Universidad Autónoma de Madrid
Escuela Politécnica Superior

Trabajo fin de grado

DISEÑO Y ADQUISICIÓN MULTI-DISPOSITIVO DE BASE DE DATOS DE FIRMA MANUSCRITA DINÁMICA

Grado en Tecnologías y Servicios de Telecomunicación

Sandra Gaytán Grande
Julio 2014

DISEÑO Y ADQUISICIÓN MULTI-DISPOSITIVO DE BASE DE DATOS DE FIRMA MANUSCRITA DINÁMICA

AUTOR: Sandra Gaytán Grande
TUTOR: Javier Ortega García

Biometric Recognition Group - ATVS
Dpto. de Tecnología Electrónica y de las Comunicaciones
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Julio 2014

Resumen

En la actual era tecnológica, el crecimiento emergente de las tecnologías de reconocimiento biométrico brinda la posibilidad de mejorar los procesos de verificación de identidad del usuario mediante el uso de un rasgo biométrico propio, en un mundo en dónde el acceso ubicuo a la información, el control de acceso y la identificación de usuarios son tareas claves realizadas principalmente mediante el uso de contraseñas fáciles de robar u olvidar. En el area del reconocimiento biométrico, en contraposición a las contraseñas, se usan rasgos fisiológicos (iris, huella dactilar, imagen facial) y de comportamiento (firma, voz, forma de caminar) para identificar al usuario; dichos rasgos se caracterizan por ser imposibles de olvidar y difíciles de falsificar.

Toda esta tecnología biométrica compone un campo cada vez más presente en todos los ámbitos de la sociedad, encontrándose implementada en la actualidad en tres sectores principales:

- **Comercial**: presente en aplicaciones comerciales, tales como registros en la red, seguridad de datos electrónicos, e-commerce, tarjetas de crédito, smartphones, acceso a registros médicos y aprendizaje a distancia.
- **Gubernamental**: este tipo de aplicaciones incluyen tarjetas de identificación nacional (DNI), licencias de tráfico, seguridad social, controles fronterizos y pasaportes.
- **Forense**: aplicaciones forenses tales como investigación criminal, identificación terrorista, análisis de paternidad y desapariciones.

Es imprescindible tener en cuenta el gran mercado tecnológico existente, el cual ofrece multitud de dispositivos comerciales diferentes, e incluso para un mismo dispositivo, diferentes y cada vez más avanzadas versiones del mismo; todo ello complica en gran medida la tarea de reconocimiento, constituyendo así como principal objetivo de este proyecto el hacer frente a este constante aumento de variabilidad tecnológica en el campo de reconocimiento de escritor.

Actualmente, existen múltiples sistemas de reconocimiento de escritor ya implementados, sin embargo, el problema que se plantea es conseguir unicidad a la hora de analizar resultados cuando las muestras son recogidas a través de diferentes dispositivos con diferentes características entre sí. Este proyecto plantea la posibilidad, inexistente hasta el momento, de recoger una amplia base de datos con muestras provenientes de diferentes dispositivos, todas ellas ergonómicamente compatibles, es decir, recogidas siguiendo el mismo protocolo. Esto otorga la posibilidad de mejorar las técnicas de reconocimiento así como poder incorporar las nuevas tecnologías, como los smartphones y las tabletas, no diseñadas específicamente con el objetivo de servir para este propósito, dentro de los sistemas de reconocimiento de escritor, proporcionando resultados competentes.

Palabras Clave

Reconocimiento biométrico, base de datos, e-BioFirma, dispositivo, firma, escritura, verificación, identificación, variabilidad, tecnología, adquisición, multimodal, pen, dedo, WACOM, Samsung.

Abstract

In today's technological era, the growth of emerging biometric recognition technologies offers the possibility of improving the processes that verify the identity of the user with respect to its own biometric trait, in a world where ubiquitous access to information, control access and user identification are key tasks performed mainly by using passwords that are easy to steal or forget. In the biometric field, as opposed to passwords, anatomical features (iris, fingerprint, facial image) and behavioral features (signature, voice) are used to identify the user; these features are known for being hard to forget or falsify.

All this biometric technology makes up a field increasingly present in all areas of society, being currently implemented in three main sectors:

- **Commercial**: present in commercial applications such as web logs, electronic data security, e-commerce, credit cards, smartphones, medical record access and distance learning.
- **Government**: this type of application include national identification cards, traffic licenses, social security, border controls and passports.
- **Forensic**: forensic applications such as criminal investigation, terrorist identification, paternity test and disappearances.

It is essential to take into account the large technological market that exists, which offers many different commercial devices, and even for the same device, different and increasingly advanced versions of the same; all of this greatly complicates the task of recognition, thus constituting the main objective of this project to address this steady increase in technological variability in the field of recognition of a writer.

Currently, there are multiple writer recognition systems already in place, however, the problem that arises is to obtain unicity when analyzing results where samples are collected through different devices with different characteristics to one another. This project poses the inexistent possibility, to date, of collecting a large database with samples from different devices, all ergonomically compatible,that is to say collected following the same protocol. This gives the possibility of improving the recognition techniques and to incorporate new technologies such as smartphones and tablets, not specifically designed to serve this purpose, within the writer recognition systems, providing relevant results.

Key words

Biometric recognition, database, e-BioFirma, device, signature, handwritting, verification, identificaction, variability, technology, acquisition, multimodal, pen, finger, WACOM, Samsung.

Agradecimientos

En primer lugar, me gustaría agradecer a mi tutor, Javier Ortega, por haberme dado la oportunidad de realizar este trabajo, por sus consejos y por su asesoramiento a lo largo de estos meses. Merecen también mención especial los profesores Rubén Vera y Julián Fierrez, por su importante participación en el proyecto, su ayuda y sus ideas.

A Ram, colaborador del laboratorio, por su paciencia tanto en temas de programación como de idiomas. No olvidar a mis compañeros de laboratorio, aquellos que han amenizado tantas horas de trabajo, especialmente Rubén. Agradecer también a todos aquellos que han participado en la adquisición de la base de datos, invirtiendo su tiempo y aguantándome en el proceso.

Quiero dar las gracias a las personas que he conocido en la carrera, que tanto me han hecho reír en los malos y sobretodo en los buenos momentos, y tanto me han enseñado a lo largo de estos cuatro años. No podría decir que me arrepiento de haber tomado la decisión de estudiar esta carrera, y en gran parte es gracias a vosotros; a todos mis compañeros del itinerario de Audio y Video, sin los cuales las tardes de los jueves nunca habrían sido el momento más esperado de la semana; a Sergio, por demostrar que lo más importante es estar ahí, por que sigas estando; a Pali, por ser el mejor compañero de autobús, y ahora de prácticas; pero especialmente quiero mencionar a "las supernenas / pretty little liars / trío calavera ", ellas saben quienes son, personas con quienes he recorrido los pasillos de la universidad mil y una veces, que a pesar de las diferencias, los malos momentos y la distancia, siempre te apoyan, amigas de verdad. Dentro de este grupo en el que he tenido la suerte de estar, no puedo no poner su nombre, esa persona que no todo el mundo encuentra, que te entiende, con quien las conversaciones no son para seres humanos, alguien a quien tuve la suerte de llamar mejor amiga una vez, gracias Nerea.

Como olvidar a los amigos de toda la vida, esos con los que te pegas en el cole, te insultas en el instituto y finalmente, cuando te das cuenta de que ya no vas a verlos día si y día también, te sigues peleando pero vía whatsapp. Ahora en serio, no se que haría sin vosotras, gracias por vuestro apoyo, por aguantarme tantos años y demostrar que la universidad no significa distancia, por muchas noches de viernes más, Laura, Marina, Sandra, Ana, Cris, GRACIAS.

Y como suele pasar, lo mejor y más importante siempre se deja para el final, y los más importantes no pueden ser otros que mi familia, en especial mis padres y mi hermano, quienes lo han dado todo por mí desde el día uno, han creído en mí cuando yo no lo hacía, me han hecho reír cuando más lo necesitaba y me han enseñado todo. Soy quien soy gracias a vosotros, espero no defraudaros nunca. Os quiero.

A todos vosotros, os dedico este trabajo. Gracias

Sandra Gaytán Grande

Julio 2014

Índice general

Índice de figuras

Índice de tablas

Preámbulo

Organización de la memoria

La memoria de este trabajo queda organizada en los siguientes capítulos:

- **Capítulo 1**: Objetivos, motivación del proyecto y metodología de trabajo.
- **Capítulo 2**: Introducción al reconocimiento biométrico. Principales modalidades biométricas utilizadas en verificación e identificación de identidad. Privacidad y aceptación en la sociedad en relación a los sistemas de reconocimiento biométrico.
- **Capítulo 3**: Introducción a la verificación de firma. Descripción detallada de los sistemas de verificación de firma on-line.
- **Capítulo 4**: Estado del arte de bases de datos existentes que recogen rasgos biométricos: MCYT, BIOMET, MyIDEA, BiosecureID, Biosecure.
- **Capítulo 5**: Base de datos e-BioFirma. Diseño, desarrollo y proceso de adquisición. Programación de las aplicaciones de captura de la base de datos.
- **Capítulo 6**: Conclusiones y trabajo futuro.

Glosario de acrónimos

- **FA**: False Acceptance
- **FR**: False Reject
- **FAR**: False Acceptance Rate
- **FRR**: False Reject Rate
- **EER**: Equal Error Rate
- **DET**: Dinamic
- **HMM**: Hidden Markov Models
- **DTW**: Dinamic Time Wrapping
- **VGA**: Video Graphics Array
- **AES**: Advanced Encryption Standard
- **RSA**: Rivest, Shamir y Adleman (cryptographic system)
- **LCD**: Liquid Crystal Display

- **USB**: Universal Serial Bus
- **DNI**: Documento Nacional de Identidad
- **SDK**: Software Development Kit
- **UAM**: Universidad Autónoma de Madrid

Herramientas utilizadas

Para el desarrollo de este proyecto de han utilizado los siguientes programas y lenguajes de programación:

- Lenguajes de programación: Java, Java-Android y C-Sharp.
- Programas utilizados: Eclipse, Visual Studio y Texmaker.

1 Introducción

1.1. Motivación del proyecto

La problemática fundamental que motiva la realización de este proyecto reside en la necesidad de obtener resultados competentes frente al gran mercado tecnológico, cada día más competitivo y avanzado, en lo que se refiere a dispositivos, tanto específicamente diseñados para la recogida de firma, como dispositivos de uso común tal como smartphones y tabletas incluidos dentro de un mercado emergente en la sociedad actual.

Este gran impacto tecnológico ha dado lugar a una necesidad de verificación personal mediante vía no directa, es decir, a través de Internet. Un claro ejemplo de esto son las aplicaciones móviles bancarias, a través de las cuales es posible realizar operaciones mediante el propio smartphone, ordenador o tableta sin necesidad de acudir al sitio físico. Hasta el momento, el principal método para realizar estas operaciones es mediante el uso de contraseñas, sin embargo éstas son fáciles de perder, olvidar o robar; por este motivo surgen métodos de reconocimiento biométrico en sustitución a las contraseñas como método más fiable y seguro para la verificación del usuario.

En relación al campo de reconocimiento biométrico de firmante, la firma como verificación de usuario constituye el método de reconocimiento biométrico más ampliamente extendido y aceptado en la sociedad; esto se debe a que se trata de un rasgo característico del individuo, rápido de realizar y fácil de incorporar en los nuevos dispositivos tecnológicos ya mencionados; sin embargo, dentro de los métodos de reconocimiento biométrico, resulta uno de los menos robustos en relación a la posibilidad de ser falsificado, en contraposición a otros métodos más difíciles de falsificar como son la huella dactilar o el iris. Por este motivo, la base de datos diseñada recoge múltiples y variadas falsificaciones de la firma de los usuarios con el objetivo de desarrollar sistemas de verificación robustos ante posibles suplantaciones de identidad. Además, en caso de que el sistema no resulte suficientemente robusto ante falsificaciones de firma, se ha incorporado un proceso de escritura de nombre, esperando que con estos dos rasgos el proceso de verificación sea realista y competente.

1.2. Objetivos y enfoque

Dentro del amplio sector del reconocimiento biométrico, los sistemas de reconocimiento de firmante están cobrando un papel fundamental sustituyendo a los tradicionales métodos de firma sobre papel.

Este trabajo está enfocado en el reconocimiento de escritor sometido a la interoperabilidad existente entre diferentes dispositivos de captura, entre los que se encuentran algunos dispositivos portátiles cuyo principal uso no es el de captura de escritura y por tanto, las firmas serán realizada tanto con el dedo como con un *pen* específico, abarcando así todas las posibilidades referentes a dispositivos diseñados para la captura de escritura y dispositivos de uso no específico.

Mediante la captura de una amplia base de datos que contempla tanto variabilidad temporal como interoperabilidad, se podrán evaluar los sistemas de reconocimiento biométrico de la forma más realista posible, dando lugar al desarrollo de nuevos métodos que permitan compensar dichas variabilidades.

Por todo esto, los objetivos de este proyecto se pueden desglosar en los siguientes puntos:

1. **Estudio detallado del estado del arte**: Estudio de las bases de datos biométricas existentes hasta la fecha, con el fin de entender los protocolos de captura y poder adaptarlos a los objetivos y características de este proyecto.

2. **Desarrollo de las aplicaciones de captura**: se han desarrollado cuatro aplicaciones de captura de escritura (Java y Java-Android) cuya funcionalidad cumple el protocolo de adquisición establecido.

3. **Captura de la base de datos**: captura de una base de datos multimodal (en relación a la captura tanto de firma como de escritura), multisesión (con varias sesiones de adquisición para cada usuario), estadísticamente representativa de los usuarios potenciales de aplicaciones biométricas, y suficientemente grande como para poder ofrecer resultados estadísticamente significativos.

1.3. Metodología y plan de trabajo

Para poder cumplir con los objetivos establecidos al inicio del proyecto, se ha dedicado una gran parte del tiempo de trabajo a la crítica tarea de desarrollar las aplicaciones de captura de escritura en los diferentes dispositivos, imprescindibles para que, la ya por sí ardua tarea de recolección de la base de datos, sea realizada de la manera más exacta y rápida posible, sin errores, y con la posibilidad de corregir los mismos de manera rápida y efectiva, en el caso extremo de que la adquisición falle en algún punto.

Una vez asegurada la correcta programación de todas las aplicaciones, se ha procedido a iniciar el proceso de captura de la base de datos, en la cual se ha incluido intra e inter-variabilidad, variabilidad temporal (multisesión) e interoperabilidad (múltiples dispositivos).

Dicha captura se encuentra en proceso y pretende continuar con una segunda e incluso una tercera sesión, así como el posterior análisis de los resultados obtenidos mediante la aplicación de sistemas biométricos de reconocimiento de escritor sobre las muestras obtenidas. Esto permitirá conocer la capacidad de reconocimiento biométrico a través de dispositivos comúnmente utilizados en la sociedad actual; y en un futuro, desarrollar sistemas más robustos ante las variabilidades observadas.

2

Introducción al reconocimiento biométrico

El reconocimiento biométrico es una rama teconológico-cientifica utilizada, en general, con objetivos de identificación o verificación de usuarios. Mientras que el primer objetivo hace referencia al proceso de determinar a cuál de los usuarios registrados en la base de datos corresponde la muestra de interés (relación 1:N, donde N corresponde al número de usuarios registrados en la base de datos); la verificación de usuarios corresponde a autenticar a un individuo que dice ser un usuario específico ya registrado (relación 1:1).

La principal ventaja del uso de rasgos biométricos en la verificación/identificación de usuarios reside en que el reconocimiento está basado en quién es la propia persona, y no en lo que sabe o porta. En contraposición a los métodos tradicionales de reconocimiento, que utilizan información correspondiente a objetos portados por el individuo (p.ej llaves o tarjetas), fáciles de perder o ser sustraídos; así como claves conocidas por dicha persona (código o contraseñas), fáciles de olvidar; los métodos biométricos tratan al individuo (junto con sus características anatómicas y de comportamiento) como la propia 'llave/clave' del sistema, rasgos difíciles de alterar, transferir u olvidar, y en general, perdurables en el tiempo.

El rendimiento de los sistemas de reconocimiento de usuario mediante rasgos biométricos se mide en función de un umbral preestablecido por experimentación, de forma que se pueden obtener dos resultados: *aceptación* o *rechazo*. Cuando una nueva muestra a verificar es introducida y comparada con una muestra registrada en la base de datos, en función de la puntuación resultante de la comparación, la muestra será reconocida como genuina siempre que dicha puntuación supere el umbral establecido. En relación a estas consideraciones, los posibles fallos del sistema serían aceptar como genuina una muestra realizada por otro usuario (*FA* - Falsa Aceptación), o bien establecer como falsa una firma original de un usuario (*FR* - Falso Rechazo).

Dado un considerable número de muestras genuinas y e impostoras (o no genuinas), así como un conjunto de pruebas de verificación, se pueden establecer las Tasas de Falsa Aceptación (FAR) y Falso Rechazo (FRR) para diferentes umbrales de decisión, permitiendo evaluar el rendimiento del sistema de reconocimiento biométrico.

Con el fin de comparar el rendimiento entre diferentes sistemas de verificación, se suele utilizar como medida el punto en el cual la FAR y la FRR son iguales, es decir, la ERR (*Equal Error Rate*), y que sería el punto de trabajo del sistema. Para establecer el punto de trabajo del sistema se utiliza la representación mediante curvas *DET*, en donde cada punto de la gráfica define un valor de Falsa Aceptación (FAR) y de Falso Rechazo (FRR), permitiendo la evaluación

y comparación entre diferentes sistemas sin necesidad de tener en consideración múltiples curvas.

2.1. Modalidades biométricas

El reconocimiento biométrico es la ciencia que establece la identidad de una persona en función de sus rasgos fisiológicos y de comportamiento. Dentro de los rasgos biométricos mas comúnmente usados, pueden destacar huella dactilar, rostro, iris, voz, geometría de la mano, forma de la oreja, huella palmar, firma, escritura, forma de andar y dinámica de tecleo (Figura 2.1).

Figura 2.1: *Ejemplos de rasgos personales que pueden ser usados para el reconocimiento biométrico.*

Los rasgos fisiológicos incluyen rostro, huella dactilar, iris, huella palmar, geometría de la mano y forma de la oreja; mientras que la forma de andar, firma, escritura y dinámica de tecleo son características incluidas dentro de los rasgos de comportamiento.

En general, cualquier característica humana fisiológica y/o de comportamiento puede ser considerada, y usada, como una característica biométrica siempre que satisfaga los siguientes requerimientos:

- **Universalidad**: el rasgo debe estar presente en todos los individuos.
- **Perdurabilidad**: en relación con la invarianza imprescindible del rasgo a lo largo del tiempo.
- **Distintividad**: característica relacionada con el poder de discriminación entre individuos que presenta el rasgo biométrico.
- **Mensurabilidad**: la característica debe ser medible cuantitativamente.

Sin embargo, en la práctica, a la hora de utilizar un sistema que emplee rasgos biométricos para el reconocimiento, es necesario considerar un conjunto de características adicionales:

- Rendimiento: referente a la necesidad de precisión del sistema.
- Aceptabilidad: indica el grado de uso de una característica biométrica en la vida diaria.
- Elusión: característica que refleja la facilidad con que el sistema puede ser engañado mediante el uso de métodos fraudulentos.

La utilización de una u otra técnica biométrica depende, en gran medida, de los requerimientos de la aplicación a desarrollar. No existe una única técnica que supere a todo el resto en todos los entornos operacionales. En este sentido, todas las técnicas serán admisibles y cada una será óptima en su campo de aplicación.

En particular, un sistema biométrico debe proporcionar la precisión de reconocimiento necesaria, la velocidad y recursos requeridos, ser aceptado por la población hacia la que está dirigido, así como ser inofensivo para la misma, y ser suficientemente robusto ante posibles ataques al sistema.

2.2. Aceptación en la sociedad y privacidad

El éxito de los sistemas de reconocimiento de identidad basados en técnicas biométricas está dictaminado en gran parte por factores humanos. La facilidad y confort que presenten dichos sistemas ayudará a su aceptación en la sociedad. Por ejemplo, un sistema capaz de extraer las características de un individuo sin contacto con el mismo, como la utilización de la voz y el iris, o sistemas que requieren muy poca cooperación por parte de éste, como el uso del rostro, pueden ser considerados más amigables para el usuario.

Por otro lado, hay características biométricas que, sin el conocimiento del usuario, pueden ser capturadas durante el proceso, atacando la privacidad personal; entre éstas podemos destacar, por ejemplo, cuando una persona es identificada cada vez que realiza una compra con su tarjeta de crédito, la información sobre dónde se encuentra dicho individuo o qué está comprando es capturada y puede ser usada en contra de la ética humana.

En el caso específico de este proyecto, en el cual estamos tratando con el rasgo de la firma, la privacidad se convierte en un punto clave del proceso, puesto que las firmas recogidas podrían ser usadas para suplantar la identidad del individuo participante. Es por esto que todos los usuarios participantes en el proceso son avisados previamente de los objetivos y el uso de carácter investigador de los datos que van a proporcionar, asentando unas bases legales sobre los mismos, e iniciando el proceso de captura únicamente cuando el individuo haya entendido y aceptado todos los términos del acuerdo.

En el lado positivo de la privacidad del individuo con respecto a los sistemas biométricos, cabe destacar que dichos sistemas son utilizados como uno de los métodos más efectivos para evitar, precisamente, la invasión de la privacidad de las personas. De hecho, el objetivo de este proyecto es analizar el rendimiento de dichos sistemas evitando la suplantación de la identidad de los usuarios mediante firmas falsificadas con un alto grado de precisión.

3

Verificación de firma

3.1. Introducción

La verificación o reconocimiento de firma compone un gran campo de estudio dentro de la ciencia de reconocimiento biométrico. Se define como un método de identificación personal basado en escritura.

El reconocimiento de individuos mediante sistemas de verificación de firma constituye un gran reto para la biometría debido a múltiples factores:

- *Grandes variaciones intraclase*: un mismo individuo puede realizar diferentes versiones de su propia firma, todas ellas genuinas, generando grandes variabilidades intrapersonales que será necesario tener en cuenta a la hora de verificar la identidad de un usuario.
- *Pequeñas variaciones interclase*: los sistemas de verificación de firma deben tener en cuenta posibles falsificaciones de firmas, la cuales pueden ser muy similares a las firmas genuinas.
- *Baja universalidad*: en sentido en que no todo el mundo posee, o es capaz de realizar una firma.
- *Baja permanencia*: la firma de un individuo tiende a variar con el tiempo.

Dentro de las posibles falsificaciones que tiene que hacer frente el sistema de verificación, los impostores pueden conocer información acerca del usuario, lo que empeora el rendimiento del sistema. Con respecto a esta información, se pueden distinguir dos tipos de impostores: *Impostores casuales* e *Impostores reales*. Mientras que los primeros se caracterizan por no conocer información sobre las propiedades de la firma a falsificar, produciendo falsificaciones aleatorias (*random forgeries*); los impostores reales conocen información estática y/o dinámica en relación a la firma del usuario original y producen falsificaciones expertas (*skilled forgeries*).

Los métodos de verificación de firma pueden ser clasificados en dos grandes grupos:

- **On-line**: dentro de este grupo se encuentran los sistemas de verificación de firma que utilizan funciones de tiempo correspondientes a procesos de firma dinámica (p.ej. trayectorias, presión, tiempo,etc.). Estos parámetros son obtenidos mediante el uso de dispositivos como tabletas digitales o pantallas táctiles.

- **Off-line**: en relación al uso, únicamente, de la imagen estática de la firma.

Ambos métodos están muy relacionados, de forma que parte de la información dinámica puede ser estimada a partir de imágenes estáticas así como se pueden generar imágenes estáticas a partir de información dinámica.

En este proyecto, se van a recoger muestras con el posterior objetivo de aplicar sobre ellas técnicas de *verificación de firma tanto on-line como off-line* para evaluar los diferentes esquemas de reconocimiento basados en la interoperabilidad existente.

3.1.1. Estandarización

Siguiendo con el objetivo de este proyecto, es imprescindible permitir la interoperabilidad entre las muestras recogidas y los diferentes dispositivos en lo que se refiere a estandarizar el formato de transmisión y almacenamiento de la firma. Para ello se han fijado una serie de canales estándar (posiciones x e y, marcas de tiempo, frecuencia de captura y normalización de la presión) comunes para todos los sistemas de captura, con el fin de conseguir resultados óptimos a la hora de comparar los diferentes sistemas.

3.2. Sistemas de verificación de firma On-Line

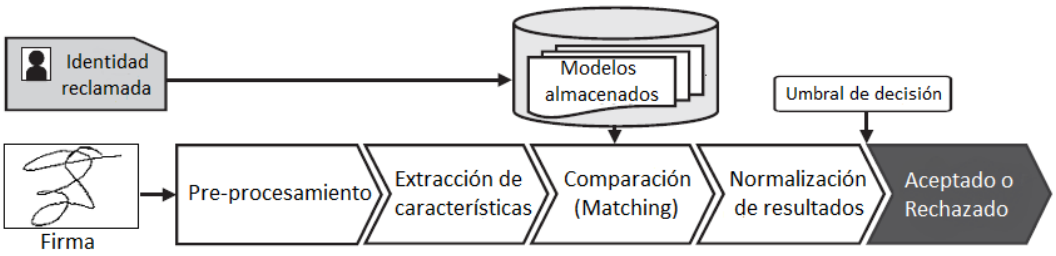

Figura 3.1: *Arquitectura de un sistema de verificación de firma.*

3.2.1. Adquisición de datos y pre-procesamiento

En general, la adquisición de las funciones de tiempo correspondientes a una firma escrita tiene lugar a través de dispositivos tales como tabletas digitales, PDAs, smartphones o Tablet PCs. Estos dispositivos serán los encargados de proveer la información sobre la trayectoria, tiempo, presión y ángulos de inclinación del pen (azimut). La frecuencia de captura de muestras correspondiente a este tipo de dispositivos se encuentra en torno a los 100-200 Hz (muestras por segundo). Esta frecuencia es suficiente para obtener una representación precisa de la firma, puesto que la frecuencia media de realización de una firma se encuentra por debajo de los 20-30Hz.

Tras la adquisición de datos se realiza un pre-procesamiento de los mismos, previo a la extracción de características, con el objetivo de filtrar posible ruido, así como de realizar un remuestreo para obtener una representación estática consistente de puntos equidistantes.

Dentro de todo el sistema de verificación, esta es la fase específicamente desarrollada e implementada en el proyecto.

3.2.2. Extracción de características

Este proceso tiene como resultado la extracción de información discriminatoria a partir de los datos de la firma on-line.

Los métodos de extracción de características se agrupan en dos grandes clases:

1. **Basados en características**: extraen el conjunto de características globales derivadas de la trayectoria de la firma.
2. **Basados en funciones**: extraen secuencias de tiempo que describen las propiedades de la firma, como la velocidad, presión, trayectoria, etc. Estos métodos, a partir de experimentación, han demostrado ser más adecuados que los anteriores, adecuándose mejor a los problemas que presenta la verificación de firma.

La extracción de características se puede realizar durante la fase de registro, o durante la fase de desarrollo; sin embargo, debido a las grandes diferencias de información y complejidad entre diferentes firmantes, es aconsejable realizarla antes del desarrollo, es decir, durante la fase de registro.

3.2.3. Registro

En función de la estrategia de comparación (matching) a utilizar, la fase de registro se puede dividir en dos modalidades:

- *Basado en referencia*: las características extraídas a partir de una firma de entrenamiento son almacenadas como un modelo de firma, de forma que cada firma de entrenamiento de un usuario poseerá un modelo de firma. El proceso de correspondencia (matching) se lleva a cabo, por tanto, comparando las firmas de entrada con cada uno de los modelos almacenados y combinando los resultados coincidentes mediante técnicas de fusión.
- *Basado en modelo*: el conjunto de firmas de entrenamiento de un sujeto dado se usa para estimar el modelo único estadístico el cual escribe el comportamiento de cada firmante particular. Cada modelo estadístico requiere un mínimo de 4-6 firmas de entrenamiento para que el sistema tenga un rendimiento aceptable.

Por tanto, cuando el conjunto de firmas de entrenamiento es pequeño (<5), el registro basado en referencia será el más adecuado, y viceversa. Sin embargo, a pesar de que los modelos basados en referencia pueden dar resultados satisfactorios para un conjunto de entrenamiento de menos de 5 firmas, el mejor rendimiento para cualquier modelo se obtiene con un mínimo de 5 firmas.

3.2.4. Pre-Alineamiento y Matching

La fase de comparación o *matching* puede venir precedida por un proceso de pre-alineamiento entre la muestra de entrada y la muestra registrada en el modelo correspondiente. En el caso de sistemas que no utilicen un proceso de pre-alineamiento específicamente separado y previo al matching, se realizará un proceso similar embebido en el matching, o bien directamente se alinearan las muestras durante el proceso de adquisición.

Con respecto al proceso de matching, para un sistema de verificación que conste de un proceso de extracción basado en características seguido de un registro basado en referencia, la puntuación resultante de la comparación entre dos muestras es obtenida en relación a una serie de medidas de

distancia entre las mismas, como puede ser la distancia Euclidea, o la distancia de Mahalanobis. En el caso de sistemas cuya extracción está basada en funciones, en función de la estrategia de comparación utilizada, los sistemas pueden ser divididos en dos enfoques:

1. *Local*: Con este enfoque, las funciones de tiempo procedentes de las diferentes muestras son directamente comparadas mediante el uso de medidas de distancia elásticas como DTW (Alineamiento Temporal Dinámico - *Dynamic Temporal Warping*). Mediante DTW se busca alinear temporalmente las firmas a comparar para poder realizar medidas de distancia de manera satisfactoria.

2. *Regional*: Si se elige un enfoque regional, las funciones temporales de las muestras son convertidas a una secuencia de vectores, de forma que cada vector describe una propiedad regional de un segmento de la firma. Uno de los enfoques más utilizados es el método basado en HMM (Modelos Ocultos de Markov - *Hidden Markov Models*); éstos modelan de manera probabilista, en contraposición a DTW el cual modela de forma determinista, las muestras a comparar utilizando un modelo basado en:

   - Número de estados.
   - Número de símbolos observables.
   - Matriz de probabilidades de transición.
   - Distribución de probabilidades de observación en cada estado.
   - Probabilidad de ocupación inicial de cada estado.

3.2.5. Normalización de resultados

Las puntuaciones obtenidas tras la comparación de la muestra de entrada con las muestras registradas son normalizadas a un rango común como puede ser [0,1], antes de compararlas con un umbral de decisión para determinar si se trata de una muestra genuina o no, usando diferentes funciones de mapeo [13]. El paso de normalización de resultados es crucial en el caso de combinar diferentes procesos de comparación o diferentes escenarios de captura.

4

Bases de datos. Estado del arte

4.1. Introducción

Durante años, se han utilizado mezclas de bases de datos unimodales existentes para generar conjuntos multimodales y utilizarlos como bases de datos multimodales reales, sin embargo, estos datos no están correlados puesto que no han sido adquiridos siguiendo el mismo protocolo de captura, lo que provoca que los resultados obtenidos no sean óptimos ni reales. Por este motivo, con el objetivo de eliminar el uso de bases de datos multimodales falsas, surgen bases de datos tales como MCYT (2003), BIOMET (2003), MyIDEA (2005), BioSec (2007), BiosecurID (2007) o Biosecure (2008), bases multimodales reales, con las que obtener resultados de reconocimiento reales y válidos. Las principales características de estas bases de datos quedan esquematizadas en la Tabla 4.1 y posteriormente serán explicadas más detalladamente.

El inconveniente de estas bases de datos es el gran aumento de tiempo de captura que conllevan, así como los posibles inconvenientes que pueden generar en los usuarios a registrar a la hora de tener que solicitarles realizar capturas de múltiples rasgos personales, lo que ataca su privacidad y provoca una gran inversión de tiempo por su parte. Son estas las principales razones de que exista un número muy limitado de bases de datos bimétricas multimodales.

4.2. Bases de datos existentes

	Año	Ref.	Usuarios	Sesiones	Rasgos	2Fa	3Fa	Hd	Gm	Es	Ir	Dt	Fi	Vz
Biosecure	2008	[2]	971 (DS1, Internet)	2	2	X								X
			667 (DS2, Escritorio)	2	6	X		X	X		X		X	X
			713 (DS3, Móvil)	2	4	X		X					X	X
BiosecurID	2007	[6]	400	4	8	X		X	X	X	X	X	X	X
BioSec	2007	[5]	250	4	4	X		X			X			X
MyIDEA	2005	[4]	104 (aprox.)	3	6	X		X	X	X			X	X
MBioID	2007	[7]	120 (aprox.)	2	6	X	X	X			X		X	X
MCYT	2003	[3]	330	1	2			X					X	

Tabla 4.1: *Bases de datos más significativas. La nomenclatura es la siguiente:* 2Fa *se utiliza para referirse a Imagen facial (Rostro) en 2D,* 3Fa *para Imagen facial en 3D,* Hd *para Huella dactilar,* Gm *para Geometría de la mano,* Es *para Escritura,* Ir *para Iris,* Dt *para Dinámica de tecleo,* Fi *para Firma y* Vz *para Voz.*

A continuación se va a realizar un desglose más detallado de las características que poseen las principales bases de datos multimodales existentes, ordenadas temporalmente.

4.2.1. MCYT

La adquisición fue llevada a cabo por diversas instituciones universitarias españolas, entre las que se encuentra el Grupo de Reconocimiento Biométrico, *ATVS*, de la Universidad Autónoma de Madrid (UAM). Esta base de datos se caracteriza por incorporar firmas y huellas dactilares de 330 individuos.

Con respecto a las huellas dactilares recogidas, para cada individuo han sido adquiridas doce muestras de cada uno de los dedos mediante dos sensores diferentes.

Por el otro lado, para cada individuo se registraron 25 firmas genuinas y 25 firmas falsificadas; las firmas incluyen información tanto on-line (trayectorias, tiempo, azimut y presión) como off-line (imagen de la firma escrita).

4.2.2. BIOMET

Esta base de datos presenta cinco modalidades diferentes: Imagen facial (en 2D y 3D), huella dactilar, geometría de la mano, firma y voz. En relación al rostro o imagen facial, además de tomar imágenes con una cámara digital convencional, se utilizan también imágenes tomadas con una cámara de luz infrarroja, eliminando la posible influencia de la luz ambiental.

Se contempla variabilidad temporal mediante una adquisición dividida en tres sesiones con tres y cinco meses de diferencia temporal entre ellas. El número de participantes resultó en 130 para la primera sesión, 106 para la segunda y 91 para la última. El género y la edad de los individuos presenta una distribución balanceada en todas las sesiones, asegurando resultados realistas.

4.2.3. MyIDEA

La base de datos MyIDEA presenta muestras para seis rasgos biométricos: Imagen facial en 2D, huella dactilar, geometría de la mano, escritura, firma y voz. Además de realizar una adquisición independiente de cada rasgo biométrico, esta base de datos se caracteriza por realizar dos capturas conjuntas sincronizadas: rostro-voz y escritura-voz.

Las principales características de MyIDEA se pueden resumir en: 104 individuos registrados, múltiples sensores de diferente calidad, varios escenarios que aseguran una adquisición realista y una organización clara de las muestras recogidas para simplificar la posterior utilización de las mismas, en investigación abierta al público.

4.2.4. BiosecurID

Esta base de datos surge como consecuencia del éxito de bases de datos anteriores, tales como MCYT. Se trata de un proyecto fundado por el Ministerio de Ciencia y Tecnología en el cual han participado seis instituciones académicas españolas entre las que se encuentra el Grupo de Reconocimiento Biométrico ATVS de la UAM.

Uno de los principales objetivos que persigue es construir una nueva base de datos multimodal extendiendo la ya existente base de datos BIOSEC, en términos de incluir nuevas sesiones para sujetos ya registrados, así como incluir nuevos datos biométricos y nuevos sujetos.

Esta nueva base de datos consta de los siguientes rasgos biométricos: Imagen facial en 2D, geometría de la mano, huella dactilar, escritura, iris, dinámica de tecleo, firma y voz. El número de usuarios registrados aumenta hasta 400 y consta de 4 sesiones distribuidas en cuatro-un mes de margen temporal.

4.2.5. Biosecure

Este proyecto está impulsado por la necesidad de coordinar los múltiples esfuerzos en el campo de la investigación biométrica a lo largo de toda Europa; más de 30 instituciones de investigación procedentes de 15 países diferentes han participado en el proyecto. El grupo de Reconocimiento Biométrico ATVS se encuentra a cargo de las actividades relacionadas con la adquisición de base de datos a través de la red (Internet). Esta nueva base de datos, la cual incorpora tres conjuntos diferenciados : Internet, escritorio y móvil, captura diferentes rasgos biométricos en función del escenario (Tabla 4.1).

Biosecure se caracteriza por ser la única base de datos que incorpora dos dispositivos diferentes para la adquisición de firmas: WACOM y PDA. Cabe destacar cómo, a pesar de que las PDAs pueden estar actualmente clasificadas como dispositivos desfasados debido a su baja calidad, todavía son ampliamente utilizadas.

5

Base de datos e-BioFirma, diseño y adquisición

5.1. Base de datos e-BioFirma. Introducción

Como ya se ha hecho hincapié anteriormente, la firma es el rasgo biométrico más ampliamente aceptado en el campo de verificación de identidad. Por este motivo, las nuevas tecnologías buscan incorporar esta posibilidad de identificación en los dispositivos emergentes como una técnica de reconocimiento satisfactoria para el usuario.

El principal problema que presenta este rasgo es su baja perdurabilidad, así como la facilidad de ser falsificada por un individuo con información suficiente sobre la misma.

Con toda esta información en mente, la base de datos e-BioFirma surge con el objetivo de dar solución a todos estos problemas permitiendo el desarrollo de sistemas competentes ante toda esta variabilidad.

Debido a la gran variedad de dispositivos comerciales existentes, así como al acelerado desarrollo y avance de los mismos, se ha decidido crear una base de datos multi-dispositivo que abarque la mayor parte de las características de los dispositivos comercializados, incluyendo tanto tabletas específicamente diseñadas para la captura de escritura y firma, como tabletas de uso general.
Es por ello que la base de datos incluye firmas y escritura capturadas mediante cinco dispositivos (Figura 5.1) :

1. **WACOM STU-500**: Dispositivo de adquisición de firmas que se caracteriza por poseer 512 niveles de presión real de superficie similar al papel, rápida visualización en tiempo real y una pantalla TFT-LCD reflectante que proporciona una sensación de escritura natural. Características:
   - Frecuencia de muestreo: 200Hz (5 ms/muestra).
   - Resolución: VGA de 640×480 pixeles.
   - Pantalla monocromática de 5 pulgadas.

Figura 5.1: *Entorno de trabajo e-BioFirma. Dispositivos utilizados en la captura.*

2. **WACOM STU-530**: Dispositivo mejorado, caracterizado por poseer 1024 niveles de sensibilidad a la presión y un cifrado AES (256 bits)/RSA (2048 bits) de las firmas recogidas, lo que garantiza transacciones seguras. Características:
   - Frecuencia de muestreo: 200Hz (5 ms/muestra).
   - Resolución: VGA de 640×480 pixeles.
   - Pantalla a color de alta resolución de 5 pulgadas.
3. **WACOM DTU-1031**: Dispositivo que combina una gran pantalla (26cm) y un cifrado actual RSA/AES para asegurar transacciones seguras. La pantalla permite al usuario añadir anotaciones manuscritas directamente sobre el monitor con un bolígrafo digital. Además, permite visualizar documentos de tamaño completo y firmarlos digitalmente. Características:
   - Frecuencia de muestreo : 200Hz (5 ms/muestra).
   - Pantalla LCD a color de 10.1 pulgadas.
   - Bolígrafo sin batería que mejora la sensación de escritura natural y ofrece un perfil de presión durante todo el proceso de escritura y firma.
4. **SAMSUNG ATIV 7 (WIN8)**: Dispositivo en el que se encuentran integrados en la propia pantalla todos sus componentes, resultando en una tablet ligera y con posibilidad de ser utilizada como ordenador portátil gracias al teclado que incorpora. A su vez, el dispositivo integra 3 puertos USB (2.0 y 3.0). Presenta una pantalla de 11.6 pulgadas, resolución de 1920×1080 puntos y 10 puntos de presión simultanea que aseguran una correcta experiencia táctil. Por último, incorpora un lápiz óptico S-pen para asegurar una precisión absoluta.
5. **SAMSUNG GALAXY NOTE 10.1 (ANDROID)**: Se trata de una tablet de 10.1 pulgadas en la cual, por primera vez en la gama de dispositivos Samsung Galaxy Note, es prescindible el uso del lápiz digital táctil. Presenta una resolución de 1280×800 puntos y un puerto USB 2.0.

Mediante la combinación de estos dispositivos, fijando un área de firma igual en todos ellos, así como un mismo protocolo de adquisición, se puede desarrollar una base de datos multi-dispositivo.

Sin embargo, con el objetivo de capturar una base de datos lo más completa posible, queda tener en cuenta un punto crucial como es el actual desarrollo de las actividades vía Internet, sustituyendo a las operaciones tradicionales, no solo en dispositivos estáticos como puede ser un ordenador de sobremesa, sino principalmente en dispositivos portátiles como los smartphones. Por este motivo, puesto que queda claro que la seguridad es la clave fundamental del éxito de las operaciones vía Internet, pensando en dispositivos portátiles se ha incorporado en la base de datos un proceso de firma e introducción de DNI (*Documento Nacional de Identidad*) realizado con el dedo, adaptando así la base de datos al escenario real en el que se realizaría la verificación de identidad.

5.2. Diseño y descripción

La base de datos e-BioFirma ha sido recogida en múltiples entornos, tanto en laboratorio cómo en lugares no específicamente preparados para la adquisición, con el fin de ser lo mas realista posible. Se caracteriza por capturar dos rasgos biométricos: firma y escritura; la recogida de estos dos rasgos tiene su razón de ser en el hecho de que en un futuro, a la hora de verificar la identidad de un usuario, en caso de que la firma no sea información suficiente para determinar si se trata del usuario genuino, el proceso puede ser apoyado por la escritura del individuo. En el caso de esta base de datos se solicita escribir nombre y primer apellido en minúsculas y mayúsculas, consiguiendo así resultados de reconocimiento más robustos.

Otra característica innovadora que recoge esta base de datos, tanto en firma como en escritura, son los *"hovering points"(puntos flotantes)*, es decir, los puntos de trayectoria del pen cuando el usuario no está presionando físicamente la pantalla, pero tiene el pen cerca de ella y, por tanto, forma parte de la información de su firma o escritura. Mediante la incorporación de este parámetro, se espera que los resultados de reconocimiento y verificación de identidad mejoren en gran medida con respecto a sistemas desarrollados previamente.

Como ya se ha comentado, puesto que esta base de datos va dirigida a futuras operaciones con dispositivos móviles, los cuales se suelen caracterizar por poseer una pantalla mas reducida, así como por ser manejados con el dedo en lugar de con un pen, la base de datos incorpora un proceso de firma e introducción de DNI con el dedo; la razón por la que se ha decidido incluir la introducción de DNI es la misma que la de introducir el nombre, es decir, para aumentar la seguridad; sin embargo, puesto que en las pequeñas pantallas de los smartphones es inviable escribir nombre y apellido con el dedo, se ha decidido sustituir este proceso por la introducción de DNI.

Por motivos de privacidad, no se ha solicitado a los usuarios registrados escribir su DNI oficial, por lo que para cada individuo se ha pedido realizar todos los números del 0-9 y una letra de las 23 posibles existentes en los DNI, calculada a partir de su posición en un vector común a todos los usuarios, posición resultante del módulo de 23 con el número del usuario correspondiente, de forma que todas las letras posibles resulten escritas por algún usuario.

El objetivo de e-BioFirma es recoger los datos ya mencionados para dos conjuntos de usuarios en dos sesiones diferentes, con una diferencia temporal de 2 meses. El primer conjunto, constituido por usuarios de la UAM, espera contar con alrededor de 50 usuarios, mientas que el segundo conjunto, constituido por usuarios de una empresa que mantiene una colaboración con el ATVS, espera contar con otros 50 usuarios. La diferencia entre los dos conjuntos se basa, de nuevo, en motivos de privacidad de la identidad del usuario; es por este motivo que a los usuarios de la empresa solo se les solicita realizar firmas originales, sin nombre, DNIs ni falsificaciones.

Las muestras recogidas con el pen se almacenaran en ficheros '.txt' con la siguiente nomenclatura:

`U[uid]_s[sid]_g[group]_[info]_[tool]_[mode]_[num].txt`

Dónde:

- *uid*: Número de identificación de usuario (User identification number).
- *sid*: Número de sesión (Acquisition session number).
- *group*: Número de grupo: g1 (UAM) o g2 (Empresa).
- *info*: sign (firma), nam1 (Nombre y Apellidos) o nam2 (NOMBRE y APELLIDOS)
- *tool*: Tipo de dispositivo: w1 (Wacom STU-500), w2 (Wacom STU-530), w3 (Wacom DTU-1031), w4 (Samsung ATIV 7), w5 (Samsung Galaxy Note 10.1)
- *mode*: c (cliente), s (impostor)
- *num*: Número de muestra recogida.

Cada archivo `('U[uid]_s[sid]_g[group]_[info]_[tool]_[mode]_[num].txt')` contendrá la siguiente información relativa a cada firma (o nombre) recogido:

- Primera fila: numero de muestras que compone la firma/nombre/secuencia alfanumérica.
- Resto de filas:
  - Puntos 'x' e 'y' (1^a y 2^a columna del archivo).
  - Tiempo (3^a columna).
  - Presión (4^a columna).

Cabe destacar el caso del dispositivo WACOM DTU-1031, el cual permite capturar tanto el tiempo de la tableta (3^a columna) como el tiempo del sistema (5^a columna), siendo éste último menos constante que el de la tableta, como se puede observar en el ejemplo de la figura 5.2. Por esta razón, los archivos que contienen muestras capturadas con WACOM DTU-1031 contendrán una columna adicional que podrá ser eliminada en una etapa de post-procesamiento en caso de necesidad.

En el resto de los casos, el tiempo de captura se corresponde con el tiempo de la tableta (constante, 5ms entre muestras consecutivas) para la WACOM STU-500 y WACOM STU-530, y con el tiempo del sistema para Samsung ATIV 7 y Samsung Galaxy Note 10.1, debido a que estos últimos, al no ser dispositivos específicos de captura de escritura, no permiten obtener el tiempo de tableta.

Con respecto a las muestras recogidas con el dedo, las cuales solo son recogidas con los dos últimos dispositivos : w4 (Samsung ATIV 7) y w5 (Samsung Galaxy Note 10.1) puesto que son los únicos táctiles así como los únicos en los que tiene sentido recoger este tipo de muestras realísticamente hablando, imitando el caso del uso de un smartphone, la nomenclatura es la misma con la excepción de:

- *info*: sFin (firma con el dedo), nFin (DNI con el dedo).
- *tool*: Tipo de dispositivo: w4 (Samsung ATIV 7), w5 (Samsung Galaxy Note 10.1).

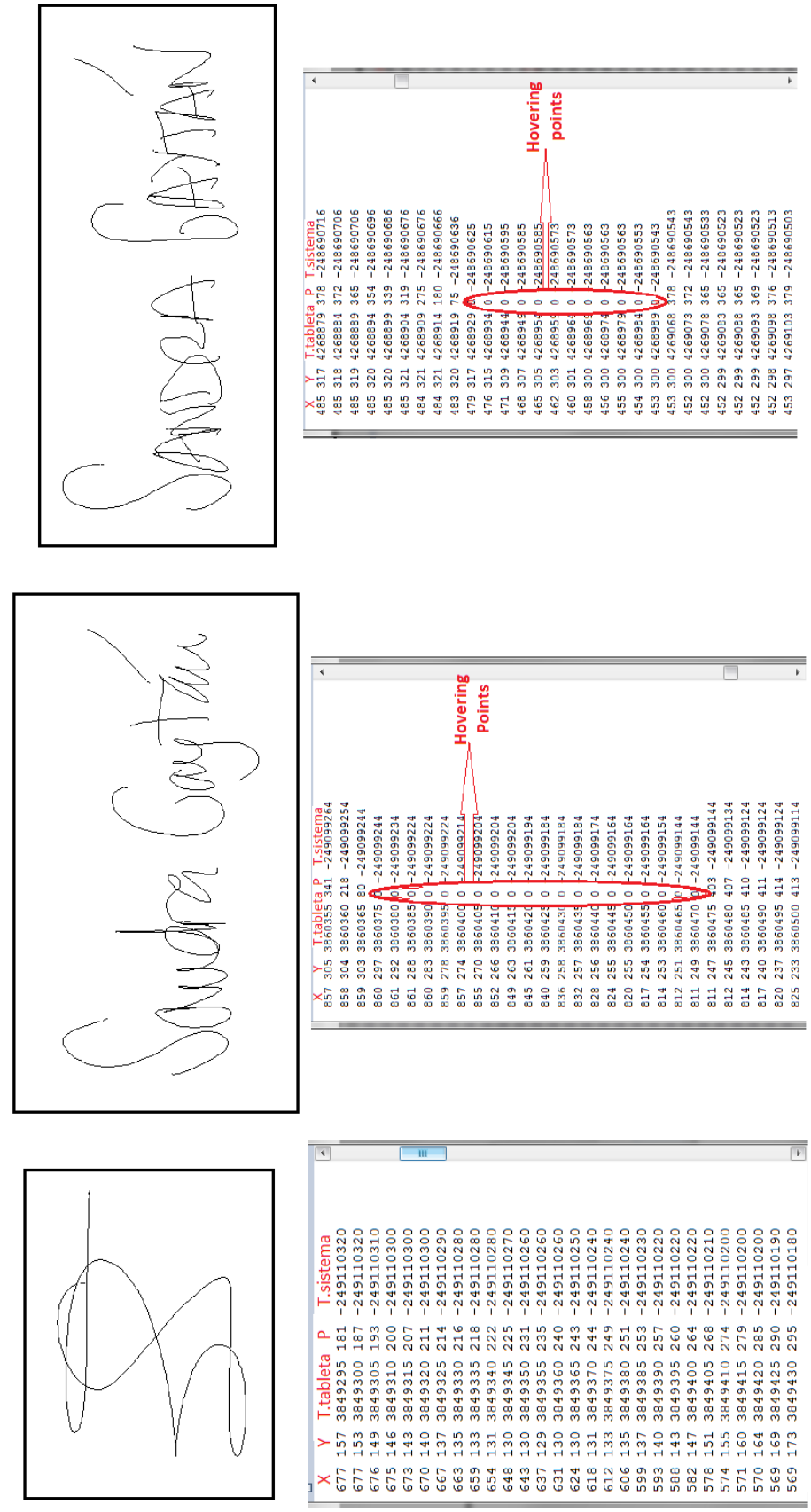

Figura 5.2: *Muestras reales realizadas con el pen capturadas con la WACOM DTU-1031.*

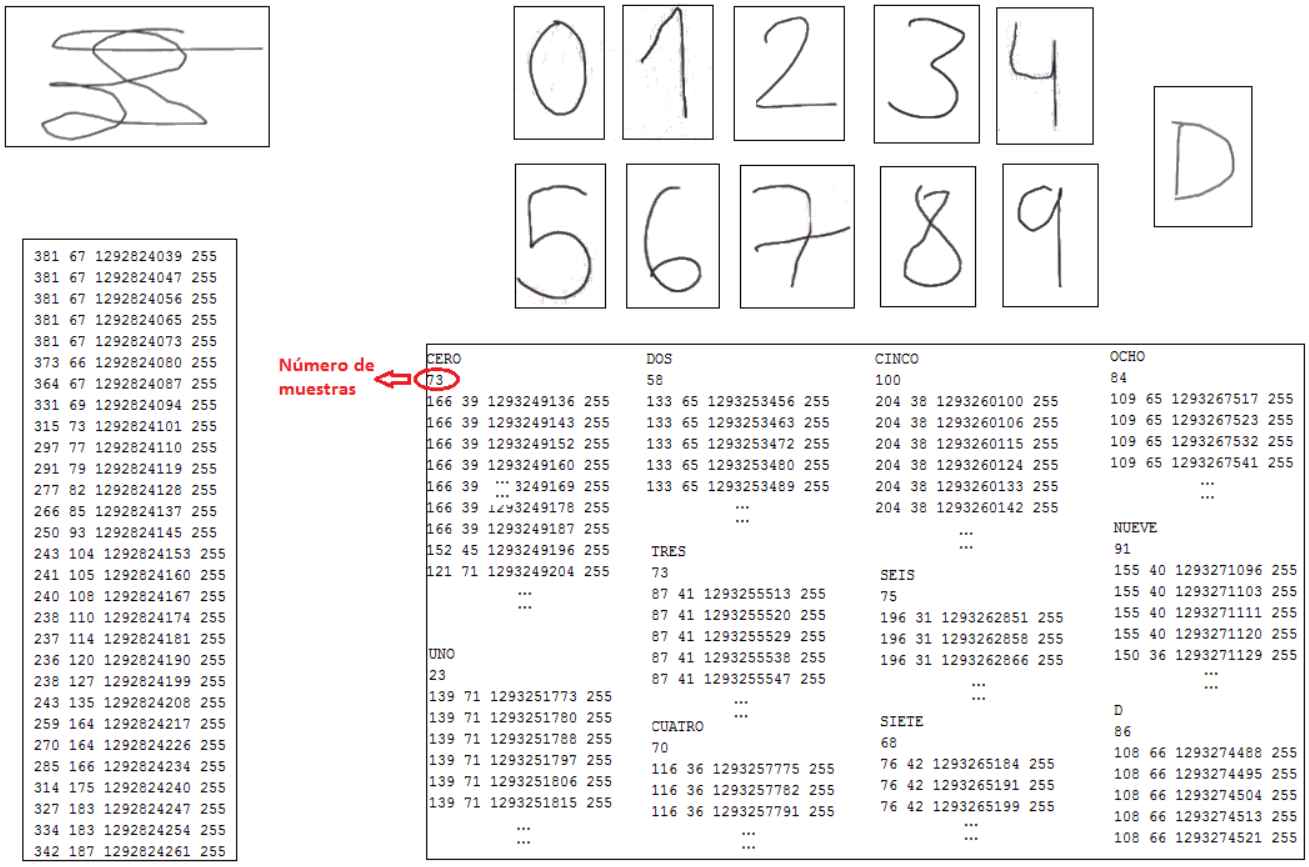

Figura 5.3: *Muestras reales realizadas con el dedo capturadas con el Samsung Galaxy Note 10.1.*

Los archivos que contienen las muestras realizadas con el dedo poseen la misma información que las muestras recogidas con el pen, sin embargo, en el caso del DNI la información se organiza en las mismas columnas, pero con todos los números recogidos y la letra en el mismo '.txt'. Un ejemplo de muestras recogidas realizadas con dedo se puede observar en la figura 5.3. Cabe destacar que para las muestras recogidas con el dedo, las tabletas no aportan información de presión, por lo que se ha fijado dicho valor a 255 con el fin de guardar la coherencia con los archivos que contienen las muestras recogidas con el pen.

5.3. Adquisición y validación de los datos adquiridos

El proceso de adquisición, ordenado temporalmente, queda esquematizado en la Figura 5.4. Un usuario que realice este proceso habrá completado una sesión de captura de la base de datos.

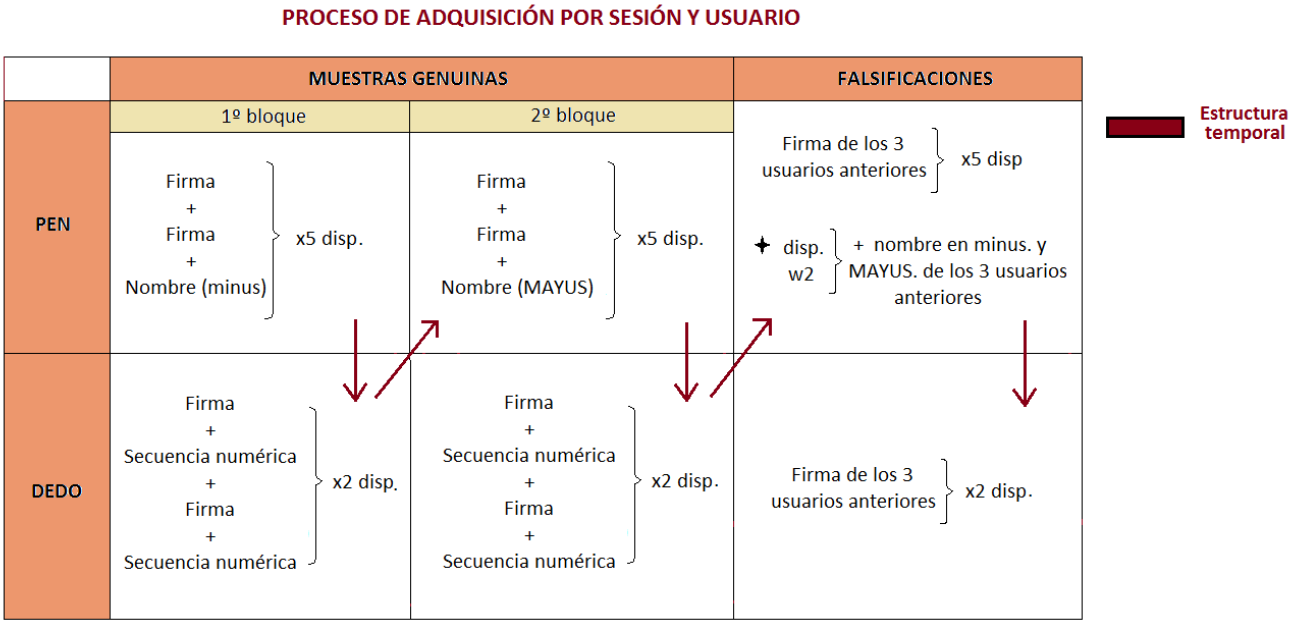

Figura 5.4: *Proceso generalizado de adquisición de la base de datos e-BioFirma realizado por un usuario para completar una sesión.*

Con respecto a las falsificaciones, mientras que para la primera sesión se muestra la firma original del usuario a imitar de manera dinámica, es decir, a tiempo y velocidad real de realización, tantas veces como el usuario lo requiera; para la segunda sesión se ha establecido un proceso de falsificación con calco proporcionando la firma impresa en papel del usuario original, de forma que el falsificador pueda colocarla sobre la pantalla del dispositivo e intentar imitarla. En este segundo caso, queda patente cómo la forma de la firma falsificada será muy similar a la original, por lo que las principales diferencias se encontrarán en la velocidad y presión. La decisión de incluir este tipo de falsificaciones se ha tomado debido a que consideramos que el caso de falsificación más realista en el mundo empresarial actual es un caso a nivel interno en el que el imitador posee la firma concreta del usuario.

Además, otra propuesta interesante a incorporar en la segunda sesión de captura serían los *disguised*, también conocidos como firmas disfrazadas; en este tipo de captura, el usuario debe realizar su propia firma de forma que aparentemente parezca la original, pero que tenga alguna modificación tal como la velocidad de realización, el orden de escritura, etc. Esto es interesante en el caso de que un individuo realice una firma que aparenta ser la suya, y posteriormente declare que no es genuina apoyándose en resultados de reconocimiento biométrico, los cuales efectivamente la clasificarán de falsificación cuando se trata de una firma original. Con ello, un programa de reconocimiento a tiempo real que reciba un *disguised* , y lo identifique como tal, advertirá al usuario y obligará a realizar una firma correcta.

Para llevar a cabo la fase de adquisición de la base de datos e-BioFirma se han desarrollado cinco aplicaciones, una para cada dispositivo utilizado, con el fin de seguir un protocolo de captura adecuado, constituyendo la parte principal del proyecto.

Estas aplicaciones han sido programadas en dos lenguajes de programación diferentes:

- **Java**: para los tres dispositivos WACOM (Figura 5.5 y Figura 5.6) y para el Samsung Galaxy Note 10.1.
- **C-Sharp**: para dispositivo Samsung ATIV 7 (aplicación desarrollada de forma paralela al resto de aplicaciones por Ram Phasad Krish, miembro del laboratorio ATVS).

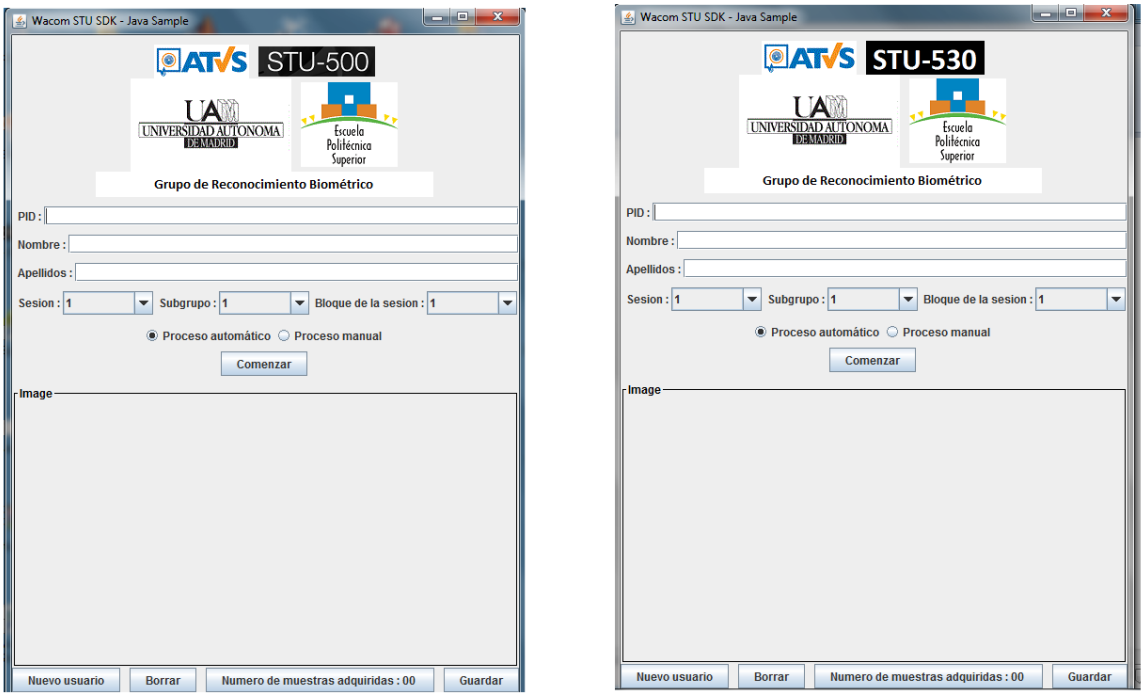

Figura 5.5: *Aplicaciones desarrolladas para los dispositivos WACOM STU-500 y WACOM STU-530.*

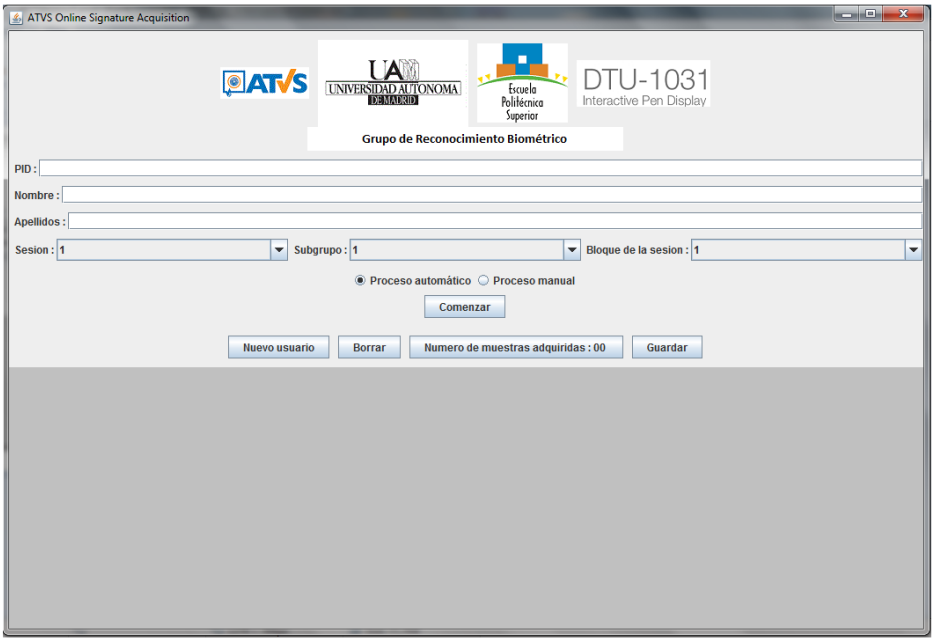

Figura 5.6: *Aplicación desarrollada para el dispositivo WACOM DTU-1031.*

Centrándonos en los dispositivos programados en Java, cabe destacar la programación del Samsung Galaxy Note 10.1, el cual posee un sistema operativo Android y por tanto ha sido programado en una clase especifica de Java conocida como Java Android.

A pesar de que cada dispositivo posee un software de desarrollo (SDK - *Software Development Kit*) propio, motivo por el cual ha sido necesario desarrollar cinco aplicaciones diferentes, el funcionamiento final de los dispositivos es igual, siguiendo exactamente el mismo protocolo de adquisición diseñado específicamente para esta base de datos, y haciendo de ella una base de datos coherente. La funcionalidad de todos los dispositivos se puede desglosar en:

- **Registro/Identificación de usuario**: Todas las aplicaciones constan de una primera fase de registro (en caso de que sea un usuario nuevo) o identificación (en caso de que el usuario ya haya participado en la captura previamente), en la cual se solicita un número de identificación de usuario único para cada individuo, nombre y primer apellido, grupo al que pertenece el usuario (1 = UAM, 2 = Empresa), número de sesión a realizar, bloque de la misma y si el usuario va a realizar firmas originales (perfil *Cliente*) o falsificaciones (perfil *Falsificador*).
- **Captura de muestras**: En función de los parámetros introducidos en la fase anterior, las aplicaciones están programadas automáticamente de forma que un usuario debe realizar todas las firmas correspondientes a la fase del proceso en la que se encuentra antes de poder continuar con la captura; como ejemplo, un usuario que se encuentre realizando el primer bloque de la primera sesión se le solicitará automáticamente que introduzca dos firmas y su nombre y primer apellido, en minúsculas, de manera consecutiva en los cinco dispositivos, antes de poder pasar a realizar el segundo bloque. Además, una vez realizado un bloque de la sesión en un determinado dispositivo, si se intenta volver a realizar, las aplicaciones están programadas para advertir al usuario de que ese proceso ya ha sido realizado.
- **Almacenamiento de las muestras recogidas**: Cada vez que se realiza una firma, se almacena en el directorio correspondiente con la nomenclatura especificada. En el caso de los tres dispositivos WACOM, las muestras recogidas se almacenan en el propio ordenador utilizado para la inicialización de las aplicaciones en el nivel superior (entendiendo como nivel inferior los procesos llevados a cabo por la propia tableta); con respecto a los dispositivos Samsung, las muestras se almacenan en los propios dispositivos, con una organización idéntica de directorios. Al final del día, todas las muestras se unifican en un mismo conjunto de directorios en el ordenador mencionado, y se realizan copias de seguridad de la base de datos en un dispositivo de almacenamiento externo, así como en un sitio de almacenamiento en red, con el fin de asegurar la captura pudiendo hacer frente a posibles perdidas de información recogida. La organización de los directorios, idéntica en todos los dispositivos, queda especificada en la Figura 5.7.

Puesto que las cinco aplicaciones tienen el mismo funcionamiento, por cuestiones de simplicidad, se ha decidido poner como ejemplo, en lo que se refiere a imágenes del proceso de adquisición, sólo una de ellas, la correspondiente al Samsung Galaxy Note 10.1, programada en Java Android, ya que se puede considerar la aplicación más completa incluyendo adquisición con *pen* y con dedo; sin olvidar que el resto de aplicaciones desarrolladas en el proyecto siguen protocolos similares.

Se va a tomar como ejemplo un usuario real existente en la base de datos, concretamente el usuario registrado con número identificativo *122* y nombre *Sandra Gaytán*. Los pasos en los que se divide la aplicación que lleva a cabo el proceso de adquisición de la primera sesión del usuario 122 (y de forma similar, la segunda sesión) son:

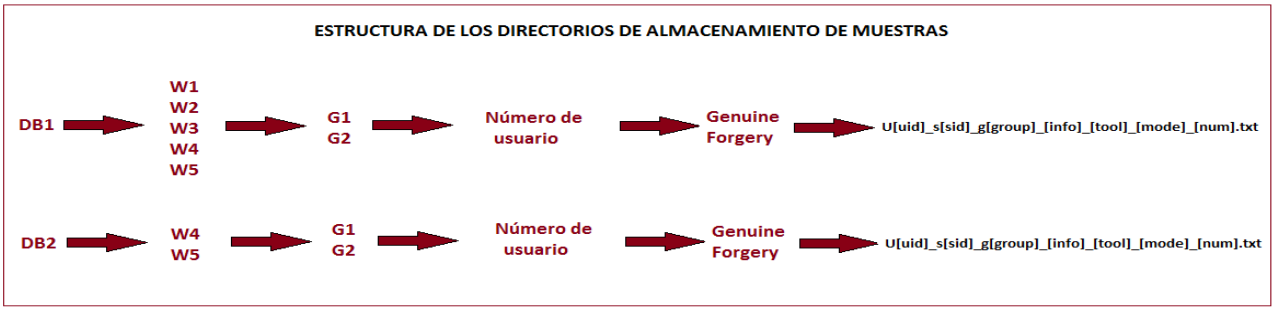

Figura 5.7: *Estructura de los directorios de almacenamiento de muestras. La nomenclatura de las carpetas es la que sigue: DB1 para las muestras realizadas con el pen (todos los dispositivos) y DB2 para las realizadas con el dedo (solo los dispositivos portátiles), W1/W2/W3/W4/W5 para referirse a los diferentes dispositivos, G1 para los usuarios del grupo de la UAM y G2 para la Empresa, y por último Genuine para las muestras falsificadas y Forgery para las falsificaciones realizadas por otros usuarios).*

- Primer paso: introducción de los datos (Figura 5.8). En el caso de que el numero de identificación se encuentre asignado a otro usuario, las aplicaciones te avisan e impiden crear otro usuario con dicho ID. (Figura 5.9).

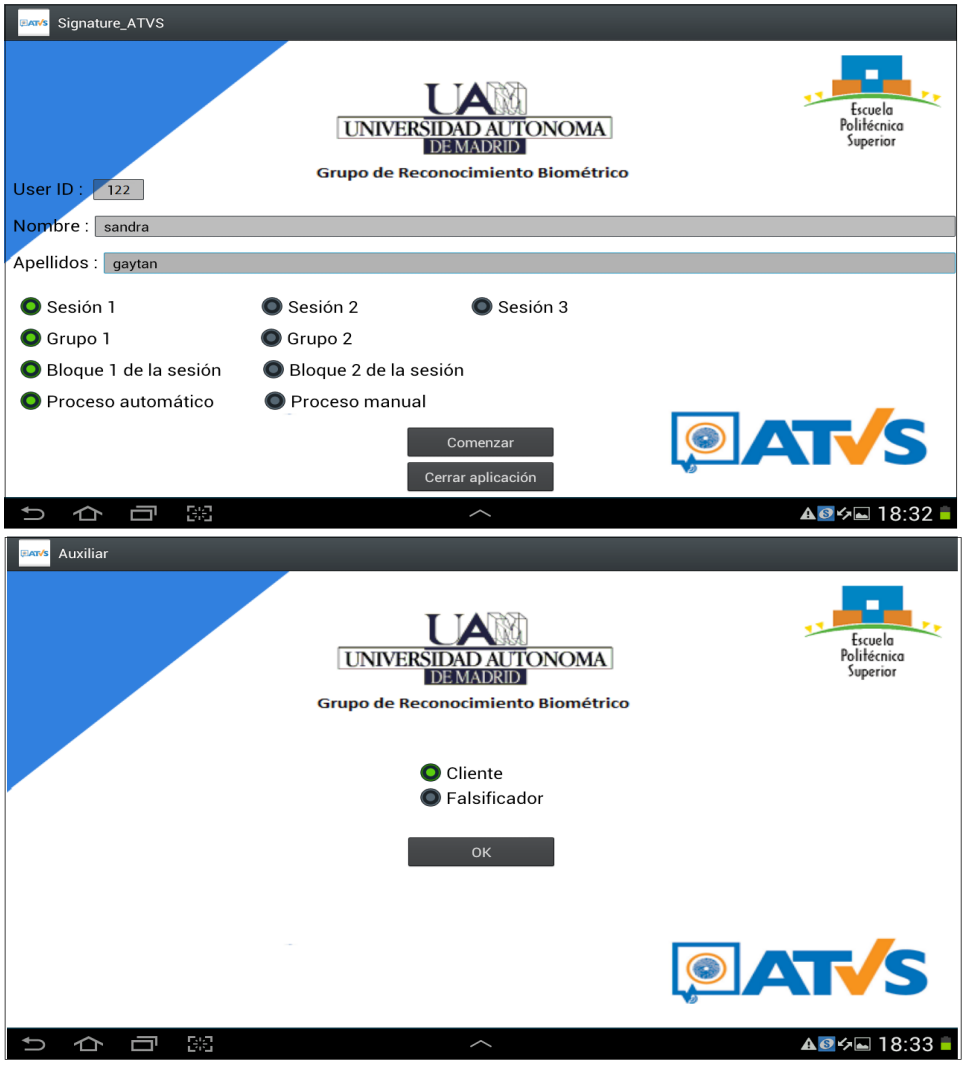

Figura 5.8: *Proceso de introducción de datos de usuario.En particular, observamos el proceso de registro del usuario 122, en el caso de que no exista ningún otro usuario registrado con ese ID.*

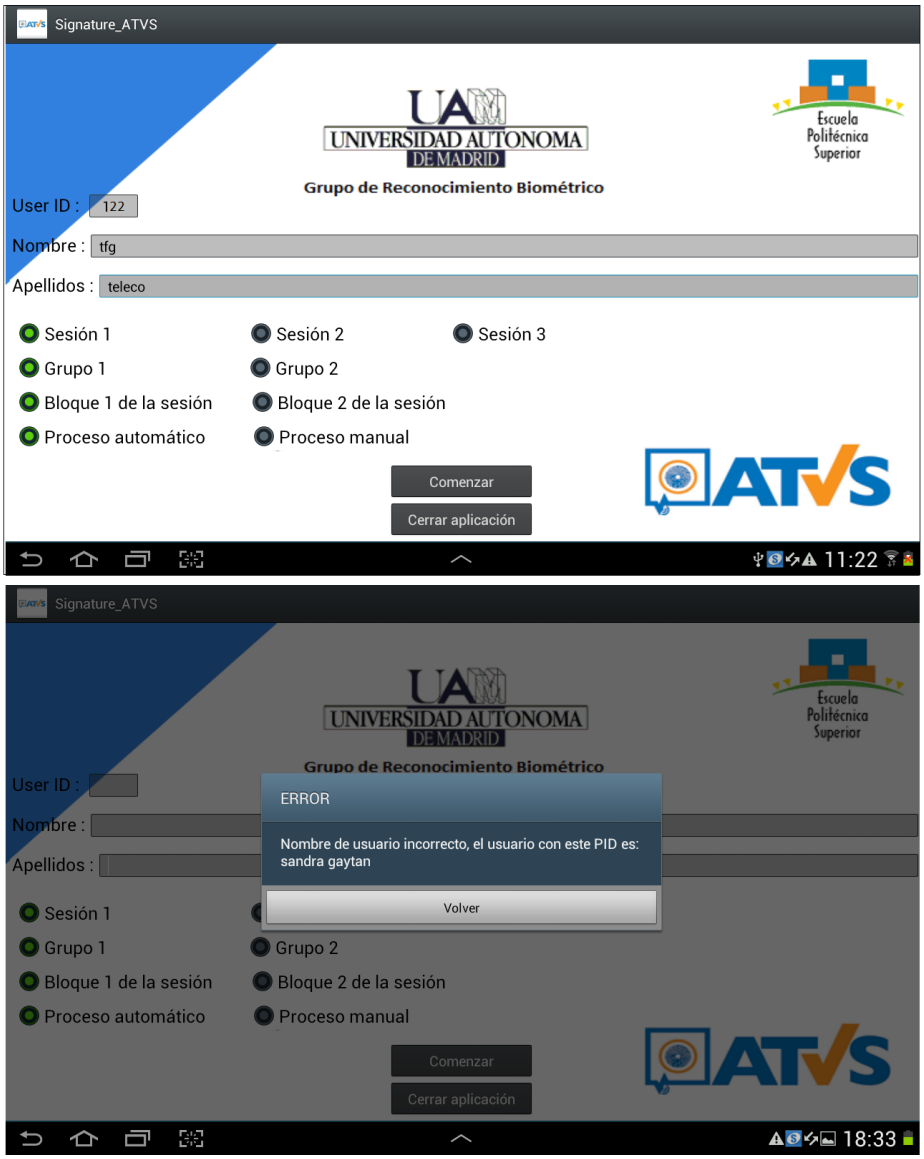

Figura 5.9: *Proceso de introducción de datos de usuario. Se observa el caso en el cual se intenta registrar un usuario diferente con el mismo ID anterior, surgiendo un error.*

- Segundo paso: Realización de las firmas y el nombre originales con el pen (Figura 5.10).

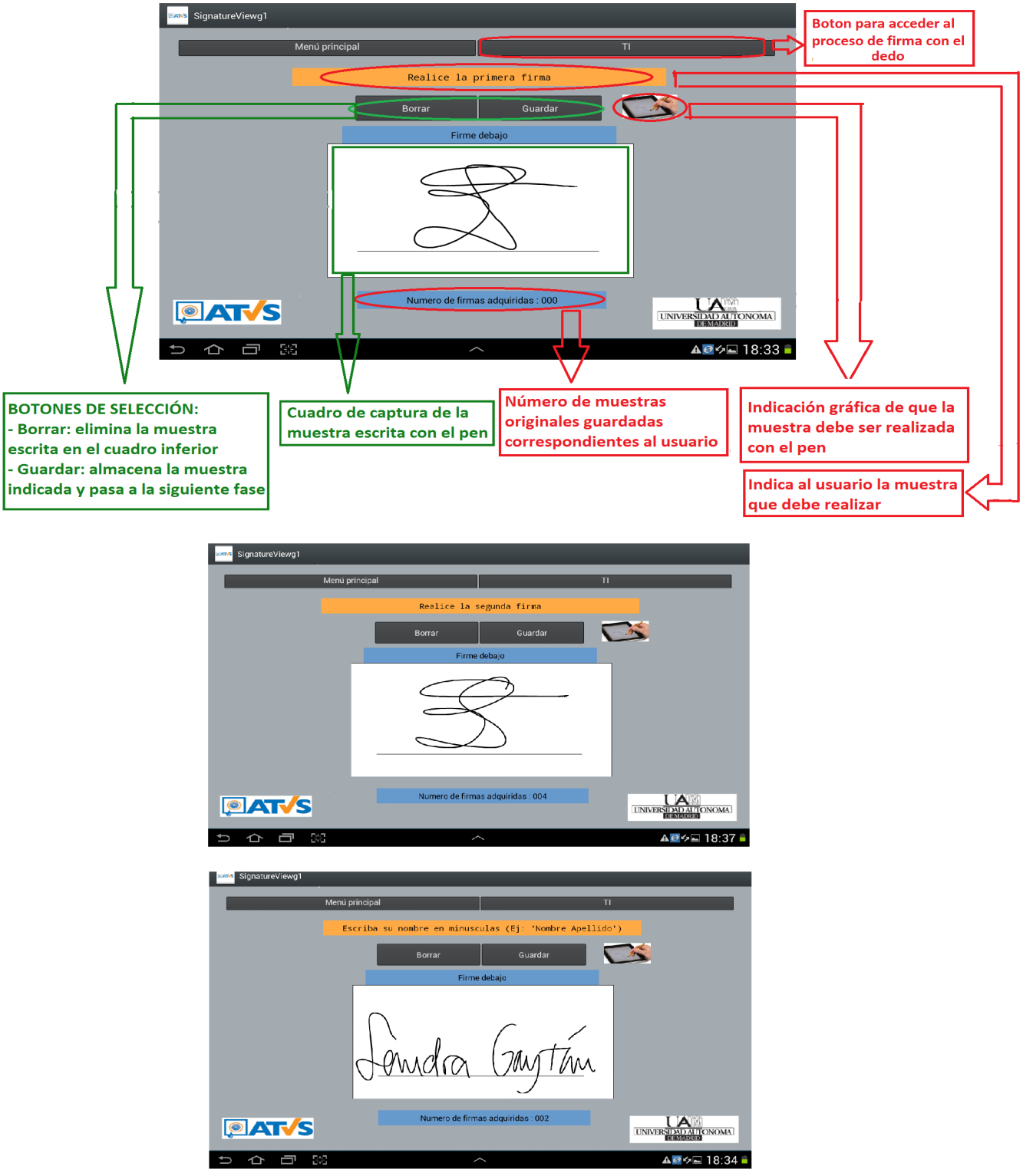

Figura 5.10: *Proceso de firma realizado con el pen durante el primer bloque de la primera sesión.*

- Tercer paso: Realización de las firmas y secuencias alfanuméricas con el dedo (Figura 5.11).

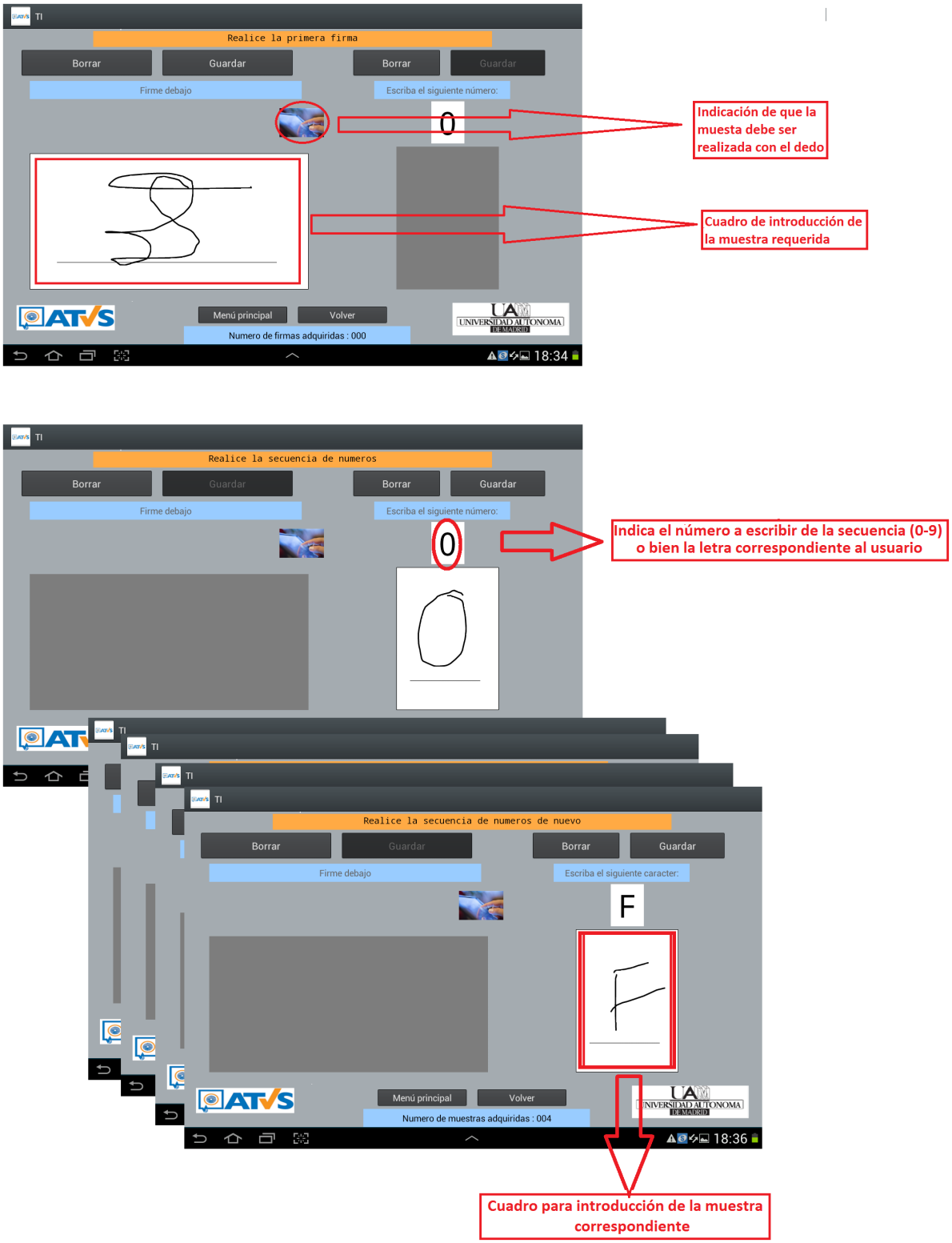

Figura 5.11: *Proceso de firma realizado con el dedo durante el primer bloque de la primera sesión.*

- Cuarto paso: Tras haber completado los tres pasos anteriores en los cinco dispositivos, se vuelven a realizar los pasos anteriores con la excepción de que en este caso el nombre debe ser escrito en mayúsculas. Si se intenta volver a realizar algún proceso ya efectuado, las aplicaciones avisan sobre ello, impidiendo repetirlo de manera automática (Figura 5.12).

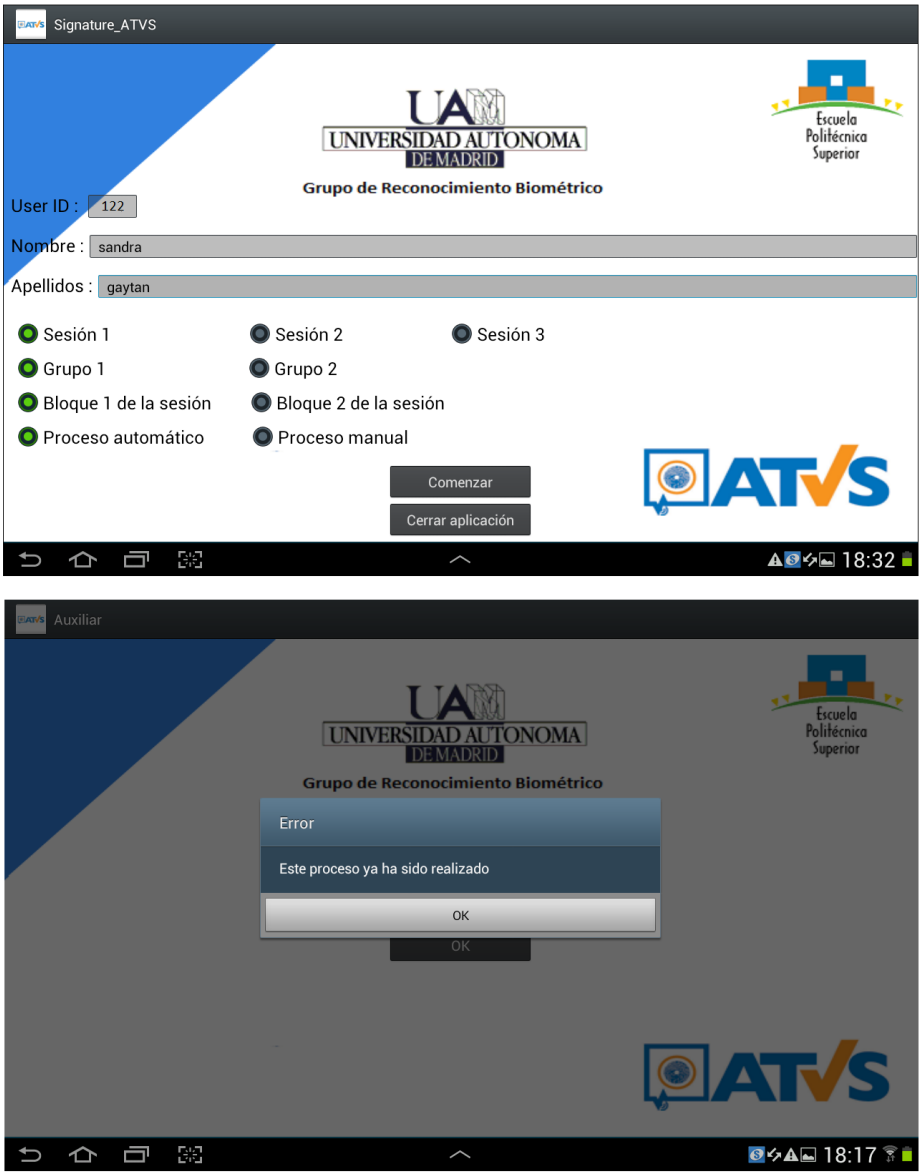

Figura 5.12: *Intento de repetición de un bloque ya realizado. En caso de haber ocurrido algún error durante la primera adquisición de dicho bloque, se podrá corregir mediante el proceso manual.*

- Quinto paso: Tras haber realizado el cuarto paso en todos los dispositivos, se pasa a realizar las falsificaciones correspondientes a los tres usuarios registrados anteriormente (Figura 5.13). Automáticamente las aplicaciones están programadas de forma que solicitan a un usuario que realice las firmas de los tres usuarios anteriores consecutivamente. Para mostrar las firmas originales, se ha desarrollado una aplicación que reproduce a tiempo real la dinámica de la firma original de dichos usuarios realizada en el dispositivo WACOM DTU-1031. Para las falsificaciones correspondientes a la firma con el dedo, en el propio dispositivo Samsung Galaxy Note 10.1 se ha desarrollado un apartado adicional, equivalente a la aplicación desarrollada para mostrar las firmas originales realizadas con el pen, que permite visualizar la dinámica real de las firmas de los tres usuarios anteriores (Figura 5.14).

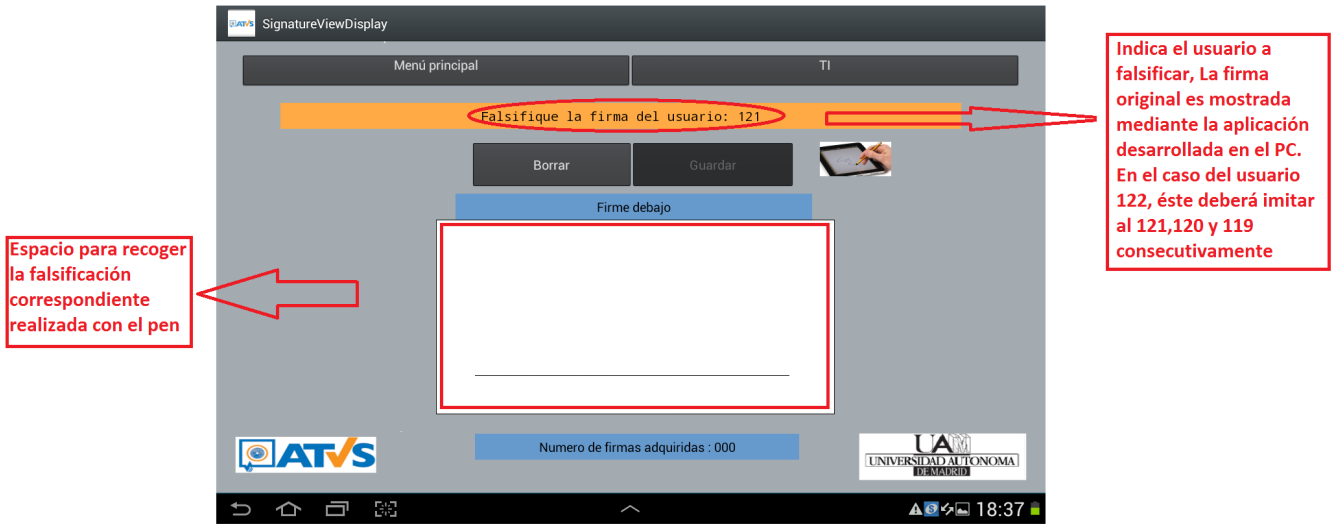

Figura 5.13: *Proceso de falsificación realizado con el pen durante el primer bloque de la primera sesión.*

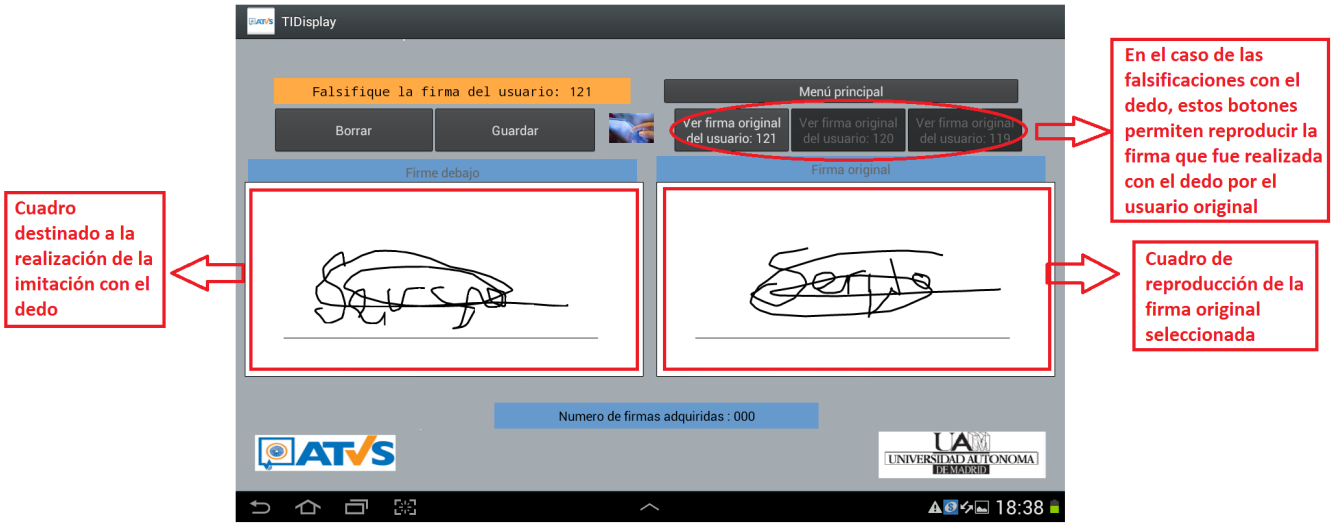

Figura 5.14: *Proceso de falsificación realizado con el dedo durante el primer bloque de la primera sesión.*

- Proceso manual: En el caso de que se haya producido algún error durante la captura automática de firmas, se ha programado un apartado manual de almacenamiento de muestras que permite elegir la muestra errónea a reemplazar. Este apartado, en función de los parámetros introducidos en la página de inicio, procederá a sustituir la muestra indicada (Figuras 5.15 y 5.16).

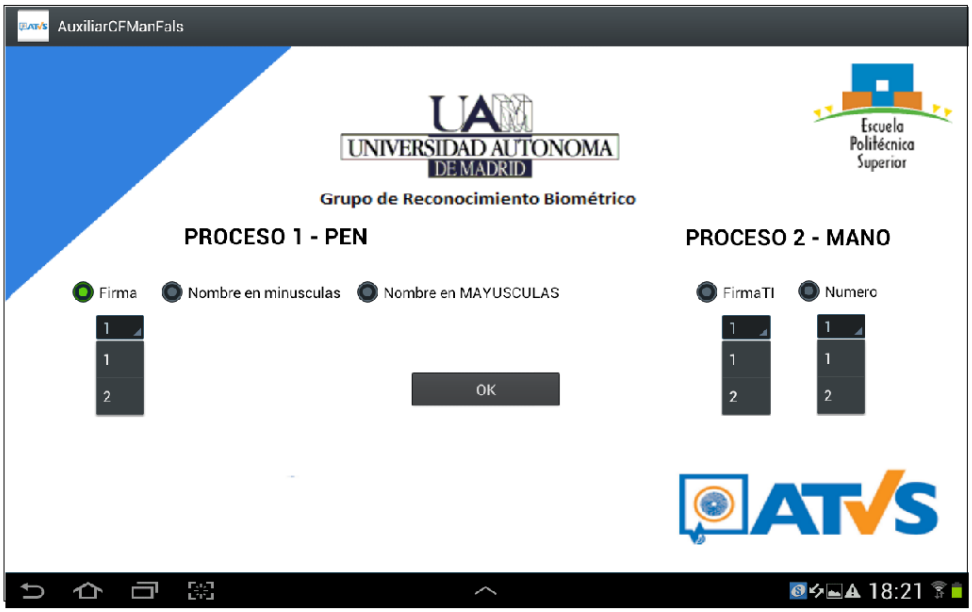

Figura 5.15: *Proceso manual de sustitución de muestra original.*

Figura 5.16: *Proceso manual de sustitución de falsificación.*

Por último, como resumen, se puede observar la tabla 5.1, en la cual queda especificado el número de muestras totales que quedarán almacenadas en la base de datos e-BioFirma para cada usuario registrado.

Para un usuario perteneciente al grupo de la UAM, el número total de muestras recogidas durante el proceso de adquisición son:

- Firmas genuinas: 5 dispositivos × 2 sesiones × 2 bloques por sesión × 4 firmas por bloque = 80 firmas.
- Nombres genuinos: 5 dispositivos × 2 sesiones × 2 bloques por sesión × 1 nombre por bloque = 20 nombres.
- Secuencias alfanuméricas: 5 dispositivos × 2 sesiones × 2 bloques por sesión × 2 secuencias por bloque = 40 secuencias.
- Firmas no genuinas: 5 dispositivos × 2 sesiones × 1 bloque por sesión × 6 firmas por bloque = 60 firmas falsificadas por 3 usuarios diferentes.
- Nombres no genuinos: 1 dispositivo (WACOM STU-530) × 2 sesiones × 1 bloque por sesión × 6 nombres falsificados por bloque = 12 nombres falsificados.

Esto resulta en un total de 120 muestras genuinas + 72 imitaciones = **212 muestras** por usuario perteneciente a la UAM.

Con respecto al grupo de la Empresa, siguiendo un razonamiento paralelo:

- Firmas genuinas: 5 dispositivos × 2 sesiones × 2 bloques por sesión × 2 firmas por bloque = 40 firmas.

Con esto, para el grupo de la empresa se tiene un total de **40 muestras** por usuario.

	UAM	EMPRESA
Dispositivos	5	5
Modalidad de firma	Pen + dedo	Pen
Sesiones por dispositivo	2	2
Bloques por sesión	2	2
Firmas genuinas por bloque	4 (2 con pen y 2 con dedo)	2
Nombres genuinos por bloque	1	-
Conjunto de números (DNI) por bloque	2	-
Firmas falsificadas por sesión	6 (3 usuarios / pen y dedo)	-
Nombres falsificados por sesión	6 (3 usuarios / minus y MAYUS, solo en STU-530)	-
TOTAL (por usuario)	212 muestras	40 muestras

Tabla 5.1: *Base de datos e-BioFirma. No se ha considerado la posible adición de disguises en la segunda sesión.*

5.4. Problemas encontrados durante la adquisición

Durante la adquisición llevada a cabo hasta el momento, se han encontrado una serie de problemas que podemos resumir en:

- Problema relacionado con la validez de muestras inexactas: Se han dado por validas aquellas muestras recogidas que no estén perfectamente alineadas con respecto a la linea de referencia marcada (ejemplo en la Figura 5.17), así como muestras de firmas originales con algunas variaciones entre sí, con el fin de adaptarse lo más posible a casos reales futuros.
- Problema relacionado con el tamaño: Se han dado por validas todas aquellas muestras, más grandes o más pequeñas, que se encuentren dentro del cuadrado delimitado en las pantallas de los dispositivos, obligando repetir aquellas muestras que sobrepasen los margenes delimitados.(Ejemplo en la Figura 5.17).
- Problema relacionado con las falsificaciones: Todas aquellas imitaciones realizadas con una dinámica no natural, es decir, a una velocidad no realista, así como aquellas que no guardasen un parecido con la firma original han sido descartadas y repetidas.

Para hacer frente a todos estos problemas se ha llevado a cabo un seguimiento humano exhaustivo del proceso de captura; con el fin de realizar este seguimiento de la forma más precisa y satisfactoria posible, solo se ha permitido realizar el proceso a un usuario a la vez, es decir, hasta que un usuario no completa una sesión en todos los dispositivos no se permite iniciar el proceso con otro usuario.

Figura 5.17: *Problemas de validez (izquierda, aceptada) y tamaño (derecha, descartada).*

6

Conclusiones y trabajo futuro

Este trabajo tenía como objetivo el diseño y captura de una base de datos multi-dispositivo. Ha sido motivado por el inminente desarrollo tecnológico que hace imprescindible contar con bases de datos que proporcionen la información necesaria con respecto a la variabilidad existente entre capturas realizadas con diferentes y variados dispositivos que capturen un mismo rasgo biométrico; la existencia de este tipo de base de datos permitirá desarrollar sistemas de reconocimiento biométrico viables independientemente del dispositivo utilizado.

Esto genera un gran avance en lo que se refiere al desarrollo de aplicaciones que incorporen identificación de usuario mediante reconocimiento biométrico, específicamente mediante firma, las cuales pueden ser utilizadas en múltiples dispositivos, tanto fijos como portátiles, sin ello afectar a su correcto funcionamiento.

Mediante el desarrollo de la base de datos e-BioFirma se ha intentado hacer frente a todas las posibles variabilidades y dificultadas que puedan surgir en lo que a un proceso de reconocimiento biometrico real se refiere. Por este motivo se ha introducido robustez multi-dispositivo, multimodal (captura de firma, escritura y secuencia alfanumérica), temporal y ante falsificaciones.

Como trabajo futuro se proponen los siguientes objetivos:

- Incorporar los ya explicados *disguised* en la segunda sesión de captura.
- Considerar la posible realización de una tercera sesión de adquisición en la que solo se capturarían muestras realizadas con el dedo, puesto que son las más variables y novedosas en lo que se refiere a procesos de adquisición de base de datos y sería interesante contar con más muestras de este tipo para poder desarrollar sistemas de reconocimiento óptimos y competentes.
- Una vez finalizada la adquisición de la base de datos, probar los sistemas de reconocimiento ya existentes para medir la eficiencia de los mismos con las variabilidades introducidas.
- A través de los resultados observados al aplicar técnicas de reconocimiento ya existentes, desarrollar nuevos sistemas que tengan en cuenta todas las novedades introducidas, como son los *hovering points*, falsificaciones realizadas con calco, muestras recogidas con diferentes dispositivos, firmas realizadas tanto con pen como con dedo, etc.

- Por último, en lo que se refiere a las aplicaciones desarrolladas, sería interesante acelerar el proceso de captura en la tableta Samsung ATIV 7, en la cual actualmente se quieren entre 2-5 segundos en guardar cada firma realizada. Además, se podría mejorar la representación gráfica de la firma con el dedo, puesto que a pesar de que esta tableta captura las muestras a una frecuencia igual que el resto de dispositivos (200Hz), la frecuencia representación gráfica de la firma con el dedo en el momento en el que se está realizando es menor que la frecuencia de muestreo real, provocando una visualización poligonal de la misma.

Bibliografía

[1] J. Fierrez and J. Ortega-Garcia. Handbook of Biometrics, chapter *On-line signature verification*. Eds. A. K. Jain and A. Ross and P. Flynn, Springer, 2007.

[2] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez. "*The multi-scenario multi-environment BioSecure multimodaldatabase (BMDB)*", IEEE Trans. on Pattern Analysis and Machine Intelligence, 2010.

[3] J. Ortega-Garcia, J. Fierrez, F. Simon, D.Gonzalez, J.Faundez-Zanuy, M.Espinosa, V.Satue, A.Hernaez, I.Igarza,J-J.Vivaracho, C.Escudero, D. and Moro. "*MCYT Baseline Corpus: A multimodal Biometric Database*", IEEE Proceedings Vision, Image and Signal processing, Vol.150, pages 395-401, 2003.

[4] B. Dumas, J.Hennebert, A. Humm, R.Ingold, D.Petrovska, C. Pugin and D. Rot., "*MyIdea Sensors Specification and Acquisition Protoco*l", Computer Science Department Research, University of Fribourg in Switzerland, 2005.

[5] J. Fierrez, J. Ortega-Garcia, D. Torre-Toledano, and J. Gonzalez-Rodriguez. "*BioSec Baseline Corpus: A Multimodal Biometric Database*", Pattern Recognition, vol. 40, no. 4, pages 1389-1392, 2007.

[6] J. Fierrez, J. Galbally, J. Ortega-Garcia, M. Freire, F. Alonso-Fernandez, D. Ramos, D. Toledano, J. Gonzalez-Rodriguez, J. Siguenza, J. Garrido Salas, E. Anguiano-Rey, G. Gonzalez-de Rivera, R. Ribalda, M. Faundez-Zanuy, J. Ortega, V. Cardenoso-Payo, A. Viloria, C. Vivaracho, Q. Moro, J. Igarza, J. Sanchez, I. Hernaez, C. Orrite-Urunuela, F. Martinez-Contreras, and J. Gracia-Roche. "*BiosecurID: A Multimodal Biometric Database*", Pattern Analysis and Applications, 2009.

[7] M. Faundez-Zanuy, J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez, "*Multimodal Biometric Databases: An Overview*", 2005.

[8] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia, and D. Maltoni. *An online signature verification system based on fusion of local and global information*, IAPR Intl. Conf. on Audio- and Video-Based Biometric Person Authentication, AVBPA, pages 523-53,. Springer LNCS-3546, 2005.

[9] J. Ortega-Garcia J. Fierrez-Aguilar, D. Ramos-Castro and Joaquin Gonzalez-Rodriguez. *HMM-based on-line signature verfication: feature extraction and signature modeling*. Pattern Recognition Letters, 2007.

[10] A. Ross, K. Nandakumar, and A. K. Jain.*Handbook of Multibiometrics*, Springer, 2006.

[11] A. K. Jain, K. Nandakumar, and A. Nagar. *Biometric template security*. EURASIP Journal onAdvances in Signal Processing, Article ID 579416, 2008.

[12] A. K. Jain, A. Ross, and S. Prabhakar. *An introduction to biometric recognition*. IEEE Trans. on Circuits and Systems for Video Technology, pages 4-20, 2004.

[13] A. K. Jain, K. Nandakumar and A. Ross. *Score normalization in multimodal biometric systems*. Patern Recognition, 2002.

[14] M. Martínez. *Dynamic signature verification for portable devices*. MPhil Thesis, 2008.

[15] SDK for Wacom STU tablets: `http://gsdt.wacom.eu/download/Wacom-STU-SDK.xml`.

[16] SDK for Wacom DTU-10311 tablet (JPen - Java Pen Tablet Access Library) : `http://sourceforge.net/projects/jpen/`.