Sistema Avanzado de Verificación de la Asistencia a Clase por Medio de la Firma

Moises Diaz*, Miguel Angel Ferrer*, Cristina Carmona*
*Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC)
Universidad de Las Palmas de Gran Canaria, Spain
Email: {mdiaz, mferrer, ccarmona}@idetic.eu

***Resumen*—Motivados con la norma del Espacio Europeo de Educación Superior (EEES) de evaluar la asistencia a clase, los profesores recogen las firmas manuscritas de sus alumnos matriculados como evidencia de su asistencia. Esta evidencia es susceptible de ser impostada mediante la falsificación de las firmas de aquellos alumnos que no asisten a clase. Aprovechando la aceptación de este medio que verifica la asistencia a clase, en este artículo se propone un sistema basado en las nuevas tecnologías para automáticamente verificar las firmas manuscritas de los alumnos. Así mismo, en este artículo se proponen y se comparan dos alternativas de sistemas de verificación automática de firmas capaces de detectar a los impostores.**

Palabras clave: Verificación automática de firmas manuscritas, sistemas avanzados, ayudas al profesor.

I. Introducción

La evaluación continua y la asistencia a clase son elementos que puntúan en la calificación final de un alumno de acuerdo a las normativas del Espacio Europeo de Educación Superior (EEES). Esto requiere de un sistema que de constancia formativa y asistencia continuada del alumno a la universidad. La asistencia del alumno se puede contabilizar a través de diferentes medios. La forma más común es a través de hojas de firmas, la cual consiste en tantos folios como sean necesarios que contienen el nombre completo de los estudiantes y un recuadro para que evidencien su asistencia a través de la firma manuscrita. El EEES asume que una vez la clase finaliza, el profesor contabiliza el número de asistencias y asigna la puntuación respectiva.

Por la parte del profesor, este sistema cuenta con dos deficiencias fundamentales que se discuten a continuación:

1. *Muchos alumnos.* En asignaturas donde hay más de 50 asistentes matriculados, la labor de contar qué alumno asistió no suele ser meticulosa, además de aburrida y de baja motivación para el docente. Se puede decir que a más alumnos, menor el grado de atención en la verificación manual de firmas.
2. *Muchas asignaturas*. Los factores negativos mencionados anteriormente se acrecientan cuando el número de asignaturas a cargo del docente es mayor.

Estos motivos, entre otros, ha motivado a los estudiantes a cometer fraudes en el sistema actual de evaluación de la asistencia a clase. Estos ataques se producen cuando el alumno que asiste a clase firma por su compañero que no asistió. Este tipo de fraudes o "ataques" se dividen en dos categorías:

Figura 1. Esquema de trabajo en 4 pasos: i) hojas de firmas, ii) escáner, iii) ordenador, iv) resultados

1. *Ataque sin esfuerzo*. Se produce cuando el impostor que firma no conoce la firma del compañero ausente y firma de manera arbitraria.
2. *Ataque cuidadoso*. Se produce cuando el impostor tiene conocimiento de la firma de su compañero y reproduce una firma impostora con un alto parecido a una firma genuina real.

Desde la década de los 80 hasta hoy [1]–[3], los sistemas automáticos de verificación de firmas por computador han ido mejorando y suponen un avance considerable en la era de la comunicación. Estos sistemas usan un conjunto de firmas que entrenan un modelo computacional. Una vez el modelo es entrenado, los sistemas son testeados con firmas genuinas (hechas por el firmante auténtico) y firmas no genuinas. Las firmas no genuinas atacan a los modelos produciendo dos tipos de ataque. El primer ataque se realiza con firmas que no tienen ningún parecido a las firmas del modelo, *ataque sin esfuerzo*. Este ataque es común en fraudes relativos a pagos con tarjetas de créditos donde el impostor debe firmar una transacción hecha con una tarjeta de crédito robada, por ejemplo. El segundo ataque se realiza deliberadamente conociendo la firma a impostar, *ataque cuidadoso*. Este ataque es el más difícil de determinar y depende de la habilidad del impostor.

La alta similitud entre los fraudes en el sistema actual de evidenciar la asistencia a clase y los sistemas automáticos de verificación de firma manuscrita hace pensar que su combinación podría mejorar el espíritu del EEES en cuanto a la evaluación de la asistencia a clase se refiere.

Debido a ello, este artículo propone un sistema completo de ayuda al profesor en la tarea de verificación de firmas. El sistema consiste en escanear de manera automática múltiples hojas de firmas. Luego, de manera automática un software determinará cuales de esas firmas son fraudulentas o no con un cierto error. El diagrama de trabajo es mostrado en la figure 1. Brevemente, para poder hacer uso de dicho sistema, el profesor

ISBN: 978-84-608-3145-7

Figura 2. Hoja de firmas real no útil para el sistema automático de verificación.

sólo necesitaría de materiales como un escáner y un ordenador, encontrados a menudo en los despachos o secretarías de los departamentos.

El resto del artículo es organizado como sigue: Algunas consideraciones sobre cómo se debe configurar el escáner son dadas en la sección 2. La sección 3 está dedicada al diseño de las hojas de firmas. Un caso de estudio con firmas reales y dos sistemas de verificación de firmas son discutidos en la sección 4. El artículo termina con las Conclusiones en la sección 5.

II. Configuración del escáner

Idealmente, para facilitar el procedimiento, sería deseable contar con un escáner de alimentación automática con el fin de depositar sobre la superficie del dispositivo todas las hojas de firmas.

Debido a que los sistemas de verificación de firmas operan en su mayoría con imágenes en escala de grises - incluso con imágenes en blanco y negro - configurar la calidad del escáner adecuadamente ayudará al sistema informático.

Una vez que el escáner se haya conectado al ordenador, habrá que ser cuidadosos en los ajustes de los “DPIs”. DPIs es un término anglosajón que significa puntos por pulgadas. Esta unidad de medida establece la resolución de escaneo de una imagen. A mayor número de DPIs, mayor será la calidad del escaneo.

Los DPIs varían según la aplicación concreta. Por ejemplo, si queremos obtener una imagen para una página web un resultado aceptable rondaría los 75-100 DPIs. En cambio, una imagen fotográfica básica sería aceptable con 150 DPI y una de calidad estaría en los 300 DPIs. Para aplicaciones técnicas concretas, una configuración deseable ronda desde los 600 hasta los 1200 DPIs.

Nuestro caso se encuentra en aplicación técnica. Sin embargo, a mayor resolución mayor el tiempo de procesamiento. El compromiso técnico entre tiempo de procesamiento y calidad sugiere que para la verificación automática de firmas, 600 DPIs es una buena configuración.

III. Hoja de Firmas

Una vez la hoja de firma es escaneada, esta se guarda en algún formato específico y en escala de grises o en color. La primera tarea del sistema informático consiste en segmentar las firmas de dicha hoja. Es decir, separar cada firma independiente para almacenarla en un fichero. Este tipo de segmentación automática podría complicar el sistema informático en algunos

Figura 3. Propuesta de hoja de firmas para el control de asistencia a clase.

casos. Un ejemplo de hoja de firmas real muy complicado de segmentar se ilustra en la figure 2.

Debido a ello, algunas consideraciones sobre el diseño de la hoja de firmas han de ser propuestas.

Las firmas españolas normalmente están compuestas por texto y rúbrica. Estas firmas suelen ser ovaladas donde el radio horizontal es mayor que vertical. La relación aproximada de radios es de 0.5. Debido a ello, conviene que el tamaño donde el alumno tiene que firmar guarde tales proporciones.

Además, si el espacio es suficientemente mayor, podremos ayudar al proceso de segmentación automático evitando la superposición de una firma con otra así como la superposición de una firma con el recuadro.

Por otro lado, si el tamaño del cuadro de firma fuese pequeño la forma de la firma podría verse afectada, modificando la variabilidad intra personal y empeorando así el funcionamiento del sistema automático de verificación de firmas.

Debido a ello, se propone un diseño de hoja de firmas como el que se muestra en la figure 3. Cabe mencionar que la hoja de firmas de la figure es ficticia y, por lo tanto, ni los nombres ni las firmas corresponden a alumnos reales. Una de las ventajas de esta hoja es que el cuadro de escritura es bastante amplio, de 8 cm x 4 cm, permitiendo que el alumno firme con comodidad. Además, ya que el color de los bolígrafos suelen ser azul, rojo, negro o incluso verde, el programa informático mejoraría la separación individual de las firmas si el color del cuadro fuese diferente, por ejemplo color ambar, cuyo código es #FFBF00.

IV. Caso práctico

Supongamos que el sistema de verificación de firmas manuscrito es probado en una clase de 100 alumnos. Estos sistemas informáticos crean un modelo usando firmas genuinas de entrenamiento. Debido a ello, supongamos que el profesor en una sesión de tutoría o en una de las primeras sesiones de clases, por ejemplo, recolecta de cada alumno 8 ejemplares de sus firmas.

Con estas firmas, supongamos ahora que tenemos los dos siguientes sistemas automáticos de verificación de firmas:

ISBN: 978-84-608-3145-7

1. **Sistema A: Características geométricas + HMM. [4]** La firma está parametrizada usando coordenadas cartesianas y polares. Ambas características se combinan de acuerdo a la puntuación obtenida por el clasificador de manera individual. Los parámetros cartesianas consisten en muestras equidistantes de la altura y la longitud de la envolvente de la firma, más el número de veces que la línea vertical y horizontal corta el trazo de firma. En coordenadas polares los parámetros son muestras equidistantes del radio de la envolvente más el área del trazo total de cada sector. Un modelo oculto de Markov (HMM) con múltiples observaciones discretas de izquierda a derecha modela las características de cada firmante. La clasificación (evaluación), decodificación, y los problemas de formación se resuelven con el algoritmo adelante-atrás, el algoritmo de Viterbi, y el algoritmo de Baum-Welch. El método de inicialización es el método de ocupaciones iguales.
2. **Sistema B: Características de textura + SVM. [5]** Este sistema se basa en características de textura como el patrón local binario (LBP) y el patrón derivado local (LDP). La firma se transforma en las imágenes LBP y LDP y se dividen en 12 sectores. Se elabora el histograma de cada sector, luego se concatenan todos los histogramas individuales y su dimensión se reduce con la Transformada Discreta del Coseno (DCT) obteniendo dos vectores de características separadas de acuerdo con los operadores de LBP y del LDP. La combinación se realiza según la puntuación de cada una por separado y se evalúa a través de una suma ponderada. El clasificador se basa en una máquina de soporte vectorial [6]. Este sistema habría ocupado el segundo lugar con un error global (OE) de 11,4 % en la muy dura competición de verificación de firmas 4NSigComp2010 [7] (el sistema ganador tenía un 8,9 % OE, mientras que el resto de algoritmos presentaron resultados en torno al 16 %).

Mientras el tiempo computacional promedio de verificación de una firma es de 7 s para el sistema A, el sistema B consume unos 5 s. Estos tiempos fueron medidos usando un PC con Ubuntu 12.04 LTS con Intel®Core™i7-3770 CPU @ 3.40 GHz × 8, 15.6 GiB RAM de memoria y 64 bits.

Además, asumimos que por cada firmante tenemos recolectadas 15 firmas genuinas y 24 firmas falsificadas. Con todo este conjunto de firmas, analizamos los dos tipos de ataques:

1. *Ataque sin esfuerzo*. Para este ataque usaremos una firma genuina del resto de estudiantes para cada uno de los alumnos registrados, es decir 99 ataques para cada alumno. En total, el sistema contabilizará 100 x 99 = 9900 ataques sin esfuerzo. Cada ataque nos dará un valor y con él construiremos la curva de falsa aceptación "FAR". Esta curva analiza cuanto de esos ataques no han sido detectados por nuestro sistema.
2. *Ataque cuidadoso*. De manera análoga, usaremos las firmas que deliberadamente han sido falsificadas para construir la curva de falsa aceptación (FAR) relativa a este ataque. En total, este ataque contabilizará 100 x 24 = 2400 valores.

Para cada uno de los ataques se construirá la curva de falso rechazo (FRR). El falso rechazo contabiliza aquellas firmas genuinas que atacan al sistema y el sistema erróneamente las clasifica como falsas. Como por cada usuario disponemos de 15 firmas, en total tendremos 100 x 15 = 1500 valores para la curva FRR.

Para obtener un escalar que describa el error del sistema, en este tipo de aplicaciones se usa el punto donde la curva FRR corta con la curva FAR. Ese punto de corte es conocido como el ratio de igual error (ERR) y representa el mismo error en el acierto o en el rechazo de un sistema biométrico.

Debido a que tenemos dos sistemas y hemos considerado dos ataques, los resultados experimentales se muestran en la figure 4. Nótese que las firmas han sido extraídas de la base de datos GPDS, completada en su mayoría por estudiantes universitarios de Ingeniería de Telecomunicaciones de la Universidad de Las Palmas de Gran Canaria.

IV-A. Discusión

El caso práctico ha mostrado el error que tienen dos sistemas de verificación de firmas que se encuentran en el estado del arte científico. Dicho error se localiza en el punto de trabajo donde la falsa aceptación es igual al falso rechazo.

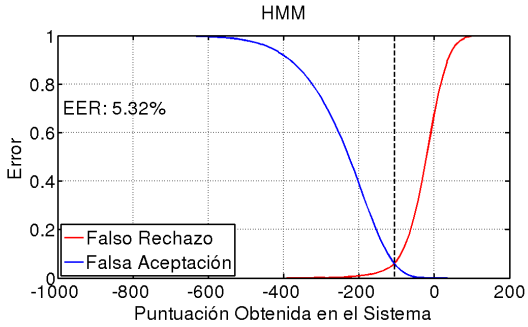
The computational time to generate a duplicated signature from a seed is less than 5 sec in average. This time is calculated using the duplicator on a regular PC Ubuntu 12.04 LTS with Intel®Core™i7-3770 CPU @ 3.40 GHz × 8, 15.6 GiB RAM memory, 64 bits. Nevertheless, for the same hardware, the computational time depends on the size of input image. The signature duplicator has been made publicly available for researching purposes at no cost in the GPDS group web site.

Es posible, que el profesor desee que su sistema sea más restrictivo y más transparente para él y, por tanto, quiera reducir el falso rechazo, es decir, reducir el número de firmas genuinas que el sistema rechaza como firmas genuinas y las clasifica como impostoras. En ese caso, el umbral podría desplazarse a la derecha en las gráficas presentadas en la figure 4. En caso contrario, asumiendo que el profesor quiere ser más transparente de cara al alumno y no darle importancia a que alguna firma impostora sea clasificada como genuina, el umbral del error del sistema podría desplazarse a la derecha. El efecto en el sistema es el aumento del error en la falsa aceptación, es decir, el número de firmas impostoras que son clasificadas como verdaderas será mayor.

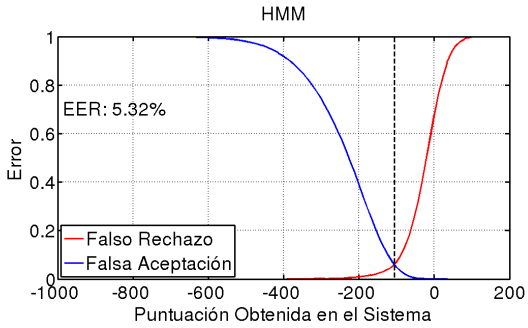
En otras palabras, si los sistemas funcionaran en el punto de control óptimo, el profesor podría ver sombreado en rojo, por ejemplo, aquellos alumnos que el sistema rechaza como posibles impostores. Sin embargo, si el profesor quisiera ser menos restrictivo y ver menos alumnos sombreados, podría reducir el punto de control. En caso de que quisiera ser más restrictivo y detectar más posibles impostores, tendría que mover el punto de operación hacía la derecha.

Cabe mencionar que hay que ser cautos a la hora de tomar medidas con aquellos alumnos que suelen aparecer en rojo. Brevemente, podrían suceder dos hipótesis: que ciertamente el sistema haya sido capaz de detectar a algún tramposo o que la variabilidad intra personal de las firmas de ese alumno sea

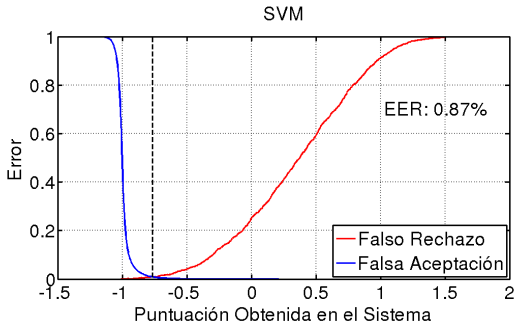
ISBN: 978-84-608-3145-7



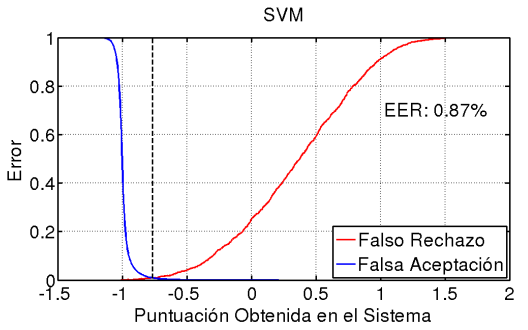
(a) Ataque sin esfuerzo, sistema A



(b) Ataque cuidadoso, sistema A



(c) Ataque sin esfuerzo, sistema B



(d) Ataque cuidadoso, sistema B

Figura 4. Resultados de los sistemas a diferentes tipos de ataque.

tan grande que el sistema no sea capaz de clasificarlo bien. Si la segunda hipótesis fuese aceptada, el sistema requerirá de más firmas genuinas de dicho alumno con el fin de modelarlo mejor.

V. Conclusiones

De acuerdo a la normativa común del Espacio Europeo de Educación Superior (EEES) de evaluar la asistencia a clase, la firma manuscrita ha sido extensamente usada para tales fines. Contrario al procedimiento manual/visual de verificar los asistentes matriculados a clase, en este trabajo se propone el diseño de un sistema avanzado de verificación de firmas por ordenador.

Dos son los fraudes detectados durante el proceso de verificación de firmas: ataque sin esfuerzo y ataque cuidadoso. El presente artículo discute la configuración del sistema y propone un caso práctico basado en verificadores del estado del arte. Los resultados obtenidos animan a que el docente se plantee la opción de usar estos sistemas con el fin de mejorar la gestión docente.

Una línea futura a partir de este trabajo es una investigación en la pregunta: ¿quién ha falsificado mi firma? Aunque la literatura ha tratado esta pregunta [8], un estudio dual sobre qué firma es falsa y quién la falsificó podría completar este artículo, asumiendo que el falsificador es alumno matriculado y también ha dejado su firma original en la hoja de firmas.

Agradecimientos

M. D. está apoyado con un contrato de investigador en formación por la ULPGC. Este estudio está apoyado por el gobierno de España a través del proyecto de investigación MCINN TEC2012-38630-C04-02.

Referencias

[1] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification — the state of the art," *Pattern Recognition*, vol. 22, no. 2, pp. 107 – 131, 1989.

[2] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 38, no. 5, pp. 609–635, 2008.

[3] M. Diaz-Cabrera, A. Morales, and M. A. Ferrer, "Emerging issues for static handwritten signature biometric," in *Advances in Digital Handwritten Signature Processing. A Human Artefact for e-Society*. Giuseppe Pirlo, Donato Impedovo, Michael Fairhurst, 2014, pp. 111–122.

[4] M. Ferrer, J. Alonso, and C. Travieso, "Offline geometric parameters for automatic signature verification using fixed-point arithmetic," *Pattern Analysis and Machine Intelligence, IEEE Transactions on*, vol. 27, no. 6, pp. 993–997, June 2005.

[5] M. Ferrer, J. Vargas, A. Morales, and A. Ordonez, "Robustness of offline signature verification based on gray level features," *IEEE Trans. on Information Forensics and Security*, vol. 7, no. 3, pp. 966–977, 2012.

[6] J. A. K. Suykens, T. V. Gestel, J. D. Brabanter, B. D. Moor, and J. Vandewalle, *Least Squares Support Vector Machines*. Singapore: World Scientific, 2002.

[7] M. Blumenstein, M. Ferrer, and J. Vargas, "The 4nsigcomp2010 offline signature verification competition: Scenario 2," in *Frontiers in Handwriting Recognition (ICFHR), 2010 International Conference on*, 2010, pp. 721–726.

[8] M. Ferrer, A. Morales, J. Vargas, I. Lemos, and M. Quintero, "Is it possible to automatically identify who has forged my signature? approaching to the identification of a static signature forger," in *Document Analysis Systems (DAS), 2012 10th IAPR International Workshop on*, March 2012, pp. 175–179.

ISBN: 978-84-608-3145-7

Aceptabilidad del Uso de Sistemas Biométricos en el Aula

Moises Diaz*, Ester González-Sosa†, Aythami Morales†, Patricia Henríquez* and Miguel Angel Ferrer*
*Instituto Universitario para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC)
Universidad de Las Palmas de Gran Canaria, España
Email: {mdiaz, phenriquez, mferrer}@idetic.eu †Biometric Recognition Group - ATVS
EPS, Universidad Autónoma de Madrid, España
Email: {ester.gonzalezs, aythami.morales}@uam.es

***Resumen*—La evidencia de que el alumnado matriculado asiste a clase se realiza clásicamente a través de la firma manuscrita. El auge reciente de los sistemas biométricos ofrece alternativas innovadoras al método clásico de firmas manuscritas. En este artículo presentamos los resultados de la aceptación de varios sistemas biométricos en el aula encuestando a dos grupos de estudiantes. El primer grupo estaba formado por 100 alumnos que usaron un sistema multibiométrico durante cuatro meses en condiciones controladas. Estos sistemas estaban basados en dos tipos de rasgos biométricos: por un lado la cara y la mano como rasgos físicos y la firma dinámica como rasgo de comportamiento. El segundo grupo, formado también por 100 alumnos, utilizó un sistema biométrico basado en la mano sin contacto durante el mismo tiempo y bajo el mismo entorno experimental. Este segundo experimento comenzó un año más tarde que el primero y aproximadamente el 30 % de alumnos participaron en ambas experiencias. Después de los dos experimentos, los alumnos realizaron de manera anónima una encuesta con varias preguntas acerca de la aceptación de los diferentes sistemas biométricos utilizados. De la respuesta se concluye que la biometría de la mano es el rasgo más aceptable comparado con el resto de rasgos usados.**

Palabras clave: Biometría, aceptación del usuario, sistemas de identificación basados en la firma, mano y cara.

I. Introducción

A partir de los nuevos planes de estudio, la asistencia al aula se ha convertido en un elemento que interviene en la puntuación final de cualquier asignatura. Clásicamente, la firma manuscrita ha sido el elemento clave que evidencia la asistencia de un alumno a clase. A través de varias hojas con los nombres de todos los matriculados en una asignatura, los alumnos firman en aquellos recuadros donde se encuentra su identificador, a menudo el nombre y apellidos. Posteriormente, el profesor revisa manualmente que alumno matriculado asistió para darle la puntuación correspondiente.

Sin embargo en la nueva era de la información, los métodos automáticos que usan otro tipo de identificadores han mostrado su potencial tecnológico para verificar la identidad de las personas. En este contexto surge la biometría, la cual juega un papel cada vez más importante en este tipo de tareas. Los procesos de reconocimiento biométrico permiten la identificación del individuo a través de rasgos físicos o de comportamiento. Por lo general, las diferentes tecnologías biométricas son evaluadas por medio de las siguientes medidas de calidad:

1. Universalidad: el rasgo biométrico considerado debe estar presente en todos los individuos.
2. Unicidad: Debe ser capaz de discriminar entre diferentes usuarios.
3. Invariante: debe ser un rasgo que permanezca en el tiempo lo más estable posible sin cambios bruscos.
4. Accesibilidad: facilidad de adquisición del rasgo.
5. Rendimiento: precisión, velocidad y robustez de la tecnología utilizada.
6. Vulnerabilidad: Robustez del sistema frente a ataques.
7. Aceptabilidad: grado de aprobación de una tecnología.

La universalidad, unicidad, invariante, accesibilidad, rendimiento y vulnerabilidad han sido los factores más estudiados en los últimos 10 años por lo general en términos de medidores FAR, FRR, EER, curvas DET, etc. En cambio, pocos estudios han enfocado la atención en la aceptación del usuario.

Buscar el éxito en la implementación de una nueva tecnología implica considerar su aceptación entre los potenciales usuarios. ¿Qué hace que los usuarios acepten o rechacen una nueva tecnología? Uno de los factores más determinantes es la facilidad de uso percibida. Es decir, el grado en que una persona cree que el uso de un sistema en particular queda libre de esfuerzos. El modelo de aceptación de tecnología [2] es un modelo general conocido para evaluar tal éxito. La utilidad percibida y la facilidad de uso constituyen factores que influyen en la decisión acerca de cómo y cuándo usar un nuevo sistema biométrico

En [3] se presentó un estudio de aceptabilidad percibida de los sistemas biométricos. Los 76 usuarios respondieron diferentes preguntas sobre la aceptabilidad y la sensibilidad de la política de privacidad. Se realizó la misma encuesta para rasgos de comportamiento (firma, voz y golpe de teclado) y rasgos físicos (huellas dactilares, geometría de la mano y de la retina). En general, los sistemas basados en rasgos de comportamiento muestran mejores resultados que los rasgos físicos. Además, los 76 encuestados indicaron que todos los sistemas biométricos fueron percibidos como menos aceptables que el enfoque tradicional de la contraseña. Es importante destacar que éste fue un estudio de percepción de la aceptabilidad y no del uso del sistema biométrico. Además, cabe mencionar que los usuarios de dicho estudio no fueron interrogados acerca de su experiencia en el uso de dichos sistemas biométricos.

Otro factor interesante relacionado con la aceptabilidad es la

ISBN: 978-84-608-3145-7

"familiaridad", la cual puede ser definida como el proceso en el que un usuario se adapta a usar un dispositivo biométrico. En [4] se estableció un modelo de los procesos de familiaridad a partir de la geometría de la mano con el fin de mostrar cómo funciona este concepto con la experiencia de uso de un sistema real. ¿Cómo afecta la familiaridad a la calidad de la imagen adquirida? En [5] se trata de responder a esta pregunta. Centrado en la biometría de huellas dactilares, los autores se encontraron con que la familiaridad sin retroalimentación, entendida como una imagen mostrada al usuario de su rasgo biométrico recién adquirido, no afectaba a la calidad de las impresiones.

Obviamente, el rendimiento está relacionado con la fuerte aceptación de los usuarios. Si un sistema biométrico tiene un mal rendimiento (alto EER[1]) el usuario no tendrá confianza en él y será rechazado. Además, la aceptación del usuario también depende de la evaluación subjetiva de la velocidad y la facilidad de la interacción persona-máquina, es decir, la disponibilidad de los usuarios a interactuar con todas las acciones necesarias requeridas por la máquina. Aspectos como la *guía de usuario* también son importantes ya que los usuarios ocasionales tienden a olvidar los detalles de dicha interacción, tales como qué dedo se debe presentar.

Cabe mencionar que cuando el sistema requiere más cooperación del usuario, éste será menos aceptado. Por el contrario, menos interacción podría traducirse en mayor procesamiento de datos y, por lo tanto, en mayor consumo de tiempo y de nuevo menor aceptación del usuario. Es por ello que se requiere de un compromiso tecnológico entre ambos términos.

Otras razones por las que algunos usuarios podrían negarse a realizar la prueba biométrica son debidas a la violación de la intimidad, problemas de higiene o por motivos religiosos.

Más allá de las tasas de reconocimiento de los sistemas biométricos usados, este artículo se centra en la aceptabilidad del uso de dispositivos multibiométricos en el aula, bajo un escenario de control y en condiciones realistas. El artículo queda dividido como sigue: en la sección II se describen los dos escenarios considerados, en la Sección III se presentan las preguntas formuladas a los alumnos acerca de la aceptación de las diferentes biometrías y la discusión de las respuestas de los usuarios. El artículo se cierra con las conclusiones.

II. Descripción de los escenarios

Se han realizado dos experimentos. El primero utiliza la mano y la cara como rasgos biométricos físicos y la firma como rasgo biométrico de comportamiento. La figura 1 muestra un ejemplo de estos rasgos biométricos. En total, 100 alumnos matriculados asistieron al experimento una vez por semana durante 4 meses.

Durante el experimento, se pidió a los alumnos introducir un número de identificación personal (PIN) y su identidad se verificó pidiendo dos de los tres sistemas biométricos seleccionados al azar. El sistema concede el acceso si ambas biometrías están de acuerdo y proporcionan una verificación positiva de la identidad del alumno. En nuestros experimentos, el rendimiento o EER, es 2 %.

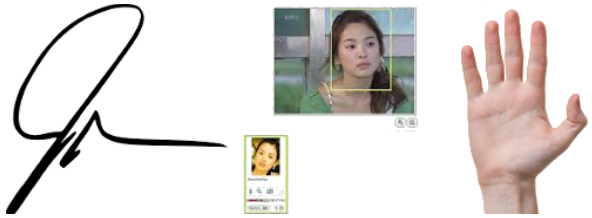


Figura 1. Rasgos biométricos usados en el reconocimiento: a la izquierda la firma manuscrita, la cara en el centro y la mano a la derecha.

La tecnología basada en la cara es un ejemplo de sistema sin contacto con una mínima interacción del alumno. La labor del alumno consiste básicamente en poner la cara delante de un dispositivo de adquisición. Para ello se ha implementado un sistema biométrico de cara sencillo compuesto por un PC y una cámara web. Para la biometría basada en la mano, hemos propuesto un dispositivo biométrico base de mano sin contacto [5]. Con el fin de mejorar la aceptabilidad del usuario, se muestra en la pantalla del PC una plantilla con la forma de la mano y estando obligado el alumno a ajustar su mano derecha a dicha plantilla o máscara. La máscara de la mano en la pantalla es lo más amplia posible con el fin de facilitar el procedimiento de ajuste mano-máscara. Cuando la superposición entre la mano del usuario y la máscara supera el 75 %, la mano queda parametrizada. Las imágenes de la mano fueron adquiridas con una cámara web usando la banda infrarroja.

La firma dinámica fue adquirida mostrando un cuadro en la pantalla del PC y pidiendo al usuario que firmase dentro de un cierto área. Este rasgo biométrico requiere del contacto del lápiz con la pantalla.

La tableta digital fue construida en un dispositivo que incluía una webcam y una iluminación IR para la biometría basada en la mano, así como una fuente de alimentación con un relé que abría la puerta. El dispositivo se puede ver en la figura 2.

La inscripción al sistema se realizó con la ayuda de un supervisor que explicaba cómo utilizarlo. Las adquisiciones sucesivas se realizaban sin supervisión. Los alumnos hacían uso del experimento una vez por semana durante cuatro meses.

El segundo experimento se realizó solamente con la biometría basada en la mano sin contacto. La posición de la mano durante la adquisición fue cambiando, desde la posición vertical en el primer experimento a un plano horizontal en el segundo. La experimentación se llevó a cabo en el mismo lugar que el primer experimento. Además, cabe mencionar que el segundo experimento comenzó un año más tarde que el primero. Un 30 % de los alumnos participaron en ambos experimentos. El dispositivo utilizado en este caso se puede ver en la figura 2.

III. Encuestas de satisfacción

El último día de cada experimento, los alumnos respondían a varias preguntas acerca de la aceptación del dispositivo usado. Las preguntas se dividían en dos grupos. En el primer

[1]EER, *ratio de igual error*, es un escalar que representa el mismo error en el acierto o en el rechazo de un sistema biométrico

ISBN: 978-84-608-3145-7

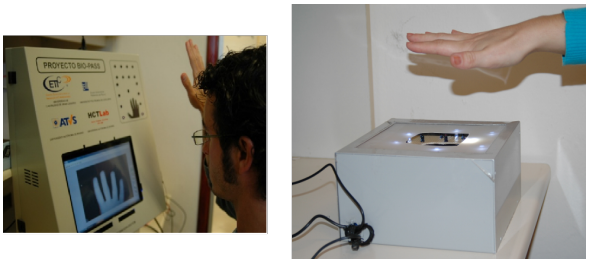


Figura 2. Dispositivo usado en el primer y segundo experimento (izquierda y derecha, respectivamente).

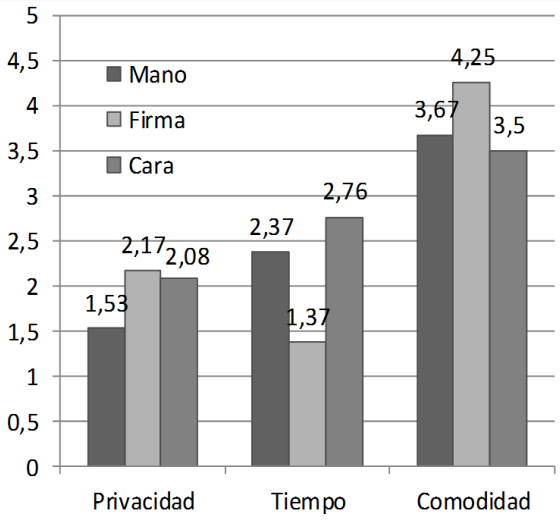


Figura 3. Percepción de los alumnos en el primer experimento

grupo se comparaban los diferentes sistemas biométricos. Las preguntas trataban de medir la percepción de los usuarios en las diferentes tecnologías: la firma, la cara y la mano sin contacto. En el segundo grupo de preguntas se comparaban los dos experimentos y la percepción de los alumnos acerca de los sistemas de identificación biométricos. Las preguntas en el primer experimento fueron:

1. ¿Siente que el sistema ataca su privacidad? Donde 5 corresponde a una fuerte percepción de ataque de la privacidad - 4 fuerte ataque de privacidad - 3 ataque normal de privacidad - 2 poco ataque de privacidad - 1 ataque bajo de la privacidad y 0 una muy baja percepción de ataque de la privacidad.
2. El tiempo necesario para realizar la autenticación es: Donde 5 corresponde a demasiado - 4 excesivo - 3 normal - 2 bueno - 1 bajo y 0 muy bajo.
3. ¿Es cómodo el sistema? Donde 5 corresponde a sistema totalmente cómodo - 4 muy cómodo - 3 cómodo - 2 poco cómodo - 1 no muy cómodo y 0 nada confortable.

Los resultados se muestran en la figura III.

Para el segundo experimento, las preguntas acerca la percepción del alumno sobre el sistema fueron:

1. ¿Siente que el sistema ataca su privacidad? Donde 5 corresponde a una fuerte percepción de ataque de la privacidad - 4 fuerte ataque de privacidad - 3 ataque normal de privacidad - 2 poco ataque de privacidad - 1 ataque bajo de la privacidad y 0 una muy baja percepción de ataque de la privacidad.
2. ¿Se considera el sistema una solución higiénica? Donde 5 corresponde a una percepción totalmente higiénica - 4 buena percepción de la higiene - 3 percepción higiénica media - 2 mala percepción higiénica - 1 baja percepción higiénica y 0 muy baja percepción de la higiene
3. ¿Es cómodo el sistema? Donde 5 corresponde a sistema totalmente cómodo - 4 muy cómodo - 3 cómodo - 2 poco cómodo - 1 no muy cómodo y 0 nada confortable.

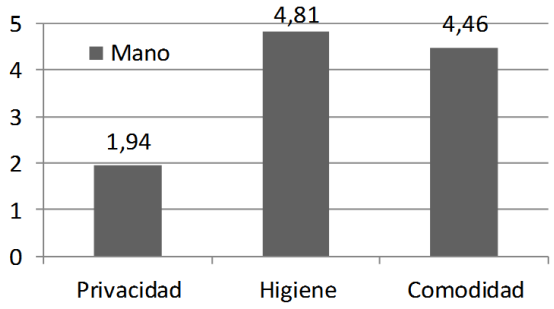


Figura 4. Percepción de los alumnos en el segundo experimento

La respuesta de los alumnos se ilustra en la figura III.

Adicionalmente, se cuestionó sobre cuál de las siguientes tecnologías era más invasiva: la mano sin contacto, la huella dactilar, la cara, la firma, el habla y el iris. Los alumnos respondieron que la tecnología que más invade su privacidad es la cara seguido en orden por la huella dactilar, el iris, el habla, la mano sin contacto y la firma.

En la figura 5 se muestra la comparación de las encuestas de satisfacción de ambos experimentos. En el primer experimento, cada persona utiliza los tres sistemas biométricos, un sistema que requiere el contacto (firma) y dos sistemas que no (cara y mano). Para el segundo experimento, el alumno sólo utilizó el sistema biométrico de la mano sin contacto. Las preguntas fueron:

1. ¿Prefiere los sistemas sin contacto en vez de los sistemas con contacto? Sí / No.
2. ¿Prefiere la identificación biométrica frente a los métodos de identificación clásicas (contraseñas, tarjetas ID)? Sí / No.
3. ¿Estaría usted dispuesto a utilizar el sistema biométrico de la mano sin contacto a diario? Sí / No.

La figura 5 muestra el porcentaje de respuesta “Sí” para ambos experimentos.

IV. Conclusiones

El presente artículo muestra la aceptabilidad de los sistemas de identificación de los alumnos que asisten al aula. A diferencia de los métodos clásicos, estos sistemas identifican automáticamente al alumno por sus rasgos biométricos, físicos o de comportamiento. La principal ventaja de esta tecnología es que el profesor puede prescindir de la tarea de verificar la asistencia del alumnado incorporando al aula tecnología de innovación.

ISBN: 978-84-608-3145-7

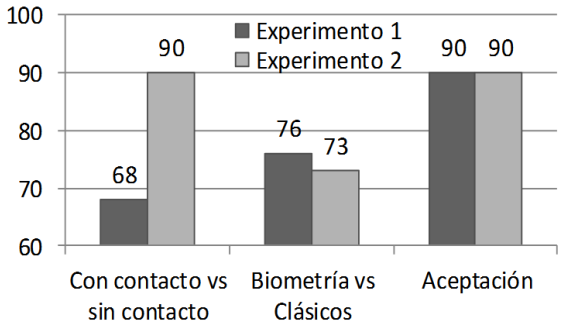


Figura 5. Comparación entre ambos experimentos

De acuerdo a los resultados mostrados, en general todos los sistemas obtuvieron una buena aceptación por parte de los alumnos. Comparando los resultados, de acuerdo a este estudio, el uso de la mano como identificador biométrico es el rasgo más aceptado. En este estudio, la mano ha obtenido una mejor respuesta en términos de privacidad. Sin embargo, cabe mencionar que la firma muestra la mejor respuesta en comodidad. Creemos que la respuesta se debe a que los alumnos están habituados a este tipo de sistemas. La firma es usada a menudo por los alumnos en el ambiente académico, por ejemplo, para verificar su asistencia a clase, además de otros ejemplos como en los pagos que hacen con las tarjetas de crédito o en bancos, etc. Para las nuevas tecnologías, la familiaridad es un factor importante en la aceptación del usuario.

Por otro lado, si el alumno está acostumbrado a usar sólo un tipo de biometría, el uso de dicha biometría parece invadir su privacidad. La experiencia del usuario con el sistema es un factor importante a tener en cuenta en este tipo de evaluaciones. En este estudio, tres de cada cuatro alumnos prefieren la identificación biométrica en contra de los métodos de identificación clásicas y nueve de cada diez usuarios están dispuestos a utilizar a diario el sistema biométrico de mano sin contacto.

Finalmente, con este tipo de sistemas, la evidencia de la asistencia a clase se registra de modo automático, evitando la fácil suplantación de identidad a través de una firma manuscrita, por ejemplo. Además, es una tarea que cada alumno puede realizar de manera independiente, liberando al profesor de llevar el control manual de la asistencia a clase de los alumnos matriculados.

AGRADECIMIENTOS

Los autores agradecen la colaboración de los alumnos que participaron en el presente estudio. M. D. está apoyado por un contrato de investigador en formación por la ULPGC. Este estudio está apoyado por el gobierno de España a través del proyecto de investigación MCINN TEC2012-38630-C04-02.

REFERENCIAS

[1] F. Davis, *Perceived usefulness, perceived ease of use, and user acceptance of information technology*. MIS Quarterly, 13(3): Pages(s). 319-340, 1989.

[2] F. Deane, K. Barrelle, R. Henderson and D. Mahar, *Perceived acceptability of biometric security systems*. Computers & Security. Volume 14, Issue 3, Pages 225-231, 1995.

[3] E.P. Kukula, S.J. Elliott, B.P. Gresock and N.W Dunning, *Defining Habituation using Hand Geometry* on IEEE Workshop on Automatic Identification Advanced Technologies, Page(s):242 – 246. 7-8 June 2007.

[4] M. Theofanos, B. Stanton, R. Micheals and S. Orandi *Biometric Systematic Uncertainty and the User* on First IEEE International Conference on Biometrics: Theory, Applications, and Systems, BTAS. Page(s):1 – 6, 27-29 Sept. 2007.

[5] A. Morales, M.A. Ferrer, J.B. Alonso and C.M. Travieso, *Comparing infrared and visible illumination for contactless hand based biometric scheme* on Security Technology, 2008. ICCST 2008. 42nd Annual IEEE International Carnahan Conference, Page(s):191 – 197, 2008.

ISBN: 978-84-608-3145-7