

Autenticación Automática de Estudiantes Mediante Reconocimiento de Firma Dinámica

Automatic Student Authentication Using Dynamic Signature Recognition

Ruben Vera-Rodriguez, Julian Fierrez, Aythami Morales, Ruben Tolosana, Javier Ortega-Garcia
{ruben.vera, julian.fierrez, aythami.morales, ruben.tolosana, javier.ortega}@uam.es

Departamento de Tecnología Electrónica y de las Comunicaciones
Universidad Autónoma de Madrid
Madrid, Spain

Resumen- Este trabajo realiza un análisis sobre la aplicación de sistemas de reconocimiento biométrico para la autenticación de estudiantes, en particular haciendo uso de la firma manuscrita dinámica, que es uno de los rasgos biométricos más aceptados socialmente. En el ámbito educativo, la firma se suele utilizar para control de asistencia, ya sea para clases o exámenes, pero no para la autenticación (automática) de los estudiantes. Además, el uso de esta tecnología se puede extender a diferentes servicios administrativos en el sistema educativo, con el fin de añadir un mayor nivel de seguridad a los procedimientos tradicionales de autenticación. Este trabajo analiza dos escenarios de aplicación para esta tecnología: i) un escenario de oficina con una tableta de adquisición de alta calidad diseñada específicamente para adquirir firmas (dispositivo Wacom), y ii) un escenario móvil donde los usuarios pueden firmar sobre sus smartphones con el dedo, mejorando de esta forma la usabilidad.

Palabras clave: *Innovación, reconocimiento biométrico, autenticación, firma dinámica, biometría.*

Abstract- This paper focuses on the application of biometric recognition for automatic student authentication, in particular making use of dynamic handwritten signatures, which are one of the most socially accepted biometric traits. In education, signatures are used for attendance control, either to lectures or exams, but not for (automatic) authentication. Also, the use of this technology can be extended to different administrative services within the education system, in order to add a higher security level to the traditional procedures of authentication. This paper analyses two application scenarios for this technology: i) an office scenario with a high quality pen tablet specifically designed to acquire signatures (i.e., Wacom device), and ii) a mobile scenario where users sign on their smartphones with the finger improving this way the usability.

Keywords: *Innovation, person authentication, signature recognition, biometrics.*

1. INTRODUCCIÓN

La autenticación de usuarios en servicios y sistemas es una necesidad imprescindible en la actualidad, siendo innumerables las ventajas que aporta a este proceso el

reconocimiento biométrico, que evita los problemas de los procedimientos tradicionales, basados en lo que el usuario sabe (passwords, claves, etc.) o en lo que el usuario posee (tarjetas, tokens). Los rasgos biométricos no pueden ser extraviados, no resulta necesario memorizarlos, forman parte de nuestra persona, los llevamos siempre encima y permanecen con el tiempo. De hecho, podemos considerar la autenticación biométrica como una tecnología madura, y los sistemas basados en reconocimiento de huella dactilar, en reconocimiento de iris o en verificación de cara resultan ya habituales en controles de acceso en aeropuertos y recintos securizados, y son almacenados en nuestros DNIs y pasaportes. No obstante, existen numerosos retos aún por resolver.

Los rasgos biométricos pueden ser clasificados, atendiendo a su naturaleza, en: a) rasgos fisiológicos o morfológicos, como por ejemplo la huella dactilar y palmar, el iris, la cara, la geometría de la mano y de la oreja, o el patrón venoso de la mano; y b) rasgos conductuales, derivados de alguna conducta o comportamiento humanos, y generados a partir de algo que la persona produce: la voz, la escritura y la firma manuscrita, la forma de teclear, o el modo de andar son buenos ejemplos.

Este trabajo realiza un análisis sobre la aplicación de sistemas de reconocimiento biométrico para la autenticación de estudiantes, en particular, haciendo uso de la firma manuscrita dinámica, que es uno de los rasgos biométricos más aceptados socialmente. La firma se lleva utilizando en acuerdos legales y financieros desde hace más de cien años (Plamondon & Lorette, 1989). En el caso particular del sistema educativo, la firma se utiliza para control de asistencia, ya sea para clases o exámenes, y también para la firma de todo tipo de documentos administrativos de una forma manual (como puede ser la comprobación visual de la cara y/o firma de la persona que aparece en el DNI o tarjeta universitaria).

Sin embargo, no existe un control riguroso de dichas firmas, y es común encontrar casos de estudiantes que firman fichas de asistencia por otros, o incluso suplantación de la

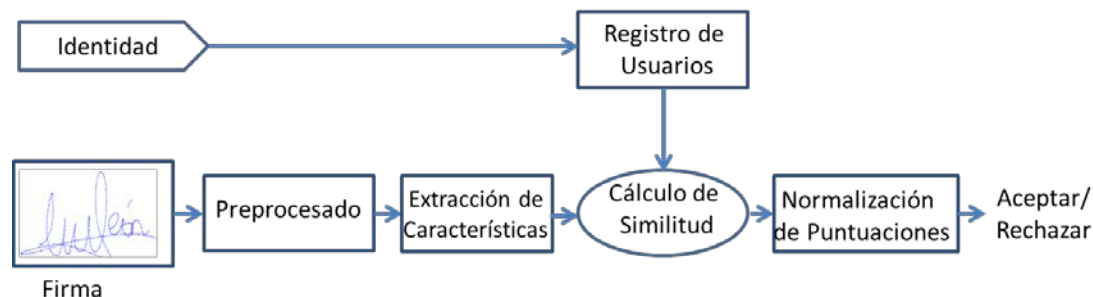


Figura 1: Arquitectura general de un sistema de verificación de firma dinámica.

identidad en la realización de exámenes, con las implicaciones que ello conlleva.

Con el uso de sistemas de reconocimiento automático de firma biométrica, se permite continuar realizando la misma operativa que hasta ahora, pero con la gran diferencia de que se dota al proceso de autenticación de la identidad de un nivel de seguridad y de rendimiento mucho mayor, ayudando tanto a los profesores como personal de administración a realizar dicho proceso de autenticación de forma sencilla y certera.

Con el rápido desarrollo de sistemas de reconocimiento de firma dinámica (Fierrez & Ortega-García, 2008, Tolosana et al., 2015), esta tecnología está lista para ser usada, y de hecho se está implantando en el sector bancario por el presente grupo de investigación con resultados muy positivos (Proyecto e-BioFirma, 2014) y en el sector educativo se está desarrollando un piloto de reconocimiento de firma biométrica en la Universidad Autónoma de Madrid (Proyecto e-DemoFirma, 2015).

El uso de la firma dinámica manuscrita tiene enormes ventajas en los procesos de autenticación de usuarios, ya que se percibe como algo natural en un proceso de autenticación, el proceso dinámico de la escritura no puede ser extrapolado al completo a partir de la visualización de la firma realizada, ya que contiene información de identidad que no queda reflejada en el grafo.

A diferencia de la firma estática o realizadas sobre papel, las firmas dinámicas son aquellas adquiridas sobre dispositivos electrónicos que permiten obtener información de la realización de dicha firma en el tiempo, como son las coordenadas X e Y y la presión al menos. En los últimos años se ha producido una gran evolución en los dispositivos electrónicos que permiten la adquisición de firmas dinámicas (por ejemplo, tabletas, PDA, bolígrafos digitalizadores, smartphones, etc.) (Martínez-Díaz & Fierrez, 2009). Por esta razón, la popularidad de este rasgo biométrico está aumentando rápidamente en los últimos años. Además, cabe destacar que también se pueden realizar firmas sobre smartphones utilizando el dedo como útil de escritura (Martínez-Díaz et al., 2013; Vera-Rodríguez, et al., 2014). Estos dispositivos representan un objetivo atractivo para el despliegue de sistemas de verificación de firmas, proporcionando capacidades de procesamiento suficientes y una interfaz basada en el contacto (Vivaracho-Pascual & Pascual-Gaspar, 2012). Sin embargo, la verificación de firmas en dispositivos móviles se ve afectada por factores que no están presentes en otros dispositivos, principalmente debido a

la pequeña zona de pantalla sobre la que escribir, su pobre ergonomía o el hecho de que el usuario puede estar en movimiento. Los usuarios deben firmar en una superficie poco familiar y por lo general inestable con un pequeño lápiz o con el dedo. Como consecuencia, el proceso de generación de firmas se puede degradar.

En este trabajo analizamos dos escenarios de aplicación para esta tecnología en el ámbito de la autenticación de estudiantes: i) Escenario de Oficina, donde los usuarios firman sobre una tableta de adquisición de alta calidad diseñada específicamente para adquirir firmas (dispositivo Wacom), y ii) un Escenario de Movilidad, donde los usuarios pueden firmar sobre sus smartphones con el dedo, mejorando de esta forma la usabilidad. Este es un caso de estudio muy novedoso en el ámbito de la innovación docente y del reconocimiento de firma dinámica, ya que la mayoría de trabajos previos se han centrado en el uso de tabletas o dispositivos móviles usando lápices de escritura pero no el dedo (Houmani et al., 2012; Ortega-García et al., 2010; García-Salicetti et al., 2007), lo cual empieza a ser muy popular.

En el primer caso considerado (Escenario de Oficina) se analiza la inclusión de la autenticación automática de usuarios en escenarios donde es común la autenticación de usuarios mediante su firma (por ejemplo, los servicios administrativos de una universidad). En el segundo caso (Escenario de Movilidad), la autenticación automática de usuarios en un escenario de movilidad abre la puerta a muchas nuevas aplicaciones en las que los usuarios poseen el sensor necesario para la adquisición de la firma (smartphone). En educación existen aplicaciones como la autenticación de usuarios en MOOCs, control de asistencia en las clases o exámenes, el uso en bibliotecas, etc. También existen aplicaciones en otros sectores como la administración electrónica, la sanidad, la banca o los seguros. En función de los resultados experimentales obtenidos en este estudio se realizan ciertas recomendaciones sobre la conveniencia de los dos escenarios considerados en distintas aplicaciones en función de las restricciones de seguridad requeridas.

Para este estudio experimental, hacemos uso de la base de datos e-BioSign (Vera-Rodríguez et al., 2014), que fue capturada utilizando diversos dispositivos como tabletas y smartphones. En dicho trabajo se encuentran detalles de la adquisición y evaluación preliminar de dichos datos. En el presente trabajo nos centramos en analizar escenarios de aplicación de la tecnología de firma biométrica en el ámbito educativo (escenarios fijo y en movilidad). La base de datos contiene firmas de 70 usuarios, incluyendo a estudiantes y



Figura 2: Dispositivos de captura empleados en este estudio para adquirir firmas dinámicas. Izquierda Wacom STU-530, derecha Samsung Galaxy Note 10.1.

profesores universitarios, y fue capturada en dos sesiones en días distintos. El trabajo experimental de autenticación automática mediante firmas dinámicas se han realizado teniendo en cuenta dos tipos de falsificaciones, a saber: i) falsificaciones aleatorias (*random forgeries*), aquellas en las que un impostor usa su propia firma pero dice ser otra persona), y ii) falsificaciones cualificadas (*skilled forgeries*), aquellas en las que los impostores imitan la firma de otras personas.

2. CONTEXTO

Este trabajo se contextualiza en el análisis de dos escenarios de aplicación de un sistema de reconocimiento de firma dinámica como forma de autenticar automáticamente estudiantes. Estos dos escenarios de aplicación son un escenario de oficina (tableta de altas prestaciones y firma con lápiz de escritura) y un escenario de movilidad (firma con dedo sobre smartphone). Se va a analizar el rendimiento en forma de tasas de error de reconocimiento biométrico en dichos escenarios de aplicación y en base a los resultados obtenidos proponemos recomendaciones de uso.

En general los sistemas de verificación de firma dinámica comparten una arquitectura común como la que se muestra en la Figura 1. A continuación describimos cada una de las etapas del sistema de verificación de firma dinámica implementado:

1. Adquisición de datos: Para la adquisición de datos tuvimos en cuenta dos dispositivos para este estudio, una tableta digitalizadora (Wacom STU-530) y un smartphone (Samsung Galaxy Note 10.1) para estudiar el rendimiento del sistema en dos aplicaciones diferentes (de oficina y movilidad).

2. Preprocesado: La etapa de preprocesado consistió en la eliminación de las muestras iniciales y finales de cada firma sin presión, manteniendo de esta manera sólo la información entre el primer y el último apoyo sobre la tableta. También se realizó una normalización espacial de los datos mediante una alineación del centro de masas de cada firma a una posición común de coordenadas.

3. Extracción de características: Existen principalmente dos enfoques de extracción de características en sistema de verificación de firma dinámica: i) sistemas basados en parámetros globales y ii) sistemas basados en funciones

temporales. En este caso hemos seguido un enfoque basado en funciones temporales, haciendo una selección de funciones extraídas a partir de las coordenadas X , Y y presión, tales como su primera y segunda derivadas de orden, la velocidad, el radio de curvatura, etc.

4. Cálculo de similitud: Este paso implica la pre-alineación si es necesario y un proceso de correspondencia, que devuelve una puntuación de coincidencia. En este caso, Dynamic Time Warping (DTW) algoritmo se utiliza como el clasificador, que permite calcular una alineación elástico entre secuencias de tiempo de diferente longitud, y la obtención de una medida de distancia.

5. Normalización de puntuaciones: La última etapa es la normalización de puntuaciones, en la que las puntuaciones se normalizan a un rango dado. Esta etapa es crítica en caso de combinar las puntuaciones de múltiples clasificadores o en sistemas multi-biométricos.

Finalmente, una firma de entrada se considera como perteneciente al usuario que dice ser si su puntuación es superior a un umbral dado.

3. DESCRIPCIÓN

En esta sección se describe la base de datos utilizada así como el protocolo experimental seguido.

A. Descripción de la base de datos

Los experimentos llevados a cabo en este trabajo se han realizado haciendo uso de un subconjunto de la base de datos e-BioSign. En este caso hemos utilizado dos de los cinco dispositivos: Wacom STU-530 y Samsung Galaxy Note 10.1 (ver Figura 2). El primero (Wacom) está diseñado específicamente para la captura de datos manuscritos y será utilizado en este estudio para simular un escenario de oficina. El segundo dispositivo (Samsung) es un dispositivo de propósito general no diseñado específicamente para capturar firmas dinámicas, y se utiliza en este estudio en un escenario de movilidad donde los usuarios pueden firmar con el dedo.

- **Wacom STU-530:** pantalla a color TFT-LCD de 5 pulgadas, con resolución VGA de 640 x 480 píxeles. Tiene una tasa de muestreo de 200 Hz, y 1024 niveles de presión. Este dispositivo sólo permite escribir usando un lápiz (pen stylus).

- **Samsung Galaxy Note 10.1:** Se trata de un dispositivo con sistema operativo Android. Tiene una pantalla LCD de 10.1 pulgadas con una resolución de 1280 x 800 píxeles y 1024 niveles de presión. Este dispositivo permite utilizar tanto un pen stylus como el dedo.

La base de datos de e-BioSign se capturó en dos sesiones con un intervalo de tiempo de al menos tres semanas entre sesiones. En cada sesión, 4 firmas genuinas y 3 falsificaciones cualificadas (*skilled forgeries*) fueron adquiridas por cada uno de los 70 usuarios de la base de datos.

El proceso de captura fue supervisado por un operador que explicaba todos los pasos que los usuarios debían seguir. Por lo tanto, e-BioFirma es una base de datos multi-sesión y multi-

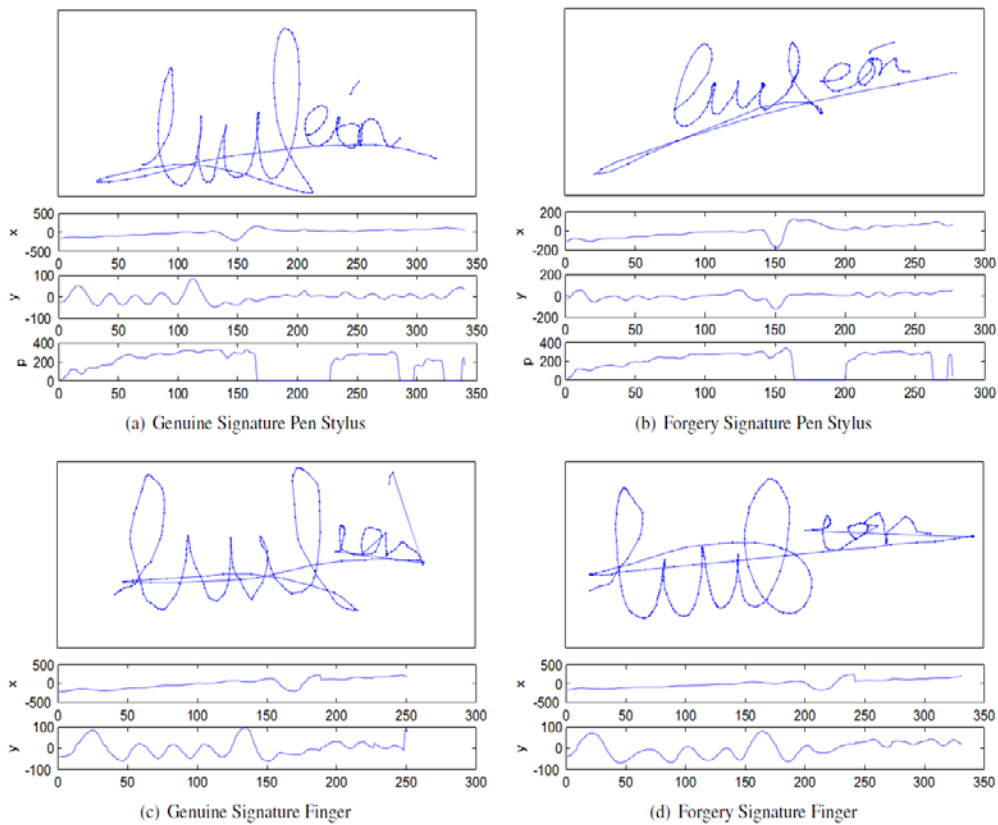


Figura 3: Ejemplos de datos adquiridos con el dispositivo Samsung Galaxy Note 10.1 en la base de datos e-BioSign.

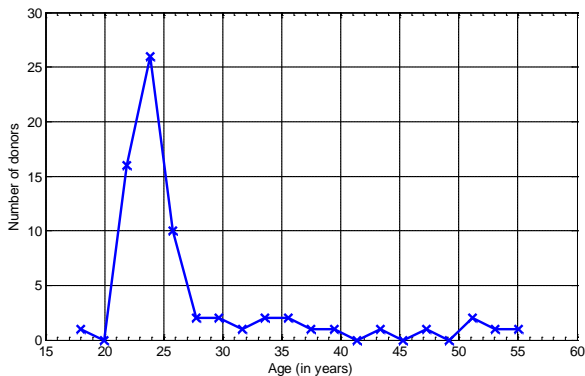


Figura 4: Distribución de la edad de usuarios de e-BioSign.

dispositivo con muestras capturadas utilizando tanto un lápiz de escritura como el dedo. La Figura 3 muestra ejemplos de los datos recogidos en e-BioSign para el Samsung Galaxy Note 10.1, con firmas genuinas y falsificaciones utilizando el lápiz y el dedo. Cabe señalar que los datos capturados utilizando el dedo para el Samsung Galaxy Note 10.1 no contienen información de presión ya que esta información no se proporciona por este dispositivo cuando se usa el dedo, y también que no hay información de la trayectoria (coordenadas X e Y) al hacer levantamientos (pen-ups) en la escritura. Para el caso de utilizar el lápiz con el dispositivo Wacom la información de la presión y trayectorias pen-up está disponible

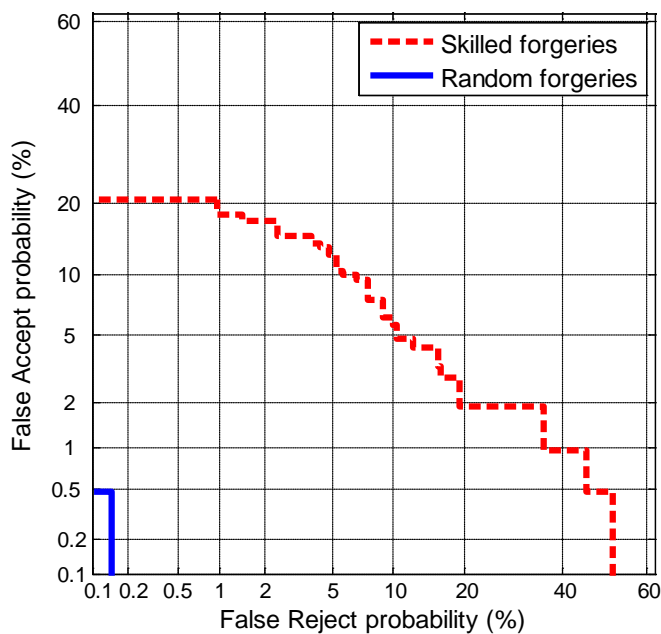
y se ha utilizado en la evaluación de rendimiento mostrada en este estudio.

La Figura 4 muestra estadísticas de la población de la base de datos de e-BioSign. En cuanto a la distribución por edad, la mayoría de los usuarios (67,1%) tienen entre 22 y 27 años de edad, ya que la base de datos se recogió en un ambiente universitario. Un 11,4% tiene entre 17 y 21 años de edad, también 11,4% tiene entre 28 y 38 años de edad y el 10% están por encima de los 39 años. Adicionalmente, se conocen los detalles sobre la distribución de género y mano de escritura. Existe un 58,6% de varones y un 41,4% de mujeres. En cuanto a la distribución de la mano de escritura, el 88,6% de la población es diestra.

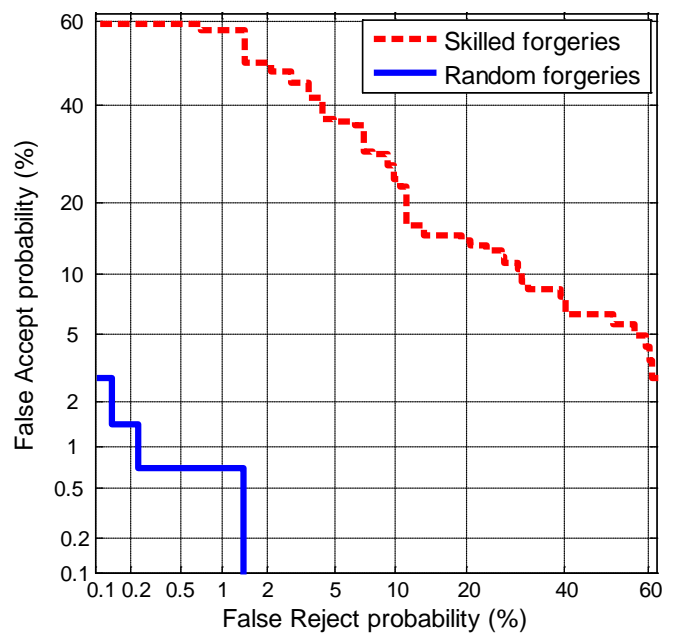
B. Protocolo experimental

El protocolo experimental fue diseñado para obtener una comparación de rendimiento de un sistema de verificación de firma dinámica sobre los dos escenarios de interés, es decir, Escenario de Oficina (dispositivo Wacom con lápiz) y Escenario de Movilidad (dispositivo Samsung con el dedo). En esta evaluación la evaluación se basa en comparaciones de firmas 1 a 1. De esta manera, se utilizó un enfoque *leave-one-out* sobre los datos genuinos de cada usuario.

En los experimentos se han considerado dos tipos de falsificaciones: “falsificaciones aleatorias” (*random forgeries*), que se dan cuando un falsificador utiliza su propia firma haciéndose pasar por otro usuario del sistema. En este caso las



(a) Escenario de Oficina



(b) Escenario de Movilidad

Figura 5: Curvas DET con resultados de los dos escenarios operacionales considerados en este estudio. Se muestra en cada gráfica los resultados para imitaciones aleatorias y cualificadas (*random* y *skilled forgeries* respectivamente).

Tabla 1. Rendimiento (EER) de los escenarios de aplicación considerados

Escenarios considerados	EER (%)	
	Imitaciones Skilled	Imitaciones Random
Escenario de Oficina	7.6	0.3
Escenario de Movilidad	14.9	0.7

puntuaciones se obtienen comparando las firmas genuinas del usuario con una muestra de la firma de todos los usuarios restantes. Las puntuaciones para las “falsificaciones cualificadas” (*skilled forgeries*) se obtienen comparando las firmas genuinas con las 6 firmas de tipo *skilled forgeries* disponibles por usuario.

4. RESULTADOS

En esta sección se describen los resultados experimentales obtenidos para los dos escenarios operacionales considerados en este trabajo.

En un sistema de verificación de firma existen dos tipos de errores que se pueden cometer. El error de falsa aceptación se produce cuando el sistema acepta un impostor. Por otro lado el error de falso rechazo se produce cuando un usuario genuino es rechazado. Para evaluar el rendimiento de un sistema biométrico de verificación, se procesa un conjunto de tests con comparaciones procedentes de firmas de los mismos usuarios y de usuarios distintos y se obtienen las probabilidades de los dos

tipos de errores cometidos. Dichas probabilidades se pueden ver gráficamente mediante curvas DET (véase Figura 5).

Una medida de rendimiento muy común en sistemas biométricos es la tasa de igual error (EER), que es el punto de operación en el que la probabilidad de falsa aceptación y la probabilidad de falso rechazo tienen el mismo valor. Cuanto menor sea el EER, mejor rendimiento tiene el sistema biométrico.

En el trabajo experimental llevado a cabo en este estudio, el rendimiento de los sistemas de verificación de firmas se expresa en forma de EER (Tabla 1) y de curvas DET (Figura 5). Como se puede ver tanto en la Tabla 1 como en la Figura 5, en términos generales el rendimiento del sistema biométrico en el Escenario de Oficina es mejor en comparación con el rendimiento del Escenario de Movilidad. Las tasas de EER obtenidas para el Escenario de Oficina son aproximadamente la mitad, con un 0.3% EER para falsificaciones aleatorias (*random*) en comparación con un 0.7% EER obtenido en el Escenario de Movilidad. En cuanto a las falsificaciones tipo *skilled*, se obtiene un 7.6% EER para el Escenario de Oficina en comparación con un 14.9% EER para el Escenario de Movilidad.

Mientras que esta diferencia en el rendimiento es significativa, los resultados obtenidos en el Escenario de Movilidad son aceptables para falsificaciones cualificadas (*skilled*) y muy buenos para falsificaciones aleatorias (*random*). Las razones de esta diferencia en el rendimiento pueden ser varias, como que la información de la presión no está presente en el dispositivo móvil cuando se firma con el dedo, la información de los levantamientos tampoco está disponible en ese caso, y que al escribir con el dedo se puede producir una

mayor variabilidad intra-persona en comparación con el caso en el que se escribe con un lápiz de escritura.

5. CONCLUSIONES

Este trabajo analiza dos escenarios para la autenticación de estudiantes utilizando la firma dinámica: i) un escenario de oficina con una tableta de alta calidad diseñada específicamente para adquirir firmas (dispositivo Wacom), y ii) un escenario de movilidad en el que los usuarios pueden firmar en sus smartphones usando el dedo, mejorando de esta manera la capacidad de uso. Para este estudio experimental se ha hecho uso de la base de datos de e-BioSign, que fue capturada utilizando varias tabletas y smartphones actuales. La base de datos contiene firmas de 70 usuarios, incluyendo a estudiantes y profesores universitarios, y fue capturada en dos sesiones en distintos días.

Los resultados experimentales muestran muy buenas tasas de rendimiento de los sistemas en el escenario de oficina (0.3% EER para falsificaciones aleatorias y 7.6% EER para falsificaciones cualificadas). En el escenario de movilidad el rendimiento es muy bueno para la detección de falsificaciones aleatorias (0.7% EER), pero se degrada al 15% EER en los casos de falsificaciones cualificadas. Todavía hay espacio para mejoras de estos resultados, por ejemplo entrenando modelos de usuario haciendo uso de un conjunto de varias firmas de entrenamiento (alrededor de 5 a 10). De esta manera la variabilidad intra-persona se puede incluir en los modelos y obtener mejoras de rendimiento.

Por lo tanto, concluimos que en vista a los resultados obtenidos, apoyamos firmemente el uso de esta tecnología en un entorno educativo universitario para la autenticación automática de personas. Para escenarios de oficina los resultados obtenidos en este estudio muestran que dicha tecnología está lista, y para escenarios de movilidad se podrían usar modelos de usuario para obtener mejoras de rendimiento y obtener resultados similares a los del escenario de oficina.

AGRADECIMIENTOS

Este trabajo está financiado parcialmente por los siguientes proyectos: Bio-Shield (TEC2012-34881), Cecabank e-BioFirma, BEAT (FP7-SEC-284989) y Cátedra UAM-Telefónica.

REFERENCIAS

Fierrez, J. y Ortega-García, J. (2008). On-line Signature Verification. A. K. Jain, A. Ross and P.Flynn (Eds.), Handbook of Biometrics, Springer, pp. 189-209.

García-Salicetti, S., Fierrez-Aguilar, J., Alonso-Fernández, F., Vielhauer, C., Guest, R., Allano, L., Trung, T.Do., Scheidat, T., Van Ly, B., Dittmann, J., Dorizzi, B., Ortega-García, J., González-Rodríguez, J., Bacile Di Castiglione, y M., Fairhurst, M. (2007). Biosecure reference systems for on-line signature verification: A study of complementarity. Annals of Telecommunications, Special Issue on Multimodal Biometrics, 62 (1-2), pp. 36-61.

Houmani, N., Mayoue, A., García-Salicetti, S., Dorizzi, B., Khalil, M. I., Moustafa, M. N., Abbas, H., Muramatsu, D., Yanikoglu, B., Kholmatov, A., Martínez-Díaz, M., Fierrez, J., Ortega-García, J., Roure Alcobe, J., Fabregas, J., Faundez-Zanuy, M., Pascual-Gaspar, J. M., Cardenoso-Payo, V., y Vivaracho-Pascual, C. (2012). BioSecure signature evaluation campaign (BSEC2009): Evaluating online signature algorithms depending on the quality of signatures. Pattern Recognition, 45 (3), pp. 993-1003.

Martínez-Díaz, M. y Fierrez, J. (2009). Signature Databases and Evaluation. Encyclopedia of Biometrics, Springer, pp. 1178-1184.

Martínez-Díaz, M., Fierrez, J. y Galbally, J. (2013). The DooDB Graphical Password Database: Data Analysis and Benchmark Results. IEEE Access, vol. 1, pp. 596-605.

Ortega-García, J., Fierrez, J., Alonso-Fernández, F., Galbally, J., Freire, M., González-Rodríguez, J., García-Mateo, C., Alba-Castro, J.L., González-Aguila, E., Otero-Muras, E., García-Salicetti, S., Allano, L., Ly-Van, B., Dorizzi, B., Kittler, J., Bourlai, T., Poh, N., Deravi, F., Ng, M., Fairhurst, M., Hennebert, J., Humm, A., Tistarelli, M., Brodo, L., Richiardi, J., Drygajlo, A., Ganster, H., Sukno, F.M., Pavani, S.K., Frangi, A., Akarun, L. and Savran, A. (2010). The Multi-Scenario Multi-Environment BioSecure Multimodal Database (BMDB), IEEE Trans. on Pattern Analysis and Machine Intelligence, 32(6), pp. 1097-1111.

Plamondon, R. y Lorette, G. (1989). Automatic signature verification and writer identification - the state of the art. Pattern Recognition, 22(2), pp.107-131.

Proyecto e-DemoFirma. (2015). Piloto demostrador de firma biométrica, ATVS y Tecnologías de la Información, Universidad Autónoma de Madrid.

Proyecto e-BioFirma. (2014). Mejora de Algoritmos Biométricos de Comparación de Firmas Digitalizadas. Contrato de investigación entre Universidad Autónoma de Madrid y Cecabank.

Tolosana, R., Vera-Rodríguez, R., Ortega-García, J., y Fierrez, J. (2015). Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification. IEEE Access, 3, pp. 478 - 489.

Vera-Rodríguez, R., Tolosana, R., Ortega-García, J., y Fierrez, J. (2014). e-BioSign: Stylus- and Finger-Input Multi-Device Database for Dynamic Signature Recognition. Proc. 3rd International Workshop on Biometrics and Forensics (IWBF), IEEE Press.

Vivaracho-Pascual, C. y Pascual-Gaspar, J.M. (2012). On the use of mobile phones and biometrics for accessing restricted web services. IEEE Trans. Syst. Man Cybern. C, Appl. Rev., 42, (2), pp. 213-222.