

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}@idetec.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

“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 EER¹) 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

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



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.

positiva de la identidad del alumno. En nuestros experimentos, el rendimiento o EER, es 2 %.

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



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

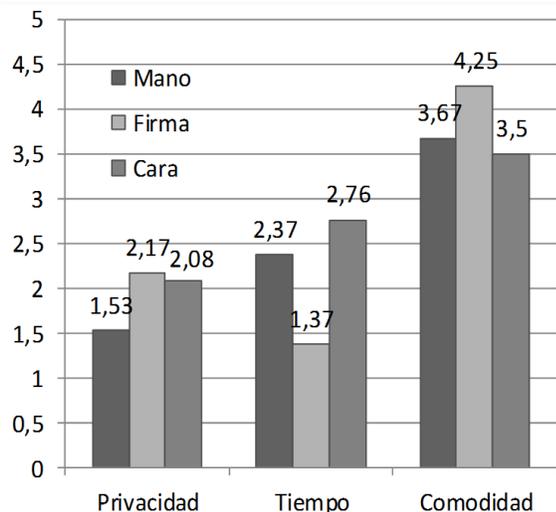


Figura 3. Percepción de los alumnos en el primer experimento

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

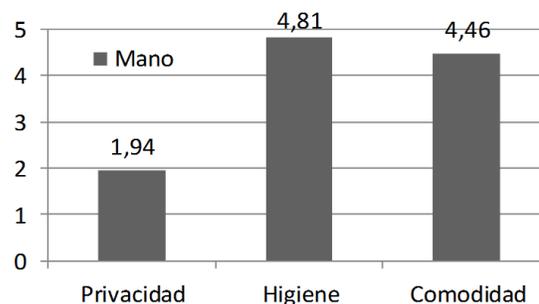


Figura 4. Percepción de los alumnos en el segundo experimento

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.

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.

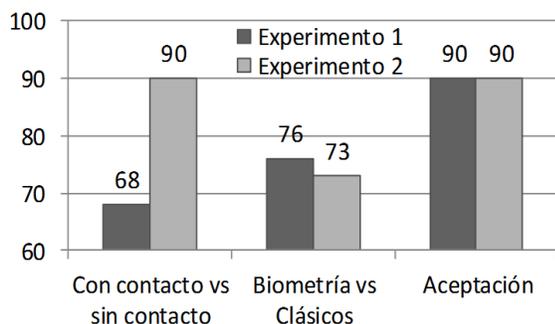


Figura 5. Comparación entre ambos experimentos

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.