la carrera, con los que he pasado tantos momentos. Gracias a todos aquellos que me han animado y me han sacado una sonrisa incluso en los largos días de prácticas y tardes de sufrimiento.

A mis amigos de siempre, tanto del pueblo como de Sanse y Alcobendas, que incluso en duras épocas de exámenes y prácticas se han preocupado de animarme para conseguir todos los objetivos, como han hecho a lo largo de toda mi vida.

Pero sin lugar a dudas a quien más tengo que agradecer su apoyo constante, su confianza en mí en todo momento y su ayuda incondicional, es a mis padres y a mis hermanos Álvaro y Jorge que han sabido guiarme en todo momento por el buen camino.

A todos muchas gracias.

Rubén Tolosana Moranchel
Octubre 2014

Índice general

Índice de figuras	VII
Índice de tablas	x
Preámbulo	1
1. Introducción.	3
1.1. Motivación del proyecto.	3
1.2. Objetivos y enfoque.	4
1.3. Metodología y plan de trabajo.	5
1.4. Organización de la memoria.	6
2. Estado del arte.	7
2.1. Introducción	7
2.2. Sistemas de reconocimiento biométrico	7
2.2.1. Modos de operación	7
2.2.2. Características de los rasgos biométricos	9
2.3. Sistemas de verificación de firma manuscrita dinámica	12
2.3.1. Arquitectura	12
2.3.2. Sistemas globales o basados en características globales	14
2.3.3. Sistemas locales o basados en funciones temporales	14
2.3.3.1. <i>Dynamic Time Warping</i>	15
2.3.3.2. <i>Hidden Markov Models</i>	16
2.3.4. Algoritmos de selección de características	17
2.3.4.1. <i>Scalar Feature Selection</i>	18
2.3.4.2. <i>Sequential Forward/Backward Selection</i>	18
2.3.4.3. <i>Floating Search</i>	18
2.3.5. Bases de datos de firma manuscrita dinámica	19

3. Sistema de verificación de firma dinámica. Implementación.	23
3.1. Sistema global de verificación de firma	23
3.2. Sistema local de verificación de firma	25
4. Experimentos.	29
4.1. Base de datos	29
4.2. Protocolo de experimentación. Interoperabilidad	31
4.3. Desarrollo experimental	32
4.3.1. Rendimiento del sistema. Experimentos iniciales	32
4.3.1.1. Características globales	32
4.3.1.2. Características locales	34
4.3.2. Normalizaciones de los datos de entrada	37
4.3.2.1. Normalización por el centro de masas	37
4.3.2.2. Normalización por la media y desviación típica	37
4.3.2.3. Normalización por el máximo y el mínimo	38
4.3.3. Rendimiento del sistema aplicando normalizaciones	39
4.3.3.1. Características globales	39
4.3.3.2. Características locales	42
4.3.4. Selección de las características del sistema	44
4.3.4.1. Características globales	45
4.3.4.2. Características locales	48
4.3.5. Fusión de los sistemas global y local	49
4.4. Validación experimental	51
5. Conclusiones y trabajo futuro.	55
5.1. Conclusiones.	55
5.2. Trabajo futuro	56
Glosario de acrónimos	57
Bibliografía	58
A. Normalizaciones estudiadas. Resultados	63
A.0.1. Características Globales.	63
A.0.2. Características Locales.	63
B. Presupuesto	69
C. Pliego de condiciones	71

Índice de figuras

1.1.	<i>Diagrama del plan de trabajo seguido.</i>	5
2.1.	<i>Esquema de funcionamiento de un sistema de reconocimiento biométrico en la etapa registro. Figura adaptada de [1].</i>	8
2.2.	<i>Esquema de funcionamiento de un sistema de reconocimiento biométrico en modo identificación. Figura adaptada de [1].</i>	8
2.3.	<i>Esquema de funcionamiento de un sistema de reconocimiento biométrico en modo verificación. Figura adaptada de [1].</i>	9
2.4.	<i>Ejemplo de una curva DET para un sistema biométrico.</i>	10
2.5.	<i>Rasgos biométricos humanos.</i>	11
2.6.	<i>Arquitectura típica de un sistema de verificación de firma.</i>	13
2.7.	<i>(a) Ejemplo de un factor de ponderación $w(k)$ simétrico para DTW. (b) Ejemplo de la correspondencia punto a punto usando DTW entre dos secuencias de firmas genuinas.[2]</i>	16
2.8.	<i>Estructura de un modelo HMM de izquierda a derecha de N estados, con M componentes GMMs y sin saltos entre estados. Ref.[2]</i>	17
2.9.	<i>(a) Proceso de captura utilizando una PDA en BioSecure DS3 - Mobile Scenario dataset. (b) Proceso de captura utilizando el pen-tablet en BioSecure DS2 - Access Control Scenario dataset.</i>	21
2.10.	<i>Ejemplos de firmas y sus correspondientes señales disponibles para BioSecure Multimodal DataBase DS2 y DS3, capturadas usando un pen tablet (superior) y una PDA (inferior), respectivamente. Ref. [2]</i>	22
3.1.	<i>Ejemplos de las 21 funciones temporales (características locales) consideradas en el sistema. Las gráficas de la izquierda se corresponden a una firma genuina, mientras que las de la derecha a una imitada (skilled forgery). Ambas firmas se han obtenido de un usuario particular de la base de datos BIOSECURE DS2.</i>	27
4.1.	<i>Izquierda: Firmas genuinas de un mismo usuario capturadas con la PDA y el pen tablet. Derecha: Firmas skilled forgeries para el mismo usuario capturadas con la PDA y el pen tablet. Figura adaptada de [2]</i>	30
4.2.	<i>Firmas utilizadas para la realización de los experimentos. G corresponde a un bloque de 5 firmas genuinas y F a un bloque de 5 firmas forgery. Los bloques en gris no son utilizados.</i>	31

4.3.	<i>Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. Sin aplicar ningún tipo de normalización de los datos de entrada.</i>	33
4.4.	<i>Histograma del tipo de características obtenidas para cada uno de los casos. Las imágenes de la izquierda representan el caso sin interoperabilidad y las de la derecha con interoperabilidad.</i>	35
4.5.	<i>Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. Sin aplicar ningún tipo de normalización de los datos de entrada.</i>	36
4.6.	<i>Representación de firmas de las bases de datos DS2 y DS3 sin normalizar.</i>	38
4.7.	<i>Tipos de normalizaciones estudiadas.</i>	39
4.8.	<i>Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Aplicando normalización por el centro de masas.</i>	40
4.9.	<i>Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Aplicando normalización por el centro de masas.</i>	41
4.10.	<i>Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Aplicando normalización por la media y la desviación típica.</i>	43
4.11.	<i>Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Aplicando normalización por la media y la desviación típica.</i>	44
4.12.	<i>Características globales. Rendimiento medio del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. El punto indicado en la gráfica es el que proporciona el mejor resultado para las dos condiciones a optimizar.</i>	47
4.13.	<i>Características globales. Histograma del tipo de características seleccionadas por el algoritmo SFFS para el sistema global óptimo.</i>	48
4.14.	<i>Características locales. Rendimiento medio del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. El punto indicado en la gráfica es el que proporciona el mejor resultado para las dos condiciones a optimizar.</i>	49
4.15.	<i>Evolución del EER al variar el parámetro k para la fusión de los sistemas global y local.</i>	50
4.16.	<i>Curvas DET para los casos (a) skilled forgeries y (b) random forgeries usando fusión de sistemas para el set de 70 usuarios de evaluación.</i>	52
A.1.	<i>Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS2.</i>	64
A.2.	<i>Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS3.</i>	64

A.3. Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS2.	65
A.4. Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS3.	65
A.5. Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS2.	66
A.6. Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS3.	66
A.7. Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS2.	67
A.8. Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS3.	67

Índice de tablas

2.1.	<i>Comparación cualitativa de las características de los distintos rasgos biométricos (A=Alto, M=Medio, B=Bajo). Fuente: [3].</i>	12
2.2.	<i>Bases de datos de firma manuscrita dinámica.</i>	20
3.1.	<i>Set de características globales. T denota intervalo de tiempo, t denota instante de tiempo, N denota número de eventos y θ denota el ángulo. Notar que algunos símbolos son definidos en diferentes características de la tabla (e.g. Δ de la característica 7 está definido en la característica 15). Fuente: [2]</i>	24
3.2.	<i>Set de características locales utilizado en el presente proyecto. El punto situado encima de algunas características (e.g. \dot{x}_n) indica derivada en el tiempo. Tabla adaptada de [2].</i>	26
4.1.	<i>Características globales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 30 de características óptimo para cada caso) y el caso de elegir únicamente el vector de características del caso crítico (skilled-DS2-DS3).</i>	45
4.2.	<i>Características globales que más se repiten en el conjunto de los 8 vectores de características óptimos (seleccionando 30 características en cada uno de ellos).</i>	45
4.3.	<i>Características globales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 30 características óptimo para cada caso) y el caso de elegir únicamente el vector de características más repetido.</i>	46
4.4.	<i>Características globales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 30 características óptimo para cada caso) y el caso de elegir únicamente un vector de características obtenido con el algoritmo SFFS.</i>	47
4.5.	<i>Características locales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 8 características óptimo para cada caso) y el caso de elegir únicamente el vector de características obtenido con el algoritmo SFFS.</i>	48
4.6.	<i>Resultados de EER para el sistema global, sistema local y la fusión de ambos sistemas con la fórmula propuesta 4.3.5 para el caso skilled forgeries.</i>	51
4.7.	<i>Resultados de EER para el sistema global, sistema local y la fusión de ambos sistemas con la fórmula propuesta 4.3.5 para el caso random forgeries.</i>	51
4.8.	<i>Rendimiento del sistema sobre el conjunto de 70 usuarios de evaluación utilizando fusión de los sistemas global y local. Comparación de los resultados de EER obtenidos en [2] con el sistema implementado en el presente proyecto.</i>	52

Preámbulo

Notaciones utilizadas

Los *términos* pertenecientes al ámbito de las disciplinas tratadas han sido por norma general traducidos al castellano, salvo en dos casos: cuando el término en inglés es de uso común en la literatura en castellano y cuando, aun no estando extendido, su traducción no resulta directa.

El significado de los *acrónimos* aparecidos en el trabajo se incluye en el Glosario. Se han utilizado las siguientes *abreviaturas*: Cap. (capítulo), Sec. (sección), Fig. (figura) y Ecu. (Ecuación).

Para la *bibliografía* se ha optado por la notación **unsrc** de L^AT_EX por considerarla la más adecuada para este tipo de documentos por legibilidad y elegancia. Ejemplos de esta notación son [2] para referencias entre corchetes y para referencias *inline*.

Herramientas utilizadas

El presente trabajo ha sido redactado por el autor usando L^AT_EX. El formato del texto es Computer Roman Modern a tamaño 11pt.

Los programas utilizados para la elaboración del proyecto son Matlab, Texmaker, Cygwin y Putty.

Nota sobre el copyright ©

Los derechos de cualquier marca comercial o registrada mencionada en el presente documento son propiedad de sus respectivos titulares.

1

Introducción.

La necesidad de mejorar la seguridad en diferentes contextos de la sociedad actual dan lugar a un nuevo concepto de identidad de cada individuo. Los sistemas tradicionales de identificación tienen carencias que contrastan con dichas necesidades: están basados o requieren información adicional que el sujeto **recuerda** como claves de acceso o que el sujeto **posee** como documentos de identidad o tarjetas de acceso que se pueden perder, robar e incluso falsificar fácilmente provocando problemas de seguridad. Esto da lugar al desarrollo de varias técnicas de reconocimiento automático basadas en rasgos biométricos que permiten la identificación de individuos de forma segura y rápida en función de lo que el sujeto **es** o cómo se **comporta**, puesto que no se precisa mayor información que la contenida en dichos rasgos inherentes a las personas como la voz, la firma, la cara, el iris, la huella dactilar, las manos, etc. [4]

Hoy en día es común observar sistemas de verificación de huella dactilar en dispositivos móviles o PCs, sistemas de reconocimiento de cara en controles fronterizos y de iris en algunos aeropuertos (e.g. Emiratos Árabes Unidos).

La **firma** es uno de los rasgos biométricos más aceptados socialmente, ya que ha sido utilizada en transacciones financieras y legales durante cientos de años. Otra de las ventajas de los sistemas de firma es la **facilidad** para adquirir las firmas de los usuarios, firmando para ello en papel con un bolígrafo de tinta o utilizando dispositivos tecnológicos (e.g. pen tablet, PDA, smartphone). Además hay que tener en cuenta que la firma, como rasgo biométrico, no se ve tan afectado por condiciones externas (e.g. luz, ruido, suciedad de la mano) frente a otros rasgos como puede ser la cara o la huella dactilar.

1.1. Motivación del proyecto.

La proliferación en los últimos años de dispositivos táctiles ha permitido el desarrollo de sistemas de reconocimiento biométrico basados en la escritura y la firma manuscrita. El reconocimiento biométrico de firma es un problema complejo, ya que presenta una **alta** variabilidad entre firmas de un mismo sujeto (intra-clase), y una **baja** variabilidad entre firmas de diferentes sujetos (inter-clase), lo que complica la tarea de detección de firmas falsificadas.

En la práctica **las firmas** de los usuarios **pueden ser adquiridas por una gran cantidad de dispositivos** (e.g. PDA, pen tablet, smartphone). La gran evolución tecnológica que se está produciendo en este sector origina como resultado la aparición constante de nuevas versiones de estos dispositivos, con una mayor precisión y prestaciones. Todo esto conlleva a la desaparición de las versiones anteriores y por lo tanto un grave problema en el ámbito de reconocimiento biométrico. ¿Qué ocurre con las firmas de los usuarios almacenadas en la *BDD* que han sido capturadas con un dispositivo distinto al que se utiliza en la actualidad para verificar al usuario? ¿Afectará mucho al rendimiento del sistema? ¿Se debe volver a registrar a los usuarios cada vez que se actualicen los dispositivos de captura? Estas son algunas de las cuestiones que nos podemos plantear ante este escenario.

Interoperabilidad entre sistemas biométricos ha recibido relativamente poca atención en la literatura. Algunos de los ejemplos encontrados en las diferentes modalidades biométricas se recogen en [5] [6] [7].

Por otro lado, la gran aceptación por parte de la sociedad hacia los dispositivos táctiles, así como su uso común en aplicaciones legales y financieras, origina también como resultado la necesidad de realizar un estudio del comportamiento de dispositivos no pensados especialmente para la recogida de firmas manuscritas (e.g. PDA, smartphone, tablet). Además hay que destacar la posibilidad bastante común de que un mismo usuario intente acceder a una aplicación desde distintos tipos de dispositivos móviles.

Por estos motivos, este proyecto se enmarca en el área del estudio de **interoperabilidad en sistemas biométricos de firma manuscrita dinámica**.

1.2. Objetivos y enfoque.

Los trabajos realizados en este ámbito suelen ir enfocados a la mejora de un sistema cuando éste se encuentra entrenado y testeado por un mismo dispositivo de captura. Sin embargo, en este proyecto enfocado en la interoperabilidad de dispositivos se tienen los siguientes objetivos:

- Estudio de las diferentes técnicas del estado del arte que han producido buenos resultados en la última década con respecto al sistema de verificación de firma manuscrita dinámica.
- Comprensión e implementación de código que permita la realización de experimentos con distintas bases de datos.
- Evaluación de los resultados obtenidos en los experimentos al aplicar interoperabilidad de sistemas. Aplicación de técnicas de normalización en distintas etapas para mejorar el rendimiento del sistema (medido a través del *EER*).
- Obtención de la mejor configuración de parámetros para el sistema final y su correspondiente evaluación. Intentar mantener el rendimiento del sistema para los casos sin interoperabilidad y mejorarlo para los casos con interoperabilidad.
- Entender en profundidad el desafío de la interoperabilidad en sistemas de verificación de firma manuscrita dinámica. La tarea contenida en este proyecto es clave en los sistemas de firma manuscrita dinámica de la actualidad, por lo que se pretenden reconocer las limitaciones y posibles mejoras para poder continuar la investigación iniciada en este proyecto.

1.3. Metodología y plan de trabajo.

Para el correcto desarrollo y consecución de los objetivos marcados en el presente Proyecto Fin de Carrera, se ha seguido un plan de trabajo organizado en el tiempo como muestra la Fig. 1.1, detallado a continuación.

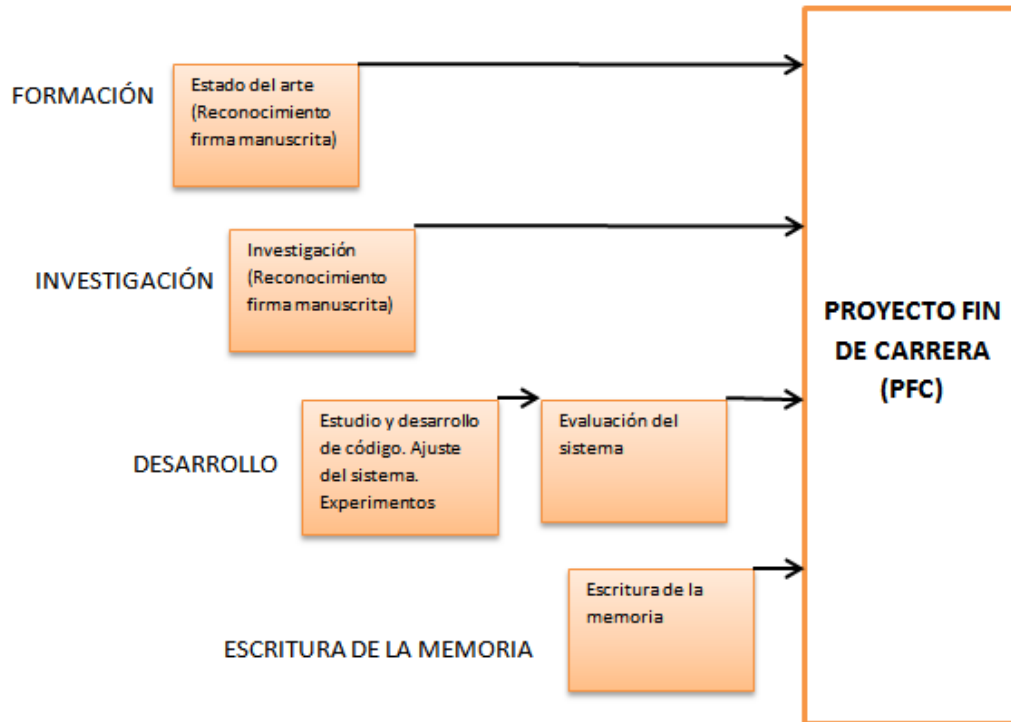


Figura 1.1: Diagrama del plan de trabajo seguido.

- **Estudio del estado del arte.** Todo inicio fundamental de un proyecto pasa por una etapa de formación en la que se obtienen los conocimientos necesarios para su desarrollo. Para este proyecto en concreto, se ha realizado en primer lugar un estudio de las características básicas del reconocimiento biométrico seguido del estado del arte en reconocimiento de firma manuscrita dinámica, utilizando libros clásicos y publicaciones del estado del arte para sistemas basados en *verificación*.
- **Estudio del software.** En la segunda fase del proyecto el alumno se ha familiarizado con los programas y herramientas necesarias para la realización del proyecto. A continuación se ha estudiado el software desarrollado por el grupo ATVS.
- **Experimentos y desarrollo de software.** Posteriormente, se ha realizado experimentos siguiendo los protocolos de las evaluaciones *BMEC* (Biosecure Multimodal Evaluation Campaign), con el objetivo de analizar diferentes técnicas y poder comparar posteriormente los resultados obtenidos con los de dicha evaluación. Además se ha analizado de qué forma afectan los distintos parámetros del sistema, para finalmente elegir aquellos que

proporcionan un mejor rendimiento en el sistema en términos de *EER*. Todo el código desarrollado se ha organizado y comentado para su uso posterior.

- **Evaluación de resultados y elaboración de la memoria.** Se ha realizado un análisis de los resultados obtenidos en las pruebas llevadas a cabo así como una comparativa entre las diferentes técnicas utilizadas. Estos análisis, junto con la revisión del estado del arte y un estudio completo del proyecto llevado a cabo, han servido para elaborar la memoria del presente proyecto fin de carrera.

1.4. Organización de la memoria.

El presente trabajo se estructura en cinco capítulos:

- **Capítulo 1: Introducción.** Este capítulo presenta la motivación para el desarrollo de este proyecto, así como, los objetivos a cumplir durante la ejecución del proyecto, la estructura de este documento y las contribuciones del mismo.
- **Capítulo 2: Estado del arte.** En este capítulo se presentan en primer lugar las propiedades y los modos de operación que existen en los sistemas biométricos en general. A continuación se realiza un estudio detallado del estado del arte en sistemas de verificación de firma manuscrita dinámica. Se explica la arquitectura de estos sistemas, los tipos de sistemas existentes, los algoritmos utilizados para la extracción de características y las bases de datos más utilizadas en los últimos años.
- **Capítulo 3: Sistemas de Verificación de firma.** En este capítulo se describen las componentes principales del sistema de verificación de firma implementado en el presente proyecto. Para ello se describe en primer lugar el sistema de características globales, para posteriormente detallar el sistema de características locales.
- **Capítulo 4: Experimentos.** En este capítulo se presentan en primer lugar las bases de datos que se utilizan para la realización de los experimentos así como el protocolo de experimentación utilizado. A continuación se presentan los resultados obtenidos a lo largo de la evaluación de los sistemas analizados. Así mismo, se detalla la secuencia de experimentos realizados para dar con la configuración de parámetros que mejor se ajusta al problema de interoperabilidad.
- **Capítulo 5: Conclusiones y trabajo futuro.** En este capítulo se presentan las conclusiones extraídas del proyecto realizado, así como las futuras líneas a seguir en este ámbito.

Al final del presente documento se añaden una serie de apéndices con información adicional para completar la información del proyecto.

2

Estado del arte.

2.1. Introducción

En este capítulo se presenta en la primera sección, una descripción de la arquitectura y modos de funcionamiento de los sistemas de reconocimiento biométrico, dedicando mayor atención a aquellos basados en firma. A continuación se detallan las distintas etapas de un sistema de verificación de firma manuscrita dinámica. Posteriormente se explican los tipos de sistemas que hay en el estado del arte actual en firma dinámica y los diferentes algoritmos utilizados para llevar a cabo la selección de las características del sistema. Finalmente se describen las bases de datos más utilizadas en los últimos años en el ámbito de firma y las diferencias entre ellas.

2.2. Sistemas de reconocimiento biométrico

El ser humano se desarrolla en una sociedad cada vez más interconectada y global, en la que el reconocimiento de los individuos representa, cada vez más, un papel fundamental. Desde el control de fronteras hasta el pago mediante dispositivos electrónicos, la identificación fiable del individuo es un requisito imprescindible. Las dos modalidades más usadas en la actualidad se basan en algo que el individuo **sabe** (e.g. una contraseña), o en algo que **tiene** (e.g. una tarjeta). Un sistema de reconocimiento biométrico se basa en el reconocimiento de patrones, rasgos biométricos extraídos a partir de rasgos intrínsecos de una persona. El reconocimiento biométrico permite que estas aplicaciones se basen en algo que el individuo **es** (e.g. su voz) o en cómo se **comporta** (e.g. su firma)[3]. Frente a los otros dos tipos de reconocimiento, presenta la ventaja de que un rasgo biométrico no puede ser olvidado, robado o perdido.

2.2.1. Modos de operación

En los sistemas de reconocimiento biométrico se pueden distinguir dos modos de operación: identificación y verificación. [3]. Previamente al funcionamiento del sistema existe una etapa de **registro**. En las figuras 2.1, 2.2 y 2.3 podemos ver un esquema específico para cada uno de ellos.

Durante el **registro**, ver Fig. 2.1, los usuarios son dados de alta en el sistema. Los rasgos biométricos del usuario son adquiridos por el sensor. Tras una etapa opcional de pre-procesado se procede a la extracción de las características identificativas del usuario. En algunos sistemas estas características conforman el patrón de referencia, en otros sistemas estas características son utilizadas para *entrenar* un modelo estocástico de la identidad a reconocer, por lo que esta etapa es también conocido como **fase de entrenamiento**.

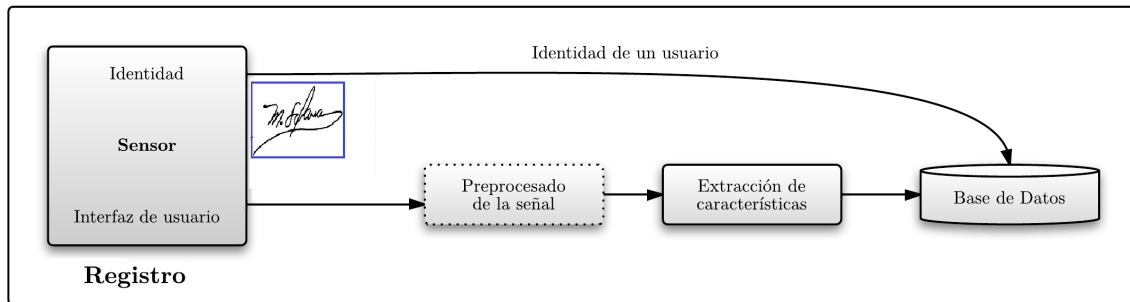


Figura 2.1: Esquema de funcionamiento de un sistema de reconocimiento biométrico en la etapa registro. Figura adaptada de [1].

Una vez los usuarios han sido registrados en la base de datos el sistema puede entrar en funcionamiento en dos modos diferentes:

En el modo de **identificación**, ver Fig. 2.2, el sistema realiza una comparación del patrón obtenido mediante el sensor con todos los patrones almacenados en la base de datos. Es, por tanto, una comparación uno-a-muchos en la que el sistema no necesita ningún tipo de identidad. El sistema tratará de encontrar la identidad del usuario a la que pertenece el rasgo extraído, en caso de que ésta se encuentre en la base de datos. Este modo exige un mayor coste computacional, aumentando de forma lineal con el número de entradas de la base de datos. La salida de este modo será la identidad del usuario al que pertenece el rasgo recibido o un mensaje indicando que dicha identidad no se encuentra en la base de datos.

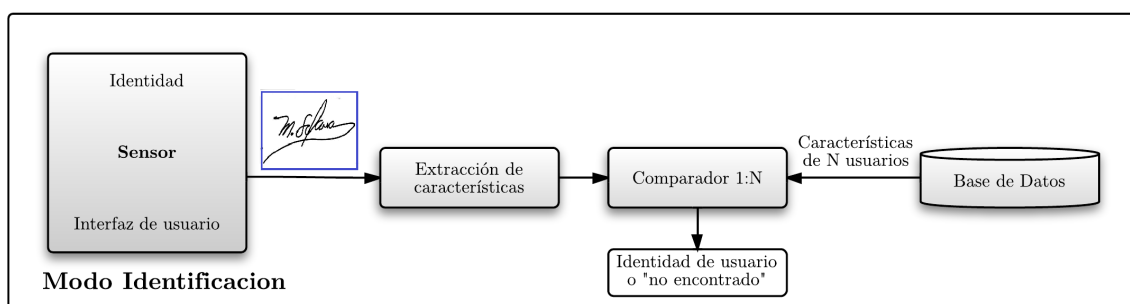


Figura 2.2: Esquema de funcionamiento de un sistema de reconocimiento biométrico en modo identificación. Figura adaptada de [1].

En el modo de **verificación**, ver Fig. 2.3, el usuario proporciona la identidad mediante una tarjeta identificativa, un número PIN o un nombre de usuario. A continuación, el sistema obtiene el rasgo biométrico del usuario y realiza una comparación uno-a-uno entre éste y el

patrón almacenado en la base de datos del usuario obteniendo una identificación positiva, en caso de que el sistema detecte que los rasgos coinciden con una similitud suficiente o negativa, en caso contrario.

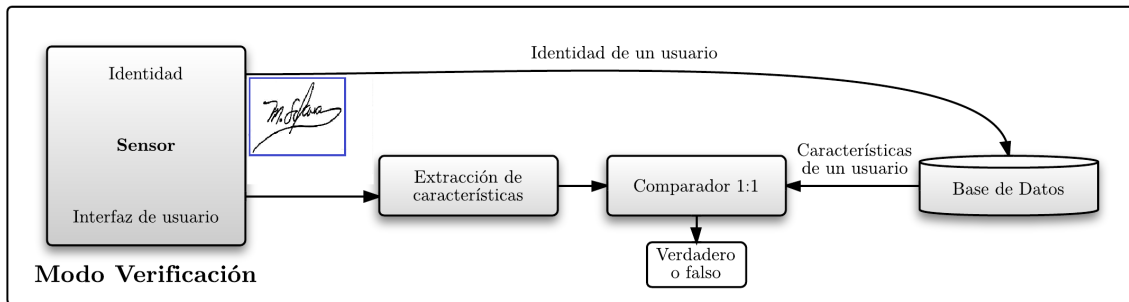


Figura 2.3: Esquema de funcionamiento de un sistema de reconocimiento biométrico en modo verificación. Figura adaptada de [1].

En los sistemas de verificación, estudiados en el presente proyecto, podemos distinguir dos tipos de errores:

- **Falsa Aceptación (FA):** es producido cuando un usuario impostor intenta hacerse pasar por otro usuario y el sistema lo detecta como el usuario auténtico, genuino.
- **Falso Rechazo (FR):** es producido cuando un usuario auténtico, genuino, es rechazado por el sistema como si fuese impostor.

Dado un conjunto de usuarios genuinos e impostores y una serie de pruebas de verificación, la Tasa de Falsa Aceptación (FAR) y la Tasa de Falso Rechazo (FRR) del sistema de verificación biométrico puede ser obtenida para cualquier umbral de decisión.

Una medida común para comparar el rendimiento de los sistemas biométricos es el *Equal Error Rate (EER)*. Esta medida indica la tasa de error del sistema cuando el umbral de decisión satisface la condición $FAR = FRR$. Debido a que la salida de los sistemas de verificación de firma es en general una decisión binaria (i.e. aceptación/rechazo), el rendimiento de los sistemas biométricos es frecuentemente representado mediante gráficas *Receiver Operating Characteristic (ROC)* o *Detection Error Trade-off (DET)*. Este tipo de gráficas permite una fácil comparación entre los sistemas para cualquier umbral de decisión. Un ejemplo de este tipo de gráficas se puede observar en la figura 2.4.

2.2.2. Características de los rasgos biométricos

Se pueden utilizar diferentes rasgos para identificar al usuario. Estos se pueden clasificar asimismo en patrones morfológicos o anatómicos (e.g. voz, huella, iris, cara) y patrones de comportamiento (e.g. firma, escritura, forma de andar). La Fig. 2.5 contiene ejemplos de rasgos biométricos. La conveniencia de un rasgo para una aplicación está determinada en base a una serie de características que todo rasgo debe cumplir en mayor o menor medida [4]:

- **Universalidad:** existencia del rasgo en todos los usuarios.

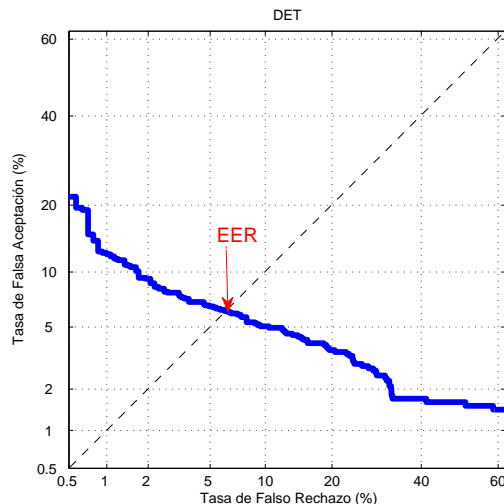


Figura 2.4: Ejemplo de una curva DET para un sistema biométrico.

- **Unicidad:** capacidad discriminativa del rasgo (personas distintas deben poseer rasgos distintos).
- **Permanencia o Estabilidad:** invariabilidad del rasgo en el tiempo.
- **Mensurabilidad o Evaluabilidad:** capacidad para caracterizar el rasgo cuantitativamente, es decir, para ser medido.

En los sistemas de reconocimiento biométrico deben cumplirse también, en mayor o menor medida, los siguientes requisitos:

- **Aceptabilidad:** grado de aceptación personal y social.
- **Rendimiento:** precisión y rapidez en la identificación.
- **Seguridad o Evitabilidad:** resistencia a ser eludido o burlado.

Desafortunadamente ningún rasgo biométrico cumple todos los atributos con éxito, presentando cada uno ventajas y desventajas. En la tabla 2.1 podemos ver el grado de cumplimiento de las características para distintos rasgos.

En función del tipo de rasgo empleado por el sistema biométrico, existen dos grandes categorías:

- **Biometría estática:** Engloba las medidas de características corporales o físicas del individuo. En este primer grupo se encuentran, por ejemplo, la huella dactilar, el ADN y el iris, entre otras.
- **Biometría dinámica:** Engloba las medidas de características conductuales del individuo. En este segundo grupo se encuentran, por ejemplo, la firma manuscrita, la forma de andar y la dinámica de tecleo, entre otras.

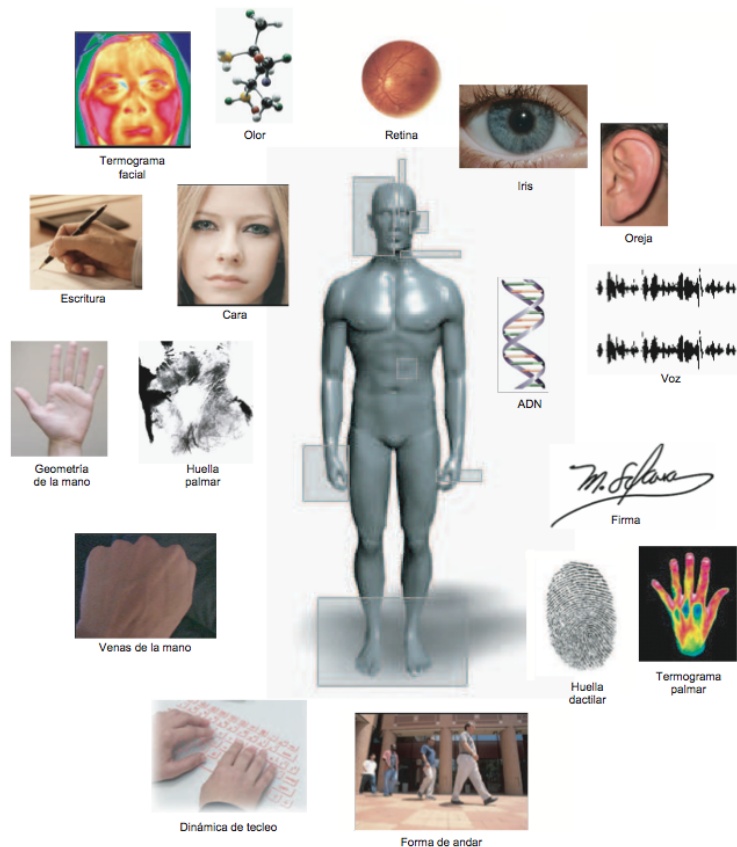


Figura 2.5: Rasgos biométricos humanos.

En la tabla 2.1 podemos ver el grado de cumplimiento de la firma como rasgo biométrico. Cabe destacar su alta **aceptabilidad**, ya que ha sido utilizada por las personas desde hace cientos de años como método para validar documentos financieros y legales. Aunque no se trate de uno de los rasgos más distintivos como puede ser el ADN o el iris, proporciona un alto grado de seguridad, debido a la gran cantidad de información discriminatoria que se puede extraer de la firma de un usuario. Por último destacar la **mensurabilidad**, ya que hoy en día gracias a la evolución tecnológica se puede recoger firmas con cualquier dispositivo táctil (e.g. PDA, tablet, smartphone) o simplemente firmando en un papel y escaneándolo posteriormente.

A pesar de las ventajas descritas anteriormente, el reconocimiento de individuos mediante sistemas de verificación de firma constituye un gran reto para la biometría debido a múltiples factores:

- **Alta variabilidad intra-clase:** un mismo individuo puede realizar diferentes versiones de su propia firma, todas ellas genuinas, generando variabilidades intra-clase que será necesario tener en cuenta a la hora de verificar la identidad del usuario.
- **Baja variabilidad inter-clase:** los sistemas de verificación de firma deben tener en cuenta posibles falsificaciones de firmas, las cuales pueden ser muy similares a las firmas genuinas.
- **Baja permanencia:** la firma de un individuo tiende a variar con el paso del tiempo.

Existen dos tipos de sistemas de verificación de firma dependiendo de la información extraída de la firma:

Rasgo biométrico	Universalidad	Unicidad	Permanencia	Mensurabilidad	Rendimiento	Aceptabilidad	Evitabilidad
ADN	A	A	A	B	A	B	B
Oreja	M	M	A	M	M	A	M
Cara	A	B	M	A	B	A	A
Termograma facial	A	A	B	A	M	A	B
Venas de la mano	M	M	M	M	M	M	B
Huella dactilar	M	A	A	M	A	M	M
Forma de andar	M	B	B	A	B	A	M
Geometría de la mano	M	M	M	A	M	M	M
Iris	A	A	A	M	A	B	B
Huella palmar	M	A	A	M	A	M	M
Olor	A	A	A	B	B	M	B
Retina	A	A	M	B	A	B	B
Firma	B	B	B	A	B	A	A
Forma de teclear	B	B	B	M	B	M	M
Voz	M	B	B	M	B	A	A
Escritura	B	B	B	A	B	A	A

Tabla 2.1: Comparación cualitativa de las características de los distintos rasgos biométricos (A=Alto, M=Medio, B=Bajo). Fuente: [3].

- **Sistemas de verificación de firma Off-line:** en este tipo de sistemas se extraen las características a partir de imágenes de firmas estáticas.
- **Sistemas de verificación de firma On-line:** en este tipo de sistemas se capturan las firmas utilizando dispositivos electrónicos (i.e. pen tablet, PDA, smartphone). Estos dispositivos permiten obtener durante toda la firma la evolución en el tiempo de algunos parámetros como puede ser la presión, la posición X e Y , inclinación del bolígrafo, etc. Tradicionalmente este tipo de sistemas han proporcionado unos resultados mejores que los sistemas Off-line, debido a la mayor cantidad de información disponible. Estos resultados se pueden observar en algunas evaluaciones recientes, como la realizada en el *ICDAR 2009* (International Conference on Documents Analysis and Recognition) [8]. Por este motivo, en el presente proyecto se estudiará en detalle un sistema de verificación de firma manuscrita On-line.

2.3. Sistemas de verificación de firma manuscrita dinámica

Dado que el sistema implementado en este Proyecto Final de Carrera es un sistema de verificación de firma manuscrita dinámica, a continuación se procede a explicar en detalle las características que presentan este tipo de sistemas.

2.3.1. Arquitectura

Los sistemas de verificación de firma manuscrita dinámica comparten una arquitectura común. La típica arquitectura que presenta un sistema automático de verificación de firma se representa en Fig.2.6. En general está compuesto de las siguientes etapas:

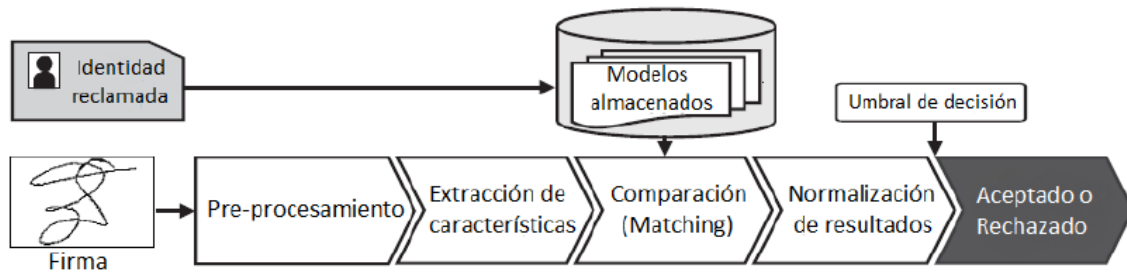


Figura 2.6: *Arquitectura típica de un sistema de verificación de firma.*

- **1. Adquisición de datos:** las señales de una firma son capturadas utilizando dispositivos como tabletas digitales (i.e. *WACOM*) o dispositivos táctiles (i.e. PDAs, smartphones, etc). Dependiendo del dispositivo de captura utilizado, la información almacenada será mayor. Las tabletas digitales proporcionan información de presión, ángulo de inclinación del bolígrafo durante el proceso de firmado y la trayectoria del bolígrafo durante un pen-up (información muy relevante como se puede ver en los recientes estudios realizados [9] [10]), mientras que esta información no se encuentra disponible en dispositivos de uso más común (PDA, smartphone). Las señales son muestreadas en el tiempo y posteriormente almacenadas en forma de series discretas. La frecuencia de muestreo utilizada por los dispositivos de captura suele ser entre 100-200 Hz. Esta frecuencia de muestreo cumple con el criterio de Nyquist, ya que la mayor frecuencia observada a la hora de realizar una firma suele ser de entre 20-30 Hz [11].

Tras la adquisición de datos suele ser común encontrar una etapa de de pre-procesamiento. El objetivo de esta etapa es realizar un filtrado del ruido, aplicar técnicas de diezmado para eliminar posibles muestras repetidas por el dispositivo de captura o interpolación para solucionar el problema de muestras perdidas durante la captura de la firma (e.g. PDA). Esta etapa será muy importante en la realización de este proyecto, con el objetivo de conseguir que una firma de un mismo usuario en los distintos dispositivos de captura se parezca lo máximo posible. Esto proporcionará buenos resultados al aplicar interoperabilidad de sistemas.

- **2. Extracción de características:** en este proceso se obtiene la información discriminativa de un usuario a partir de los datos de la firma On-line.

Se distinguen dos tipos de aproximaciones:

- **Sistemas basados en características:** basados en la extracción de características globales de la firma (e.g. duración de la firma, número de pens-ups, velocidad promedio) con el objetivo de obtener un vector de características discriminatorio de cada usuario.
 - **Sistemas basados en funciones:** basados en la comparación de secuencias en el tiempo de propiedades de la firma (e.g. presión, trayectoria). Generalmente éste tipo de sistemas proporcionan unos resultados mejores que los sistemas basados en características.
- **3. Registro:** en función de la estrategia de comparación (matching) a utilizar, se puede distinguir dos tipos de registro:

- **Basado en modelo:** se obtiene un modelo estadístico particular de cada usuario a partir de un conjunto de firmas genuinas de entrenamiento. Este modelo se utilizará para futuras comparaciones en la etapa de matching. Cada modelo estadístico necesita un mínimo de 4-6 firmas de entrenamiento para obtener unos rendimientos aceptables.
 - **Basado en referencia:** almacena las características de cada una de las firmas de entrenamiento como plantillas. En el proceso de matching se compara la firma entrante de un usuario con cada una de las plantillas almacenadas en el sistema para este usuario. Posteriormente se combinan los resultados mediante técnicas de fusión.
- **4. Cálculo de similitud (pre-alineamiento y matching):** en esta etapa suele ser común realizar en primer lugar un pre-alineamiento de las muestras de la firma de entrada y las muestras almacenadas en el modelo correspondiente, para mejorar el rendimiento del sistema. A continuación se realiza el proceso de comparación (matching). En sistemas basados en características, se suelen utilizar técnicas basadas en la medida de distancias (e.g. distancia de Mahalanobis, distancia Euclidea). En sistemas basados en funciones se utilizan otro tipo de técnicas como *HMM* (Hidden Markov Models) o *DTW* (Dynamic Time Warping) para comparar entre modelos de firmas.
- **5. Normalización de Scores:** las puntuaciones obtenidas tras realizar el matching son normalizadas en un rango común, antes de verificar si se trata de una firma genuina o impostora. Este proceso es muy importante cuando se utilizan técnicas de fusión de sistemas. Algunas de las técnicas de normalización más utilizadas en sistemas biométricos se recogen en [12].

2.3.2. Sistemas globales o basados en características globales

En este tipo de sistemas se obtiene un vector de características a partir de una firma en su conjunto, como puede ser la duración, el número de pen-ups, la velocidad promedio de la firma, etc. A pesar de la gran cantidad de características globales propuestas [13], a la hora de implementar un sistema el número de características utilizado es menor, debido a la pequeña cantidad de datos de entrenamiento disponibles. Por esta razón es muy importante utilizar técnicas de selección de características (ver Subsec. 2.3.4), siendo el algoritmo *SFFS* uno de los que proporcionan mejores resultados, a costa de un mayor coste computacional.

En la fase de comparación (matching), es frecuente utilizar clasificadores estadísticos como Gaussian Mixture Models [14], Parzen Windows [14], distancia de Mahalanobis [15], etc.

2.3.3. Sistemas locales o basados en funciones temporales

En este tipo de sistemas las técnicas más utilizadas son *HMM* y *DTW*. Las funciones capturadas en el tiempo (e.g. presión, coordenadas, etc) son utilizadas para modelar la firma de cada usuario.

La fusión de los sistemas basados en características y basados en funciones han demostrado proporcionar un rendimiento mejor que considerando cada uno de los sistemas por separado. [13].

2.3.3.1. *Dynamic Time Warping*

Dynamic Time Warping (DTW) es un algoritmo que consigue comparar el parecido entre dos secuencias temporales que pueden ser de distinto tamaño. El objetivo de DTW es calcular el camino óptimo entre dos secuencias de muestras X e Y que minimice una medida de distancia. El algoritmo puede ser definido como sigue en [16]. En primer lugar vamos a definir dos secuencias temporales

$$X = x_1, x_2, \dots, x_i, \dots, x_I \quad Y = y_1, y_2, \dots, y_j, \dots, y_J \quad (2.1)$$

y una medida de distancia

$$d(i, j) = \| x_i - y_j \| \quad (2.2)$$

entre dos muestras de secuencias. Un camino de alineamiento puede ser definido como

$$C = c_1, c_2, \dots, c_k, \dots, c_K \quad (2.3)$$

donde cada c_k representa una correspondencia (i, j) entre muestras de las secuencias X e Y . La condición inicial del algoritmo es

$$g_1 = g(1, 1) = d(1, 1) \cdot w(1) \quad (2.4)$$

donde g_k representa la distancia acumulada después de k pasos y $w(k)$ es un factor de ponderación que debe ser definido. Para cada iteración, g_k es calculado como

$$g_k = g(i, j) = \min_{c_{k-1}} [g_{k-1} + d(c_k) \cdot w(k)] \quad (2.5)$$

hasta alcanzar la muestra final I y J de ambas secuencias. La distancia acumulada final es normalizada

$$D(X, Y) = \frac{g_k}{\sum_{k=1}^K w(k)} \quad (2.6)$$

donde $\sum w(k)$ compensa los efectos de la longitud de la secuencia. El factor de ponderación w_k se define con el objetivo de restringir la correspondencia entre muestras de ambas secuencias. En la Fig. 2.7.a, se representa una posible definición de w_k . En este caso concreto, solo tres transiciones están permitidas en el cálculo de g_k . Consecuentemente con la definición de Ecu. 2.5 se obtiene

$$g_k = g(i, j) = \min \left(\begin{array}{c} g(i, j-1) + d(i, j) \\ g(i-1, j-1) + 2d(i, j) \\ g(i-1, j) + d(i, j) \end{array} \right) \quad (2.7)$$

que es una de las más comunes implementaciones encontradas en la literatura. En la Fig. 2.7.b se muestra un ejemplo de la correspondencia punto a punto entre dos muestras genuinas, observando los resultados del alineamiento temporal. El algoritmo ha sido mejorado para verificación de firma por algunos autores [17]. Esta mejora en concreto consiguió ganar el SVC (Signature Verification Competition) 2004 [18].

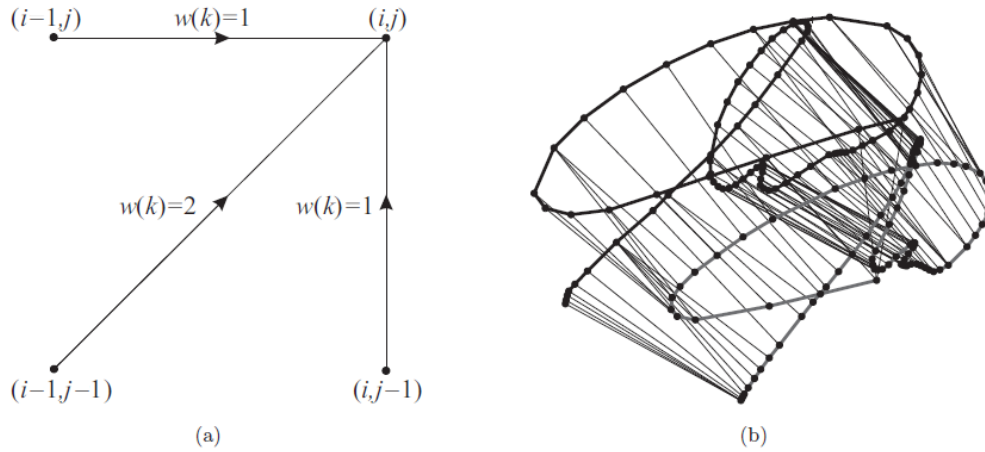


Figura 2.7: (a) Ejemplo de un factor de ponderación $w(k)$ simétrico para DTW. (b) Ejemplo de la correspondencia punto a punto usando DTW entre dos secuencias de firmas genuinas.[2]

2.3.3.2. Hidden Markov Models

Hidden Markov Models (*HMM*) es una técnica muy utilizada en biometría, especialmente en reconocimiento de voz. En el ámbito de verificación de firma manuscrita dinámica también se han utilizado diferentes aproximaciones de este algoritmo [19] [20]. Un HMM representa un proceso doblemente estocástico, en el que se asume que el sistema que se quiere modelar es un proceso de Markov de parámetros desconocidos. El objetivo es determinar esos parámetros desconocidos u ocultos a partir de las observaciones. Las observaciones son modeladas mediante GMMs en la mayor parte de aplicaciones de reconocimiento de voz y escritura. Los GMMs, que puede ser considerados como un HMM de un solo estado, han mostrado un alto rendimiento en verificación de firma [21].

La estructura básica de un HMM usando GMMs para modelar las observaciones se define mediante los siguientes elementos:

- Número de estados ocultos: N .
- Número de Mezclas de Gaussianas por estado: M .
- Matriz de probabilidad de transición $A = \{ a_{ij} \}$, que contiene la probabilidad de saltar de un estado a otro o de permanecer en el mismo estado.

La Fig. 2.8 representa un ejemplo de configuración de un HMM. Encontrar una estructura robusta y que proporcione buen rendimiento en verificación de firma dinámica es una tarea complicada. La elección de un HMM simple puede no modelar correctamente las firmas de los usuarios, pudiendo ser incapaz de modelar realizaciones complejas de firmas. Por otro lado, como un modelo simple tiene menos parámetros que estimar, su estimación será más robusta que para los modelos complejos. Por lo tanto el número de estados y el número de mezclas de gaussianas por estado son los parámetros a evaluar para obtener un sistema óptimo [19].

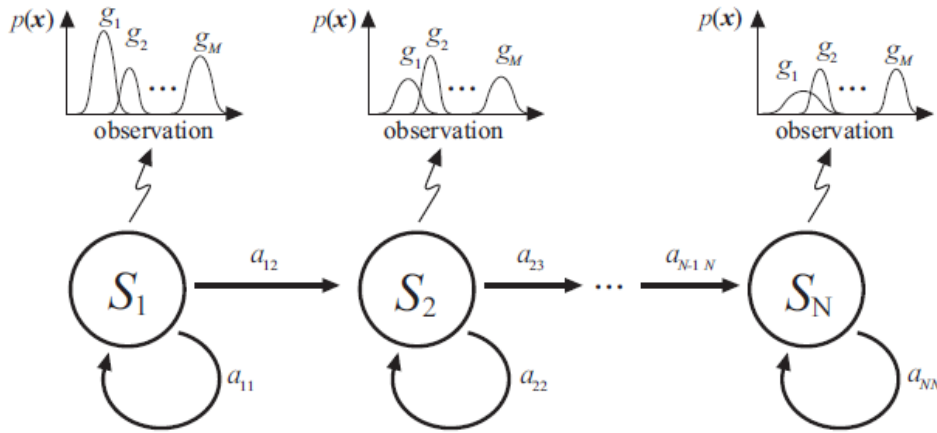


Figura 2.8: Estructura de un modelo HMM de izquierda a derecha de N estados, con M componentes GMMs y sin saltos entre estados. Ref.[2]

2.3.4. Algoritmos de selección de características

Debido al *curse of dimensionality* [22], el rendimiento de un sistema se degrada cuando los datos de entrenamiento son demasiado pequeños comparados con el número de dimensiones del vector de características. Esto es lo que ocurre frecuentemente en el caso de verificación de firma, donde el número de muestras por firma es de unos pocos cientos de muestras y el número de firmas disponible por usuario es relativamente pequeño (de 3 a 5 firmas).

La utilización de técnicas de selección de características pretende disminuir la dimensionalidad del vector de características con el objetivo de optimizar el rendimiento del sistema. Para ello, estos algoritmos obtienen el conjunto de características que optimizan el sistema para un criterio dado (como por ejemplo el *EER*). Lo ideal sería, dado un vector compuesto por F características, comprobar todas las posibles combinaciones desde 1 hasta F características con el objetivo de obtener la combinación óptima. Sin embargo esto no es posible debido al gran coste computacional.

En función del criterio de optimización utilizado se puede distinguir:

- **Filter method:** el vector de características óptimo es seleccionado de acuerdo a propiedades intrínsecas de los datos de entrenamiento, como las propiedades estadísticas. Posteriormente, los resultados de la clasificación de los problemas bajo consideración son usados como criterio de optimización.
- **Wrapper method:** el criterio de optimización utilizado para seleccionar el vector de características óptimo es el *EER*. Este tipo de métodos requiere en general un mayor coste computacional, ya que la evaluación del criterio de optimización suele ser más compleja que la computación de las propiedades estadísticas de los datos de entrenamiento.

Muchas técnicas de selección de características han sido propuestas en la literatura con el objetivo de reducir el número de combinaciones de características a testear [13] [23] [24]. Sin embargo todas ellas encuentran soluciones subóptimas al problema. Una excepción sería el algoritmo

Branch and Bound [25], pero que solo es aplicable cuando el criterio a optimizar incrementa de manera monótona con el tamaño del subconjunto de características. A continuación exponemos el conjunto de algoritmos más popular para la selección de las características.

2.3.4.1. *Scalar Feature Selection*

Las características son consideradas individualmente en este procedimiento. Cada una de las características recibe una puntuación en función de su separabilidad usando un criterio predefinido C , como puede ser el EER o una medida de distancia. Posteriormente se selecciona el conjunto de N características con mayor puntuación en términos de C como el vector de características de N dimensión óptimo. Este método tiene la ventaja de tener un coste computacional bajo. Sin embargo no considera la posible correlación entre características.

2.3.4.2. *Sequential Forward/Backward Selection*

En el método *Sequential Forward Selection*, dado un conjunto de F características, el primer paso es seleccionar aquella característica más discriminatoria x_i . Posteriormente se prueban todas las combinaciones posibles entre esta característica x_i y el resto de características disponibles, seleccionando la mejor combinación $\{x_i, x_f\}$. Este algoritmo se repite de manera iterativa añadiendo características hasta alcanzar el tamaño del vector de características deseado. El algoritmo *Sequential Backward Selection* es similar al explicado anteriormente pero en lugar de empezar con una sola característica empieza con todo el conjunto de características F y va eliminando una característica de manera iterativa, hasta alcanzar el tamaño del vector deseado.

2.3.4.3. *Floating Search*

Este algoritmo pretende corregir algunas de las limitaciones de los anteriores. En los anteriores casos, cuando una característica era seleccionada (o descartada en el caso *Backward*), ya no podía ser descartada (o seleccionada en el caso *Backward*). Esto es conocido como los efectos de anidación. Como ocurre en *Sequential Selection*, existen las aproximaciones *forward* y *backward*. Nosotros nos centramos en el método *forward*, referido como ***Sequential Forward Floating Search (SFFS)***. Este algoritmo puede ser implementado como sigue en [22]

Vamos a considerar un conjunto de F características, de donde pretendemos encontrar el subconjunto de N características que optimizan el criterio C . Consideramos el vector de características $X_n = \{x_1, x_2, \dots, x_n\}$ como el mejor vector de n características y Y_{F-n} el set de las restantes $F - n$ características. En este algoritmo se almacena además los mejores vectores de características de menor dimensión X_1, X_2, \dots, X_{n-1} . Los siguientes pasos son realizados hasta obtener un set estable X_n .

- 1. *Inclusión.*

Elegir el elemento x_{n+1} de Y_{F-n} que añadido al vector X_n produce el mejor valor del criterio de optimización C . Pasamos por lo tanto a tener un nuevo vector, $X_{n+1} = \{X_n, x_{n+1}\}$

- 2. *Test.*

- (a) Encontrar la característica x_r que tiene el menor efecto negativo (o más positivo) en el criterio de optimización C cuando ésta es eliminada del vector X_{n+1} .
- (b) Si $r = n + 1$, cambiar n por $n + 1$ e ir al paso 1.
- (c) Si $r \neq n + 1$ y $C(X_{n+1} - \{x_r\}) < C(X_n)$ ir al paso 1, esto es, si eliminando cualquier característica no mejora el criterio C en el subconjunto X_n previo, no se realiza la búsqueda *backward*.

■ *3. Exclusión.*

- (a) Eliminar x_r para conseguir el vector $X'_n = X_{n+1} - \{x_r\}$.
- (b) Encontrar la característica x_s que tiene el menor efecto negativo en el criterio C cuando ésta es eliminada de X'_n .
- (c) Si $C(X'_n - \{x_s\}) < C(X_{n-1})$, entonces $X_n = X'_n$ y se vuelve al paso 1, esto es, si eliminando otra característica no mejora el criterio de optimización C en el subconjunto X_n seleccionado previamente, no se realiza la búsqueda *backward*.
- (d) Eliminar x_s , obteniendo un nuevo subconjunto $X'_{n-1} = X'_n - \{x_s\}$ y $n = n - 1$.
- (e) Ir al paso 3.b.

Cabe destacar que algunas condiciones del primer paso no han sido especificadas para simplificar la descripción del algoritmo. El algoritmo *backward* es equivalente al explicado pero eliminando características en lugar de añadiendo. El algoritmo *SFFS* ha sido comprobado como un algoritmo altamente eficiente, obteniendo unos resultados cercanos al vector de características óptimo obtenido con el algoritmo *Branch and Bound*.

Otros algoritmos para la selección de características son redes neuronales y algoritmos genéticos [24], aunque produce diferentes resultados subóptimos en cada ejecución.

2.3.5. Bases de datos de firma manuscrita dinámica

La disponibilidad de bases de datos públicas permite la comparación de los algoritmos implementados. Hasta hace unos años, uno de los mayores problemas era la carencia de bases de datos públicas, debido en gran medida a los problemas legales y a la privacidad de los usuarios.

En la actualidad se dispone de un conjunto de bases de datos de firma manuscrita dinámica, gracias en gran medida al esfuerzo realizado por las instituciones de investigación. Algunas de las más conocidas son MCYT (2003), BIOMET (2003), SVC (2004), MyIDEA (2005), BiosecureID (2007) o Biosecure (2008). Las principales características de estas bases de datos quedan esquematizadas en la tabla 2.2.

No hay que olvidar a la hora de trabajar con bases de datos de firmas la variación existente entre las firmas de diferentes culturas. Las firmas en Asia están formadas generalmente por caracteres asiáticos, que contienen un mayor número de trazos cortos comparadas con las firmas de Europa por ejemplo.

A continuación explicamos en detalle las características de cada una de ellas.

- **MCYT**: la adquisición fue llevada a cabo por diversas instituciones universitarias españolas, entre las que se encuentra el Grupo de Reconocimiento Biométrico ATVS, de la Universidad Autónoma de Madrid. Esta base de datos cuenta con un total de 330 usuarios.

	Año	Usuarios	Sesiones
BIOMET	2003	84	2
Biosecure	2008	971 (DS1, Internet)	2
		667 (DS2, Escritorio)	2
		713 (DS3, Móvil)	2
BiosecureID	2007	400	4
MyIDEA	2005	104 (aprox.)	3
MCYT	2003	330	1
SVC	2004	40	2

Tabla 2.2: Bases de datos de firma manuscrita dinámica.

Las firmas fueron capturadas usando una WACOM Intuos A6 tablet con una frecuencia de muestreo de 100 Hz, permitiendo capturar las coordenadas, la presión y los ángulos del bolígrafo (azimuth y altitud). Hay 25 firmas genuinas y 25 firmas falsificadas por usuario. Firmas fueron capturadas en grupos de 5. Primero 5 firmas genuinas, luego 5 firmas falsificadas de otro usuario, repitiendo este procedimiento hasta alcanzar las 25 firmas de cada tipo. Cada usuario proporciona 5 firmas falsificadas para los 5 usuarios previos en la base de datos.

- **BIOMET**: las firmas fueron capturadas usando una WACOM Intuos2 A6 Pen-tablet y un bolígrafo de tinta con una frecuencia de muestreo de 100 Hz, permitiendo capturar las coordenadas de posición, la presión y los ángulos del bolígrafo (azimuth y altitud). Hay un total de 84 usuarios, con 15 firmas genuinas y 12 falsificaciones por usuario. Las firmas fueron capturadas en 2 sesiones con un espacio de tiempo entre ellas de 5 meses. El género y la edad de los individuos presenta una distribución balanceada en todas las sesiones, asegurando resultados realistas.
- **SVC**: las firmas fueron capturadas usando dos dispositivos de captura, una tableta digital *WACOM* y un *Grip Pen*. Por temas de privacidad los usuarios realizaron firmas inventadas como si fuesen sus firmas genuinas. Se tuvieron en cuenta dos escenarios. El primero de ellos solo considera información de coordenadas. El segundo incluye información de presión e inclinación del bolígrafo. Cada escenario contiene 40 usuarios con 20 firmas genuinas y 20 firmas falsificadas, obtenidas en 2 sesiones. La peculiaridad de esta base de datos es que contiene firmas de usuarios occidentales y asiáticos.
- **MyIDEA**: las firmas fueron capturadas usando una WACOM Intuos2 A4 con una frecuencia de muestreo de 100 Hz. Cuenta con un total de 70 usuarios y 54 firmas por usuario, recogidas en 3 sesiones. El número de firmas genuinas por usuario es de 18, recogiendo 6 firmas por sesión. A su vez el usuario realizó firmas falsificadas de los otros usuarios en 2 escenarios. En el primer escenario el usuario solo contaba con una imagen de la firma a falsificar, mientras que en el segundo escenario el usuario tenía acceso también a la información dinámica de la firma. Al igual que con las firmas genuinas, cada usuario realizaba 6 falsificaciones en cada escenario por sesión, dando como resultado 36 firmas falsificadas entre los dos escenarios.
- **BiosecureID**: esta base de datos surge como consecuencia del éxito de la base de datos MCYT. Se trata de un proyecto financiado por el Ministerio de Ciencia y Tecnología en el cual han participado seis instituciones académicas españolas entre las que se encuentra el Grupo de Reconocimiento Biométrico ATVS de la UAM.

El objetivo es extender la base de datos BIOSEC ya existente, en términos de incluir nuevas sesiones para usuarios ya registrados, así como incluir nuevos usuarios. El número de usuarios final aumenta a 400 y consta de 4 sesiones distribuidas entre sí por un margen temporal de un mes. Una característica de esta base de datos es la distribución balanceada en la edad de los usuarios que participaron, contando con usuarios entre 18 y más de 45 años. Las firmas fueron capturadas con una WACOM Intuos3 A4. En cada una de las 4 sesiones, cada usuario realiza 4 firmas genuinas y 1 firma falsificada para cada uno de los 3 usuarios anteriores. Se consideran 4 escenarios de falsificación.

- **Biosecure:** este proyecto está impulsado por la necesidad de coordinar los múltiples esfuerzos en el campo de la investigación biométrica a lo largo de toda Europa; más de 30 instituciones de investigación procedentes de 15 países diferentes han participado en el proyecto. El Grupo de Reconocimiento Biométrico ATVS también participó en la elaboración de dicha base de datos. Las firmas fueron recogidas por dos dispositivos distintos, originando las siguientes modalidades:
 - **Biosecure Signature DS2 - Access Control Scenario:** esta base de datos fue capturada utilizando una WACOM Intuos3 A6 digitalizada a una frecuencia de muestreo de 100 Hz, con un procedimiento similar al seguido en la base de datos MCYT. El dispositivo captura información de coordenadas de posición, presión y ángulos de inclinación del bolígrafo (*azimuth* y *altitude*). Cuenta con un total de 667 usuarios, de 7 países diferentes. Por cada uno de los usuarios se posee un total de 30 firmas genuinas y 20 falsificadas, capturadas en 2 sesiones con un espacio temporal de 2 meses aproximadamente. Las firmas fueron capturadas en bloques de 5. En cada sesión los usuarios realizaron 3 sets de 5 firmas genuinas y 5 firmas falsificadas entre cada set. Cada usuario realizó 5 falsificaciones para los 4 usuarios anteriores de la base de datos. El usuario tenía acceso visual a la información dinámica de la firma a falsificar. Un ejemplo de la captura de una firma con este dispositivo se muestra en la Fig. 2.9.(b).

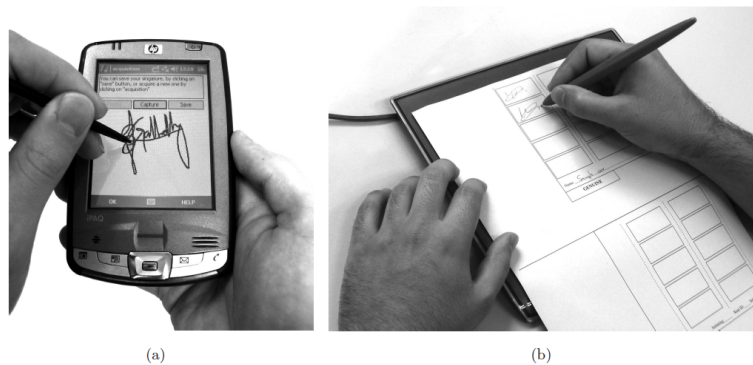


Figura 2.9: (a) Proceso de captura utilizando una PDA en BioSecure DS3 - Mobile Scenario dataset. (b) Proceso de captura utilizando el pen-tablet en BioSecure DS2 - Access Control Scenario dataset.

- **Biosecure Signature DS3 - Mobile Scenario:** esta base de datos fue capturada bajo el mismo procedimiento que *DS2-Access Control Scenario* pero en un escenario móvil. Fue adquirida en 8 emplazamientos diferentes de Europa. El dispositivo de captura es una PDA HP iPAQ hx2790 con una frecuencia de muestreo de 100 Hz. El dispositivo captura información de coordenadas de posición y tiempo entre muestras.

Los usuarios realizaron las firmas de pie mientras sujetaban con una mano la PDA y firmaban con la otra. Esto emula unas condiciones reales de operación. Un ejemplo del protocolo de captura se puede observar en la Fig. 2.9(a). El protocolo de adquisición fue el mismo que el realizado en DS2. El número de usuarios aumenta a 713. Las firmas capturadas con la PDA necesitan de un preprocesado para corregir el efecto de pérdidas de muestras durante la adquisición.

En la Fig. 2.10 se representan algunos ejemplos de firmas genuinas y falsificadas capturadas en los escenarios DS2 y DS3.

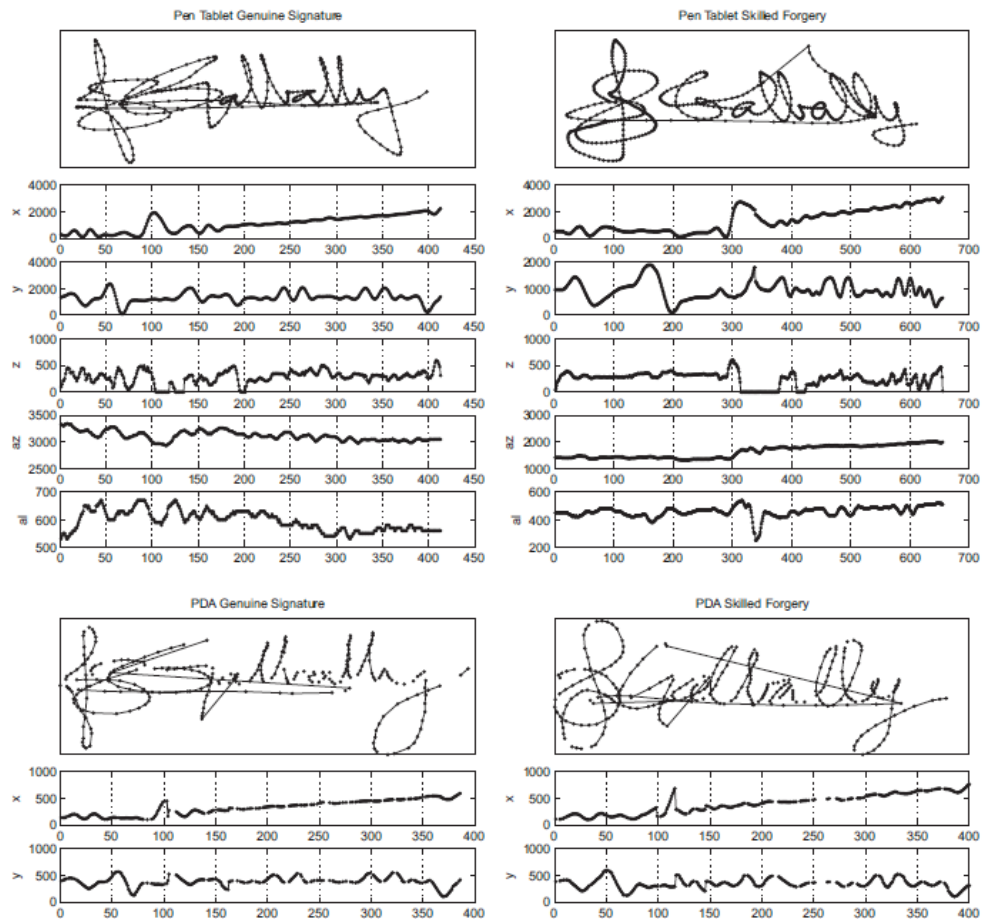


Figura 2.10: Ejemplos de firmas y sus correspondientes señales disponibles para BioSecure Multimodal DataBase DS2 y DS3, capturadas usando un pen tablet (superior) y una PDA (inferior), respectivamente. Ref. [2]

3

Sistema de verificación de firma dinámica. Implementación.

El presente capítulo describe en detalle el sistema automático de verificación de firma dinámica implementado en el presente proyecto. Se ha utilizado un **sistema basado en características globales** (referido como sistema global a partir de ahora) así como un **sistema basado en funciones temporales** (referido como sistema local a partir de ahora). El sistema local implementado está basado en el trabajo presentado en [26], junto con algunas características extraídas de trabajos más recientes [9] [2]. El sistema global implementado está basado en el set de características descrito en [2].

3.1. Sistema global de verificación de firma

En el sistema global implementado en este proyecto se ha considerado un **set de 100 características globales** obtenido de [2]. Este vector de características es extraído para cada firma. Una descripción completa de las 100 características se representa en la tabla 3.1. El set de 100 características puede ser dividido en 4 categorías, dependiendo de la magnitud a medir por la característica (la nomenclatura de las características coincide con la usada en [13]).

- **1. Tiempo** (25 características): relacionado con la duración de la firma, tiempo de eventos como pen-ups o de máximos locales: 1, 13, 22, 32, 38, 40-42, 50, 52, 58-60, 62, 64, 68, 79, 81-82, 87-90, 94, 100.
- **2. Velocidad y aceleración** (25 características): referidas a la primera y a la segunda derivada en el tiempo de las funciones temporales de posición, como la velocidad media o la velocidad máxima: 4-6, 9-11, 14, 23, 26, 29, 31, 33, 39, 44-45, 48, 69, 74, 76, 80, 83, 85, 91-92, 96.
- **3. Dirección** (18 características): extraídas de la trayectoria de la firma, como la dirección al comienzo de la firma, la dirección media entre pen-ups: 34, 51, 56-57, 61, 63, 66, 71-73, 77-78, 84, 93, 95, 97-99.

- 4. Geometría (32 características): asociadas a los trazos o la relación de aspecto de la firma.

#	Tiempo	#	Dirección
#	Velocidad y aceleración	#	Geometría

Ranking	Feature Description	Ranking	Feature Description
1	signature total duration T_s	2	N(pen-ups)
3	N(sign changes of dx/dt and dy/dt)	4	average jerk \bar{j}
5	standard deviation of a_y	6	standard deviation of v_y
7	(standard deviation of \bar{y})/ Δ_y	8	N(local maxima in x)
9	standard deviation of a_x	10	standard deviation of v_x
11	J_{rms}	12	N(local maxima in y)
13	$t(2nd\ pen-down)/T_s$	14	(average velocity \bar{v})/ $v_{x,max}$
15	$\frac{A_{min}=(y_{max}-y_{min})(x_{max}-x_{min})}{(\Delta_x=\sum_{i=1}^{pen-downs}(x_{max i}-x_{min i}))\Delta_y}$	16	$(x_{last\ pen-up} - x_{max})/\Delta_x$
17	$(x_{1st\ pen-down} - x_{min})/\Delta_x$	18	$(y_{last\ pen-up} - y_{min})/\Delta_y$
19	$(y_{1st\ pen-down} - y_{min})/y$	20	$(T_w \bar{v})/(y_{max} - y_{min})$
21	$(T_w \bar{v})/(x_{max} - x_{min})$	22	(pen-down duration T_w)/ T_s
23	$\bar{v}/v_{y,max}$	24	$(y_{last\ pen-up} - y_{max})/\Delta_y$
25	$\frac{T((dy/dt)/(dx/dt)>0)}{T((dy/dt)/(dx/dt)<0)}$	26	\bar{v}/v_{max}
27	$(y_{1st\ pen-down} - y_{max})/\Delta_y$	28	$(x_{last\ pen-up} - x_{min})/\Delta_x$
29	(velocity rms v)/ v_{max}	30	$\frac{(x_{max}-x_{min})\Delta_x}{(y_{max}-y_{min})\Delta_x}$
31	(velocity correlation $v_{x,y}$)/ v_{max}^2	32	$T(v_y > 0 pen-up)/T_w$
33	$N(v_x = 0)$	34	direction histogram s_1
35	$(y_{2nd\ local\ max} - y_{1st\ pen-down})/\Delta_y$	36	$(x_{max} - x_{min})/x_{acquisition\ range}$
37	$(x_{1st\ pen-down} - x_{max})/\Delta_x$	38	$T(curvature > Threshold_{curv})/T_w$
39	(integrated abs. centr. acc. a_{Ic})/ a_{max}	40	$T(v_x > 0)/T_w$
41	$T(v_x < 0 pen-up)/T_w$	42	$T(v_x > 0 pen-up)/T_w$
43	$(x_{3rd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	44	$N(v_y = 0)$
45	(acceleration rms a)/ a_{max}	46	(standard deviation of x)/ Δ_x
47	$\frac{T((dx/dt)/(dy/dt)>0)}{T((dx/dt)/(dy/dt)<0)}$	48	(tangential acceleration rms a_t)/ a_{max}
49	$(x_{2nd\ local\ max} - x_{1st\ pen-down})/\Delta_x$	50	$T(v_y < 0 pen-up)/T_w$
51	direction histogram s_2	52	$t(3rd\ pen-down)/T_s$
53	(max distance between points)/ A_{min}	54	$(y_{3rd\ local\ max} - y_{1st\ pen-down})/\Delta_y$
55	$(\bar{x}-x_{min})/\bar{x}$	56	direction histogram s_5
57	direction histogram s_3	58	$T(v_x < 0)/T_w$
59	$T(v_y > 0)/T_w$	60	$T(v_y < 0)/T_w$
61	direction histogram s_8	62	$(1st\ t(v_{x,min}))/T_w$
63	direction histogram s_6	64	$T(1st\ pen-up)/T_w$
65	spatial histogram t_4	66	direction histogram s_4
67	$(y_{max} - y_{min})/y_{acquisition\ range}$	68	$(1st\ t(v_{x,max}))/T_w$
69	(centripetal acceleration rms a_c)/ a_{max}	70	spatial histogram t_1
71	$\theta(1st\ to\ 2nd\ pen-down)$	72	$\theta(1st\ pen-down\ to\ 2nd\ pen-up)$
73	direction histogram s_7	74	$t(j_{x,max})/T_w$
75	spatial histogram t_2	76	$j_{x,max}$
77	$\theta(1st\ pen-down\ to\ last\ pen-up)$	78	$\theta(1st\ pen-down\ to\ 1st\ pen-up)$
79	$(1st\ t(x_{max}))/T_w$	80	\bar{j}_x
81	$T(2nd\ pen-up)/T_w$	82	$(1st\ t(v_{max}))/T_w$
83	$\bar{j}_{y,max}$	84	$\theta(2nd\ pen-down\ to\ 2nd\ pen-up)$
85	\bar{j}_{max}	86	spatial histogram t_3
87	$(1st\ t(v_{y,min}))/T_w$	88	$(2nd\ t(x_{max}))/T_w$
89	$(3rd\ t(x_{max}))/T_w$	90	$(1st\ t(v_{y,max}))/T_w$
91	$t(j_{max})/T_w$	92	$t(j_{y,max})/T_w$
93	direction change histogram c_2	94	$(3rd\ t(y_{max}))/T_w$
95	direction change histogram c_4	96	\bar{j}_y
97	direction change histogram c_3	98	$\theta(initial\ direction)$
99	$\theta(before\ last\ pen-up)$	100	$(2nd\ t(y_{max}))/T_w$

Tabla 3.1: Set de características globales. T denota intervalo de tiempo, t denota instante de tiempo, N denota número de eventos y θ denota el ángulo. Notar que algunos símbolos son definidos en diferentes características de la tabla (e.g. Δ de la característica 7 está definido en la característica 15). Fuente: [2]

Las características globales no son normalizadas en un rango (0,1), al contrario de lo que se puede observar en otros trabajos [9] [2]. El motivo es que los resultados obtenidos al normalizar las características globales eran peores en algunos casos a los no normalizados.

El método utilizado para comparar la similitud entre una firma entrante de un usuario y su correspondiente modelo almacenado en el sistema es la **distancia de Mahalanobis**. La ventaja de este tipo de medida es el bajo coste computacional, además de proporcionar unos resultados razonables. Los modelos de los usuarios $C = (\mu, \Sigma)$ son creados a partir de un set de firmas de entrenamiento, donde Σ es la diagonal de la matriz de covarianza. El *score* se obtiene a través de la inversa de la distancia de Mahalanobis entre el vector de características \mathbf{x} de la firma entrante y el correspondiente modelo C del sistema:

$$s(\mathbf{x}, C) = ((\mathbf{x} - \mu)^T (\Sigma)^{-1} (\mathbf{x} - \mu))^{-1/2} \quad (3.1)$$

Si el *Score* $s(\mathbf{x}, C)$ está por encima de un umbral específico, la firma es considerada como genuina. En el caso contrario ésta es rechazada por el sistema.

3.2. Sistema local de verificación de firma

El sistema local implementado en este proyecto está basado en el algoritmo *DTW*. El motivo por el cual se usa este algoritmo es debido al bajo coste computacional y a la pequeña cantidad de datos de entrenamiento que se posee en un caso común de verificación de firma. Además, hay que tener en cuenta que la implementación realizada en [17] utilizando este algoritmo consiguió ganar la competición *SVC* en el año 2004 [18] y ha seguido obteniendo muy buenos resultados en evaluaciones recientes [10].

El set de características locales (funciones en el tiempo) del que se partía al inicio de la realización del proyecto es el mismo que se recoge en [9], es decir, un total de 27 características. Sin embargo, debido a que el dispositivo PDA no recoge información de presión ni inclinación del bolígrafo (*azimuth* y *altitude*), para realizar los experimentos se ha utilizado solo la información de coordenadas de posición, tanto para el caso de interoperabilidad como sin ella. Por lo tanto en total se trabaja con 21 de las 27 características, explicadas en detalle en la tabla 3.2. Un ejemplo de la extracción de estas características para una firma se puede ver en la Fig. 3.1.

La función utilizada para calcular el *score* entre las características locales de una firma entrante al sistema y las características locales almacenadas en el sistema para ese mismo usuario es:

$$score = e^{-D/K} \quad (3.2)$$

donde D es la distancia mínima acumulada total entre los dos vectores de muestras a comparar y K es el factor de normalización que tiene en cuenta el número de puntos alineados entre las dos secuencias [27].

#	Feature	Description
1	x-coordinate	x_n
2	y-coordinate	y_n
3	Path-tangent angle	$\theta_n = \arctan(\dot{y}_n/\dot{x}_n)$
4	Path velocity magnitude	$v_n = \sqrt{\dot{y}_n^2 + \dot{x}_n^2}$
5	Log curvature radius	$\rho_n = \log(1/k_n) = \log(v_n/\dot{\theta}_n)$, where k_n is the curvature of the position trajectory
6	Total acceleration magnitude	$a_n = \sqrt{t_n^2 + c_n^2} = \sqrt{v_n^2 + v_n^2 \theta_n^2}$, where t_n and c_n are respectively the tangential and centripetal acceleration components of the pen motion
7-12	First-order derivate of features 1-6	$\dot{x}_n, \dot{y}_n, \dot{\theta}_n, \dot{v}_n, \dot{\rho}_n, \dot{a}_n$
13-14	Second-order derivate of features 1-2	\ddot{x}_n, \ddot{y}_n
15	Ratio of the minimum over the maximum speed over a window of 5 samples	$v_n^r = \min\{v_{n-4}, \dots, v_n\} / \max\{v_{n-4}, \dots, v_n\}$
16-17	Angle of consecutive samples and first order difference	$\alpha_n = \arctan(y_n - y_{n-1} / x_n - x_{n-1})$ $\dot{\alpha}_n$
18	Sine	$s_n = \sin(\alpha_n)$
19	Cosine	$c_n = \cos(\alpha_n)$
20	Stroke length to width ratio over a window of 5 samples	$r_n^5 = \frac{\sum_{k=n-4}^{k=n} \sqrt{(x_k - x_{k-1})^2 + (y_k - y_{k-1})^2}}{\max\{x_{n-4}, \dots, x_n\} - \min\{x_{n-4}, \dots, x_n\}}$
21	Stroke length to width ratio over a window of 7 samples	$r_n^7 = \frac{\sum_{k=n-6}^{k=n} \sqrt{(x_k - x_{k-1})^2 + (y_k - y_{k-1})^2}}{\max\{x_{n-6}, \dots, x_n\} - \min\{x_{n-6}, \dots, x_n\}}$

Tabla 3.2: Set de características locales utilizado en el presente proyecto. El punto situado encima de algunas características (e.g. \dot{x}_n) indica derivada en el tiempo. Tabla adaptada de [2].

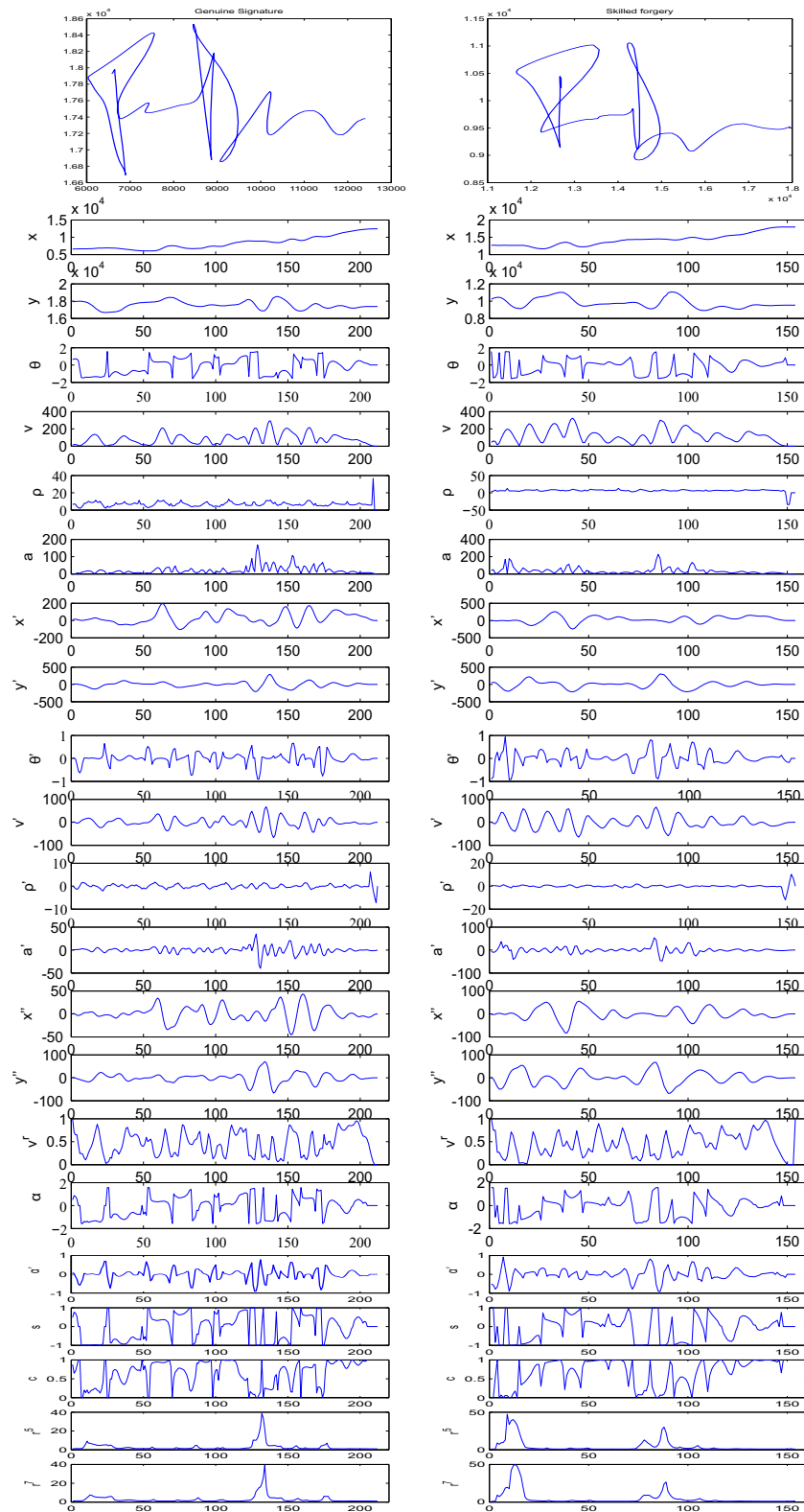


Figura 3.1: Ejemplos de las 21 funciones temporales (características locales) consideradas en el sistema. Las gráficas de la izquierda se corresponden a una firma genuina, mientras que las de la derecha a una imitada (skilled forgery). Ambas firmas se han obtenido de un usuario particular de la base de datos BIOSECURE DS2.

4

Experimentos.

En el presente capítulo se describen los experimentos y resultados obtenidos a lo largo de la realización del proyecto. Dichos experimentos se han realizado usando firmas del mismo conjunto de usuarios adquiridas en los dos escenarios considerados, es decir, con firmas obtenidas de una PDA y con firmas obtenidas de un pen tablet Wacom, permitiendo una clara comparación de los resultados entre ellos.

4.1. Base de datos

Para la realización de los experimentos se ha utilizado un subconjunto de firmas de PDA y pen tablet disponibles en la base de datos multimodal *Biosecure* [28]. En total se han utilizado 120 usuarios (son los que están presentes en ambas bases de datos), con 20 firmas genuinas y 20 firmas *skilled forgeries* por usuario y por dispositivo de captura (e.g. PDA y pen tablet). Las firmas fueron capturadas en dos sesiones diferentes separadas entre ellas por un espacio temporal de 2 meses aproximadamente. En cada sesión, las firmas fueron capturadas en bloques de 5, dejando un espacio de tiempo entre bloques de algunos minutos. En el caso de DS3, las firmas fueron capturadas con un HP iPAQ 2790 PDA, estando el usuario de pie y sujetando con una mano la PDA. En el caso de DS2, las firmas fueron capturadas con una Wacom Intuos A6 tablet, estando el usuario sentado y firmando con un bolígrafo sobre un papel situado encima del tablet (ver Fig. 2.9). Este procedimiento emula unas condiciones reales de uso de los dispositivos a la hora de realizar una firma.

En el caso de la PDA, se captura información de la posición X , Y y del instante de tiempo en el que se realizó el muestreo. No captura información relativa a la presión ni a la inclinación del bolígrafo. Esta información si que está presente en el pen tablet. Sin embargo como ya se comentó en la Sec. 3.2 esta información no será utilizada a la hora de realizar los experimentos, pues no contamos con ella en el caso del dispositivo PDA.

Las firmas *skilled forgeries* de cada uno de los usuarios fueron realizadas por 4 usuarios diferentes (5 firmas *skilled forgeries* por usuario) en un escenario que se daría en el peor de los casos: cada impostor tenía acceso visual a la información dinámica de la firma genuina a

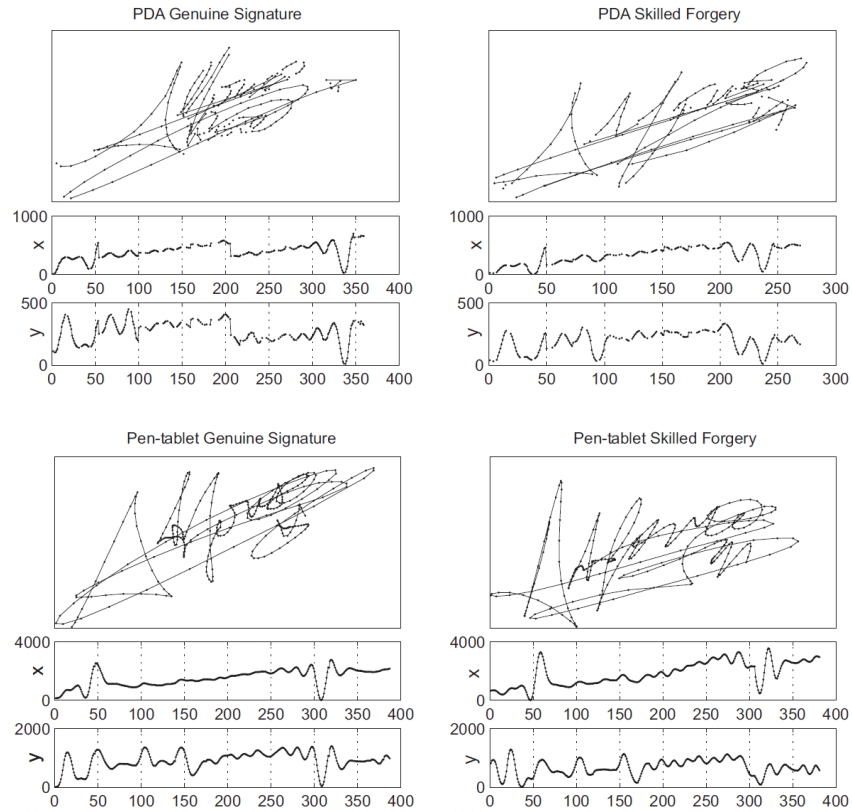


Figura 4.1: Izquierda: Firmas genuinas de un mismo usuario capturadas con la PDA y el pen tablet. Derecha: Firmas skilled forgeries para el mismo usuario capturadas con la PDA y el pen tablet. Figura adaptada de [2]

falsificar, pudiendo visualizar los trazos originales de la firma. En el escenario de la PDA, los trazos originales de la firma fueron mostrados en la propia pantalla de la PDA, donde algunos usuarios incluso pudieron firmar mientras observaban estos trazos. En el escenario del pen tablet, los trazos de la firma fueron presentados en la pantalla de un ordenador.

Un ejemplo de una misma firma capturada con la PDA y con el pen tablet se representa en la Fig. 4.1. A primera vista se puede observar cómo el rango de valores que toman la posición X, Y es distinto en ambos escenarios. Esto es debido a que el espacio disponible para realizar una firma es mucho mayor en el pen tablet que en la PDA. En el caso de las firmas capturadas con la PDA, se aprecia la pérdida de muestras durante la firma debido a errores en la captura. Un preprocesado, basado en la interpolación de las muestras se realiza en el caso de las firmas capturadas con la PDA, con el objetivo de corregir los errores en el muestreo. Para ello se ha utilizado una interpolación basada en *splines* [29], ya que proporciona unos resultados mejores que la interpolación lineal. Además, como la PDA no almacena información relativa a la presión, los *pen-ups* son determinados de manera eurística cuando hay una diferencia entre muestras igual o superior a los 50 ms. Las muestras entre el *pen-up* y el *pen-down* son también interpoladas para obtener un mayor parecido con las firmas obtenidas con el pen tablet. Se han probado distintos tipos de normalizaciones de las firmas en ambas bases de datos, pretendiendo conseguir un mayor parecido entre las firmas de los distintos dispositivos de captura. El objetivo es obtener un mejor comportamiento del sistema en el caso de interoperabilidad. Esto se describe más en detalle en la Sec. 4.3.2.

De los 120 usuarios disponibles en ambas bases de datos, los primeros 50 usuarios son utilizados para realizar el entrenamiento del sistema, mientras que los restantes 70 usuarios son utilizados para evaluar el comportamiento del sistema realizado. El entrenamiento del sistema, es decir, la obtención del vector de características global y local que optimizan el sistema en términos de *EER*, se obtiene a partir del algoritmo *SFFS* (Sec. 2.3.4.3). Este protocolo sigue el mismo comportamiento que la competición *BMEC*, donde un conjunto de firmas provenientes de 50 usuarios son dados previamente a la realización de la competición. La evaluación es posteriormente realizada por los organizadores con un conjunto de usuarios mayor al del entrenamiento.

4.2. Protocolo de experimentación. Interoperabilidad

Los modelos de los usuarios son entrenados con las 5 primeras firmas genuinas de la primera sesión, mientras que las 15 firmas genuinas de la segunda sesión son utilizadas para realizar el testeo.

Los *scores* para el caso *random forgery* (el caso en el que un usuario utiliza su propia firma para hacerse pasar por otro usuario del sistema) son obtenidos comparando el modelo del usuario con una firma genuina del resto de usuarios. Para el caso *skilled forgery*, los *scores* se obtienen comparando el modelo del usuario con las 20 firmas falsificadas disponibles de ese mismo usuario. La figura 4.2 muestra las firmas utilizadas del total disponibles en la base de datos para el caso de un usuario.

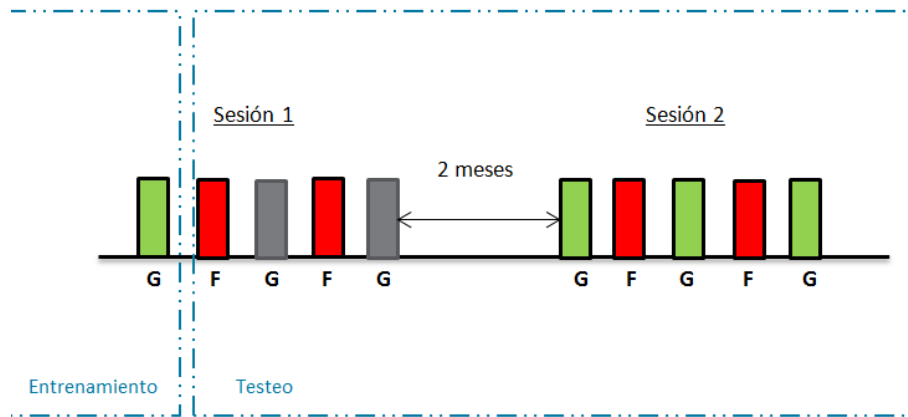


Figura 4.2: Firmas utilizadas para la realización de los experimentos. *G* corresponde a un bloque de 5 firmas genuinas y *F* a un bloque de 5 firmas forgery. Los bloques en gris no son utilizados.

En cuanto a la **interoperabilidad entre sistemas**, se realizan pruebas entrenando el sistema con las firmas de un dispositivo y testeando con las mismas firmas del otro dispositivo. Un ejemplo de la nomenclatura utilizada a lo largo de todo el proyecto para denotar los experimentos realizados es la siguiente:

$$a_b_c$$

donde **a** indica el caso estudiado (random o skilled forgeries), **b** indica la base de datos utilizada para entrenar el sistema (DS2 o DS3) y **c** representa la base de datos utilizada para testear el sistema. Por ejemplo, *skilled_DS2_DS3* sería el estudio del caso skilled forgeries cuando se

utilizan las firmas del dispositivo DS2 para entrenar el sistema y las firmas del dispositivo DS3 para testear.

4.3. Desarrollo experimental

En esta sección, en primer lugar, se va a comprobar el rendimiento del sistema con y sin interoperabilidad sin aplicar ningún tipo de normalización de los datos de entrada. Para ello se ha estudiado el comportamiento para las características de los sistemas global y local en términos de *EER*. Posteriormente se analizará en detalle distintos tipos de normalizaciones que mejorarán el rendimiento del sistema al aplicar interoperabilidad, para finalmente seleccionar el conjunto de características del sistema final.

Los 50 primeros usuarios de las bases de datos *Biosecure DS2 y DS3* son utilizados a lo largo de toda esta sección.

4.3.1. Rendimiento del sistema. Experimentos iniciales

En esta sección el objetivo es presentar el rendimiento del sistema inicial con y sin interoperabilidad, **sin aplicar ningún tipo de normalización de los datos de entrada**. Para ello se ha utilizado el algoritmo *SFFS* de la Sec. 2.3.4.3, representando la evolución del sistema en términos de *EER* acorde con el tamaño del vector óptimo de características. Esto se ha realizado tanto para las características globales como para las características locales.

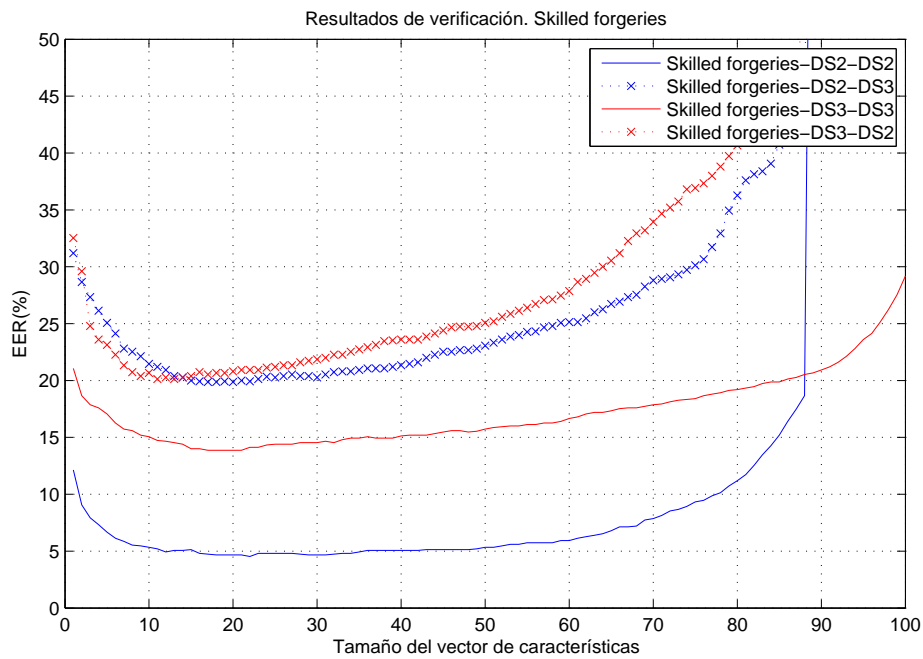
4.3.1.1. Características globales

El vector de 100 características globales descrito en la Sec. 3.1 se ha tenido en cuenta en estos experimentos. En la figura 4.3 se representa la evolución del *EER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* para los casos *skilled forgeries* y *random forgeries*.

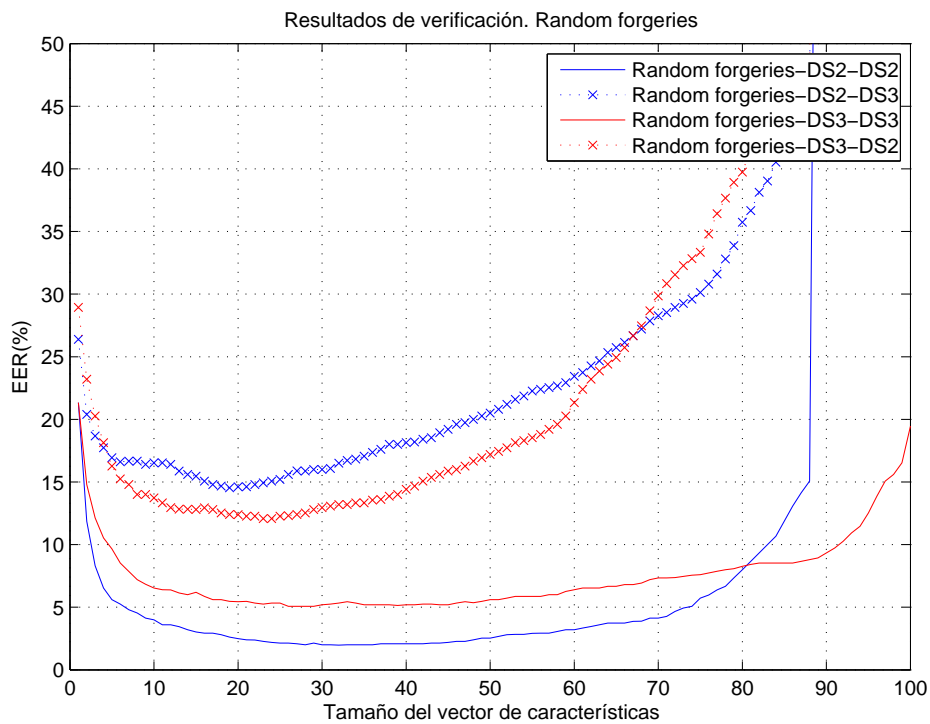
Hay que tener en cuenta que el algoritmo *SFFS* se ha aplicado de manera **independiente** para cada uno de los casos. Por lo tanto si elegimos por ejemplo el vector de 30 características en cada uno de ellos, el conjunto de características almacenado en cada vector será distinto para cada uno de los casos.

Observando las gráficas en el caso sin interoperabilidad (DS2-DS2, DS3-DS3) se pueden extraer varias deducciones. En primer lugar vemos como el comportamiento del dispositivo de captura DS2 (pen tablet) es mejor en ambos escenarios, especialmente en el caso *skilled forgeries*, donde el *EER* desciende en torno a un 9 % respecto a DS3 (PDA). Por otro lado, si observamos cuidadosamente el comportamiento del *EER* para el caso de DS3 (PDA), vemos como el número de características necesarias hasta llegar a una zona estable de *EER* es inferior, especialmente en el caso *random forgeries*. Estos resultados coinciden con los obtenidos en [2].

Realizando un análisis de los resultados para el caso con interoperabilidad (DS2-DS3, DS3-DS2) se pueden extraer también ciertas conclusiones. El rendimiento del sistema para el caso DS3-DS2, es decir, entrenar el sistema con la base de datos DS3 (PDA) y testear con la base de datos DS2 (pen tablet) proporciona unos resultados iguales (en el caso *Skilled forgeries*, Fig. 4.3(a)) o incluso mejores (en el caso *Random forgeries*, Fig. 4.3(b)) que para el caso DS2-DS3. Esto es un resultado bastante curioso y que demuestra como la base de datos DS2 (pen tablet)



(a) *Skilled forgeries.*



(b) *Random forgeries.*

Figura 4.3: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. Sin aplicar ningún tipo de normalización de los datos de entrada.

tiene un mejor comportamiento a la hora de capturar firmas (menor variación intra-clase y más variación inter-clase). Es decir, es preferible entrenar el sistema con un dispositivo de peores prestaciones y utilizar durante el testeo un dispositivo más fiable. No hay que olvidar que el dispositivo utilizado en DS3 es una PDA y que por lo tanto no está diseñado para la captura de firmas, al contrario del dispositivo DS2, en el que se emplea una Wacom de altas prestaciones diseñada exclusivamente para la captura de firmas.

De acuerdo con lo comentado anteriormente, se puede observar como hay una mayor diferencia absoluta de *EER* entre el caso sin y con interoperabilidad (DS2-DS2 vs DS2-DS3) cuando entrenamos el sistema con DS2 (pen tablet). Esto es especialmente crítico en el caso *skilled forgeries*, donde hay una diferencia absoluta de un 15 % de *EER* entre el caso de sin interoperabilidad (testear con DS2) y con interoperabilidad (testear con DS3) para el conjunto de características óptimo. Por lo tanto éste será el caso más importante a tener en cuenta a la hora de optimizar el sistema. En el caso sin y con interoperabilidad (DS3-DS3 vs DS3-DS2) al entrenar con DS3 (PDA), se aprecia una menor diferencia absoluta de *EER* para el conjunto de características óptimo, siendo más importante en el caso *random forgeries*.

La contribución de cada tipo de característica (ver tabla 3.1) en el vector de características óptimo (aquel que proporciona un menor *EER*) para cada uno de los casos posibles se describe a continuación. La Fig. 4.4 representa el tipo de características globales seleccionadas para el caso *skilled forgeries* y *random forgeries*.

Analizando el tipo de características seleccionadas en el caso sin interoperabilidad (DS2-DS2, DS3-DS3), se puede apreciar un predominio de las características de tipo 2 (velocidad y aceleración) y de tipo 4 (geometría) tanto para el caso *skilled forgeries* como para el caso *random forgeries*. Sin embargo en el caso con interoperabilidad (DS2-DS3, DS3-DS2) se produce una pérdida de la importancia del tipo de características 4 (geometría), a favor de las características de tipo 1 (tiempo), tanto para el caso *skilled forgeries* como para el caso *random forgeries*. El motivo de este efecto puede deberse a las grandes diferencias existentes entre los dispositivos PDA y pen tablet en cuanto al tamaño de la pantalla, precisión (píxeles/pulgada) y percepción de comodidad del usuario al realizar la firma, ya que la PDA no está diseñada para ello.

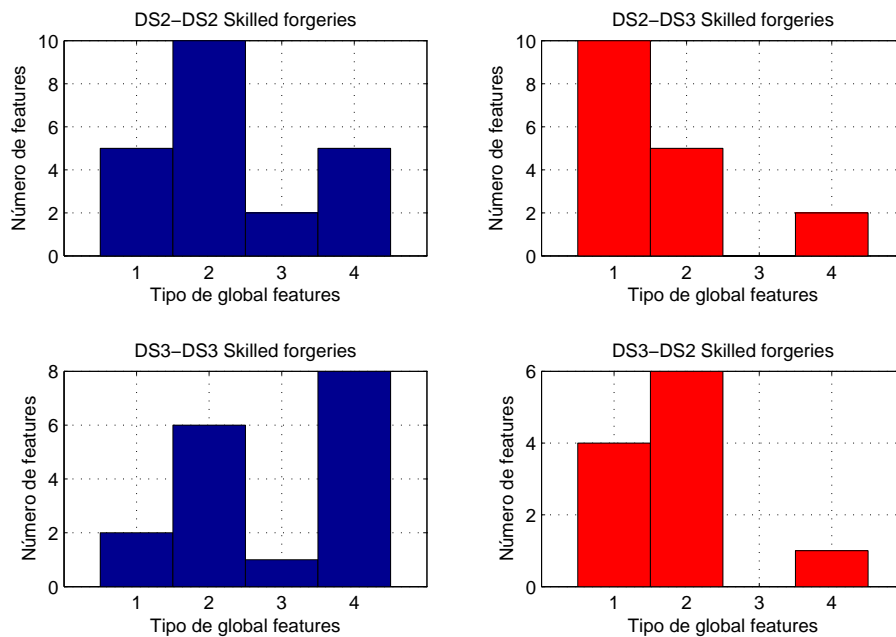
Otro aspecto a mencionar en todos los casos es la poca aportación de las características de tipo 3 (dirección). Un motivo puede ser el hecho de que no se haya aplicado ningún tipo de normalización de rotación de la firma. Este efecto parece estar más controlado en el dispositivo PDA, ya que el usuario tiende a cogerla siempre de la misma forma.

4.3.1.2. Características locales

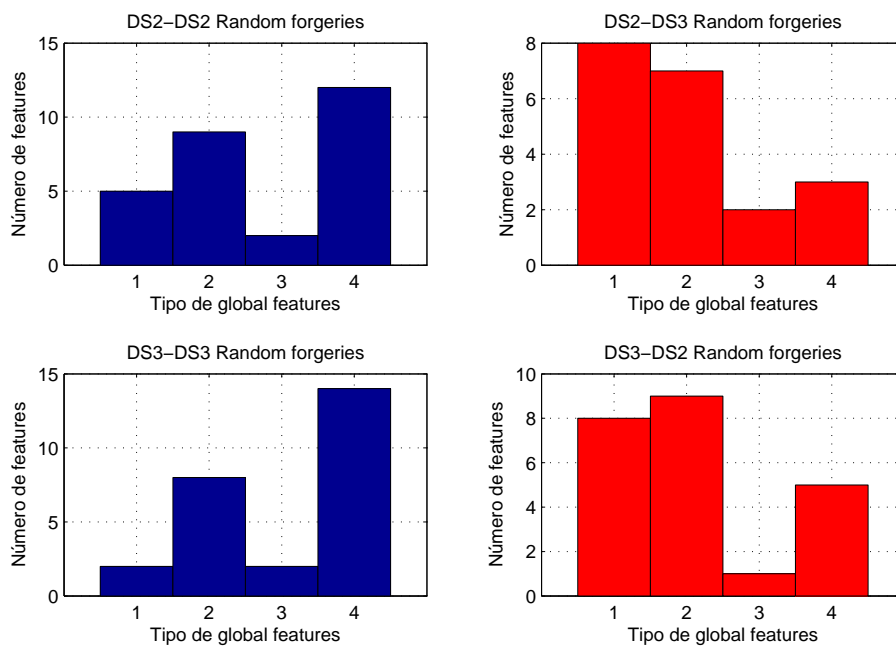
El vector de 21 características locales descrito en la Sec. 3.2 se ha tenido en cuenta en estos experimentos. En la figura 4.5 se representa la evolución del *EER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* para los casos *skilled forgeries* y *random forgeries*.

Hay que tener en cuenta que el algoritmo *SFFS* se ha aplicado de manera **independiente** para cada uno de los casos. Por lo tanto si elegimos por ejemplo el vector de 15 características en cada uno de ellos, el conjunto de características almacenado en cada vector será distinto para cada uno de los casos.

Analizando el caso sin interoperabilidad (DS2-DS2, DS3-DS3), se puede apreciar de nuevo un mejor comportamiento del sistema para el pen tablet, especialmente en el caso *skilled forgeries*. En el caso de DS3 (PDA) se aprecia una mayor degradación del rendimiento del sistema a medida que se incrementa el número de características, especialmente en el caso *skilled forgeries*.

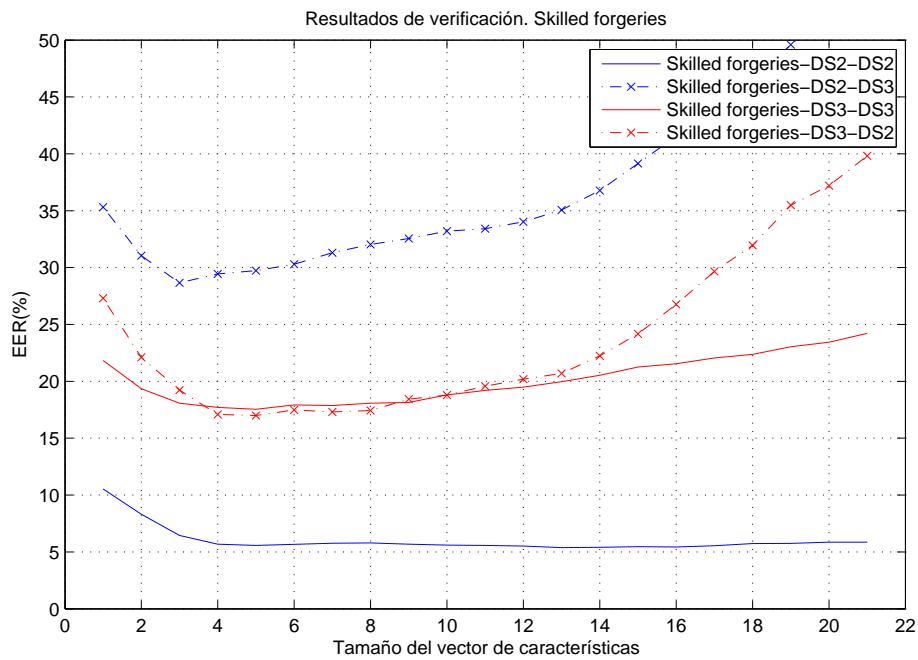


(a) *Skilled forgeries.*

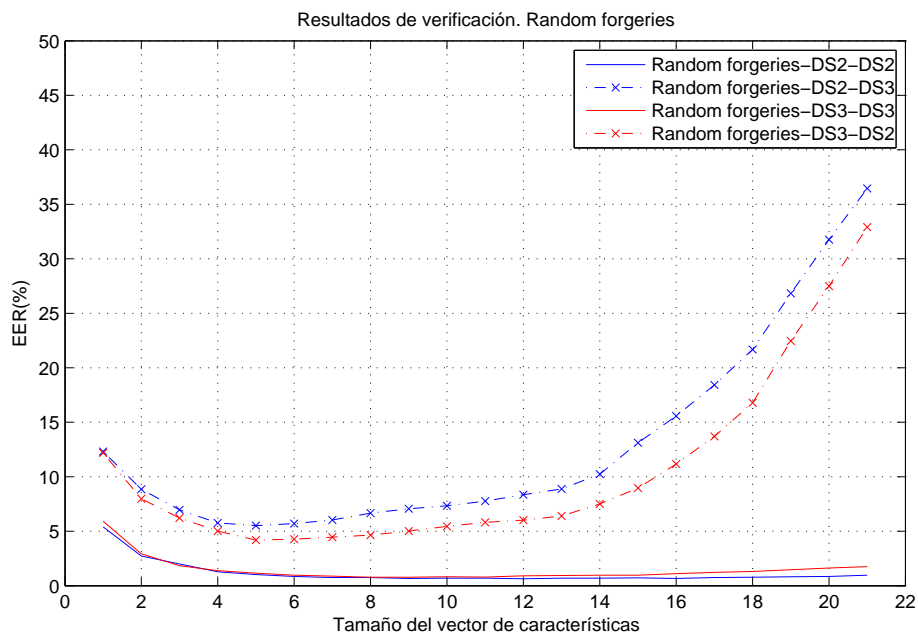


(b) *Random forgeries.*

Figura 4.4: Histograma del tipo de características obtenidas para cada uno de los casos. Las imágenes de la izquierda representan el caso sin interoperabilidad y las de la derecha con interoperabilidad.



(a) *Skilled forgeries.*



(b) *Random forgeries.*

Figura 4.5: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. Sin aplicar ningún tipo de normalización de los datos de entrada.

Analizando el caso con interoperabilidad (DS2-DS3, DS3-DS2) volvemos a observar los mismos resultados que en la Sec. 4.3.1.1. El entrenamiento del sistema con DS3 (PDA) y el posterior testeo con DS2 (pen tablet) proporciona mejores resultados. Esto llega hasta el punto de que es mejor el caso con interoperabilidad que sin ella (DS3-DS2 vs DS3-DS3) para el caso de entrenar el sistema con DS3 (PDA).

Realizando un análisis general, se aprecia de nuevo como el caso que obtiene peores resultados es el entrenamiento del sistema con DS2 (pen tablet) y testeo con DS3 (PDA) para el caso *skilled forgeries*. Por lo tanto éste será de nuevo el caso a tener más en cuenta para su posterior mejora.

4.3.2. Normalizaciones de los datos de entrada

Debido a las grandes diferencias entre los dos dispositivos de captura utilizados (PDA y pen tablet), es necesario realizar un análisis en detalle de las propiedades de cada uno de ellos a la hora de realizar una firma. Esto servirá para obtener una misma normalización de las firmas y por tanto mejorar el rendimiento del sistema en el caso con interoperabilidad.

Para ello, en primer lugar se comprobó la disposición de las firmas de un mismo usuario para cada dispositivo. En la Fig. 4.6(a) y Fig. 4.6(b) se representan las firmas de un mismo usuario para las bases de datos DS2 y DS3 sin realizar ningún tipo de normalización. Como se aprecia en las figuras, las firmas presentan una alta variabilidad en el posicionamiento espacial, especialmente en el caso DS2 (pen tablet) debido a que la pantalla de captura es mucho mayor que la de la PDA.

Otro aspecto relevante en ambos dispositivos es el tamaño de las firmas. La Fig. 4.6(c) es un ejemplo de ello. La firma de DS2 (pen tablet) posee un tamaño mucho mayor que la de DS3 (PDA). Esto puede ser debido a que un usuario tiende a firmar más grande al tener una pantalla de mayor tamaño y a la resolución de las pantallas, dependiendo del tamaño de los píxeles.

Con el objetivo de solucionar las diferencias encontradas en los dispositivos, se han estudiado distintos tipos de normalizaciones de los datos de entrada.

4.3.2.1. Normalización por el centro de masas

Este tipo de normalización consigue que todas las firmas tengan el mismo centro espacial. Un ejemplo de ello se puede apreciar en la Fig. 4.7(a), donde las firmas utilizadas son las mismas que las indicadas en la Fig. 4.6(a) pero con un mismo centro espacial.

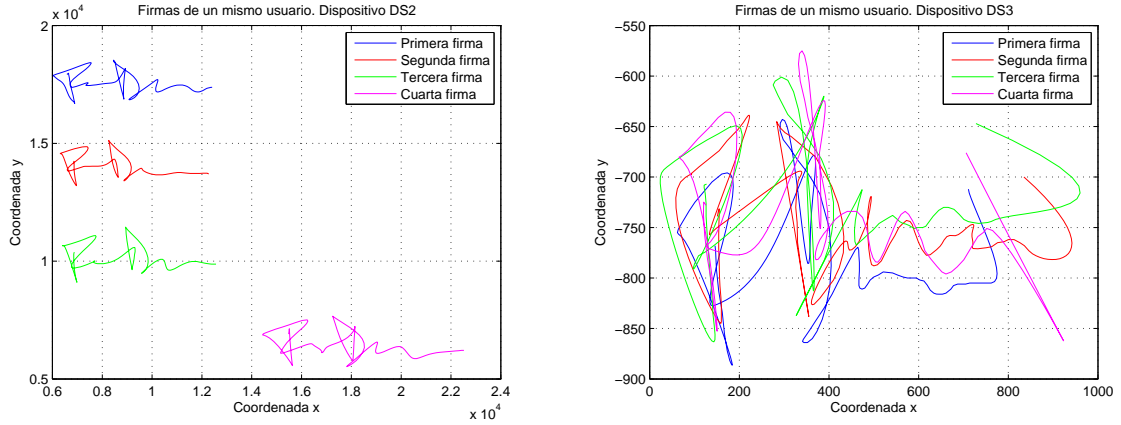
Esta normalización se aplica a cada una de las muestras de una firma, para las coordenadas X, Y . La fórmula utilizada es la siguiente:

$$x(i)_{norm} = x(i) - \mu_x. \quad (4.1)$$

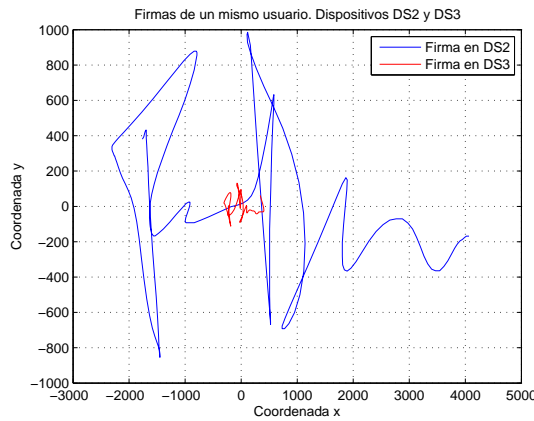
donde $x(i)$ representa una muestra de la coordenada X en este caso concreto y μ_x la media de las coordenadas X para esa firma en concreto.

4.3.2.2. Normalización por la media y desviación típica

Este tipo de normalización consigue que todas las firmas se encuentren normalizadas tanto en centro espacial como en tamaño, solucionando así los problemas de la Fig. 4.6. Un ejemplo de ello se puede apreciar en la Fig.4.7(b).



(a) Representación de distintas firmas de un mismo usuario en DS2 sin normalizar. (b) Representación de distintas firmas de un mismo usuario en DS3 sin normalizar.



(c) Firma de un mismo usuario en DS2 y DS3 sin normalizar el tamaño.

Figura 4.6: Representación de firmas de las bases de datos DS2 y DS3 sin normalizar.

Esta normalización se aplica a cada una de las muestras de una firma, para las coordenadas X, Y . La fórmula utilizada es la siguiente:

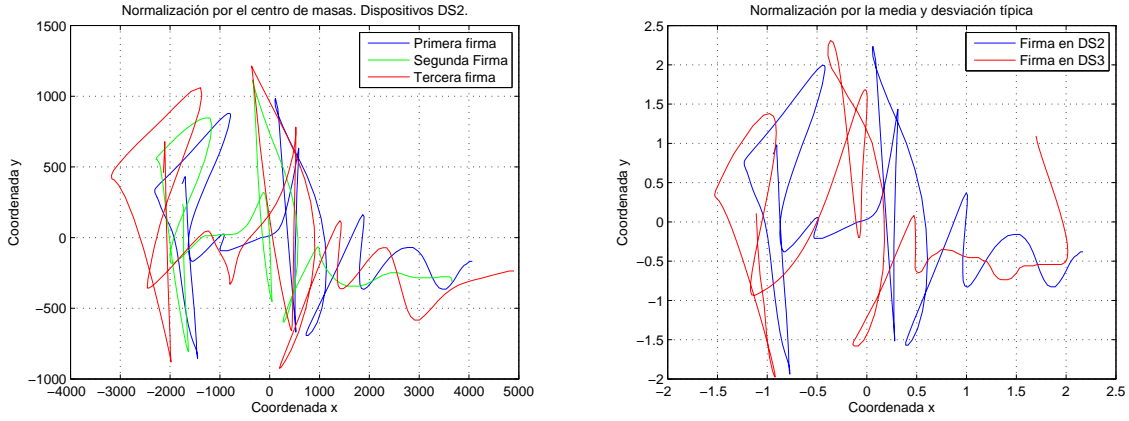
$$x(i)_{norm} = (x(i) - \mu_x) / \sigma_x. \tag{4.2}$$

donde $x(i)$ representa una muestra de la coordenada X en este caso concreto y μ_x, σ_x a la media y a la desviación típica respectivamente de las coordenadas X para esa firma en concreto.

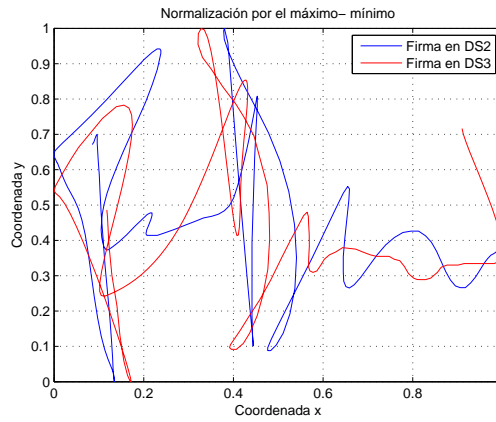
4.3.2.3. Normalización por el máximo y el mínimo

Este tipo de normalización consigue que todas las firmas se encuentren normalizadas tanto en centro espacial como en tamaño, solucionando así el problema de las figuras Fig. 4.6. Un ejemplo de ello se puede apreciar en la Fig.4.7(c).

Esta normalización se aplica a cada una de las muestras de una firma, para las coordenadas X, Y . El inconveniente que presenta este tipo de normalización es que es poco robusta a variaciones en los extremos de la firma, por ejemplo en la rúbrica, ya que origina diferentes centros espaciales en cada una de las firmas. La fórmula utilizada es la siguiente:



(a) Firmas de un mismo usuario de DS2 normalizadas por el centro de masas. (b) Firmas de un mismo usuario en DS2 y DS3 normalizadas por la media y la desviación típica.



(c) Firmas de un mismo usuario en DS2 y DS3 normalizadas por el máximo-mínimo.

Figura 4.7: Tipos de normalizaciones estudiadas.

$$x(i)_{norm} = (x(i) - \min(x)) / (\max(x) - \min(x)). \quad (4.3)$$

donde $x(i)$ representa una muestra de la coordenada X en este caso concreto y \max , \min al máximo y al mínimo valor respectivamente de las coordenadas X para esa firma en concreto.

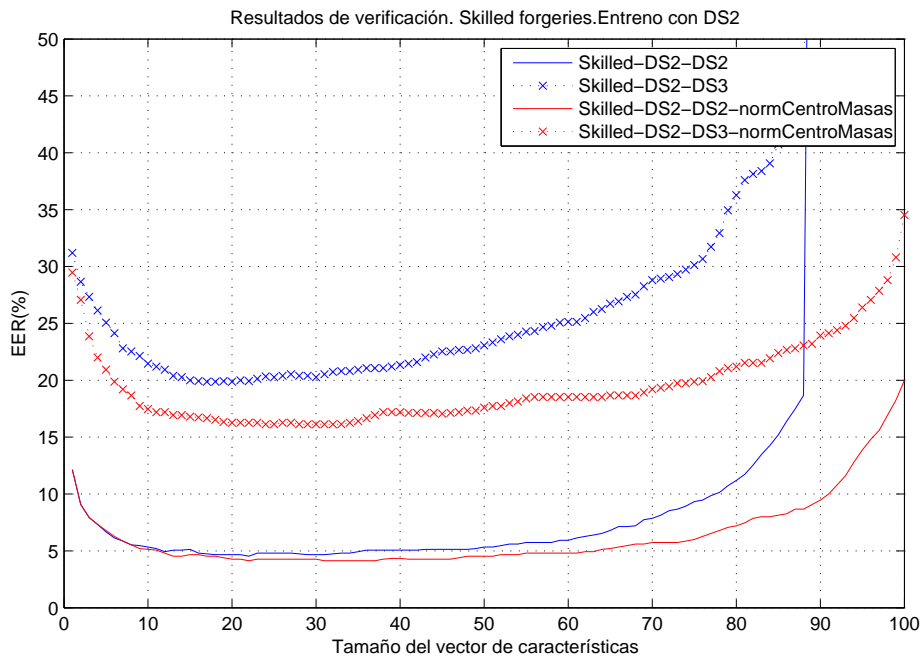
4.3.3. Rendimiento del sistema aplicando normalizaciones

En esta sección se representan los resultados del rendimiento del sistema en términos de *EER* al aplicar las normalizaciones descritas anteriormente a los datos de entrada. El procedimiento a seguir es el mismo que el descrito en la Sec. 4.3.1.

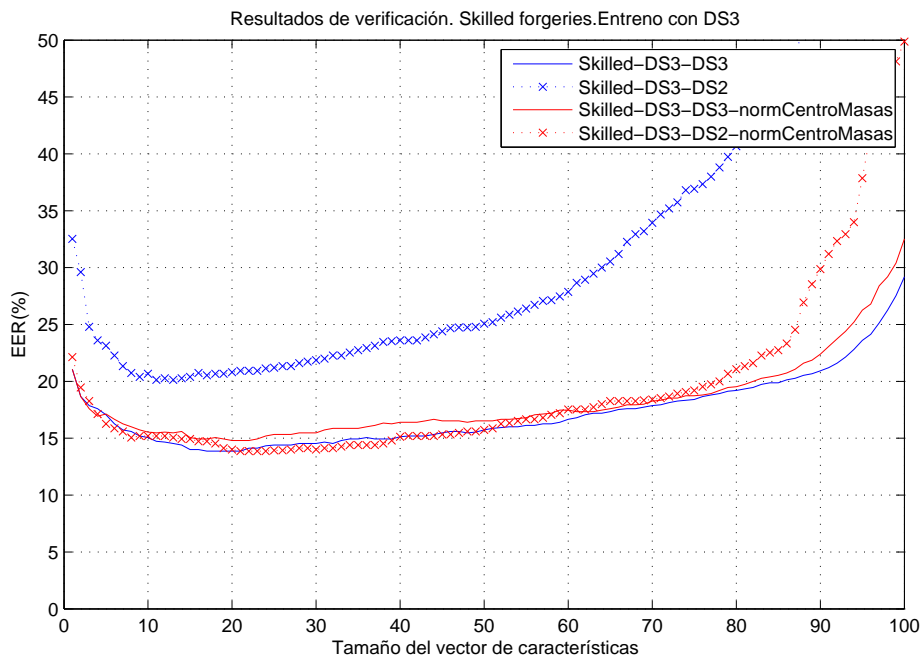
4.3.3.1. Características globales

Se ha tenido en cuenta de nuevo el vector de 100 características globales descrito en la Sec. 3.1. En Fig. 4.8 y Fig. 4.9 se representa la evolución del *EER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* para la normalización

de los datos de entrada por el centro de masas. Esta normalización ha sido la que ha proporcionado un mejor rendimiento en el sistema en todos los casos. Los resultados de *EER* obtenidos para cada tipo de normalización de los datos de entrada se muestran en el *anexo A*.

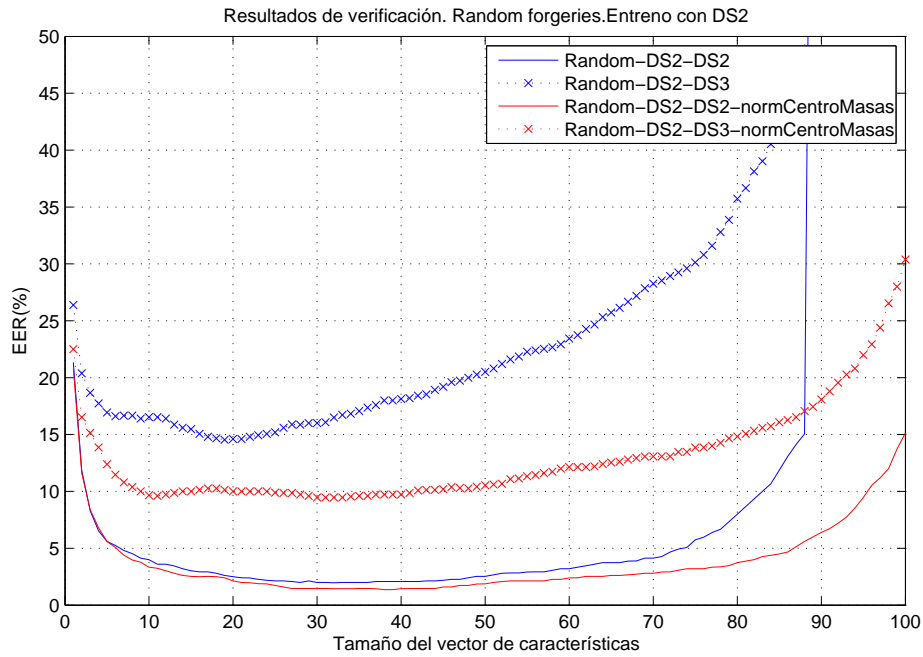


(a) Entrenamiento del sistema con DS2.

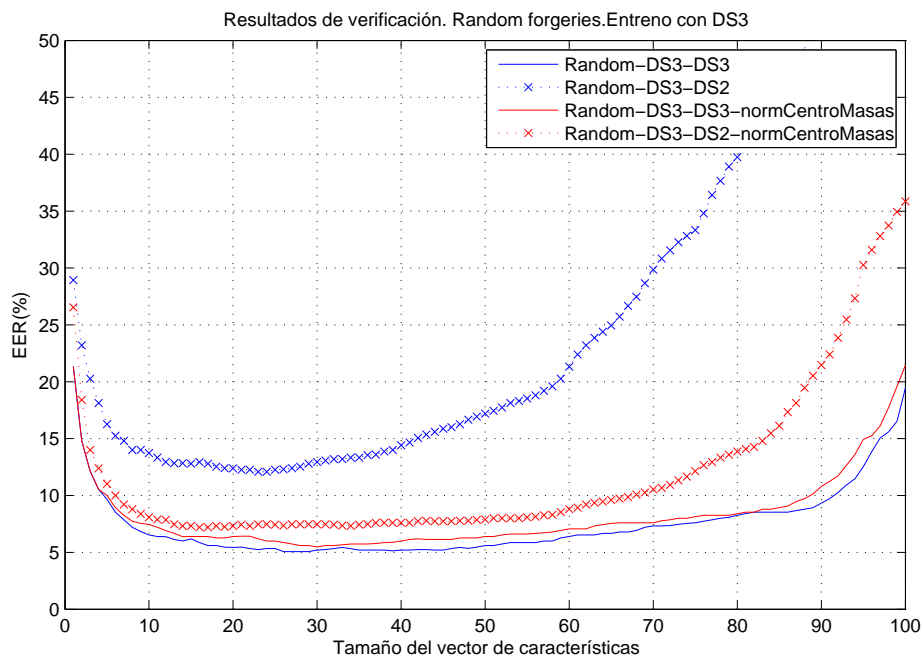


(b) Entrenamiento del sistema con DS3.

Figura 4.8: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo *SFFS* para el caso *skilled forgeries*. Aplicando normalización por el centro de masas.



(a) Entrenamiento del sistema con DS2.



(b) Entrenamiento del sistema con DS3.

Figura 4.9: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo *SFFS* para el caso **random forgeries**. Aplicando normalización por el centro de masas.

Analizando el caso sin interoperabilidad (DS2-DS2, DS3-DS3) se aprecia como la normalización realizada conserva prácticamente el mismo rendimiento del sistema que se tenía sin aplicar

ningún tipo de normalización. Sin embargo, en el caso con interoperabilidad (DS2-DS3, DS3-DS2) vemos como la normalización realizada de los datos de entrada consiguen una gran mejora en el rendimiento del sistema, consiguiendo así uno de los principales objetivos de este proyecto. Esto es especialmente relevante para el entrenamiento del sistema con DS3 (PDA), ya que el *EER* obtenido en los casos con y sin interoperabilidad son prácticamente iguales. En el caso de entrenar el sistema con DS2 (pen tablet), vemos como hay bastante diferencia en el *EER* entre el caso con y sin interoperabilidad, pero a pesar de ello la normalización de los datos de entrada consigue una mejora del *EER* de hasta un 5 % respecto al sistema inicial en el caso con interoperabilidad sin normalizar.

Por lo tanto a la vista de los resultados se puede deducir que el caso crítico a optimizar, como ocurría también en la Sec. 4.3.1.1, es *skilled-DS2-DS3-normCentroMasas*, ya que hay una diferencia de *EER* de un 10 % aproximadamente entre los casos con y sin interoperabilidad (DS2-DS3 vs DS2-DS2), además de que es el peor *EER* que se obtiene en el sistema.

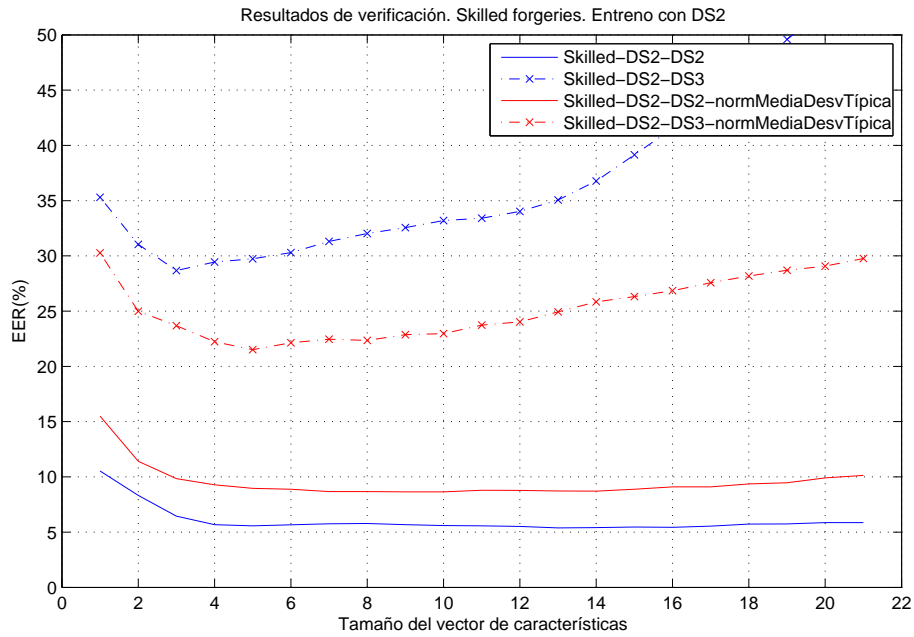
4.3.3.2. Características locales

Se ha tenido en cuenta de nuevo el vector de 21 características locales descrito en la Sec. 4.3.1.2. En Fig. 4.10 y Fig. 4.11 se representa la evolución del *EER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* **para la normalización de los datos de entrada por la media y la desviación típica**. Esta normalización ha sido la que ha proporcionado un mejor rendimiento en el sistema para todos los casos. Los resultados de *EER* obtenidos para cada tipo de normalización de los datos de entrada se muestran en el *anexo A*.

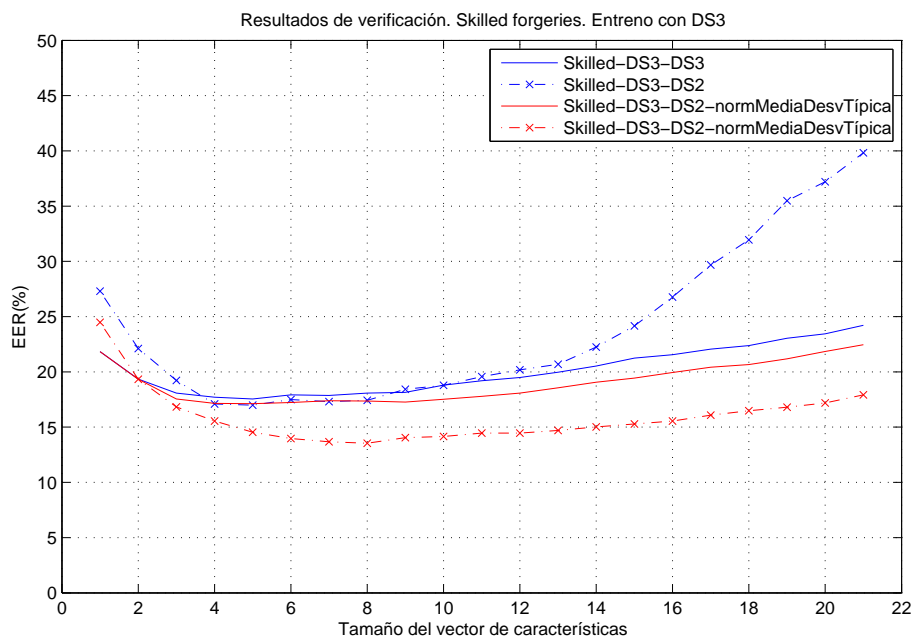
Analizando el caso *skilled-DS2-DS2* se aprecia cómo la normalización realizada produce un aumento del 3 % en el *EER* respecto al caso inicial en el que no se realizaba ningún tipo de normalización. Sin embargo, realizando esta normalización conseguimos mejorar en el caso de interoperabilidad (*skilled-DS2-DS3*) hasta en un 7 % el *EER* respecto al sistema inicial en el que no se aplicaba ninguna normalización. Por lo tanto, puesto que *skill-DS2-DS3* es el caso crítico, es preferible aplicar la normalización por la media y la desviación típica a los datos de entrada.

Analizando el resto de casos, se aprecia como esta normalización consigue muy buenos resultados, ya que el rendimiento del sistema es bastante parecido en los casos con y sin interoperabilidad.

Esta gran mejora que se produce en el *EER* se debe a que conseguimos que las coordenadas de ambos dispositivos estén en un mismo rango, de tal manera que al aplicar el algoritmo *DTW*, el alineamiento temporal dinámico producido entre las firmas de ambos dispositivos es mayor y proporcionará mejores resultados en el rendimiento del sistema.

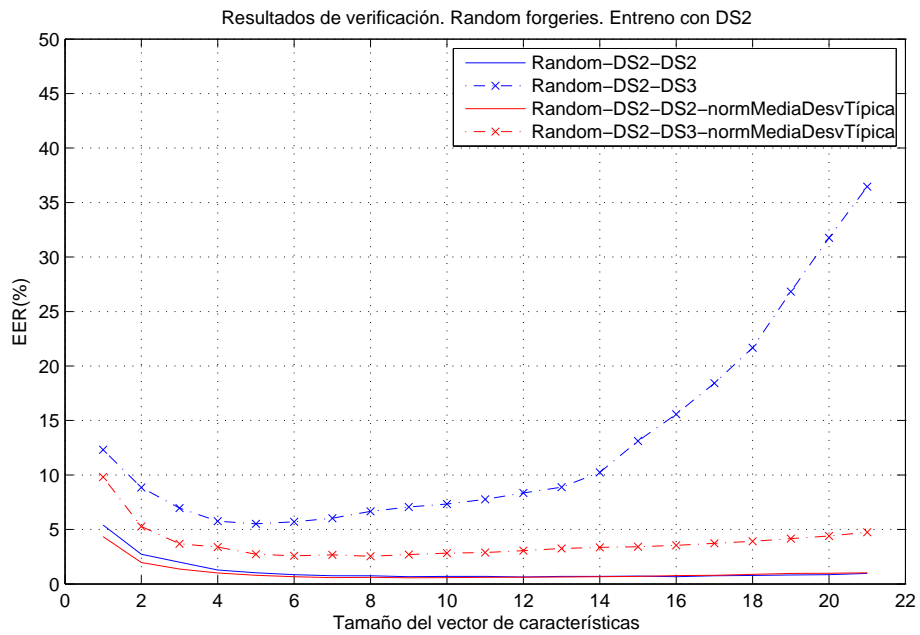


(a) Entrenamiento del sistema con DS2.

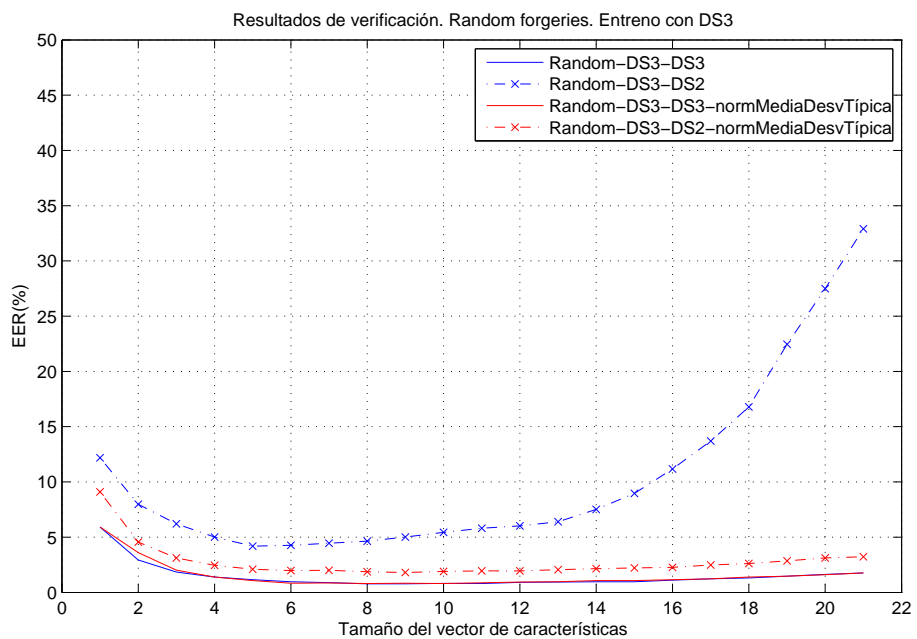


(b) Entrenamiento del sistema con DS3.

Figura 4.10: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo *SFFS* para el caso *skilled forgeries*. Aplicando normalización por la media y la desviación típica.



(a) Entrenamiento del sistema con DS2.



(b) Entrenamiento del sistema con DS3.

Figura 4.11: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso *random forgeries*. Aplicando normalización por la media y la desviación típica.

4.3.4. Selección de las características del sistema

Una vez realizada la normalización de los datos de entrada, tanto para las características globales como locales, procedemos a realizar la selección de las características que formarán

parte de nuestro sistema final.

En cada uno de los casos vistos anteriormente se consigue el mejor *EER* para un vector de características distinto, tanto en tamaño como en las características seleccionadas. Esto daría como resultado la implementación de 8 sistemas distintos (uno para cada caso). Como el objetivo de este proyecto es **obtener un sólo sistema final**, cuyo comportamiento sea bueno tanto en el caso con interoperabilidad como sin ella, es necesario realizar un estudio de diferentes métodos que consigan proporcionar un buen rendimiento del sistema para todos los casos. A continuación explicamos en detalle el procedimiento seguido para la obtención del conjunto de características globales y locales del sistema final.

4.3.4.1. Características globales

La primera posibilidad planteada, la más sencilla, fue la **selección del vector de características que optimiza el caso crítico**, es decir, *skilled-DS2-DS3*, explicado en la Sec. 4.3.3.1. La tabla 4.1 muestra los *EER* obtenidos para este caso (casos *Vector elegido*) frente a los *EER* que se obtendría si considerásemos 8 vectores de 30 características óptimos (una vez aplicada la normalización de los datos de entrada), uno para cada caso (casos *Baseline*).

	<i>Skilled forgeries</i>		<i>Random forgeries</i>	
	Baseline	Vector elegido	Baseline	Vector elegido
EER_DS2_DS2	4.273 %	9.866 %	1.473 %	7.467 %
EER_DS3_DS3	15.472 %	23.600 %	5.475 %	13.867 %
EER_DS2_DS3	16.100 %	16.100 %	9.464 %	15.211 %
EER_DS3_DS2	14.226 %	34.876 %	7.458 %	28.267 %

Tabla 4.1: *Características globales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 30 de características óptimo para cada caso) y el caso de elegir únicamente el vector de características del caso crítico (skilled-DS2-DS3).*

Como se puede apreciar en la tabla 4.1, se consigue alcanzar para el caso crítico el mejor comportamiento posible, sin embargo en el resto de casos empeora mucho el rendimiento del sistema, llegando a incrementar el *EER* hasta cuatro veces más en algunos casos. Por lo tanto esta solución no es válida.

La siguiente solución en la que se pensó fue la posibilidad de seleccionar aquellas características que más se repetían en el conjunto de los 8 vectores de características óptimos. De esta manera conseguiríamos que en el vector de características elegido estuvieran las características habituales de cada uno de los casos. La tabla 4.2 muestra las características más repetidas.

Número de repeticiones	Características
8	31
7	26, 45, 66, 69
6	23, 43, 48, 54, 65, 70, 86
5	3, 39
4	1, 18, 19, 20, 21, 24, 29, 44, 58, 62, 75, 76, 83, 89
3	14, 17, 28, 40, 46, 49, 51, 53, 56, 61, 64, 74, 79, 94

Tabla 4.2: *Características globales que más se repiten en el conjunto de los 8 vectores de características óptimos (seleccionando 30 características en cada uno de ellos).*

Se realizaron pruebas con diferentes vectores de características, en los que se fueron introduciendo cada vez más características en función de su repetición (tabla 4.2). El vector de características que proporcionaba unos mejores resultados fue aquel que incluía todas aquellas características que se repetían hasta 4 veces en el conjunto de los 8 casos posibles. Los resultados obtenidos para el caso de seleccionar estas características se representan en la tabla 4.3.

	<i>Skilled forgeries</i>		<i>Random forgeries</i>	
	Baseline	Vector elegido	Baseline	Vector elegido
EER_DS2_DS2	4.273 %	7.200 %	1.473 %	4.000 %
EER_DS3_DS3	15.472 %	19.067 %	5.475 %	8.193 %
EER_DS2_DS3	16.100 %	21.467 %	9.464 %	16.933 %
EER_DS3_DS2	14.226 %	37.867 %	7.458 %	35.200 %

Tabla 4.3: *Características globales. Comparación de los resultados de EER obtenidos para el caso baseline (un vector de 30 características óptimo para cada caso) y el caso de elegir únicamente el vector de características más repetido.*

A la vista de los resultados, el rendimiento del sistema está muy lejos de los resultados que nos gustaría obtener en el sistema. Seguimos observando como en algunos casos el *EER* obtenido es hasta cinco veces peor que el óptimo. Esto se debe a que con este método tampoco vamos a ser capaces de conseguir el conjunto de características global óptimo. Puede darse el caso de que haya un conjunto de características que se repitan pocas veces, pero que sin embargo, si se introducen en el conjunto de características elegido, mejora mucho el *EER* en algunos casos y en otros no afecta.

Por este motivo es necesario pensar en otro método que consiga extraer el conjunto de características globales que minimice el *EER* en todos los casos, obteniendo unos resultados cercanos al *baseline*. Este algoritmo no podía ser otro que el **SFFS**. Como ya habíamos comentando en la Sec. 2.3.4.3, este algoritmo consigue obtener el conjunto de características que optimiza una condición. En nuestro caso, pretendemos obtener un sistema con un rendimiento bueno para todos los casos y en especial para el caso crítico *skilled-DS2-DS3*, como se ha visto en la Sec. 4.3.3.1. Por esta razón la condición impuesta en el algoritmo *SFFS* es que se obtenga el menor *EER* total (suma del *EER* de los 8 casos) y que proporcione el menor *EER* en el caso crítico, *skilled-DS2-DS3*.

Los resultados obtenidos al aplicar el algoritmo *SFFS* con las condiciones impuestas anteriormente se representan en la Fig. 4.12. En esta figura se representa el *EER* medio, es decir, la media de los *EER* de los 8 casos posibles. En la tabla 4.4 se representan además los *EER* obtenidos para cada uno de los casos posibles cuando se selecciona el vector óptimo de 28 características, que como se aprecia en la Fig. 4.12 es el que proporciona un mejor rendimiento en el sistema y además un menor *EER* para el caso crítico *skilled-DS2-DS3*. A la vista de los resultados, el conjunto de características obtenido con el algoritmo *SFFS* proporciona un equilibrio mayor que en el resto de casos estudiados anteriormente. En todos los casos, los resultados de *EER* se acercan bastante al *EER* que se obtendría si se utilizase un conjunto de características distinto para cada uno de los casos.

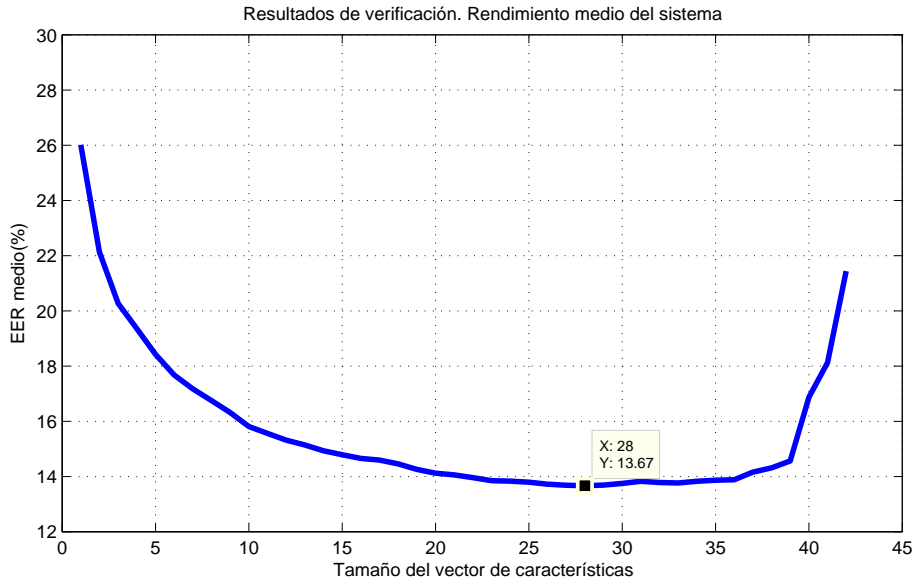


Figura 4.12: Características globales. Rendimiento medio del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo *SFFS*. El punto indicado en la gráfica es el que proporciona el mejor resultado para las dos condiciones a optimizar.

	<i>Skilled forgeries</i>		<i>Random forgeries</i>	
	Baseline	Vector elegido	Baseline	Vector elegido
EER_DS2_DS2	4.273 %	8.333 %	1.473 %	4.000 %
EER_DS3_DS3	15.472 %	20.533 %	5.475 %	8.609 %
EER_DS2_DS3	16.100 %	20.000 %	9.464 %	13.733 %
EER_DS3_DS2	14.226 %	21.933 %	7.458 %	13.200 %

Tabla 4.4: Características globales. Comparación de los resultados de *EER* obtenidos para el caso *baseline* (un vector de 30 características óptimo para cada caso) y el caso de elegir únicamente un vector de características obtenido con el algoritmo *SFFS*.

El conjunto de características globales óptimo obtenido con el algoritmo *SFFS* está compuesto por un total de 28 características (ver Fig. 4.12). De estas características, hay algunas de ellas que se repiten únicamente en 3 de los 8 casos posibles. Sin embargo, otras características que se repiten más veces no aparecen dentro del conjunto de características óptimo. Esto demuestra la teoría lanzada previamente, en el que no por repetirse más una característica significa influir más en el rendimiento del sistema.

La contribución de cada tipo de característica (ver tabla 3.1) en el vector de características seleccionado por el algoritmo *SFFS* se representa en la Fig. 4.13. Observando los resultados se aprecia un predominio de las características de tipo 2 (velocidad y aceleración) y sobre todo de tipo 4 (geometría). Estos resultados coinciden con los obtenidos en la Sec. 4.3.1.1 para el caso del sistema sin interoperabilidad (DS2-DS2, DS3-DS3). Esto se debe a que con las normalizaciones realizadas, las firmas de ambos dispositivos tienen un comportamiento en geometría muy parecido, de ahí el predominio de este tipo de características.

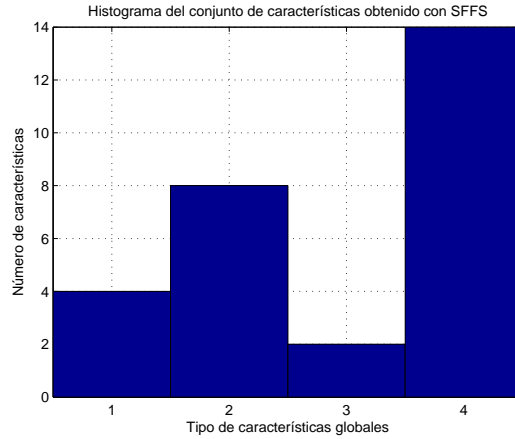


Figura 4.13: Características globales. Histograma del tipo de características seleccionadas por el algoritmo SFFS para el sistema global óptimo.

4.3.4.2. Características locales

Tras lo visto en la Sec. 4.3.4.1 procedemos a obtener el conjunto de características óptimo utilizando el algoritmo SFFS. Para ello volvemos a utilizar las mismas condiciones a optimizar. Obtener el menor *EER* total (suma del *EER* de los 8 casos posibles) y minimizar el *EER* para el caso crítico (*skilled-DS2-DS3*).

Los resultados obtenidos al aplicar el algoritmo SFFS con las condiciones impuestas anteriormente se representan en la Fig. 4.14. En esta figura se representa el *EER* medio, es decir, la media de los *EER* de los 8 casos posibles. En la tabla 4.5 se representan además los *EER* obtenidos para cada uno de los casos posibles cuando se selecciona el vector óptimo de 7 características, que como se aprecia en la Fig. 4.14 es el que proporciona un mejor rendimiento en el sistema y además un menor *EER* para el caso crítico *skilled-DS2-DS3*.

	<i>Skilled forgeries</i>		<i>Random forgeries</i>	
	Baseline	Vector elegido	Baseline	Vector elegido
EER_DS2_DS2	8.670 %	9.306 %	0.602 %	0.880 %
EER_DS3_DS3	17.374 %	18.080 %	0.825 %	1.520 %
EER_DS2_DS3	22.350 %	22.933 %	2.544 %	4.267 %
EER_DS3_DS2	13.533 %	15.707 %	1.872 %	2.907 %

Tabla 4.5: Características locales. Comparación de los resultados de *EER* obtenidos para el caso baseline (un vector de 8 características óptimo para cada caso) y el caso de elegir únicamente el vector de características obtenido con el algoritmo SFFS.

A la vista de los resultados, el conjunto de características obtenido con el algoritmo SFFS proporciona unos resultados de *EER* bastante cercanos al *EER* que se obtendría si se utilizase un conjunto de 8 características distinto para cada uno de los casos.

El conjunto de características locales óptimo obtenido con el algoritmo SFFS está compuesto por un total de 7 características (ver Fig. 4.14), donde tiene especial relevancia las características relacionadas con la coordenada *Y*.

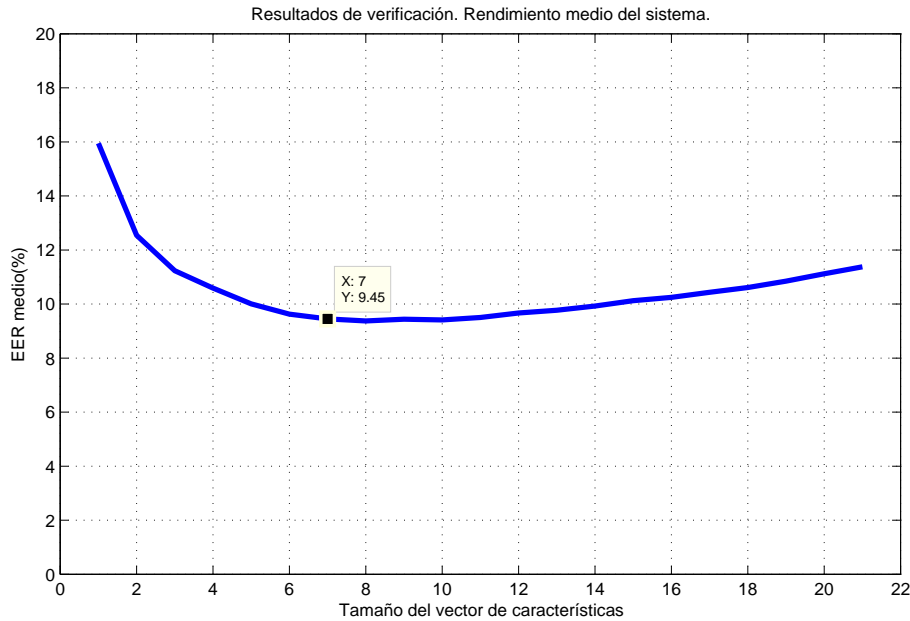


Figura 4.14: *Características locales. Rendimiento medio del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS. El punto indicado en la gráfica es el que proporciona el mejor resultado para las dos condiciones a optimizar.*

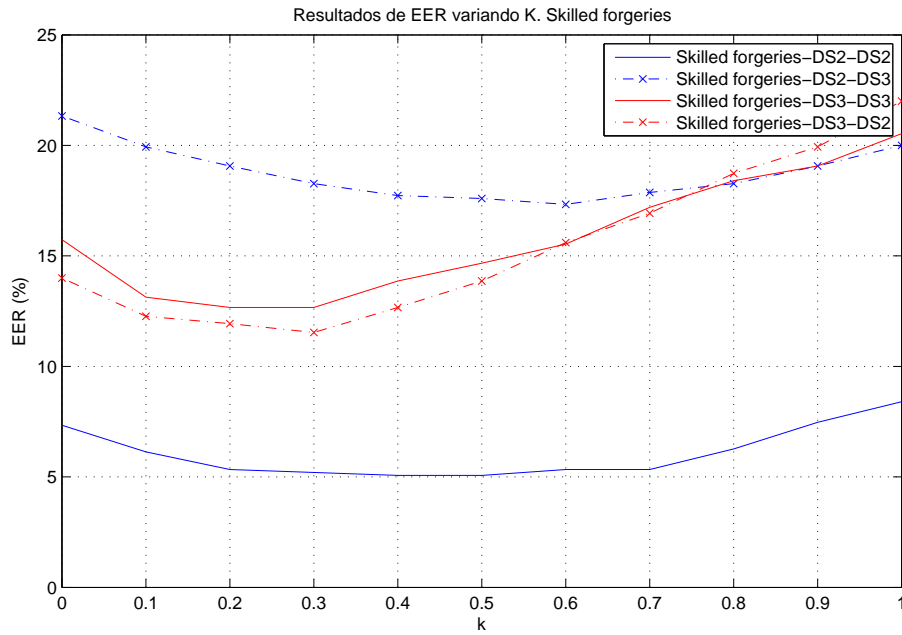
4.3.5. Fusión de los sistemas global y local

La fusión de los sistemas global y local con los vectores de características óptimos es realizado como suma de *scores* [1]. Es necesario realizar una normalización de los *scores* previamente a la fusión de los mismos. El motivo es que los *scores* obtenidos por el sistema global pueden ser de diferente orden a los obtenidos por el sistema local, además de que se consigue una mejora en el rendimiento del sistema y una mayor robustez [12]. Se realizaron pruebas con la normalización de los *scores tanh-stimulators* y con la normalización *min-max*, siendo ésta última la elegida al proporcionar mejores resultados en el rendimiento del sistema. La fusión de los *scores* es obtenida como:

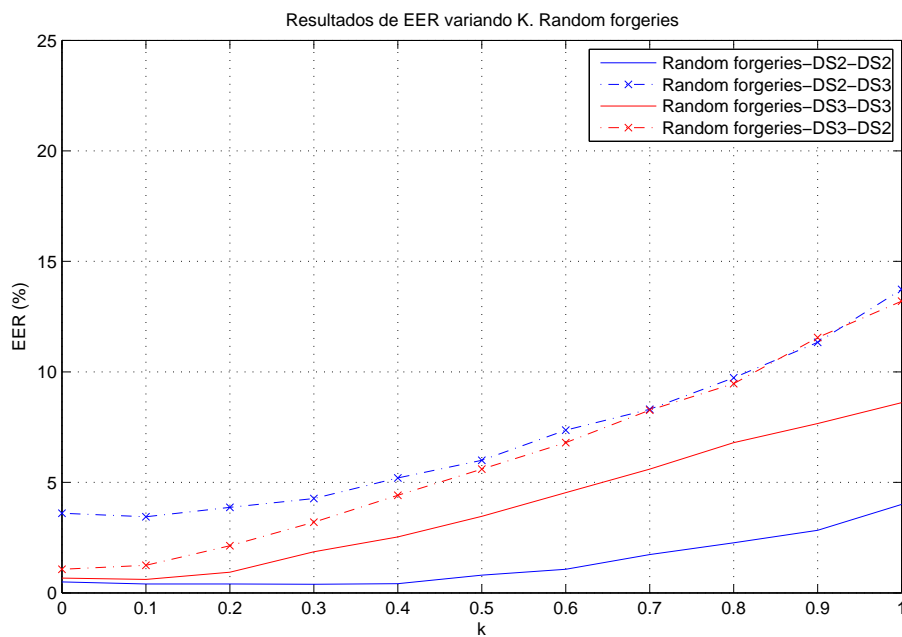
$$s_f = k \cdot s_g + (1 - k) \cdot s_l \quad (4.4)$$

donde s_f es el *score* final, s_g y s_l son los *scores* globales y locales del sistema respectivamente. El valor de la constante k se obtiene observando el rendimiento del sistema en términos de *EER* según se varía este valor de 0 a 1. Esto se representa en la figura Fig. 4.15.

A la vista de los resultados obtenidos en las figuras, la elección de elevados valores de la constante k produce una degradación del rendimiento del sistema. Esto quiere decir que el sistema tiene un mejor comportamiento cuando se da prioridad a los resultados obtenidos por el sistema local. El valor elegido de la constante k ha sido 0.3. Este valor produce el mejor *EER* para casi todos los casos *skilled forgeries*. Además se consigue un equilibrio con los valores de *EER* del caso *random forgeries*.



(a) *Skilled forgeries.*



(b) *Random forgeries.*

Figura 4.15: Evolución del EER al variar el parámetro k para la fusión de los sistemas global y local.

De esta manera la fusión de los *scores* de los sistemas global y local queda representada por la siguiente ecuación:

$$s_f = 0,3 \cdot s_g + 0,7 \cdot s_l \quad (4.5)$$

donde s_f es el *score* final, s_g y s_l son los *scores* global y local del sistema respectivamente.

	Sistema Global	Sistema Local	Fusión de sistemas
EER_skilled_DS2_DS2	8.333 %	9.306 %	5.200 %
EER_skilled_DS3_DS3	20.533 %	18.080 %	12.667 %
EER_skilled_DS2_DS3	20.000 %	22.933 %	18.267 %
EER_skilled_DS3_DS2	21.933 %	15.707 %	11.533 %

Tabla 4.6: *Resultados de EER para el sistema global, sistema local y la fusión de ambos sistemas con la fórmula propuesta 4.3.5 para el caso skilled forgeries.*

	Sistema Global	Sistema Local	Fusión de sistemas
EER_random_DS2_DS2	4.000 %	0.880 %	0.386 %
EER_random_DS3_DS3	8.609 %	1.520 %	1.859 %
EER_random_DS2_DS3	13.733 %	4.267 %	4.267 %
EER_random_DS3_DS2	13.200 %	2.907 %	3.200 %

Tabla 4.7: *Resultados de EER para el sistema global, sistema local y la fusión de ambos sistemas con la fórmula propuesta 4.3.5 para el caso random forgeries.*

En las tablas 4.6 y 4.7 se representan los resultados de *EER* obtenidos para el caso de considerar los sistemas global y local independientes y para el caso de realizar la fusión de los sistemas.

A la vista de los resultados obtenidos en la tablas, se aprecia como la fusión de los sistemas global y local por el método propuesto consigue mejorar mucho el rendimiento del sistema, especialmente en los casos *skilled forgeries*. Estos resultados han sido obtenidos utilizando el conjunto de 50 usuarios de entrenamiento.

4.4. Validación experimental

A continuación se describe el rendimiento del sistema con la fusión de los sistemas global y local sobre el conjunto de 70 usuarios de evaluación. En la Fig. 4.16 se representa por medio de las curvas *DET* dicho rendimiento para los casos *skilled forgeries* y *random forgeries*. El *EER* obtenido para cada uno de los 8 casos queda representado también en la tabla 4.8.

A la vista de los resultados, se aprecia como el tipo de dispositivo de captura utilizado para el entrenamiento y el testeo del sistema influyen en el rendimiento. De esta manera, al entrenar el sistema con un dispositivo *más fiable* (DS2, pen tablet) y utilizar para el testeo un dispositivo *menos fiable* (DS3, PDA) el rendimiento del sistema se degrada mucho. Este efecto no se agrava tanto en el caso contrario. Cabe destacar uno de los pocos estudios previos encontrados en la literatura sobre interoperabilidad de dispositivos de captura en firma [5]. Los resultados obtenidos difieren de los obtenidos en [5], donde el rendimiento del sistema se degradaba mucho menos en el caso de entrenar el sistema con el dispositivo *más fiable*.

Con el objetivo de comparar los resultados obtenidos con el sistema implementado, se ha realizado un estudio de las últimas evaluaciones realizadas en sistemas de verificación de firma manuscrita dinámica [10] [8]. Sin embargo los resultados obtenidos no se pueden comparar con estas evaluaciones, pues el protocolo de evaluación es distinto al seguido en el presente proyecto (en estas evaluaciones se utilizan un conjunto de 382 usuarios, frente a las 70 utilizados en el

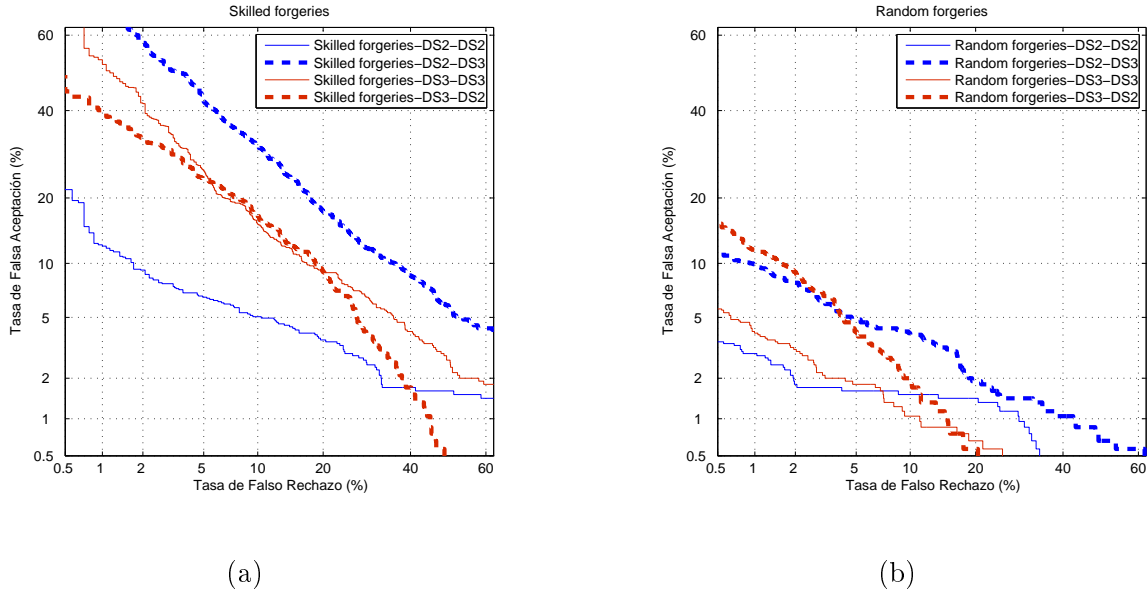


Figura 4.16: Curvas DET para los casos (a) skilled forgeries y (b) random forgeries usando fusión de sistemas para el set de 70 usuarios de evaluación.

	Skilled forgeries		Random forgeries	
	Sistema [2]	Sistema implementado	Sistema [2]	Sistema implementado
EER_DS2_DS2	7.80 %	6.191 %	5.65 %	1.988 %
EER_DS3_DS3	12.29 %	12.762 %	4.70 %	2.667 %
EER_DS2_DS3	-	18.858 %	-	4.857 %
EER_DS3_DS2	-	13.429 %	-	4.667 %

Tabla 4.8: Rendimiento del sistema sobre el conjunto de 70 usuarios de evaluación utilizando fusión de los sistemas global y local. Comparación de los resultados de EER obtenidos en [2] con el sistema implementado en el presente proyecto.

presente proyecto). Por este motivo se ha decidido comparar los resultados con los obtenidos en [2], donde se emplea el mismo protocolo de experimentación. La tabla 4.8 muestra una comparativa de los resultados obtenidos por el sistema implementado en el presente proyecto y los obtenidos en [2].

Antes de analizar los resultados obtenidos, es preciso hacer hincapié en las diferencias existentes en el sistema implementado en [2] y el sistema implementado en el presente proyecto. En primer lugar el sistema implementado en [2] no contempla el caso de interoperabilidad de sistemas. Los resultados obtenidos en [2] **contemplan la implementación de dos sistemas independientes**, uno para DS2 (pen tablet) y otro para DS3 (PDA), donde cada uno de ellos se encuentra **optimizado para el caso sin interoperabilidad**. Además hay que tener en cuenta que tanto presión como información de inclinación del bolígrafo es considerado en [2] para el caso DS2 (pen tablet). Por último indicar que en [2] se utiliza el algoritmo *HMM* en lugar de *DTW* y que la fusión de los sistemas global y local se realiza de manera diferente. En el presente proyecto, **se ha creado un sólo sistema** para todos los casos, tanto con interoperabilidad como sin ella, **optimizando las características del sistema para el caso con interoperabilidad**, pues es el caso que proporciona peor rendimiento.

A pesar de todo lo explicado anteriormente, los resultados de *EER* obtenidos en el sistema

implementado mejoran mucho los resultados obtenidos en [2], a excepción del caso *EER-skilled-DS3-DS3*, donde empeora un poco. Hay que tener en cuenta que el sistema implementado tenía como objetivo optimizar el caso con interoperabilidad. A pesar de esto se han conseguido incluso mejorar los resultados sin interoperabilidad. Esto puede ser debido a que la implementación utilizada en [2] está basada en *HMM*, mientras que en el presente proyecto se utiliza *DTW*. Otras diferencias que pueden influir en el rendimiento del sistema es la normalización de los datos de entrada, el criterio de optimización utilizado a la hora de obtener las características del sistema global y local, así como el método empleado a la hora de realizar la fusión de los sistemas.

En cuanto a la comparación de los resultados obtenidos para el caso con interoperabilidad, no se ha encontrado ningún artículo presente en el estado del arte que haya realizado pruebas de interoperabilidad utilizando las bases de datos BioSecure DS2 y DS3. A pesar de esto, los resultados obtenidos son bastante aceptables, observando relativamente poca variación al aplicar interoperabilidad, a excepción del caso *skilled-DS2-DS3*. Hay que tener en cuenta que los dispositivos de captura utilizados son muy diferentes entre sí, siendo la PDA un dispositivo poco fiable para la obtención de firmas comparado con el pen tablet.

5

Conclusiones y trabajo futuro.

5.1. Conclusiones.

El presente Proyecto Final de Carrera se ha centrado en el estudio de la interoperabilidad de los sistemas de verificación de firma manuscrita dinámica. Se ha implementado un sistema de verificación de firma dinámica haciendo uso de la fusión de los sistemas global y local. Este sistema consigue obtener un buen comportamiento tanto para el caso con interoperabilidad como sin ella. La selección de las características globales y locales del sistema se ha realizado utilizando el algoritmo *SFFS*. La condición impuesta al algoritmo para la selección de las características ha sido tomada para optimizar los casos de interoperabilidad.

Los dispositivos de captura utilizados han sido un pen tablet (DS2) y una PDA (DS3). Con el objetivo de mejorar el rendimiento del sistema al aplicar interoperabilidad, se han estudiado distintas técnicas de normalización de los datos de entrada. La normalización de las firmas por el centro de masas ha sido la que ha proporcionado mejores resultados en el sistema global. Sin embargo, ha sido la normalización por la media y la desviación típica la que ha proporcionado mejores resultados en el sistema local. Finalmente se ha visto como la fusión de los sistemas global y local mejora el rendimiento del sistema.

De los análisis y experimentos llevados a cabo durante el proyecto podemos extraer las siguientes conclusiones generales:

- Las distintas normalizaciones estudiadas han demostrado proporcionar una gran mejora en el rendimiento del sistema al aplicar interoperabilidad.
- El dispositivo de captura utilizado para el entrenamiento y el testeo influye en el rendimiento del sistema. Se ha visto como es preferible entrenar el sistema con las firmas de un dispositivo *menos fiable* y testear posteriormente con las firmas de un dispositivo con mejores prestaciones.
- El estudio realizado sobre interoperabilidad y la posterior elaboración del sistema final ha proporcionado buenos resultados. Se han mejorado incluso los resultados obtenidos en [2]

para el caso sin interoperabilidad, teniendo en cuenta que se utilizaba en dicho proyecto **dos sistemas distintos**, uno optimizado para DS2 y otro para DS3 y que en el presente proyecto se ha implementado **un único sistema**, que además está optimizado para el caso de interoperabilidad entre sistemas.

5.2. Trabajo futuro

A pesar del trabajo realizado durante el presente Proyecto Fin de Carrera, existen varios aspectos que deben ser estudiados y se proponen como diferentes líneas de trabajo futuro que pueden continuar y mejorar el estudio realizado en este proyecto:

- La realización de un estudio en mayor profundidad sobre las técnicas de normalización. Técnicas de normalización de las firmas para que tengan un mismo eje rotacional no han sido consideradas en el presente proyecto. También se puede realizar un estudio más en detalle de las técnicas de normalización de los scores [30], donde se podría conseguir una mejora considerable en el rendimiento del sistema.
- Realizar un estudio similar al realizado en el presente proyecto, pero utilizando una base de datos con dispositivos más actuales (e.g. smartphone, tablet, pen tablet) y con un mayor número de usuarios. En este tipo de dispositivos se almacena la presión, además de las coordenadas. Esto podría mejorar mucho el rendimiento del sistema, como se ha visto en algunas evaluaciones [10].
- Realizar experimentos de interoperabilidad, utilizando para el entrenamiento y el posterior testeo del sistema una base de datos con firmas mezcladas de distintos dispositivos de captura. Esto nos permitirá conocer el comportamiento del sistema en un caso mixto.

Glosario de acrónimos

- **BDD**: *Base de Datos*.
- **BMEC**: *Biosecure Multimodal Evaluation Campaign*.
- **BSEC**: *Biosecure Signature Evaluation Campaign*.
- **DET**: *Detection Error Trade-off*.
- **DTW**: *Dynamic Time Warping*.
- **EER**: *Equal Error Rate*. Tasa de error, en los sistemas de reconocimiento biométrico, en el punto de trabajo en que error de falsa aceptación y error de falso rechazo son iguales.
- **FA**: *False Acceptance*.
- **FR**: *False Rejection*.
- **FAR**: *False Acceptance Rate*.
- **FRR**: *False Rejection Rate*.
- **GMM**: *Gaussian Mixture Models*.
- **HMM**: *Hidden Markov Models*.
- **ICDAR**: *International Conference on Documents Analysis and Recognition*.
- **ROC**: *Receiver Operating Characteristic*.
- **Score**: Puntuación obtenida por un sistema de reconocimiento biométrico en la comparación entre un patrón de referencia y un rasgo biométrico de test.
- **SFFS**: *Sequential Forward Floating Search*.
- **SVC**: *Signature Verification Competition*.
- **UAM**: *Universidad Autónoma de Madrid*.
- **WACOM**: marca de dispositivos de captura específicos para la recogida de firmas.

Bibliografía

- [1] Arun A Ross, Anil K Jain, and Karthik Nandakumar. *Handbook of Multibiometrics: Human Recognition Systems*. Springer, Dordrecht, 2006.
- [2] Marcos Martinez-Diaz. Dynamic signature verification for portable devices. Master's thesis, Universidad Autonoma de Madrid, November 2008.
- [3] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14:4–20, 2004.
- [4] Anil K. Jain, Patrick Flynn, and Arun A. Ross. *Handbook of Biometrics*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.
- [5] F. Alonso-Fernandez, J. Fierrez-Aguilar, and J. Ortega-Garcia. Sensor interoperability and fusion in signature verification: A case study using tablet pc. In *Proc. IWBRIS*, volume 3781 of *LNCS*, pages 180–187. Springer, October 2005.
- [6] Arun Ross and Anil K. Jain. Biometric sensor interoperability: A case study in fingerprints. In *Proc. ECCV Workshop BioAW*, volume 3087 of *Lecture Notes in Computer Science*, pages 134–145. Springer, 2004.
- [7] F. Alonso-Fernandez, R. N. J. Veldhuis, A. M. Bazen, J. Fierrez-Aguilar, , and J. Ortega-Garcia. Sensor interoperability and fusion in fingerprint verification: A case study using minutiae- and ridge-based matchers. In *Proc. IEEE Intl. Conf. on Control, Automation, Robotics and Vision, ICARCV, Special Session on Biometrics*, pages 422–427, December 2006.
- [8] Vivian L. Blankers, C. Elisa van den Heuvel, Katrin Franke, and Louis Vuurpijl. Icdar 2009 signature verification competition. In *Proc. ICDAR*, pages 1403–1407. IEEE Computer Society, 2009.
- [9] M. Martinez-Diaz, J. Fierrez, R. P. Krish, and J. Galbally. Mobile signature verification: Feature robustness and performance comparison. *IET Biometrics*, 2014.
- [10] Nesma Houmani, Sonia Garcia-Salicetti, Bernadette Dorizzi, Jugurta Montalvão, Jânio Canuto, Marcus V. A. Andrade, Yu Qiao, Xingxing Wang, Tobias Scheidat, Andrey Makrushin, Daigo Muramatsu, Joanna Putz-Leszczynska, Michal Kudelski, Marcos Faúndez-Zanuy, Juan Manuel Pascual-Gaspar, Valentín Cardeñoso-Payo, Carlos Vivaracho-Pascual, Enrique Argones-Rúa, José Luis Alba-Castro, Alisher Kholmatov, and Berrin A. Yanikoglu. Biosecure signature evaluation campaign (esra'2011): evaluating systems on quality-based categories of skilled forgeries. In *Proc. IJCB*, pages 1–10, 2011.
- [11] Marcos Martinez-Diaz and Julian Fierrez. *Signature Databases and Evaluation*. Springer Verlag, July 2009.

- [12] Anil K. Jain, Karthik Nandakumar, and Arun Ross. Score normalization in multimodal biometric systems. *Pattern Recognition*, 2005.
- [13] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Peñalba, J. Ortega-Garcia, and D. Maltoni. An on-line signature verification system based on fusion of local and global information. In *Proc. 5th IAPR Intl. Conf. on Audio- and Video-based Biometric Person Authentication, AVBPA*, volume 3546 of *LNCS*, pages 523–532. Springer, July 2005.
- [14] M. Martinez-Diaz, J. Fierrez, and J. Ortega-Garcia. Universal background models for dynamic signature verification. In *Proc. IEEE Conference on Biometrics: Theory, Applications and Systems, BTAS*, pages 1–6, September 2007.
- [15] J. Galbally, J. Fierrez, and J. Ortega-Garcia. Bayesian hill-climbing attack and its application to signature verification. In *Proc. IAPR International Conference on Biometrics, ICB*, volume 4642 of *LNCS*, pages 386–395. Springer, August 2007.
- [16] Hiroaki Sakoe and Seibi Chiba. Dynamic programming algorithm optimization for spoken word recognition. *IEEE Transactions on Acoustics, Speech, and Signal Processing*, (1):43–49, 1978.
- [17] Alisher Kholmatov and Berrin A. Yanikoglu. Identity authentication using improved online signature verification method. *Pattern Recognition Letters*, 26(15):2400–2408, 2005.
- [18] Dit-Yan Yeung, Hong Chang, Yimin Xiong, Susan E. George, Ramanujan S. Kashi, Takashi Matsumoto, and Gerhard Rigoll. Svc2004: First international signature verification competition. In *Proc. ICBA*, volume 3072 of *Lecture Notes in Computer Science*, pages 16–22. Springer, 2004.
- [19] Julian Fierrez, Javier Ortega-Garcia, Daniel Ramos, and Joaquin Gonzalez-Rodriguez. Hmm-based on-line signature verification: feature extraction and signature modeling. *Pattern Recognition Letters*, 28(16):2325–2334, December 2007.
- [20] Daigo Muramatsu and Takashi Matsumoto. An hmm on-line signature verifier incorporating signature trajectories. In *Proc. ICDAR*, pages 438–442. IEEE Computer Society, 2003.
- [21] J. Richiardi and A. Drygajlo. Gaussian mixture models for on-line signature verification. In *Proc. ACM SIGMM Multimedia, Workshop on Biometrics methods and applications (WBMA)*, pages 115–122, Berkeley, USA, November 2003.
- [22] Sergios Theodoridis and Konstantinos Koutroumbas. *Pattern recognition*. Academic Press, 1999.
- [23] Jonas Richiardi, Hamed Ketabdar, and Andrzej Drygajlo. Local and global feature selection for on-line signature verification. In *Proc. ICDAR*, pages 625–629, 2005.
- [24] J. Galbally, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. Feature selection based on genetic algorithms for on-line signature verification. In *Proc. IEEE Workshop on Automatic Identification Advanced Technologies, AutoID*, pages 198 – 203, June 2007.
- [25] G. Degirmenci and M. Azizoglu. Branch and bound based solution algorithms for the budget constrained discrete time/cost trade-off problem. *JORS*, 64(10):1474–1484, 2013.
- [26] J. Fierrez and J. Ortega-Garcia. *Function-based on-line signature verification*, pages 225–245. Springer, 2008.

- [27] Ester Gonzalez-Sosa, Ruben Vera-Rodriguez, Julian Fierrez, and Javier Ortega-Garcia. Reconocimiento biométrico basado en la forma del cuerpo usando imágenes en la banda mmw. In *Proc. Jornadas de Reconocimiento Biométrico de Personas, JRBP*, pages 42–53, September 2013.
- [28] F. Alonso-Fernandez, J. Fierrez, D. Ramos, and J. Ortega-Garcia. Dealing with sensor interoperability in multi-biometrics: the upm experience at the biosecure multimodal evaluation 2007. In *Proc. Defense and Security Symposium, Biometric Technologies for Human Identification, BTHI*, March 2008.
- [29] M. Martinez-Diaz, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. On the effects of sampling rate and interpolation in hmm-based dynamic signature verification. In *Proc. Intl. Conf. on Document Analysis and Recognition, ICDAR*, volume 2, pages 1113–1117, September 2007.
- [30] Fernando Alonso-Fernandez, Julian Fierrez, Daniel Ramos, and Joaquin Gonzalez-Rodriguez. Quality-based conditional processing in multi-biometrics: application to sensor interoperability. *IEEE Transactions on Systems, Man and Cybernetics Part A*, 40(6):1168–1179, 2010.



Normalizaciones estudiadas. Resultados

Introducción

En este anexo se representan los resultados obtenidos en el rendimiento del sistema aplicando distintos tipos de normalizaciones de los datos de entrada. Esto se realizará tanto para el caso de las características globales como locales.

A.0.1. Características Globales.

Se ha tenido en cuenta de nuevo el vector de 100 características globales descrito en la Sec. 3.1. En las figuras Fig. A.1, Fig. A.2, Fig. A.3 y Fig. A.4 se representan la evolución del *EEER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* para cada uno de los casos.

A.0.2. Características Locales.

Se ha tenido en cuenta de nuevo el vector de 21 características locales descrito en la Sec. 4.3.1.2. En las figuras Fig. A.5, Fig. A.6, Fig. A.7 y Fig. A.8 se representan la evolución del *EEER* del sistema en función del tamaño del vector de características óptimo elegido con el algoritmo *SFFS* para cada uno de los casos.

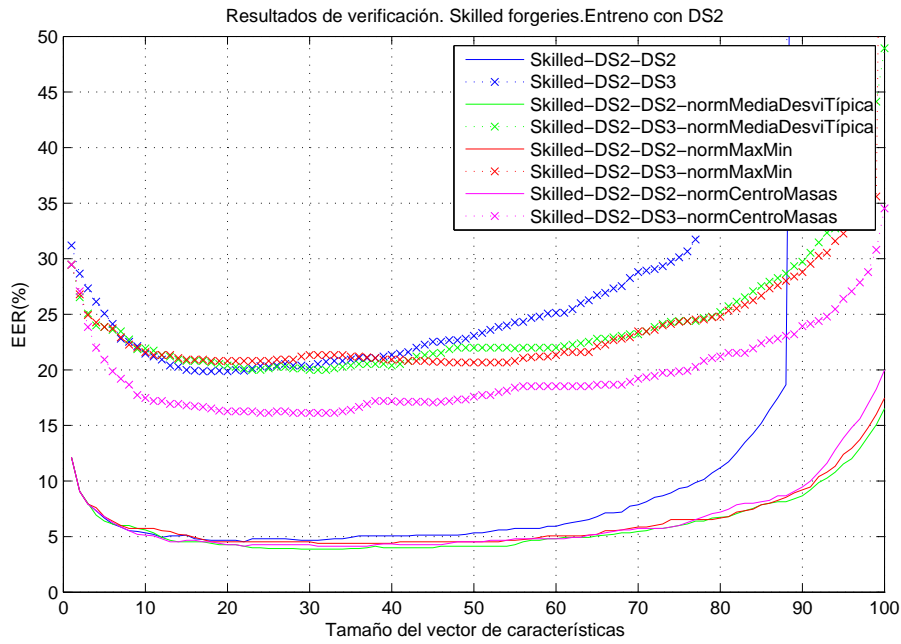


Figura A.1: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS2.

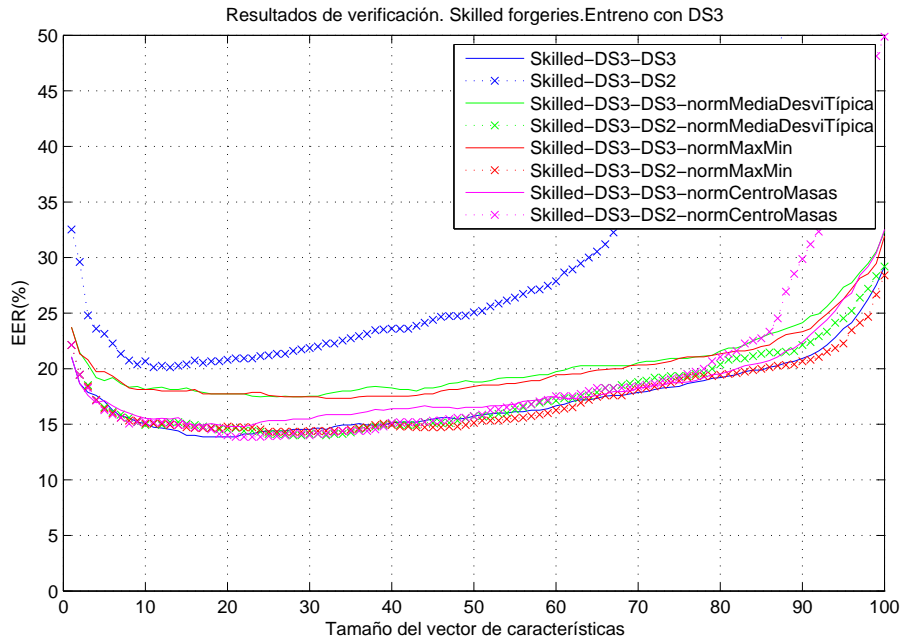


Figura A.2: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS3.

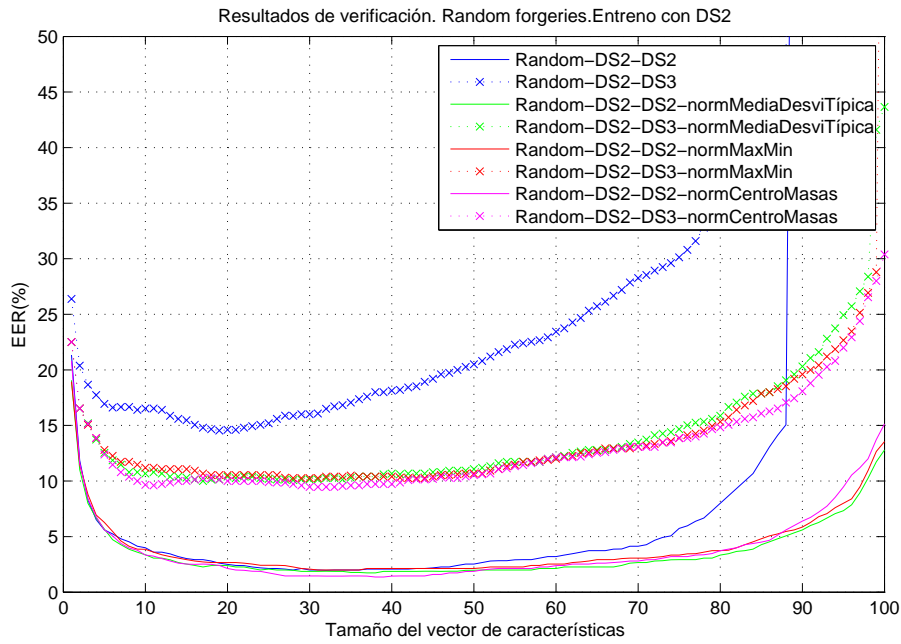


Figura A.3: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS2.

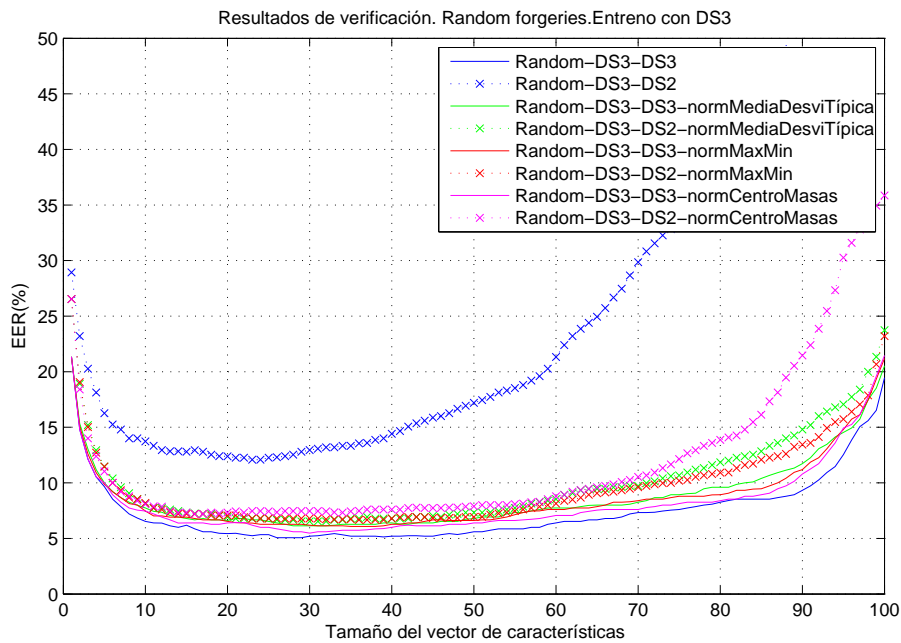


Figura A.4: Características globales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS3.

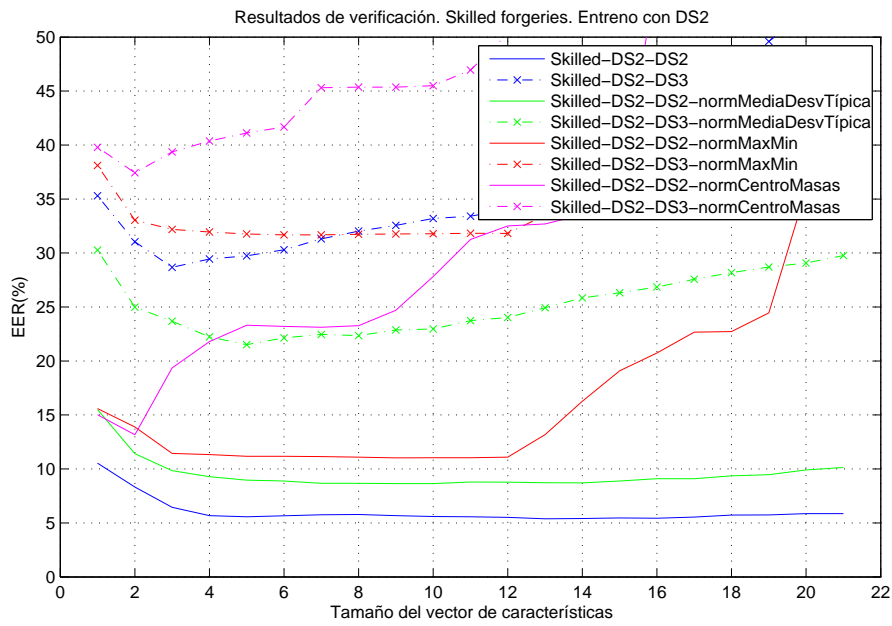


Figura A.5: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS2.

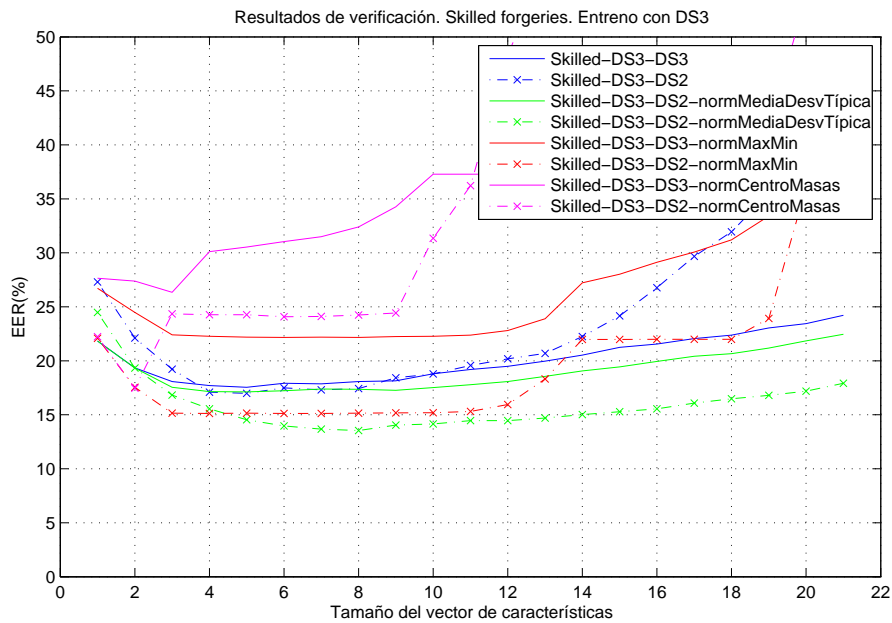


Figura A.6: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso skilled forgeries. Entrenamiento del sistema con DS3.

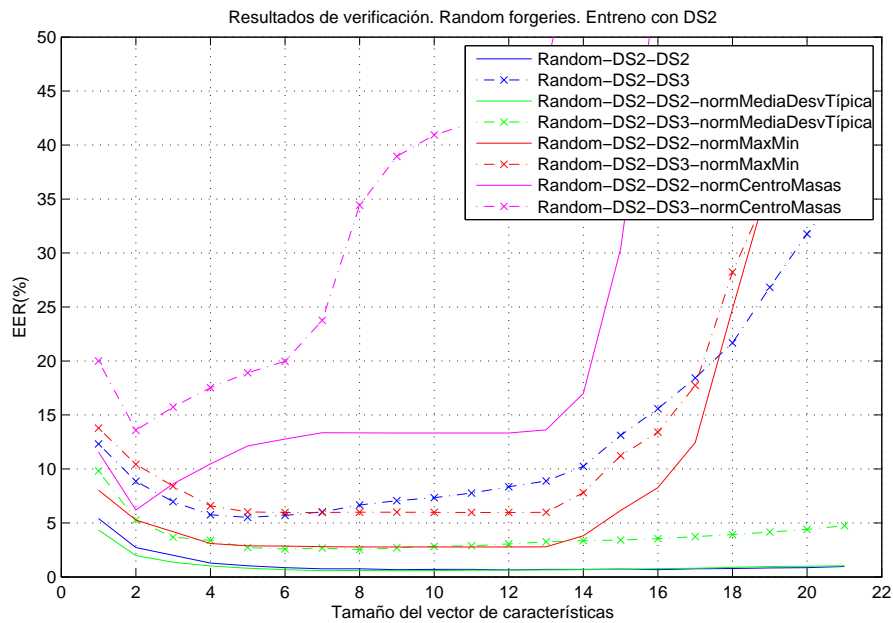


Figura A.7: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS2.

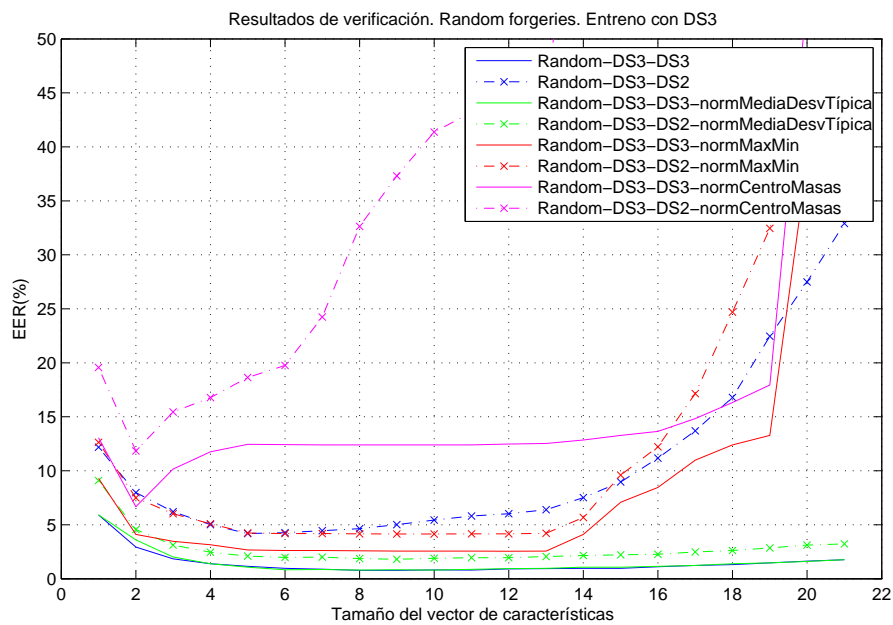


Figura A.8: Características locales. Rendimiento del sistema en términos del tamaño del vector de características óptimo obtenido con el algoritmo SFFS para el caso random forgeries. Entrenamiento del sistema con DS3.

B

Presupuesto

1) Ejecución Material	
▪ Compra de ordenador personal (Software incluido)	1000 €
▪ Material de oficina	150 €
▪ Total de ejecución material	1150 €
2) Gastos generales	
▪ sobre Ejecución Material	180 €
3) Beneficio Industrial	
▪ sobre Ejecución Material	70 €
4) Honorarios Proyecto	
▪ 800 horas a 15 €/ hora	12000 €
5) Material fungible	
▪ Gastos de impresión	100 €
▪ Encuadernación	200 €
6) Subtotal del presupuesto	
▪ Subtotal Presupuesto	14850 €
7) I.V.A. aplicable	
▪ 21 % Subtotal Presupuesto	3118,5 €

8) Total presupuesto

■ Total Presupuesto	17968,5 €
---------------------	-----------

Madrid, Octubre 2014

El Ingeniero Jefe de Proyecto

Fdo.: Rubén Tolosana Moranchel

Ingeniero de Telecomunicación



Pliego de condiciones

Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un *estudio de interoperabilidad en sistemas biométricos de firma manuscrita dinámica*. 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
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 Contrataz 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.

