Universidad Autónoma de Madrid
Escuela politécnica superior

Proyecto fin de carrera

RECONOCIMIENTO DE PASSWORDS GRÁFICOS EN DISPOSITIVOS MÓVILES

Ingeniería de Telecomunicación

Cristina Martín Díaz
Febrero 2010

RECONOCIMIENTO DE PASSWORDS GRÁFICOS EN DISPOSITIVOS MÓVILES

AUTORA: Cristina Martín Díaz
TUTOR: Marcos Martínez Díaz

Biometric Recognition Group - ATVS
Dpto. de Ingeniería Informática
Escuela Politécnica Superior
Universidad Autónoma de Madrid
Febrero 2010

Resumen

Resumen

Este proyecto de investigación estudia la verificación automática de usuarios a través de passwords gráficos (medias firmas y *doodles*) trazados sobre pantallas táctiles de dispositivos móviles. Para ello se desarrolla un sistema de verificación basado en el estado del arte en reconocimiento de firma manuscrita. Se ha tomado como punto de partida trabajos previos en firma manuscrita on-line, desarrollando y adaptando sistemas basados en parámetros globales y locales.

Este nuevo sistema de verificación ha sido evaluado sobre una base de datos capturada durante el desarrollo del proyecto ya que no se tiene constancia de la existencia de una base de datos pública de estas características. Se ha contado con la participación de 100 usuarios constituyendo un total de 5000 muestras por cada tipo de identificador; uno se caracteriza por una serie de trazos que componen un dibujo o boceto constituyendo lo que se llama *doodle*; el otro consta de una versión simplificada de la firma.

El sistema de verificación se basa en la información global y local de las muestras y se han estudiado distintos conjuntos de características para evaluar el rendimiento en cada caso. Como conjunto de parámetros globales se han desarrollado tres sets de características del estado del arte para reconocimiento de gestos sobre pantalla táctil y firmas on line. La similitud de las características se ha calculado mediante distancia Euclídea y de Mahalanobis. Para estudiar el sistema de parámetros locales se han realizado las pruebas con dos conjuntos de funciones y se ha utilizado el algoritmo DTW (Dynamic Time Warping) básico y una ampliación de éste. La ampliación del DTW clásico se basa en la alineación de las muestras y un método que fusiona trazos si la alineación se produce entre puntos que no pertenecen al mismo trazo. El DTW es una técnica que se utiliza generalmente como método de alineación de vectores que tienen diferente longitud.

Por último, se han llevado a cabo diferentes experimentos con el objetivo de evaluar el sistema de verificación de usuarios propuesto considerando los enfoques de parámetros globales y locales. También se ha considerado la fusión de los dos sistemas implementados con la configuración que ofrece mejor rendimiento. Por último, se documentan los rendimientos y limitaciones de cada método y se señalan posibles futuras direcciones en este área.

Palabras Clave

Biometría, doodle, DTW (*Dynamic Time Warping*), firma manuscrita, media firma, password gráficos, reconocimiento biométrico, sistema de verificación.

Abstract

This project studies the usage of finger-drawn graphical passwords ("passdoodles") as a user-verification method. Several verification systems, based on the state-of-the-art of on-line signature verification, have been developed in order to study and compare their performance. The systems use both global and local features, which are extracted from previous works in signature verification and gesture recognition.

A new graphical password database has been acquired during the development of the project. This is the first database of such characteristics to the extent of our knowledge. The database comprises 100 subjects totalling 5000 samples of two passwords each one; the first group of samples consist on a sketch-based password and the second is a simplified version of the signature.

The verification methods that have been analyzed, exploit both local and global information from the samples. The global information is extracted by three different feature-based representations used in previous works in signature verification and gesture recongition. The Mahalanobis and Euclidean distance is used to compare graphical passwords for the global feature sets. Two sets of functions have been developed for the local study. To calculate the distance between samples the Dynamic Time Warping (DTW) algorithm and one extension of it have been used. The DTW is an algorithm which is widely used for the alignment of time sequences of different lengths. The DTW extension consists on a stroke-based approach, which penalizes the distance between time functions when samples from non-corresponding strokes are selected as corresponding.

Experiments have been carried out to determine the robustness of the proposed user verification. In the experiments, the performance of the developed global and local systems is studied, as well as some preprocessing and score normalization methods. Fusion of the global and local system with optimal feature vectors is also performed. The strengths and limitations of each method have been discussed and future research directions in this area have been pointed out.

Keywords

Biometrics, biometric recognition, doodle, DTW, graphical passwords, handwritten signature, passdoodle, pseudo-signature, touchscreen, verification system.

Agradecimientos

Quiero agradecer en primer lugar a mi ponente, Javier Ortega, la oportunidad que me ha brindado de colaborar en el ATVS.

Mi más sincero agradecimiento a Marcos, por haberme dirigido en esta última etapa de mi carrera universitaria como tutor de este proyecto. Gracias por la confianza depositada en mí para la realización del presente proyecto, por todo el tiempo que me has dedicado y por todo lo que he aprendido en los últimos meses gracias a tu ayuda.

A mis amigos de la universidad por hacerme el día a día más agradable y sacar siempre la parte positiva de todas las situaciones. En especial, no puedo dejar de mencionar a Leti, porque para mi las palabras carrera, asignaturas y universidad adquieren una idea mental en la que no falta. Gracias Leti por tu cariño, apoyo y paciencia.

Además gracias a todos los compañeros, amigos, amigos de amigos y conocidos que habéis participado en la captura de la base de datos con alegría y paciencia, a todos vosotros os pertenece un cachito de este trabajo.

Y sin duda alguna este proyecto va dedicado a mis padres, Lourdes y Jesús quienes sin escatimar esfuerzo alguno han sacrificado gran parte de su vida para formarme y educarme. Muchísimas gracias por haberme brindado un hogar cálido y enseñarme que la perseverancia y el esfuerzo son el camino para lograr objetivos. A mis hermanos, Irene, Jesús y Lara por su paciencia y comprensión.

A mi abuela, quien me ha sucedido el tesoro más valioso que puede dársele a un nieto: amor.

A Gábor por su amor y su ayuda incondicional.

Por esto y más. Gracias.

Índice general

Índice de figuras

Índice de tablas

1 Introducción

1.1. Motivación del proyecto

El crecimiento que la sociedad de la información ha experimentado en los últimos años, así como el avance de la tecnología, han contribuido a que tareas que antes eran realizadas por las personas, ahora se realicen de manera automática. Dentro del amplio abanico de posibilidades que brinda el desarrollo e innovación tecnológica, se observa que los sistemas de autenticación de personas son un área emergente. Las técnicas de verificación y reconocimiento de personas han experimentado un gran avance debido a la proliferación de aplicaciones y servicios que requieren autenticación. Además las actuales posibilidades de conexión y las facilidades de portabilidad de dispositivos de todo tipo hacen que el acceso a cualquier servicio con su correspondiente identificación se puedan realizar en cualquier parte (ubicuidad).

Actualmente las técnicas biométricas han cobrado gran relevancia en sistemas y servicios que requieren métodos fiables de reconocimiento personal. Su propósito es asegurar que los servicios prestados son sólo accesibles por personas legítimas. Por ello, su principal característica es la autenticación de la identidad a través de un rasgo personal. Los rasgos biométricos no pueden, en general, ser prestados, robados o copiados mientras que si puede ocurrir en otros métodos de identificación basados en llaves o claves identificadoras. Los sistemas biométricos usan características o comportamientos fisiológicos propios de cada individuo para identificarlo [9].

Los rasgos biométricos se dividen en dos grandes grupos, rasgos biométricos fisiológicos y rasgos biométricos de comportamiento o conducta. Entre los rasgos biométricos fisiológicos se encuentran el iris, la huella dactilar, la geometría de la mano y la retina. Estos representan una manifestación tangible de lo que uno es, se caracterizan por una menor variabilidad a lo largo del tiempo pero su adquisición es más invasiva y requiere una alta cooperación. En cuanto a los rasgos biométricos de comportamiento o conducta, entre los que están la voz, la firma o escritura, son menos invasivos pero hay una alta variabilidad inherente al proceso de realización de los mismos.

A pesar de sus ventajas la biometría tiene limitaciones tales como su aceptación y necesidad de cooperación por parte de los usuarios, la complejidad en el método de captura así como la necesidad de dispositivos específicos y el hecho de que algunos rasgos no pueden ser revocados. Por ejemplo, para realizar operaciones que requieren seguridad a través de dispositivos móviles sólo sería posible la identificación por cara o a través de la pantalla táctil. Por otra parte, existe un incipiente interés en una técnica denominada *passdoodle*, que posee características de identificación pertenecientes tanto al ámbito de las contraseñas como al entorno biométrico [10]. Un *passdoodle* consiste en un boceto como contraseña realizado con el dedo como instrumento de

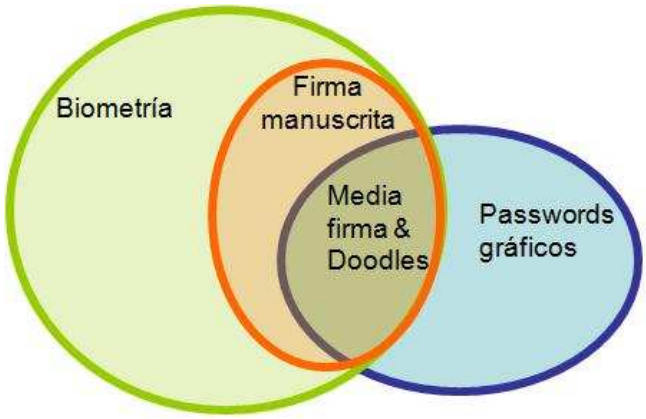


Figura 1.1: Diagrama de Venn que muestra la posible ubicación de los passwords gráficos bajo estudio (media firma y *doodles*) en relación a los sistemas de identificación personal.

escritura. Posee una parte privada, secreta que sólo el usuario sabe, igual que para las contraseñas y se pueden obtener características intrínsecas de las realizaciones hechas por cada usuario, idea que pertenece a la percepción que se tiene de la biometría. Identificarse utilizando un password gráfico es una buena alternativa a los métodos actuales ya que posee las ventajas de la biometría en cierta medida y no requiere de hardware extra. Algunos posibles inconvenientes serían la alta variabilidad y la tendencia a una excesiva simplicidad en la realización.

Varias de las propiedades ideales de los rasgos biométricos son la universalidad ya que toda persona debe poseer dicho rasgo así como su unicidad que hace que personas distintas posean rasgos diferenciados y distintos. También debe caracterizarse por ser invariante en el tiempo a corto plazo (permanencia) y a largo plazo (perennidad). Para facilitar la tarea de reconocimiento deber ser caracterizado cuantitativamente (mensurabilidad) de la forma menos molesta e invasiva posible para el usuario. En el caso de los *passdoodles* estas características se cumplen en cierta medida, al ser comparable con la realización de una firma manuscrita. La firma ha suscitado un alto interés en la comunidad científica debido a su aceptación tanto social y legal como método de autenticación y actualmente se está acrecentando un interés en esta variante llamada *passdoodle* derivada del concepto de password gráfico [1].

Los factores humanos son usualmente el eslabón débil de un sistema de seguridad. Cualquiera que trabaje con ordenadores o Internet estará de acuerdo en que la identificación y por tanto el uso de contraseñas o passwords juegan un papel importante a la hora de mantener nuestra información a salvo, sin embargo, nuestros datos están tan a salvo como inquebrantable es la contraseña que se elige. El método de autenticación más común es la presentación del nombre del usuario y una contraseña [11]. El mayor problema de este método, consiste en que la dificultad para recordar ciertas contraseñas hace que los usuarios elijan una fácil y de un pequeño subgrupo de todos los posibles [12]. Desafortunadamente estas claves o contraseñas son a la vez fáciles de adivinar o "craquear". Para tratar este tipo de problemas se propone por tanto un nuevo esquema de verificación basado en passwords gráficos realizados con el dedo (media firmar y *doodle*) como método de identificación personal.

1.2. Objetivos y enfoque

Este proyecto se centra en el estudio y desarrollo de un nuevo sistema de autenticación basado en trazos sobre un dispositivo móvil táctil realizados con el dedo, denominados *passdoodles*. Se implementa un sistema completo de verificación de usuario y se documentan los resultados obtenidos. El proyecto se desarrolla apoyándose en el estado del arte actual en reconocimiento

de passwords gráficos y en sistemas de verificación de firma on line.

En este trabajo confluyen dos líneas de identificación personal: el ámbito de las contraseñas y el ámbito de la biometría. En la figura 1.1 se muestra gráficamente las líneas que convergen en el estudio que se ha desarrollado. Por lo tanto, para el reconocimiento mediante passwords gráficos (*passdoodles*) se incorporan elementos que sólo el usuario conoce y tiene que recordar (idea de contraseña) además de características que se obtienen de la realización (idea de rasgo biométrico de conducta).

Este proyecto estudia la viabilidad del proceso de identificación utilizando dos conjuntos de passwords gráficos, uno denominado *"doodle"* y otro que consiste en una versión simplificada de la firma y se denomina "media firma", proponiéndose su uso como pseudo rasgo biométrico. Los métodos hasta ahora consolidados para reconocimiento en firma on line, han sido estudiados con el objetivo de emplearlos como punto de partida en el reconocimiento de *passdoodles*. Se busca confirmar si un *passdoodle* se puede tratar como posible rasgo biométrico de conducta y principalmente como medio de verificación.

En el capítulo 2, se detalla el estado del arte de los sistemas de reconocimiento biométrico. Se presentan los rasgos biométricos más comunes en la actualidad, se clasifican y se comparan atendiendo a las diferentes características que poseen.

El estado del arte en reconocimiento basado en passwords gráficos se presenta en el capítulo 3. Estos estudios son precursores del tema central del proyecto y se expone la evolución hasta el objeto de nuestro estudio. También se desarrollan en el capítulo 4 las técnicas de reconocimiento de firma on-line debido a que se reproducen estas técnicas para *passdoodles*. Se parte de la conjetura de que los *passdoodles* pueden tratarse como un rasgo biométrico de conducta.

Ha sido necesaria la captura de una base de datos para evaluar el sistema de verificación de usuario basado en *doodles* y medias firmas, ya que no se conoce ninguna base de datos pública de estas características hasta el momento. El proceso de captura y las características de la base de datos se exponen en el capítulo 5.

Las diferentes tecnologías implementadas en el estudio del sistema de verificación definido, se desarrollan y justifican en el capítulo 6. El desarrollo del sistema de verificación de usuario se ha enfocado desde varias perspectivas diferentes, globales y locales, que se explican en esta sección. A continuación se describen en el capítulo 7 los experimentos realizados durante el estudio del sistema de verificación. Los datos obtenidos en términos de rendimiento se presentan para todos los escenarios propuestos. Por último, en el capítulo 8 se presentan las conclusiones extraídas de los diferentes experimentos y se proponen posibles líneas de trabajo futuro.

2

Reconocimiento biométrico

La biometría permite la identificación de los seres humanos a través de las características físicas o comportamientos de éstos. Este método, reconoce a la persona teniendo en cuenta "quien" es ésta y no otros parámetros como "lo que la persona lleva" o "lo que la persona conoce". Los métodos clásicos de identificación dan relevancia a este tipo de información que es de alto riesgo ya que los objetos que una persona puede llevar, como llaves y tarjetas de identificación, pueden ser fácilmente perdidas, sustraídas y/o duplicadas; los datos que una persona conoce, tales como passwords y códigos, pueden ser olvidados o copiados. Por lo tanto, la diferencia entre los métodos clásicos y los biométricos radica en que la propia persona es la "llave/clave". La biometría aprovecha que existen ciertas características biológicas o conductuales singulares e inalterables, por lo que pueden ser analizadas y medidas para crear un identificador biométrico. Estas características son difíciles de perder, transferir u olvidar y, en general, son perdurables en el tiempo.

La biometría se establece como una de las alternativas más sólidas en el futuro de los sistemas de seguridad, muy demandados en los últimos años por la imperante y cada vez mayor necesidad de identificación fiable y protegida. Su potencial la hace especialmente interesante en determinadas áreas. Las aplicaciones de los sistemas biométricos pueden clasificarse en tres grandes grupos [13]:

- **Aplicaciones comerciales** como protección de una red o de datos electrónicos, compras a través de internet o acceso al mismo, cajeros automáticos, control de acceso físico, enseñanza a distancia, etc.
- **Aplicaciones gubernamentales** tales como el documento nacional de identidad, la licencia de conducir, la tarjeta de la seguridad social, el pasaporte, etc.
- **Aplicaciones forenses** entre las que encontramos investigaciones criminales, identificación terrorista, determinación de parentesco, etc.

Durante años, las aplicaciones comerciales han empleado generalmente sistemas basados en un PIN o contraseñas. Las aplicaciones gubernamentales se apoyaban básicamente en el documento de identidad y las aplicaciones forenses han contado con expertos en el cuerpo humano que identificaban datos biométricos. De un tiempo a esta parte, se ha incrementado el número de aplicaciones que se basan en rasgos biométricos, un ejemplo de ello se encuentra en el aeropuerto de Amsterdam donde emplean escáner de iris para acelerar los controles via pasaporte [13].

A pesar de todo, son los factores humanos los que en gran medida determinan el éxito de un sistema de reconocimiento basado en un rasgo biométrico. La facilidad y comodidad a la hora de

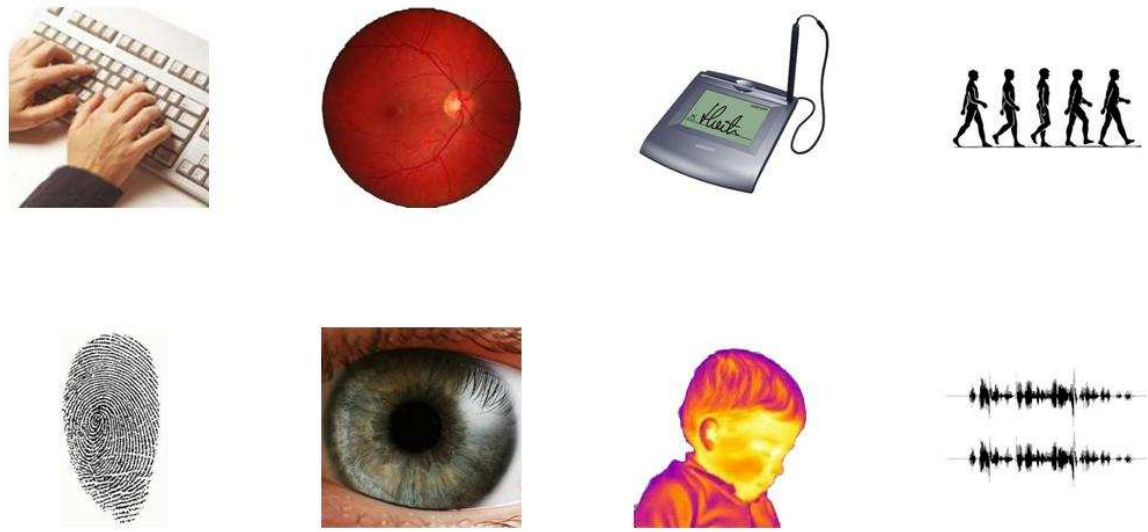


Figura 2.1: Ejemplo de varias modalidades biométricas.

interactuar con los sistemas de captación del rasgo, contribuyen notablemente a su aceptación. Son generalmente más aceptados aquellos sistemas que no necesitan del contacto directo con el individuo a la hora de medir una característica, así como aquellos sistemas que requieren poca cooperación o participación de los usuarios. Además, aquellos rasgos biométricos capturados sin el conocimiento del usuario pueden ser considerados como una amenaza a la privacidad.

En lo que se refiere a la privacidad adquieren una importancia especial los sistemas de reconocimiento biométrico porque estos pueden proporcionar información personal de un individuo. Por ejemplo, muestras de retina pueden dar información sobre diabetes o alta presión arterial de un individuo, y un seguro médico puede utilizar esta información con finalidades económicas.

No obstante y paradójicamente, la biometría se utiliza como uno de los métodos más efectivos a la hora de proteger la privacidad individual, asegurando su integridad. Por ejemplo, si una persona perdiera su tarjeta de crédito y otra persona la encontrara la facilidad de hacer un uso fraudulento de ella es mayor que si esa tarjeta necesitara de unos rasgos biométricos para ser utilizada.

2.1. Modalidades biométricas

Actualmente existen diversos rasgos biométricos que son utilizados en diferentes aplicaciones. No todos poseen los mismos atributos, por ello la selección de un rasgo biométrico puntual dependerá de las características del mismo, así como de las necesidades de la aplicación. A continuación se describen brevemente algunos de los más significativos (véase figura 2.1):

Dinámica del tecleo: cada persona tiene una forma de teclear que le caracteriza. Este rasgo se clasifica como conductual, por lo que podría variar a lo largo del tiempo y es poco distintivo, por lo tanto proporcionaría información básica en escenarios controlados para casos sencillos de aplicaciones on-line.

Escáner de retina: la estructura vascular de la retina es característica de cada individuo y cada ojo. Por su unicidad y su dificultad a la hora de duplicación está clasificado como el rasgo biométrico más seguro. La captura de este rasgo requiere una alta cooperación del usuario y alto contacto con el sensor, lo que compromete su aceptabilidad.

Firma: la manera en la que una persona firma la define. Aunque su captura requiere el contacto con el instrumento de escritura y un esfuerzo por parte del usuario, este viene siendo desde hace años el método de identificación más aceptado en transacciones comerciales y legales. No obstante, la firma es un rasgo biométrico de conducta que también puede cambiar a lo largo de los años y cuya adquisición puede verse influida por condiciones físicas o emocionales.

Forma de caminar: la forma de caminar de cada individuo es un rasgo biométrico complejo a nivel espacio-temporal. No es especialmente distintivo pero puede ser suficientemente discriminatorio en aplicaciones que requieran un bajo nivel de seguridad. Forma parte de los rasgos biométricos de comportamiento por lo que una de sus desventajas es su variabilidad a lo largo del tiempo, en cambio su adquisición no es nada invasiva.

Geometría de la mano y el dedo: aquí se presenta otro rasgo que tiene una distintividad baja. Este rasgo biométrico se basa en diferentes medidas de la mano como la forma, el tamaño de la palma, el grosor y longitud de los dedos, etc. Actualmente están en funcionamiento sistemas de verificación de usuarios basados en la geometría de la mano. El usuario debe situar la palma de la mano en un escáner u otro dispositivo para adquirir este rasgo biométrico.

Huella dactilar: de entre todas las técnicas biométricas, la identificación basada en huella dactilar es la más antigua como método de identificación así como la más fiable. La huella consiste en un conjunto de valles y crestas que se forman durante los primeros siete meses del desarrollo del feto [14]. Es única para cada individuo y cada dedo. Hoy en día se dispone de una amplia variedad de sistemas basados en huellas debido a la reducción del coste de los sensores. Así, podemos encontrar diversos dispositivos que añaden este sistema de identificación (teléfonos móviles, PDA's, ordenadores portátiles, etc.)

Iris: es altamente distintivo para cada uno de los ojos de un individuo. Su captura requiere una alta cooperación del usuario, el cual debe situarse a una distancia determinada del sensor. Es un rasgo difícil de falsificar aunque también es difícil detectar una muestra de iris falsa, por ejemplo la que puede imprimirse en una lente de contacto que posteriormente se pasaría por un sensor [15]. Aunque los primeros sistemas de reconocimiento de iris necesitaban una alta participación y eran caros, los nuevos sistemas están siendo más aceptados y más rentables económicamente.

Olor: se sabe que cada objeto desprende un olor que es característico de la composición química que lo forma. El olor que una persona emite es capturado por un haz de sensores químicos, cada uno sensible a una sustancia diferente que le identifica. Es posible que el olor del cuerpo no se mantuviera invariable con la utilización de desodorantes, perfumes y cremas que alterarían su composición química.

Oreja: se ha sugerido que la forma y estructura cartilaginosa de la oreja son distintivas de cada individuo. La adquisición de este rasgo geométrico se basa en una fotografía por lo que no se considera invasivo. Los sistemas que se han propuesto en la actualidad suelen emplear la distancia de los salientes del borde de la oreja con respecto a una referencia común del interior de la oreja.

Rostro: el rostro es una de los rasgos biométricos más aceptados ya que es el comúnmente empleado en el reconocimiento humano entre individuos y no es intrusivo. Uno de los inconvenientes que acompañan a este rasgo es la facilidad con que pueden quebrantarse los sistemas de vigilancia con máscaras. También existe el problema de la variabilidad temporal, por lo que los sistemas tendrían que adaptarse a los cambios del usuario con la edad, a las diferentes expresiones de la cara y a los diversos ángulos con respecto a la cámara.

Termogramas: el calor irradiado por el cuerpo humano es característico de cada individuo. Puede ser capturado mediante una cámara de infrarrojos de forma no intrusiva o incluso oculta. La mayor desventaja de esta clase de sistemas es el coste de los sensores, así como su vulnerabilidad ante otras fuentes de calor no controlables. Los termogramas pueden ser también empleados para capturar la estructura de las venas de la mano.

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

En general, las modalidades biométricas anteriormente presentadas deben poseer ciertas características en común. Así, cualquier rasgo o característica que una persona posea se puede utilizar como rasgo biométrico siempre que satisfaga los siguientes requisitos:

- *Universalidad*: toda persona debe poseer dicho rasgo biométrico.
- *Distintividad*: personas distintas deben poseer rasgos diferenciados/distintos.
- *Permanencia*: el rasgo debe ser invariable con el tiempo.

Sin embargo, en la práctica debe tenerse en cuenta también los siguientes factores:

- *Mensurabilidad*: el rasgo debe poder ser caracterizado cuantitativamente.
- *Rendimiento*: el proceso de identificación debe ser preciso.
- *Aceptabilidad*: grado de aceptación/rechazo personal y social del sistema biométrico.
- *Evitabilidad*: capacidad de eludir el sistema mediante procedimientos fraudulentos.

Atendiendo a estas características y a las necesidades del sistema, se elegirá un rasgo biométrico u otro. Esto se debe a que ningún rasgo biométrico es "óptimo" por sí solo.

2.2. Sistemas biométricos

Un sistema biométrico consiste en un reconocedor de patrones cuya operativa puede resumirse en los siguientes pasos: captura un rasgo biométrico, extracción de un conjunto de características y comparación con diferentes patrones almacenados en una base de datos para decidir sobre la identidad del individuo.

Dentro del ámbito de los sistemas de reconocimiento, éstos pueden tener dos finalidades: el reconocimiento positivo o el negativo. El reconocimiento positivo es aquél que busca comprobar que un usuario es realmente quien dice ser. En el caso de reconocimiento negativo, se trata de lograr determinar que un usuario no es quien afirma ser.

La figura 2.2 muestra los módulos y algoritmos principales que constituyen un sistema de reconocimiento biométrico. En general el usuario tiene acceso al sensor que recoge la muestra del rasgo biométrico a tratar. Los módulo opacos son las entidades (*hardware*) o (*software*) básicas del sistema, sobre las que se deberán realizar algunas etapas de procesado opcionales identificadas mediante los módulos transparentes.

Figura 2.2: Esquema de funcionamiento de un sistema de reconocimiento biométrico.

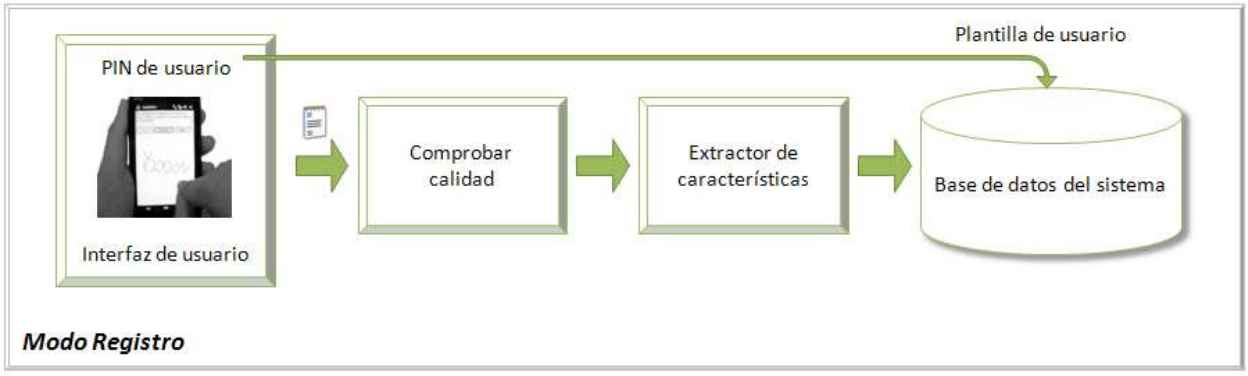


Figura 2.3: Esquema de funcionamiento en modo registro.

2.2.1. Modos de operación de un sistema biométrico

Desde el punto de vista del funcionamiento de los sistemas automáticos de reconocimiento de personas mediante rasgos biométricos, se distinguen tres modos de trabajo:

Modo registro: Modalidad en la que los usuarios se dan de alta en el sistema. En un primer paso, se introduce el rasgo con la tecnología necesaria para la captura en cada caso en el sistema y se da de alta en una base de datos, quedando almacenada así la plantilla de cada usuario. La base de datos puede almacenar otra información del usuario. Un ejemplo de ello puede verse en la figura 2.3.

Identificación: El objetivo de este modo de trabajo, es el de clasificar una realización determinada de un rasgo biométrico de identidad desconocida como perteneciente a uno de entre un conjunto de N posibles individuos; por lo tanto, es el sistema el que hace el trabajo de búsqueda entre todas las realizaciones de la base de datos. Se realiza una comparación de tipo $1 : N$ como se representa en la figura 2.4. Se puede realizar identificación en conjunto cerrado, cuyo resultado será la asignación de identidad a uno de los individuos modelados por el sistema, o identificación en conjunto abierto, en la que se debe considerar una posibilidad adicional que sería que el individuo a identificar no pertenezca al grupo de usuarios.

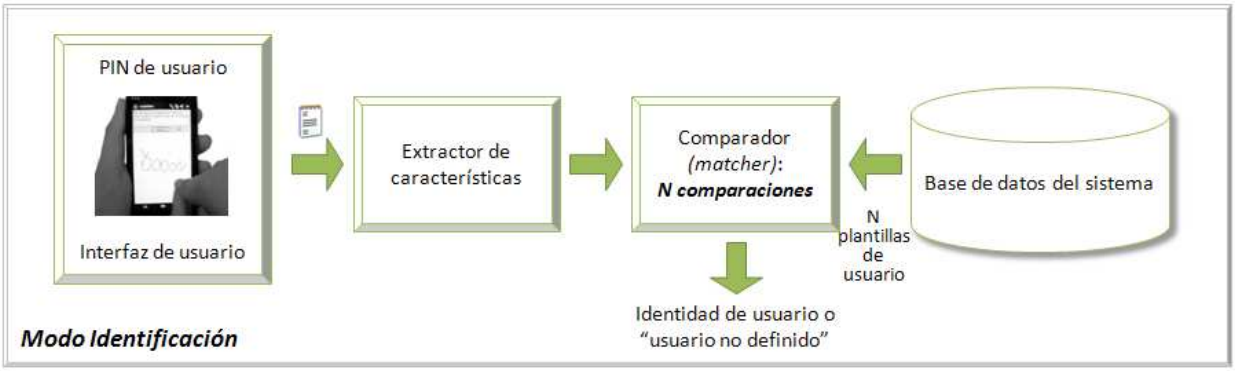


Figura 2.4: Esquema de funcionamiento en modo identificación.

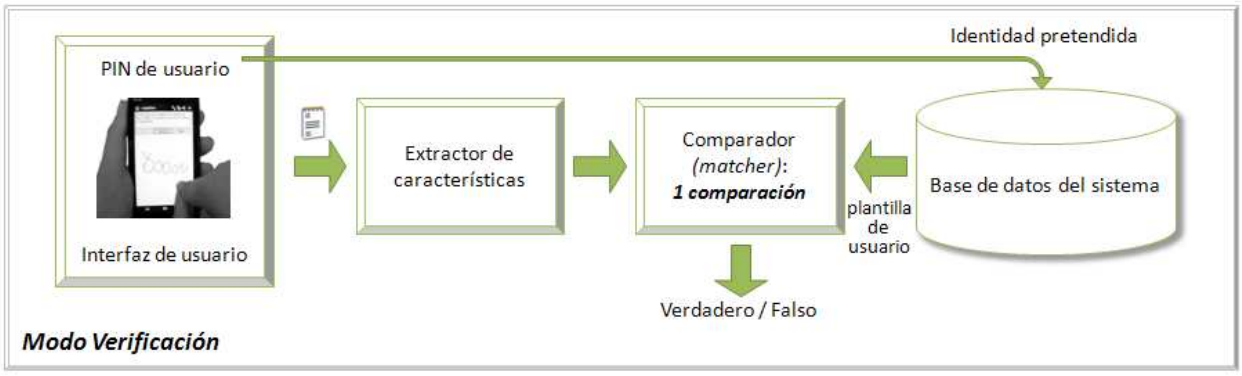


Figura 2.5: Esquema de funcionamiento en modo verificación.

Verificación: Los sistemas de verificación de individuos toman dos entradas (véase figura 2.5).

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

Las dos únicas salidas de este sistema son la aceptación o el rechazo del individuo como aquel que pretende ser. De esta forma el individuo solicitante de la identidad será clasificado como **usuario auténtico** o bien como **impostor**. La decisión de aceptar ó rechazar la muestra de entrada como correspondiente al individuo solicitado dependerá de si el valor de parecido o probabilidad obtenido supera o no un determinado umbral de decisión.

2.2.2. Rendimiento de los sistemas biométricos

Al diseñar e implementar sistemas de reconocimiento se necesita disponer de herramientas y procedimientos que nos permitan medir la fiabilidad del sistema. Esto dará lugar a medidas de rendimiento que servirán para evaluar nuevas mejoras o desarrollos sobre el mismo sistema, así como para comparar los resultados de un sistema con los de otros.

Los sistemas de verificación se llevan a cabo generalmente en dos pasos. En primer lugar, se calcula un valor de similitud (o distancia) entre la muestra introducida por el individuo y la de referencia; posteriormente, este valor es comparado con un umbral tomándose entonces la decisión de aceptación o rechazo. La puntuación es función del parecido entre la muestra de la base de datos y la introducida por el individuo en el momento de la verificación. Cuanto mayor

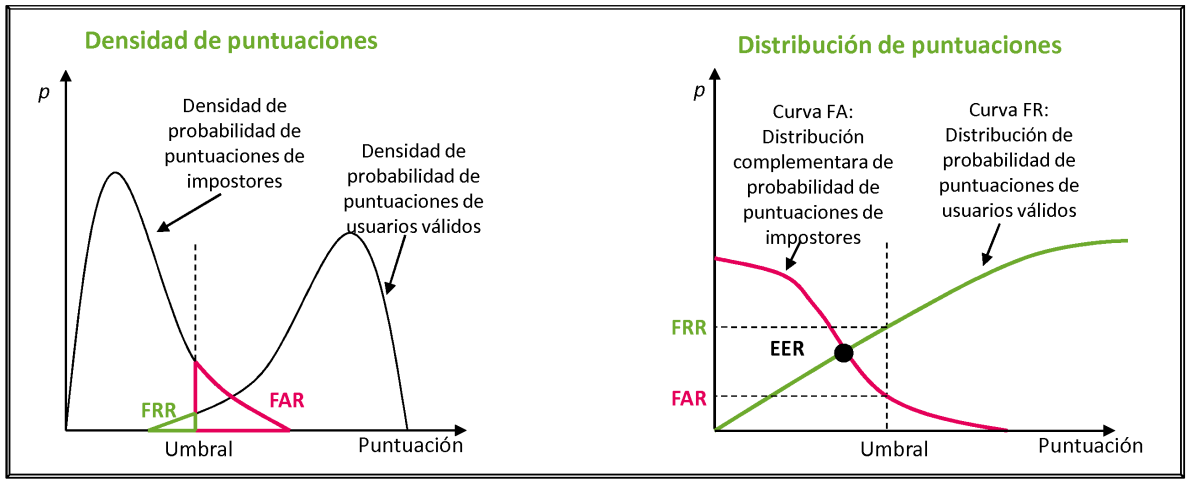


Figura 2.6: Ejemplos de densidades y distribuciones de probabilidades de usuarios e impostores.

sea el parecido entre las muestras, mayor será la puntuación devuelta por el comparador y habrá a priori más certeza de que las dos medidas biométricas pertenecen a la misma persona.

La decisión del sistema queda definida por el umbral, así los pares de muestras que generen puntuaciones mayores o iguales que el umbral se supondrán correspondientes a la misma persona, mientras que los que no alcancen el umbral se considerarán personas diferentes.

Medidas de evaluación de sistemas en modo verificación: Según las distribuciones de puntuaciones de usuarios y de impostores se obtendrá un sistema con menor o mayor capacidad de discriminación. Así, en el caso en el que las distribuciones de impostores y usuarios auténticos estén totalmente separadas, se podrán discriminar perfectamente ambas clases, mientras que en el caso de que exista solapamiento se fijará un umbral para dividir ambas regiones.

Si se fija un umbral, todas las puntuaciones, tanto de usuarios como de impostores, cuyo valor sea superior a ese umbral, serán interpretadas por el sistema como usuarios registrados. El área bajo la curva de impostores que queda por encima del umbral es la probabilidad de que un impostor sea aceptado y se conoce como la tasa de falsa aceptación (FAR, *False Acceptance Rate*). El área bajo la curva de usuarios válidos que queda por debajo del umbral es la probabilidad de que un usuario registrado no sea aceptado por el sistema y se denomina tasa de falso rechazo (FRR, *False Rejection Rate*)(veáse figura 2.6). Las tasas FAR y FRR son también conocidas como tasas FMR *(False Match Rate)* y FNMR *(False Non-Match Rate)*.

Los valores del umbral influyen de forma directa en las tasas de falsa aceptación y falso rechazo. Así, para un valor de umbral pequeño, pocos intentos auténticos serán rechazados, pero un número más alto de impostores serán aceptados de forma errónea. Y al contrario, si aumentamos el valor del umbral decrecerán las falsas aceptaciones a costa de incrementar los falsos rechazos. Por tanto, el establecimiento de umbrales estará condicionado por el punto de trabajo que exprese el compromiso a adquirir entre ambos tipos de error.

El punto en el que la FAR y la FRR son iguales se denomina *Equal Error Rate (EER)* y a menudo es empleado para comparar el rendimiento de diferentes sistemas sobre un conjunto de datos determinado. Para establecer el punto de trabajo óptimo del sistema se suele emplear la representación en forma de curvas DET *(Detection Error Tradeoff)*(veáse figura 2.7), variante de las curvas ROC cuya diferencia es un cambio de escala en los ejes, resultado curvas cuasi lineales. En este tipo de curvas cualquier punto define un valor de falsa aceptación (FAR) y otro de falso rechazo (FRR), de modo que no es necesario manejar varias curvas para conocer el rendimiento de un sistema y compararlo con otros.

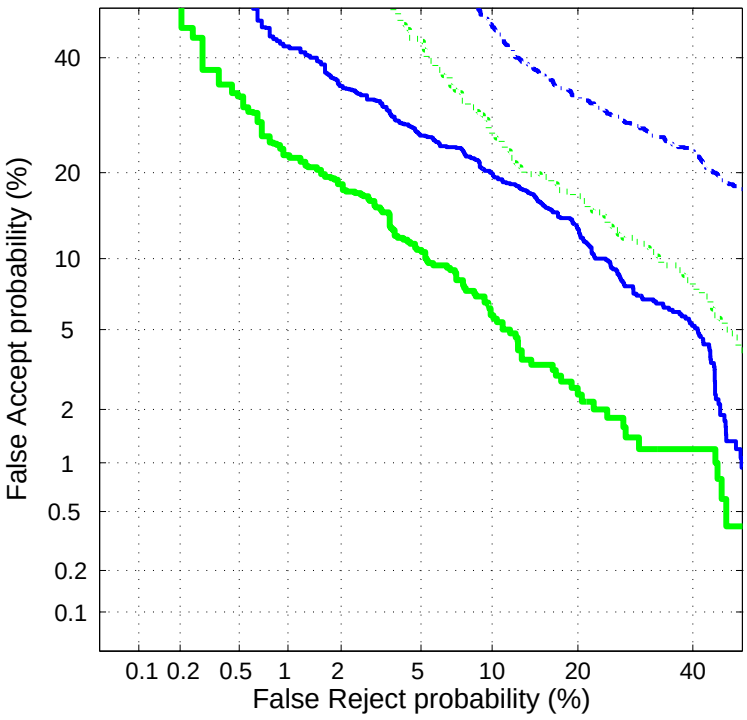


Figura 2.7: Ejemplo de curvas DET.

3

Reconocimiento de passwords gráficos

El método más habitual de identificación a través de dispositivos móviles o el ordenador es el uso de nombres de usuario y/o contraseñas alfanuméricas. Este método posee algunos inconvenientes. Los usuarios tienden a utilizar contraseñas fáciles de recordar, y en ocasiones fáciles de adivinar. Por otro lado, si una contraseña es difícil de adivinar suele ser también difícil de recordar. Para evitar este problema, se ha estudiado de un tiempo a esta parte métodos de autenticación que utilizan dibujos o imágenes como contraseñas, lo que se denomina *passwords gráficos* [10].

Los esquemas basados en passwords gráficos se han propuesto como una alternativa a los esquemas más conocidos de contraseñas/passwords basados en texto. Esto ha sido motivado parcialmente por el hecho de que las personas pueden recordar dibujos o gráficos con mayor facilidad que el texto [16]. Además, el hecho de que el número de dibujos a elegir o realizar es mayor hace que estos puedan ofrecer más resistencia a los ataques. Debido a estas ventajas, hay un crecimiento en el interés de estas nuevas técnicas de identificación basadas en passwords gráficos. Es posible aplicar esta técnica en estaciones de trabajo, aplicaciones web y dispositivos móviles.

Las técnicas basadas en passwords gráficos se pueden dividir en dos grupos: basadas en **reconocimiento** o en **repetición**. A continuación se resumen algunas propuestas de esquemas basados en técnicas de reconocimiento. Estas técnicas se caracterizan por presentar un conjunto de imágenes al usuario, éste tiene que reconocer el set seleccionado en el momento de registrarse. También se presentarán ejemplos de técnicas basadas en recordar, donde el usuario tendrá que reproducir lo que ha creado o seleccionado durante su registro.

Este Proyecto de Fin de Carrera centra su estudio en los passwords basados en repetición, concretamente en un subgrupo que consiste en la repetición de la realización hecha en el momento de registrarse en el sistema.

3.1. Técnicas basadas en el reconocimiento

Dhamija y Perrig [17] proponen un esquema de autenticación basado en *Hash Visualization algorithm (HVA)*. En este sistema el usuario tiene que elegir una serie de imágenes de un conjunto amplio generadas aleatoriamente. Posteriormente en la fase de identificación, el usuario selecciona las mismas imágenes elegidas en el momento de registro. El problema que presenta este sistema es que el proceso de identificación puede ser largo además de que los servidores tienen que almacenar un gran número de imágenes.

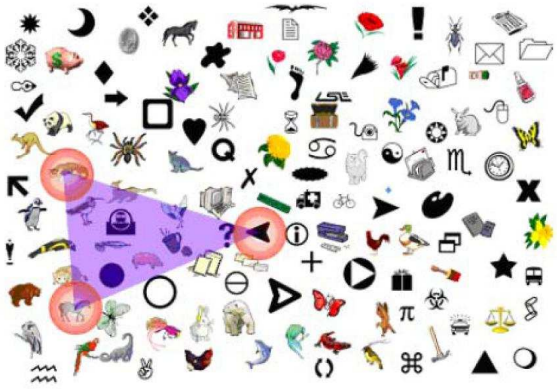


Figura 3.1: Password Gráfico desarrollado por Sobrado y Birget [1].

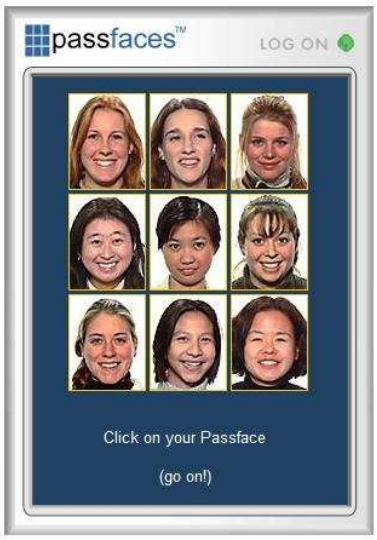


Figura 3.2: Ejemplo de Passfaces (fuente: www.realuser.com)

Sobrado y Birget [18] desarrollaron una técnica que trata el problema de posibles falsificadores con acceso visual a la realización del password (*shoulder-surfing*). El sistema muestra un número de objetos entre los que se encuentran algunos seleccionados previamente en la etapa de registro por el usuario. Para evitar el problema de que un posible impostor vea los objetos, lo que proponen es que estos se presenten con un tamaño reducido entre muchos otros. Posteriormente presentaron una pequeña variación que consistía en trasladar un marco poligonal de forma que las objetos seleccionados tocaran los vértices, en la figura 3.1 se observa un ejemplo de este sistema. Sugirieron repetir el proceso varias veces para minimizar la probabilidad de poder insertar el password de manera aleatoria. El mayor inconveniente de este sistema es que el proceso de registro es lento.

Un algoritmo que presenta una resistencia a posibles falsificadores de tipo *shoulder-surfing* es el propuesto por Man y Hong [19]. Los usuarios también elegirán en la etapa de registro una serie de objetos/imágenes como password. Cada objeto tendrá una serie de variantes y a cada una de ellas se le asigna un código. Durante el proceso de acreditación, se reta al usuario con varias escenas en las que aparecen los objetos que forman parte del password junto con otros como señuelo. El usuario tiene que introducir el código asociado a cada variante del objeto que este eligió como password. Posteriormente se hizo otra aproximación permitiendo al usuario introducir los códigos a los objetos. Este método sigue teniendo el inconveniente de memorizar datos.

Otra técnica desarrollada por "Real User Corporation" [20] se denomina "Passface" (veáse figura 3.2). La idea consiste en que el usuario elige un subconjunto de cuatro imágenes, cuya

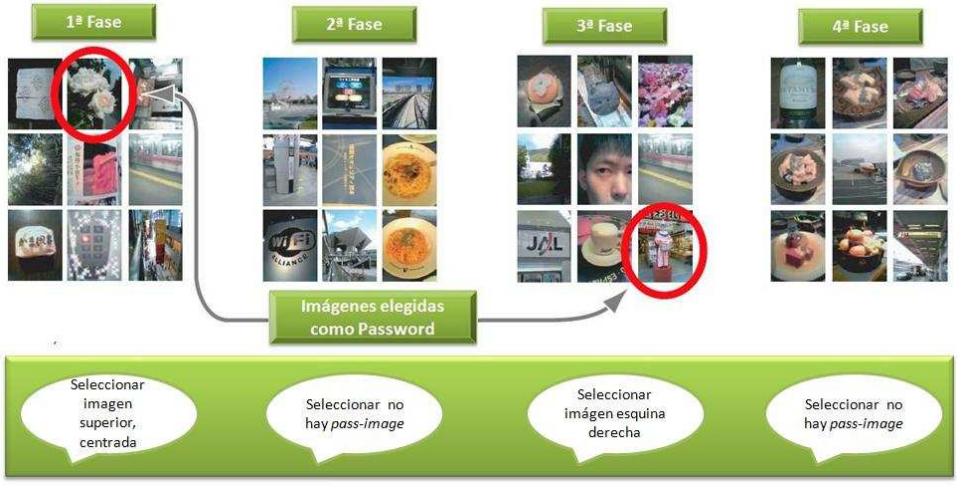


Figura 3.3: Etapas de proceso de verificación propuesto por Takada y Koike [2]. Esquema compuesto por cuatro etapas con nueve imágenes en cada etapa.

temática son caras humanas, de un conjunto más amplio. En la etapa de autenticación el usuario se enfrenta a una imagen compuesta por nueve caras entre las que se encuentra una del subconjunto elegido en la etapa de registro, el usuario tiene que pulsar sobre la cara. Este procedimiento se repite varias veces hasta reconocer las cuatro caras de su subconjunto de inscripción.

Un estudio en este ámbito es el propuesto por Takada y Koike para dispositivos móviles [2]. Esta técnica permite a los usuarios introducir sus propias imágenes para mayor facilidad en el proceso de identificación. En un primer momento el usuario registra sus imágenes favoritas (*pass-images*) y posteriormente éstas serán utilizadas para identificarse. Durante el proceso de verificación, el usuario tendrá que identificar las imágenes previamente seleccionadas. El programa autoriza al usuario si todas las elecciones son correctas. Este sistema facilita al usuario su recuerdo, pero no resuelve la problemática de que otra persona pueda tener acceso visual a la realización y reproducirla posteriormente. En la figura 3.3 se muestra en detalle el proceso de verificación, se representa un esquema de cuatro etapas pero este puede estar constituido por tantas como el usuario quiera.

3.2. Técnicas basadas en repetición

En este subconjunto el usuario tiene que repetir una acción creada o seleccionada con anterioridad. Dentro de este subgrupo se distinguen dos técnicas diferenciadas, las que se basan en reproducir un dibujo previamente realizado y las que se basan en repetir una selección.

Dentro de este conjunto, es importante la aportación de Jermyn *et al.* que proponen dos esquemas donde la importancia radica en orden temporal del password. Uno de los trabajos se denomina password textual con asistencia gráfica (*Textual Password with Graphical Assistance*) que como su nombre indica se basa en un contraseña textual extendida a una interfaz gráfica. En primer lugar se define una contraseña textual basada en k caracteres. Al usuario se le presenta una pantalla con un número de huecos, en la que se le indica el orden en que tiene que rellenar los huecos. Como se puede en la figura 3.4 el usuario puede introducir la contraseña en el orden normal de derecha a izquierda, pero también existe la posibilidad de introducirlo en otro orden, como rotado hacia la izquierda, de dentro hacia fuera o como una combinación de los dos casos anteriores.

El segundo esquema se conoce como DAS [3] (*Draw a Secret*) y se clasifica dentro de las técnicas de realización. Al usuario se le pide que realice un dibujo en una pantalla cuadriculada de tamaño $G \times G$, donde G es el tamaño de la cuadrícula. Un dibujo completo se codifica como

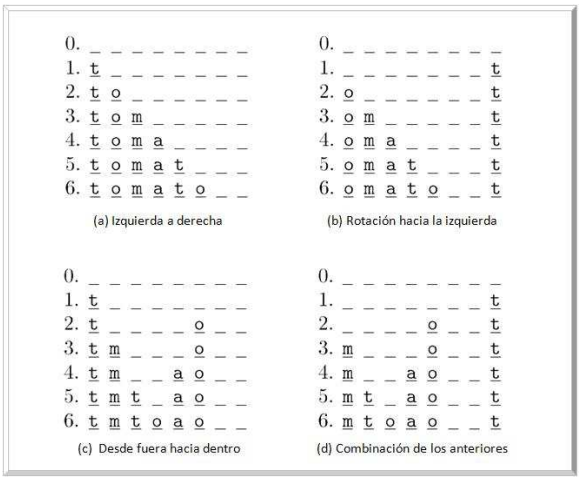


Figura 3.4: Variaciones de posición al introducir la contraseña "tomato". Se puede introducir de la manera corriente de izquierda a derecha (a). El paso 0 es la fila inicial y de la fila 1 a la 6 indica el orden temporal en el que el usuario rellena los huecos. Se puede variar la posición de las letras como se ve en el paso (b en el que se rota la primera letra hacia la izquierda, en el caso de (c) se representa una estrategia de fuera hacia dentro y la (d) que es una combinación de (b) y (c) [3].

una secuencia de coordenadas por las cuales el trazo va pasando a través de las celdas. En la etapa de verificación el usuario tiene que volver a realizar el dibujo, si este sigue la misma secuencia grabada en la etapa de registro entonces el usuario será clasificado como genuino. Un ejemplo es el representado en la figura 3.5.

En la figura 3.5 se muestra cómo en la primera captura de pantalla (etapa de registro) el usuario dibuja sobre la cuadrícula un password secreto (a), en el paso (b) y (c) se guarda la codificación de las celdas que el usuario toca con el dibujo y su consecución temporal. En el punto (e) el usuario tiene que introducir el password para identificarse, como las casillas dibujadas no son las mismas que en el paso de registro no se identifica al usuario como genuino.

Por último, dentro de este marco de reproducir dibujos como passwords se encuentra el trabajo realizado por Syuri *et al* [4]. Propone un sistema donde la identificación se lleva a cabo realizando un dibujo con el ratón sobre una pantalla cuadriculada, ver figura 3.6. Esta técnica consta de dos pasos: registro y verificación. En el proceso de registro se tomará muestras del dibujo del usuario realizado con el ratón. La información se guardara en una base de datos con las características extraídas de la muestra tras un proceso de normalización. En el proceso de verificación se le preguntará al usuario por su password, que introducirá de nuevo y de esta nueva muestra se extraerán los parámetros necesarios para comparar posteriormente con los datos de la base almacenada. El problema que presenta esta técnica es hay sujetos que no están familiarizados con el hecho de dibujar con el ratón.

Dentro de este grupo de passwords basados en repetición, se encuentra un subgrupo que se caracteriza por repetir una secuencia de acciones. En este grupo se encuentra el trabajo realizado por Blonder [21] que desarrolló un esquema de password basado en seguir una secuencia de puntos en una imagen. Para identificar al usuario como legítimo este deberá hacer click en áreas aproximadas a estos puntos. La imagen puede ayudar a los usuarios a recordar su password y por tanto se consideran más adecuados que passwords que no proporcionan esta ayuda. Passlogix diseñó un sistema basado en esta idea [22].

Passlogix ha desarrollado varias técnicas basadas en esta idea y añadiendo variaciones (véase figura 3.7). Por ejemplo, el sistema vGo incluye un esquema de password gráfico donde los usuarios pueden crear un cocktail combinando diferentes ingredientes. El inconveniente de este sistema es que provee de un número limitado de passwords y no hay modo de impedir que los usuarios no elijan passwords sencillos o predecibles.

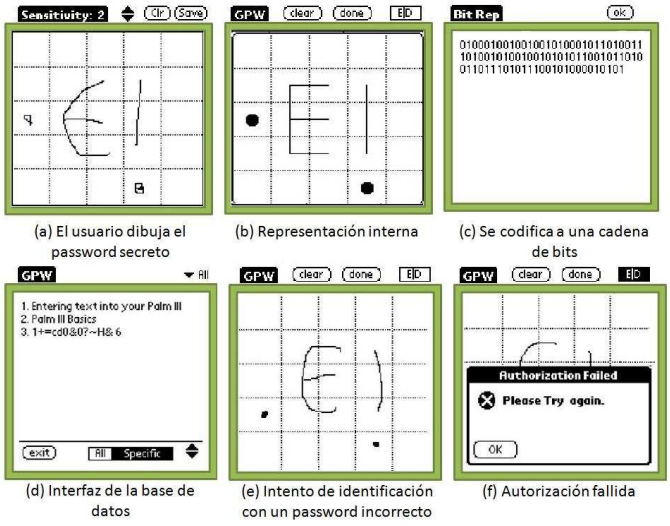


Figura 3.5: Etapas de registro y verificación en el sistema DAS [3].

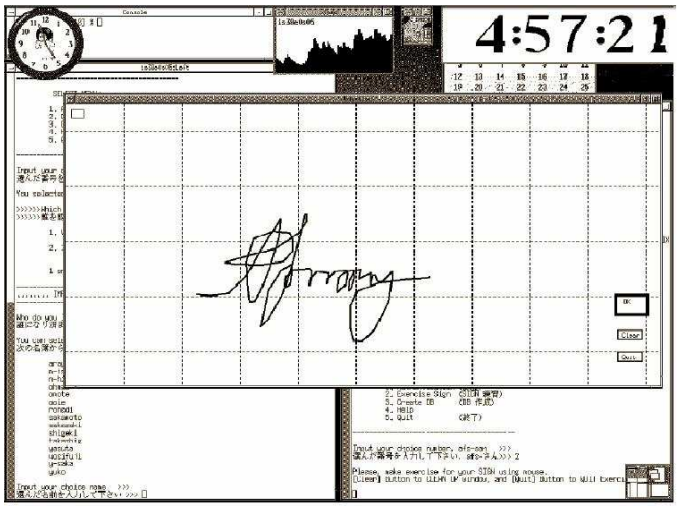


Figura 3.6: Ejemplo de firma realizada con el ratón [4].

Dentro de este grupo de passwords basados en el recuerdo, este proyecto se centra en los que requieren la repetición de un dibujo, trazo, garabato, etc. A continuación se explica con mayor detalle el subgrupo en el que se encuadra este trabajo.

3.3. Passdoodles

Los *passdoodles* reúnen varias de las características demandadas por los usuarios en sistemas de verificación: fiabilidad y comodidad entre otras. Se definen como un password que se crea manualmente dibujando. El termino *passdoodle* es presentado por Goldberg *et al.* [23] que lo define como un password compuesto por elementos escritos con la mano, pueden ser letras, números, dibujos o garabatos. Lo importante es que no es mecanografiado y que el usuario realiza un dibujo sobre una pantalla táctil.

Trabajos precursores de esta idea, que han impulsado la aparición de esta técnica de identificación son los realizados por Jermyn *et al.* [3], que introduce dos esquemas de passwords gráficos que no sólo se basan en lo que introduce el usuario si no en su orden temporal. Aquí reside la diferencia entre los passwords introducidos por teclado, en los que el orden temporal determina la posición de los caracteres en la contraseña, y este tipo de passwords gráficos (primera variación que se introduce en la idea de *passdoodles*) que pueden consistir en varios trazos o

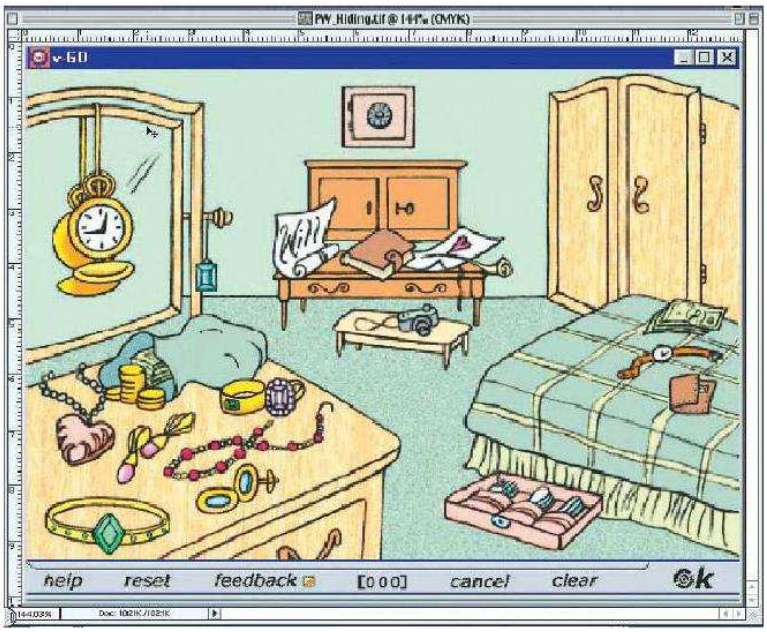


Figura 3.7: Técnica basada en repetición de acciones desarrollada por Passlogix (fuente: www.passlogix.com)

líneas, cuyo aspecto visual final es independiente de la consecución de trazos que ha realizado el usuario al dibujar el password. Este estudio muestra la independencia entre el aspecto final del password y su secuencia temporal a la hora de crearlo, es decir, el verlo no te proporciona toda la información, lo que da lugar a un método de autenticación que en algunos casos es más robusto que los passwords alfanuméricos y no por ello más difíciles de recordar.

El trabajo de Jermyn *et al.* se basa en la realización de un dibujo secreto (DAS, *Draw-a-Secret*), y se encuadra en lo que se conoce como password gráfico basado en una repetición. Es la idea predecesora al tema central de este proyecto, los *passdoodles*. DAS consiste en realizar un dibujo en una cuadrícula, que se mapea como una secuencia de pares de coordenadas por las que se pasa a la hora de realizar el dibujo. Por ejemplo en la figura 3.8 se codificaría como $(2,2),(3,2),(3,3),(2,3),(2,2),(2,1),(5,5)$ donde la coordenada $(5,5)$ indica que se ha levantado el lápiz, cursor o dedo y la secuencia continuaría como $(1,4),(1,3),(2,3),(1,3)(1,4),(5,5)$.

El problema de este tipo de passwords, es que es posible que dos realizaciones posean la misma consecución de coordenadas sin tener ninguna característica más en común, es decir, que la apariencia exterior del dibujo así como características ligadas a su realización sean dispares. Posterior a DAS es el estudio realizado por Varenhorst que propone como elementos para la verificación una combinación entre la velocidad de realización y la distribución de las muestras. El sistema de reconocimiento empieza encuadrando el *passdoodle* entre sus límites superior e inferior y se combinan varias muestras de entrenamiento haciendo una convolución gaussiana que da lugar a una muestra borrosa que se usará para distribuir los valores en la cuadrícula. Para acreditar una muestra como genuina se procesa con la distribución creada sobre la cuadrícula. Se busca una correspondencia entre cada punto de la muestra y la distribución [5]. Otra característica que obtiene del password gráfico es la velocidad de la muestra que también es útil en el proceso de reconocimiento ya que esta puede determinar la unicidad del *passdoodle*. Para ello, crea un vector de velocidades promedio para posteriormente comparar.

Otro estudio que se basa en la idea de *passdoodles* es el sistema de reconocimiento llamado "garabato secreto" (SAS *Scribble-a-Secret*) [24]. En este trabajo realizado por Oka *et al.*, se expone que su trabajo está relacionado con los sistemas de reconocimiento de firma on line. Se argumenta que aunque se podría pensar que su esquema SAS y los sistemas de verificación de firma son iguales se diferencian en algunos aspectos. Primero, las firmas manuscritas son consideradas como una forma de identificación biométrica por lo que se suelen tratar como un

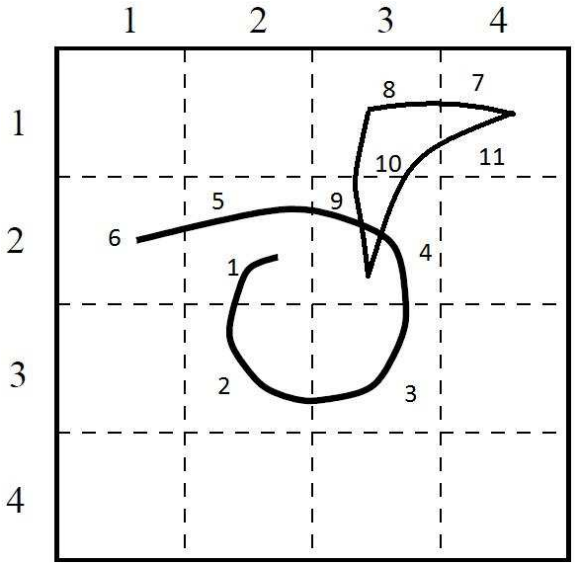


Figura 3.8: Password gráfico dibujado sobre una cuadrícula 4×4. El dibujo se mapea como la serie de pares de coordenadas que se recorren al dibujarlo [3].

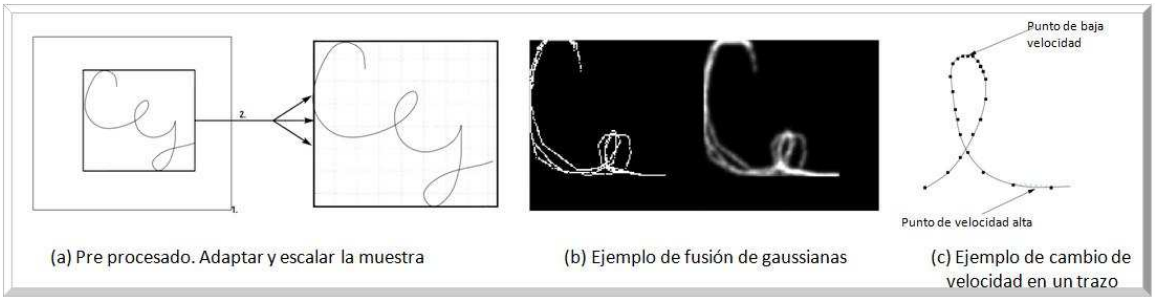


Figura 3.9: Vista general del proceso de reconocimiento de Doodles propuesto por Varenhorst [5].

rasgo de identificación único para cada individuo. El estudio de la firma on-line se basa en la suposición de que incluso observando la realización de la misma, es difícil reproducirla con el suficiente nivel de precisión y lo diferencia de su contraseña, argumentando que en general esta se mantendría en secreto. En este sistema las muestras se capturan como imágenes (off-line) y se calcula el modelo de orientación de los bordes. En los experimentos desarrollados cada boceto de usuario se compara con sus propios bocetos y con el resto de usuarios como si estos fueran falsificadores aleatorios.

Propuestas más recientes de sistemas basados en *passdoodles*, incorporan tanto elementos que deben ser recordados por el usuario como características que se sacan de la propia realización, es decir, no sólo se utiliza para el reconocimiento "qué hace" (ámbito de los passwords gráficos) sino "cómo lo hace" (ámbito de la biometría) donde el password se convierte en un rasgo de conducta.

En este apartado se ha presentado la idea de relacionar los *passdoodles* con algunas características y estudios que se han realizado sobre firma on-line. La verificación basada en firma on-line ha suscitado una alta aceptación e interés en la comunidad científica dando lugar a diversos trabajos científicos [25, 26]. La eclosión de dispositivos móviles y ordenadores portátiles tales como tabletPC, PDA, ultra-portablePC, móviles 3G o PocketPC están representando escenarios prometedores para la verificación basada en firma on-line, marco que se puede adaptar a los *passdoodles*.

4

Técnicas de reconocimiento de firma on-line

4.1. Reconocimiento de firma on-line

En este capítulo se resume el estado del arte en el reconocimiento automático de firma manuscrita on line. Las técnicas de reconocimiento ya consolidadas para firma on line se han tomado como base de nuestro estudio, con el objetivo de verificar si la realización de un dibujo simple a modo de password (*passdoodle*), posee características dinámicas útiles para su reconocimiento.

Existen dos grandes grupos de sistemas de verificación basados en la firma, dependiendo de la información que se extraiga de la muestra. Los sistemas de reconocimiento de firma dinámica *(on-line)* hacen uso de la información instantánea proporcionada por un dispositivo capturador, muestreando la trayectoria del trazo y generando una secuencia temporal con la misma. En contraposición, se habla de firma estática *(off-line)* cuando sólo se tienen acceso a la firma ya realizada y únicamente se dispone de su imagen.

Las ventajas del reconocimiento biométrico basado en firma son la alta aceptación personal, social y legal como medio de autenticación. Esta aceptación personal como rasgo biométrico se debe a que es poco invasivo en el proceso de adquisición. Además posee una buena adaptación en escenarios móviles o de bajo control, lo que ultimamente ha impulsado su estudio en estos entornos [27].

La firma ha sido utilizada durante años para validar documentos y transacciones legales. A pesar de su antigüedad sigue acaparando importantes estudios en la actualidad [28]. Los mayores retos del reconocimiento automático basado en firma on-line se fundamentan en la alta variabilidad intra-clase que ésta posee, en la alta variabilidad temporal entre sesiones y en la dificultad que añaden los posibles impostores entrenados.

La verificación basada en firma on-line puede ser utilizada en diversas aplicaciones. A continuación se citan las más destacadas:

Pagos comerciales: la firma se usa para validar pagos realizados via WiFi, UMTS, GPRS, o mediante otras redes móviles, lo que permite un acceso ubicuo.

Transacciones legales: documentos legales o certificados son firmados para añadir una seguridad adicional. Por ejemplo, en aplicaciones gubernamentales se podrían utilizar esquemas basados en firma on-line, recomendables a la hora de comprobar la legitimidad del usuario.

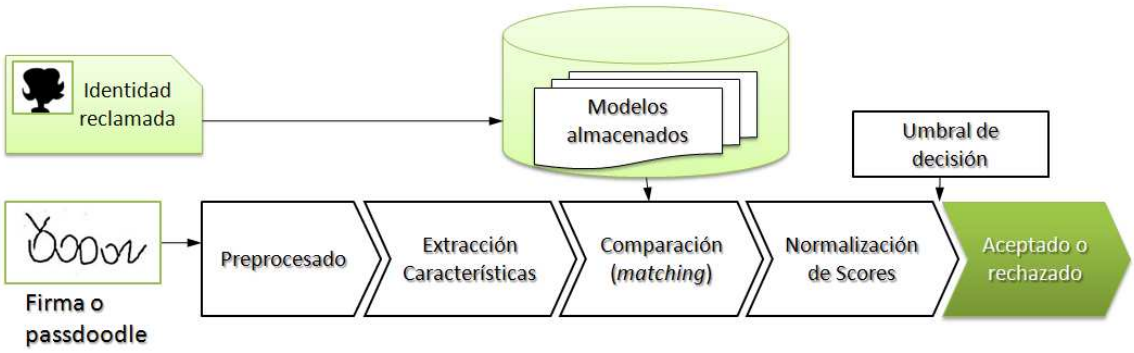


Figura 4.1: Esquema típico de un sistema de verificación de usuarios

Inicio de sesiones de usuario: la firma puede ser utilizada para iniciar una sesión en un sistema remoto o local, sustituyendo a los métodos tradicionales basados en PINs o passwords.

Validación de clientes: un cliente puede validar una acción mediante su firma on-line. La acreditación se puede realizar firmando en un dispositivo móvil declarando así su conformidad con el servicio recibido.

Documentos digitales: hoy en día vivimos el auge de la era digital y muchos documentos se firman electrónicamente proporcionándoles una identificación y un acceso selectivo.

En todas estas aplicaciones el sistema de verificación puede ser remoto o local. La única diferencia es dónde se lleva a cabo el proceso de comparación (*matching*). En el caso de verificación local, el proceso de comparación se lleva a cabo en el propio dispositivo capturador, mientras que cuando el sistema de verificación es remoto se necesita un servidor externo.

Puede haber reticencias por parte de algunos usuarios a realizar su firma y que ésta sea digitalizada ya que la firma se ha utilizado durante años, no sólo como señal de acreditación o consentimiento en un escrito sino también como método que establece la capacidad de una persona en la realización de una transacción (p. ej. el pago con tarjeta de crédito). Además, la ausencia de estilete en los dispositivos electrónicos más modernos complicaría la realización de la firma o su posible verificación debido a la variabilidad que introduciría el hecho de no tener un hábito de escritura sin un instrumento de caligrafía. Por estos motivos, entre otros, se ha propuesto el uso de passwords gráficos (*passdoodles*) en dispositivos móviles realizados directamente con el dedo como posible método de reconocimiento.

A continuación se exponen las diferentes arquitecturas y métodos de reconocimiento en firma dinámica que se han adaptado al objeto de este estudio

4.1.1. Arquitectura de un sistema de verificación en firma on-line

En rasgos generales, los sistemas de verificación de usuarios utilizando la firma on-line siguen un procedimiento común, el cual se reproduce para el caso del presente estudio, los passwords gráficos. La estructura típica de un sistema de verificación se representa en la figura 4.1.

1. **Adquisición de la muestra**: la captura consiste en la reproducción de la firma sobre un dispositivo que posea sensor al efecto como una PDA, tabletPC o terminal táctil. El dispositivo digitalizador almacena las secuencias temporales procedentes de los trazos capturados. Normalmente la velocidad de muestreo alcanza o supera los 100 Hz. Este valor de muestreo es adecuado debido a que se ha estudiado que la frecuencia máxima a la que se realiza la firma es aproximadamente de 20-30 Hz [26]. Después de capturar la muestra se suele llevar a cabo un preprocesado de la señal adquirida.

2. **Extracción de características**: las características pueden clasificarse en dos grupos, globales y locales. Los sistemas basados en parámetros globales extraen de un vector de parámetros (p. ej. velocidad, aceleración, duración) que definen de forma general (global) las firmas. Los parámetros locales están formados por una o varias funciones base cuyas muestras constituyen los vectores de características (p. ej. secuencia de coordenadas x o y). Después de la obtención del vector de características puede ser necesario llevar a cabo algún tipo de normalización.

3. **Registro**: en los sistemas basados en un modelo se calcula un modelo estadístico a partir de varias firmas genuinas del usuario. Posteriormente, se utilizará este modelo para compararlo con la muestra introducida en el momento de identificarse. Por contra, los sistemas basados en referencia se almacenan todas las características de cada firma de entrenamiento como un vector de patrones. El proceso de *matching* se llevará a cabo con cada una de las firmas de entrenamiento.

4. **Matching**: la comparación o *matching* de las muestras es el paso central en un sistema de verificación. Para calcular la puntuación o *score* se pueden utilizar dos métodos. Los sistemas basados en parámetros globales constan de un vector de características global y su similitud se mide por la distancia entre vectores (Mahalanobis, Euclídea, etc.). Los sistemas basados en secuencias (funciones) usan otras técnicas como los Modelos Ocultos de Markov - HMM (*Hidden Markov Models*) [29], o el alineamiento temporal dinámico - DTW (*Dynamic Time Warping*) [30] para comparar las distintas muestras.

5. **Normalización de scores**: La puntuación obtenida se normaliza hasta un rango dado, por ejemplo $[0, 1]$. Cuando se trabaja con un sistema multi-biométrico (sistema constituido por varias modalidades biométricas) es necesario una normalización de los *scores* precisa, dado que es necesario combinar las salidas de varios sistemas.

4.1.2. Parámetros globales

Los métodos de reconocimiento de firma dinámica basados en parámetros globales (vector de características) emplean en general técnicas del ámbito de reconocimiento de patrones [31].

En esta clase de sistemas se crea un vector compuesto por características que definen de forma general a la firma, como la duración, velocidad media o el número de trazos. Existen en la literatura diversos trabajos que intentan resolver la cuestión de qué características que definen a la firma pueden diferenciarla mejor con respecto a otras, así como cuál debe ser el tamaño del vector de características [32, 33, 34]. Existe una gran cantidad de parámetros globales propuestos a lo largo de los últimos años [8]. Los parámetros globales también se usan en otros ámbitos como en sistemas basados en reconocimiento de trazos; un ejemplo es el presentado en GRANDMA (*Gesture Recognizers Automated in a Novel Direct Manipulation Architecture*), cuyo vector de características consta de 12 parámetros [6].

4.1.3. Parámetros locales

Los sistemas basados en secuencias (funciones) se conocen como sistemas locales. Los más populares en el reconocimiento de firma on-line son los presentados a continuación:

1. **DTW (Dynamic Time Warping)**: Técnica que compensa la problemática inherente a diferentes realizaciones de una firma, en las que se observa una variabilidad interna de modo que no existe una sincronización temporal, originalmente propuesta para voz. Esta falta de alineamiento se da de forma heterogénea en cada realización de la firma. Yasuhara y Oka fueron los primeros en emplear este algoritmo para medir las funciones temporales extraídas de una firma on-line [35]. La idea básica de este algoritmo ha sido

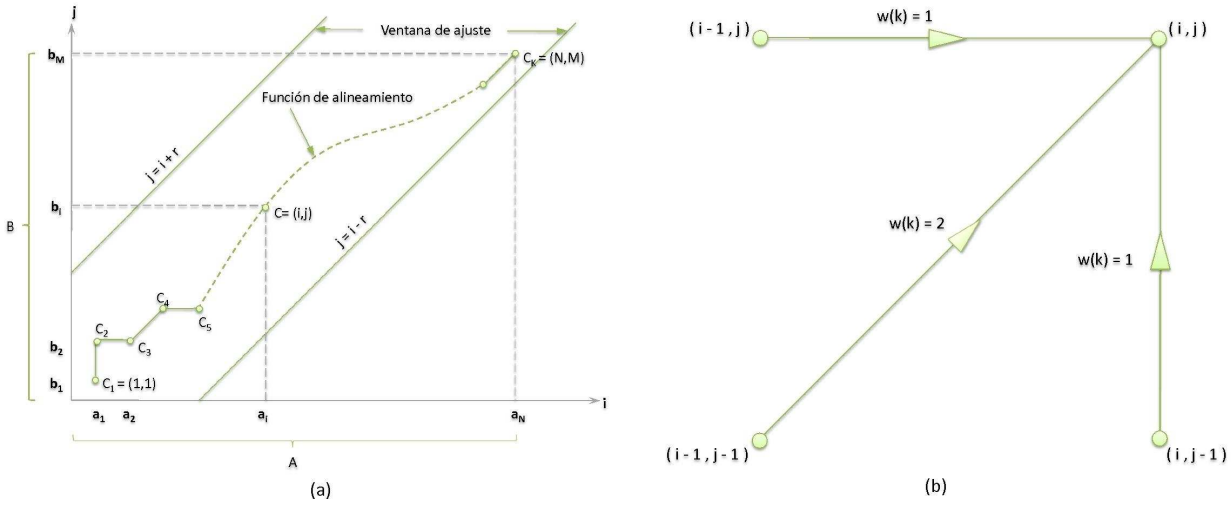


Figura 4.2: (a) Representación de la función de alineamiento del DTW. (b) Ejemplo de los pesos para diferentes transiciones.

mostrada en varias publicaciones aunque son Sakoe y Chiba los pioneros en presentarla para reconocimiento de habla [30]. Se presenta a continuación el algoritmo DTW.

Se definen dos vectores de características (patrones) A y B:

$$\begin{aligned} A &= a_1, a_2, ..., a_i, ..., a_M \\ B &= b_1, b_2, ..., b_j, ..., b_N \end{aligned} \tag{4.1}$$

llamando c a la función de alineamiento y siendo $c(k)$ un par de punteros a los elementos a comparar, se obtiene

$$C = c(1), c(2), ..., c(k), ..., c(K)c(k) = [i(k), j(k)] \tag{4.2}$$

para cada $c(k)$ se define una función de coste, donde es típico utilizar la distancia Euclídea.

$$d(i,j) = \|a_i - b_j\| \tag{4.3}$$

El problema de calcular la función de alineamiento se resuelve mediante técnicas de programación dinámica. Una posible idea para la resolución del problema consistiría en calcular $D(c)$ por todos los caminos posibles, eligiendo posteriormente el de menor coste, pero sería muy costoso a efectos de cálculo. La programación dinámica dice que el mejor camino entre (1,1) y cualquier punto (i,j) es independiente de lo que suceda en puntos posteriores por lo que se calcula el coste total del punto $[i(k), j(k)]$:

$$g_k = g(i,j) = \min_{c_{k-1}} [g_{k-1} + d(c_k) \cdot w(k)] \tag{4.4}$$

g_k es la distancia acumulada después de k pasos y $w(k)$ es el peso de cada camino a seguir. Una de las limitaciones que debe cumplir la función de alineamiento es que debe ser monótona creciente y que debe alinear los puntos finales de A y B lo que significa terminar en la muestra $M \times N$. La distancia normalizada es

$$D(X,Y) = \frac{g_K}{\sum_{k=1}^{K} w(k)} \tag{4.5}$$

donde el sumatorio de los pesos, $w(k)$, compensa el efecto de la longitud de las secuencias. Existen unos límites locales que dan lugar a la denominada "restricción de pendiente". En este caso sólo se permite llegar a un punto desde tres caminos diferentes:

$$g_k = g(i,j) = \min \begin{bmatrix} g(i,j-1) + d(i,j) \\ g(i-1,j-1) + 2d(i,j) \\ g(i-1,j) + d(i,j) \end{bmatrix} \tag{4.6}$$

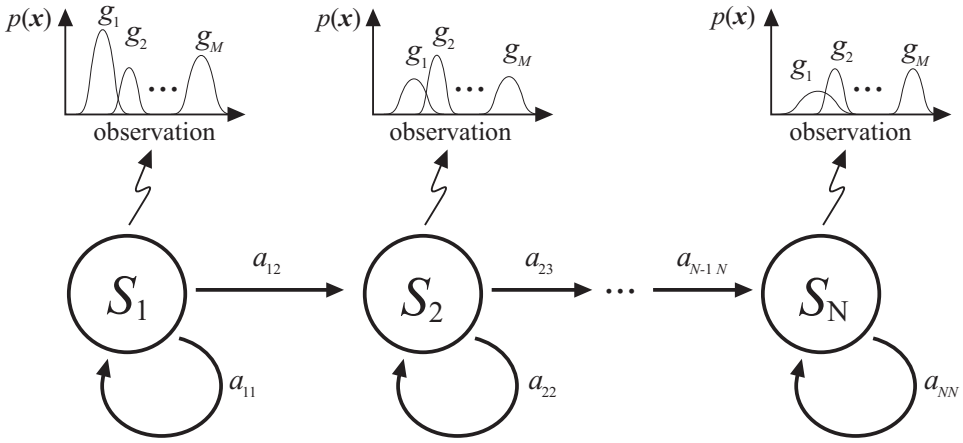


Figura 4.3: Representación de un HMM de N estados.

esta restricción es una de las más utilizadas en las literatura. En la figura 4.2 se muestra una representación de la función de alineamiento y un ejemplo de definición de pesos.

2. **HMM (Hidden Markov Models)**: Los modelos ocultos de Markov (*Hidden Markov Models*, HMM) son muy utilizados para el reconocimiento de habla [36] así como para algunas aplicaciones de reconocimiento de escritura [37]. Los HMM son modelos estadísticos en el que el sistema a modelar es una cadena de Markov con un número finito de estados, a cada estado se asocia un conjunto de funciones que generan un vector de observaciones. Este vector de observaciones se considera que ha sido generado según una función de densidad de probabilidad que se puede describir como una suma ponderada de gaussianas multivariadas, GMMs (*Gaussian Mixture Models*).

   Un HMM queda caracterizado por los siguientes elementos:

   - Número de estados en el modelo, N.
     - Denotamos cada estado como S_i
     - Denotamos el estado en el instante t como q_t
     - Si el sistema está en el estado S_i en el instante t se escribe $q_t = Si$
   - Número de símbolos observables por estado M.
   - La distribución de probabilidades de transición entre estados $\mathbf{A} = \{a_{ij}\}$.
     $a_{ij} = P[q_{t+1} = S_j | q_t = S_i]$

   En la figura 4.3 se muestra un HMM cuya topología es de Bakis o de izquierda a derecha donde se establece que una vez se abandona un estado no es posible volver a él.

5

Captura de una base de datos de passwords gráficos

En este proyecto se ha llevado a cabo la captura de una base de datos constituida por varias realizaciones de un *doodle* y una media firma por usuario. Esta base de datos permite la realización de experimentos sistemáticos sobre un conjunto de tamaño significativo en términos estadísticos. No se tiene constancia de la existencia de una base de datos de estas características, al menos de ámbito público. El protocolo de captura se ha basado en el seguido en otras bases de datos como BioSecure [28].

5.1. Procedimiento de adquisición

La base de datos consta de una media firma y un *doodle* capturados con un dispositivo móvil táctil "HTC Touch HD" que dispone de una pantalla WVGA de 3,8 pulgadas sobre la que se dibuja con el dedo. La pantalla digitalizadora captura la información on line de las muestras realizadas. Alguna de las características de esta base de datos son: escenario realista en el proceso de captura, equilibrio de género en el número de participantes y tiempo de entrenamiento para permitir al usuario acostumbrarse al dispositivo.

Las muestras se han recogido a lo largo de un periodo de seis meses utilizando un dispositivo móvil provisto por el ATVS. La captura consiste en dibujar con el dedo, tanto la media firma como el *doodle*, sobre la pantalla táctil (véase figura 5.1). La media firma consiste en una versión simplificada de la firma o rúbrica de cada usuario, en general está constituida por las iniciales junto con una rúbrica. El *doodle* se basa en un dibujo realizado sobre la pantalla a modo de contraseña. En el momento de la captura se ha dado especial importancia a la postura del usuario al realizar la muestra, reiterando que se mantuviera el móvil en la mano sin apoyarlo en ninguna superficie para simular un escenario lo más realista posible. Además, como paso previo, los usuarios practicaban su firma y password para familiarizarse con el dispositivo. Los passwords recogidos son muestreados a 100 Hz guardándose una muestra que consiste en un conjunto de valores de la posición horizontal (x) y la vertical (y); así como el tiempo entre muestras consecutivas.

Han participado un total de 100 usuarios. El conjunto de media firma y *doodle* genuino se ha capturado en dos sesiones separadas por un periodo de una a dos semanas. En cada sesión el usuario realizaba un total de 25 firmas: 15 de ellas genuinas, y las 10 restantes, falsificaciones. La secuencia de adquisición era la siguiente: 5 firmas genuinas - 5 falsificaciones - 5 firmas genuinas - 5 falsificaciones - 5 genuinas. Las falsificaciones de cada usuario han sido realizadas por 4 falsificadores distintos (5 falsificaciones cada uno), y antes de cada realización se permitía al

Figura 5.1: Ejemplo de adquisición de un *doodle*.

falsificador ver la ejecución on-line sobre la pantalla y ensayar hasta que estuviese satisfecho con la imitación.

Algunos ejemplos de medias firmas (genuina y falsificada) y de *doodles* junto con las señales capturadas se muestran en la figura 5.2 y en la figura 5.3 respectivamente.

Cada usuario se identifica por tres dígitos. Para diferenciar a la media firma del *doodle* les precede un dígito, 1 para el caso de la firma y 2 para el *doodle* quedando la identificación como 1uuu donde *uuu* es el número de usuario para medias firmas y 2uuu para *doodles*. Cada muestra se almacena en un archivo de texto individual con la extensión ".txt" y se identifican con un nombre:

- $SIGN-GENX-USmuuu-USmuuu-T$ identificación de muestra(*signature*) genuina.
- $SIGN-FORX-USmfff-USmuuu-T$ identificación de muestra falsificada.

Se diferencian la realización genuina de la falsificada de un usuario por la abreviatura GEN *genuine* (genuina) y FOR de *forgery* (falsificación). La "X" define el conjunto de genuinas/falsificadas al que pertenece la muestra. Se han realizado tres capturas separadas por dos conjuntos de falsificaciones por lo que las genuinas pueden pertenecer al conjunto 1, 2 o 3 mientras que las falsificadas pueden pertenecer al primero (1) o segundo grupo (2). La "m" que precede al número de identificación del usuario corresponde al identificador de media firma o *doodle*. La "T" establece el número de muestras realizadas, se va incrementando a medida que se realizan firmas, en general va de 1 hasta 50 que son las firmas que se tiene por usuario cuando la captura se ha completado. En el caso de las falsificaciones se guarda un identificador denotado por "fff" que identifican al impostor que es uno de los cuatro participantes posteriores, los dos siguientes para la primera sesión (SS1) y los otros dos sucesivos para la segunda sesión (SS2). Por último "uuu" identifica al usuario falsificado.

En el momento en el que un usuario tiene que realizar una falsificación, el *software* del móvil reproduce en la pantalla la media firma o *doodle* realizado por el participante anterior, es decir, el falsificador aleatorio accede a la reproducción temporal de la muestra. Además, se permite al falsificador ver la ejecución sobre la pantalla del password antes de cada falsificación a realizar,

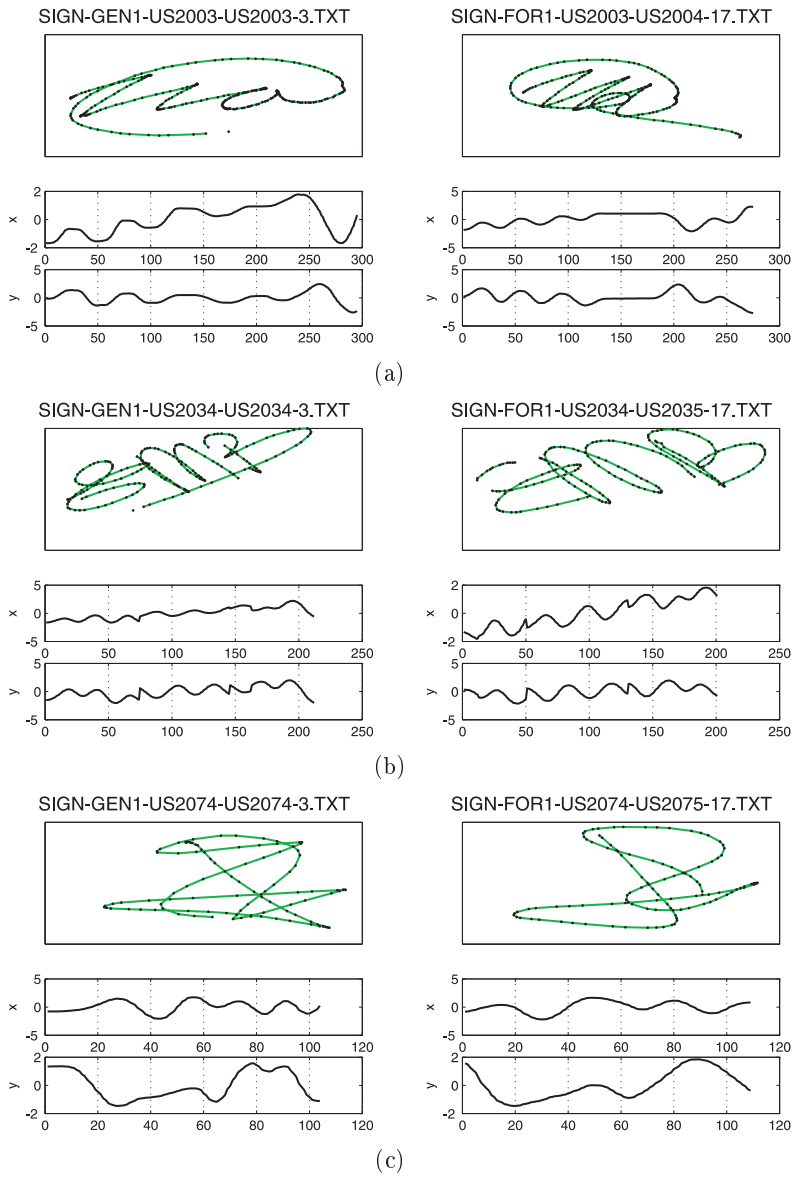


Figura 5.2: (a), (b) y (c) Ejemplos de medias firmas genuinas en el lado izquierdo y su correspondiente falsificación a la derecha con las coordenadas que se capturan.

por lo que podemos clasificar las falsificaciones realizadas por cuatro usuarios aleatorios como falsificaciones entrenadas.

5.2. Características de la base de datos

En esta base de datos han participado un total de 100 usuarios de los cuales la mayoría pertenece al ámbito universitario, por lo que el 80 % tiene edades comprendidas entre 20 y 25 años y género equilibrado. Hay un conjunto de participantes con edades comprendidas entre los 30 y 60 años también. Esta diferencia de edad se ha reflejado en la habilidad de los diferentes grupos de usuarios a la hora de realizar el dibujo en la pantalla. En general, los usuarios más jóvenes estaban más familiarizados con esta tecnología. Se ha intentado que participaran usuarios que ya lo habían hecho en bases de datos anteriores (p. ej. BioSecure) con el objetivo de solapar los máximos posibles y así comparar las realizaciones.

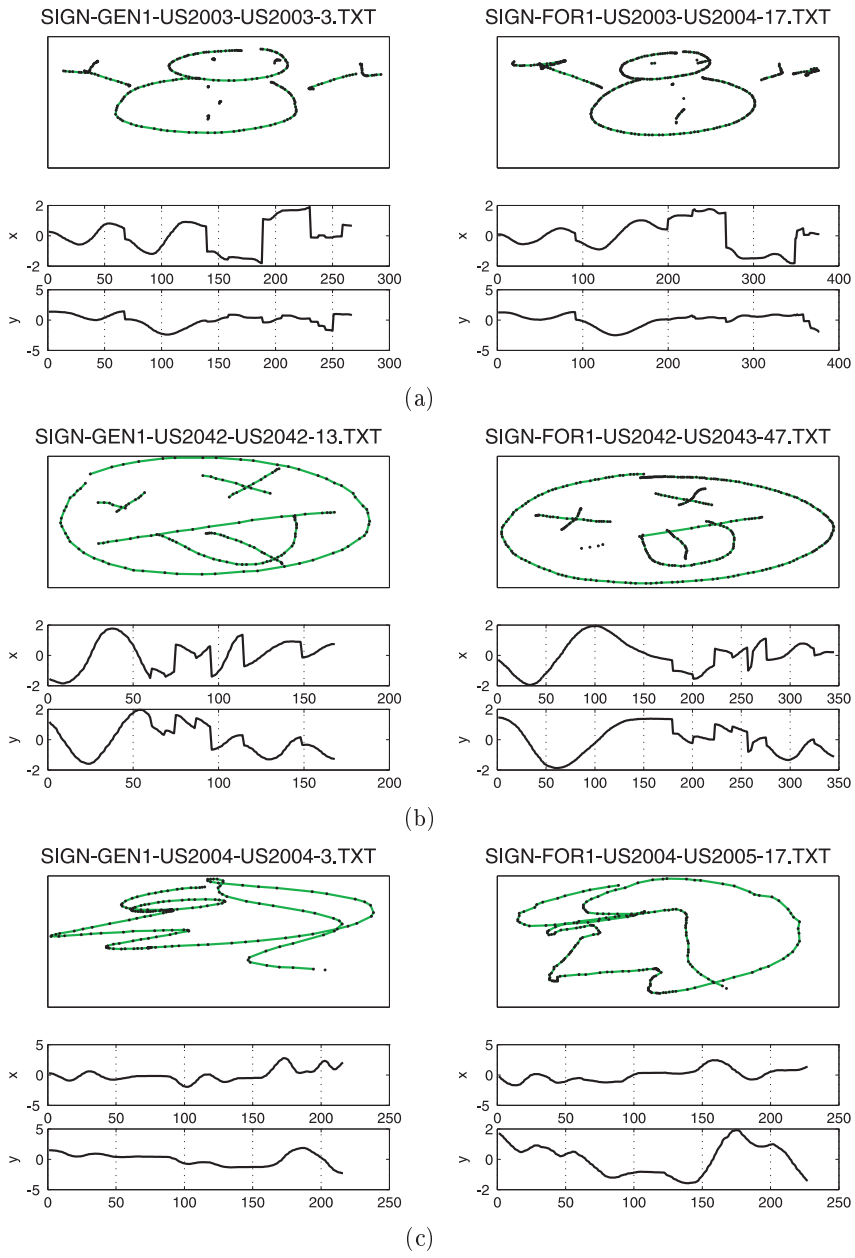
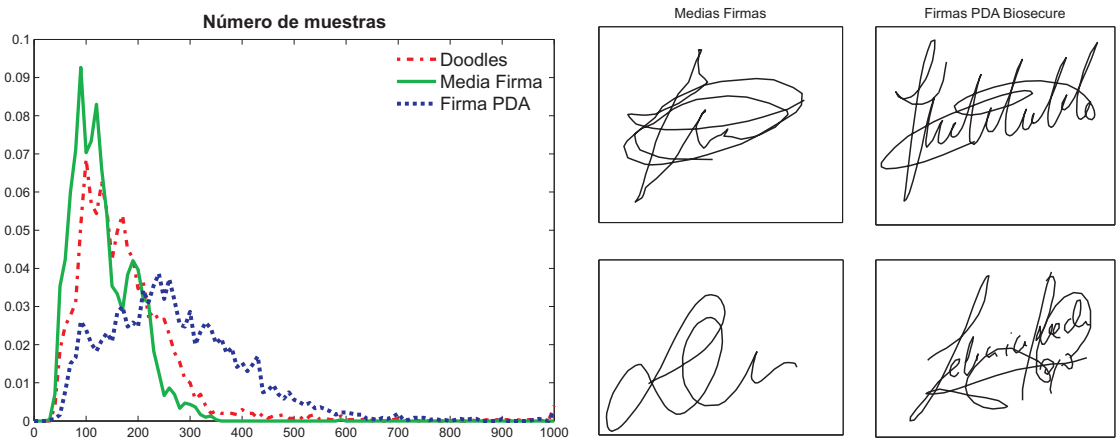


Figura 5.3: (a), (b) y (c) Ejemplos de *doodles* genuinos en el lado izquierdo y su correspondiente falsificaciones a la derecha con las coordenadas que se capturan.

5.2.1. Análisis cualitativo

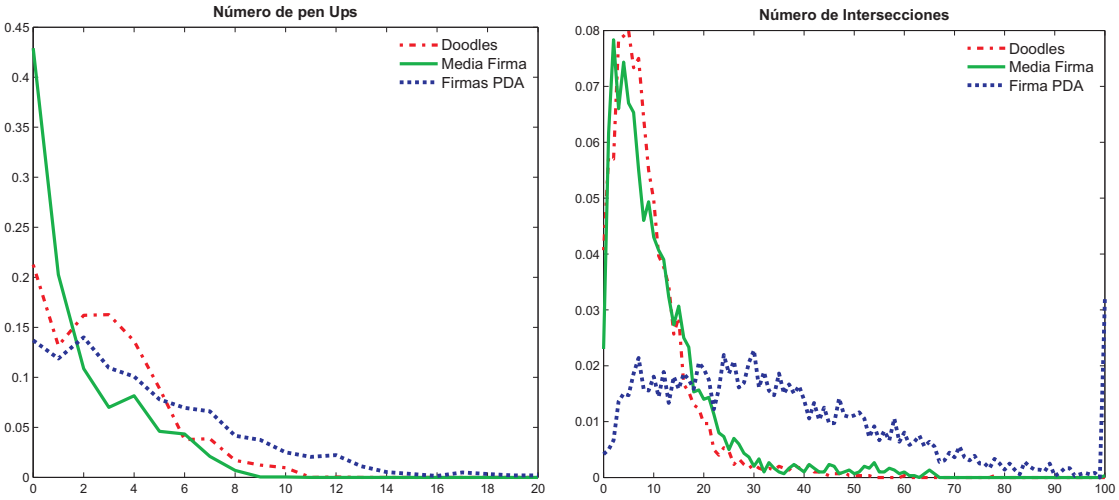
Se han analizado y comparado las similitudes y diferencias estadísticas entre firmas, *doodles* y medias firmas. Para este apartado se ha empleado una base de datos de firma on-line capturada sobre PDA por el ATVS perteneciente a la base de datos BioSecure [38]. Como paso previo a la comparación entre bases de datos se ha realizado un preprocesado previo idéntico al realizado para media firma y *doodle*. Este preprocesado se basa en interpolar linealmente los puntos cuya captura ha sido errónea debido a errores del dispositivo y se realiza una normalización tanto de coordenadas como de tamaño. Una vez realizado este preprocesado común se obtienen los siguientes resultados que se muestran de forma gráfica. Es interesante la comparación con una base de datos de firma on-line ya que puede permitir predecir, o al menos establecer hipótesis, sobre cómo será el rendimiento del reconocimiento de passwords gráficos (media firma y password gráfico) frente a firma sobre PDA con estilete.

En la figura 5.4 se muestra la distribución estadística de la cantidad de muestras de las tres bases de datos a comparar. Se observa que en general el número de muestras en el caso de las



(a) (b)

Figura 5.4: (a) Distribución del número de muestras de los tres escenarios a comparar. (b) Ejemplos de medias firmas y firmas realizadas con un estilete sobre la PDA de los mismos usuarios.



(a) (b)

Figura 5.5: Diagrama comparativo de la distribución del número de pen-ups de los tres escenarios (a) y el número de intersecciones (b).

medias firmas es mucho menor que en el caso de firmas genuinas realizadas sobre una PDA con un estilete. Para passwords gráficos el número de muestras también es menor en términos generales que para firma on-line y en general para *doodles* es algo mayor que para medias firmas. Por lo tanto según lo que muestra la distribución se puede afirmar que los *doodles* y las medias firmas son realizaciones en principio más simples que contienen mucha menos información, al menos desde un punto de vista intuitivo, que las firmas reales.

La figura 5.5 (a) representa el número de *pen ups*, alzamientos del dispositivo de escritura (estilete para firma y dedo para los *passdoodles*). Es notable la diferencia en el caso de medias firmas en el que el número de pen-ups es muy bajo, esto se debe a que la realización solía contar en su mayoría con un sólo trazo al tratarse de iniciales o rúbricas. Es razonable pensar por tanto que en general son más simples, lo cual se refleja también en el número de intersecciones 5.5 (b). Las medias firmas y los bocetos como passwords gráficos tienen pocas intersecciones al tratarse de trazos abiertos y simples, mientras que en la firma son realizaciones más complejas y el hecho de que posean letras aumenta el número de intersecciones.

La distribución representada en la figura 5.6 se obtiene del cálculo de la velocidad media de todas las muestras genuinas. Se puede apreciar que los *doodles* en general tienen velocidades

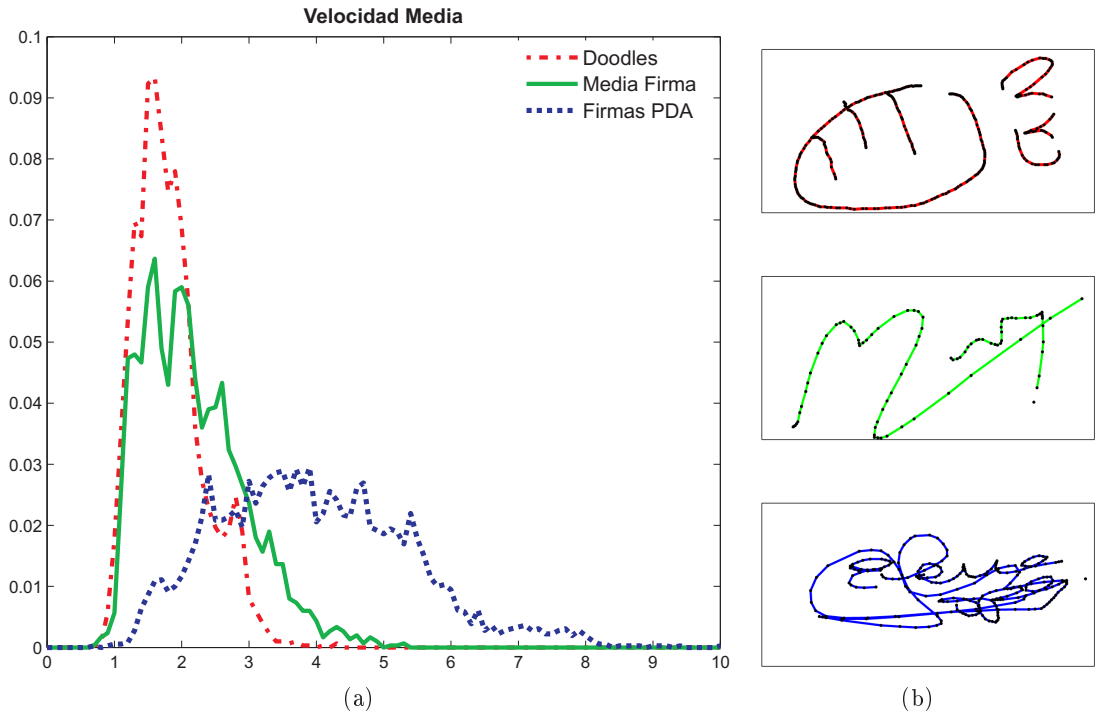


Figura 5.6: (a) Distribución de la velocidad media en los tres escenarios. (b) Ejemplos de *doodle*, media firma y firma.

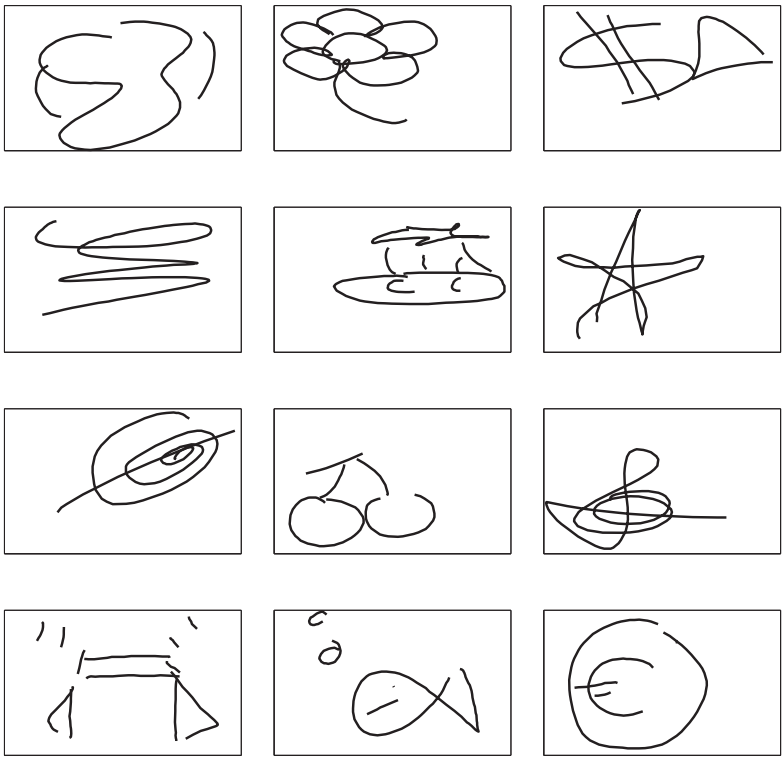
menores que las medias firmas y las firmas capturadas por la PDA. Este hecho se puede deber a que en muchos casos se le plantea al usuario una problemática al preguntarle por un password gráfico que no están acostumbrados a hacer y que en la mayoría de los casos se inventaban en el momento, por lo tanto no es un acto que realicen con mucha frecuencia. Sin embargo, para el caso de las medias firmas que suelen consistir en las iniciales del nombre o una versión simplificada de su firma, la ejecución de la misma es un acto aprendido y por tanto la velocidad es mayor que en los *doodles* en la mayoría de los casos. Por último es la firma sobre PDA la que posee una velocidad media superior en general ya que el movimiento es aprendido, los usuarios tienen mayor habilidad con el estilete y este ofrece menos rozamiento con la superficie al escribir. La velocidad media se representa de forma adimensional al ser irrelevante para la comparación estadística.

5.2.2. Clasificación subjetiva

Atendiendo al tipo de *doodle* que los usuarios han realizado como password gráfico, se ha hecho una clasificación que divide a estos en tres subgrupos (representados en la figura 5.7):

- **Abstracto**, no representa algo concreto sino que atiende exclusivamente a elementos de forma como rayas, círculos, flechas, etc.
- **Conceptual**, representan una idea o noción, suelen ser passwords que representan un objeto reconocible, entre ellos encontramos por ejemplo un coche o una flor.
- **Simbólico**, formados por uno o varios símbolos reconocibles que representan una idea perceptible, un ejemplo de este subgrupo es el "yin-yan".

Del estudio individual de las muestras según la clasificación anterior, puede ser posible predecir características interesantes del rendimiento de la verificación. Cabe esperar que los passwords conceptuales sean más fáciles de recordar y realizar por un falsificador, mientras que no sea tan sencillo en el caso de un password abstracto que suele estar constituido por un conjunto de



(a) (b) (c)

Figura 5.7: (a) Ejemplos de passwords abstractos. (b) Ejemplo de passwords que representan un concepto (flor-vaca-cerezas-pez). (c) Ejemplos de passwords simbólicos

líneas y trazos inconexos. Además a la hora de recordar la secuencia de trazos en un password conceptual es más sencillo el realizar una asociación de ideas.

6

Sistemas de verificación de passwords gráficos

En este capítulo se definen los principales sistemas de verificación que se han utilizado en este trabajo. En la implementación del sistema de verificación que nos ocupa se utilizan tanto métodos basados en parámetros globales como locales, cuyo fundamento se encuentra en estudios de firma on-line. Para el desarrollo del sistema basado en parámetros globales se han utilizado diferentes grupos de características extraídas directamente de la firma [6, 27] para estudiar aquellas que presentan mejor rendimiento. El sistema de parámetros locales se basa en la técnica de DTW [30] junto con la extracción correspondiente de un conjunto de parámetros.

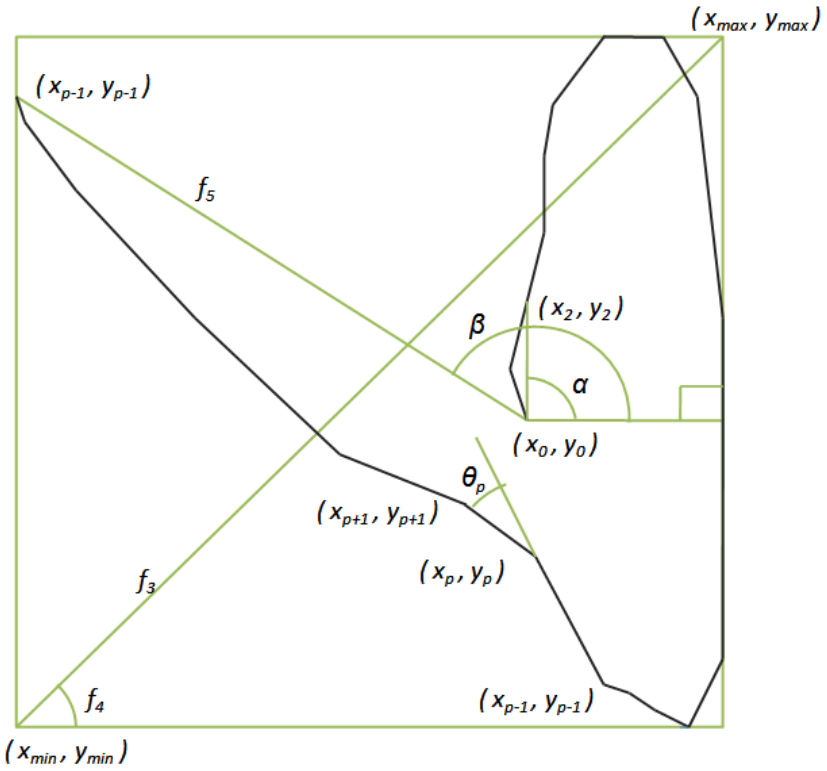
6.1. Sistema de verificación basado en parámetros globales

El sistema de verificación basado en parámetros globales consiste en una etapa de extracción de características que definen de forma general a la firma y tras esta etapa de extracción se aplican técnicas de medida de distancias entre los vectores extraídos. Como conjunto de características en este proyecto se evalúan tres: características GRANDMA [6], conjunto de 100 características y selección de 40 características. En cuanto a las técnicas de medida de similitud entre los vectores, se utilizará la distancia Euclídea y la distancia de Mahalanobis.

El primer vector de características globales (GRANDMA) está constituido por 12 parámetros que se extraen de cada media firma y password gráfico. Estos 12 valores utilizados previamente en reconocimiento de trazos [6] se han adaptado al objeto de este estudio. Previamente se han definido las muestras capturadas, media firma y password gráficos como *doodles* cuya apariencia consta de varios trazos y por ello que se haya propuesto este conjunto de características.

En la figura 6.2 se presenta de forma geométrica el conjunto de los **12 parámetros GRANDMA** utilizados. El vector de características está constituido por el coseno (f_1) y el seno (f_2) del ángulo inicial del trazo, la diagonal (f_3) y el ángulo (f_4) del rectángulo que limita el password, la distancia entre el inicio y final del password (f_5), el coseno (f_6) y el seno (f_7) del ángulo que se forma entre el primer punto y el último, la longitud total del trazo (f_8), el sumatorio (f_9), el sumatorio del valor absoluto (f_{10}) y el sumatorio del cuadrado (f_{11}) del ángulo encerrado entre dos puntos y por último la duración del trazo (f_{12}).

Antes de obtener las características de cada muestra, debido a la metodología de adquisición y errores de captura que se producen en el dispositivo se hace una interpolación lineal entre todos aquellos valores cuyas coordenadas tienen un cero. También debido a la variación inherente en el punto inicial donde el usuario comienza a dibujar, es necesario realizar una normalización de coordenadas para que el centro de masa de las muestras tenga el mismo punto.



$$f_1 = \cos\alpha = (x_2 - x_0)/\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2}$$

$$f_2 = \sin\alpha = (y_2 - y_0)/\sqrt{(x_2 - x_0)^2 + (y_2 - y_0)^2}$$

$$f_3 = \sqrt{(x_{max} - x_{min})^2 + (y_{max} - y_{min})^2}$$

$$f_4 = arctan\frac{y_{max} - y_{min}}{x_{max} - x_{min}}$$

$$f_5 = \sqrt{(x_{p-1} - x_0)^2 + (y_{p-1} - y_0)^2}$$

$$f_6 = \cos\beta = (x_{p-1} - x_0)/f_5$$

$$f_7 = \sin\beta = (y_{p-1} - y_0)/f_5$$

Sea $\Delta x_p = x_{p+1} - x_p \quad \Delta y_p = y_{p+1} - y_p$

$$f_8 = \sum_{p=0}^{P-2}\sqrt{\Delta x_p^2 + \Delta y_p^2}$$

Sea $\theta_p = arctan\frac{\Delta x_p \Delta y_{p-1} - \Delta x_{p-1}\Delta y_p}{\Delta x_p \Delta x_{p-1} + \Delta y_p \Delta y_{p-1}}$

$$f_9 = \sum_{p=1}^{P-2}\theta_p$$

$$f_{10} = \sum_{p=1}^{P-2}|\theta_p|$$

$$f_{11} = \sum_{p=1}^{P-2}\theta_p^2$$

Sea $\Delta t_p = t_{p+1} - t_p$

$$f_{12} = t_{p-1} - t_0$$

Figura 6.1: Conjunto de características para identificar trazos [6].

Esta normalización se consigue de manera sencilla restando tanto al vector de coordenadas x como al de y su media. Aunque la pantalla del dispositivo no es grande se ha realizado una normalización de tamaño para evitar la posible variabilidad que puede ocasionar las diferentes dimensiones de muestras dibujadas.

Otro conjunto de características utilizadas en el sistema de verificación basado en parámetros globales considera 100 valores. Estas características han sido extraídas de [8] y se utilizan como una herramienta de comparación con las características GRANDMA. Este conjunto de propiedades globales de cada realización, se ha utilizado en trabajos relacionados con verificación de firma on line [39] y es una fusión ampliada de características generales para firma manuscrita que provienen de diferentes trabajos [32, 33, 34]. Los **100 parámetros** se pueden clasificar en cuatro categorías:

- **Tiempo** (25 parámetros) relacionados con la duración o características que se obtienen teniendo en cuenta el tiempo que dura la realización.
- **Velocidad y aceleración** (25 parámetros) tales como las primeras y segundas derivadas de la posición, la velocidad media o máxima velocidad del trazo.
- **Dirección** (18 parámetros), características extraídas de la trayectoria de la muestra como la dirección inicial o direcciones medias entre trazos (*pen-ups*).
- **Geometría** (32 parámetros), asociados a los trazos u orientación de la firma.

Por último, se ha utilizado un **set de 40 parámetros** que corresponde con los cuarenta primeros valores de la tabla 6.1. Este subconjunto de características se corresponden con los que presentan una mayor distancia inter-usuario para firma on-line en [8].

Las técnicas de medida de similitud entre los vectores de características que se han utilizado para evaluar el sistema son: la distancia de Mahalanobis y Euclídea. El cálculo de estas distancias es sencillo y rápido computacionalmente. Para el cálculo de la distancia Euclídea se crea

Tabla 6.1: Conjunto de características globales. Tabla extraída de [8]. T indica el intervalo de tiempo, t indica instantes de tiempo, N indica el número de eventos, and θ indica el ángulo. Otros símbolos utilizados son definidos previamente en la tabla (p.ej. En la característica 7 se utiliza Δ definida en 15)

#	Time related feature	#	Direction related feature
#	Speed and Acceleration related feature	#	Geometry related feature

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

Tabla 6.2: Conjunto f_2 de parámetros locales. Los puntos sobre las variables (p.ej. $\dot{x}_n$) indica la primera y segunda derivada respectivamente.

#	Parámetro	Descripción
1	x-coordinate	x_n
2	y-coordinate	y_n
3	Path velocity magnitude	$\upsilon_n = \sqrt{\dot{y}_n + \dot{x}_n}$
4	Log curvature radius	$\rho_n = \log(1/\kappa_n) = \log(\upsilon_n/\dot{\theta}_n)$, donde κ_n es la curvatura de la trayectoria
5-8	First-order derivative of features 1-4	$\dot{x}_n, \dot{y}_n, \dot{\upsilon}_n, \dot{\rho}_n$
9-10	Second-order derivative of features 1-2	$\ddot{x}_n, \ddot{y}_n$

previamente un modelo constituido por varias firmas genuinas del usuario y posteriormente se mide la distancia entre ambos vectores. Para determinar la similitud entre dos variables con la distancia de Mahalanobis se introduce la correlación entre ambas. De esta manera el modelo de usuario $C = (\boldsymbol{\mu}, \boldsymbol{\Sigma})$ se define a partir de un subconjunto de muestras genuinas del usuario a validar, donde $\boldsymbol{\mu}$ es la media y $\boldsymbol{\Sigma}$ es la matriz diagonal de covarianzas. La distancia entre la muestra $\mathbf{x}$ y el modelo C se calcula como:

$$d(\mathbf{x}, C) = \left((\mathbf{x} - \boldsymbol{\mu})^T (\boldsymbol{\Sigma})^{-1} (\mathbf{x} - \boldsymbol{\mu})\right)^{1/2}.$$

Por lo tanto, se tienen tres conjuntos de características globales, los 12 parámetros GRANDMA, los 100 valores utilizados para el reconocimiento en firma on line y por último un subconjunto de 40 parámetros que ha obtenido mejores resultados en reconocimiento basado en firma. Junto con ello para calcular la medida de similitud entre la muestra del usuario que reclama ser y el modelo almacenado en la etapa de registro, se utilizan dos distancias: Euclídea y Mahalanobis. Se tiene por tanto 6 combinaciones para evaluar el sistema de parámetros globales.

6.2. Sistema de verificación basado en parámetros locales

El sistema implementado en este proyecto está basado en el algorítmo DTW, utilizando dos vectores de características diferentes. En la etapa de extracción de características se han obtenido dos conjunto de funciones definidas en trabajos previos de sistemas de verificación basados en *doodles* y basados en firma on-line [40, 41]. Se reproducen ambos conjuntos con el objetivo de confrontar resultados y extraer conclusiones. Uno de ellos contiene funciones correspondientes a la posición y sus derivadas primera y segunda formando un vector de 6 características. El otro grupo de funciones está constituido por algunas de las anteriores y otras como la velocidad, aceleración y el logaritmo del radio de curvatura. Las señales (coordenadas de la media firma y el *passdoodle*) capturadas en el dispositivo móvil se digitalizan y se extraen un conjunto de funciones. El dato de entrada es un vector compuesto por las coordenadas del trazo dependientes del tiempo (x_t, y_t).

El primer conjunto que se denota como f_1 está constituido por 6 valores que corresponden a los vectores de posición y su respectivas primeras y segundas derivadas que tienen en cuenta la trayectoria, velocidad y aceleración de las muestras [41].

$$f_1 = [x_n, y_n, \dot{x}_n, \dot{y}_n, \ddot{x}_n, \ddot{y}_n] \tag{6.1}$$

Este conjunto fue propuesto para reconocimiento de passwords gráficos (utilizando caracteres tamil aislados) trazados sobre TabletPCs y PDAs. Con el propósito de comparar los resultados

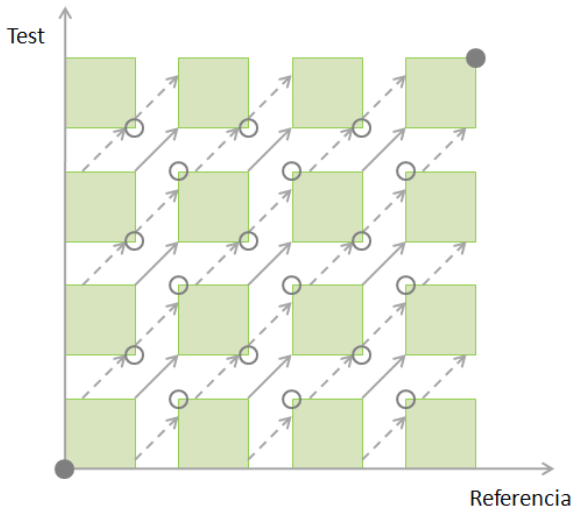


Figura 6.2: Esquema del DTW modificado en el que tanto la muestra de test como la de referencia tienen cuatro trazos. Se muestran los puntos que no se permite pasar al algoritmo para evitar múltiples alineamientos [7].

obtenidos con el conjunto de características propuesto en [40], se evalúa el sistema con otro vector de parámetros del estado del arte utilizado para reconocimiento de firma. Este conjunto de parámetros f_2 se presentó en BSEC 2009, en una evaluación de sistemas de verificación de firma manuscrita sobre tableta y PDA en la que participaban 9 universidades, y obtuvo excelentes resultados Biosecure [42]. Los resultados experimentales de este sistema, obtenidos por el set de características ajustado para *skilled forgeries* (falsificaciones entrenadas) utilizando el algoritmo DTW, alcanzaron posiciones destacadas con respecto a los demás participantes [42]. El conjunto está constituido por los 7 parámetros descritos en la tabla 6.2.

$$f_2 = [\ddot{y}_n, \dot{\rho}_n, \ddot{x}_n, \dot{y}_n, x_n, \dot{v}_n, v_n] \tag{6.2}$$

Para el cálculo de similitud entre los vectores de parámetros locales se han utilizado dos algoritmos, DTW básico y un DTW por trazos. Primero evaluamos el sistemas con el DTW básico [30] para el cálculo de la similitud entre la muestra introducida en el momento de la verificación y un conjunto de muestras de referencia de un usuario. Este algoritmo no tiene en cuenta la información de los trazos a la hora de calcular el camino de alineamiento y puede alinear muestras que pertenecen a diferentes trazos. Partiendo de esta idea, se ha implementado un DTW por trazos [7] en el que se penaliza el hecho de que se asocien muestras que pertenecen a diferentes trazos y se establece una serie de restricciones por donde se deben alinear los trazos. Se explican los pasos implementados:

- Paso 1. Se suma una penalización en la tabla de distancias, a aquellas muestras que no pertenecen al mismo trazo para evitar su alineación.
- Paso 2. la función de alineamiento debe cumplir unos límites locales. Se define ${s_{ref}}^i$ y ${e_{ref}}^i$ como el inicio y el fin del trazo i en la firma de referencia y ${s_{test}}^i$ y ${e_{test}}^i$ definen el inicio y fin de un trazo i de la muestra de test. En el proceso de alineamiento no se permiten los siguientes movimientos:
  - Los movimientos desde los puntos $({e_{ref}}^i, {e_{test}}^i)$,$({e_{ref}}^i, b)$,$(a, {e_{test}}^i)$ se permiten a los siguientes puntos $({s_{ref}}^{i+1}, {s_{test}}^{i+1})$,$({s_{ref}}^{i+1}, b+1)$,$(a+1, {s_{test}}^{i+1})$
  - No se permite que la función de alineamiento recorra los siguientes puntos, $({s_{ref}}^{i+1}, {e_{test}}^i)$ y $({e_{ref}}^i, {s_{test}}^{i+1})$

(a) (b) (c)

Figura 6.3: (a) Ejemplo de password en el que no se realiza interpolación alguna. (b) Ejemplo de interpolación para tiempos 50ms<t<100ms. c) Ejemplo de interpolación total para tiempos t>50ms, en el que se unen todos los trazos.

El hecho de crear una nueva matriz de distancias en la que se añade una penalización por pertenecer a diferentes trazos, propicia al algoritmo DTW a unir puntos pertenecientes al mismo trazo. El propósito de estas limitaciones es evitar múltiples saltos al inicio y final de los trazos.

6.3. Preprocesado para ambos sistemas

Antes de la extracción de características se adecuan las señales para su procesado. Tanto para parámetros globales como locales el paso de preprocesado consiste en una interpolación lineal de muestras erróneas capturadas por el dispositivo móvil. Estas muestras erróneas se identifican porque se guardan como 0's en el archivo de texto. También se realiza una normalización de coordenadas para centrarlas a una coordenada común y una normalización de tamaño. Además de este preprocesado imperativo que se realiza por cada muestra se han realizado tres tipos de interpolaciones para evaluar el sistema de verificación en diferentes entornos.

Tanto los passwords gráficos como las medias firmas están constituidas por dos tipos de trazos, aquellos en los que el instrumento de escritura (dedo) se encuentra sobre el dispositivo *pen-down* y otros en los que no está en contacto con la pantalla *pen-up*. Se ha estudiado el efecto de interpolación de esta información, es decir, se han introducido muestras entre los trazos y se ha calculado el rendimiento. Se considera que se levanta el dedo de la pantalla (pen-up) cuando el tiempo transcurrido entre la captura de muestras es mayor de 100 ms. Se puede observar un ejemplo de cada tipo de interpolación en la figura 6.3.

- Sin interpolación, lo que significa que hay saltos entre los momentos en los que el dedo está contacto con la pantalla (se dibuja) y en los que se levanta el dedo (pen-up). Por lo tanto hay información de los trazos.
- Interpolación para tiempos con una separación de entre 100 a 50 ms; se considera que los pen-ups se producen cuando el tiempo entre muestras es mayor de 100 ms, por lo que se intenta estudiar un escenario en el que se interpolarán las muestras erróneas en las que se hubieran producido errores de captura por parte del dispositivo y no se debiera a un levantamiento del dedo. Estos errores se producen en general cuando el usuario no realiza suficiente presión sobre la pantalla. En este caso por tanto se tiene en cuenta la información de los pen-ups intentando mitigar el efecto de pérdidas de muestras debidas a falsos levantamientos.
- Interpolación para periodos de muestreo mayores de 50 ms; en este caso se interpola linealmente la información de los pen-ups, lo que quiere decir que se introducen muestras ficticias entre los levantamientos creando finalmente una muestra constituida por un solo trazo.

En el caso de parámetros locales se ha realizado la normalización de las distancias en función de la variabilidad intra-usuario, calculándose para el efecto un valor de variabilidad (mínima y media) por cada usuario. La variabilidad se obtiene como la distancia media (o mínima) entre las muestras de usuario recogidas en la etapa de registro. Con este valor se calcula la distancia como el cociente entre la distancia que devuelve el algoritmo DTW y el valor de variabilidad de cada usuario.

6.4. Resumen de los sistemas descritos

A continuación se resumen los sistemas propuestos:

Preprocesado común de los datos erróneos calculados por el dispositivo de captura.

- **Parámetro globales**
  - Set parámetros GRANDMA (tabla 6.2).
  - Set de 100 parámetros (tabla 6.1).
  - Set de 40 parámetros.

  Para medir la similitud se utiliza la distancia euclídea y de mahalanobis.

- **Parámetro locales** (tabla 6.2)
  - Set de funciones f_1 (6.1).
  - Set de funciones f_2 (6.2)

  La similitud entre muestras se calcula con el DTW básico y el DTW propuesto con una penalización. También se tiene en cuenta la normalización de las distancias en función de la variabilidad intra-usuario mínima y media.

Estos conjuntos de características con sus respectivas medidas se estudian para los tres casos de interpolación entre muestras. Para ambos sistemas se han obtenido resultados en función de los diferentes grupos de características utilizadas. En el siguiente capítulo se describen los experimentos lanzados.

7

Experimentos y resultados

En este capítulo se describen los experimentos y resultados obtenidos de este trabajo. Durante el desarrollo del mismo, se definen y justifican los pasos seguidos en el proceso de evaluación de este nuevo sistema de verificación de usuarios basado en los dos conjuntos de passwords gráficos capturados, *doodles* y media firma. A continuación se explican de manera ordenada los rendimientos obtenidos en los escenarios de estudio vistos en el capítulo 6.

7.1. Protocolo experimental

Se ha definido el protocolo experimental en dos partes: primero experimentos de desarrollo y posteriormente experimentos de validación. En la etapa de desarrollo se utiliza un conjunto de 50 usuarios de los 100 de la base de datos y se evalúan los diferentes esquemas propuestos: sistema de parámetros globales y locales con diferentes configuraciones en cada caso. En la etapa de validación se utiliza el segundo grupo de 50 usuarios, en este caso sólo se evalúa el sistema con la configuración que ha ofrecido mejores resultados en la etapa de desarrollo. Esto se realiza para asegurar que los resultados obtenidos con el conjunto de desarrollo se reproducen en el conjunto de validación.

Se emplean 5 muestras genuinas de cada usuario para el entrenamiento de los modelos (o como conjunto de referencia), procedentes de la primera sesión. El cálculo de similitud entre muestras se realizará con el modelo del usuario y la muestra de test. Para cada escenario evaluado, se señala la configuración que ofrece mejores resultados atendiendo al rendimiento para falsificaciones entrenadas.

El rendimiento de los sistemas desarrollados se compara a través de la EER (*Equal Error Rate*) para falsificaciones entrenadas (*skilled forgeries*) y falsificaciones casuales (*random forgeries*). Se definen las falsificaciones entrenadas como aquellas cuyo falsificador ha tenido acceso a la reproducción de la muestra y ha podido practicar su realización. Las falsificaciones casuales consisten en que un usuario puede ser validado por casualidad como otro realizando su propia muestra. Para el cálculo de los *scores* (puntuación) genuinos se utilizan las 15 muestras genuinas de la segunda sesión (**SS2**) y para analizar el efecto de la variabilidad inter-sesión se utilizan las 10 genuinas restantes de la primera sesión (**SS1**). Para el cálculo de los *scores* de falsificaciones entrenadas, se utilizan todas las falsificaciones disponibles para cada usuario, que suman un total de 20. En último lugar, se calculan los *scores* de falsificaciones casuales, que se obtienen comparando una muestra del usuario genuino con el conjunto de firmas del resto de usuarios. Esto

Tabla 7.1: Rendimiento para los 3 conjuntos de características y las 2 distancias utilizadas.

Conjunto de características	**Distancia Euclídea**		**Distancia de Mahalanobis**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma, GRANDMA	14,6	35,0	16,2	27,7
Media firma, 100 parámetros	5,4	28,9	8,8	30,2
Media firma, 40 parámetros	6,6	29,0	**6.7**	**24.1**
Doodle, GRANDMA	12,8	38,3	18,8	29,7
Doodle, 100 parámetros	7,8	34,5	8,3	29,5
Doodle, 40 parámetros	8,6	34,8	**6.4**	**28.8**

Tabla 7.2: Rendimiento para el set de 40 parámetros con diferentes escenarios de interpolación.

Conjunto de características	**Distancia de Mahalanobis**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma, sin interpolar pen-ups	6,7	24,1
Media firma, interpolación 50ms<t<100ms	**6**	23,1
Media firma, interpolación t>50ms	7,3	**22.8**
Doodle, sin interpolar pen-ups	6,4	**28.8**
Doodle, interpolación 50ms<t<100ms	7,0	29,0
Doodle, interpolación t>50ms	**5.0**	29,7

proporciona información sobre la probabilidad de que un usuario realizando su propio password pudiera acceder al sistema como si fuera otro.

7.2. Experimentos

7.2.1. Parámetros globales

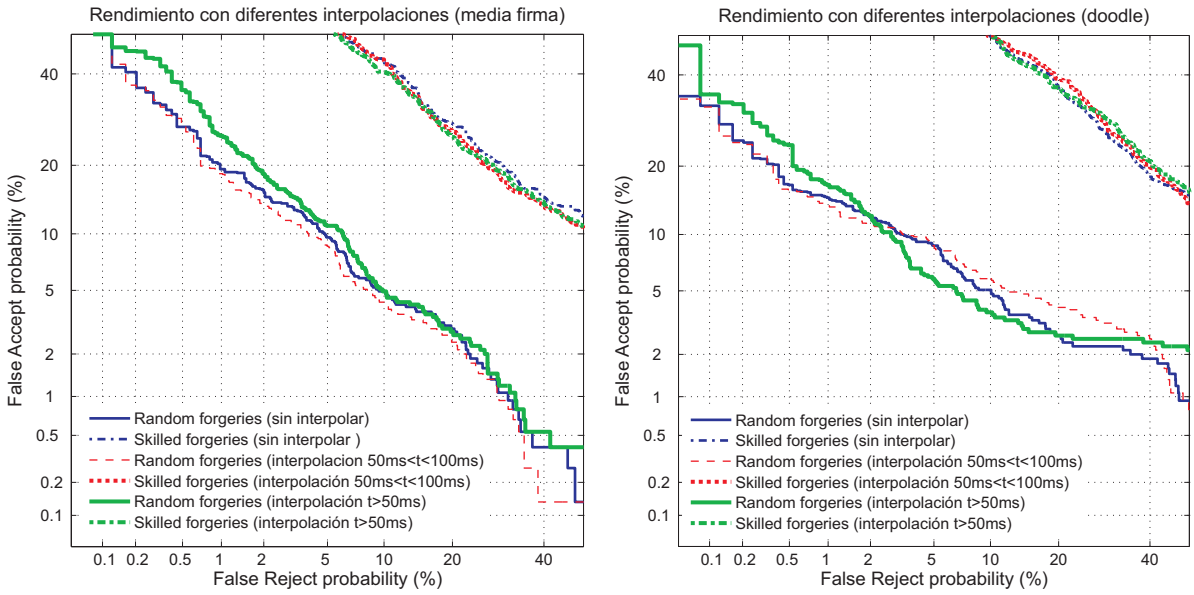
Para analizar el rendimiento del sistema de verificación utilizando parámetros globales se han lanzado diferentes experimentos. Estos se dividen según los grupos de características utilizados: parámetros GRANDMA, set de 100 parámetros y set de 40 parámetros. Los resultados se presentan en forma de curvas DET y se muestran los valores de la EER (*Equal Error Rate*) para falsificaciones entrenadas (*skilled forgeries*) y falsificaciones aleatorias (*random forgeries*).

En primer lugar se presentan los valores de rendimiento obtenidos con los tres vectores de características globales calculando la similitud entre muestras mediante las dos distancias utilizadas, Euclídea y Mahalanobis (véase tabla 7.1). Como se puede observar, para ambos casos el cálculo de la similitud con la distancia de Mahalanobis es mejor para falsificaciones entrenadas pero no ocurre lo mismo para falsificaciones aleatorias. También se observa que en general las medias firmas presentan mejor rendimiento que los *doodles* para los diferentes conjuntos de parámetro globales. Por lo tanto el sistema óptimo, dentro de los considerados, para esta clasificación sería el constituido por el conjunto de 40 parámetros globales cuya similitud se calcula mediante la distancia de Mahalanobis, debido a que proporciona un mejor rendimiento para falsificaciones entrenadas.

En segundo lugar, una vez seleccionada la distancia de Mahalanobis como mejor método de cálculo de similitud entre las muestras y el conjunto de 40 características, se presentan los valores obtenidos según el efecto de la interpolación. Se ha estudiado el efecto de tres preprocesados diferentes añadidos al básico (que consistía en la interpolación lineal de muestras erróneas capturadas por el dispositivo móvil), realizando una interpolación lineal de los *pen-ups* con tres criterios diferentes. En principio se propuso una interpolación total de los *pen ups* (tiempo entre

Tabla 7.3: Rendimiento del sistema final para parámetros globales.

Escenario	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma	7,3	22,8
Doodle	6,4	28,8



(a) (b)

Figura 7.1: (a) Efecto de la interpolación de pen-ups para media firma. (b) Efecto de la interpolación de pen-ups para *doodle*.

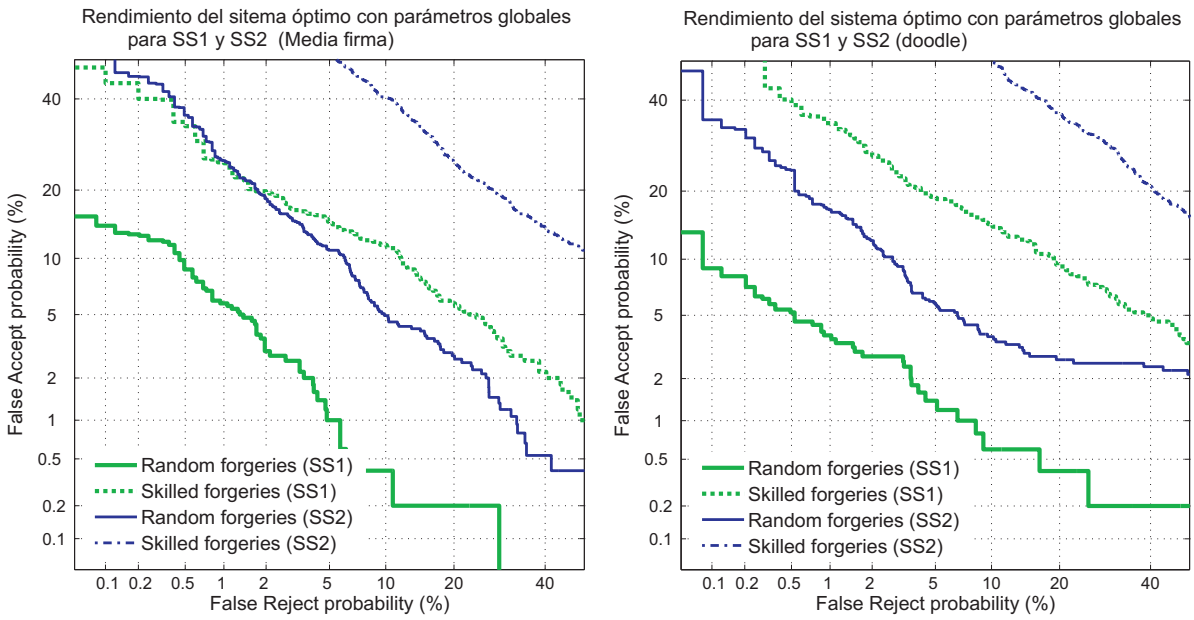
muestras $t > 50$ ms) como se ha realizado en estudios de firma on-line, perdiendo información de los trazos. Posteriormente se ha propuesto una interpolación de las muestras no capturadas por falta de precisión del dispositivo móvil, interpolando para tiempos entre muestras de 100 ms a 50 ms. Y el último caso es cuando no se realiza interpolación alguna.

De la tabla 7.2 se puede concluir que para media firma, el rendimiento para falsificaciones entrenadas (*skilled forgeries*) mejoran con la interpolación de las muestras. Comienza con una pequeña mejora para la interpolación de 50 ms $< t <$ 100 ms y mejora un poco más aún con la interpolación total de los pen-ups ($t > 50$ ms). Sin embargo esta compensación del rendimiento de *skilled forgeries* con la interpolación no se produce para *random forgeries*. En el caso de los *doodles* el efecto es justo el contrario, realizar una interpolación de los pen-ups empeora el rendimiento de falsificaciones entrenadas mientras que mejoran las falsificaciones casuales. Esto nos muestra que al menos para parámetros globales la información que introducen los *pen-ups* en los *doodles* es importante. El rendimiento del sistema para los diferentes métodos de interpolación se representan en la figura 7.1.

Finalmente la configuración óptima del sistema basado en parámetros globales para los dos conjuntos de estudio son:

- Media firma: Interpolación total de los pen-ups, utilizando el set 40 parámetros globales y distancia de Mahalanobis para el cálculo de similitud.
- Doodle: Sin interpolación de los pen-ups, utilizando el set 40 parámetros globales y distancia de Mahalanobis para el cálculo de similitud.

En la tabla 7.3 se expone el rendimiento de la configuración final.



(a) (b)

Figura 7.2: (a) Efecto de la variabilidad temporal para firma. (b) Efecto de la variabilidad temporal para passdoodle .

Tabla 7.4: Rendimiento del sistema de parámetros globales, utilizando las muestras de la SS1 y SS2 respectivamente. Representa la variabilidad inter-sesión.

Conjunto	**Primera sesión (SS1)**		**Segunda sesión (SS2)**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma	2,6	11,0	7,3	22,8
Doodle	2,2	12,9	6,4	28,8

Utilizando esta configuración final clasificada como óptima dentro de los diferentes experimentos lanzados, se comprueba el rendimiento del sistema utilizando las muestras genuinas de la primera sesión (SS1). Posteriormente se comparan los rendimientos de la SS1 y SS2 para estudiar el efecto de la variabilidad inter-sesión. Así los valores del rendimiento en SS1 presentan una mejora para falsificaciones entrenadas alrededor de un 50 % para ambos escenarios con respecto a los rendimientos obtenidos con el escenario de desarrollo (SS2). En la primera sesión las muestras de test pertenecen al mismo conjunto que las muestras que forman el modelo por lo que hay menos variabilidad entre ellas, por el contrario, las muestras de una segunda sesión presentan una distancia mayor. En general, son más representativos los resultados pertenecientes a la sesión 2, ya que la primera sesión coincidiría con el momento de registrarse en el sistema y la segunda sesión correspondería con la verificación entre la muestra realizada y el modelo almacenado previamente. En la figura 7.2 se representa el rendimiento de la SS1 y SS2 en el que se aprecia el efecto de la variabilidad inter-sesión, es decir, el efecto temporal produce un empeoramiento en el rendimiento del sistema (véase tabla 7.4).

Estos son los diferentes resultados obtenidos de las pruebas realizadas con las diferentes configuraciones propuestas para el caso de parámetros globales. Aunque las variaciones entre sistemas son pequeñas se elige la mejor configuración atendiendo al rendimiento para falsificaciones entrenadas.

Tabla 7.5: Rendimiento para los dos set de características (f_1 y f_2) con las diferentes configuraciones de normalización.

Características	N. con mínimo		N. con media		Sin normalización	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
f_1 Media firma	8,8	23,8	11,6	23,5	4,3	27
f_2 Media firma	9,6	23,5	14,1	**22.7**	4,9	26,1
f_1 Doodle	13	33,2	15,9	33,8	7,2	38,9
f_2 Doodle	14,7	**32.9**	16,1	33	7,6	38,8

7.2.2. Parámetros locales

En el estudio del sistema de verificación basado en parámetros locales se utiliza una secuencia de experimentos similar a la seguida para globales. En primer lugar se estudia el rendimiento de los dos conjuntos de características utilizados $f_1 = [x_n, y_n, \dot{x}_n, \dot{y}_n, \ddot{x}_n, \ddot{y}_n]$ y $f_2 = [\ddot{y}_n, \dot{\rho}_n, \ddot{x}_n, \dot{y}_n, x_n, \dot{\upsilon}_n, \upsilon_n]$. Una vez evaluados, se llevan a cabo tres tipos de interpolación con el conjunto que ofrece mejores resultados y por último se evalúa el efecto de la variabilidad inter-sesión en este caso. Para medir la similitud entre las muestras se utiliza el DTW clásico y una modificación de éste a la que se añade una penalización, DTW con penalización.

DTW clásico

En la tabla 7.5 se muestran los resultados de las diferentes configuraciones utilizando el DTW como algoritmo de medida. En primer lugar se muestran los rendimientos para los dos conjuntos de características que se han utilizado: f_1 y f_2. En el caso de parámetros locales se ha tenido en cuenta la variabilidad intra-usuario por lo que se han normalizado las distancias con la media y el mínimo. Esto genera un total de 12 configuraciones entre las que se elige la que presenta mejor rendimiento.

El sistema presenta mejor rendimiento para el conjunto de características f_2 tanto en el caso de la media firma como para los *doodles*, aunque la mejora es prácticamente despreciable. Como ocurría en parámetros globales la mejora producida para falsificaciones entrenadas no está acompañada de una mejora en falsificaciones casuales. A partir de ahora todos los datos presentados son con el conjunto de características f_2 que se selecciona como óptimo sobre este conjunto de valores obtenidos. En el siguiente paso se analiza el efecto de la interpolación de los *pen-ups*.

En la tabla 7.6 se puede observar cómo la interpolación primero de los falsos *pen-ups* (muestras separadas por un tiempo $50ms < t < 100ms$), así como la interpolación total de la información de los *pen-ups* (muestras separadas por un tiempo $t > 50ms$) introduce una pequeña mejora. Por ello en ambos casos la interpolación total de los *pen-ups* es el caso mejor de los tres ensayos. Sin embargo la normalización que presenta mejores resultados varía de *doodles* a media firma, aunque la diferencia es pequeña. Estos resultados pertenecen a los experimentos lanzados para el caso de SS2, es decir, con variabilidad inter-sesión, en el que se calcula la similitud entre el modelo de usuario y las 15 realizaciones genuinas de la segunda sesión, utilizándose para el cálculo de analogía el DTW clásico. Finalmente, teniendo en cuenta todos los rendimientos de las diferentes configuraciones implementadas, se elige como configuración óptima:

- Media firma: Interpolación total de los pen-ups, utilizando el set f_2 y utilizando el mínimo para normalización inter-usuario.

Tabla 7.6: Rendimiento con las diferentes configuraciones de normalización añadiendo una interpolación diferente en cada caso. Todos los valores se obtienen utilizando el conjunto de características f_2.

Características	**N. con mínimo**		**N. con media**		**Sin normalización**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma, sin interpolar	9,6	23,5	14,1	23	4,9	26,1
Media firma, interpolación 50ms<t<100ms	4,8	22,4	11,4	22,7	4,7	24,6
Media firma, interpolación t>50ms	8,4	**19.0**	10,0	21,4	3,7	24,8
Doodle, sin interpolar	14,7	32,9	16,1	33,0	14,7	38,8
Doodle, interpolación 50ms<t<100ms	14,2	32,1	14,4	32,7	7,6	38,7
Doodle, interpolación t>50ms	14,9	28,4	15,5	**27.8**	6,5	35,5

Tabla 7.7: Rendimiento del sistema final para parámetros locales utilizando el DTW clásico.

Escenario	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma	8,4	19
Doodle	15,5	27,8

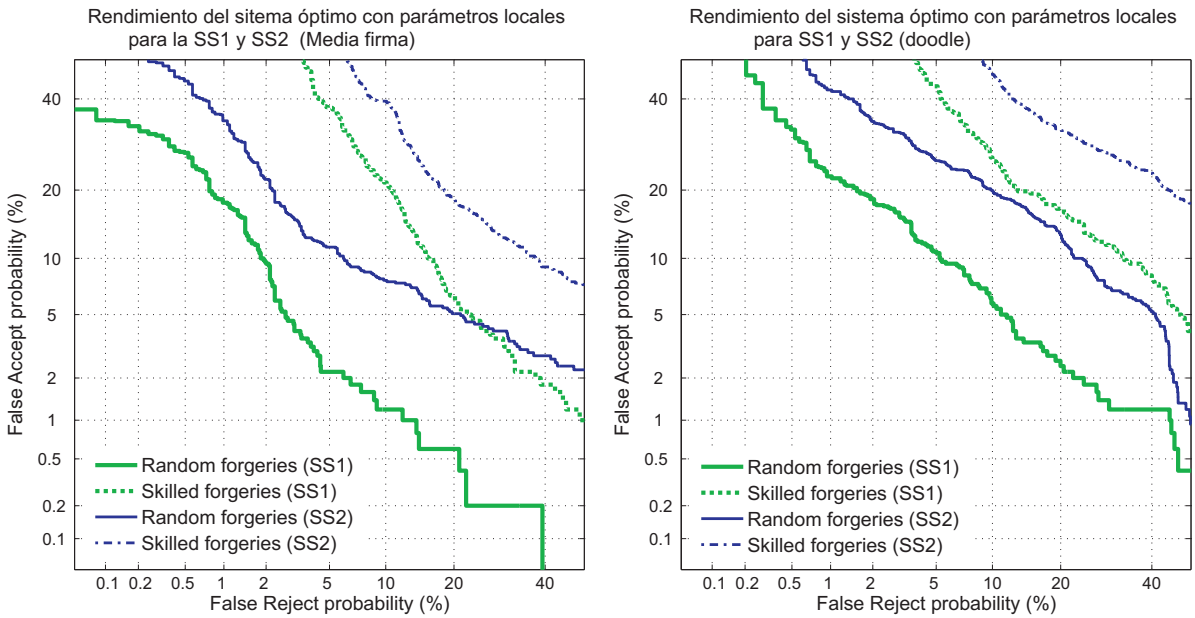
- Doodle: Interpolación total de los pen-ups, utilizando el set f_2 y utilizando la media para normalización inter-usuario.

Los valores de este clasificación final están representados en la tabla 7.7.

También para el sistema basado en parámetros locales se estudia el efecto que produce la captura de muestras espaciadas en el tiempo (variabilidad inter-sesión). Los resultados quedan representados en la figura 7.3 para la que se han utilizado los valores adquiridos con la configuración óptima tanto para medias firmas como para los *doodles* en la SS1 y SS2. Como cabía esperar, el rendimiento para las muestras de la SS1 es notablemente mejor que para la SS2 como puede verse en la tabla 7.8.

DTW con penalización

A continuación se muestran los valores obtenidos cuando el algoritmo de cálculo de similitud es el DTW modificado en el que se tiene en cuenta una penalización en caso de que se alineen muestras que pertenecen a distinto trazo. En este caso se realizan dos configuraciones en cuanto a



(a) (b)

Figura 7.3: (a) Efecto de la variabilidad temporal para firma utilizando el DTW convencional. (b) Efecto de la variabilidad temporal para los doodles utilizando el DTW convencional.

Tabla 7.8: Rendimiento del sistema de parámetros locales, utilizando las muestras de la SS1 y SS2 respectivamente. Representa la variabilidad inter-sesión.

Conjunto	**Primera sesión (SS1)**		**Segunda sesión(SS2)**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma	3,6	13,4	8,4	19,0
Doodle	7,6	17,5	15,5	27,8

interpolación de pen-ups: sin interpolación y interpolación de muestras con $50ms < t < 100ms$. Se elimina de este caso la interpolación de tiempos $t > 50ms$ ya que con esta lo que hacemos es unir todos los trazos, generando uno único. Sin la información del número de trazos el DTW que se utiliza para evaluar el sistema no tendría el efecto de la penalización y se obtendrían los mismos resultados que en el caso del DTW convencional.

Como se puede observar de los valores representados en la tabla 7.9, el DTW con penalización no parece introducir mejora alguna en el rendimiento del sistema. Comparándola con la tabla 7.5 se aprecia que los rendimientos empeoran ligeramente con el uso de este algoritmo. Para el caso de *doodles* el sistema óptimo utilizando este algoritmo, es decir, el que presenta mejor rendimiento para falsificaciones entrenadas, es el set de características f_1 con normalización de distancias utilizando el mínimo, mientras que para medias firmas el conjunto de funciones locales que ofrece mejores resultados es el f_2 con la media para normalizar. Aunque los experimentos utilizando este algoritmo empeoren los resultados, se presentan los rendimientos teniendo en cuenta la interpolación. De la tabla 7.10 se aprecia que para los *doodles* el efecto de la interpolación parcial 50 ms$< t <$ 100 ms empeora el rendimiento mientras que para media firma el rendimiento mejora con ese mismo preprocesado. Para el caso de media firma se produce una pequeña mejora en el caso de interpolar y normalización con el mínimo. Para *doodles* el mejor rendimiento se mantiene sin la interpolación y normalización con el mínimo.

Se muestra en la figura 7.4 el rendimiento de los dos sistemas óptimos para el caso de DTW básico y la versión de éste modificado, con curvas DET tanto para media firma como para doodle. Se observa que en el caso de la media firma tanto el rendimiento de falsificaciones aleatorias como entrenadas no mejoran con el uso del DTW con penalización, mientras que para los *doodles* este

Tabla 7.9: Rendimiento para los dos set de características (f_1 y f_2) con las diferentes configuraciones de normalización utilizando el DTW por trazos.

Características	**N. con mínimo**		**N. con media**		**Sin normalización**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
f_1 Media firma	9,4	24,9	10,7	25,1	6	29,2
f_2 Media firma	11,0	25,2	12,2	**24.1**	8,2	28,7
f_1 Doodle	14,0	**33.8**	16,9	34,6	6,4	42,2
f_2 Doodle	14,4	34,6	15,7	34,5	7,0	42,5

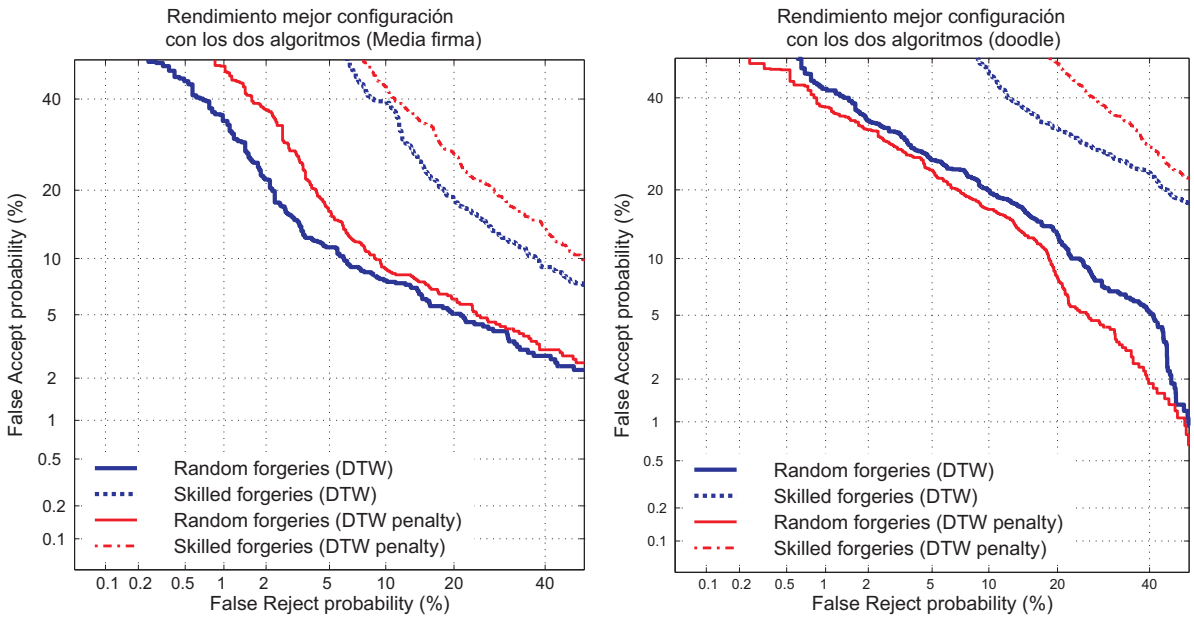
Tabla 7.10: Rendimiento con las diferentes configuraciones de normalización añadiendo los dos tipos de interpolación, para el mejor conjunto de características, f_2, utilizando el DTW por trazos.

Características	**N. con mínimo**		**N. con media**		**Sin normalización**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma, sin interpolar	11,0	25,2	12,2	24,1	8,2	28,7
Media firma, interpolación 50ms<t<100ms	10,5	**23.6**	11,6	23,9	8,4	28,7
Doodle, sin interpolar	14,0	**33.8**	16,9	34,6	6,4	42,2
Doodle, interpolación 50ms<t<100ms	14,1	34,6	17,6	34,6	5,9	41,5

algoritmo produce mejora en el caso de falsificaciones aleatorias. Se selecciona como sistema óptimo el que posee mejor rendimiento para falsificaciones entrenadas por lo tanto el algoritmo establecido es el DTW clásico.

Análisis individual de parámetros locales

Con el objetivo de extraer conclusiones de los dos escenarios bajo estudio, se han lanzado pruebas utilizando el conjunto de características f_1 por pares. Esto puede dar ideas de qué caracteriza mejor a cada conjunto de muestras y sacar conclusiones en función de los rendimientos mostrados anteriormente. De los resultados mostrados en la tabla 7.11 se observa que para media firma es más característica la aceleración, cuyo conjunto formado por $[\ddot{x}_n, \ddot{y}_n]$ presenta para falsificaciones entrenadas un valor menor. En el caso de passdoodle es la velocidad, $[\dot{x}_n, \dot{y}_n]$, la que mejor le caracteriza aunque la diferencia entre los 3 conjuntos no es tan significativa como en el caso de la media firma. Con esto queda reflejado que hay diferencias considerables dentro de los *doodles* de un mismo usuario, mientras que las medias-firmas, al ser movimientos en general aprendidos presentan características dinámicas más estables.



(a) (b)

Figura 7.4: (a) Comparación del rendimiento para el sistema óptimo de media firma usando DTW y DTW por trazos (DTW penalty). (b) Comparación del rendimiento para el sistema óptimo de doodle usando DTW y DTW por trazos (DTW penalty).

Tabla 7.11: Configuración básica del DTW utilizando las características f_1 por pares.

Escenario básico por pares	**Media firma**		**Doodle**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
$[x_n, y_n]$	5,31	34,4	11,5	38,5
$[\dot{x}_n, \dot{y}_n]$	5,9	28,0	9,8	35,8
$[\ddot{x}_n, \ddot{y}_n]$	5,5	22,5	10,0	36,2

7.3. Validación de los resultados experimentales

Los resultados experimentales expuestos en las secciones 7.2.1 y 7.2.2 del presente capítulo han sido obtenidos con un conjunto de prueba constituido por los 50 primeros usuarios de la base de datos. Con el objetivo de validar los conjuntos óptimos elegidos tanto de parámetros globales como locales, se calculan los rendimientos del sistema de verificación para los 50 usuarios restantes. Los sistemas óptimos obtenidos son los siguientes:

- **Globales**
  - Media firma, conjunto formado por 40 características, interpolando los pen-ups y utilizando distancia de Mahalanobis.
  - Doodle conjunto formado por 40 características, sin interpolar los pen-ups y utilizando distancia de Mahalanobis.
- **Locales**
  - Media firma, conjunto de características f_2, con interpolación de pen-ups y utilizando el DTW básico con variabilidad inter-usuario mínima.
  - Doodle conjunto de características f_2, con interpolación de pen-ups y utilizando el DTW básico con variabilidad inter-usuario media.

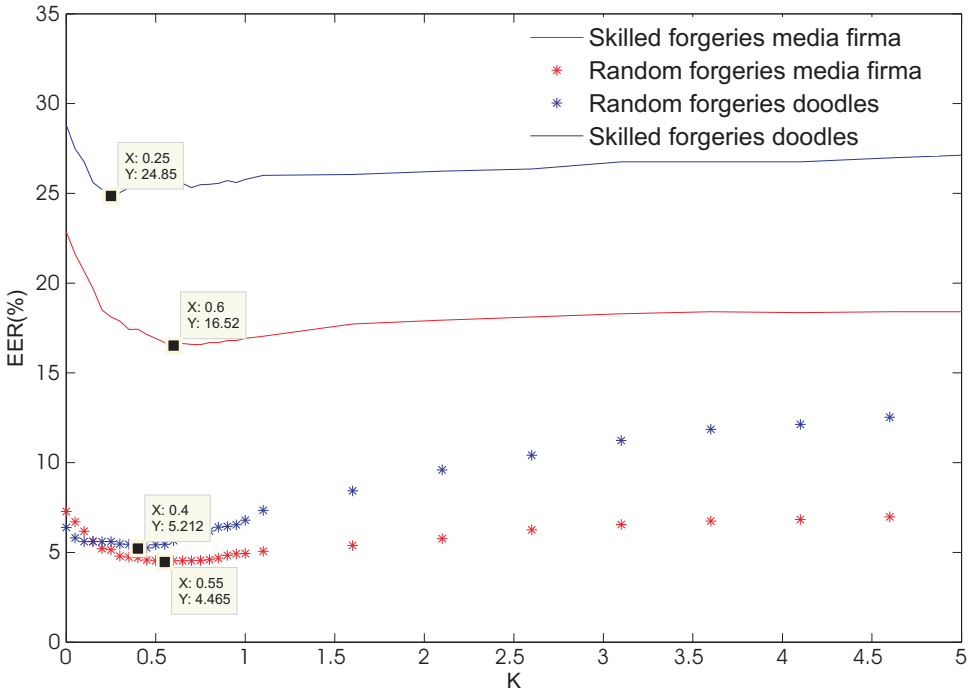


Figura 7.5: Figura de evolución del rendimiento del sistema de verificación para los diferentes valores de k.

Tabla 7.12: Comparación de rendimiento entre el conjunto de desarrollo y el conjunto de validación.

Escenario	**Conjunto desarrollo**		**Conjunto validación**	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media firma (globales)	7,3	22,8	8,9	25,3
Media firma (locales)	8,4	19	9,7	22,2
Doodle (globales)	6,4	28,8	4,1	25,8
Doodle (locales)	15,5	27,8	9,6	24,6

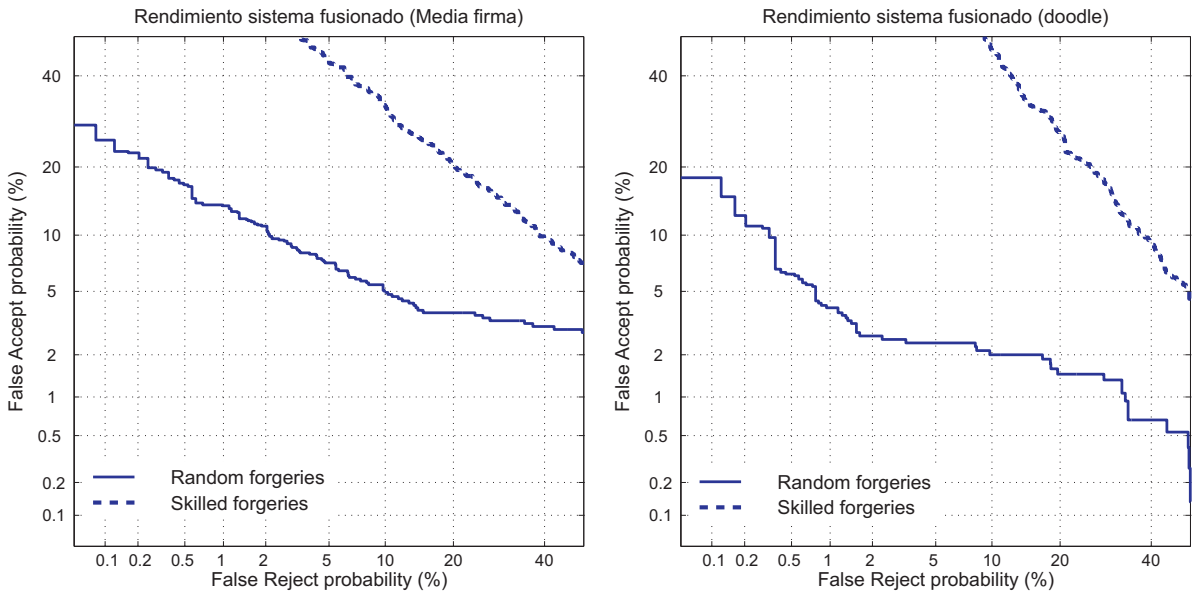
En la tabla 7.12 se representan los rendimientos obtenidos tanto para el conjunto de desarrollo como para el de validación con las configuraciones óptimas estudiadas para el sistema basado en parámetros globales y el sistema basado en parámetros locales. Para obtener los resultados finales de rendimiento del sistema con el conjunto de validación se realiza la fusión de *scores* de los parámetros globales y locales.

7.4. Fusión de los sistemas basados en parámetros globales y locales

Para la fusión de los resultados del sistema global y local se realiza una suma ponderada de los scores de ambos sistemas [43]. Se realiza la fusión en base a minimizar la ERR para falsificaciones entrenadas. La fusión de *scores* s_f se obtiene como

$$s_f = s_g + k \cdot s_l$$

donde s_g corresponde a los *scores* obtenidos de los parámetros globales y s_l son los *scores* de parámetros locales ambos pertenecientes al sistema óptimo. En la figura 7.5 se representa la evolución de la EER en función de K para el conjunto de desarrollo (formado por los 50 primeros usuarios), es decir, el rendimiento varía según se le de más peso a parámetros globales o a parámetros locales. Se observa que para los dos escenarios de estudio, media firma y *doodles*



(a) (b)

Figura 7.6: Rendimiento para el conjunto de validación con firma (a) y con doodle (b).

Tabla 7.13: Sistema de validación de los resultados experimentales con el conjunto de 50 usuarios restantes (conjunto de test) utilizando fusión de scores.

Escenario óptimo	$EER_{rd}(\%)$	$EER_{sk}(\%)$
Media Firma	5,8	20
Doodle	2,5	22,2

el valor de k está comprendido entre 0 y 1. Por lo tanto aproximamos su valor a una k igual a 0,4. Una vez elegido este valor de k en función del mejor rendimiento para falsificaciones entrenadas se comprueban los resultados que se obtendrían con el conjunto de validación (formado por los 50 usuarios restantes). Los resultados finales de la fusión están representados en la tabla 7.13 y su representación mediante curvas DET corresponde a la figura 7.6.

El rendimiento final, ante falsificaciones entrenadas, de alrededor del 20 % de EER es prometedor, dada la calidad de las falsificaciones y la alta variabilidad inter-sesión.

8

Conclusiones y trabajo futuro

En este proyecto se estudian los passwords gráficos desde la perspectiva de un rasgo biométrico de comportamiento y se analizan qué resultados permiten alcanzar como método de autenticación de usuarios. Las dos vías implementadas para el estudio del sistema de verificación de usuarios (parámetros globales y locales) se han apoyado en el estado del arte de firma on-line, reproduciendo y adaptando las técnicas al nuevo escenario propuesto.

Se ha capturado una base de datos de passwords gráficos con dos modalidades: doodles y medias-firmas. Para estudiar el rendimiento de los sistemas desarrollados se han lanzado experimentos sistemáticos sobre la base de datos capturada.

Los resultados mostrados en el capítulo anterior corresponden a los dos sistemas desarrollados, sistema de verificación basado en parámetros globales y en parámetros locales. En ambos sistemas se han obtenido resultados utilizando distintos conjuntos de características; realizando un preprocesado/postprocesado diferente; introduciendo la interpolación de pen-ups para estudiar el impacto de esta sobre el rendimiento en los diferentes sistemas.

Finalmente se ha estudiado el rendimiento de un sistema que combina los anteriores basado en fusión de scores. En este capítulo final se presentan las conclusiones extraídas de este trabajo de investigación.

8.1. Conclusiones

En el capítulo 5 (captura de una base de datos) se realiza una comparación cualitativa entre los dos grupos de muestras capturados para este estudio (media firma y *doodles*) y un conjunto de muestras de firma on line. De estos histogramas es interesante observar que los ejemplares capturados para este estudio contienen menos información que las firmas reales. Los *passdoodles* contienen un número menor de muestras, de intersecciones y trazos, por lo que cabe suponer que su complejidad es en general menor que la firma. Al poseer menos información y ser las muestras más sencillas en general se deduce que puede producirse un peor rendimiento tanto en media firma como en los *doodles* con respecto a las firmas reales. Se ha observado en los experimentos, que el rendimiento de los sistemas de verificación es en general peor para *doodles* que para media firma. Esto puede ser debido a que no son movimientos aprendidos.

El peor rendimiento de los *doodles* frente a media firma se puede deber a la mayor simplicidad y peor ejecución de los trazos, de hecho, se ha observado que la velocidad media para *doodles*

era menor que para firma y media firma lo que puede confirmar que estos no son movimientos aprendidos y por ello que el rendimiento sea peor.

Se ha observado que en el caso de media firma, el llevar a cabo una interpolación de los pen-ups mejora el rendimiento en falsificaciones entrenadas no ocurriendo lo mismo en el caso de los *doodles*. Este hecho sugiere que la adaptación de los sistemas basados en firma a *passdoodle* no es totalmente inmediata, puesto que en este caso el tener información de los trazos parece que mejora los resultados con parámetros globales.

Para el sistema de parámetros locales la interpolación total de los pen-ups es satisfactoria en ambos casos para mejorar parcialmente el rendimiento. De los valores presentados en las tablas se deduce que compensar la variabilidad intra-usuario mediante normalización de scores mejora el rendimiento en falsificaciones entrenadas pero no en aleatorias. Además el algoritmo basado en el DTW que trata de dar más importancia al número de trazos, no muestra mejoras con respecto al DTW clásico. El hecho de que para parámetros locales el rendimiento con interpolación mejore puede deberse a que la interpolación total añade más uniformidad a las muestras debido a que la realización de las mismas presenta una alta variación por no ser movimientos totalmente aprendidos.

Estos resultados muestran que la adaptación de los sistemas basados en firma a *passdoodle* no es directa y que orientar a trazos el sistema no parece una solución correcta ya que la variante propuesta, DTW por trazos, no ha ofrecido resultados mejores. Esto se puede deber a que el dispositivo presenta saltos entre capturas que no constituyen un levantamiento (pen-up) sino un error, aunque se ha intentado mitigar este efecto con la interpolación parcial (entre 50 ms y 100 ms). También el hecho de utilizar como dispositivo de escritura el dedo puede ocasionar levantamientos erróneos y mayor variabilidad entre las muestras al no estar acostumbrados a utilizar este método de escritura. Actualmente muchos dispositivos móviles no proveen de estilete para manejarlos, lo que puede provocar que en un futuro próximo los usuarios estén más familiarizados con el uso del dedo para escribir y las muestras sean más precisas.

Del análisis individual de parámetros locales, los resultados muestran que para las muestras clasificadas como media firma el conjunto de parámetros que presentan rendimientos mejores son los relacionados con la aceleración. Sin embargo, para *doodles* los rendimientos para los tres pares de características (posición, velocidad y aceleración) no distan tanto entre ellos, concluyendo que la consistencia de su proceso de realización es baja. Estos resultados permiten reiterar la idea de que los *doodles* en general no son movimientos aprendidos como el caso de media firma y más aún firma on-line. Algunos usuarios tampoco estaban acostumbrados a realizar una media firma y por ello el rendimiento es peor que el que se pueda obtener para firma on-line. No obstante al tratarse de iniciales o rúbricas simplificadas de sus firmas originales presentarían una variabilidad menor y por ello el rendimiento es mejor que en el caso de los *doodles*.

Teniendo en cuenta todos los datos aportados y analizados, se puede concluir que las diferencias notables en el rendimiento se pueden deber al hecho de que variabilidad inter-sesión es diferente para movimientos aprendidos (media-firma) y movimientos no aprendidos (*doodles*). Funcionan mejor todos los escenarios experimentados para el caso de media firma que para *doodles*, lo que contribuye a pensar que no sólo la inexperiencia con el utensilio de escritura hace que la variabilidad sea alta, sino el hecho de que para la mayoría de los casos la realización del password era una novedad. Otro factor que puede haber afectado al rendimiento de los passwords gráficos (*passdoodles*) en general, es la sencillez de estos frente a firma on-line. La media firma es una versión simplificada de la firma y los *doodles* en algunos eran tanto sencillos de realizar como de recordar.

Los resultados obtenidos para el escenario de fusión de scores son prometedores. Una EER del 20 % frente a falsificaciones entrenadas posee margen de mejora, pero es un punto de partida razonable teniendo en cuenta la calidad de las falsificaciones y la simplicidad de los *doodles*.

8.2. Trabajo futuro

Como líneas de trabajo futuro se destaca la posibilidad de un estudio longitudinal o prospectivo de un conjunto menor de usuarios. Para ello se recogerían muestras menos espaciadas en el tiempo y con más continuidad para evaluar el sistema de nuevo cuando el usuario tiene más experiencia con el utensilio de escritura (en este caso su dedo) y el hecho de que la realización continuada del password puede convertirlo en un rasgo de conducta. Además se conseguiría un escenario más realista debido a que una contraseña se suele utilizar con mucha frecuencia.

Un estudio paralelo al anterior sería analizar si la repetición del *passdoodle* con su consecuente aprendizaje mejoraría el rendimiento. Una de las conclusiones derivada de los experimentos es que el peor rendimiento de los *passdoodles* frente a media firma puede deberse a que en muchos de los casos las muestras realizadas eran inventadas en el momento y por tanto la variabilidad temporal es muy alta en este caso. Estudiar por tanto si se mantiene constante esta variabilidad temporal a pesar de la repetición continuada del password.

En el desarrollo del sistema de identificación basado en parámetros globales, se ha utilizado un set de 100 parámetros y posteriormente un subconjunto de 40 parámetros que para firma on-line son aquellos que presentan mayor separación inter-usuario. Una linea que puede mejorar el rendimiento es comprobar para *doodles* el conjunto de características que presenta mayor distancia inter-usuario mediante técnicas de selección de características.

Cuando se analizaron los tipos de *doodles* realizados, se clasificaron subjetivamente en tres grupos, conceptual, abstracto y simbólico. Se puede pensar que estos tres grupos pueden presentar diferentes rendimientos, ya que es más fácil de recordar un password conceptual frente a uno abstracto de cara al falsificador entrenado. Se propone por tanto estudiar el rendimiento en función de los tres grupos definidos.

También se ha concluido que en algunos *doodles* las muestras eran demasiado sencillas, constituidas por trazos simples como rectas y círculos cuya falsificación ha sido sencilla de realizar. Se propone el estudio de técnicas que permitan identificar muestras sencillas y no dejara al usuario registrarse hasta conseguir una muestra con un determinado grado de dificultad.

Glosario

- **DET**: Detection Error Tradeoff, curvas cuasi lineales que enfrentan los porcentajes de Falsa Aceptación y Falso Rechazo de un sistema de verificación.
- **Doodle**: En el contexto del proyecto, boceto o dibujo realizado con el dedo sobre un dispositivo digitalizador.
- **DTW**: Dynamic Time Warping, algoritmo de medida de similitud entre muestras mediante técnicas de programación dinámica.
- **EER**: Error Equal Rate, punto en el que se iguala la tasa de falsa aceptación y la de falso rechazo de un sistema de verificación.
- **FAR**: False Acceptance Rate, es la tasa falsa aceptación, es decir, la tasa con la que un sistema acepta a impostores como usuarios genuinos.
- **FRR**: False Rejection Rate, es la tasa de falso rechazo, es decir, la tasa con la que un usuario genuino es rechazado por el sistema.
- **Media firma**: firma simplificada en la que se omite el nombre de pila.
- **Passdoodle**: técnica utilizada para verificación de usuarios que posee características de identificación del ámbito biométrico y del ámbito de las contraseñas. Consiste en la realización de un dibujo por parte del usuario.
- **Password gráfico**: medio de autenticación compuesto principalmente por imágenes, dibujos o elementos visuales.
- **Pen-up**: levantamiento del instrumento de caligrafía durante el proceso de escritura.
- **Random-forgery**: Falsificación aleatoria, es decir, aquella en la que un impostor trata de acceder a un sistema identificándose como un usuario diferente, pero presentando su propio rasgo biométrico sin intento de falsificar.
- **ROC**: Receiver Operating Curve. En el contexto del proyecto, curvas que enfrentan los porcentajes de Falsa Aceptación y Falso Rechazo de un sistema de verificación.
- **Skilled forgeries**: falsificaciones entrenadas, es decir, aquellas en las que el impostor trata de imitar el rasgo biométrico del usuario al que pretende suplantar.

Bibliografía

[1] L. Sobrado and J.-C. Birget. Graphical passwords. *An Electronic Bulletin for Undergraduate Research*, 4, 2002.

[2] H. Hoike T. Takada. Awase-e: Image-based authentication for mobile phones using user's favorites images. In *Mobile HCI*, 2003.

[3] F. Monrose M. K. Reiter I. Jeremyn, A. Mayer. The design and analysis of graphical passwords. In *SSYM'99: Proceedings of the 8th conference on USENIX Security Symposium*, 1999.

[4] E. Okamoto A. F. Syukri and M. Mambo. A user identification system using signature written with mouse. In *ACISP*, pages 403–4414, 1998.

[5] C. Varenhorst. Passdoodles; a ligthweigth authentication method. 2004.

[6] D. Rubine. Specifying gestures by example. *SIGGRAPH Comput. Graph.*, 25:329–337, 1991.

[7] W. Chang and J. Shin. Modified dynamic time warping for stroke-based on-line signature verification. In *ICDAR '07: Proceedings of the Ninth International Conference on Document Analysis and Recognition*, pages 724–728, Washington, DC, USA, 2007. IEEE Computer Society.

[8] J. Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia, and D. Maltoni. An on-line signature verification system based on fusion of local and global information. In *Proc. of IAPR Intl. Conf. on Audio- and Video-Based Biometric Person Authentication, AVBPA*, pages 523–532. Springer LNCS-3546, 2005.

[9] F. Alonso-Fernandez, J. Fierrez-Aguilar, F. del Valle, and J. Ortega-Garcia. On-line signature verification using Tablet PC. In *Proc. IEEE Intl. Symposium on Image and Signal Processing and Analysis, ISPA*, pages 245–250, Zagreb, Croatia, September 2005.

[10] *Graphical passwords: a survey*, 2005.

[11] J. Goldberg, J. Hagman, and V. Sazawal. Doodling our way to better authentication. In *CHI '02: CHI '02 extended abstracts on Human factors in computing systems*, pages 868–869, New York, NY, USA, 2002. ACM.

[12] D. V. Klein. "foiling the cracker" – A survey of, and improvements to, password security. In *Proceedings of the second USENIX Workshop on Security*, pages 5–14, Summer 1990.

[13] A. K. Jain, A. Ross, and S. Prabhakar. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*, 14(1):4–20, 2004.

[14] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar. *Handbook of fingerprint recognition.* Springer, 2003.

[15] F. Alonso-Fernandez V. Ruiz-Albacete, P. Tome-Gonzalez, J. Fierrez J. Galbally, and Ortega-García J. In *Proce. COST 2101 Workshop on Biometrics and Identity Management, BIOID, Roskilde, Denmark*, 2008.

[16] R. N. Shepard. Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6:156–163, 1967.

[17] D. Rachna and A. Perrig. Déjà vu: a user study using images for authentication. In *SSYM'00: Proceedings of the 9th conference on USENIX Security Symposium*, Berkeley, CA, USA, 2000. USENIX Association.

[18] L. Sobrado y J.-C. Birget. Graphical passwords. *The Rutgers Scholar, An Electronc Bulletin for Undergraduate Research*, 4, 2002.

[19] *A shoulder-surfing resistant graphical password schemes*, 2003.

[20] www.realuser.com, last accessed in November 2009.

[21] G. E. Blonder. Graphical passwords, 1996.

[22] www.passlogix.com, last accessed in November 2009.

[23] J. Hagman J. Goldberg and V. Sazawal. Doodling our way to better authentication. In *Conference on Human Factors in Computing Systems*, 2002.

[24] Mizuki Oka, Kazuhiko Kato, Yingqing Xu, Lin Liang, and Fang Wen. Scribble-a-secret: Similarity-based password authentication using sketches. In *ICPR*, pages 1–4, 2008.

[25] 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.

[26] R. Plamondon and G. Lorette. Automatic signature verification and writer identification: the state of the art. *Pattern Recognition*, 22(2):107–131, 1989.

[27] M. Martinez-Diaz, J. Fierrez, J. Galbally, and J. Ortega-Garcia. Towards mobile authentication using dynamic signature verification: useful features and performance evaluation. In *Proc. Intl. Conf. on Pattern Recognition, ICPR*, 2008.

[28] J.Ortega-Garcia, J.Fierrez, F.Alonso-Fernandez, J.Galbally, M.R.Freire, J.Gonzalez-Rodriguez, C.Garcia-Mateo, J.-L.Alba-Castro, E.Gonzalez-Agulla, E.Otero-Muras, S.Garcia-Salicetti, L.Allano, B.Ly-Van, B.Dorizzi, J.Kittler, T.Bourlai, N.Poh, F.Deravi, M.W.R.Ng, M.Fairhurst, J.Hennebert, A.Humm, M.Tistarelli, L.Brodo, J.Richiardi, A.Drygajlo, H.Ganster, F.M.Sukno, S.-K.Pavani, A.Frangi, L.Akarun, and A.Savran. The multi-scenario multi-environment biosecure multimodal database (bmdb). *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 2009.

[29] J. Ortega-Garcia J. Fierrez-Aguilar, D. Ramos-Castro and Joaquin Gonzalez-Rodriguez. HMM-based on-line signature verification: feature extraction and signature modeling. *Pattern Recognition Letters*, 28(16):2325–2334, 2007.

[30] H. Sakoe and S. Chiba. Dynamic programming algorithm optimization for spoken word recognition. *IEEE Trans. on Acoustics, Speech, and Signal Processing*, 26:43–49, 1978.

[31] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez, and J. Ortega-Garcia. An off-line signature verification system based on fusion of local and global information. In D. Maltoni and A. K. Jain, editors, *Proc. of Intl. Workshop on Biometric Authentication, BIOAW*, pages 295–306. Springer LNCS-3087, 2004.

[32] W. Nelson and E. Kishon. Use of dynamic features for signature verification. In *Proc. of IEEE Intl. Conf. on Systems, Man, and Cybernetics*, volume 1, pages 201–205, 1991.

[33] W. Nelson, W. Turin, and T. Hastie. Statistical methods for on-line signature verification. *Intl. Journal of Pattern Recognition and Artificial Intelligence*, 8(3):749–770, 1994.

[34] L. L. Lee, T. Berger, and E. Aviczer. Reliable on-line human signature verification systems. *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 18(6):643–647, 1996.

[35] M. Yasuhara and M. Oka. Signature verification experiment based on nonlinear time alignment: a feasibility study. *IEEE Trans. on Systems, Man and Cybernetics, part C*, 12(3):212–216, 1977.

[36] L. R. Rabiner. A tutorial on Hidden Markov Models and selected applications in speech recognition. *Proceedings of the IEEE*, 77(2):257–286, 1989.

[37] J. G. A. Dolfing, E. H. L. Aarts, and J. J. G. M. van Oosterhout. On-line signature verification with Hidden Markov Models. In *Proc. of the Intl. Conf. on Pattern Recognition, ICPR*, pages 1309–1312. IEEE CS Press, 1998.

[38] Biosecure Network of Excellence. Biosecure multimodal database. (http://www.biosecure.info), 2007.

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

[40] N. S. Govindarajulu and S. Madhvanath. Doodles for authentication: recognition and user study results. Technical report, HP Laboratories, India, 2008.

[41] A. Toselli M. Pastor and E. Vidal. Writing speed normalization for on-line handwritten text recognition. In *ICDAR '05: Proceedings of the Eighth International Conference on Document Analysis and Recognition*, pages 1131–1135, Washington, DC, USA, 2005. IEEE Computer Society.

[42] A. Mayoue and N. Houmani, S. García-Salicetti. Biosecure signature evaluation campaign 2009 (bsec'2009): Results. Technical report, 2009.

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

Presupuesto

1) **Ejecución Material**

▪ Compra de ordenador personal (Software incluido)	800 €
▪ Compra dispositivo móvil para captura de la base de datos	700 €
▪ Material de oficina	100 €
▪ Total de ejecución material	1.600 €

2) **Gastos generales**

▪ sobre Ejecución Material	352 €

3) **Beneficio Industrial**

▪ sobre Ejecución Material	132 €

4) **Honorarios Proyecto**

▪ 1800 horas a 7 €/ hora	12600 €

5) **Material fungible**

▪ Gastos de impresión	280 €
▪ Encuadernación	200 €

6) **Subtotal del presupuesto**

▪ Subtotal Presupuesto	15.164 €

7) **I.V.A. aplicable**

▪ 16 % Subtotal Presupuesto	2.426,24 €

8) **Total presupuesto**

▪ Total Presupuesto	17.590,24 €

Madrid, Febrero 2010

El Ingeniero Jefe de Proyecto

Fdo.: Cristina Martín Díaz

Ingeniero de Telecomunicación

Pliego de condiciones

Pliego de condiciones

Este documento contiene las condiciones legales que guiarán la realización, en este proyecto, de un *Reconocimiento de Passwords gráficos en Dispositivos Móviles*. En lo que sigue, se supondrá que el proyecto ha sido encargado por una empresa cliente a una empresa consultora con la finalidad de realizar dicho sistema. Dicha empresa ha debido desarrollar una línea de investigación con objeto de elaborar el proyecto. Esta línea de investigación, junto con el posterior desarrollo de los programas está amparada por las condiciones particulares del siguiente pliego.

Supuesto que la utilización industrial de los métodos recogidos en el presente proyecto ha sido decidida por parte de la empresa cliente o de otras, la obra a realizar se regulará por las siguientes:

Condiciones generales.

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

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

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

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

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

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

7. Se abonará al contratista la obra que realmente ejecute con sujeción al proyecto que sirvió de base para la contratación, a las modificaciones autorizadas por la superioridad o a las órdenes que con arreglo a sus facultades le hayan comunicado por escrito al Ingeniero Director de obras siempre que dicha obra se haya ajustado a los preceptos de los pliegos de condiciones, con arreglo a los cuales, se harán las modificaciones y la valoración de las diversas unidades sin que el importe total pueda exceder de los presupuestos aprobados. Por consiguiente, el número de unidades que se consignan en el proyecto o en el presupuesto, no podrá servirle de fundamento para entablar reclamaciones de ninguna clase, salvo en los casos de rescisión.

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

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

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

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

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

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

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

15. La garantía definitiva será del 4

16. La forma de pago será por certificaciones mensuales de la obra ejecutada, de acuerdo con los precios del presupuesto, deducida la baja si la hubiera.

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

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

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

20. Durante la realización de la obra, se girarán visitas de inspección por personal facultativo de la empresa cliente, para hacer las comprobaciones que se crean oportunas. Es obligación del contratista, la conservación de la obra ya ejecutada hasta la recepción de la misma,

por lo que el deterioro parcial o total de ella, aunque sea por agentes atmosféricos u otras causas, deberá ser reparado o reconstruido por su cuenta.

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

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

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

Condiciones particulares.

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

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

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

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

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

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

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

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

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

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

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

11. La empresa consultora tendrá prioridad respecto a otras en la elaboración de los proyectos auxiliares que fuese necesario desarrollar para dicha aplicación industrial, siempre que no haga explícita renuncia a este hecho. En este caso, deberá autorizar expresamente los proyectos presentados por otros.

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

Apéndice

Publicación

Este Proyecto Fin de Carrera ha generado la publicación, *DooDB: a Graphical Password Database containing Doodles and Pseudo-Signatures*, que se adjunta a continuación. Los resultados obtenidos durante el desarrollo del mismo se han enviado al congreso ICFHR 2010 (*International Conference on Frontiers in Handwriting Recognition*).

DooDB: a Graphical Password Database containing Doodles and Pseudo-Signatures

M. Martinez-Diaz, J. Fierrez, C. Martin-Diaz, and J. Ortega-Garcia
Biometric Recognition Group - ATVS, EPS - Univ. Autonoma de Madrid, Spain
marcos.martinez@uam.es, julian.fierrez@uam.es, javier.ortega@uam.es

Abstract

Touchscreen-enabled devices are proliferating in the communications and entertainment markets. In this scenario, the use of graphical passwords for user validation is receiving an increasing interest in the last years. Unlike in other fields of research on automatic user authentication, such as biometrics, there are no public databases of graphical passwords usable for research purposes (the extent of our knowledge). In the present work, the recently captured DooDB database is introduced. This database comprises two subcorpora: doodles and simplified signatures (pseudo-signatures). These data were produced by 100 users, who were asked to draw with their fingertips over a mobile device touchscreen. Forgeries are also included in the database. A quantitative analysis of both datasets is first performed. Preliminary verification experiments using the two kinds of graphical passwords are reported.

1. Introduction

Nowadays, the ubiquity of touchscreen-enabled devices has become a fact. The presence of touchscreens in entertainment devices, computers and mobile phones is now common. This represents a new scenario for user interaction with respect to traditional input methods, and has allowed the rise of a wide range of new applications. One of these applications is user-authentication with graphical passwords, a topic that has been subject of research in the last years [1]. The term ”graphical password” comprises many different graphical authentication methods, such as image recognition, point selection in images and drawing repetition. In the present work we focus in the methods based on an individual drawing or sketch made by the user, which is afterwards used for verification (e.g. a handwritten signature). These kind of graphical passwords have received different names in the literature, like “Draw-A-Secret” or DAS [2], “passdoodle” [3], “Scribble-a-Secret” [4] or the general term “doodle” [5] which is the one that is used throughout this work. Graphical passwords are seen as an alternative to traditional passwords, which tend to be complex and may be forgotten. The memorability of pictures (which is in general higher than the one of words) is one of their main advantages [6].

Automatic doodle verification has many similarities with handwritten signature verification. In fact, depending of the perspective, signatures and doodles could be considered a particular case of each other. While signatures have as a clear advantage their uniqueness (at least compared to doodles), one of the main advantages of doodles is the possibility of replacing them if they are compromised. Another variant of doodle, which we propose here, are pseudo-signatures. These consist on a simplified version of a signature, which is traced with the fingertip. Pseudo-signatures share with signatures the advantage of being composed of learned strokes (and thus being theoretically more distinctive than doodles), while they are more suitable for touchscreen devices than traditional signatures, as doodles are.

Signature verification on touchscreen-enabled handheld devices is an emergent field within biometrics [7]. This can be corroborated by the recent acquisition of the BioSecure Multimodal Database [8], in which a corpus of signatures captured on a PDA was acquired. It is well known that publicly available databases make possible for researchers to develop and objectively compare verification algorithms on the same dataset. Experiments carried out using private databases are usually hard to replicate, since database-specific effects, which cannot be reproduced by a third party, may take place. Unfortunately, there is not such a public database in the field of graphical passwords, to the extent of our knowledge. Experiments carried out in the last years related to doodle verification have used proprietary databases [2, 3, 4, 5]. Moreover, in these works there is no reference to forgeries, since only genuine doodles are considered.

The main contribution of this work is to present DooDB, a doodle and pseudo-signature database containing data from 100 users. This database has been captured on a handheld device under realistic conditions. It has two main advantages compared to the ones used in the literature: two acquisition sessions were performed, so inter-session variability effects can be analyzed, and skilled forgeries are provided for each user. The DooDB database is publicly available from the Biometric Recognition Group website [9].

The paper is structured as follows. In Sect. 2 the database is described. Quantitative properties of the database are analyzed in Sect. 3. Preliminary verification experiments using the data from DooDB are reported in Sect. 4 and conclusions are finally drawn in Sect. 5.

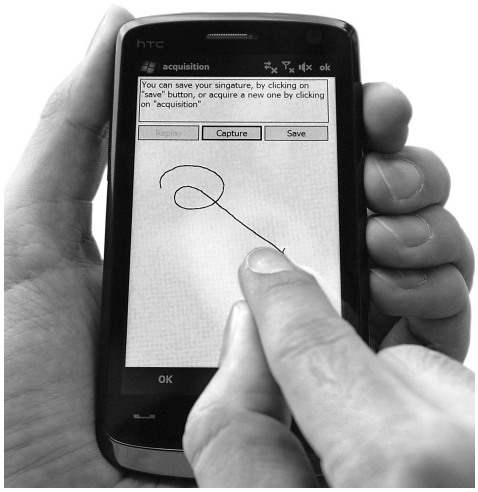


Figure 1. Doodle acquisition setup.

2. The DooDB database

The DooDB database was captured by the Biometric Recognition Group - ATVS. It comprises two subcorpora, each one containing a different modality:

- **Doodles**. Participants were asked to draw with their fingertip a doodle in the touchscreen that they would use as a graphical password on a regular basis for authentication (e.g. instead of the PIN code). There were no restrictions regarding duration or shape. In most cases, users invented their own doodle at the time of acquisition.
- **Pseudo-signatures**. Participants were also asked to draw with their fingertip a simplified version of their signature. This could be, for example, their initials or part of their signature flourish. The main difference between this modality and the doodles is that in this case, the motor process to produce the drawing is in general composed of natural and trained movements.

2.1. Acquisition protocol

Acquisition was performed using an HTC Touch HD mobile phone (see Fig. 1). The device has a resistive touchscreen of 2×3.5in (ca. 5×8.5cm). The x and y coordinates of the fingertip position are sampled as discrete values at 100Hz when the user presses the screen. The coordinate values represent milli-inches, so x values range between $[0, 2000]$ (width) and y values between $[0, 3500]$ (height). The time interval t between consecutive samples is also stored, so the limits of each different stroke can be detected as the samples with a time interval over 10 ms. However, the device has some sampling errors, such as samples that are lost (erroneous values are assigned to their coordinates) or samples that are not captured due to insufficient pressure. To summarize, each drawing is stored as a sequence of discrete values $[x, y, t]$. Some examples of doodles and pseudo-signatures are shown in Fig. 2 and Fig. 3 respectively.

The acquisition process was divided in two sessions, separated by an average period of two weeks. This period was chosen in order to allow enough inter-session variability while trying to avoid that users forgot their doodles. Participants were briefed in the first session about the purpose of the acquisition. Each modality (doodles and pseuso-signatures) was explained to them following the same instructions so each user received the same information. The donors were asked to draw with their fingertip on the handset touchscreen holding it in their own hand, simulating thus real operating conditions. They were let to practice their drawings until they felt comfortable with them.

Forgeries have also been captured in this database. To perform forgeries, users had visual access to the doodle or pseudo-signature they had to forge. The acquisition software replayed the strokes on the screen showing their dynamic properties (i.e. speed). This animation was shown to users up to three times, and then they were left to train until they felt confident with their forgery. The usage of the replay software makes possible to produce forgeries with a notable degree of accuracy, as can be observed in Fig. 2 and Fig. 3.

During the two sessions, the same protocol was followed for each user and modality: 5 genuine samples, then 5 forgeries, 5 genuine samples, followed by 5 forgeries and finally 5 genuine samples. This separation in blocks of 5 signatures allows analyzing intra-session

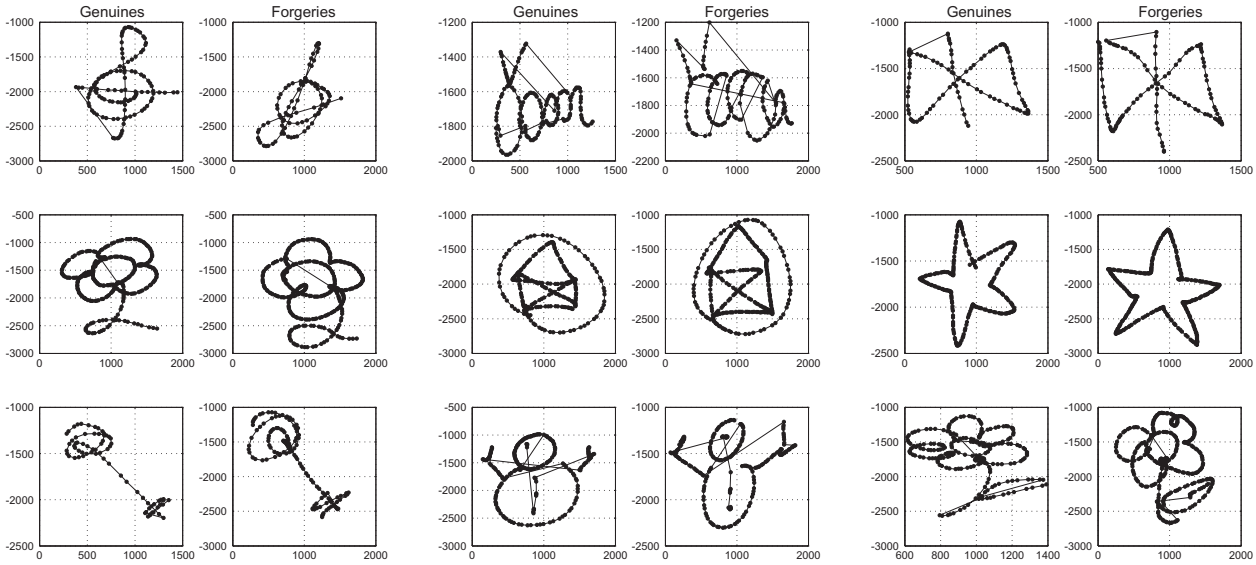


Figure 2. Example of doodles from the database. The right doodle is a forgery of the left one.

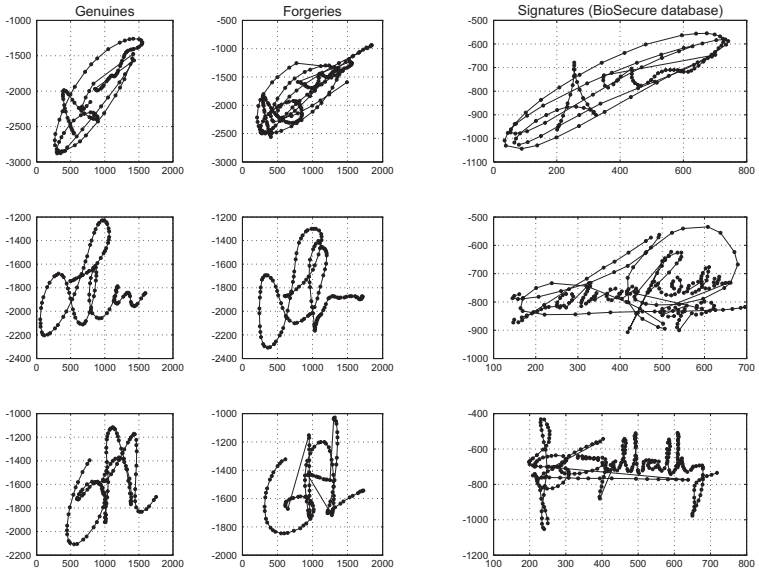


Figure 3. Example of pseudo-signatures from the database. Genuine pseudo-signatures (left), forgeries (middle) and the corresponding signature (right) from the BioSecure database [8].

variability. Consequently, at the end of the two sessions, each user had produced 30 genuine drawings (15 per session) and 20 forgeries. In the first session, user n produced forgeries for users $n-1$ and $n-2$, while in the second, forgeries for users $n-3$ and $n-4$ were produced. A summary of the database contents and properties is shown in Table 1.

2.2. Demographics and Discussion

The participants of the database acquisition present the following age distribution: 75 are less than 25 years old, 14 are between 25 and 40 years old, and 11 are older. The gender distribution is 44 women and 56 men. It was observed during capture that participants not familiar with touchscreen devices required a significant longer training than the rest. This case was more common in older participants.

Table 1. Summary of properties of DooDB.

Property	Description
Subcorpora	2, Doodles and Pseudo-signatures
Donors	100
Gender (male/female)	56 / 44
Age (< 25 / 25-40 / > 40)	75 / 14 / 11
Sessions	2, separated by an average of 2 weeks
Samples per donor	30 genuine and 20 forgeries

A subset of 13 participants of this database have also participated in the BioSecure Multimodal Database (BMDB) [8]. In that database, on-line signatures were captured both using a pen-tablet and a PDA with a stylus. This overlap makes possible to observe the evolution of signatures from a controlled scenario (signature with pen and paper placed on a pen-tablet), towards more degraded conditions (signature in a PDA) and, finally, the pseudo-signature extreme case (simplified signature traced with the fingertip). Some examples of genuine signatures and their corresponding pseudo-signatures from the same user are shown in Fig. 3.

One of the critical issues in graphical passwords is memorability. During the second acquisition session, it was observed that ca. 90% of the participants remembered correctly their pseudo-signature. On the other hand, nearly 40% of the participants had difficulties to recall their doodle from the first session. Users could request to see the tracing process of their own drawings from the first session. This was done by using the aforementioned functionality designed to train forgers. This high percentage of users that requested help to recall their doodle is affected by the fact that the had not used it between sessions on a regular basis. Consequently, in a real scenario where users use their doodles frequently, memorability may not be so problematic.

3. Data Analysis

3.1. Statistical properties

Given the different nature of doodles and pseudo-signatures it is expected that they present differences in their properties such as their length or graphical complexity. A statistical analysis of the properties from the two captured subcorpora has been performed. These properties have also been compared with the ones from a BioSecure PDA Signature subcorpus of 120 users, allowing thus a comparison between handwritten signatures, finger-traced pseudo-signatures and doodles. Four basic properties have been analyzed: length, complexity (as the number of intersections and number of strokes), and dynamics.

In Fig. 4.a, the statistical distribution of the three sets in terms of their number of samples is represented. As can be seen, handwritten signatures tend to be longer than the finger-traced drawings. Moreover, signatures present a higher variability in terms of length. Doodles also tend to be longer than pseudo-signatures.

The distribution of the number of intersections in the drawings is represented in Fig. 4.b, where we observe that signatures present more intersections. The differences between doodles and pseudo-signatures are small in this case. A low amount of intersections indicates in general low graphical complexity.

In Fig. 4.c, the distribution of the amount of strokes from each dataset is represented. Pseudo-signatures tend to have the lowest amount of strokes (75% have less than 4 strokes), followed by doodles. The low amount of strokes in the case of pseudo-signatures may be due to the fact that donors normally use their initials or a simple flourish, with few isolated components. On the other hand, users tend to create more complex drawings when choosing a doodle.

The stroke speed distributions are compared in Fig. 4.d. As can be seen, doodles are the "slowest" from the three datasets. The main cause for this may be that doodles are in general new and invented drawings for the participants, while pseudo-signatures are (or at least contain) previously learned movements. The higher speeds of signatures might be affected by three main factors: the stylus tip has less friction than a fingertip on a touchscreen, signatures are composed of learned movements and, finally, using a writing instrument (e.g. stylus) is more natural than the fingertip. A writer moves the stylus with a combination of his fingers and wrist movements (i.e. the natural writing process), while in the case of finger-drawn sketches, the wrist is the main motor element, since the finger used for drawing is kept mainly fixed.

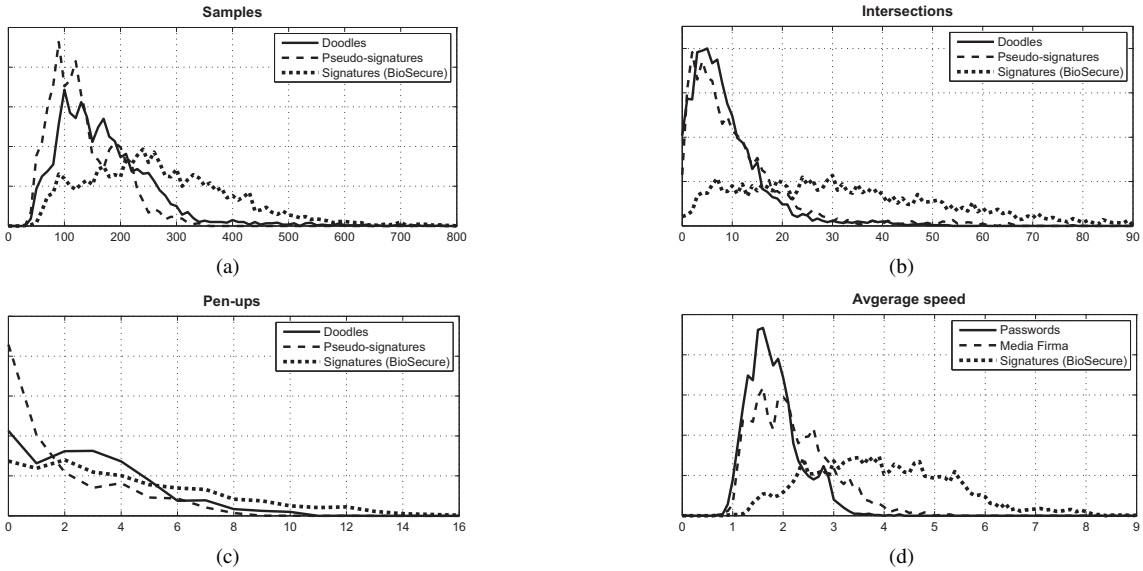


Figure 4. Distribution of (a) the stroke length, (b) the number of intersections, (c) the number of isolated strokes and (d) the average speed in each dataset (normalized to [0,9]).

3.2. Graphical and qualitative properties

When the whole doodle dataset is visually inspected, it can be seen that there are three main types of doodles:

- **Abstract** doodles, which cannot be directly interpreted as representing an object or idea.
- **Conceptual** doodles, which represent an object or idea (e.g. a flower).
- **Symbolic** doodles, which are known and recognizable symbols, like currency or musical notation.

Doodles that are abstract for an observer may be conceptual to another that is able to interpret them. However, it can be hypothesized that abstract doodles may be more resilient to forgers with visual access to them, since the are harder to remember [6]. The proportion of these three doodle types in the DooDB database is: 43 abstract, 37 conceptual, and 20 symbolic doodles, although this is based on a subjective evaluation. It has also been observed some repetitions among the doodles provided by participants, specially for common drawings. Some examples of repeated doodles are a flower symbol (see Fig. 2) and a smiling face.

Regarding pseudo-signatures, a clear classification between different types cannot be established. It is observed that most participants tend to produce a simplified version of the signature, including flourish. However, ca. 20% of the participants have written their initials, their name or a shortened version of it without flourish.

4. Preliminary verification experiments

In order to assess the distinctiveness of the acquired doodles and pseudo-signatures, some preliminary experiments have been carried out. A simple system, based on Dynamic Time Warping (DTW) to compare the captured time sequences has been used [10]. Three sets of features are used: the coordinate sequence $[x, y]$, the speed sequence, $[x', y']$ and the acceleration sequence $[x'', y'']$. This allows performing a preliminary assessment of which type of dynamic features are more distinctive for doodles and pseudo-signatures.

4.1. Experimental protocol

The whole sets of doodles and pseudo-signatures are used for the experiments. For each user, the first 5 genuine samples from the first session are used as reference templates. The 15 genuine signatures of the second session are used to compute genuine user scores, simulating thus real operating conditions, in which inter-session variability affects the verification performance. To compute skilled forgery scores, the 20 available forgeries per user are employed. Random forgeries are also considered. A random forgery is the case where a user claims to be another one while using his own doodle or pseudo-signature. Random forgery scores are obtained

Features	Pseudo-signatures		Doodles	
	$EER_{rd}(\%)$	$EER_{sk}(\%)$	$EER_{rd}(\%)$	$EER_{sk}(\%)$
$[x, y]$	5.3	34.3	7.5	36.0
$[x', y']$	4.3	28.8	6.5	33.3
$[x'', y'']$	4.6	24.6	7.8	33.4

Table 2. Verification performance for the 3 feature pairs considered. EER_{sk} refers to the EER for skilled forgeries and EER_{rd} for random forgeries.

by comparing the user reference set to one signature sample of all the remaining users. For each comparison against the 5 reference templates, an output score is generated by averaging the 5 obtained DTW distances.

4.2. Results

The verification performance in terms of Equal Error Rate (EER) is shown in Table 3.2. As can be seen, the performance is better for pseudo-signatures both for random and skilled forgeries. One of the main reasons of the higher error rate against random forgeries for doodles may be the presence of doodles from different users that are notably similar.

It can also be observed that performance against skilled forgeries improves for pseudo-signatures when dynamic properties (i.e. speed or acceleration) are used. This effect may be due to the higher consistency in the drawing process of pseudo-signatures, since they are composed in general of natural or learned movements. On the other hand, when doodles are considered, the usage of speed or acceleration properties does not increase the performance in the same proportion. This may be due to an increased variability in the drawing process. In fact, it was observed during the doodle subset acquisition, that some users varied the stroke order of their doodles even in the same session. This was not the case for pseudo-signatures.

5. Conclusions and Future Work

The DooDB database has been presented. This database comprises doodles and pseudo-signatures from 100 users, and forgeries from all of them. The acquisition protocol has been described and various data analyses have been performed. Preliminary verification experiments have been carried out, revealing that one of the main challenges of doodle and pseudo-signature verification may be protection against forgeries.

It has been observed that some users tend to produce well-known symbols as doodles. This motivates repetition of the similar doodles among different users.

Based on the preliminary results, doodles and pseudo-signatures are seen as a potential lightweight authentication method oriented to mobile devices. One of the main advantages of this kind of graphical password is its convenience and the possibility of performing user authentication needing no extra hardware unlike, for example, most biometric traits, in fingerprint authentication.

Future work includes the analysis of the impact of doodle complexity in the performance against skilled forgeries. Additionally, the impact of each kind of doodle (symbolic, abstract or conceptual) in the quality of forgeries is also source for future work.

References

[1] X. Suo, Y. Zhu and G. Owen, "Graphical passwords: a survey", *Proc. of 21st Annual Computer Security Applications Conf., ACSAC*, 2005, pp 463–472, Tucson, USA.

[2] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter and A. D. Rubin, "The design and analysis of graphical passwords", *Proc. of 8th USENIX Security Symposium*, 1999, Berkeley, USA.

[3] J. Goldberg, J. Hagman and V. Sazawal, "Doodling our way to better authentication", *Proc. of CHI '02 extended abstracts on Human factors in computing systems*, 2002, pp 868–869.

[4] M. Oka, K. Kato, X. Yingqing, L. Liang and F. Wen, "Scribble-a-Secret: Similarity-based password authentication using sketches", *Proc. of Intl. Conf. on Pattern Recognition, ICPR*, Dec. 2008, pp 1–4.

[5] N. S. Govindarajulu and S. Madhvanath, "Password management using doodles", *Proc. of 9th Intl. Conf. on Multimodal Interfaces, ICMI*, 2007, pp 236–239.

[6] K. Renaud, "On user involvement in production of images used in visual authentication", *Journal of Visual Languages & Computing*, 20(1):1 – 15, 2009.

[7] M. Martinez-Diaz, J. Fierrez, J. Galbally and J. Ortega-Garcia, "Towards mobile authentication using dynamic signature verification: useful features and performance evaluation", *Proc. Intl. Conf. on Pattern Recognition, ICPR*, 2008, pp 1–6.

[8] J. Ortega-Garcia, J. Fierrez, F. Alonso-Fernandez et al., "The multi-scenario multi-environment BioSecure multimodal database (BMDB)", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, (to appear), 2010.

[9] http://atvs.ii.uam.es/.

[10] M. Martinez-Diaz, J. Fierrez and S. Hangai, *Encyclopedia of Biometrics*, chapter Signature matching, pp 1192–1196, Springer, 2009.