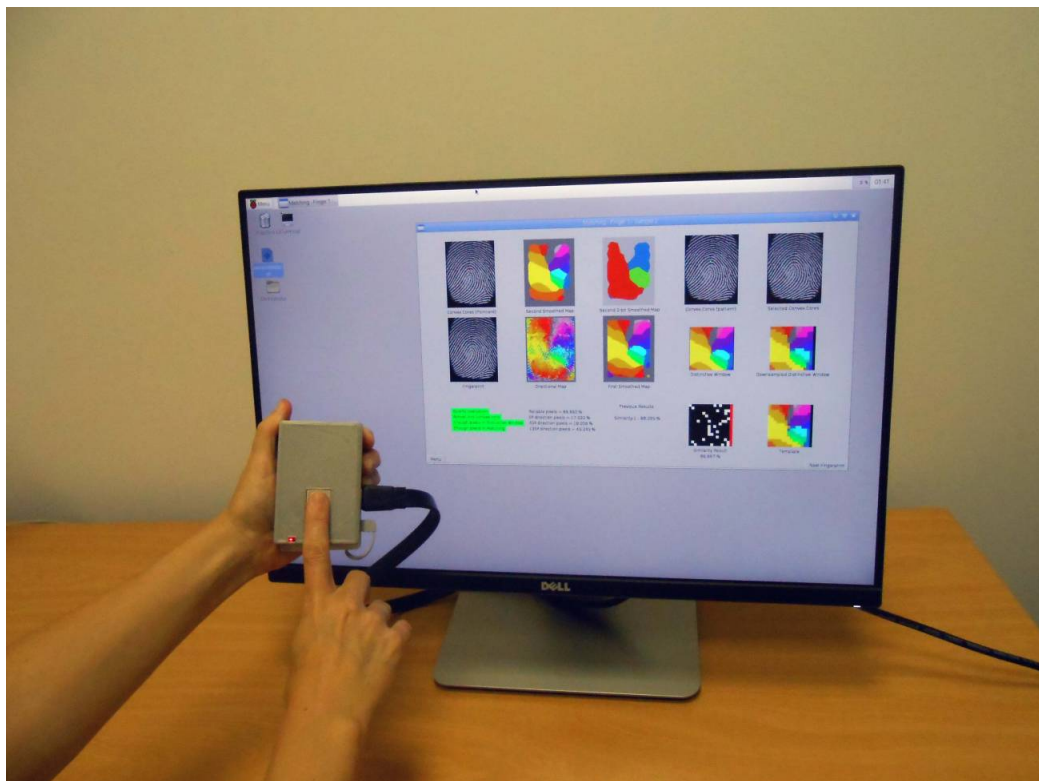


Patentan un nuevo método de identificación a través de huella dactilar

Investigadoras del Instituto de Microelectrónica de Sevilla han desarrollado un procedimiento seguro de autenticación mediante huella dactilar que requiere pocos recursos de procesamiento y memoria. Al mismo tiempo, han diseñado un dispositivo con un tamaño, coste y consumo reducidos que permite su aplicación a multitud de objetos de la vida cotidiana, como bolsos y llaves.

SINC

25/10/2017 11:33 CEST



Ejemplo de realización en la que el método se ejecuta conectada al sensor de huellas y a un monitor en el que una interfaz gráfica de usuario permite verificar todos los pasos de ejecución del método. / Fundación Descubre

Investigadoras del [Instituto de Microelectrónica de Sevilla](#) (IMSE-CNM), centro mixto de la [Universidad de Sevilla](#) y el [Consejo Superior de Investigaciones Científicas](#), han patentado una nueva técnica de autenticación personal a través de la marca dactilar para su proceso

mediante soluciones microelectrónicas de menor consumo, ya que requieren pocos recursos de procesamiento y memoria.

El nuevo método y su aplicación posibilitan no solo la identificación de un individuo en multitud de artículos, sino también la generación de claves asociadas a su persona para realizar transacciones electrónicas seguras.

Las expertas han simplificado los procesos de identificación al máximo para que puedan ser ejecutados por un circuito integrado con un tamaño, coste y consumo mínimos, lo que permite aprovechar las ventajas del reconocimiento de huella dactilar en cualquier artículo.

En la actualidad, el uso de la huella en el acceso a edificios, por ejemplo, o para determinadas aplicaciones en teléfonos móviles resulta habitual. Sin embargo, las investigadoras apuntan que son necesarias soluciones adecuadas en todo tipo de objetos que mantengan buenos resultados de autenticación y que el coste en *hardware* sea mínimo, incluyendo la pila o batería, mediante la biometría, es decir, a través del reconocimiento inequívoco de personas basado en uno o más rasgos físicos.

Es el caso de agendas privadas que contengan información sensible, carteras, maletas o bolsos, entre otros muchos artículos, en los que se quiera evitar de manera segura el acceso de cualquier persona. También es posible su aplicación en objetos en los que se requiere la autorización de individuos concretos para la ejecución fiable de transacciones, como pueden ser llaves, mandos a distancia o pulseras que monitorizan parámetros sobre la salud y luego los transmiten.

Los individuos pueden autenticarse ante un sistema autónomo con alguna parte de su cuerpo, como puede ser la voz, el rostro, el iris o las marcas dactilares

El planteamiento consiste en algoritmos sencillos que procesan datos binarios mediante operaciones matemáticas más simples que las utilizadas en otros sistemas conocidos. "La novedad de nuestra propuesta con respecto a otros métodos existentes consiste en que puede ejecutarse como

software en tiempo real en microcontroladores de bajo coste, o aplicarse mediante un circuito integrado de aplicaciones específicas más fácil de diseñar y con mejores prestaciones de velocidad y consumo”, indica la investigadora del Instituto de Microelectrónica de Sevilla, Iluminada Baturone, una de las inventoras de la patente.

La clave está en el cuerpo

A través de la biometría, los individuos pueden autenticarse ante un sistema autónomo con alguna parte de su cuerpo, como puede ser la voz, el rostro, el iris o las marcas dactilares. Los sistemas automáticos de identificación de huellas (AFIS, *Automatic Fingerprint Identification Systems*) están ampliamente extendidos actualmente y requieren dos fases de cálculo.

Por un lado, la extracción de características distintivas de la imagen de la impresión digital y, por otro, la comparación con las plantillas almacenadas. En estas aplicaciones, los individuos se registran previamente mediante sus señales dactilares. Posteriormente, cuando se quiere reconocer a una persona, se vuelven a extraer los rasgos de los dedos y se comparan con la base de datos. Las plantillas almacenadas deben protegerse muy bien porque representan las identidades digitales de los individuos.

Las técnicas usadas en este nuevo dispositivo ofrecen prestaciones competitivas en cuanto a la protección de las plantillas, ya que estas nunca salen del dispositivo y además pueden almacenarse de forma ofuscada, es decir, que incluso con ataques complejos al *hardware* del dispositivo no conseguirían obtener información sensible. “En términos de seguridad, es significativo que todo el proceso de extracción, almacenamiento y emparejamiento se pueda realizar en el mismo dispositivo, porque así las características distintivas de los individuos se circunscriben dentro de un perímetro mucho más pequeño, que, por tanto, es más fácil de controlar y defender”, añade la investigadora.

Al mismo tiempo, esta simplificación de algoritmos conlleva la reducción de precisión en el reconocimiento, pero el método permite compensarlo con el uso de varios dedos por parte del usuario. Según indica Baturone, las posibilidades que abre esta invención son múltiples, ya que puede aplicarse

en muchos contextos. Además, cumple con toda la normativa europea y norteamericana actual en materia de protección de datos, ya que la información sensible asociada a la identidad digital del individuo nunca sale del dispositivo, ni siquiera es necesario almacenarla en él.

La patente es uno de los resultados de las investigaciones que comenzaron en 2008 con el proyecto de excelencia 'Diseño microelectrónico para autenticación criptobiométrica' financiado por la Consejería de Economía y Conocimiento y que continuaron desarrollando las autoras en el contexto de un proyecto del subprograma INNPACTO financiado por el Ministerio de Economía y Competitividad y fondos FEDER.

A partir de este momento, las científicas trabajan en aprovechar el enfoque multi-biométrico, es decir, en incluir nuevos elementos que puedan añadirse al reconocimiento como podría ser el uso de la huella y los gestos de manera conjunta. También trabajan en extraer identidades digitales del hardware de los objetos para asegurar que no solo los individuos, sino también los dispositivos con los que interactuamos, sean de confianza y auténticos y que, por tanto, sean más robustos a suplantaciones y falsificaciones.

Derechos: **Creative Commons**

TAGS

HUELLA DACTILAR | PATENTE | MICROELECTRÓNICA |

Creative Commons 4.0

Puedes copiar, difundir y transformar los contenidos de SINC. [Lee las condiciones de nuestra licencia](#)

