Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

DISEÑO Y EVALUACIÓN DE UN SISTEMA BIOMÉTRICO BASADO EN FIRMA EN EL AIRE CON UN DISPOSITIVO MÓVIL CON ACELERÓMETRO

TRABAJO FIN DE MÁSTER

Javier Guerra Casanova

2010

Universidad Politécnica de Madrid
Escuela Técnica Superior de Ingenieros de Telecomunicación

Máster Universitario en
Ingeniería de Redes y Servicios Telemáticos

TRABAJO FIN DE MÁSTER

DISEÑO Y EVALUACIÓN DE UN SISTEMA BIOMÉTRICO BASADO EN FIRMA EN EL AIRE CON UN DISPOSITIVO MÓVIL CON UN ACELERÓMETRO

Autor
Javier Guerra Casanova

Director
Mercedes Garijo Ayestarán

Departamento de Ingeniería de Sistemas Telemáticos

2010

Resumen

Resumen

Este trabajo de investigación se centra en el diseño y la evaluación de una técnica biométrica novedosa aplicada a dispositivos móviles. Esta técnica se basa en la realización de una firma en el aire sujetando el teléfono móvil, con el único requisito de que éste disponga de un acelerómetro. A partir de dicho sensor, el sistema biométrico es capaz de extraer la información relativa a las aceleraciones en cada eje de la realización de la firma, que serán utilizadas para autenticar al usuario.

Además, se propone un método matemático fundamentado en la búsqueda del alineamiento máximo de las señales de aceleración en cada eje, mediante técnicas de programación dinámica. Así pues, este método permite analizar las distintas señales de aceleraciones para tratar de averiguar si una firma pertenece a un usuario o no.

Para evaluar la calidad del sistema biométrico propuesto, se ha obtenido una base de datos biométrica de personas realizando una firma o gesto identificativo propio en el aire, donde cada una de las sesiones han sido grabadas en vídeo. A partir de estas grabaciones, tres voluntarios han intentado imitar cada una de las firmas, obteniéndose una gran cantidad de intentos de falsificación de cada usuario original. Esta recopilación de muestras ha sido posible gracias a la implementación previa de una aplicación en un iPhone que fuera capaz de muestrear y almacenar los valores de aceleración de cada ejecución de una firma en el aire.

A partir de la base de datos de firmas en el aire y del método matemático propuesto para analizar cada una de las muestras, se han estudiado distintos escenarios de fusión multibiométrica, obteniéndose en el mejor de los casos una tasa de Equal Error Rate del 2.5 %.

Por último, se ha desarrollado un prototipo para un iPhone que integre todo lo estudiado en este trabajo de investigación. Este prototipo por sí mismo, podría constituir perfectamente el módulo de autenticación de cualquier aplicación en un móvil que desee añadir un grado de seguridad implementando esta técnica biométrica.

Abstract

Abstract

This article proposes an innovative biometric technique based on the idea of authenticating a person in a mobile device by gesture recognition. To accomplish this aim, a user is proposed to be recognized by a in-air signature he/she performs moving his/her hand while holding a mobile device with an accelerometer embedded.

As users are not able to repeat exactly a gesture in the air, an algorithm based on Dynamic Programming is proposed to correct slightly differences between different executions of the same signature.

Results of the robustness of this technique are obtained with a database of 40 original individuals, performing their identifying signatures and 3 volunteers who tried to imitate each original signature by studying their sessions recorded on video.

Different multibiometric fusion scenarios have been studied, obtaining a best result of Equal Error Rate of 2.5 %.

Moreover, a prototipe of this biometric technology has been implemented on an iPhone. This prototipe may fulfill all the requirements of an authentication module of any mobile application which desired to implement this in-air signature biometric technique.

Índice general

I Introducción y contexto **19**

1. Introducción **21**
1.1. Motivación del Trabajo 21
1.2. Marco del Trabajo Fin de Máster 22
1.3. Estructura del Trabajo Fin de Máster 22
1.4. Publicaciones derivadas de este trabajo de investigación 23

II Estado del arte **25**

2. Introducción a la biometría **27**
2.1. Métodos de identificación de personas en la actualidad 28
2.2. Conceptos básicos de biometria 29
2.3. Técnicas Biométricas 30
2.3.1. ADN 30
2.3.2. Huella Dactilar 30
2.3.3. Iris 30
2.3.4. Cara 30
2.3.5. Firma manuscrita 31
2.3.6. Manera de Andar 31
2.3.7. Otras 31
2.4. Arquitecturas y Esquemas de los Sistemas biométricos 32
2.5. Evaluación del Rendimiento de un Sistema Biométrico 34
2.6. Técnicas biométricas aplicadas en dispositivos móviles 35

3. Programación dinámica para alineamiento de secuencias **37**
3.1. Definiciones de conceptos de programación dinámica 37
3.1.1. Problemas clásicos de programación dinámica 39
3.2. Principio de Optimalidad de Bellman 40
3.2.1. Ejemplo de aplicación 40
3.3. Algoritmos de alineamiento basados en programación dinámica . 44
3.3.1. Introducción al problema de alineamiento de secuencias . 44
3.3.2. Algoritmo Longest Common Subsequences 45

3.3.3. Generalización del Algoritmo LCS como solución a cualquier problema de alineamiento global 48
3.3.4. Algoritmo de Alineamiento Local de Secuencias 49

4. Desarrollo de aplicaciones en el iPhone 51
4.1. Arquitectura Modelo Vista Controlador 51
4.2. Detalles de programación en el iPhone 53
4.2.1. Sistema de ficheros en una aplicación para el iPhone . . . 53
4.2.2. Instrucciones para desarrollar una aplicación para el iPhone 54
4.2.3. Lenguaje utilizado en aplicaciones iPhone 57
4.2.4. Descripción de funciones importantes 57

III Desarrollo 61

5. Propuesta de técnica biométrica basada en firmas en el aire. 63
5.1. Descripción de la técnica biométrica propuesta. 63
5.2. Decisiones de implementación de la técnica biométrica de firma en el aire propuesta. 65
5.2.1. Elección del dispositivo móvil 65
5.2.2. Extracción de características 66
5.2.3. Decisiones relativas a la fase de enrolamiento 67
5.2.4. Decisiones relativas a la fase de acceso 67

6. Fundamentos matemáticos del análisis de señales de firmas en el aire 69
6.1. Motivación de la utilización de un algoritmo de alineamiento para el análisis de señales biométricas de firmas en el aire 70
6.2. Algoritmo utilizado para analizar señales de aceleraciones de firmas en el aire 71
6.3. Fundamentos matemáticos de la fase de enrolamiento 73
6.4. Fundamentos matemáticos de la fase de acceso 74
6.5. Fundamentos matemáticos de fusión de información 75
6.5.1. Fusión a nivel de extracción de características 76
6.5.2. Fusión a nivel de comparación 77
6.5.3. Fusión a nivel de decisión 77

7. Obtención de una base de datos biométrica de firmas en el aire 83
7.1. Preparación de la Base de Datos 83
7.1.1. Definición de la sesión de toma de muestras originales . . 84
7.1.2. Definición de la sesión de falsificaciones 84
7.2. Características de la base de datos obtenida 85
7.3. Tipos de firmas que solían hacer los usuarios 86

8. Valoración de la técnica biométrica por el usuario final 87
8.1. Encuesta presentada a los usuarios 87
8.2. Respuestas de los usuarios a la encuesta 89
8.3. Análisis de las respuestas de los usuarios. 89
8.4. Conclusiones de la aceptabilidad de la técnica 90

9. Resultados experimentales 93
9.1. Optimizacion h y σ 93
9.2. Resultados de analizar la base de datos de firmas en el aire . . . 95
9.2.1. Experimentos con las señales de aceleración de los tres X-Y-Z 96
9.2.2. Experimentos con señales de aceleración en dos ejes (X-Y, X-Z, Y-Z) 98
9.2.3. Experimentos con una señal aceleración en un único eje (X, Y o Z). 101
9.3. Tiempo de ejecución de cada experimento 101
9.4. Análisis de los resultados 103

10. Desarrollo de una aplicación para obtener una base de datos de firmas en el aire de distintos usuarios 105
10.1. Aplicación para obtención de firmas originales 106
10.1.1. Nomenclatura de las muestras originales 108
10.2. Aplicación para obtención de firmas falsificadas 109
10.2.1. Nomenclatura de las muestras de falsificaciones 111

11. Desarrollo de un prototipo de la técnica biométrica basada en la firma en el aire para el iPhone 115
11.1. Enrolamiento en el sistema implementado en el prototipo 116
11.2. Acceso al sistema implementado en el prototipo 117

IV Conclusiones y líneas futuras 121

12. Conclusiones 123

13. Líneas futuras 125

V Bibliografía 127

Índice de figuras

2.1. Resumen de características de las técnicas biométricas más importantes 32
2.2. Bloques de un sistema biométrico completo. 33
2.3. Definición de Equal Error Rate (EER) 35

3.1. Ejemplo del problema clásico del viajero. 41
3.2. Ejemplo de obtención de la matriz de similitud de dos secuencias v y w que proporciona la subsecuencia común TCTA más larga posible 47
3.3. Ejemplo de obtención de la matriz de distancias de dos secuencias v y w que proporciona la distancia de edición. 48
3.4. Aplicación de los algoritmos de Alineamiento Global y Local para analizar dos secuencias. 50

4.1. Arquitectura "Modelo Vista Controlador" 52

6.1. Ejemplo de dos repeticiones de una misma firma realizadas por el mismo usuario. 78
6.2. Ejemplo de aplicar el algoritmo de alineamiento global modificado a dos repeticiones de la misma firma realizada por el mismo usuario. 79
6.3. Resultado del análisis completo (alineamiento + interpolación) de dos repeticiones de la misma firma realizada por el mismo usuario 80
6.4. Resultado del análisis completo (alineamiento + interpolación) de dos repeticiones de distintas firmas realizadas por usuarios diferentes. 81

9.1. Tasa de error EER obtenida (%) para una configuración de $h = 0{,}4$ y $\sigma = 0{,}225$. 95
9.2. Tasa de error EER obtenida (%) al fusionar las señales de los ejes X, Y y Z a nivel de decisión. 96
9.3. Tasa de error EER obtenida (%) al fusionar las señales de los ejes X, Y y Z a nivel de comparación. 97

9.4. Tasa de error EER obtenida (%) al concatenar las señales de los ejes X, Y y Z. 98
9.5. Tasa de error EER obtenida (%) al calcular el módulo de las señales de los ejes X, Y y Z. 99
9.6. Tasas de error EER obtenidas (%) al fusionar las señales de dos ejes a nivel de decisión. 99
9.7. Tasas de error EER obtenidas (%) al fusionar las señales de dos ejes a nivel de comparación. 100
9.8. Tasas de error EER obtenidas (%) al concatenar las señales de dos ejes. 101
9.9. Tasas de error EER obtenidas (%) al calcular el módulo de las señales de dos ejes. 102
9.10. Tasas de error EER obtenidas (%) analizando la señal de un único eje. 102

10.1. Pantallas de la aplicación de toma de muestras originales desarrollada en un iPhone 112
10.2. Pantallas de la aplicación de toma de muestras de falsificaciones desarrollada en un iPhone 113

11.1. Pantallas del enrolamiento en el prototipo de la técnica biométrica de firma en el aire implementado en un iPhone 119
11.2. Pantalla de realización de gesto de acceso 120
11.3. Pantallas de acceso al prototipo desarrollado para el iPhone según el resultado de la autenticación utilizando la técnica biométrica de firma en el aire 120

Índice de Tablas

3.1. Ejemplo de Algoritmo backward: Etapa 4 41
3.2. Ejemplo de Algoritmo backward: Etapa 3 42
3.3. Ejemplo de Algoritmo backward: Etapa 2 42
3.4. Ejemplo de Algoritmo backward: Etapa 1 42
3.5. Ejemplo de Algoritmo backward: Ruta óptima 42
3.6. Ejemplo de Algoritmo forward: Etapa 2 43
3.7. Ejemplo de Algoritmo forward: Etapa 3 43
3.8. Ejemplo de Algoritmo forward: Etapa 4 43
3.9. Ejemplo de Algoritmo forward: Etapa 5 44
3.10. Ejemplo de Algoritmo forward: Ruta óptima 44

7.1. Resumen de las características de la base de datos de firmas en el aire 85

8.1. Respuestas de la encuesta 89

9.1. Resultados de EER (%) para distintas configuraciones de h y σ. 94
9.2. Tiempo de procesamiento de dos firmas en el aire para cada escenario de fusión de información 103
9.3. Resumen de los resultados de EER y tiempos de procesamiento de los escenarios de fusión estudiados. 104

Parte I

Introducción y contexto

Capítulo 1

Introducción

En este Capítulo de Introducción se presentarán los objetivos principales y motivaciones que han llevado a la realización de este trabajo de investigación. Además, se ofrecerá una visión del contexto en el que se ha llevado a cabo este trabajo, puesto que está enmarcado en un Proyecto nacional mucho más grande. A continuación, se explicará la estructura que se va a seguir en la presentación de este documento, dividida en cinco partes diferenciadas para facilitar la comprensión del lector. Por último, se presentarán las publicaciones aceptadas en congresos nacionales e internacionales que han sido derivadas de este trabajo de investigación, cuyos resultados han sido considerados interesantes por la comunidad investigadora internacional.

1.1. Motivación del Trabajo

Este trabajo trata de profundizar en el ámbito de la seguridad biométrica en dispositivos móviles. Hoy en día, los teléfonos móviles se han convertido en pequeños ordenadores, desde los cuales pueden realizarse multitud de operaciones que pueden necesitar una comprobación de la identidad del usuario. Esta evolución de las prestaciones de los teléfonos no ha ido acompañada, sin embargo, de una mejora en la seguridad de los mismos, manteniendo de momento el control de acceso basado en código PIN como principal opción de seguridad, con todas sus limitaciones.

Como consecuencia de esta premisa, nace este trabajo de investigación, donde se trata de profundizar y proponer una nueva técnica biométrica de autenticación en los dispositivos móviles, que ayude a mejorar la seguridad en la utilización de los mismos, de una manera sencilla y adaptada al entorno móvil.

Por tanto, este trabajo de investigación está enmarcado en el ámbito de la seguridad en dispositivos móviles, más concretamente en la utilización de técnicas biométricas en un teléfono móvil.

Esta investigación se presenta como el Trabajo Fin de Máster del Programa de Postgrado de la Universidad Politécnica de Madrid denominado: “Máster

Universitario en Ingeniería de Redes y Servicios Telemáticos", donde la asignatura de "Seguridad en Redes de Telecomunicación" ha sido de especial interés, puesto que en ella se exponen muchos conceptos generales de biometría y técnicas de control de acceso útiles para este trabajo.

Este trabajo ha sido tutorizado por D.ª Carmen Sánchez Ávila y revisado por D.ª Mercedes Garijo Ayestarán, ambas profesoras titulares de la Universidad Politécnica de Madrid.

1.2. Marco del Trabajo Fin de Máster

Este trabajo se ha desarrollado en el marco de un proyecto Cenit denominado: "Proyecto Segur@: Seguridad y Confianza en la Sociedad de la Información", liderado por Telefónica I+D y financiado por el Centro para el Desarrollo Tecnológico Industrial (CDTI), organismo dependiente del Ministerio de Industria, Turismo y Comercio.

Dentro de este trabajo, y desde el Grupo de Biometría y Tratamiento Numérico de la Información de la Universidad Politécnica de Madrid, se han desarrollado durante 3 años varias tareas, siendo una de ellas la correspondiente a este trabajo de investigación.

1.3. Estructura del Trabajo Fin de Máster

La memoria de este trabajo de investigación se ha dividido en cinco partes diferenciadas, tal y como se proponía en los requisitos del mismo:

- En la primera parte del Trabajo, correspondiente a este Capítulo se ha introducido la motivación, los principales objetivos y el marco en el que se encuadra el trabajo realizado.

- La segunda parte del trabajo presenta el estudio del estado del arte de la tecnología utilizada en el desarrollo del trabajo. En el Capítulo 2 se presenta una introducción general al campo de la biometría, donde el trabajo de investigación trata de aportar una nueva técnica biométrica adaptada a dispositivos móviles. En el Capítulo 3 se presenta la teoría de las técnicas matemáticas de programación dinámica y alineamiento de señales en las que se basa el algoritmo desarrollado para analizar las señales en este trabajo. Por último, el Capítulo 4 presenta una serie de conceptos teóricos necesarios para ser capaces de programar aplicaciones en un iPhone, puesto que es el teléfono móvil donde se implementará un prototipo final del sistema que permita verificar la validez de la técnica biométrica propuesta.

- La tercera parte del trabajo muestra el desarrollo que se ha realizado, dividido en distintos Capítulos. En particular, el Capítulo 5 describe la técnica biométrica basada en firmas en el aire que se propone en este trabajo y su

manera de utilización. Además, el Capítulo 6 explica el método matemático que se propone para analizar las señales de dicha técnica biométrica. El resto de Capítulos tratan de verificar la validez de esta técnica biométrica analizada con el algoritmo propuesto. Para ello, ha sido necesario recabar una base de datos biométrica, explicada en el Capítulo 7, con la que poder probar el sistema. Por otro lado, se ha realizado un estudio de la valoración de los usuarios finales que han realizado sus firmas en el aire con un dispositivo móvil y cuyos resultados se presentan en el Capítulo 8. Una vez explicados todos los elementos necesarios para realizar los experimentos que validen la fiabilidad de la técnica, se presentan los resultados de los mismos, en el Capítulo 9. Finalmente, el Capítulo 10 presenta las aplicaciones desarrolladas e implementadas en un iPhone que se han utilizado para la obtención de firmas en el aire para la base de datos, mientras que el Capítulo 11 muestra una aplicación prototipo final del sistema.

- El estudio de la tecnología y el desarrollo implementado derivará en una serie de conclusiones que se presentarán en la cuarta parte en el Capítulo 12. Asimismo, el Capítulo 13 mostrará las líneas de trabajo futuro en las que se puede seguir investigando y profundizando para la mejora de los resultados de esta técnica biométrica.

- Por último, el trabajo finalizará con la parte de referencias, donde se presentará la bibliografía consultada y utilizada para la realización de este trabajo.

1.4. Publicaciones derivadas de este trabajo de investigación

Como fruto del trabajo presentado en este documento, han sido aceptados tres artículos con diversas partes de la investigación en distintos congresos nacionales e internacionales.

En particular, en el momento de la presentación de este trabajo, han sido aceptados los siguientes artículos:

- Javier Guerra Casanova, Carmen Sánchez-Ávila, Alberto de Santos Sierra, Gonzalo Bailador del Pozo, Vicente Jara Vera. *"A real-time in-air signature biometric technique using a mobile device embedding an accelerometer"*. Aceptado en el congreso internacional Network Digital Technologies, en la sesión especial "Real Time Biometric Solutions for Networked Society". Praga, Julio de 2010. Pendiente de publicar en "Communications in Computer and Information Science" (CCIS) of Springer Lecture Notes Series (ISSN: 1865-0929)

- Javier Guerra Casanova, Carmen Sánchez-Ávila, Alberto de Santos Sierra, Gonzalo Bailador del Pozo, Vicente Jara Vera. *"Acceleration axis selection in biometric technique based on gesture recognition"*. Aceptado en

el congreso internacional del IEEE "The Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing". Darmstadt, Octubre de 2010. Pendiente de publicar en los Proceedings del congreso.

- Javier Guerra Casanova, Carmen Sánchez-Ávila, Alberto de Santos Sierra, Gonzalo Bailador del Pozo, Vicente Jara Vera. *"Modelo criptobiométrico de liberación de clave basado en firmas en el aire"*. Aceptado en la IX Reunión Española sobre Criptología y Seguridad de la Información. Tarragona, Septiembre de 2010. Pendiente de publicar en los Proceedings del congreso.

Además, se han preparado y están en proceso de revisión dos artículos en revistas internacionales incluidas en el JCR.

Parte II

Estado del arte

Capítulo 2

Introducción a la biometría

Este capítulo trata de presentar conceptos fundamentales del mundo de la biométrica que serán utilizados a lo largo de este trabajo.

Para comenzar, en la Sección 2.1 se muestra una visión de los métodos de identificación históricamente más utilizados, que motivan el nacimiento de las técnicas biométricas para ofrecer un paso más de seguridad a las técnicas de identificación tradicionales.

A continuación, la Sección 2.2 presenta varios conceptos básicos de biometría: la clasificación de técnicas biométricas según su origen y los requisitos que debe tener una técnica biométrica. A lo largo del trabajo se hará referencia constante a estos requisitos, buscando optimizar la mayor parte de ellos.

En la Sección 2.3 se presenta un breve estado del arte de las técnicas biométricas más importantes en la actualidad. Sin entrar en grandes detalles, se ofrece una visión panorámica de qué se está haciendo y hacia donde va el mundo de la biometría.

La Sección 2.4 ofrece un punto más de detalle en el mundo de la biometría, explicando el esquema general de las distintas partes que forman cualquier sistema biométrico concreto en cualquier técnica biométrica de reconocimiento. Estas partes serán implementadas en el sistema que se ha desarrollado en este trabajo, por lo que es de vital importancia tener una idea clara de cómo se divide una aplicación biométrica, y por tanto, los bloques de los que ha de consistir.

Otro aspecto muy importante de la biometría es valorar lo bueno que es un sistema. Para ello, se ha incluido la Sección 2.5 donde se muestran las medidas de fiabilidad típicas de los sistemas biométricos. De hecho, estas medidas serán las utilizadas para evaluar el rendimiento del sistema presentado en este trabajo.

Por último, debido a que la técnica biométrica que se propone en este trabajo de investigación hace referencia al entorno de los dispositivos móviles, en la Sección 2.6 se presentará un estado del arte de otros trabajos que se están llevando a cabo en la actualidad para llevar la biometría a los teléfonos móviles.

2.1. Métodos de identificación de personas en la actualidad

La aparición, desarrollo y proliferación de equipos electrónicos en nuestra sociedad, tales como ordenadores personales, cajeros automáticos, teléfonos móviles, redes de acceso seguro, etc. ha provocado la necesidad de desarrollar nuevos sistemas de identificación personal para evitar el uso fraudulento de dicha tecnología.

Una gran variedad de aplicaciones requieren sistemas de reconocimiento personal para determinar o confirmar la identidad del individuo que solicita sus servicios. El objetivo de los mismos es asegurar que únicamente se da servicio a usuarios autorizados. En ausencia de sistemas de reconocimiento personal fiables, dichos equipos serían vulnerables al acceso a sus servicios de usuarios no legítimos, con las consecuencias que esto conllevaría.

Hoy en día es necesario que nuestras actividades tengan un alto grado de seguridad, es decir, que la probabilidad de fraude sea prácticamente nula.

En la actualidad existen tres modelos de identificación personal generales:

- Primer Nivel: Identificación en base a algo que se tiene: Por ejemplo, una llave, una tarjeta, una credencial con una fotografía, etc.

- Segundo Nivel: Identificación en base a algo que se sabe: Una contraseña, una clave, un número de acceso, etc. Éste es el método tradicional más comúnmente utilizado por su sencillez y flexibilidad.

- Tercer nivel: Identificación en base a lo que se es o algo que se hace. Es la denominada tecnología biométrica.

En lo que se refiere al modelo de identificación del primer nivel, tienen especial importancia las tarjetas. Una propuesta de identificación se basa en la utilización de las denominadas “Tarjetas Inteligentes”. Estas tarjetas son capaces de crear firmas digitales únicas mediante un chip que incluyen en su interior. Así pues, la identificación se basa en la posesión de la tarjeta, lo cual implica una gran vulnerabilidad, puesto que la tarjeta se puede duplicar, robar o perder.

El segundo nivel consiste en decidir si el usuario es quien dice ser en base a una prueba de conocimiento que, en principio, sólo el usuario podría superar (una clave). Estos tipos de sistemas son los más baratos, pero a su vez los más vulnerables a ataques, puesto que estas claves se pueden adivinar, olvidar o copiar.

El tercer nivel ofrece un grado de seguridad mayor, puesto que se propone identificar a un usuario donde la “llave” del sistema es él mismo. Se trata de una tecnología que mide características físicas y biológicas que son únicas e inimitables por otros usuarios, proporcionando un sistema de seguridad a priori más robusto debido a que las características biométricas, en teoría, no se pueden duplicar, robar, perder, adivinar, olvidar ni copiar.

2.2. Conceptos básicos de biometria

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

En biometría existen dos grandes familias de técnicas de reconocimiento de personas, según el tipo de característica que se utilice para su identificación:

- Técnicas fisiológicas: Están basadas en una característica física de la persona, suficientemente distintiva e intrasferible. Por ejemplo, la huella dactilar, el iris, la mano, la cara, etc.
- Técnicas de comportamiento: Se basan en cómo el usuario realiza una acción, de manera unívoca. Ejemplos de estas técnicas son el reconocimiento según la manera de andar, la manera de teclear, la firma, etc.

En general, las técnicas fisiológicas aportan un mayor grado de seguridad, puesto que ofrecen características físicas que permanencen invariantes en distintos momentos. En cambio, las técnicas de comportamiento proporcionan datos que dependen de la manera en la que el usuario lo realiza, existiendo una mayor variabilidad entre las muestras del propio usuario (Ejemplo: Una persona nunca realiza su firma dos veces igual, pero el iris de la persona es siempre el mismo)

Además, existen algunas técnicas híbridas, que contienen propiedades comunes a las técnicas fisiológicas y de comportamiento, como por ejemplo las técnicas basadas en el reconocimiento de voz. En esta técnica en particular, la identificación de un usuario depende de características físicas que producen un timbre de voz único y propio del usuario (la disposición de las cuerdas vocales, la forma de la boca, el tamaño de los labios, etc.), así como de características de comportamiento (manera de pronunciar ciertos sonidos, rapidez y tono en el habla, estado anímico en el que se encuentra, etc.).

Los requisitos básicos que deben reunir las características biométricas son [10]:

- Universalidad: Toda persona debe poseer dicha característica.
- Singularidad o univocidad: La característica ha de ser suficientemente distintiva para diferenciar a dos personas distintas.
- Permanencia: La característica ha de ser invariable en el tiempo y en distintas condiciones externas (ambientales, iluminación, etc.)
- Colectividad: Es necesario que la característica se pueda medir.
- Rendimiento o actuación: La característica ha de ofrecer un alto nivel de exactitud a la hora de identificar a personas.
- Aceptabilidad: Las persona han de estar dispuestas a aceptar el uso de la técnica biométrica en la vida diaria del usuario, para ello, la extracción de la característica ha de realizarse de una manera poco intrusiva.

- Fiabilidad o Resistencia a fraude: La característica biométrica no ha de poderse copiar o imitar.

2.3. Técnicas Biométricas

En la actualidad, existen una gran cantidad de técnicas, desarrolladas y en fase de investigación, para identificar a las personas. Cada una de ellas se basa en una característica, física o de comportamiento, que tiene sus fortalezas y debilidades, siendo la elección óptima dependiendo de la aplicación en particular que se quiere proteger.

En esta Sección, se presentan algunas de las técnicas biométricas más comunes:

2.3.1. ADN

El ADN es un código unidimensional único para cada individuo (excepto gemelos). Es una técnica con alto grado de precisión, de hecho, es el rasgo biométrico más utilizado en aplicaciones forenses [8]. Los principales inconvenientes son que es un proceso lento (requiere un estudio químico) y poco aceptado por el usuario (a las personas no les gusta que su ADN se extraiga y estudie).

2.3.2. Huella Dactilar

La huella dactilar proporciona un patrón de surcos y valles en la superficie de la yema de los dedos único para cada usuario [13]. Se forma en los primeros siete meses del embarazo y permanece invariante toda la vida. Además, son diferentes para cada gemelos e incluso para cada dedo de la persona. Es un método muy extendido en la actualidad, debido a su gran seguridad y el bajo precio de los sensores necesarios. Por otro lado, existe una pequeña fracción de la población que no puede hacer uso de este sistema de identificación por motivos como avanzada edad, cortes en los dedos o desgastes propios de trabajadores manuales.

2.3.3. Iris

El iris es la región ocular, única y distintiva (incluso entre los ojos de una misma persona) comprendida entre la pupila y el cristalino. La textura y la forma del iris se forma en la etapa fetal y se estabiliza en los dos primeros años de vida, para permanecer igual el resto de la vida del individuo. Es la técnica biométrica con menores tasas de error existente en la actualidad, aunque los sistemas de detección de iris son caros [5].

2.3.4. Cara

El reconocimiento facial es un método no intrusivo, y probablemente el más natural de los humanos. La forma más común de diferenciar una cara es localizar,

situar y reconocer los atributos que la definen, es decir, ojos, nariz, labios, barbilla, etc. Los sistemas basados en este rasgo tienen dificultades relacionadas con las distintas condiciones en la obtención de la imagen (iluminación, pose, etc.) así como en la variación con el tiempo de la misma [12].

2.3.5. Firma manuscrita

La forma en la que una persona firma con su nombre es característica de cada individuo. La firma es un rasgo biométrico basado en la conducta del usuario, por lo que puede cambiar con el paso del tiempo, y está influenciada por las condiciones físicas y emocionales del individuo. Es un método comúnmente utilizado y muy extendido en cualquier tipo de ámbito de seguridad, aunque tiene un bajo nivel de fiabilidad por su facilidad de copia [25].

2.3.6. Manera de Andar

Es una característica biométrica basada en los movimientos espacio temporales de cada persona. Es una técnica muy poco intrunsiva, ya que sólo es necesaria una cámara que grabe a los usuarios andando. Es un rasgo que puede variar a lo largo del tiempo, debido a factores como el peso corporal, lesiones, edad, etc. Se utiliza para aplicaciones de baja seguridad puesto que no es suficientemente distintiva [22].

2.3.7. Otras

Otras técnicas biométricas para el reconocimiento de personas utilizadas en la actualidad son:

- Geometría de la mano
- Venas de la mano
- Retina
- Oído
- Voz
- Dinámica de tecleo
- Olor
- Termogramas

Como resumen de estas técnicas se presenta la Tabla de la Figura 2.1, donde puede observarse en qué medida cumple cada característica biométrica cada uno de los requisitos presentados anteriormente.

Tecnología	Universalidad	Univocidad	Permanencia	Colectividad	Actuación	Aceptación	Fraude
Rostro	Alta	Baja	Media	Alta	Baja	Alta	Baja
Huella Dactilar	Media	Alta	Alta	Media	Alta	Media	Alta
Geometría de la mano	Media	Media	Media	Alta	Media	Media	Media
Tecleo	Baja	Baja	Baja	Media	Baja	Media	Media
Venas de la mano	Media	Media	Media	Media	Media	Media	Alta
Iris	Alta	Alta	Alta	Media	Alta	Baja	Alta
Retina	Alta	Alta	Media	Baja	Alta	Baja	Alta
Firma	Baja	Baja	Baja	Alta	Baja	Alta	Baja
Voz	Media	Baja	Baja	Media	Baja	Alta	Baja
Termogramas	Alta	Alta	Baja	Alta	Media	Alta	Alta
Olor	Alta	Alta	Alta	Baja	Baja	Media	Baja
ADN	Alta	Alta	Alta	Baja	Alta	Baja	Baja
Modo de andar	Media	Baja	Baja	Alta	Baja	Alta	Media
Oído	Media	Media	Alta	Media	Media	Alta	Media

Figura 2.1: Resumen de características de las técnicas biométricas más importantes

2.4. Arquitecturas y Esquemas de los Sistemas biométricos

Los sistemas biométricos pueden utilizarse en base a dos esquemas de funcionamiento para acceder a un sistema protegido:

- Reconocimiento o identificación: (¿Quién es?) Se compara la muestra del individuo que trata de acceder al sistema con todos los patrones de los usuarios que se conocen, tratando de averiguar quién es.
- Autenticación o verificación: (¿Es quién dice ser?) La muestra del individuo que trata de acceder al sistema se compara con la del patrón del usuario que reclama su identidad.

Para cualquiera de estos esquemas, el funcionamiento del mismo puede dividirse en dos grandes fases, la fase de enrolamiento y la fase de acceso.

En la fase de enrolamiento, el sistema tiene que aprender quién es el usuario. Para ello, toma distintas muestras de la característica biométrica que utilice el sistema, y a partir de ellas calcula y almacena un patrón que irá ligado a la identidad del usuario. Una vez que el usuario ya esté enrolado en el sistema, podrá acceder al mismo cuando lo necesite.

En la fase de acceso, el sistema extraerá una muestra de la característica biométrica del usuario, y la comparará con el patrón que tiene almacenado. A partir de dicha comparación, el sistema decidirá de manera automática sobre la identidad del usuario que trata de acceder. Este esquema puede observarse en la Figura 2.2.

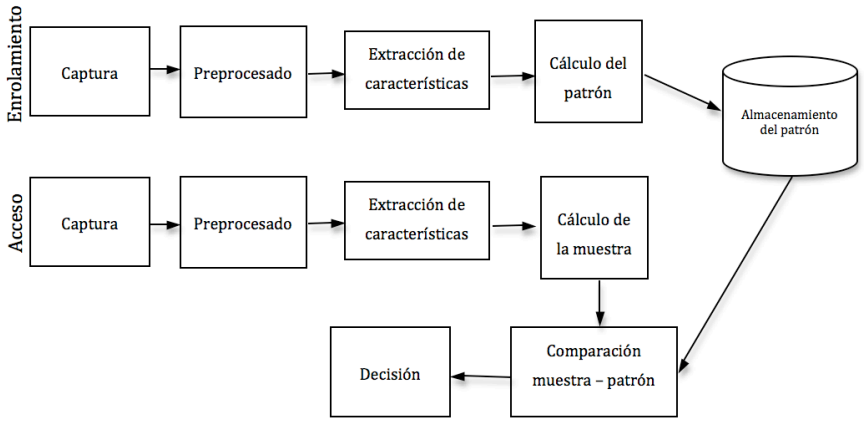


Figura 2.2: Bloques de un sistema biométrico completo.

Los distintos bloques de la Figura 2.2 tienen las siguientes características:

- Captura: El sistema toma una muestra de las características biométricas deseadas. Para ello, es necesario un dispositivo con un sensor que recoja los datos biométricos. Por ejemplo, una huella digital puede obtenerse a partir de cámaras de vídeo, cámaras de fotos, ultrasonidos, láser, tinta, etc. Esta etapa debe hacerse de la misma manera para la fase de enrolamiento y de acceso, para que las muestras sean de las mismas características.

- Preprocesado y control de calidad: Las técnicas de preprocesado permiten mejorar la calidad con la que se han obtenido las muestras o seleccionar las zonas donde reside el patrón biométrico, de cara a que la siguiente etapa de extracción de características pueda recoger los datos de manera más precisa y distintiva del usuario. Por ejemplo pueden utilizarse filtros, canceladores de ruido, técnicas de segmentación, etc. Además, en esta fase, es necesario asegurar la calidad de la toma de muestras, solicitando una nueva muestra al usuario si no se ha capturado de manera correcta (por ejemplo, en una captura de iris el usuario tenía el ojo cerrado). De nuevo, esta etapa ha de efectuarse de la misma manera para la fase de enrolamiento y de acceso, para que el patrón y las muestras de acceso tengan las mismas características.

- Extracción de características y cálculo del patrón. En este bloque se procesa la información obtenida de cada individuo, que se encuentra en la zona seleccionada durante el preprocesado, calculando el patrón biométrico necesario para comparar las identidades de los usuarios.

- Almacenamiento del patrón. El patrón biométrico ha de ser almacenado de manera segura, puesto que en los siguientes accesos del usuario, será ne-

cesario realizar una comparación contra él para comprobar la veracidad de la identidad del usuario.

- Extracción de características y cálculo de la muestra. En la fase de acceso, de una manera similar a la anterior se calcula la muestra del usuario que se comparará con el patrón biométrico almacenado. La extracción de características ha de realizarse de la misma manera en cada una de las fases.

- Etapa de Comparación: En esta etapa se contrasta el patrón biométrico almacenado en la fase de reclutamiento del individuo con la muestra obtenida del intento de acceso del usuario. El resultado de dicha comparación no es atómico (1 ó 0), sino que expresa un grado de igualdad, una probabilidad de semejanza, ya que las muestras de un mismo individuo siempre presentan algunas variaciones.

- Etapa de Decisión: En este bloque hay que situar un umbral de decisión, que defina un grado de semejanza mínimo para asegurar que la muestra de acceso se parece mucho al patrón almacenado, y por tanto pertenece al individuo asociado. Un umbral muy alto provocará que en ciertas ocasiones, la persona original no pueda acceder al sistema (Falso Rechazo), mientras que un umbral muy bajo, implicará que usuarios distintos puedan hacerse pasar por otros usuarios (Falsa Aceptación).

2.5. Evaluación del Rendimiento de un Sistema Biométrico

El rendimiento de una técnica biométrica se analiza empleando comúnmente dos tasas de error:

- Tasa de Falsa Aceptación (FAR: False Acceptance Rate), que mide el porcentaje de error de aceptar a un intruso como usuario del sistema.

- Tasa de Falso Rechazo (FRR: False Rejection Rate), que expresa la probabilidad de que el sistema rechace a un usuario legítimo del sistema.

Como se explicó anteriormente, la elección del umbral de la etapa de decisión condiciona los valores de la FAR y la FRR del sistema, y vendrá dada por los requisitos de seguridad y las condiciones de funcionamiento con las que se quiera dotar al sistema. Es decir, en entornos en los que se requiera un alto grado de seguridad, es necesario fijar un umbral alto, con el objetivo de que no acceda a las aplicaciones protegidas un usuario no autorizado. Por otro lado, cuando las condiciones de seguridad no sean tan estrictas, podremos fijar un valor del umbral más bajo, generando posibles fallos de seguridad al haber mayor probabilidad de dar acceso a personal no autorizado.

Debido a estas fluctuaciones en función del umbral se ha definido otro parámetro: Tasa de Igual Error (EER: Equal Error Rate), correspondiente al punto

donde se cruzan las curvas de la FAR y la FRR (Ver Figura 2.3). En general, se utiliza este parámetro como medida del rendimiento de los sistemas biométricos, puesto que eligiendo el valor del umbral correspondiente al punto EER, se consigue minimizar el error total del sistema y un compromiso entre las dos tasas de error existentes.

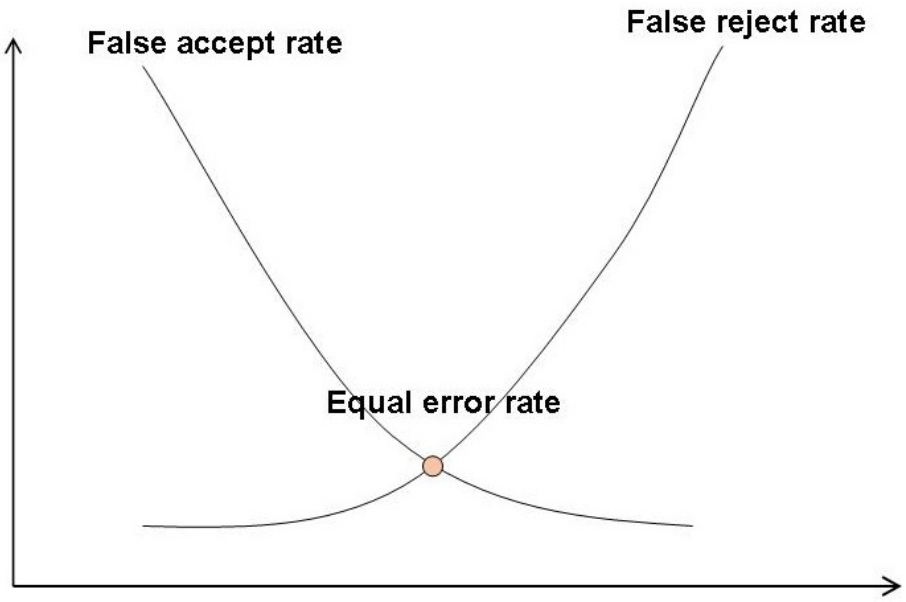


Figura 2.3: Definición de Equal Error Rate (EER)

La técnica biométrica más robusta en la actualidad es la basada en el iris, obteniendo unas tasas de EER menores del 0.01 % [5].

2.6. Técnicas biométricas aplicadas en dispositivos móviles

Hoy en día se puede acceder a aplicaciones en Internet que pueden necesitar autenticación desde la mayoría de dispositivos móviles. Mirar el saldo de una cuenta corriente, comprar un producto en una tienda online o realizar ciertas operaciones en sitios web seguros son sólo algunos ejemplos de operaciones que se pueden realizar desde un móvil con acceso a Internet y donde es importante que el usuario sea quien dice ser.

En este contexto móvil, la seguridad suele dejarse en manos de contraseñas o códigos PIN que se supone que sólo el usuario sabe. Pero, tal y como se ha comentado anteriormente, esto esconde un gran riesgo ya que las contraseñas pueden ser robadas o adivinadas comprometiendo la seguridad del sistema.

La utilización de técnicas biométricas permite solucionar estos problemas. Por un lado, el usuario no puede olvidarse de su clave, puesto que él mismo es la clave. Por otro lado, si la técnica biométrica es suficientemente distintiva, ningún usuario va a poder autenticarse en el sistema como si fuera otro, manteniendo la clave del usuario original completamente segura.

En la actualidad existen varias investigaciones que tratan de unir las técnicas clásicas de biometría en escenarios móviles, aunque hoy en día su utilización no está muy extendida. Algunas de estas líneas de trabajo son las siguientes:

- Reconocimiento de iris mediante cámaras en teléfonos móviles [7], [19], [14].
- Reconocimiento facial a través de las cámaras de los teléfonos móviles [34], [38].
- Reconocimiento por voz al hablar por teléfono [31], [20].
- Reconocimiento de la persona por la forma de andar llevando un teléfono móvil que integre un acelerómetro en el bolsillo [1], [9].
- Reconocimiento del usuario legítimo del dispositivo móvil mediante dinámica de tecleo y presión de las teclas [30].

Como puede observarse a partir del listado de técnicas biométricas anteriores, se tiende a utilizar características identificativas del usuario que puedan ser fácilmente extraíbles con sensores ya incluidos en el propio teléfono móvil, como cámaras, micrófonos, teclas o acelerómetros.

La técnica propuesta en este trabajo veremos que va en esa línea, puesto que se propone una técnica biométrica basada en la realización de la firma en el aire sujetando un teléfono móvil, donde las características de la firma son extraídas a partir de un acelerómetro ya integrado en el propio teléfono. Esta restricción no es problema, debido a que hoy en día, el número de teléfonos móviles con acelerómetros es muy amplio [33], incluyéndose más y más este sensor en los modelos que salen al mercado.

Capítulo 3

Programación dinámica para alineamiento de secuencias

La programación dinámica es una técnica muy utilizada para la resolución de problemas complejos secuenciales. En este capítulo se describirán los fundamentos de la programación dinámica, puesto que es la base del algoritmo implementado para el análisis de las señales biométricas del trabajo.

En esta exposición, se partirá de las definiciones y planteamiento del problema de la programación dinámica descritos en la Sección 3.1. A continuación, en la Sección 3.2 se definirá el Principio de Optimalidad de Bellman, pilar matemático a partir del cual se construyen los algoritmos de Programación dinámica, incluyendo un breve ejemplo de aplicación para la resolución del problema clásico del viajero.

Por último, en la Sección 3.3, se detallarán algunos algoritmos existentes para el alineamiento de secuencias genéticas basados en programación dinámica. Estos algoritmos son de especial interés en este trabajo, puesto que a partir de ellos, se ha desarrollado el algoritmo de análisis de las señales biométricas utilizado en esta investigación, que se explicará en el Capítulo 6.

3.1. Definiciones de conceptos de programación dinámica

La programación dinámica es una técnica matemática orientada a la solución de problemas secuenciales en etapas sucesivas donde se debe minimizar el coste total de dichas decisiones.

En cada etapa se valora no sólo el coste actual de tomar una decisión sino los costes futuros que se originan a partir de ella.

El número de estados puede ser finito o infinito.

Se pueden definir los siguientes conceptos:

- k el número de etapas.
- u_k las decisiones en cada etapa k.
- x_k los estados en los que puede encontrarse el sistema en cada etapa k.

A partir de una decisión u_k se va de un estado x_k de la etapa k a otro estado x_{k+1} de la etapa siguiente.

En cada etapa se evalúa la decisión óptima para cada uno de los estados x_k.

Cada estado guarda toda la información necesaria para tomar las decisiones futuras sin necesidad de conocer cómo se ha alcanzado dicho estado.

Es un procedimiento recursivo, que se resuelve de manera iterativa, hacia delante o hacia atrás. Cada vez que se añade una etapa, uno se acerca más a la solución del problema original.

Matemáticamente, el problema suele formularse de la siguiente manera:

Sea un sistema dinámico en tiempo discreto, descrito por la Ecuación 3.1:

$$x_{k+1} = f_k(x_k, u_k, w_k) \tag{3.1}$$

donde:

- $k = 0, 1, \ldots, N-1$, siendo N el número total de etapas.
- x_k pertenece a un estado de estados posibles de la etapa k.
- u_k pertenece a un estado de controles posibles de la etapa k y puede estar restringido en cada estado de cada etapa a un subconjunto del mismo.
- w_k pertenece a un estado de perturbaciones posibles y está caracterizada por una función de probabilidad que puede depender explícitamente de x_k y u_k pero no de valores anteriores de $w_{k-1} \ldots w_0$.

Por otro lado, llamamos $\pi = \{\mu_0, \mu_1, \ldots, \mu_{N-1}\}$ a una ley de control que para cada estado x_k proporciona un control u_k, según la Ecuación 3.2:

$$u_k = \mu_k(x_k) \tag{3.2}$$

Según esta formulación, el problema consiste en, dado un estado inicial x_0 encontrar una ley de control óptima $\pi^* = \{\mu_0^*, \mu_1^*, \ldots, \mu_{N-1}^*\}$ que minimice la Esperanza del coste, definida como en la Ecuación 3.3:

$$J_0(x_0) = E_{w_k}\left\{ g_N(x_N) + \sum_{k=0}^{N-1} g_k\left[f_k(x_k, \mu_k(x_k), w_k)\right] \right\} \tag{3.3}$$

Sujeto a la restricción $x_{k+1} = f_k(x_k, \mu_k(x_k), w_k)$ y conocidas las funciones de coste g_k [36], [35].

3.1.1. Problemas clásicos de programación dinámica

Algunos de los problemas clásicos que se pueden resolver fácilmente mediante técnicas de programación dinámica son:

- Ruta crítica: Se pretende seleccionar la ruta de carretera más corta entre dos ciudades. Existen diferentes conexiones entre cada una de las ciudades representado la longitud entre ellas. Éste es el problema típico de Programación dinámica, de hecho, en la Sección 3.2.1 se desarrolla el cálculo para un ejemplo de este problema. Además, es un problema tiene gran importancia en el marco de este trabajo, puesto que los algoritmos de alineamiento de señales y búsqueda de genes estudiados en la Sección 3.3 pueden formularse como este problema, aplicando de manera sencilla la misma solución.

- Número de empleados: En algunos proyectos, las contrataciones y los despidos se ejercen para mantener un número de empleados que satisfaga las necesidades del proyecto. Debido a que tanto las contrataciones como los despidos incurren en costes adicionales, se busca establecer el número de empleados a requerir a lo largo del proyecto que maximice el beneficio de la empresa.

- Reemplazo de equipo: Cuando una máquina llega a cierta edad, se elevan sus costos operacionales y de mantención, por lo que puede ser más económico reemplazarla. Luego, hay que determinar la edad de vida útil económica de la máquina. Se supone el problema de reemplazo de equipo a lo largo de un número de años. Al principio de cada año se decide prolongar el servicio del equipo un año más, o reemplazarlo por uno nuevo para minimizar el coste global de los equipos de la empresa.

- Volumen de carga: Aborda el problema de cargar artículos que poseen diferentes niveles de valor y volumen, en medios de carga con capacidad limitada. El objetivo es seleccionar las cargas que ofrezcan un mayor valor global a la carga.

- Problema de inversión: Se desean invertir las cantidades $P_1, P_2, \ldots, P_n$ al inicio de cada uno de los siguientes n años en distintos bancos con distintas tasas de interés y bonificaciones. El problema consiste en encontrar la inversión que maximice el beneficio en el año n.

- Distribución de esfuerzos: En un proyecto con muchas tareas y muchos empleados, hay que encontrar la manera óptima para que el proyecto salga adelante minimizando la duración del proyecto, el número de empleados y el porcentaje de tiempo perdido por los empleados por no tener una tarea asignada.

3.2. Principio de Optimalidad de Bellman

El principio de optimalidad de la programación dinámica, o principio de optimalidad de Bellman viene a decir que, dado un estado, la política óptima para las siguientes etapas no depende de la política tomada en las etapas anteriores.

Por tanto, la decisión óptima inmediata sólo depende del estado en el que se está, no de cómo se llegó hasta él. Toda la información sobre el pasado se resumen en el estado en que se encuentra.

Así pues, una vez conocida la solución óptima global, cualquier solución parcial que involucre sólo una parte de las etapas es también una solución óptima.

Por tanto, se cumple que todo subconjunto de una solución óptima global es a su vez una solución óptima para un problema parcial.

Gracias a esta propiedad, puede definirse una relación recursiva hacia atrás para conocer la política óptima en la etapa k conociendo las políticas óptimas de cualquier estado de la etapa $k+1$, según la Ecuación 3.4:

$$f_k^*(x_k) = \min_{u_k} \left\{ c_{x_k u_k} + f_{k+1}^*(x_{k+1}) \right\} \tag{3.4}$$

en donde:

- x_k es el estado actual en la etapa k.
- x_{k+1} es el estado al que se llega en la etapa $k+1$ dependiente del estado inicial x_k y de la decisión u_k.
- u_k es la variable de decisión en la etapa k.
- $f_k(x_k)$ es el valor acumulado de la función objetivo para el estado x_k desde la etapa k hasta N.
- $c_{x_k u_k}$ es el valor inmediato de tomar la decisión u_k desde el estado x_k

En los términos matemáticos que se definió el problema anteriormente, el Principio de Optimalidad de Bellman [2] puede expresarse según la Ecuación 3.5:

$$J_k(x_k) = \min_{u_k} E_{w_k} \left\{ g_k(x_k, u_k, w_k) + [f_k(x_k, u_k, w_k)] \right\} \tag{3.5}$$

donde $J_k(x_k)$ es el coste óptimo para la etapa k.

3.2.1. Ejemplo de aplicación

Un ejemplo de aplicación de este algoritmo puede aplicarse en el típico problema del viajero que quiere ir desde la ciudad A a la ciudad J por el camino más corto [3]. Este problema puede modelarse como el grafo de la Figura 3.2.1 donde:

Se puede resolver aplicando las ecuaciones de programación dinámica vistas anteriormente, de dos maneras, hacia atrás (backward DP) o hacia adelante (forward DP).

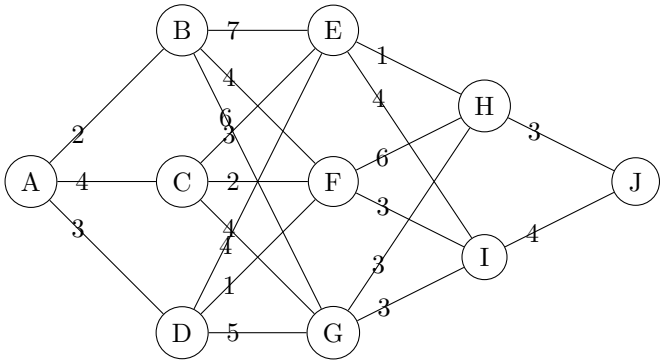


Figura 3.1: Ejemplo del problema clásico del viajero.

Si resolvemos el problema hacia atrás, empezaríamos por la etapa $k = 4$. En la Tabla 3.1 se encuentra el primer paso hacia atrás, empezando desde el nodo final J. Según esta tabla, los estados anteriores posibles serían venir del nodo H y del nodo I. Las distancias acumuladas en este paso para llegar a J serían de 3 y 4 respectivamente.

Tabla 3.1: Ejemplo de Algoritmo backward: Etapa 4

Estados x_4	Distancia acumulada f_4^*	Distancia óptima u_4^*
H	3	J
I	4	J

Continuando el algoritmo hacia atrás, en la etapa $k = 3$ podríamos llegar a los nodos E, F y G. A cada uno de ellos se puede llegar desde los estados x_4, que son los nodos H e I. En la Tabla 3.2 puede observarse las mejores decisiones para llegar a J por cada uno de los caminos H o I del paso anterior.

Por ejemplo, si nos situamos en el nodo E, sabemos que la distancia EH es 1 y la distancia EI es 4. Por otro lado, del paso anterior sabemos que la distancia acumulada para llegar a J por H es 3 y por I es 4. Calculando todas las posibilidades, obtenemos que si hemos llegado al nodo E, la decisión óptima para llegar a J es ir por H, puesto que la distancia acumulada en ese camino es 4, mientras que si vamos por I, es 8. Por tanto, hemos averiguado que el camino óptimo para ir de E a J es por H. El principio de Bellman dice que si en los pasos sucesivos encontramos que el mejor camino para ir de A a J pasa por E, entonces irremediablemente el camino óptimo para ir de A a J va a pasar también por H, puesto que el camino óptimo para ir de E a J pasa por H.

El mismo razonamiento puede hacerse para la etapa $k = 2$, donde los estados posibles x_2 son los nodos B, C y D. Los resultados de esta etapa pueden verse en la Tabla 3.3. Llegados a este punto, sabemos que si para ir de A a J vamos por B, la distancia acumulada total será de 11, y podremos ir por el nodo E o

Tabla 3.2: Ejemplo de Algoritmo backward: Etapa 3

	Estados x_4			
Estados x_3	H	I	Distancia acumulada f_3^*	Distancia óptima u_3^*
E	4	8	4	H
F	9	7	7	I
G	6	7	6	H

F. En cambio, si el camino óptimo pasa por C, existe un camino óptimo para ir a J de valor 7 si se va únicamente por E. Por otro lado, si el camino óptimo pasa por D, existen dos caminos óptimos de longitud 8 si se va por E o F.

Tabla 3.3: Ejemplo de Algoritmo backward: Etapa 2

	Estados x_3				
Estados x_2	E	F	G	Distancia acumulada f_2^*	Distancia óptima u_2^*
B	11	11	12	11	E,F
C	7	9	10	7	E
D	8	8	11	8	E,F

El último paso del algoritmo es la etapa $k = 1$, donde se suma el coste de ir de A a cada uno de los nodos adyacentes con la distancia acumulada para ir a J por cada uno de ellos. Los resultados pueden verse en la Tabla 3.4. Puede observarse que existe más de un camino óptimo de distancia 11, y que la mejor decisión de la primera etapa es ir por C o D.

Tabla 3.4: Ejemplo de Algoritmo backward: Etapa 1

	Estados x_2				
Estados x_1	B	C	D	Distancia acumulada f_1^*	Distancia óptima u_1^*
A	13	11	11	11	C,D

Deshaciendo el algoritmo, se concluye que existen tres posibles rutas óptimas (Tabla 3.5):

Tabla 3.5: Ejemplo de Algoritmo backward: Ruta óptima

Ruta óptima	Distancia
A C E H J	$4+3+1+3=11$
A D E H J	$3+4+1+3=11$
A D F I J	$3+1+3+4=11$

El mismo algoritmo puede aplicarse partiendo del nodo origen hacia delante, computando todos los caminos mínimos del origen a todos los destinos posibles en contraposición con el algoritmo "backward" que calcula todos los caminos mínimos para llegar al nodo final.

De esta manera, para la etapa $k = 2$ tendríamos los resultados presentados en la Tabla 3.6, partiendo del nodo A y pudiendo llegar a uno de los nodos x_2 (B, C o D):

Tabla 3.6: Ejemplo de Algoritmo forward: Etapa 2

	Estado x_1		
Estados x_2	A	Distancia acumulada f_2^*	Distancia óptima u_2^*
B	2	2	A
B	4	4	A
B	3	3	A

Dando un paso más, en la Tabla 3.7 se calculan los caminos mínimos correspondientes a la etapa $k = 3$, para llegar a cada uno de los nodos E, F, G a partir de los nodos anteriores B, C, D. Los resultados de esta tabla representan las decisiones óptimas para decidir el paso óptimo anterior si quisiéramos ir de manera óptima de A a los nodos del estado x_3.

Por ejemplo, si el camino óptimo para ir de A a J pasara por E, entonces la mejor decisión de la fase anterior sería construir el camino por C o por D, puesto que ambos ofrecen una distancia mínima de 7, de esta manera, se descarta el camino ABE como óptimo, ya que los caminos ACE y ADE tienen una distancia mínima menor.

Tabla 3.7: Ejemplo de Algoritmo forward: Etapa 3

	Estados x_2				
Estados x_3	B	C	D	Distancia acumulada f_3^*	Distancia óptima u_3^*
E	9	7	7	7	C,D
F	6	6	4	4	D
G	8	8	8	8	B,C,D

De manera similar, la Tabla 3.8 presenta los resultados de la etapa $k = 4$, obteniéndose los caminos mínimos y decisiones óptimas para llegar de A a H e I:

Tabla 3.8: Ejemplo de Algoritmo forward: Etapa 4

	Estados x_3				
Estados x_4	E	F	G	Distancia acumulada f_4^*	Distancia óptima u_4^*
H	8	10	11	8	E
I	11	7	11	7	F

Por último, en la etapa $k = 5$ se produce el salto final que llega al nodo destino J. En la Tabla 3.9 se calcula que el camino óptimo para llegar de A a J es de valor 11 y puede llegarse a él viniendo tanto del nodo H como del nodo I:

Deshaciendo el algoritmo, se llegan a las mismas tres posibles rutas óptimas obtenidas con el algoritmo"backward"(Tabla 3.10):

Tabla 3.9: Ejemplo de Algoritmo forward: Etapa 5

	Estados x_4			
Estados x_5	H	I	Distancia acumulada f_5^*	Distancia óptima u_5^*
J	11	11	11	H,I

Tabla 3.10: Ejemplo de Algoritmo forward: Ruta óptima

Ruta óptima	Distancia
J H E C A	$3+1+3+4=11$
J H E D A	$3+1+4+3=11$
J I F D A	$4+3+1+3=11$

Por último, se puede comparar las rutas óptimas obtenidas con este método con la solución "miope", en la que se busca siempre la mejor decisión local (se elige el nodo adyacente más cercano). En este caso, la ruta miope sería la correspondiente a la sucesión de nodos: A B F I J que implica una longitud de $2+4+3+4=13$ mayor en dos unidades respecto a las soluciones óptimas. Por tanto, el método de la programación dinámica encuentra una solución mucho más óptima al problema.

Las ideas principales del principio de Bellman y los algoritmos descritos en esta Sección, son la base para el desarrollo de otros algoritmos aplicados a muy distintos ámbitos. En la Sección 3.3 se estudiará su aplicación a algunos de ellos de interés para este trabajo.

3.3. Algoritmos de alineamiento basados en programación dinámica

En esta sección se tratarán de aplicar los conceptos teóricos de la programación dinámica explicados anteriormente al problema de alineamiento de secuencias genéticas [15], por su parecido al problema de señales biométricas que se va a tratar de resolver en esta investigación.

Para ello, nos basaremos en el ámbito de la bioinformática, en el que se requiere alinear secuencias genéticas para analizar las similitudes entre distintas cadenas de ADN, y así poder encontrar nuevos genes o zonas con información genética muy similar entre varias cadenas de ADN.

3.3.1. Introducción al problema de alineamiento de secuencias

Para calcular similitudes en secuencias de ADN hay que tener en cuenta que estas cadenas de aminoácidos están sujetas a distintas transformaciones naturales que hacen que los cálculos de similitudes clásicos basados en distancias no funcionen correctamente [6]. En particular, una cadena de ADN puede sufrir

las siguientes transformaciones:

- Inserción (insertion): Se inserta un nuevo aminoácido dentro de la cadena. Por tanto, el ácido que se encontraba en la posición i pasa a estar en la posición $i + 1$.
- Borrado (deletion): Se elimina un ácido de la cadena, por lo que un elemento en la posición i pasa a estar en la posición $i - 1$.
- Sustitución (susbtitution): Un aminoácido en la posición i muta y se transforma en otro.

Estas operaciones ocurren en la naturaleza con ciertas probabilidades, eliminando la posibilidad de comparar dos secuencias sin un alineamiento previo. Un ejemplo paradigmático de esta necesidad podría ser el intentar comparar una secuencia $S_1 = ATATATATATATAT$ con otra secuencia muy parecida a simple vista pero con una pequeña modificación $S_2 = TATATATATATATAT$. Al aplicar un algoritmo de comparación basada en distancia de Hamming se obtendría una medida de disimilitud muy alta, puesto que en ninguna posición el aminoácido coincide. En cambio, la secuencia $S_3 = ATCCCCCCCCCCC$ se parecería mucho más que la anterior, puesto que tiene dos ácidos iguales en las secuencias. Este resultado se contrapone con el sentido común que viene a decir que las dos secuencias primeras son representaciones del mismo código genético pero ha habido un borrado del primer aminoácido T en la segunda de ellas, mientras que la tercera cadena representa una cadena completamente distinta.

En 1966 Vladimir Levenshtein introdujo la noción de la "distancia de edición" para la comparación de similitudes en dos secuencias [21]. Esta distancia se define como el número mínimo de operaciones (inserciones, borrados o mutaciones) que transforman una secuencia dada en otra. En el ejemplo anterior, la distancia de edición de las secuencias S_1y S_2 es de 1, mientras que las de las secuencias S_1y S_3 es de 12. Por tanto, puede asegurarse que esta distancia refleja de manera mucho más fiel la realidad de las similitudes de cadenas.

Se proponen muchos algoritmos para calcular esta distancia, en general basados en programación dinámica. En las siguientes subsecciones veremos alguno de ellos. En particular, se presentará en detalle el algoritmo Longest Common Subsequences (LCS), que es el más sencillo y partir del cual, con pequeñas modificaciones, se han desarrollado otros más potentes para su utilización en ciertas aplicaciones.

3.3.2. Algoritmo Longest Common Subsequences

Este algoritmo permite computar de manera sencilla el análisis de la similitud de dos cadenas genéticas. En este algoritmo se utilizan únicamente dos operaciones: inserción y borrado, eliminando la opción de sustitución de un elemento por otro. Tal y como veremos más adelante, esta limitación es en realidad una ventaja para el análisis de señales de firmas biométricas, puesto que una inserción o borrado puede representar un movimiento más lento que otro en

algún momento de la realización de la firma, mientras que con la operación de sustitución no existe ningún tipo de relación directa en el contexto de las firmas biométricas.

El algoritmo, como su propio nombre indica, trata de encontrar la mayor subsecuencia común a dos secuencias dadas, ya que los puntos de dicha subsecuencia indican que no hace falta realizar ninguna operación en ese punto de las secuencias puesto que al ser común coinciden.

Formalmente, se define una "subsecuencia común" de dos cadenas v y w de longitud n y m como la secuencia z de longitud k, con $k < n$ y $k < m$, que cumple que $v_{i+t} = z_i, \forall i \leq k$ y a su vez $w_{i+s} = z_i, \forall i \leq k$, donde t y s pueden ir tomando valores positivos estrictamente crecientes para cada i.

Por ejemplo, la cadena TCTA es una subsecuencia común de A**TCT**G**A**T y **T**G**C**A**TA**.

Si la longitud de la subsecuencia común más larga para dos secuencias es $s(v, w)$, la distancia de disimilitud de v y w puede calcularse de acuerdo con la Ecuación 3.6:

$$d(v, w) = n + m - 2s(v, w). \tag{3.6}$$

Según la ecuación anterior, puede comprobarse como cuanto mayor sea la subsecuencia común asociada a dos secuencias, más se parecerán y por tanto su distancia de disimilitud será más próxima a cero.

Para representar cómo funciona el algoritmo LCS definiremos una matriz S, que se rellenará de manera recurrente mediante técnicas de programación dinámica. Esta matriz tendrá un tamaño $n \times m$, y se construye siguiendo la Ecuación 3.7:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + 0 \\ s_{i,j-1} + 0 \\ s_{i-1,j-1} + 1, \text{ if } v_i = w_j \end{cases} \tag{3.7}$$

El primer término de la Ecuación 3.7 corresponde al caso cuando v_i no está presente en la subsecuencia común más larga de v y w (borrado en v_i o inserción en w_j). El segundo término representa el caso cuando w_j no está presente (borrado de w_j o inserción de v_i), mientras que el tercer término corresponde al caso en el que tanto v_i como w_j forman parte de la LCS. Puesto que lo que se quiere encontrar es la subsecuencia máxima común, se suma uno a cada acierto, de tal manera que al finalizar el algoritmo, el elemento $s_{n,m}$ proporcionará la longitud máxima de la cadena común a las dos secuencias originales.

Para encontrar la subsecuencia común más larga a partir de la matriz S, se busca el camino que une el elemento $s_{n,m}$ con el elemento $s_{1,1}$, teniendo en cuenta que en la Ecuación 3.7 si el máximo se ha conseguido a partir del primer elemento, el movimiento correspondiente es $\leftarrow$, si se ha obtenido con el segundo, el movimiento es vertical $\uparrow$ y si el término mayor es el tercero ($v_i = w_j$) se realiza un movimiento en diagonal $\nwarrow$.

La Figura 3.2 presenta un ejemplo de la computación de la matriz de similitud $s(v, w)$ entre la secuencia $v = ATCTGAT$ y $w = TGCATA$. Puede

observarse como se ha realizado el relleno de la matriz de acuerdo a la Ecuación 3.7 y cómo se han asociado los posibles movimientos de acuerdo al término utilizado en el proceso.

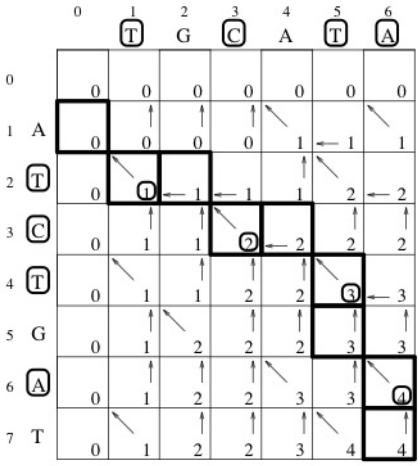


Figura 3.2: Ejemplo de obtención de la matriz de similitud de dos secuencias v y w que proporciona la subsecuencia común TCTA más larga posible

El alineamiento óptimo de las señales es inmediato, incluyendo un hueco en la secuencia v por cada movimiento horizontal que se haya realizado para ir de $s_{n,m}$ a $s_{1,1}$, y un hueco en la secuencia w por cada movimiento vertical. En el ejemplo anterior, el alineamiento óptimo es $v = AT - C - TGAT$ y $w = -TGCAT - A-$.

Además, la distancia de edición de las dos secuencias puede calcularse según la Ecuación 3.6, donde $n = 7$, $m = 6$ y $s(v, w) = 4$, resultando por tanto $d(v, w) = 7 + 5 - 2 \times 4 = 5$.

Si únicamente estamos interesados en la distancia de edición, sin importarnos cuál es la subsecuencia común, puede construirse una matriz de distancias D de manera análoga a la matriz S, pero en este caso computando directamente las distancias según la Ecuación 3.8:

$$d_{i,j} = \text{mín} \begin{cases} d_{i-i,j} + 1 \\ d_{i,j-1} + 1 \\ d_{i-1,j-1}, \text{ if } v_i = w_j \end{cases} \tag{3.8}$$

En esta ecuación, se busca la combinación de operaciones (inserciones y borrados) que ofrece una distancia mínima entre las dos secuencias. Por tanto, en la Ecuación 3.8 se busca el mínimo de las distancias, y se penaliza con la suma de 1 los movimientos que no corresponden a una equivalencia entre valores de las secuencias. El mismo ejemplo de la Figura 3.2 puede resolverse de esta manera, tal y como muestra la Figura 3.3.

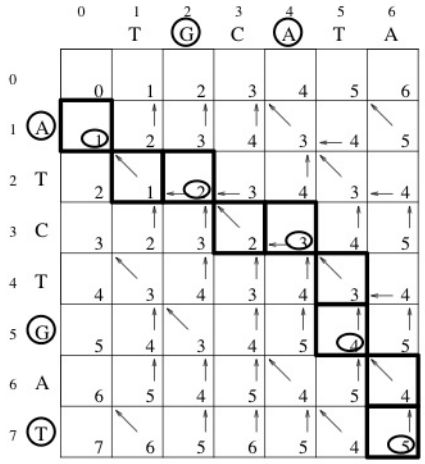


Figura 3.3: Ejemplo de obtención de la matriz de distancias de dos secuencias v y w que proporciona la distancia de edición.

3.3.3. Generalización del Algoritmo LCS como solución a cualquier problema de alineamiento global

El algoritmo LCS proporciona una puntuación bastante restrictiva, que premia con un valor de 1 los aciertos y no penaliza las inserciones o borrados. Esta puntuación se puede generalizar, extendiendo el alfabeto A de posibles k símbolos en las secuencias a un alfabeto de $k+1$ símbolos que incluya el símbolo "-" (gap). Además, puede definirse una matriz $\delta(x, y)$ de longitud $k+1 \times k+1$ que proporciona el valor de la puntuación entre cada par de posibles valores del alfabeto extendido.

De esta manera, la Ecuación 3.9 representa cómo se rellena la matriz S en base a esta nueva puntuación:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + \delta(v_i, -) \\ s_{i,j-1} + \delta(-, w_j) \\ s_{i-1,j-1} + \delta(v_i, w_j) \end{cases} \tag{3.9}$$

Además, esta ecuación puede complementarse penalizando con una constante $-\mu$ las sustituciones, con otra constante $-\sigma$ las inserciones y borrados, y recompensando los valores iguales con una constante θ. De esta manera, puede generalizarse la computación de la matriz S mediante la Ecuación 3.10:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} - \sigma \\ s_{i,j-1} - \sigma \\ s_{i-1,j-1} - \mu, \text{ if } v_i \neq w_j \\ s_{i-1,j-1} + \theta, \text{ if } v_i = w_j \end{cases} \tag{3.10}$$

En realidad, la puntuación del algoritmo LCS expuesta en la Sección anterior,

no es más que un caso particular de la generalización explicada en esta Sección, tomando los valores $\sigma = 0$, $\mu = 0$, $\theta = 1$.

Mediante esta generalización, definiendo correctamente las posibles puntuaciones de la matriz δ puede resolverse cualquier problema de Alineamiento Global, puesto que la solución obtenida será aquella que ofrece una distancia mínima de edición entre las dos secuencias que se quieren alinear.

El alineamiento óptimo global es de nuevo inmediato, incluyendo un hueco (-) en la secuencia v por cada movimiento horizontal necesario para ir de $s_{n,m}$ a $s_{1,1}$ y un hueco en la secuencia w por cada movimiento vertical.

3.3.4. Algoritmo de Alineamiento Local de Secuencias

Los algoritmos de alineamiento global de secuencias buscan similitudes entre dos cadenas completas. Esto es muy útil cuando las similitudes se extienden por toda la longitud de la cadena, por ejemplo en bioinformática, las secuencias de proteínas.

En cambio, hay otras aplicaciones donde lo importante es buscar una porción de la cadena que es muy similar a otra porción de otra. En este caso, los algoritmos alineamiento globales no encontrarían esta solución, sino otra con una mayor similitud global a las dos cadenas. Por ejemplo, los genes "homeobox" pueden encontrarse en multitud de especies, habiéndose desarrollado en cada uno de manera distinta. Sin embargo, estos genes mantienen una región sin apenas transformación denominada "homeodomain". Por tanto, para encontrar estos genes iguales en distintas especies, es necesario definir un algoritmo que pueda encontrar esas zonas con alta "similitud" a pesar de que estén rodeadas de zonas muy diferentes.

La primera solución que podría desarrollarse para encontrar esas zonas muy similares entre dos secuencias sería calcular las secuencias de alineamiento global entre cada par de vértices arbitrario (i, j) e (i', j'), de una manera similar a la solución del problema de alineamiento global para los vértices $(0, 0)$ y (n, m). Por supuesto, esta propuesta es absolutamente ineficiente, puesto que habría que computar cada par posible de vértices para poder encontrar la solución.

En 1981, se propone una modificación del algoritmo de alineamiento global que soluciona el problema de alineamiento local [32] de una manera eficiente. En esta propuesta se reduce la resolución del problema del alineamiento local a encontrar las subsecuencias comunes más largas (LCS) entre el vértice $(0, 0)$ y el resto de vértices posibles, añadiendo puentes de peso 0 en el grafo de edición entre el vértice $(0, 0)$ y cada uno del resto de vértices. Estos puentes convierten al vértice $(0, 0)$ en predecesor de cada uno de los vértices del grafo, proporcionando un camino para cada uno de ellos que elimina las posibles altas diferencias entre otras partes de las secuencias.

Por tanto, la ecuación de puntuación con la que se rellena la matriz S se transforma según la Ecuación 3.11:

$$s_{i,j} = \text{máx} \begin{cases} 0 \\ s_{i-i,j} + \delta(v_i, -) \\ s_{i,j-1} + \delta(-, w_j) \\ s_{i-1,j-1} + \delta(v_i, w_j) \end{cases} \tag{3.11}$$

El valor de $s_{i,j}$ más alto en todo la matriz S representa la puntuación de la optimización local óptima entre las secuencias v y w. (Nótese que en el problema de alineamiento global únicamente se observaba la puntuación del punto $s_{n,m}$). En la Figura 3.4 puede observarse el resultado de la aplicación de los algoritmos global y local a dos secuencias. En esta figura, puede comprobarse como hay una zona de las dos secuencias que tiene un alineamiento local óptimo (una diagonal completa), y por tanto, esas dos zonas de las secuencias tienen la misma información genética, proveniente probablemente de la información invariante del mismo gen.

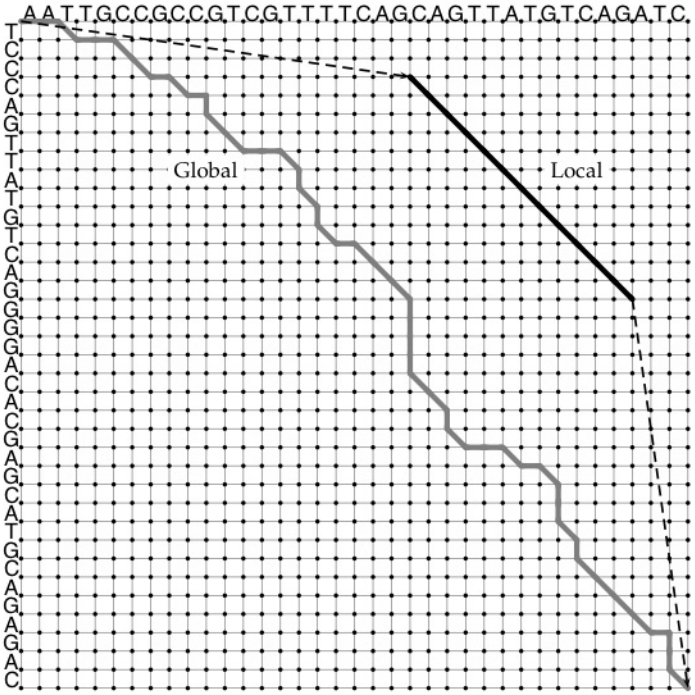


Figura 3.4: Aplicación de los algoritmos de Alineamiento Global y Local para analizar dos secuencias.

Capítulo 4

Desarrollo de aplicaciones en el iPhone

La técnica biométrica basada en firmas en el aire que se presenta en este trabajo de investigación, se ha desarrollado en un dispositivo móvil real, un iPhone. Esta implementación se explicará en la siguiente parte de este documento, pero para ello, es interesante presentar algunos conceptos teóricos sobre el iPhone, necesarios para ser capaces de programar cualquier tipo de aplicación en esta plataforma. En particular, en la Sección 4.1 se explica el esquema general de programación de las aplicaciones en el iPhone, basadas en la arquitectura "Modelo Vista Controlador". A continuación, en la Sección 4.2 se presentan algunos detalles más técnicos para la implementación de aplicaciones en un iPhone.

4.1. Arquitectura Modelo Vista Controlador

Todas las aplicaciones desarrolladas para el iPhone y otros dispositivos móviles de Apple (iPod Touch), se basan en la arquitectura MVC (Modelo Vista Controlador). Esta estructura fue introducida como parte de la versión Smalltalk-80 del lenguaje de programación Smalltalk [18].

Su principal característica es que el Modelo, las Vistas y los Controladores se tratan como entidades separadas, reduciendo enormemente el esfuerzo de programación de sistemas múltiples y sincronizados con los mismos datos. De esta manera, cualquier cambio producido en el modelo se refleja automáticamente en las vistas, permitiendo un gran ahorro de cantidad de código y una maximización de la reutilización del mismo.

En la Figura 4.1 se presenta la arquitectura MVC en su forma más general, formada por un modelo, múltiples controladores que manipulan ese modelo y varias vistas de los datos del modelo que cambian automáticamente al modificarse el estado del modelo.

Este modelo de arquitectura presenta varias ventajas:

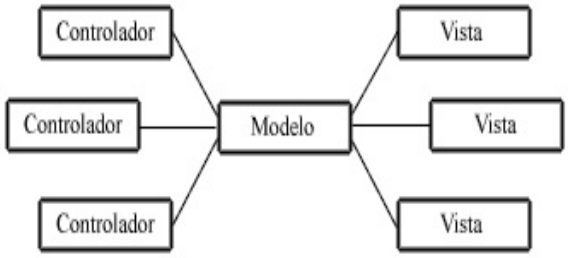


Figura 4.1: Arquitectura "Modelo Vista Controlador"

- Hay una clara separación entre los componentes de un programa, lo cual permite implementarlos, probarlos y mantenerlos por separado.
- Si hay un API bien definido (el SDK del iPhone), cualquiera que use el API, puede reemplazar el Modelo, la Vista o el Controlador, sin aparente dificultad.
- La conexión entre el modelo y sus vistas es dinámica. Cualquier cambio en el modelo se refleja en las vistas en tiempo de ejecución, no en tiempo de compilación.

Al incorporar el modelo de arquitectura MVC a un diseño, las piezas de un programa se pueden construir por separado y luego unirlas en tiempo de ejecución. Si uno de los Componentes, posteriormente, se observa que funciona mal, puede reemplazarse sin que las otras piezas se vean afectadas.

El modelo MVC divide todas las funcionalidades en tres categorías distintas:

- El Modelo es el objeto que representa los datos del programa. Maneja los datos y controla todas sus transformaciones. El Modelo no tiene conocimiento específico de los Controladores o de las Vistas, ni siquiera contiene referencias a ellos. Es el propio sistema el que tiene encomendada la responsabilidad de mantener enlaces entre el Modelo y sus Vistas, y notificar a las Vistas cuando cambia el Modelo.
- La Vista es el objeto que maneja la presentación visual de los datos representados por el Modelo. Genera una representación visual del Modelo y muestra los datos al usuario, permitiéndole interactuar con todo el sistema. Además, se comunica con el Modelo a través de una referencia al propio Modelo.
- El Controlador es el objeto que enlaza el modelo y las vistas. Es la lógica de aplicación que decide cómo manejar las órdenes del usuario, actuando sobre los datos representados por el Modelo. Cuando se realiza algún cambio, entra en actividad, bien sea por cambios en la información del

Modelo o por interacciones del usuario con las Vistas. De igual manera que las vistas, se comunica con el Modelo a través de una referencia al propio Modelo.

El objetivo en una arquitectura MVC es hacer que los objetos que implementan cualquiera de estas tres clases de código, se diferencien los uno de los otros tanto como sea posible. Por ello, cualquier objeto que se escriba debe ser fácilmente identificable y pertenecer a una de las tres categorías. Por ejemplo, un objeto que implementa un botón no debe contener el código para procesar los datos cuando se toca el botón.

La arquitectura MVC ayuda a garantizar la máxima reutilización. Una clase que implementa un botón genérico puede ser utilizado en cualquier aplicación. En cambio, una clase que implementa un botón que hace un cálculo particular cuando se hace clic sólo podrá utilizarse en la aplicación para la que fue escrito originalmente.

4.2. Detalles de programación en el iPhone

En esta Sección se presentarán detalles específicos necesarios para realizar aplicaciones en un iPhone.

En primer lugar se presentará el sistema de ficheros en una aplicación para el iPhone, imprescindible para elegir dónde almacenar los ficheros sensibles que deben permanecer en el teléfono móvil de manera segura e inaccesible para cualquier persona (por ejemplo, los patrones biométricos).

A continuación se explicarán las instrucciones para desarrollar e instalar una aplicación en un iPhone de uso propio para su prueba, y después poder ser distribuido y comercializado.

Por último, se explicarán algunos detalles propios de programación en el iPhone. El objetivo no es realizar un tutorial de cómo se programa en el iPhone desde cero, ni explicar en detalle el lenguaje de programación Objective-C con el que se desarrollan estas aplicaciones, sino mostrar únicamente aquellas clases imprescindibles que permiten implementar la funcionalidad de la técnica biométrica propuesta en una aplicación para el iPhone. Para los conceptos básicos de construcción de aplicaciones en el iPhone, así como fundamentos de programación del lenguaje utilizado, se ofrecerá una serie de referencias bibliográficas donde poder encontrar explicaciones completas de dicha información.

4.2.1. Sistema de ficheros en una aplicación para el iPhone

Al instalar una aplicación en un iPhone, el sistema operativo del teléfono crea un espacio de memoria ("Sandbox") con un sistema de ficheros accesibles únicamente por la aplicación. Se compone de las siguientes carpetas:

- *Application_Home*: Es el directorio que contiene el ejecutable de la aplicación. La aplicación no debe modificar ninguno de los ficheros del directorio

puesto que va firmada y, al ejecutarse, lo primero que hace el sistema operativo del teléfono es comprobar dicha firma.

- *Application_Home/Documents/*: Es un directorio para almacenar archivos específicos de la aplicación. Los archivos de este directorio pueden accederse vía iTunes.
- *Application_Home/Library/Caches*: Es un directorio para archivos persistentes entre distintas ejecuciones de la aplicación. Además, estos archivos permanecen en el teléfono y son accesibles únicamente por la aplicación en sí. De hecho, no se puede acceder a ellos de manera externa a la aplicación (vía iTunes u otros programas).
- *Application_Home/tmp*: En este directorio pueden almacenarse archivos temporales que se utilicen en la ejecución de la aplicación y que no sea necesario que sean persistentes.

Por lo tanto, el mejor directorio donde almacenar los patrones biométricos es el *Application_Home/Library/Caches*, que ofrece persistencia entre ejecuciones permitiendo que el usuario se enrole únicamente en la primera ejecución de la aplicación y cuando quiera acceder, en siguientes ejecuciones, los ficheros con los patrones biométricos obtenidos en la primera ejecución permanezcan disponibles para comprobar el acceso. Además, debido a que los ficheros que forman el patrón biométrico no son accesibles de manera externa, se puede asegurar que dicho patrón no saldrá del dispositivo.

4.2.2. Instrucciones para desarrollar una aplicación para el iPhone

En este apartado se presentarán los pasos que hay que seguir desde que se tiene una idea para hacer una aplicación en el iPhone hasta que ésta pueda ser distribuida y comercializada en el Apple Store.

Para realizar todos estos pasos es necesario, previamente, disponer de un ordenador MAC, en el que se realizará todo el desarrollo de la aplicación, puesto que desde otros ordenadores con otros sistemas operativos no se pueden programar aplicaciones para dispositivos Apple.

1. Obtención de la licencia de desarrollador de aplicaciones para el iPhone.

   Para obtener esta licencia, es necesario hacer una solicitud desde la página web de Apple, aportando toda la información personal del desarrollador y su equipo así como firmando una declaración para su correcto uso.

   Existen varios tipos de licencias:

   - Individual, de 99$.
   - Para compañías pequeñas (de hasta 500 empleados) de 99$.
   - Para grandes compañías, de 299$.

Para este trabajo, y dentro del grupo de investigación en el que se ha llevado a cabo, se solicitó una licencia para pequeña compañía (puesto que cuesta lo mismo que una individual). Una vez que la solicitud ha sido aceptada, pagada y activada se puede acceder a la descarga del SDK para programar aplicaciones en el iPhone así como a una gran cantidad de documentación.

Además, una vez se tiene la licencia de desarrollador de aplicaciones para iPhone, se puede acceder al portal de aprovisionamiento ("iPhone Provisioning Portal"), desde donde se realizan el resto de pasos siguientes, necesarios para poder instalar una aplicación en un iPhone o iPod Touch.

2. Instalación de un Certificado digital de desarrollador:

   Desde el portal de aprovisionamiento se puede solicitar un certificado digital de desarrollador. Todas las aplicaciones para el iPhone han de ser firmadas por un certificado válido, antes de que puedan ejecutarse en un dispositivo Apple.

   Este certificado es un documento electrónico que asocia la identidad digital del desarrollador con otra información personal como el nombre y la dirección de correo electrónico. Esta identidad digital incluye una clave pública y otra privada, con la que se firma la aplicación desarrollada en el sistema operativo del iPhone en la que se instala.

   Para solicitar un certificado digital de desarrollador, primero hay que generar una Petición de Certificado de Firma digital (CSR: "Certificate Signing Request") utilizando la aplicación "Keychain Access" de Mac OS X Leopard. Esta petición se envía en el propio portal de aprovisionamiento para que sea verificada con los datos de la licencia y en su caso, aprobada.

   Unos instantes después, cuando los agentes o administradores del portal de aprovisionamiento aprueben la solicitud, el usuario podrá descargar e instalar en su ordenador el certificado, añadiéndolo al llavero de claves que dispone su Mac.

3. Registro del dispositivo donde instalar las aplicaciones para su testeo.

   Para instalar una aplicación en un iPhone para poder probarla antes de distribuirla comercialmente, es necesario registrar el dispositivo en el portal de aprovisionamiento.

   Para registrar un iPhone o iPod, hay que realizar una solicitud completando el Identificador Único de Dipósitivo, (UDID: "Unique Device Identifier") propio del dispositivo en el portal de aprovisionamiento. El UDID es una cadena de 40 caracteres asociado de manera única a un dispositivo, cuyo valor se puede consultar fácilmente desde el menú de iTunes o el Organizer de Xcode.

   Estos UDIDs se incluirán en los perfiles de aprovisionamiento que se crearán más adelante. Estos perfiles de aprovisionamiento se incluyen en

las aplicaciones que se desarrollan, para permitir su instalación únicamente en los dispositivos móviles que hayan sido registrados.

Con la licencia de desarrollador se pueden registrar hasta 100 dispositivos iPhone o iPod para las pruebas de las aplicaciones programadas.

4. Definición de un App Id para la aplicación

   Un App Id es un identificador único de aplicación que el sistema operativo del iPhone utiliza para permitir que la aplicación se conecte al servicio de notificación de Apple ("Apple Push Notification"), comparta datos de claves entre aplicaciones y se comunique con accesorios de hardware externos. Para instalar una aplicación en un teléfono con el sistema operativo del iPhone, es necesario crear un App ID.

   Cada App ID consiste en un prefijo "Bundle Seed ID" de 10 caracteres generado por Apple y un sufijo "Bundle Identifier" proporcionado por un administrador del portal de aprovisionamiento.

   Para crear un conjunto de aplicaciones que compartan las mismas claves de aprovisionamiento puede crearse un único App Id acabando con un asterisco. En caso contrario, cada App Id vale únicamente para una aplicación en concreto.

5. Descarga del perfil de aprovisionamiento que incluye todos los datos

   Un perfil de aprovisionamiento ("Provisioning profile") es una colección de entidades digitales que unen los desarrolladores y los dispositivos a un equipo de desarrollo para iPhones autorizados, y permite que un dispositivo sea utilizado para prueba de aplicaciones.

   Un perfil de aprovisionamiento contiene todo lo explicado anteriormente: los certificados de desarrollo del iPhone, el UDID de los dispositivos registrados y el App Id correspondiente de la aplicación. El perfil de aprovisionamiento ha de ser instalado en cada dispositivo en el que se quiere ejecutar el código de aplicación.

   Los dispositivos especificados en el perfil de aprovisionamiento pueden ser utilizados para pruebas únicamente por los individuos cuyos certificados de desarrollo para el iPhone estén incluidos en el perfil. Un mismo dispositivo puede contener múltiples perfiles de aprovisionamiento.

6. Preparación para la distribución de la aplicación

   Una vez implementada la aplicación y probada en los iPhone o iPod registrados para el desarrollo, puede ser interesante distribuir la misma y comercializar con ella. Para ello, es necesario obtener un certificado de distribución para el Apple Store o bien para instalar la aplicación vía Ad-Hoc en otros dispositivos.

Todos estos pasos, permiten al programador instalar aplicaciones para su uso personal y pruebas en su propio dispositivo Apple. Para hacer esto, es necesario

en el proyecto en Xcode donde está el código de la aplicación, añadir en el campo "Code Signing Identity"la ruta del perfil de aprovisionamiento que está instalado en el ordenador donde se desarrolla la aplicación y contiene toda la información que debe ir en el teléfono para ser firmada. De esta manera, la aplicación no puede ser modificada por personas ajenas al desarrollo y además, contiene toda la información relativa al equipo que lo ha implementado

En este trabajo hemos tenido que seguir todos los pasos explicados para la instalación y uso de las aplicaciones que hemos desarrollado en un iPhone, excepto el paso de distribución, puesto que la aplicación desarrollada se ha quedado en un prototipo y no ha sido enviada para su comercialización en el Apple Store.

4.2.3. Lenguaje utilizado en aplicaciones iPhone

Las aplicaciones iPhone se desarrollan utilizando el lenguaje Objective-C. Éste es un lenguaje de programación orientado a objetos creado como un superconjunto de C pero implementando un modelo de objetos parecido al de Smalltalk. Al ser un superconjunto de C, cualquier código en C funcionará correctamente en la aplicación. De hecho, el algoritmo de procesamiento (Capítulo 6) utilizado en este trabajo de investigación se ha implementado en C y se ha incluido en distintas aplicaciones (Capítulos 10 y 11) desarrolladas en Objective-C para el iPhone.

Este lenguaje se basa en el paso de mensajes entre objetos, con una nomenclatura intuitiva basada en el uso de corchetes que encuadran cada uno de los mensajes. Algunos de los libros y manuales consultados para aprender a manejar este lenguaje son: [17], [39] y [16], cuyas referencias completas pueden ser consultadas en la Bibliografía final del trabajo. Asimismo, la documentación que ofrece Apple desde su portal para desarrolladores al que se tiene acceso si se ha comprado la licencia, es de gran calidad, ofreciendo códigos de ejemplo, tutoriales y videos demostrativos para aprender a programar en el iPhone. Además, gracias a la flexibilidad que ofrece Apple para desarrollar aplicaciones para sus dispositivos, hay una gran cantidad de desarrolladores programando aplicaciones muy diversas para el iPhone, pudiéndose encontrar en la Red una gran comunidad de usuarios muy dinámica que genera innumerables tutoriales de todos los niveles distribuidos libremente.

4.2.4. Descripción de funciones importantes

En este apartado se explicarán las funciones del iPhone necesarias para implementar la técnica biométrica basada en firma en el aire propuesta en el trabajo. Se mostrarán únicamente las funciones relativas al uso del acelerómetro del iPhone y al almacenamiento y la carga de los patrones biométricos que se guardarán en el dispositivo móvil.

Acceso al acelerómetro del iPhone

Para configurar el acelerómetro del iPhone para que muestree las aceleraciones a la frecuencia solicitada, se utiliza el siguiente comando, donde $kAccelerometerFrequency$ es la frecuencia en Hz de muestreo del acelerómetro:

```
[[UIAccelerometer sharedAccelerometer] setUpdateInterval:
(1.0 / kAccelerometerFrequency)];
```

Este comando se incluye en el primer método que se ejecuta al lanzar el programa: $(void)applicationDidFinishLaunching:(UIApplication*)application$. A partir de este momento, el acelerómetro empezará a registrar los valores de aceleración. Estos valores serán accesibles desde el siguiente método:

```
- (void)accelerometer:(UIAccelerometer *)accelerometer
didAccelerate:(UIAcceleration *)acceleration {

        float ix = (float)acceleration.x;
        float iy = (float)acceleration.y;
        float iz = (float)acceleration.z;

}
```

En ese mismo método, se pueden incluir comandos para almacenar cada uno de los valores que se vayan registrando en un vector. Asimismo, puede incluirse una comprobación booleana para que sólo se carguen en el vector los valores de aceleración de cuando el usuario está realizando su firma en el aire con el dispositivo móvil.

Guardar ficheros en el iPhone

Para almacenar los patrones biométricos de una firma en el aire que se ha muestreado y cuyos valores de aceleración se encuentran en un vector C llamado $accVector$, en primer lugar hay que incluirlos en un Array de Objective-C. Para ello, es necesario recubrir cada valor float (de C) en un NSNumber de Objective-C. Esto se hace con el siguiente fragmento de código:

```
NSMutableArray *accArray =
[[NSMutableArray alloc]initWithCapacity:1800];
int a=0;
for (a=0;a<1800; a++) {
  float f = (float)accVector[(int)a];
  NSNumber *nn =[NSNumber numberWithFloat:(float)f];
  [accArray addObject:nn];
}
```

A continuación, el NSArray de Objective-C con los datos de aceleraciones recubiertos como NSNumbers pueden almacenarse directamente en cualquier fichero del teléfono móvil, con el siguiente código, donde $accFile$ debería incluir la ruta y el nombre del fichero que se quiere crear.

```
NSString *accFile;
[accArray writeToFile:accFile atomically:YES];
```

Cargar ficheros en el iPhone

Para cargar los ficheros guardados en el iPhone de patrones biométricos almacenados según el procedimiento anterior, hay que proceder de manera inversa. En primer lugar, hay que crear un NSArray de Objective-C que se inicialice con el contenido del fichero en el que están almacenados los valores de aceleración:

```
NSString *fileName;
NSMutableArray *accArray2 = [[NSMutableArray alloc]
initWithContentsOfFile:fileName];
```

A continuación, se puede acceder al valor float (para ser usado en el método en C) de cada uno de los elementos del NSArray, accediendo al $floatValue$ de cada uno de los NSNumber que contiene el NSArray, y creando un nuevo vector en C ($accVectC$) que contenga los valores float de la firma en el aire cargada:

```
int c=0;
for (c=0;c<1800; c++) {
  NSNumber *accNumber =[accArray2 objectAtIndex:c];
  float accValue = [accNumber floatValue];
  accVectC [c]= (float) accValue;
}
```

Parte III

Desarrollo

Capítulo 5

Propuesta de técnica biométrica basada en firmas en el aire.

En este capítulo se presenta una nueva técnica biométrica basada en la realización de firmas en el aire con un dispositivo móvil que integre un acelerómetro. El conjunto de todo el trabajo de investigación se basa en la explicación, estudio y demostración de la validez de esta técnica biométrica para entornos móviles.

En la Sección 5.1 se presenta una descripción teórica detallada de la técnica biométrica propuesta y su manera de utilización.

Además, en la Sección 5.2 se presentan una serie de decisiones tomadas a la hora de implementar esta técnica biométrica en un dispositivo móvil. En particular, se explica la motivación para elegir el iPhone como dispositivo donde implementar en primer lugar el sistema biométrico, así como la manera en la que se utilizará el acelerómetro que incluye para extraer la información biométrica de la realización de las firmas. Por último, se comentarán otras decisiones relativas a la fase de enrolamiento y acceso al sistema.

5.1. Descripción de la técnica biométrica propuesta.

Esta técnica se basa en la realización de una firma en el aire con la mano sujetando un teléfono móvil. Para ello, es necesario que el teléfono móvil integre un acelerómetro, con el que se va a extraer la información de las aceleraciones en el eje X, Y y Z de la firma en el aire del usuario. Actualmente que la mayoría de los teléfonos móviles que están saliendo al mercado satisfacen esta restricción [33]. En particular, este trabajo se ha realizado con un iPhone 3G que incluye un acelerómetro configurado para recoger las aceleraciones en los tres ejes del espacio en un rango de (-2.5g,2.5g).

La técnica biométrica de reconocimiento de firma en 3D puede considerarse como una combinación entre las técnicas habituales de comportamiento y físicas. La repetición de una firma en el aire no depende únicamente de características de comportamiento del usuario, como la manera de sujetar el teléfono móvil, sino que además influyen una serie de características físicas que van a hacer que distintas personas repitan un mismo gesto de manera distinta, como por ejemplo la longitud del brazo, la capacidad de girar la muñeca, el tamaño de la mano, etc.

Esta técnica es similar al reconocimiento de usuarios por firma manuscrita [11], pero adaptada a un entorno de teléfonos móviles, con la ventaja de utilizar los tres ejes del espacio, en vez de un único plano donde realizar la firma. De hecho, al no ofrecer un plano de referencia a posibles falsificadores, la imitación de la realización de una firma en el aire es más complicada.

De igual manera, esta técnica tiene aspectos comunes con las técnicas de reconocimiento de gestos, pero el enfoque es radicalmente distinto. Las técnicas de reconocimiento gestuales intentan reconocer un mismo gesto realizado por muchas personas distintas, que lo pueden hacer de manera diferente para después realizar una acción común a todos y en respuesta a ese gesto [4]. El enfoque en esta técnica biométrica es diferenciar a la persona que realiza el gesto, así pues, si dos personas realizan el mismo gesto (o firma) en el aire, el sistema ha de ser capaz de identificar que los gestos, a pesar de su parecido, son distintos, pues corresponden a dos personas diferentes.

En esta propuesta, la extracción de características se realiza directamente en el propio móvil, sin ningún dispositivo adicional. Además, se pretende que todo el proceso de autenticación se realice también dentro del teléfono, para evitar los compromisos de seguridad en las conexiones con cualquier servidor externo. De esta manera, ejecutar todos los algoritmos involucrados en el proceso dentro del propio dispositivo móvil ofrece una gran cantidad de ventajas:

- El usuario no necesita gastarse más dinero en otros dispositivos, ya que únicamente necesita su propio teléfono móvil que ya tiene.
- Las posibilidades de ataque al sistema se reducen, ya que ninguna clave ni patrón sale fuera del dispositivo, ofreciendo una solución "Match on Card" [24].
- El sistema es resistente a ataques o caídas en las comunicaciones con un posible servidor externo que realice el proceso de autenticación.
- Esta configuración permite adoptar soluciones de criptobiometría, en el que la realización de una firma pueda generar, liberar o descifrar una clave asociada al usuario que se encuentra almacenada en el móvil, y que sólo él puede utilizar para realizar acciones que necesiten estar seguras de su identidad.

El proceso de autenticación de un usuario según esta técnica biométrica puede realizarse en un dispositivo móvil gracias al incremento de potencia de los

microprocesadores de los mismos, que permiten ejecutar los algoritmos involucrados en una cantidad de tiempo razonables, logrando así alcanzar también el requisito de tiempo "real".

Por otro lado, la realización de todo el proceso de autenticación en el propio dispositivo móvil, permite aplicar de manera sencilla un modelo criptobiométrico de liberación de clave tras autenticación. De este modo, el teléfono móvil puede tener una clave criptográfica asociada a la identidad del usuario propietario del dispositivo. Para acceder a la clave y utilizarla en cualquier aplicación que necesite autenticación, el usuario ha de repetir su firma en el aire, asegurando así su identidad.

5.2. Decisiones de implementación de la técnica biométrica de firma en el aire propuesta.

En esta Sección se describirán distintas decisiones que se han tomado para la implementación de la técnica biométrica de firmas en el aire en un dispositivo móvil.

En concreto, se explicará la motivación de la elección del iPhone como el dispositivo móvil donde implementar inicialmente esta técnica, así como los detalles del módulo para extraer las características de las firmas en el aire gracias al acelerómetro integrado en el propio móvil.

Además, se presentarán las decisiones relativas a las fases de reclutamiento y acceso, incluyendo las instrucciones que les serán dadas a los usuarios para la utilización correcta e intuitiva del sistema.

5.2.1. Elección del dispositivo móvil

Para este trabajo se ha determinado implementar la técnica biométrica de firmas en el aire en un iPhone, debido a las siguientes razones:

- Es el teléfono de referencia en el mercado, habiendo vendido millones de unidades en los últimos años.
- Proporciona un SDK para que desarrolladores externos a Apple puedan programar aplicaciones en él. Para ello es necesario comprar una licencia de desarrollador de 99$ al año, que se puede obtener directamente desde la página Web de Apple. Con esta licencia, uno puede:
  - Descargarse el SDK para desarrollar aplicaciones en el iPhone.
  - Instalar aplicaciones de test en iPhones o iPods.
  - Subir aplicaciones al Apple Store.
  - Obtener soporte para dudas y pruebas sobre las aplicaciones desarrolladas.
  - Acceder a una gran cantidad de documentación oficial para desarrollar en esta plataforma.

- Todos los teléfonos iPhone llevan integrados un acelerómetro capaz de recoger las aceleraciones en los tres ejes primarios del dispositivo.

- Las aplicaciones en el iPhone se desarrollan en un lenguaje denominado Objective-C, introducido brevemente en el Capítulo 4. Además, en estas aplicaciones se puede incluir código C. Por ello, el desarrollo del algoritmo matemático se programará directamente en C, para su facilidad de utilización en otras plataformas, dejando la parte de Objective-C para el resto de funcionamiento de las aplicaciones que se han desarrollado. (Capítulos 10 y 11).

5.2.2. Extracción de características

Para extraer las características de las firmas realizadas en el aire sujetando el iPhone, se utilizará el acelerómetro que viene integrado en el dispositivo móvil. Este acelerómetro tiene las siguientes características:

- La frecuencia de muestreo de las aceleraciones que son recogidas por el iPhone es configurable por software, a un máximo de 100Hz. Se recomiendan las siguientes utilizaciones de frecuencias de muestreo según la aplicación para la que se utilice:

  - 10-20 Hz: Aplicaciones que necesiten saber la orientación del dispositivo.
  - 30-60 Hz: Juegos y aplicaciones para entradas de tiempo real del usuario.
  - 70-100 Hz: Aplicaciones que necesiten detectar movimientos de alta frecuencia.

  En las aplicaciones que implementen la técnica biométrica de reconocimiento por firmas en el aire de los usuarios, se ha seleccionado la opción de muestreo a 100 Hz, puesto que es la ofrece mayor información de las aceleraciones de las firmas de los usuarios.

- La precisión con la que el Iphone puede representar los datos de la variación de velocidad obtenidos por su acelerómetro es de dos tipos:

  - Precisión +/- 2g: Indica que los valores de aceleración están acotados entre +/-2g, por lo que aceleraciones muy bruscas saturan el sistema. A cambio, ofrece una resolución muy alta, pudiendo distinguir cambios de aceleración de hasta 0.018g.
  - Precisión +/-8g: En este caso, el rango de aceleración es cuatro veces mayor, permitiendo al sistema obtener información de movimientos muy bruscos. A cambio, la precisión del sistema es cuatro veces peor.

En este caso, se ha preferido un rango de aceleraciones más pequeño a cambio de incrementar la precisión con la que el acelerómetro muestree las aceleraciones de cada firma en el aire, puesto que se quieren detectar los movimientos de manera muy precisa para que las firmas mantengan la información de la manera más identificativa posible.

Un muestreo de una firma en el aire genera tres valores cada 10 ms. correspondientes a la aceleración en ese momento en cada uno de los ejes. Una firma en el aire vendrá representada por una secuencia de conjuntos de tres valores, que se almacenará en un mismo fichero en el propio dispositivo móvil.

5.2.3. Decisiones relativas a la fase de enrolamiento

Para enrolarse en el sistema biométrico, es necesario que el usuario realice tres repeticiones de una misma firma, para que mediante el método de análisis matemático explicado en la Sección 6.3 se genere un patrón biométrico que se utilizará para autenticar al usuario ante nuevos intentos de acceso.

Además, se ha determinado que la firma en el aire debe durar un máximo de 6 segundos, recomendando una duración de 2 a 4 segundos, puesto que se ha considerado y comprobado que una firma más larga es complicada repetirla de manera natural, mientras que una muy corta no es suficientemente distintiva.

Instrucciones de enrolamiento

Para enrolarse en el sistema, tómese un tiempo para pensar en un gesto en 3 dimensiones que desee utilizar como su firma biométrica, considerando los siguientes factores:

- Ha de ser capaz de realizar el movimiento de la firma en el aire con su teléfono móvil en su mano.
- Debe ser capaz de recordar y repetir el gesto con facilidad. Se recomienda utilizar un gesto fácil de recordar, que haga de manera natural o que le evoque a algo en particular.
- Debe elegir un gesto lo suficientemente complejo para que nadie pueda reproducirlo de manera inmediata si tiene la ocasión de verle en directo.
- Debe durar un máximo de 6 segundos.

Una vez pensado el gesto, por favor repítalo tres veces, de la manera más precisa posible, siguiendo las instrucciones de la aplicación desarrollada para su teléfono móvil (Ver Capítulo 11 para más detalles de la aplicación final).

5.2.4. Decisiones relativas a la fase de acceso

Una vez que el usuario ya se ha enrolado en el sistema y quiere autenticarse en el mismo, se le dará únicamente una instrucción, puesto que ya ha manejado

en la fase de reclutamiento el sistema y ya tiene algo de experiencia haciendo su firma en el aire.

Simplemente, se le solicitará que realice una vez la firma en el aire con la que se enroló, tratando de hacerla de la manera más natural posible para que así sea lo más parecida posible a las firmas con las que se enroló. Este detalle es importante, puesto que aunque el algoritmo de análisis de las señales que se presentará en el Capítulo 6 corrige pequeñas variaciones de las señales, cuánto más parecidas sean de inicio, mejor funcionará el sistema.

Capítulo 6

Fundamentos matemáticos del análisis de señales de firmas en el aire

En este capítulo se presentará el algoritmo de análisis de señales biométricas de firmas en el aire que se ha desarrollado para evaluar si dos firmas pertenecen al mismo usuario o no.

Para ello, se explicará en un primer momento, en la Sección 6.1 la motivación por la que se ha elegido un algoritmo de alineación de secuencias para el análisis de las señales de aceleraciones de cada eje provenientes de las firmas en el aire, mostrando sus parecidos con el problema de alineamiento de secuencias genéticas, presentado en el Capítulo 3. Debido a estos parecidos, la utilización de las técnicas para resolver dichos problemas permite que puedan ser aplicados con éxito también en este ámbito Además, se expondrán las diferencias entre los problemas de alineamiento de secuencias y de señales biométricas de firmas, que se traducirán en ciertas modificaciones en el algoritmo desarrollado para representar el nuevo problema.

A continuación, se explicará en detalle el algoritmo utilizado para analizar las señales biométricas provenientes de las aceleraciones cuando los usuarios realizan las firmas en el aire según la técnica descrita anteriormente. Este algoritmo es una modificación de los algoritmos de alineamiento de secuencias ya presentados en el Capítulo 3.

A partir de dicho algoritmo, pueden compararse dos firmas en el aire, obteniéndose un valor de una métrica definida que representa cuánto de iguales son dos firmas. Aplicando éste algoritmo, en la Sección 6.3 y 6.4 se explicará como se realizan matemáticamente las fases de enrolamiento y acceso al sistema.

Por último, la Sección 6.5 presenta varios esquemas multibiométricos de fusión de información a distintos niveles. Estos esquemas de fusión serán estudiados para encontrar el mejor escenario de fusión de la información de las aceleraciones en cada uno de los ejes que minimice al máximo las tasas de error

del sistema.

6.1. Motivación de la utilización de un algoritmo de alineamiento para el análisis de señales biométricas de firmas en el aire

En un problema de autenticación a un usuario mediante la realización de su firma manuscrita, existe el inconveniente de que un usuario nunca será capaz de repetir su firma dos veces de manera 100 % exacta, por lo que la comparación de señales nunca podrá realizarse directamente mediante la aplicación de métodos de comparación directos.

Cada vez que un usuario repite su firma, realizará ciertas partes de la misma de manera más o menos rápido, más o menos pronunciada, etc. A pesar de estas pequeñas variaciones, lo intrínsico de la firma, que permanece siempre invariante y es identificativo de la persona, sigue estando.

Por esta razón, es necesario realizar un preprocesado de la señal que corrija estas pequeñas deformaciones mediante un alineamiento, que mantenga estas características intrínsecas de la señal, corrigiendo dichas pequeñas variaciones. De esta manera, a pesar de las pequeñas variaciones en la repetición de la firma del usuario, el sistema puede identificar la autenticidad del usuario.

De la misma manera que es importante que el algoritmo de preprocesado corrija pequeñas variaciones en la repetición de la firma, es necesario que el algoritmo no corrija "demasiado" las variaciones de la firma, puesto que en ese caso usuarios que intenten imitar la firma del usuario original, podrían hacerse pasar por él, produciendo error de falsa aceptación.

Este problema es muy parecido al problema de alineamiento global de dos secuencias expuesto en la Sección 3.3.3, ya que trata de buscar un alineamiento máximo entre las dos secuencias de la señal biométrica. Cuanto más grande sea la subsecuencia común a las dos señales biométricas, mayor será el parecido entre ellas y por tanto, es más probable que las dos firmas sean del mismo usuario.

La introducción de huecos en las secuencias que se quieren alinear, mediante el algoritmo de alineamiento global, representa la correción de las pequeñas variaciones de las secuencias de señales biométricas.

En la Figura 6.1, podemos encontrar gráficamente la motivación para la aplicación de un algoritmo de alineamiento en el preprocesado de las señales. En esta figura, podemos encontrar, separadas por eje, las aceleraciones de dos repeticiones de la misma firma realizadas por el mismo usuario en diversos momentos. Puede observarse que las señales de cada repetición en cada eje tienen un aspecto muy similar, puesto que en realidad cada una de ellos pertenece a la misma firma.

Al aplicar directamente un algoritmo de comparación entre las firmas de la Figura 6.1, obtendríamos unos resultados muy altos que indicarían que las firmas corresponden a distintas personas, cuando en realidad pertenecen al mismo usuario, solo que están realizadas en distintos momentos y de distintas mane-

ras. En particular, se pueden observar las siguientes diferencias que se pueden corregir con el algoritmo de alineamiento global:

- Las señales no comienzan en el mismo momento.
- Existen picos más pronunciados que otros.
- En algún momento de la señal, las transiciones son más lentas que otras.
- Las señales no duran exactamente lo mismo.

Por otro lado, existe una gran diferencia intrínseca a las secuencias genéticas y las señales biométricas. Las primeras son discretas, con un alfabeto cerrado, mientras que las segundas son continuas, donde cada uno de sus puntos puede tener un valor entre (-2.5, 2.5). Debido a esta razón, es posible que el valor de dos puntos de la secuencia no coincida aunque en realidad sean iguales (por ejemplo, los valores 1.2344 y 1.2343) Esta diferencia, tal y como veremos en la Sección 6.5.1 obliga a realizar una modificación en el algoritmo que extienda el mismo al caso de alfabeto abierto y continuo.

6.2. Algoritmo utilizado para analizar señales de aceleraciones de firmas en el aire

Para el alineamiento de señales de aceleraciones obtenidas de firmas en el aire, es necesario redefinir la Ecuación 3.9, incluyendo una métrica que cuantifique cuánto de iguales son dos puntos (equivalente al $v_i = w_j$ del caso discreto). Además, la puntuación del siguiente punto va a depender también de este valor. La puntuación propuesta es la definida en la Ecuación 6.1:

$$s_{i,j} = \text{máx} \begin{cases} s_{i-i,j} + \delta(v_i, -) \\ s_{i,j-1} + \delta(-, w_j) \\ s_{i-1,j-1} + \Gamma(v_i, w_j, \sigma) \end{cases} \tag{6.1}$$

en donde:

- La introducción de un hueco en la secuencia va a ser penalizada por una constante h, denominada "gap", cuyo valor habrá que determinar. Por tanto, en este problema definimos $h = \delta(v_i, -)$ y $h = \delta(-, w_j)$.
- La función $\Gamma(v_i, w_j, \sigma)$ es una función que proporciona una métrica para cuantificar cuánto de iguales son dos puntos de las señales. Esta función devuelve un valor muy próximo a 1 cuando v_i y w_j son muy cercanas y muy próximo a 0 cuando no se parecen. El valor de esta función se calcula según la Ecuación 6.2, donde σ es otra constante cuyo valor hay que determinar para el problema en cuestión.

$$\Gamma = e^{-\frac{(v_j - w_j)^2}{2\sigma^2}} \tag{6.2}$$

La elección de los valores de las constantes h y σ tiene que hacerse teniendo en cuenta que las señales biométricas tratadas tienen valores entre (-2.5,2.5). Con esta restricción, se ha seleccionado un valor de $h = 0{,}4$ y un valor de $\sigma = 0{,}225$. En estas condiciones se cumple que $|v_j - w_j| = 0{,}3$ y $\Gamma = h$, por lo que las puntos de las señales que varíen menos del valor 0.3 serán corregidos. Esta hipótesis de la elección de los valores de los parámetros h y σ ha sido evaluada en la Sección 9.1.

Aplicando este algoritmo a las señales biométricas de la Figura 6.1, se obtienen las secuencias de la Figura 6.2. En dicha figura puede observarse cómo se han introducido ceros (equivalentes a huecos de las secuencias genéticas) en cada una de las señales de firmas, para conseguir el alineamiento global óptimo de cada par de señales.

Realizando una interpolación de cada uno de los huecos que se ha generado en cada par de señales de la Figura 6.2, se obtienen las señales de la Figura 6.3. En esta figura, puede observarse cómo las señales se han alineado perfectamente y ahora sí puede aplicarse un algoritmo de comparación entre cada par de señales y obtenerse un resultado de comparación muy bajo que indique que las dos repeticiones de cada firma pertenecen al mismo usuario.

Si se analizan dos señales de distintas firmas, las diferencias una vez aplicado todo el preprocesamiento de las señales deberían mantenerse, a pesar de haber realizado un alineamiento de secuencias global. En la Figura 6.4 puede observarse el resultado del preprocesado de dos señales de firmas distintas, comprobándose que las diferencias de las firmas permanencen de manera notoria.

Finalmente, una vez alineadas dos señales, es necesario definir una métrica que cuantifique el parecido (o diferencia) de las dos señales ya alineadas, siendo éste el módulo de comparación de las señales preprocesadas. Para ello, se ha seleccionado la métrica basada en distancia Euclídea definida en la Ecuación 6.3:

$$\delta_{A,B} = \sqrt{\sum_{i=0}^{2m} (a'_i - b'_i)^2} \tag{6.3}$$

donde $A = \{a_1, \ldots, a_m\}$ y $B = \{b_1, \ldots, b_m\}$ son las señales de aceleración originales que se procesan y $A' = \{a'_1, \ldots, a'_{2m}\}$ y $B' = \{b'_1, \ldots, b'_{2m}\}$ las señales ya alineadas e interpoladas.

Por tanto, como resultado de todo el proceso de análisis de señales, se obtendrá un valor numérico $\delta_{A,B}$ correspondiente a la medida de similitud de las dos señales alineadas e interpoladas, en base al algoritmo que se ha explicado. Cuanto menor sea el valor de $\delta_{A,B}$, más parecidas serán las señales, y viceversa.

Este algoritmo se utilizará para obtener el parecido de las señales en cada eje, aunque se puede utilizar de la misma manera en otro tipo de escenarios con procesamiento previo de la información de las aceleraciones en cada eje (por ejemplo, calculando el módulo de la aceleración en cada punto). Estos

escenarios y posibilidades de fusionar la información se presentarán en detalle en la Sección 6.5.

6.3. Fundamentos matemáticos de la fase de enrolamiento

En esta Sección se presentará el método matemático en el procesamiento de las señales utilizadas para el enrolamiento del usuario, en el escenario básico en el que se realizan los análisis de señales por separado en cada eje y en todos los ejes. A partir de esta descripción, en la Sección 6.5 se describirán variaciones del mismo al realizar distintos métodos de preprocesamiento, selección y fusión de la información de cada eje.

Cada usuario U_i va a elegir una firma identificativa para autenticarse en el sistema. Este gesto G_i está formado por tres señales diferentes (G_i^x, G_i^y y G_i^z) correspondientes a la aceleración de cada gesto en cada eje del espacio a una frecuencia de muestreo de 10 ms. Cada repetición j del mismo gesto G_i llevado a cabo por el usuario U_i se define como $G_{i,j}$.

Debido a la decisión de utilizar tres repeticiones del gesto para el enrolamiento del usuario U_i, se obtienen nueve señales; tres por cada una de las repeticiones de la firma, correspondientes a las aceleraciones en cada uno de los ejes del espacio: $G_{i,j}^x, G_{i,j}^y, G_{i,j}^z, j = 1, 2, 3$.

Al inicio de la fase de enrolamiento, un usuario específico U_T repite la firma G_T con la que se quiere enrolar tres veces ($G_{T,1}$, $G_{T,2}$, $G_{T,3}$), de acuerdo a las instrucciones de enrolamiento que se ofrecieron en la Sección 5.2.3, y por tanto, se obtienen las respectivas señales de aceleración en cada eje de cada repetición.

El análisis de todas estas señales en la fase de enrolamiento, implica la ejecución nueve veces del algoritmo de procesamiento, para obtener las diferencias de cada repetición en cada eje con las otras dos. En particular, se calculan los siguientes nueve valores: $\delta_{j,k}^e$, con $j, k = 1, 2, 3$ y $j \neq k$ y $e = x, y, z$. (Por ejemplo, $\delta_{j,k}^x$ representa la diferencia en la métrica definida de comparar las señales alineadas e interpoladas de la repetición $G_{T,j}$ y $G_{T,k}$ en el eje x).

A partir de estos valores de diferencias de señales en cada eje, se calcula la diferencia entre dos muestras $G_{T,j}$ y $G_{T,k}$ de una misma firma G_T como la media de las diferencias de las señales en cada eje, tal y como exprese la Ecuación 6.4:

$$\delta_{j,k} = \frac{\delta_{j,k}^x + \delta_{j,k}^y + \delta_{j,k}^z}{3} \tag{6.4}$$

Aplicando dicha ecuación, se computan las diferencias entre cada repetición de la firma utilizada para el enrolamiento, obteniéndose los valores $\delta_{1,2}$, $\delta_{1,3}$ y $\delta_{2,3}$. En base a estos tres valores, se calcula el parámetro "diferencia del patrón", denominado μ_T y definido como la media de las diferencias entre las tres repeticiones de la firma utilizadas para enrolarse en el sistema. (Ecuación 6.5).

$$\mu_T = \frac{\delta_{1,2} + \delta_{1,3} + \delta_{2,3}}{3} \tag{6.5}$$

Por último, el patrón biométrico del usuario, que se almacena en el teléfono móvil para autenticarle, se compone de:

- Las señales $G_{T,1}$, $G_{T,2}$ y $G_{T,3}$, que incluyen las aceleraciones en cada eje de cada repetición de la firma utilizada para enrolarse en el sistema.
- El parámetro μ_T, obtenido según la Ecuación 6.5 y anteriores, que representa la similitud entre las tres repeticiones de la firma realizada por el usuario.

Cuanto más bajo es el valor de μ_T, más seguro es el patrón biométrico. μ_T representa la facilidad con la que un mismo usuario puede repetir su firma de manera precisa. En otras palabras, cuando μ_T es bajo, un falsificador que intente imitar su firma, debería hacerla de manera muy precisa. En cambio, si el valor de μ_T es alto implica que el usuario original no es capaz de repetir su firma de manera precisa, y por tanto, el umbral para permitirle el acceso debería ser más alto, ofreciendo a un posible falsificador más oportunidades para hacerse pasar por el usuario original.

6.4. Fundamentos matemáticos de la fase de acceso

Una vez que el usuario se ha enrolado en el sistema repitiendo su firma en el aire tres veces, y tras el proceso matemático explicado anteriormente, ya puede acceder al mismo realizando de nuevo su firma identificativa. El dispositivo móvil extraerá las aceleraciones del gesto de acceso G_A en cada eje a la misma frecuencia de 10 ms que en el proceso de enrolamiento, obteniéndose las señales G_A^x, G_A^y y G_A^z.

A continuación, se procesan las señales de acceso y las señales almacenadas en el patrón ejecutando el algoritmo explicado en 6.5.1, proporcionando las diferencias entre el gesto de acceso y cada uno de las repeticiones de la firma almacenada en el patrón: $\delta_{A,1}$, $\delta_{A,2}$ y $\delta_{A,3}$. A partir de estos valores, se calcula δ_A, como la media de todas ellas.

Este valor carece de interés si no se compara con otros valores equivalentes. Por ello, se propone un indicador para comparar los dos parámetros definidos en esta Sección: μ_T obtenido en la fase de enrolamiento y δ_A en la fase de acceso. Para ello hay que tener en cuenta que:

- Si $\delta_A \approx \mu_T$ significa que la realización de la firma en el acceso es muy similar a las firmas de enrolamiento, y por tanto, el usuario es quien dice ser, puesto que se supone que sólo él mismo puede repetir su firma con igual precisión.
- Si $\delta_A \gg \mu_T$, la realización de la firma de acceso es muy diferente a las firmas de enrolamiento, por lo que el usuario debe ser rechazado.

- Si δ_A es solo un poco mayor que μ_T, puede ocurrir que el usuario sea quien dice ser o no. La definición de dónde se coloca el umbral de decisión para rechazar o aceptar al usuario se realizará para minimizar el error total. Esta definición será consecuencia de los resultados obtenidos en el estudio del EER de la Sección 9.2.

- Si $\delta_A < \mu_T$ significa que la diferencia entre la firma de acceso y las firmas del patrón es más pequeña incluso que las propias del patrón entre sí, por lo que el usuario es quien dice ser.

Teniendo en cuenta estas consideraciones, se define una función umbral θ como $\theta = \delta_A/\mu_T$, que cumple todas las características anteriores de manera lineal:

- Si $\theta < 1$ implica que $\delta_A < \mu_T$.

- $\theta <\approx 1$ se cumple cuando $\delta_A \approx \mu_T$.

- Para que $\theta > 1$, δ_A debe ser un poco mayor que μ_T.

- $\theta \gg 1$ cuando $\delta_A \gg \mu_T$.

En conclusión, para valores de θ menores y próximos a 1, el sistema aceptará al usuario. Cuando θ tome valores mucho mayores que 1, el sistema rechazará al usuario. El umbral de decisión para la aceptación o el rechazo de un usuario será $\theta > \kappa$, con $\kappa > 1$ y se definirá en la Sección 9.2, buscando minimizar el error total.

Por tanto, un usuario será aceptado en el sistema siempre que se cumpla la Ecuación de Verificación 6.6:

$$\theta < \kappa \tag{6.6}$$

6.5. Fundamentos matemáticos de fusión de información

En esta técnica biométrica, se dispone de tres señales de aceleración por cada firma, correspondientes a las aceleraciones del dispositivo con el que se realiza el gesto en cada uno de los tres ejes del espacio. Existen muchas posibles maneras de fusionar esta información, según en qué bloque del esquema del sistema biométrico completo se realice dicha transformación.

Estos esquemas de fusión multibiométrica, se dividen en [29]:

- Fusión a nivel de sensor [28].

- Fusión a nivel de extracción de características [40].

- Fusión a nivel de comparación [27].

- Fusión a nivel de decisión [26].

Puesto que en el dispositivo móvil con el que se ha llevado a cabo este trabajo no se puede acceder a modificar los sensores de acelerómetros que proporciona, no se tratarán escenarios de fusión a nivel de sensor.

En cambio, se presentarán dos escenarios donde la fusión se realiza justo cuando se han extraído las aceleraciones en cada eje. Asimismo, se explicará un escenario donde la fusión se realiza en el módulo de comparación. Por último, se explicará el escenario básico, donde la fusión se realiza a nivel de decisión, que ya se ha presentado en la Sección anterior.

6.5.1. Fusión a nivel de extracción de características

Una vez extraídas las aceleraciones en cada eje, se pueden procesar estas señales para obtener que fusionen las aportaciones de cada una de ellas. En particular, se proponen dos métodos:

- Concatenar las señales
- Calcular el módulo de las señales

Concatenación de señales

Sean A_x, A_y, A_z, las aceleraciones en cada eje de una muestra de firma en el aire. En este escenario de fusión, se propone crear la señal A^C mediante la concatenación de las señales de cada eje del gesto, según la Ecuación 6.7:

$$A_C = \{A_{x1}, \ldots, A_{xL}, A_{y1}, \ldots, A_{yL}, A_{z1}, \ldots, A_{zL}\} \tag{6.7}$$

De esta manera, se obtiene una señal de longitud tres veces cada uno de los ejes, que se le pasará al algoritmo de alineamiento de manera completa. Así pues, en este escenario, el algoritmo se ejecutará una única vez por cada comparación de dos firmas diferentes, obteníendose un valor de similaritud al aplicar el algoritmo de la sección anterior a la señal concatenada de cada eje, de longitud total $3L$.

Cálculo del módulo de las señales

Otra opción para la fusión de la información en los tres ejes es el cálculo del módulo de la aceleración punto a punto, según la Ecuación 6.8:

$$A_{M_i} = \sqrt{(a_{xi})^2 + (a_{yi})^2 + (a_{zi})^2}, i = 1 \ldots L \tag{6.8}$$

Donde A_x, A_y, A_z son las aceleraciones en cada eje de una muestra de firma en el aire, y A_M es la señal módulo de las anteriores.

En consecuencia, mediante el cálculo del módulo de las señales de cada uno de los ejes se reduce el número de procesamientos del algoritmo de tres a uno, para cada comparación de dos firmas en el aire. Por cada par de firmas, se

preprocesa el módulo de cada una de ellas con la Ecuación 6.8 y se aplica el algoritmo de la Sección , obteniéndose un valor $\delta_{A,B}$ de similitud entre las dos señales comparadas.

6.5.2. Fusión a nivel de comparación

En este escenario de fusión de información, el procesamiento de las señales de aceleración de los tres ejes de cada par de firmas en el aire se realiza de manera independiente en paralelo, fusionando la información de cada eje en el bloque de comparación.

Así pues, si tenemos dos firmas en el aire A y B, con las señales de aceleración correspondientes a cada eje A_x, A_y, A_z, B_x, B_y y B_z, se realizar el alineamiento de cada par de señales de igual eje de manera independiente, obteniéndose A'_x, A'_y, A'_z, B'_x, B'_y y B'_z alineadas entre ellas. Llegados a este punto, se calcula el valor de similaritud $\delta_{A,B}$ según la Ecuación 6.9

$$\delta_{A,B} = \sqrt{\sum_{i=0}^{2L} (a'_{xi} - b'_{xi})^2 + (a'_{yi} - b'_{yi})^2 + (a'_{zi} - b'_{zi})^2} \tag{6.9}$$

El tiempo de procesamiento, por tanto, en este escenario de fusión equivale a la ejecución tres veces del algoritmo de alineamiento con señales de longitud L.

6.5.3. Fusión a nivel de decisión

La fusión a nivel de decisión es el escenario más sencillo e intuitivo de aunar la información de cada uno de los ejes. Este escenario es el que se explicó anteriormente en la Sección 6.3, donde la alineación de las señales y su posterior cuantificación de diferencias se efectuaba en cada eje por separado, obteniéndose tres valores $\delta^x_{A,B}$, $\delta^y_{A,B}$ y $\delta^z_{A,B}$. El valor de diferencias final $\delta_{A,B}$ entre las dos firmas A y B se calculaba como la media aritmética de los valores en cada eje.

El tiempo de procesamiento necesario para este escenario coincide con el anterior, es decir, tres veces la ejecución del algoritmo de alineamiento con señales de longitud L.

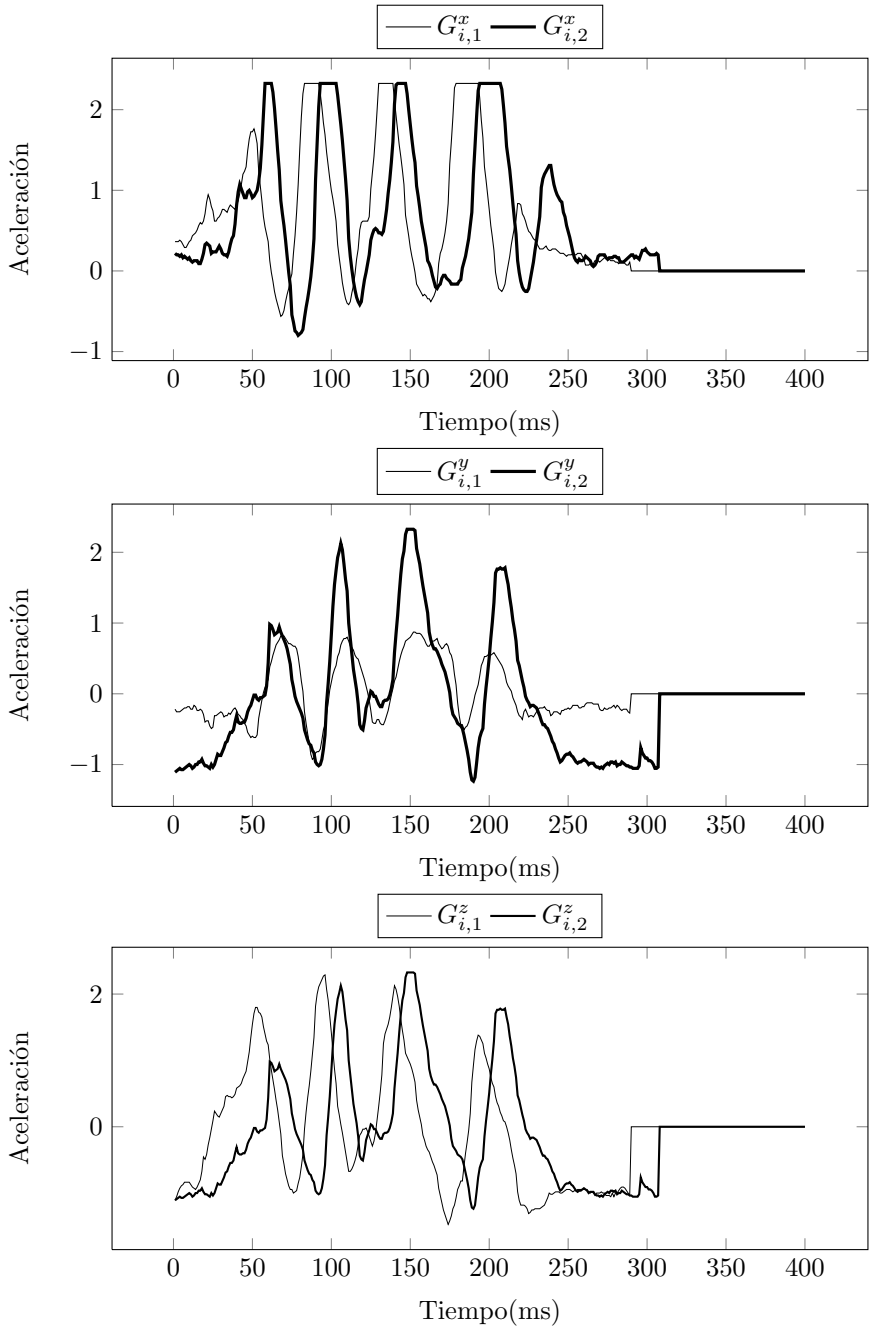


Figura 6.1: Ejemplo de dos repeticiones de una misma firma realizadas por el mismo usuario.

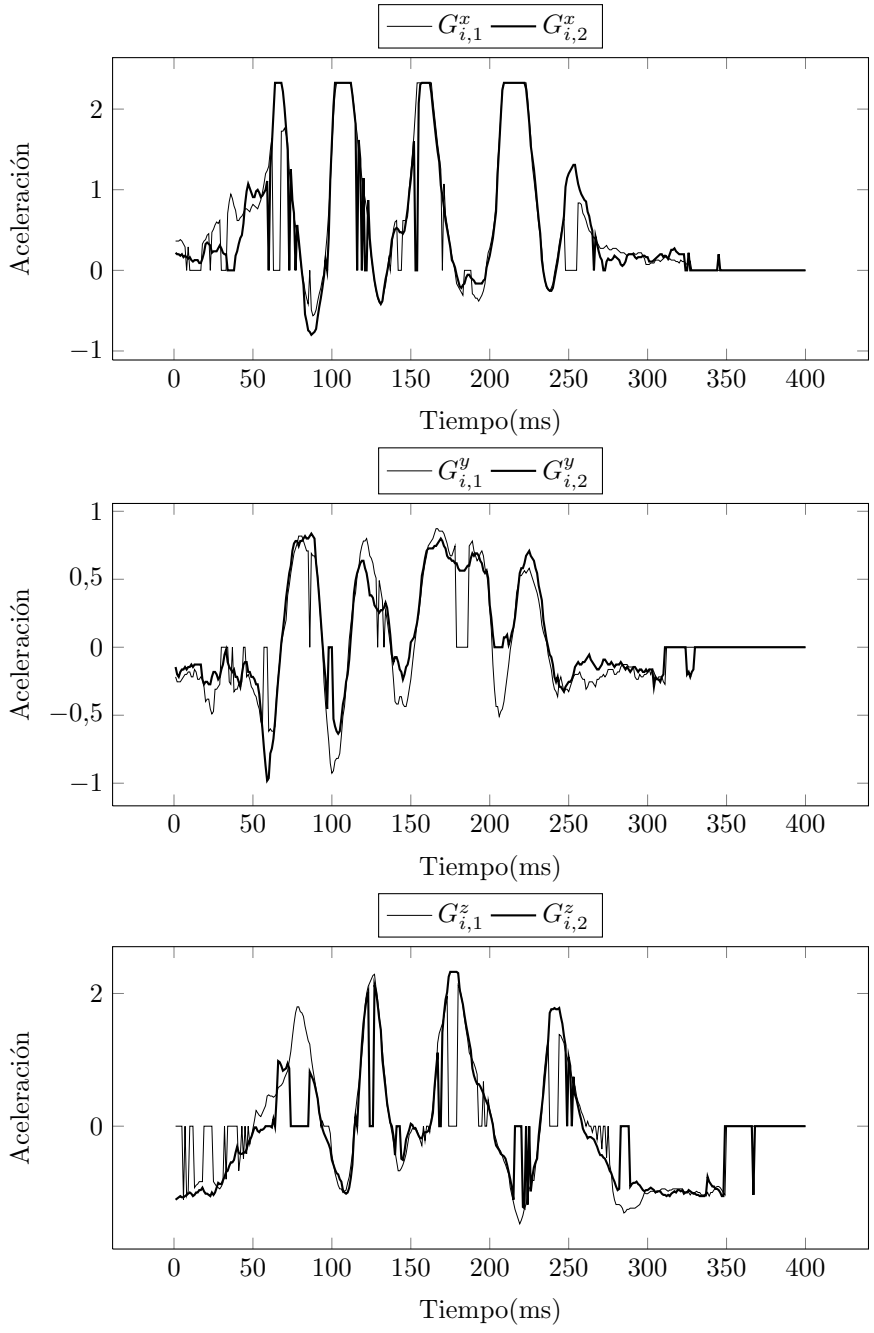


Figura 6.2: Ejemplo de aplicar el algoritmo de alineamiento global modificado a dos repeticiones de la misma firma realizada por el mismo usuario.

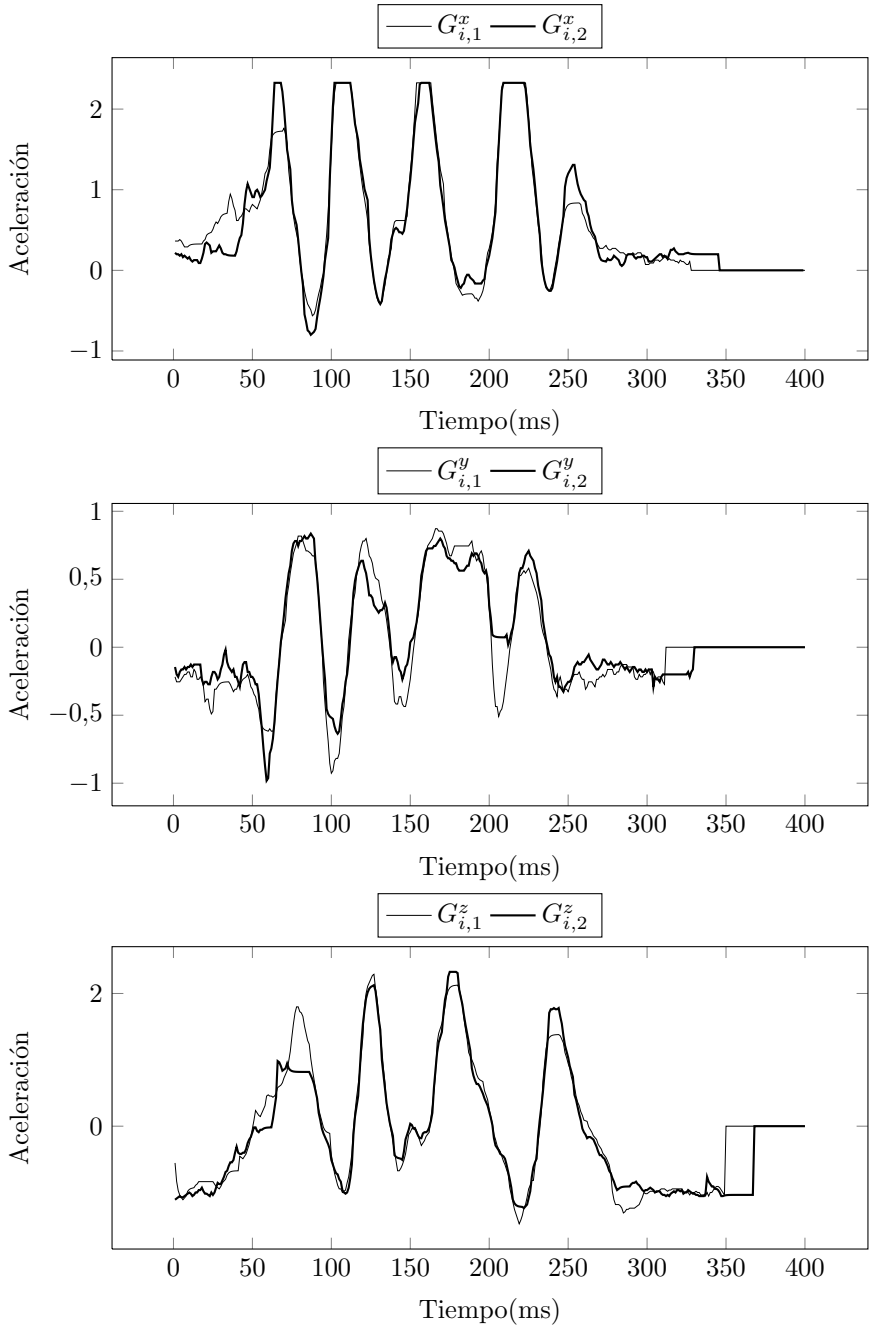


Figura 6.3: Resultado del análisis completo (alineamiento + interpolación) de dos repeticiones de la misma firma realizada por el mismo usuario

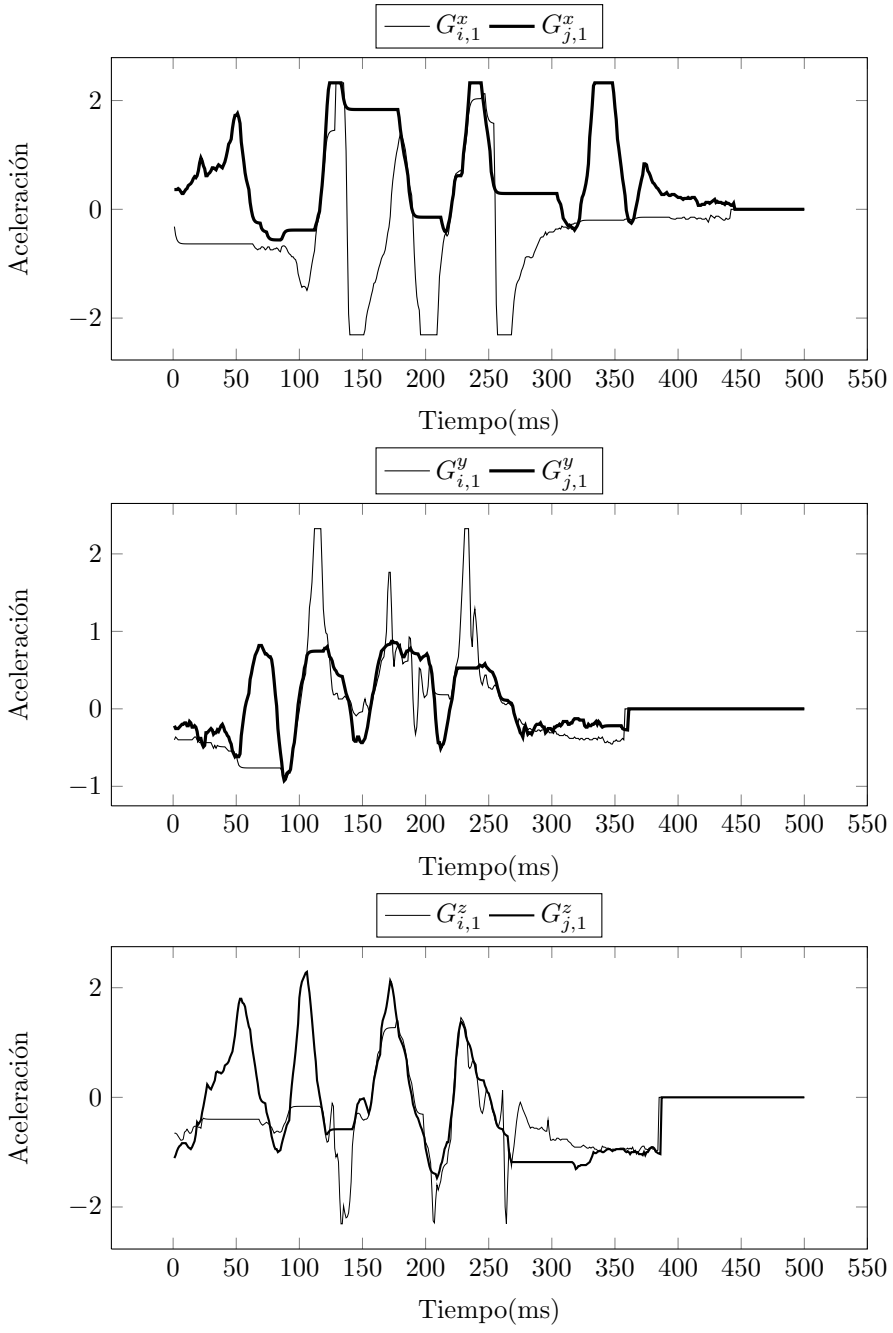


Figura 6.4: Resultado del análisis completo (alineamiento + interpolación) de dos repeticiones de distintas firmas realizadas por usuarios diferentes.

Capítulo 7

Obtención de una base de datos biométrica de firmas en el aire

En este capítulo se presenta una parte fundamental del trabajo, la Base de Datos biométrica que se ha utilizado para corroborar los resultados de la técnica biométrica basada en firmas en el aire propuesta en el trabajo de investigación.

Para este trabajo de investigación se ha obtenido una base de datos privada con personas voluntarias que han accedido a realizar una firma identificativa en el aire con un iPhone. Las bases de preparación de esta base de datos se encuentran explicadas en la Sección 7.1.

Con estas bases, se ha obtenido finalmente una base de datos de las características explicadas en la Sección 7.2 que se ha utilizado para validar la técnica biométrica propuesta.

Además, se ha incluido la Sección 7.3 donde se presentan cómo los distintos usuarios han reaccionado al problema de realizar una firma identificativa en el aire con ciertas condiciones de seguridad, y qué soluciones de gestos han adoptado.

7.1. Preparación de la Base de Datos

La construcción de la base de datos biométrica se ha construido siguiendo las recomendaciones de la norma ISO/IEC JTC 1/SC 37. La base de datos consta de dos tipos de sesiones: Sesiones en las que usuarios proporcionan sus datos biométricos (firmas en el aire) y sesiones en los que distintos usuarios tratan de falsificar los datos biométricos de otros. Cada uno de los tipos de sesiones se ha tomado siguiendo distintos pasos, que se explicarán a continuación.

7.1.1. Definición de la sesión de toma de muestras originales

La definición de los experimentos para obtener los datos biométricos necesarios para esta tarea incluyen dos sesiones separadas en el tiempo al menos un mes cada una: (Nota: En el momento de la presentación de este trabajo de fin de máster sólo se ha realizado la primera de ellas)

- 1ª Sesión (20 mins): La sesión se compone de los siguientes pasos:

    1. Firma de documento LOPD: Se ha realizado un documento que cada usuario debe firmar autorizando la recogida de datos biométricos de firmas en el aire, y su correspondiente utilización para la investigación
    2. Explicación de la obtención de gestos: Se le dan al usuario las instrucciones de enrolamiento en el sistema mediante la realización de un gesto en el aire. Se explica al usuario que va a tener que inventarse una firma que pueda ser identificativa suya y que pueda repetir con facilidad. El usuario va a tener que repetir su firma en el aire 8 veces. Además, se le informa al usuario que la sesión será grabada en vídeo, para poder realizar la fase de falsificación de firmas más adelante.
    3. Realización del gesto identificativo en el aire: El usuario tiene un tiempo ilimitado para inventarse un gesto acorde a las instrucciones. Una vez pensado, accede a una aplicación programada en el iPhone para recogida de datos de realizaciones de gestos (Explicada en la Sección 10.1). Utilizando dicha aplicación ejecuta 8 veces su firma, con un intervalo de repetición entre cada muestra de 10-15 segundos, para disminuir la dependencia de los datos.
    4. Relleno de una encuesta: Se le pide al usuario que rellene una encuesta (Sección 8.1) para ver el grado de aceptación y otras características de la técnica biométrica basada en firma en el aire.

- 2ª Sesión (15 mins):

    1. Repetición de firmas: A cada persona se le muestran sus propios vídeos para ayudarle a recordar la firma que hizo. Con esa ayuda, tratan de repetirla otras 6 veces.
    2. Encuesta: Los usuarios responden si ha sido fácil repetir el gesto y si creen que lo han hecho de manera similar a anteriormente.

7.1.2. Definición de la sesión de falsificaciones

La base de datos biométrica se completará con intentos de falsificaciones de cada uno de los gestos realizados por los usuarios originales. Para ello, tres falsificadores han tratado de imitar cada uno de los gestos originales que componen la base de datos en dos escenarios posibles:

- Observando al usuario realizar el gesto (1ª fase): Esta situación se corresponde con la posibilidad de que una persona en la calle pueda realizar el gesto y cualquier otro trate de imitarle en base a lo que ha visto. Este escenario se simula haciendo que el falsificador vea una vez a la persona haciendo su gesto original en el vídeo que se grabó en su sesión.
- Estudiando cómo el usuario realiza el gesto (2ª fase): Esta situación se corresponde con una persona que trate de estudiar cómo realiza una persona su gesto. Para ello, el falsificador va a poder ver el número de veces que quiera el vídeo de la persona realizando su gesto y un tiempo ilimitado para tratar de imitarle.

Por cada firma original en la base de datos, cada falsificador realizará tres intentos de imitación de la firma según la fase de observación, y a continuación, cuatro repeticiones habiendo estudiado en profundidad la grabación de la ejecución de la firma por el usuario original.

Para almacenar las distintas falsificaciones de cada uno de los gestos de cada usuario de manera ordenada Se ha desarrollado una aplicación específica para el iPhone, descrita en la Sección 10.2 .

7.2. Características de la base de datos obtenida

Para esta base de datos, se ha contado con la colaboración de 40 personas que han accedido a realizar una firma en el aire con un dispositivo móvil (iPhone), haciendo uso de la aplicación desarrollada para tal fin.

Asimismo, 3 personas han participado como falsificadores, tratando de imitar cada una de las firmas en el aire a partir de los vídeos donde estaban grabadas las realizaciones originales de cada usuario, según las fases explicadas anteriormente.

En conclusión, se ha obtenido una base de datos de firmas en el aire de las siguientes características:

Tabla 7.1: Resumen de las características de la base de datos de firmas en el aire

Número de usuarios originales	40
Número de repeticiones de cada firma original	8
Total de muestras originales	320
Número de falsificadores	3
Firmas falsificadas	40
Número de repeticiones de cada firma original (1ª Fase)	3
Número de repeticiones de cada firma original (2ª Fase)	4
Número de muestras de firmas falsificadas (1ª Fase)	360
Número de muestras de firmas falsificadas (2ª Fase)	480
Número Total de muestras de firmas falsificadas	840

7.3. Tipos de firmas que solían hacer los usuarios

Los usuarios han inventado sus firmas en el aire a partir de los requerimientos que se les han solicitado, es decir, firmas que fueran capaces de recordar y repetir pero a su vez suficientemente complejas para no ser imitados a simple vista. Ante estos requisitos, los usuarios han realizado distintos tipos de firmas que pueden clasificarse en los siguientes grupos:

- Escribir una palabra/número en el aire.
- Realizar un gesto que realizan habitualmente: Tocar la guitarra, jugar al tenis, un saludo, etc.
- Dibujar un símbolo en el aire: Una estrella, una arroba, una clave de sol, etc.
- Realizar un gesto complejo concatenando gestos simples: cuadrados, triángulos, círculos, etc.
- Dibujar algo que exista en el aire: árboles, nubes, etc.
- Firmar con su propia firma manuscrita en el aire.

Capítulo 8

Valoración de la técnica biométrica por el usuario final

Desde el punto de vista de un desarrollador de aplicaciones y sistemas biométricos, no se puede olvidar al usuario final, que es el que acabará utilizando el sistema. Por ello, se ha incluido este capítulo, donde los usuarios finales que han participado en la obtención de muestras de la base de datos de firmas en el aire, dan su opinión sobre distintos aspectos de la técnica.

Para ello, en la Sección 8.1, se muestra la encuesta que se ha pedido que rellenen los usuarios para conocer sus impresiones sobre distintos aspectos de la técnica que se les ha presentado. Hay que tener en cuenta que estos usuarios no son expertos en el tema de biometría, por lo que su valoración de la seguridad de la técnica no tiene por qué coincidir con los resultados experimentales. Aún así, este estudio es importante puesto que un usuario va a utilizar un sistema si su percepción de la seguridad del mismo es alta, sin ser tan importante que en realidad lo sea.

Las respuestas a las encuestas se presentan en la Sección 8.2 y son analizadas en profundidad en la Sección 8.3. Como consecuencia de este análisis, pueden extraerse ciertas conclusiones de la valoración de la técnica biométrica por los usuarios finales, presentadas en la Sección 8.4.

8.1. Encuesta presentada a los usuarios

La encuesta que han tenido que rellenar los participantes en la obtención de la base de datos es la siguiente:

Valora del 1 al 5 las siguientes características de la prueba realizada:

1. Facilidad para inventarse un gesto (1 muy fácil - 5 muy difícil):

   ¿Ha sido fácil inventarte un gesto que puedas utilizar como firma en 3D?

2. Facilidad para repetir el gesto en la misma sesión (1 muy fácil - 5 muy difícil):

   ¿Has podido repetir el gesto con facilidad?

3. Facilidad para repetir el gesto inventado en la próxima sesión (1 muy fácil - 5 muy difícil):

   Enseñándote el vídeo en otra sesión, ¿crees que puedes repetir el gesto con facilidad?

4. Facilidad para hacer tu firma manuscrita en el aire (1 muy fácil - 5 muy difícil):

   ¿Ha sido fácil reproducir tu firma cotidiana con el iPhone en el aire?

5. Facilidad para repetir la firma en la misma sesión (1 muy fácil - 5 muy difícil):

   ¿Has podido repetir tu firma con facilidad?

6. Facilidad para repetir la firma en la próxima sesión (1 muy fácil - 5 muy difícil):

   Enseñándote el vídeo en otra sesión, ¿crees que puedes repetir tu firma con facilidad?

7. Aceptación de la técnica gestual (1 muy aceptada - 5 muy poco aceptada)

   ¿Qué esfuerzo supone que alguien te recoja el patrón gestual? Ej. Mucha aceptación: Reconocimiento de voz en el que tienes que hablar por un micrófono. Ej. Poca aceptación: Dar el ADN.

8. ¿Consideras el reconocimiento gestual una técnica invasiva? (1 poco invasiva - 5 muy invasiva)

   ¿Te ha supuesto un esfuerzo muy grande realizar el gesto con el iPhone? Ej. de muy invasivo: Una técnica que te llena la cabeza de sensores Ej. de poco invasivo: Ponerse delante de una cámara para hacerte una foto de la cara

9. Facilidad de falsificación por observación (1 muy fácil - 5 muy difícil):

   ¿Crees que es fácil que otra persona falsifique los gestos que has realizado observándote una vez?

10. Facilidad de falsificación por estudio (1 muy fácil - 5 muy difícil)

    ¿Crees que es fácil que otra persona falsifique los gestos que has realizado observándote varias veces?

11. ¿Qué grado de confianza te da la técnica biométrica gestual? (1 muy poca - 5 mucha)

12. Ordena de menor confianza (1) a mayor confianza (6) las siguientes técnicas biométricas:

- Reconocimiento por iris:
- Reconocimiento de firma manuscrita:
- Reconocimiento gestual:
- Reconocimiento facial:
- Reconocimiento de huella dactilar:
- Reconocimiento de mano:

8.2. Respuestas de los usuarios a la encuesta

Las respuestas de los usuarios a la encuesta anterior pueden observarse en la Tabla 8.1, donde se han presentado los valores promedios de las respuestas de todos los usuarios que han participado en la obtención de la base de datos. Asimismo, se presentan los valores estadísticos de la moda, correspondiente a la respuesta obtenida un mayor número de veces, y la desviación, representando cómo de agrupadas han sido las respuestas.

Tabla 8.1: Respuestas de la encuesta

Nº Pregunta	Media	Moda	Desviación
1	2.1	2	0.65
2	1.9	2	0.45
3	2.7	2	0.82
4	2.4	3	0.91
5	2.1	2	0.6
6	2.1	2	0.65
7	1.9	1	0.71
8	1.6	1	0.6
9	3.8	4	0.85
10	2.9	3	0.80
11	3.3	4	0.85
12a	4.9	6	1.23
12b	2.6	1	1.23
12c	2.7	2	1.28
12d	3.2	4	1.27
12e	4.5	5	1.15
12f	3.3	4	0.99

8.3. Análisis de las respuestas de los usuarios.

- Preguntas 1, 2 y 3: El usuario no ha tenido apenas dificultad en inventar un gesto acorde a las características solicitadas ni en repetirlo en la misma sesión. El usuario tiene incertidumbre sobre si va a ser capaz de repetirlo

en el futuro. Es una incertidumbre normal puesto que no es un gesto que se realiza todos los días, como la firma manuscrita; en el caso de haber realizado una toma de muestras cada día, esta incertidumbre sería mucho más baja, puesto que el usuario habría asimilado perfectamente cómo realizar su gesto de la misma manera que tiene asimilado cómo firma documento.

- Preguntas 4, 5 y 6: En este caso, el usuario tiene más seguridad en ser capaz de repetir el gesto en el futuro, puesto que es un gesto que ya tiene aprendido. Por otro lado, la realización de la firma en el aire, aún siendo generalmente fácil, resulta raro a la gente puesto que cambia la manera que tiene uno mismo de hacerlo.

- Pregunta 7: La técnica es bastante aceptada por los usuarios.

- Pregunta 8: Los usuarios consideran la técnica gestual muy poco invasiva.

- Pregunta 9 y 10: Los usuarios consideran bastante difícil falsificar sus gestos si alguien les ve por la calle, pero esa seguridad baja si alguien tiene grabado cómo lo hace y les estudia. En cualquier caso, no consideran fácil, a pesar del estudio, que un falsificador pueda imitar su gesto correctamente.

- Pregunta 11: La técnica de reconocimiento gestual proporciona una confianza buena en los usuarios.

- Pregunta 12: Los usuarios tienen una confianza un poco superior en la técnica de reconocimiento gestual que la técnica de firma manuscrita. Los usuarios conceden una confianza mayor y más o menos superior a la técnica de mano. A los usuarios les da mucha mayor confianza las técnicas de iris y huella dactilar.

8.4. Conclusiones de la aceptabilidad de la técnica

Las reacciones de los usuarios pueden resumirse con las siguientes ideas:

- Sencillez: A los usuarios les ha resultado bastante sencillo inventar y repetir una firma en el aire con un dispositivo móvil.

- Colectividad: Los usuarios evalúan la colectividad como buena debido a que los datos biométricos se adquieren de manera no intrusiva.

- Aceptabilidad: Los usuarios se sienten seguros y cómodos cuando las características biométricas se extraen.

- Confianza: Seguridad media, por encima de la firma manuscrita debido a que no hay un plano de referencia (papel) donde poder observar con facilidad los trazos de la firma. Asimismo, los usuarios consideran muy complicado imitar una firma en el aire al observar a otra persona hacer su firma original en directo.

Capítulo 9

Resultados experimentales

En este capítulo se presentan los resultados experimentales que verifican la validez de la técnica biométrica propuesta, en base a distintos experimentos.

En primer lugar, la Sección 9.1 muestra los resultados de un primer experimento con una base de datos de firmas en el aire previa (número de firmas y muestras de cada una reducidos), en los que se trata de optimizar el algoritmo de análisis de señales de aceleración biométrica, obteniendo un primer resultado interesante sobre la unicidad de las distintas firmas en el aire.

Una vez optimizado el algoritmo, la Sección 9.2 muestra los resultados de una serie de experimentos que se han realizado para verificar la fiabilidad de esta técnica biométrica, así como para encontrar el escenario de fusión de información que reduce la tasa de error EER del sistema, para la base de datos obtenida en el Capítulo 7.

Además, la Sección 9.3 presenta los tiempos de procesamiento necesarios para ejecutar cada uno de los escenarios en un ordenador personal y directamente en un dispositivo móvil.

Por último, la Sección 9.4 analiza todos los resultados obtenidos en los experimentos de este capítulo.

9.1. Optimizacion h y σ

Para optimizar los parámetros h y σ del algoritmo explicado en el Capítulo 6, se ha utilizado una Base de Datos de firmas previa, formada por 30 personas que hicieron cuatro veces un gesto en el aire con un iPhone conectado a un ordenador, donde podían verse los valores de las aceleraciones de cada eje directamente desde el Terminal de operaciones para desarrollar aplicaciones para el iPhone.

A partir de esta pequeña base de datos, se definió el siguiente experimento que se repitió para distintos valores de h y σ, para obtener los valores de EER (Ver Sección 2.5):

- Para cada firma, se tomaban tres de las cuatro repeticiones de la base

de datos, para conformar el patrón biométrico, siguiendo el método matemático explicado en 6.3.

- Para cada patrón biométrico correspondiente a cada usuario, la repetición de la firma no utilizada para formar el patrón se utilizaba como un intento de acceso del usuario original. El resto de firmas del resto de usuarios se utilizaban como intento fraudulento de acceso.

- Todo lo anterior se repetía para cada conjunto de tres firmas originales para cada usuario. Es decir, para cada usuario se repetía cuatro veces el experimento, uno por cada posible combinación de las cuatro firmas que se tenían, de tres en tres elementos.

- A partir de estos cálculos se calculaba la Tasa de Errores de Aceptación (FAR: False Acceptance Rate) para distintos valores de un umbral. Según el valor del umbral de acceso o rechazo de un usuario, se contaban el número de accesos que no deberían haber accedido al sistema.

- De manera similar, se calculaba la Tasa de Errores de Rechazo (FRR: False Rejection Rate) como los valores originales que eran rechazados por el sistema al ir incrementando el valor del umbral de decisión.

- El punto de corte entre las dos curvas, es el Equal Error Rate (EER) que representa el punto óptimo de decisión del umbral para tener un error total mínimo.

Este experimento se ha repetido para distintos valores de h y σ, obteniendo los resultados presentados en la Tabla 9.1:

Tabla 9.1: Resultados de EER (%) para distintas configuraciones de h y σ.

h/σ	**0.1**	**0.15**	**0.2**	**0.25**	**0.3**	**0.35**	**0.4**	**0.45**	**0.5**
0.075	3.02	2.45	2.05	2.25	1.97	2.22	2.87	3.20	3.62
0.150	4.35	3.53	2.43	2.88	2.88	2.15	2.89	2.26	2.32
0.225	3.79	2.22	1.92	2.11	1.92	2.89	1.92	1.92	1.92
0.3	3.86	3.02	2.33	1.92	1.92	1.92	1.92	1.92	1.92

Observando los resultados de dicha tabla, puede comprobarse que la configuración seleccionada en la Sección 6.5.1 de $h = 0{,}4$ y $\sigma = 0{,}225$ es una de las óptimas, ya que el resultado obtenido de EER es el menor de todos. En la Figura 9.1 se representan las gráficas de FAR y FRR para la configuración de h y σ elegida, así como el punto de corte EER obtenido.

Los resultados de este experimento se corresponden con una prueba de falsificación "Zero-Effort", en la que los falsificadores tratan de acceder al sistema utilizando su propia firma, en vez de tratando de imitar la firma del usuario original. Un resultado de EER de 1.92 % en este tipo de prueba es muy competitivo respecto a otros trabajos similares de firma manuscrita [23], [11], [37].

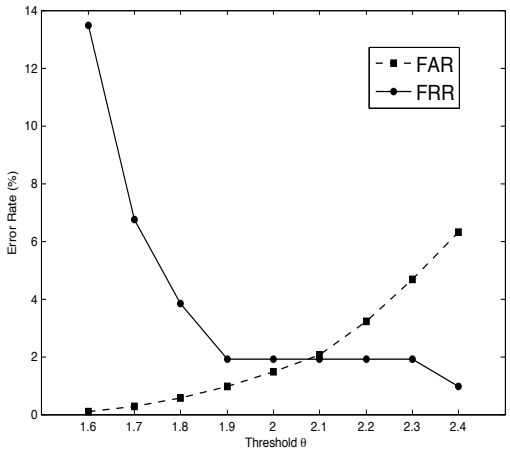


Figura 9.1: Tasa de error EER obtenida (%) para una configuración de $h = 0{,}4$ y $\sigma = 0{,}225$.

9.2. Resultados de analizar la base de datos de firmas en el aire

En esta Sección se presentarán los resultados de analizar, en distintos escenarios de fusión de información (Sección 6.5), las muestras de la base de datos de firmas en el aire, cuya obtención y características se describieron en el Capítulo 7.

Para todos los escenarios, se utilizará la configuración de $h = 0{,}4$ y $\sigma = 0{,}225$, óptima para otros datos de firmas en el aire distintos a los que se encuentran en esta base de datos. De esta manera, se cumple uno de los requisitos fundamentales de los experimentos científicos: los conjuntos de muestras de validación y entrenamiento han de ser distintos, y por tanto, no se pueden utilizar las muestras de entrenamiento para probar el sistema.

Para cada escenario, se va a calcular el EER con un procedimiento similar al explicado en la Sección 9.1, con la única diferencia, que en estos casos, se utilizarán muestras de falsificación de cada firma original como intentos de acceso que el sistema debe reconocer como fraudulentos (en vez de las muestras de firmas originales de otros usuarios).

Los escenarios que resultados de los distintos escenarios que se han estudiado se van a organizar de la siguiente manera. Se van a presentar los resultados en tres apartados según el número de ejes de aceleración que se hayan utilizado: uno, dos o los tres. En cada apartado, se presentará por separado los distintos escenarios de fusión de la información que se han estudiado.

Para todos los escenarios, se define L como la longitud inicial de las señales de aceleración en cada eje, y T_E el tiempo de ejecución del algoritmo.

9.2.1. Experimentos con las señales de aceleración de los tres X-Y-Z

En estos experimentos, se utiliza toda la información extraída de cada repetición de una firma (aceleraciones en el eje X, Y y Z). Se han estudiado tres posibles casos dependiendo el punto en el que se fusionen estas señales:

Experimento 1. Fusión a nivel de decisión.

En este escenario, el algoritmo se ejecuta tres veces, una por cada eje de aceleración de manera separada. La información se fusiona a nivel de decisión, calculando la media del resultado de cada análisis de cada par de señales. En este caso, se obtiene la tasa de Error EER de la Figura 9.2 correspondiente a un 2.5 %.

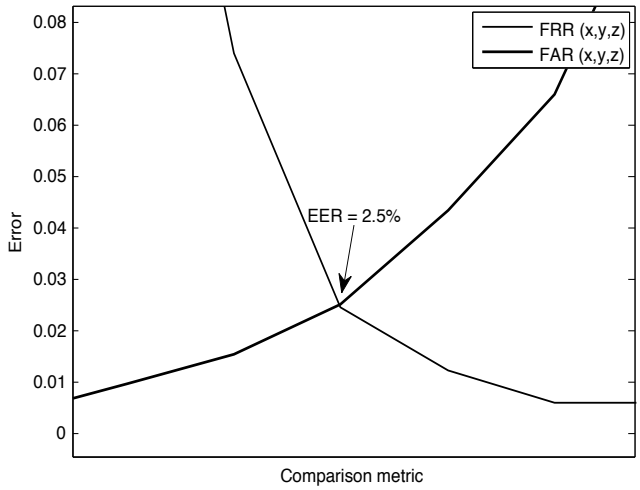


Figura 9.2: Tasa de error EER obtenida (%) al fusionar las señales de los ejes X, Y y Z a nivel de decisión.

El tiempo consumido en este escenario para cada comparación de dos repeticiones de firmas es equivalente a tres veces la ejecución del algoritmo con dos señales de longitud L ($3T_E(L)$).

Experimento 2. Fusión a nivel de comparación.

En este escenario el análisis de las señales en cada eje se hace por separado, pero en paralelo, uniendo la información en el momento de calcular el valor que representa la diferencia de dos firmas que devuelve el algoritmo. En este

experimento se ha obtenido un valor de EER de 3.3 %, representado en la Figura 9.3.

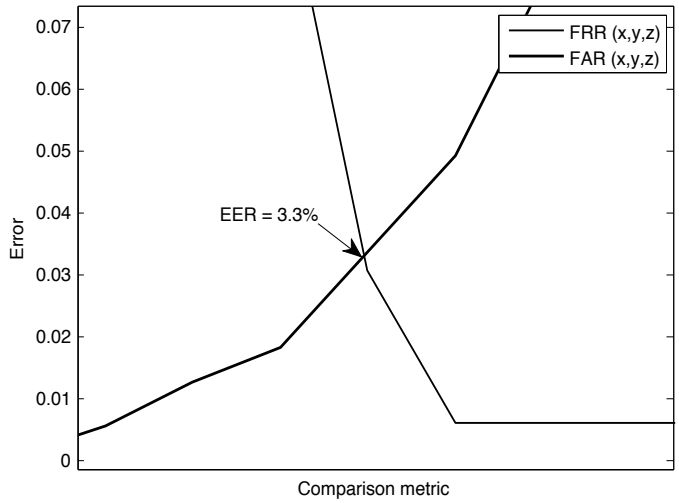


Figura 9.3: Tasa de error EER obtenida (%) al fusionar las señales de los ejes X, Y y Z a nivel de comparación.

En este contexto, el tiempo consumido en comparar dos muestras de firmas es, de nuevo, equivalente a tres veces la ejecución de un algoritmo con dos señales de longitud L ($3T_E(L)$).

Experimentos 3 y 4. Fusión a nivel de extracción de características

Estos experimentos se basan en el preprocesamiento de las señales para ejecutar una única vez el algoritmo. Las diferentes opciones que se han estudiado son:

1. Experimento 3. Concatenar las señales de los ejes X, Y y Z.

   Al concatenar las señales en el orden X-Y-Z se ha obtenido el resultado de EER de 2.7 % que puede visualizarse en la Figura 9.4. Otros órdenes de posicionamiento de las señales no mejoran este resultado. En este caso, el tiempo necesario para procesar un par de muestras de firmas en el aire equivale a la ejecución una vez del algoritmo con señales de longitud $3L$ ($T_E(3L)$).

2. Experimento 4. Calcular el módulo de las señales de los ejes X, Y y Z.

   Al calcular el módulo de las señales X, Y y Z en cada punto, se pierde información distintiva de las señales, obteniéndose una tasa de error EER

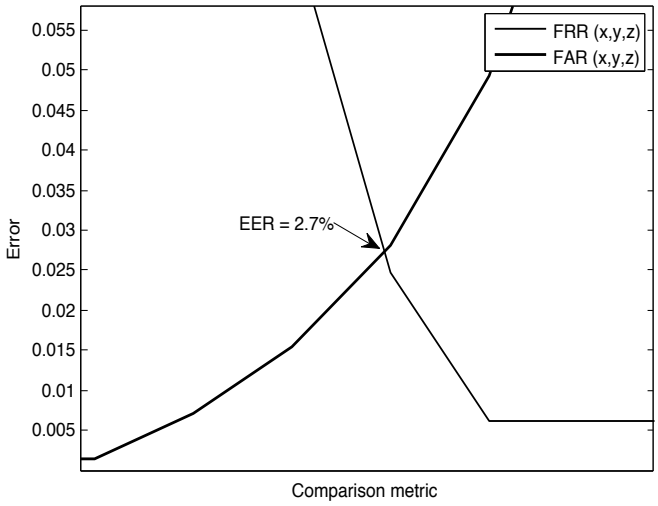


Figura 9.4: Tasa de error EER obtenida (%) al concatenar las señales de los ejes X, Y y Z.

de 13.6 %, que puede observarse en la Figura 9.5. El tiempo consumido en este escenario se reduce a una ejecución del algoritmo con señales de longitud L ($T_E(L)$).

9.2.2. Experimentos con señales de aceleración en dos ejes (X-Y, X-Z, Y-Z)

En esta Subsección se presentan los experimentos llevados a cabo únicamente con las señales de dos de los ejes de aceleración de las muestras de firmas en el aire de la base de datos. En cada figura de los resultados de los siguientes escenarios se presentarán las tasas de EER de analizar cada posible par de señales X-Y, X-Z y Y-Z de manera separada.

Experimento 5. Fusión a nivel de decisión.

Este escenario corresponde con el Experimento 1, pero en este caso la fusión de la información se realiza únicamente a partir del resultado del análisis de dos ejes. Con estas hipótesis, se han obtenido unas tasas de EER de 2.98 %, 4.35 % y 4.29 % para el análisis de las señales X-Y, X-Z y Y-Z respectivamente (Figura 9.6). El tiempo consumido en este experimento es equivalente a la ejecución dos veces (en vez de tres) del algoritmo con dos señales de longitud L ($2T_E(L)$).

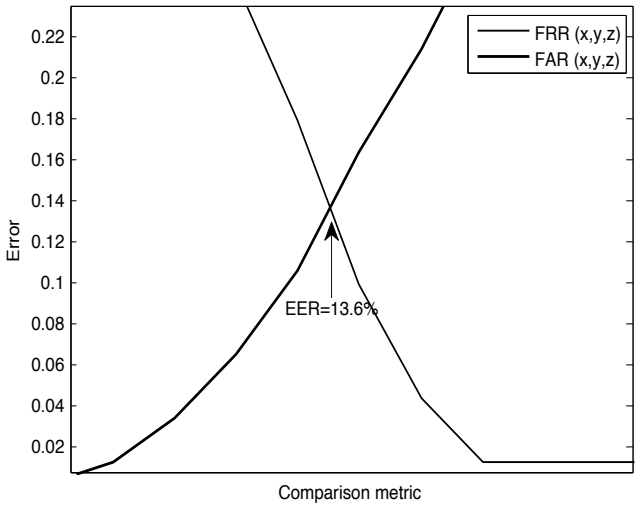


Figura 9.5: Tasa de error EER obtenida (%) al calcular el módulo de las señales de los ejes X, Y y Z.

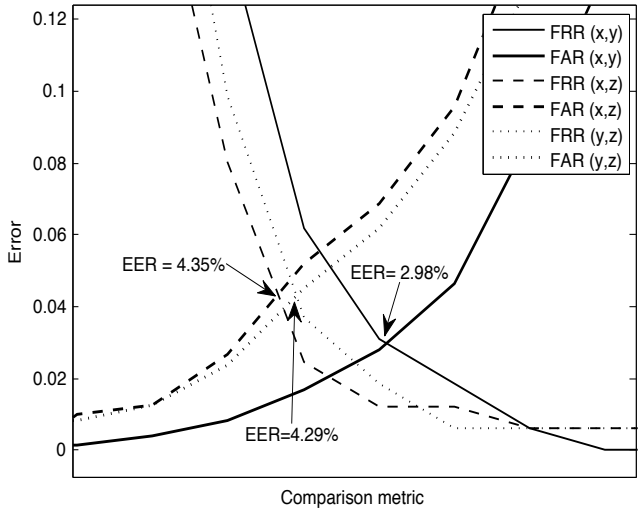


Figura 9.6: Tasas de error EER obtenidas (%) al fusionar las señales de dos ejes a nivel de decisión.

Experimento 6. Fusión a nivel de comparación.

Este experimento es análogo al Experimento 2, donde la información se fusiona a nivel de comparación, ejecutando el algoritmo en cada eje por separado

y calculando de manera conjunta un único valor de diferencia entre las muestras de firmas en el aire completas. Con ello, se han conseguido unas tasas de EER (X-Y: 3.57 %, X-Z: 4.88 %, Y-Z: 4.58 %) representados en la Figura 9.7. Este experimento consume un tiempo equivalente a dos veces la ejecución del algoritmo con dos señales de longitud L ($2T_E(L)$).

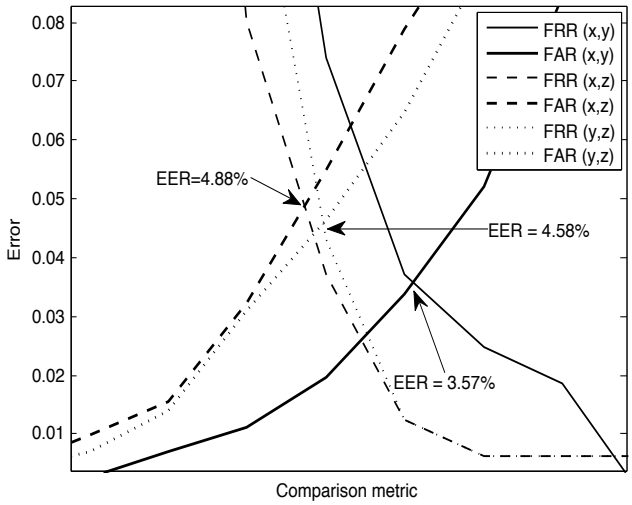


Figura 9.7: Tasas de error EER obtenidas (%) al fusionar las señales de dos ejes a nivel de comparación.

Experimentos 7 y 8. Fusión a nivel de extracción de características

Estos dos experimentos se basan en el preprocesamiento de las señales de dos ejes. Las diferentes opciones que se han estudiado son:

1. Experimento 7. Concatenar las señales de dos ejes.

   Al concatenar dos señales de longitud L se genera una nueva de longitud $2L$. Al ejecutar el algoritmo con estas señales, se obtienen los resultados de EER de 2.85 % (X-Y), 6.42 % (X-Z) y 5 % (Y-Z), según las señales que se analicen. (Figura 9.8). El tiempo requerido en este experimento es equivalente a una ejecución del algoritmo con dos señales de longitud $2L$ ($T_E(2L)$).

2. Experimento 8. Calcular el módulo de las señales de dos ejes.

   En este escenario se calcula el módulo de las señales de dos ejes punto a punto, obteniéndose los resultados de EER de X-Y: 7.41 %, X-Z: 13.78 % y Y-Z: 12.07 %, representados en la Figura 9.9. Este experimento no reduce

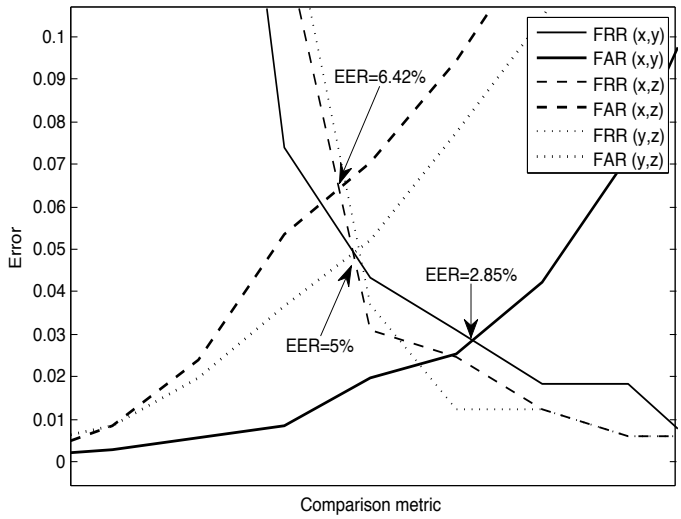


Figura 9.8: Tasas de error EER obtenidas (%) al concatenar las señales de dos ejes.

el tiempo consumido del experimento equivalente a la utilización de tres señales, puesto que se requiere una ejecución del algoritmo con señales de longitud L ($T_E(L)$).

9.2.3. Experimentos con una señal aceleración en un único eje (X, Y o Z).

Finalmente, este experimento estudia el comportamiento del sistema cuando se utiliza únicamente la señal de aceleración de un eje. En este caso no hay necesidad de fusionar información, puesto que sólo se utiliza una señal.

La Figura 9.10 muestra los resultados de ejecutar el algoritmo solo con las señales del eje X (4.34 %), Y (7.28 %) y Z (7.98 %). En este caso, los resultados obtenidos al analizar las aceleraciones en el eje X son los mejores, por lo que puede concluirse que la información en este eje ofrece la información más distintiva de las firmas en el aire.

9.3. Tiempo de ejecución de cada experimento

Los distintos tiempos de procesamiento de los escenarios de cada experimento se presentan en la Tabla 9.2. Cada experimento se ha ejecutado en un iMac a 2.4 Ghz con 1 Gb de memoria RAM. Los tiempos mostrados en la tabla se corresponden con el tiempo necesario para realizar el análisis completo de dos firmas en el aire, con el número de ejecuciones y longitud de las señales variables,

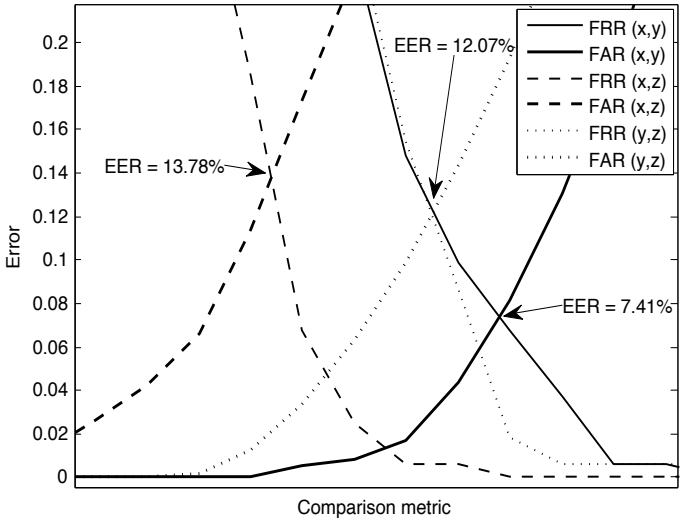


Figura 9.9: Tasas de error EER obtenidas (%) al calcular el módulo de las señales de dos ejes.

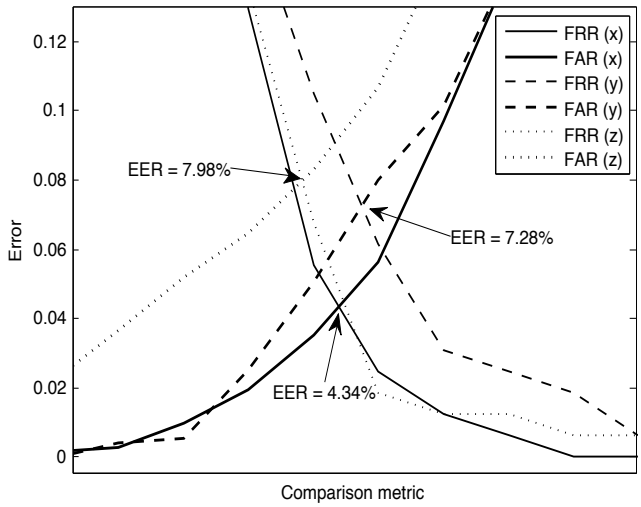


Figura 9.10: Tasas de error EER obtenidas (%) analizando la señal de un único eje.

dependiendo del escenario a estudiar. Además, se ha medido el tiempo en anali-

Tabla 9.2: Tiempo de procesamiento de dos firmas en el aire para cada escenario de fusión de información

Experimento	Tiempo de ejcución (s)	Tiempo en MAC (ms)	Tiempo en iPhone (s)
1: Decisión 3S	$3T_E(L)$	94.2	4.515
2: Comparación 3S	$3T_E(L)$	94.2	4.515
3: Concatenación 3S	$T_E(3L)$	287	13.94
4: Módulo 3S	$T_E(L)$	31.4	1.505
5: Decisión 2S	$2T_E(L)$	62.8	3.01
6: Comparación 2S	$2T_E(L)$	62.8	3.01
7: Concatenación 2S	$T_E(2L)$	114	6.263
8: Módulo 2S	$T_E(L)$	31.4	1.505
9: Una señal 1S	$T_E(L)$	31.4	1.505

zar dos señales con todo el procesamiento realizado en un iPhone. Los resultados presentados son valores medios, obtenidos al hacer una media aritmética de los valores de tiempos de procesamiento de 20 comparaciones de firmas completas.

Evidentemente, los tiempos de procesamiento en un ordenador son mucho menores que en un dispositivo móviles, debido a su gran velocidad. De hecho, puede comprobarse como en un teléfono móvil, el mismo procesamiento tarda unas 50 veces más en ejecutarse.

A pesar de ello, la opción de realizar todo el procesamiento en el propio dispositivo móvil mantiene grandes ventajas que la hacen más interesante frente a otra hipotética configuración en la que las señales de las firmas en el aire se mandan a un servidor externo que procesa la información más rápido.

Estas ventajas por las que somos capaces de perder velocidad de procesamiento se resumen en dos:

- Seguridad: Al realizar todo el procesamiento en el teléfono móvil no hay tráfico de información que puede robarse.
- Aplicaciones off-line: Permite utilizar esta técnica biométrica para aplicaciones donde no se necesite una conexión de internet, como el acceso al teléfono o a alguna de sus aplicaciones, o donde no se quiera que se utilice dicha conexión sin haberse autenticado con esta técnica biométrica primero.

9.4. Análisis de los resultados

La Tabla 9.3 resume los resultados de EER y tiempos de procesamiento de cada uno de los escenarios estudiados. En dicha tabla se adjuntan únicamente los tiempo de ejecución en un iPhone.

Analizando estos resultados, pueden extraerse las siguientes conclusiones.

- Si se requiere una estrategia lo más rápida posible (1.505 s), la mejor opción es analizar únicamente las aceleraciones en el eje X, ya que es la

Tabla 9.3: Resumen de los resultados de EER y tiempos de procesamiento de los escenarios de fusión estudiados.

Experimento	Tiempo de ejecución (s)	Resultados de EER %
1: Decisión 3S	4.515	2.52
2: Comparación 3S	4.515	3.32
3: Concatenación 3S	13.94	2.73
4: Módulo 3S	1.505	13.62
5: Decisión 2S	3.01	2.98(X-Y);4.35(X-Z);4.29 (Y-Z)
6: Comparación 2S	3.01	3.57(X-Y); 4.88(X-Z);4.58(Y-Z)
7: Concatenación 2S	6.263	2.85(X-Y);6.42(X-Z);5(Y-Z)
8: Módulo 2S	1.505	7.41(X-Y);13.78(X-Z);12.07(Y-Z)
9: Una señal 1S	1.505	4.34(X);7.28(Y);7.98(Z)

que obtiene el menor valor de EER 4.34 %, mejorando en un 3 % las tasas de error de los ejes Y y Z.

- La tasa de EER puede reducirse a un 2.98 % fusionando las aceleraciones de los ejes X e Y a nivel de decisión, consumiendo 3.01 segundos.
- La tasa menor de EER (2.52 %) se ha obtenido fusionando la información de los ejes X, Y y Z a nivel de decisión, durando este proceso 4.515 segundos.
- Otros escenarios con un tiempo de procesamiento mayor no han ofrecido mejores resultados.
- El cálculo del módulo de las señales de aceleración de cada eje no ofrece buenos resultados, ya que la información distintiva de la firma en el aire se confunde con información de otros ejes.
- Reducir el número de ejecuciones de un algoritmo concatenando las señales produce también resultados de EER bajos, pero incrementa de manera exponencial el tiempo de procesamiento, por lo que no es una estrategia que compense.

En conclusión, la mejor estrategia de fusión de información para las señales de aceleraciones en los tres ejes de firmas en el aire es la fusión a nivel de decisión. Además, al efectuar una firma en el aire con un dispositivo móvil, el eje X almacena la información más distintiva.

Capítulo 10

Desarrollo de una aplicación para obtener una base de datos de firmas en el aire de distintos usuarios

Las muestras de la base de datos de firmas en el aire, explicada en el Capítulo 7 se han obtenido utilizando dos aplicaciones para el iPhone que se han desarrollado como parte de este trabajo.

En este capítulo se presentará cada una de ellas por separado, en la Sección 10.1 la aplicación para muestras de firmas originales y en la Sección 10.2 la utilizada por los falsificadores para realizar los intentos de imitaciones de las firmas originales a partir de los vídeos grabados de las sesiones. En realidad, la segunda de ellas es tan sólo la primera modificada, por lo que en este apartado se explicará únicamente las modificaciones añadidas a la primera aplicación para almacenar las muestras de falsificación y facilitar su uso a los falsificadores que traten de imitar todas las muestras originales.

A la hora de almacenar las distintas repeticiones de las firmas realizadas, y para facilitar su posterior análisis, ha sido necesario definir una nomenclatura compleja que mantenga la mayor cantidad de información posible en el propio nombre del fichero para cada una de las muestras obtenidas. Esta nomenclatura se presentará también en este capítulo diferenciando las muestras originales y las muestras de falsificación.

10.1. Aplicación para obtención de firmas originales

La aplicación presentada en esta Sección, se ha implementado en un iPhone para extraer la información de las aceleraciones de las distintas repeticiones que han realizado distintos usuarios de sus firmas en el aire. Esta aplicación se ha utilizado en la fase de obtención de muestras originales para la base de datos de firmas en el aire.

En todo momento, los participantes que estaban ejecutando sus firmas en el aire estaban acompañados y asesorados por el desarrollador de la aplicación, que les explicó de manera muy breve el funcionamiento del programa. Debido a este hecho, no se ha puesto demasiado hincapié en realizar una interfaz llamativa y espectacular, sino que el principal objetivo que se ha tratado de conseguir es desarrollar un programa sencillo e intuitivo, que sea fácil de utilizar por el usuario y que almacene correctamente la información de las aceleraciones en cada eje de cada gesto.

A continuación se presentarán las diferentes pantallas de las que se compone la aplicación, manteniendo el orden típico de utilización del programa y explicando en detalle qué se hace en cada momento.

1. Pantalla de Bienvenida:

   Cuando se inicia la aplicación aparece la pantalla de bienvenida de la Figura 10.1(a).

   En esta pantalla de inicio de la aplicación, existe un campo de texto que hay que rellenar con el número de usuario que participa en el experimento. Este número será único para cada usuario. A efectos de la base de datos, este número es la única información personal que se almacene del usuario, es decir, las identidades de la base de datos son números, y no hay información en la base de datos para correlar una identidad real de una persona que haya participado en el experimento con su número de identidad de la base de datos. Este punto es muy importante para mantener la anonimidad de las identidades de la base de datos biométrica que se ha obtenido.

   La aplicación tiene un sistema para comprobar que se ha rellenado el campo de texto con un número de tres cifras.

   El sujeto encargado de recoger los datos de los experimentos, en la explicación que hace a los participantes les dará su número de usuario en la base de datos, que almacenará en una tabla en papel (fuera de la base de datos), para uso interno por si hubiera algún problema en alguna de las sesiones de la fase de obtención de base de datos.

   Una vez rellenado en la aplicación el número de usuario asignado, se pulsa el botón Inicio, y se accede a la siguiente pantalla.

2. Pantalla de Menú Principal:

En la pantalla de Menú principal 10.1(b) de la aplicación aparecen dos grandes botones para registrar dos gestos de cada usuario.

Debido a que una de las mayores dificultades a la hora de realizar una base de datos biométrica es encontrar voluntarios que quieran participar, se ha decidido tomar por cada usuario dos gestos diferentes, de la siguiente manera:

- En el primer gesto (Pulsando el botón "Gesto 1"), el usuario va a realizar su firma en el aire para esta técnica biométrica, tal y como se explicó en la Sección 7.1. De hecho, los tipos de gestos realizados son los presentados en la Sección 7.3; donde algunos usuarios han realizado su propia firma manuscrita en el aire y otros se han inventado nuevos gestos identificativos.
- En el segundo gesto (Pulsando el botón "Gesto 2"), si el usuario anteriormente ha realizado su propia firma manuscrita en el aire, se le pide que se invente un gesto nuevo que pueda resultar identificativo, repetible por él y no inmediato de imitar. En caso contrario, se le pide que realice su firma manuscrita en el aire.

De esta manera, para futuras investigaciones donde se quiera correlar la relación entre firmas manuscritas en una pantalla táctil con firmas en el aire, ya se dispondrá de una base de datos para realizar este estudio.

En el ámbito de este trabajo, únicamente se utilizaron las firmas en el aire almacenadas como primer gesto del usuario, puesto que es lo que el participante ha realizado de manera intuitiva y natural.

Para empezar a efectuar cada uno de sus gestos que se van a almacenar en la base de datos, se pulsa el botón correspondiente, que lleva a la siguiente pantalla.

3. Pantalla de Realización de la firma:

   La pantalla de la Figura 10.1(c) muestra la interfaz que ofrece la aplicación para que el usuario realice su gesto.

   En esta pantalla se ofrecen al usuario las instrucciones para que la aplicación pueda almacenar las distintas repeticiones de sus gestos identificativos para esta técnica biométrica. Estas instrucciones son:

   - Piensa un gesto que puedas repetir.
   - Pulsa el botón Verde para empezar.
   - Realiza el gesto con el teléfono.
   - Pulsa el botón Rojo para acabar.
   - Repite 8 veces.

Además de estas instrucciones, el responsable de la obtención de la base de datos de firmas en el aire, le explica al usuario otras características del gesto que debe realizar.

Una vez el usuario pulsa el botón Verde ("Start"), se activa la función que empieza a almacenar los valores de aceleración en cada eje muestreados por el acelerómetro del iPhone. En ese momento, el botón verde se convierte en Rojo, de nombre ("Stop").

4. Pantalla de repetición realizada correctamente:

   Cuando el usuario termina de efectuar su firma en el aire, pulsa el botón de "Stop". Entonces, la función que recoge los datos de aceleración se deshabilita, y se almacenan todos los valores recogidos por el acelerómetro en el intervalo de tiempo en el que el usuario ha realizado su gesto. Todos estos valores se guardan en un fichero dentro del teléfono, en la carpeta Application Home/Documents del Sandbox de la propia aplicación, ya que desde esta ubicación los ficheros son descargables al ordenador de manera sencilla desde el programa iTunes. El nombre de cada repetición de cada gesto sigue una nomenclatura específica, explicada más adelante en la Sección 10.1.1.

   Una vez pulsado el botón de "Stop" y almacenado el fichero correspondiente en el iPhone, aparece la pantalla de la Figura 10.1(d), que informa al usuario de las repeticiones que lleva. Al pulsar "Continuar" se vuelve a la pantalla anterior, en la que el usuario deberá realizar una nueva repetición del gesto hasta que lleve 8.

   Después de efectuar la octava repetición de su firma en el aire, aparece una ventana que informa al usuario de este hecho. En este caso, al pulsar el botón "Continuar", la aplicación vuelve a la pantalla de Menú principal, donde el participante podrá realizar su segundo gesto en caso de no haberlo realizado ya.

10.1.1. Nomenclatura de las muestras originales

Las muestras originales almacenadas en la base de datos y extraídas gracias a la aplicación desarrollada para el iPhone tienen la siguiente nomenclatura: AXXXGYNZST.txt, donde:

- A: El primer carácter del nombre del fichero denota el tipo de muestra que es. Si es una muestra original, obtenida con la aplicación explicada en esta Sección, tendrá el valor U.

- XXX: es el número de usuario que ha realizado la muestra. Éste número es único y representa la identidad real del usuario que ha firmado en el aire.

- Y: hace referencia al número de gesto al que pertenece la muestra. Tal y como se explicó anteriormente, cada usuario realizaba dos firmas en el aire y en este trabajo sólo se tomaron en cuenta las primeras realizaciones. Tiene valores 1 ó 2.
- Z: es el número de repetición de la firma en el aire del usuario. Tiene valores del 1 al 8.
- T: es el número de sesión a la que pertenece la muestra. En este trabajo únicamente podrá tomar el valor 1, pero más adelante, al tomar nuevas muestras del mismo gesto realizado por el usuario original podrá tomar otros valores.

10.2. Aplicación para obtención de firmas falsificadas

Para obtener las muestras de firmas en el aire falsificadas, se ha desarrollado la aplicación que se presenta a continuación. Para facilitar su implementación, y debido a que tiene muchas partes comunes a la aplicación de obtención de firmas en el aire originales, se ha reutilizado la mayoría del código, añadiendo pequeñas modificaciones para facilitar el proceso de falsificación de todas las muestras originales de la base de datos.

De manera similar a la Sección anterior, se explicará la aplicación presentando las distintas pantallas de las que consta, en el orden en el que cualquier falsificador la utilizará.

1. Pantalla de Bienvenida:

   Al ejecutar la aplicación, aparece la pantalla de bienvenida de la Figura 10.2(a).

   En esta pantalla se encuentran el campo de número de usuario, similar al de la aplicación de obtención de muestras originales. En este caso, éste campo corresponde con el número de usuario que el falsificador tratará de imitar observando la grabación de la toma de muestras originales de dicho usuario.

   Además, en esta pantalla aparecen dos campos de texto nuevos:

   - Código de falsificador: Cada falsificador que participa en la obtención de la base de datos tiene un código propio, único y asociado a su identidad. De esta manera, podrán estudiarse por separado las muestras de falsificación de cada uno de los voluntarios que traten de imitar las firmas originales. En este trabajo, 3 personas han participado en la elaboración de imitaciones de firmas.
   - Sesión de falsificación: Los falsificadores podrían volver a intentar repetir algunos gestos en otras sesiones, por lo que se ha habilitado este campo que almacene esta información.

Una vez rellenados todos los campos de la aplicación, y comprobando que todos tienen el formato requerido, se pulsa el botón Inicio, y se accede a la pantalla siguiente.

2. Pantalla de Menú Principal:

   En la pantalla de Menú principal 10.2(b) de la aplicación hay tres grandes botones para registrar las muestras de falsificación del usuario que se está tratando de imitar, cuyo número identificativo se puede consultar en la parte superior de la misma.

   En esta pantalla, la aplicación ofrece una breve instrucción al falsificador: "Hay que falsificar los dos gestos que ha realizado el sujeto". "Pulsa un botón para comenzar".

   Los dos botones superiores ("Gesto 1" y "Gesto 2") son similares a los de la aplicación de obtención de muestras originales. Si se pulsa uno de ellos, el falsificador podrá acceder a la pantalla siguiente donde podrá empezar a efectuar las imitaciones de los gestos correspondientes.

   Además, en esta pantalla se incluye el botón "Nuevo usuario", que permite al falsificador volver a la pantalla de Inicio y poder empezar las falsificaciones de otro usuario original introduciendo su número asignado en el campo correspondiente.

3. Pantalla de Realización de la firma:

   La pantalla de la Figura 10.2(c) muestra la interfaz que ofrece la aplicación para que el falsificador trate de imitar otro gesto.

   Las instrucciones que se le ofrecen al falsificador para la utilización de la aplicación son:

   - Mira el gesto en el vídeo.
   - Pulsa el botón Verde para empezar.
   - Realiza el gesto con el teléfono.
   - Pulsa el botón Rojo para acabar.
   - Repite 7 veces.

   En este caso, el número de repeticiones es de 7, y se le recuerda al falsificador que ha de estudiar en primer lugar la grabación del gesto correspondiente.

   El funcionamiento de la aplicación en esta pantalla es exactamente igual que en la aplicación de obtención de muestras originales. Una vez el falsificador pulsa el botón Verde ("Start"), se activa la función que muestrea y almacena los valores de aceleración en cada eje del iPhone. En ese momento, el botón verde se convierte en Rojo, de nombre ("Stop").

4. Pantalla de repetición realizada correctamente:

   Esta pantalla tiene un comportamiento muy similar al de la aplicación de obtención de muestras originales. Al pulsar el botón de "Stop", los valores de aceleración muestreados de la realización del gesto se vuelcan en un fichero, siguiendo una nomenclatura distinta explicada en la Sección 10.2.1.

   Una vez finalizado el proceso y almacenado el fichero correspondiente a la muestra que se acaba de realizar, aparece la pantalla de la Figura 10.2(d), que informa el número de repeticiones que lleva el falsificador del gesto que está tratando de imitar.

   Después de efectuar el séptimo intento la aplicación vuelve a la pantalla de Menú principal, donde el falsificador podrá realizar el otro gesto de un usuario o bien elegir el siguiente usuario a imitar.

10.2.1. Nomenclatura de las muestras de falsificaciones

Los ficheros de texto donde se almacena los valores de aceleración de las muestras de falsificaciones tienen una nomenclatura muy similar a la de las muestras originales: AXXXGYNZFDDDST.txt, en donde:

- A: La información de que la muestra almacenada con esta aplicación es un intento de falsificación se recoge en el primer carácter de la cadena de texto. Este hecho se representa asignando a A la letra W, y así poder identificar las muestras falsificadas de las originales, que se denotaban por U.
- XXX, Y, Z y T representan los mismos valores que en las muestras originales: número de usuario, número de gesto, número de repetición y número de sesión, respectivamente.
- DDD: es un código numérico asignado de manera única para cada falsificador.

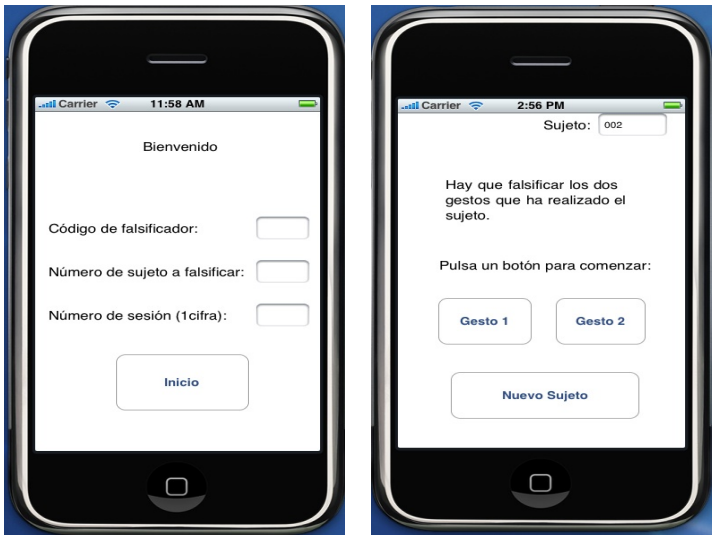
(a) Pantalla de bienvenida

(b) Pantalla de menú principal

(c) Pantalla de realización de firma

(d) Pantalla de muestra realizada

Figura 10.1: Pantallas de la aplicación de toma de muestras originales desarrollada en un iPhone



(a) Pantalla de bienvenida

(b) Pantalla de menú principal

(c) Pantalla de realización de firma

(d) Pantalla de muestra realizada

Figura 10.2: Pantallas de la aplicación de toma de muestras de falsificaciones desarrollada en un iPhone

Capítulo 11

Desarrollo de un prototipo de la técnica biométrica basada en la firma en el aire para el iPhone

Como resultado final de este trabajo de investigación se ha desarrollado un prototipo para el iPhone que englobe todo lo estudiado en una aplicación que funcione y que cualquier usuario pueda probar.

Esta aplicación implementa las dos funcionalidades imprescindibles de los sistemas de acceso biométrico:

- Enrolamiento en el sistema: En primer lugar, el usuario ha de enrolarse en el sistema realizando tres veces el gesto identificativo suejetando el teléfono móvil que desea utilizar como firma en el aire.
- Acceso al sistema: El usuario se autenticará en el sistema repitiendo su firma en el aire. Si el sistema considera que la firma realizada coincide con la firma que tiene almacenada del enrolamiento, permitirá el acceso. En caso contrario lo denegará.

En este Capítulo, se tratará la parte correspondiente a cada una de las funcionalidades por separado, manteniendo el orden lógico de utilización del prototipo. Por ello, se comenzará presentando la fase de enrolamiento en la Sección 11.1, imprescindible para poder acceder al sistema. A continuación se presentará la fase de acceso en la Sección 11.2.

El prototipo desarrollado en este trabajo puede ser incorporado fácilmente a otras aplicaciones más grandes que necesiten una autenticación del usuario. Este prototipo puede considerarse como el módulo de autenticación del sistema completo, que dicta si el usuario que está intentado acceder a la parte protegida del sistema global es quien dice ser.

En este Capítulo se presentará la interfaz de dicho prototipo, con una explicación general de lo que va haciendo el programa en cada momento. La matemática que subyace en el problema ya ha sido explicada en el Capítulo 6, por lo que se hará referencia al mismo cuando proceda. Asimismo, no se entrará en detalle de código de la implementación del prototipo, puesto que no se considera de interés y los conceptos más importantes han sido también presentados en el Capítulo 4.

11.1. Enrolamiento en el sistema implementado en el prototipo

En esta Sección se presentará la parte del prototipo implementado relativa a la funcionalidad de enrolamiento en el sistema biométrico. Para ello, se seguirá el esquema de pantallas que el usuario se va encontrando cuando trata de enrolarse en el sistema.

1. Pantalla inicial:

   Al lanzar la aplicación en un iPhone, aparece la primera pantalla de menú principal mostrada en la Figura 11.1(a). Esta pantalla consta de dos botones "Crear" y "Acceder". Pulsando el primero de ellos, se enlaza con la pantalla siguiente en la que se comenzará el proceso de enrolamiento en el sistema y se creará el patrón biométrico identificativo de la persona.

   En cambio, al pulsar el botón "Acceder", la aplicación mostrará la pantalla para tratar de acceder al sistema repitiendo la firma en el aire con la que el usuario se enroló. Si el usuario no se ha enrolado previamente, ocurrirá un error, puesto que es imprescindible para acceder al sistema que exista un patrón biométrico con las firmas en el aire que el usuario utilizó en el enrolamiento.

2. Pantalla de realización de firma de enrolamiento.

   En esta pantalla, Figura 11.1(b), se procede a la realización de las tres repeticiones de firmas en el aire del usuario necesarias para conformar el patrón biométrico. Esta pantalla tiene una aspecto y funcionalidad similar a la correspondiente de las aplicaciones para obtener la base de datos de firmas en el aire, explicadas en el Capítulo 10.

   Pulsando el botón inicio de la pantalla se activa la función que obtiene los valores de aceleración de los distintos ejes del iPhone, medidos gracias a su acelerómetro. Al volver a pulsar el botón inferior, se deshabilita esta función, volcando los datos que se han obtenido a un fichero que se almacenará en el dispositivo como muestra del patrón de la firma en el aire realizada.

   Estos archivos se almacenan en la carpeta de la aplicación de ruta: Application Home/Library/Caches, ya que se requiere que nadie pueda acceder a los datos biométricos almacenados en el teléfono.

Además, en esta pantalla aparece un campo de texto con el número de repeticiones que el usuario ha llevado a cabo. Al finalizar la tercera de ellas, el sistema procesa los tres ficheros que almacenan la información de la aceleración en cada eje de cada una de las tres repeticiones. Como fruto de este procesamiento, ya explicado en detalle en la Sección 6.3, se obtiene un valor μ_T que indica el parecido entre las tres señales de enrolamiento. Este valor se almacenará en el dispositivo móvil, formando el patrón biométrico junto a los tres ficheros que almacenan las aceleraciones muestreadas de las realizaciones de cada firma de enrolamiento.

En futuros trabajos, éste sería el punto ideal para realizar una estimación de la fortaleza de la firma en el aire. Para ello, habría que obtener las características de las señales que hacen que una firma sea segura, e implementar un sistema que comprueba si esas características se encuentran en la firma en el aire que trata de enrolarse. Un sistema muy sencillo de realizar esto sería fijar un valor máximo de μ_T, por encima del cual no se permite que el usuario se enrole en el sistema, puesto que las repeticiones de sus firmas en el aire han sido muy diferentes. Encontrar las características que hacen que una firma sea sencilla o difícil de falsificar es una línea de investigación abierta.

3. Pantalla de éxito de enrolamiento

   Una vez que el patrón biométrico se ha conformado, aparece la pantalla de éxito de enrolamiento mostrada en la Figura 11.1(c). Esta pantalla tiene un botón que permite volver al menú principal y acceder al sistema con la firma en el aire que se ha utilizado para enrolarse.

11.2. Acceso al sistema implementado en el prototipo

Una vez que el usuario se ha enrolado en el sistema, puede autenticarse en el mismo realizando la firma en el aire con la que se enroló. Para ello, se utilizan las partes del prototipo se explican en esta Sección.

1. Pantalla de realización del gesto de acceso:

   Esta pantalla es similar a la de realización del gesto de enrolamiento (Figura 11.2). En ella, se encuentra la función que activa el acelerómetro del iPhone y muestrea las aceleraciones de la realización de la firma en el aire que realiza el usuario. Una vez pulsado el botón inicio, la función se activa, hasta que se vuelve a pulsar el botón inferior. En ese momento, se recoge toda la información de las aceleraciones muestreadas en un vector.

   Este vector con los datos de la firma en el aire de acceso, se procesa según el método explicado en la Sección 6.4, utilizando los ficheros que conforman el patrón biométrico (las tres firmas en el aire de enrolamiento y el valor de μ_T) que se encuentran almacenados en el dispositivo móvil.

Como resultado de este procesamiento, se obtiene un valor δ_A que indica el grado de parecido de la señal respecto a las señales que forman el patrón biométrico. Normalizando este valor al parecido de las propias señales del patrón, se obtiene el valor final $\theta = \delta_A/\mu_T$.

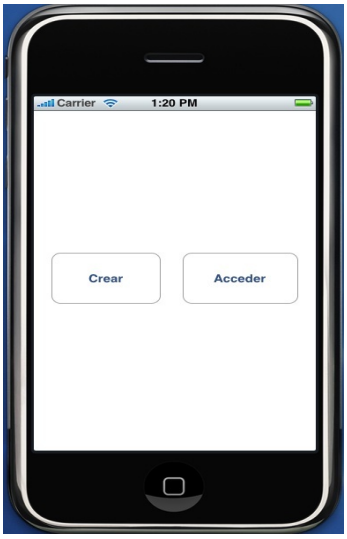
2. Pantalla de resultado del acceso:

   Dependiendo del valor θ obtenido en el procesamiento de la señal de acceso respecto al patrón biométrico almacenado en el dispositivo móvil, aparecerá una de las dos Figuras 11.3(a) o 11.3(b), según la autenticación haya sido considerada correcta o incorrecta.

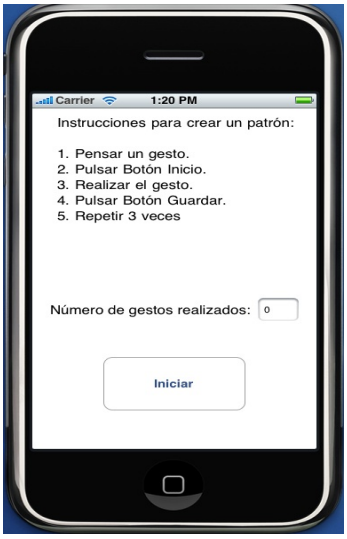
   Para que el usuario sea autenticado, el valor de θ ha de ser menor de un umbral definido para todos los gestos κ. En caso contrario, el acceso al sistema será denegado.

   El valor de κ que se ha definido en este prototipo es de 1.5, puesto que es el valor del umbral donde se alcanzaba el punto de EER mínimo de todos los experimentos realizados en el Capítulo 9. En cualquier caso, este valor se puede modificar según la aplicación global en la que se incluya este módulo de autenticación, teniendo en cuenta que:

   - Reducir el valor de κ (y por tanto, el valor máximo permitido de δ_A) provocará un mayor número de falsos rechazos, donde el usuario original no siempre será capaz de acceder al sistema con su propia firma en el aire. A cambio, el número de falsos negativos aumentará, pues será más difícil que un usuario fraudulento acceda al sistema.
   - Aumentar el valor de κ provoca el efecto contrario, disminuyendo el número de falsos rechazos del usuario original a cambio de dar más posibilidades de acceder al sistema a los usuarios fraudulentos.



(a) Pantalla de inicio



(b) Pantalla de realización de gesto de enrolamiento

(c) Pantalla de enrolamiento exitoso

Figura 11.1: Pantallas del del enrolamiento en el prototipo de la técnica biométrica de firma en el aire implementado en un iPhone

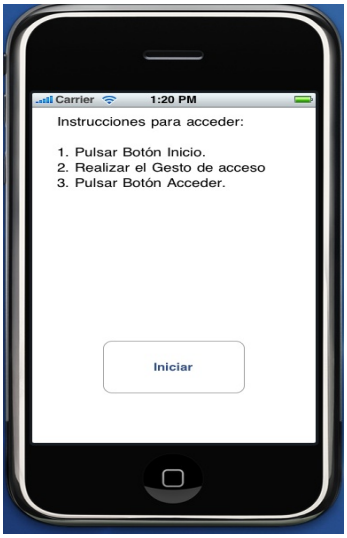


Figura 11.2: Pantalla de realización de gesto de acceso

(a) Pantalla de acceso permitido

(b) Pantalla de acceso denegado

Figura 11.3: Pantallas de acceso al prototipo desarrollado para el iPhone según el resultado de la autenticación utilizando la técnica biométrica de firma en el aire

Parte IV

Conclusiones y líneas futuras

Capítulo 12

Conclusiones

En este trabajo se ha presentado en detalle una nueva técnica biométrica basada en la firma en el aire aplicada en dispositivos móviles que integren un acelerómetro.

Esta técnica biométrica cumple en gran medida las características fundamentales que toda técnica biométrica debe tener:

- Universalidad: (Media) Esta técnica puede ser utilizado por cualquier persona capaz de sostener un teléfono móvil en su mano y mover el brazo.
- Singularidad o univocidad: (Media-Alta) Los estudios realizados demuestran que las firmas en el aire realizadas por distintas personas son bastante distinguibles entre sí.
- Permanencia: (Media) Al ser una técnica basada en el comportamiento, la manera que tiene el usuario de realizar su firma nunca es exactamente igual.
- Colectividad: (Alta) El patrón biométrico del usuario, en este caso, las señales de aceleración de la realización de la firma, es medible y se recoge con facilidad, sin la necesidad de que el usuario haga nada más aparte de su firma en el aire.
- Rendimiento o actuación: (Media-Alta) Las tasas de error de EER son bajas, aunque alejadas de otras técnicas biométricas basadas en rasgos físicos.
- Aceptabilidad: (Muy alta) Los usuarios han evaluado la aceptabilidad de la técnica como muy alta, pues ya están acostumbrados a realizar firmas manuscritas continuamente en su vida real. Además, tienen la sensación de realizar algo muy novedoso, lo que les satisface.
- Fiabilidad o Resistencia a fraude: (Media-Alta) Los usuarios que han tratado de falsificar los gestos de otros no han obtenido buenos resultados,

a pesar de tener las grabaciones en vídeo de las sesiones de obtención de datos originales.

Estas conclusiones se fundamentan en los experimentos que se han realizado sobre una base de datos de 40 usuarios que han realizado su firma en el aire y 3 falsificadores que han tratado de imitar cada una de las firmas originales mediante el estudio de grabaciones de vídeo.

Para estos experimentos, se ha definido un método matemático de análisis de las señales de aceleración de las firmas en el aire, y se han probado distintos escenarios de fusión de información multibiométricos, obteniendo una tasa de error de EER del 2.5 % en el mejor de las casos.

Asimismo, se ha realizado un estudio de la valoración que tiene el usuario sobre esta técnica biométrica, una vez que ha entrado en contacto con ella, resaltando en gran medida la facilidad que ha encontrado para su uso y la gran aceptabilidad que ofrece.

Por último, se ha implementado un primer prototipo de esta técnica en un iPhone, seleccionado por las grandes ventajas que aportaba para esta investigación. Este prototipo puede formar parte de una aplicación móvil más grande que necesite la autenticación biométrica del usuario para llevar a cabo cualquier operación.

Capítulo 13

Líneas futuras

Para continuar este trabajo de investigación en el futuro, se plantean las siguientes líneas futuras:

En primer lugar, es fundamental ampliar la base de datos de firmas en el aire, con nuevos usuarios que realicen sus firmas según la técnica propuesta y falsificadores que traten de imitarlos. Una base de datos de aproximadamente 100 usuarios rubricaría el funcionamiento de esta técnica biométrica.

En estos sistemas, es de vital importancia incluir un módulo de control de calidad de las firmas en el aire con las que un usuario se trata de enrolar en el sistema. El objetivo del mismo es que el propio dispositivo móvil pueda inferir automáticamente el grado de seguridad de una firma en base a sus características. Este módulo es similar a los sistemas de fortaleza de contraseñas, en los que se obliga al usuario a que seleccione una secuencia de caracteres suficientemente robusta (con mayúsculas, símbolos especiales, números, etc.) para que no pueda ser encontrada por fuerza bruta. Para realizar este control de calidad, será necesario estudiar las características intrínsecas a las señales que reviertan en una mayor dificultad para su falsificación, y por tanto, una mayor seguridad.

Otro aspecto que hay que considerar antes de implementar esta técnica en un sistema de uso real es el estudio de la permanencia de las firmas en el aire en el tiempo. Al ser una técnica biométrica basada en comportamiento, se presupone que un usuario no va a ser capaz de repetir nunca la misma firma dos veces, pero además, es posible que el usuario vaya evolucionando en su manera de realizar la firma. Si un usuario efectúa frecuentemente la firma, irá convirtiéndola en algo natural, y probablemente, la realización natural de la firma sea distinta a las primeras repeticiones de la misma que se utilizaron para enrolarse en el sistema. Por ello, es necesario estudiar la evolución de las firmas a lo largo del tiempo, cuando un usuario las hace de manera muy frecuente o no, para así poder implementar un sistema que sea capaz de reconocer cuándo el usuario empieza a realizar su firma de manera natural y pueda actualizar el patrón biométrico guardado en el teléfono móvil de manera continua según dicha evolución.

Por otro lado, los tiempos de procesamiento son asumibles, pero no lo suficientemente bajos, por lo que es necesario implementar una optimización del

algoritmo de procesamiento de las señales que reduzca estos tiempos.

Además, pueden estudiarse otros métodos de análisis basados en otras técnicas matemáticas, como máquinas de soportes vectorial (SVMs), cadenas ocultas de Markov (HMMs) o Dynamic Time Warping (DTW). Asimismo, puede considerarse utilizar el algoritmo implementado con ciertas modificaciones a la hora de conformar el patrón, otras medidas de comparación y/o varios procesamientos en serie de las señales.

En este trabajo, se han utilizado las señales sin ningún tipo de preprocesamiento previo. Podría ser interesante estudiar los resultados de aplicar en el sistema algunas operaciones de filtrado o normalización previas y comunes a todas las señales.

Por último, sería muy interesante poder aplicar a esta técnica biométrica algún modelo criptobiométrico complejo, donde a partir de la firma en el aire se cree automáticamente una clave criptográfica única y ligada a la identidad del usuario que ha efectuado su firma en el aire.

Parte V

Bibliografía

Bibliografía

[1] *Identifying users of portable devices from gait pattern with accelerometers*, volume 2, 2005.

[2] Richard Bellman. Dynamic programming and stochastic control processes. *Information and Control*, 1(3):228–239, 1958.

[3] Richard Bellman. Dynamic programming treatment of the travelling salesman problem. *J. ACM*, 9(1):61–63, 1962.

[4] John Daugman. Face and gesture recognition: Overview. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 19:675–676, 1997.

[5] John Daugman. How iris recognition works. *IEEE Transactions on Circuits and Systems for Video Technology*, 14:21–30, 2002.

[6] R. Durbin, S. Eddy, A. Krogh, and G. Mitchison. *Biological sequence analysis: Probabilistic Models of Proteins and Nucleic Acids*. Cambridge University Press, eleventh edition, 2006.

[7] Dal ho Cho, Kang Ryoung Park, Dae Woong Rhee, Yanggon Kim, and Jonghoon Yang. Pupil and iris localization for iris recognition in mobile phones. *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, International Conference on & Self-Assembling Wireless Networks, International Workshop on*, 0:197–201, 2006.

[8] Keith Inman and Norah Rudin. *An introduction to forensic DNA analysis*. Boca Raton : CRC Press, 1997.

[9] Toshiki Iso and Kenichi Yamazaki. Gait analyzer based on a cell phone with a single three-axis accelerometer. In *MobileHCI '06: Proceedings of the 8th conference on Human-computer interaction with mobile devices and services*, pages 141–144, New York, NY, USA, 2006. ACM.

[10] Anil K. Jain, Patrick Flynn, and Arun A. Ross. *Handbook of Biometrics*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2007.

[11] Anil K. Jain, Friederike D. Griess, and Scott D. Connell. On-line signature verification. *Pattern Recognition*, 35:2002, 2002.

[12] Anil K. Jain and Stan Z. Li. *Handbook of Face Recognition*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.

[13] Anil K. Jain and David Maltoni. *Handbook of Fingerprint Recognition*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2003.

[14] Dae Sik Jeong, Hyun-Ae Park, Kang Ryoung Park, and Jaihie Kim. Iris recognition in mobile phone based on adaptive gabor filter. In *Advances in Biometrics, International Conference, ICB 2006, Hong Kong, China, January 5-7, 2006, Proceedings*, pages 457–463, 2006.

[15] Neil C. Jones and Pavel A. Pevzner. *An Introduction to Bioinformatics Algorithms (Computational Molecular Biology)*. The MIT Press, August 2004.

[16] Scott Kelby and Terry White. *The iPhone book : how to do the most important, useful & fun stuff with your iPhone*. Peachpit Press ; Pearson Education [distributor], 2009.

[17] Stephen Kochan. *Programming in Objective-C 2.0*. Addison-Wesley Professional, 2009.

[18] Glenn E. Krasner and Stephen T. Pope. A description of the model-view-controller user interface paradigm in the smalltalk-80 system, 1988.

[19] Stan Kurkovsky, Tommy Carpenter, and Caleb MacDonald. Experiments with simple iris recognition for mobile phones. *Information Technology: New Generations, Third International Conference on*, 0:1293–1294, 2010.

[20] Martine Lapère and Eric Johnson. User authentication in mobile telecommunication environments using voice biometrics and smartcards. In *IS&N '97: Proceedings of the Fourth International Conference on Intelligence and Services in Networks*, pages 437–443, London, UK, 1997. Springer-Verlag.

[21] Vladimir I. Levenshtein. Binary codes capable of correcting deletions, insertions, and reversals. Technical Report 8, 1966.

[22] M.P. Murray. Gait as a total pattern of movement. *Am. J. Physical Medicine*, 46(1):290–329, 1967.

[23] Vishvjit S. Nalwa. Automatic on-line signature verification. In *Proceedings of the IEEE*, pages 215–239, 1997.

[24] Jonas Nilsson and Michael Harris. Match-on-card for java cards. Technical report, Precise Biometrics, 2004.

[25] Réjean Plamondon and Sargur N. Srihari. On-line and off-line handwriting recognition: A comprehensive survey. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 22:63–84, 2000.

[26] Salil Prabhakar and Anil K. Jain. Decision-level fusion in biometric verification. *IEEE Trans. Patt. Anal. and Machine Intell*, 2001:88–98, 2000.

[27] Slobodan Ribaric and Ivan Fratric. A biometric identification system based on eigenpalm and eigenfinger features. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27:1698–1709, 2005.

[28] Arun Ross and Anil Jain. Information fusion in biometrics. *Pattern Recogn. Lett.*, 24(13):2115–2125, 2003.

[29] Arun A. Ross, Karthik Nandakumar, and Anil K. Jain. *Handbook of Multibiometrics (International Series on Biometrics)*. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2006.

[30] Hataichanok Saevanee and Pattarasinee Bhatarakosol. User authentication using combination of behavioral biometrics over the touchpad acting like touch screen of mobile device. *Computer and Electrical Engineering, International Conference on*, 0:82–86, 2008.

[31] H. Abdul Shabeer and P. Suganthi. Mobile phones security using biometrics. *Computational Intelligence and Multimedia Applications, International Conference on*, 4:270–274, 2007.

[32] T. F. Smith and M. S. Waterman. Identification of common molecular subsequences. *Journal of molecular biology*, 147(1):195–197, March 1981.

[33] Joan Hoover Steve Dowling, Nancy Paxton. Apple reports first quarter results. Technical report, Apple Inc., 2009.

[34] Qian Tao and R.N.J. Veldhuis. Biometric authentication for a mobile personal device. *Mobile and Ubiquitous Systems, Annual International Conference on*, 0:1–3, 2006.

[35] Peter Whittle. *Optimization over Time*. John Wiley & Sons, Inc., New York, NY, USA, 1982.

[36] Peter Whittle. *Optimal Control: Basics and Beyond*. John Wiley & Sons, Inc., New York, NY, USA, 1996.

[37] Dit yan Yeung, Hong Chang, Yimin Xiong, Susan George, Ramanujan Kashi, Takashi Matsumoto, and Gerhard Rigoll. Svc2004: First international signature verification competition. In *In Proceedings of the International Conference on Biometric Authentication (ICBA), Hong Kong*, pages 16–22. Springer, 2004.

[38] Song yi Han, Hyun-Ae Park, Dal Ho Cho, Kang Ryoung Park, and Sangyoun Lee. Face recognition based on near-infrared light using mobile phone. In *Adaptive and Natural Computing Algorithms, 8th International Conference, ICANNGA 2007, Warsaw, Poland, April 11-14, 2007, Proceedings, Part II*, pages 440–448, 2007.

[39] Jonathan Zdziarski. *iPhone Open Application Development: Write Native Objective-C Applications for the iPhone*. O'Reilly Media, Inc., March 2008.

[40] Xiaoli Zhou and Bir Bhanu. Feature fusion of side face and gait for video-based human identification. *Pattern Recogn.*, 41(3):778–795, 2008.