International Interdisciplinary Congress on Renewable Energies, Industrial Maintenance, Mechatronics and Informatics
Booklets

RENIECYT 1702902 CONACYT

RENIECYT - LATINDEX - Research Gate - DULCINEA - CLASE - Sudoc - HISPANA - SHERPA UNIVERSIA - Google Scholar DOI - REDIB - Mendeley - DIALNET - ROAD - ORCID

Title: Biometric technological security for data and information protection

Authors: DOMÍNGUEZ-HERNÁNDEZ, Juan Pablo, CRUZ-GÓMEZ, Marco Antonio, TEUTLI-LEON, Margarita and POSADA-SANCHEZ, Ana Elena

Editorial label ECORFAN: 607-8695
BCIERMMI Control Number: 2021-01
BCIERMMI Classification (2021): 271021-0001

Pages: 10
RNA: 03-2010-032610115700-14

ECORFAN-México, S.C.
143 – 50 Itzopan Street
La Florida, Ecatepec Municipality
Mexico State, 55120 Zipcode
Phone: +52 1 55 6159 2296
Skype: ecorfan-mexico.s.c.
E-mail: contacto@ecorfan.org
Facebook: ECORFAN-México S. C.
Twitter: @EcorfanC

www.ecorfan.org

Holdings
Mexico Colombia Guatemala
Bolivia Cameroon Democratic
Spain El Salvador Republic
Ecuador Taiwan of Congo
Peru Paraguay Nicaragua

Introducción

La biometría consiste en medir las características del cuerpo humano con el fin de identificar un individuo. Para esto se debe elegir una característica dotada con fuerte variabilidad de un individuo a otro. La necesidad de incrementar la seguridad es prioridad en todo el mundo, no sólo por compañías privadas sino también por los gobiernos y las instituciones públicas. Debido a esto, sistemas de protección biométrica inteligente se han convertido en la principal opción de la seguridad. *Cortes, O. et. al. (2010).*

El investigador francés experto en biometría y creador del sensor para huellas FingerPrint, afirma que “una clave o llave no prueban que determinada persona es la que deba tener acceso a algo”. La biometría llena ese lugar, un sistema de este tipo verifica identidad, dado que es única e irrepetible, por lo que no hay forma de prestarlo o que se pierda. *Cortes, O. et. al. (2010).*

Metodología

Esta investigación tiene un análisis mixto, se irán definiendo los enfoques en diferencias que aplican tecnologías tanto cuantitativas como cualitativas, utilizando procesos sistemáticos, así como datos registrados y estimados.

Método Cuantitativo	Método Cualitativo
• Los datos cuantificables obtenidos mostrarán qué campo han abarcado al paso del tiempo, incluso identificar las dependencias que cuentan con esta tecnología • La aplicación del método cuantitativo fue necesaria para el análisis de causa y efecto en procesos secuenciales con el fin de predecir una hipótesis. *Hernández, 2010, p.275.*	• Esta investigación requiere un estudio no experimental y, por ende, fue necesario aplicar el método cualitativo. • Es metodológicamente un enfoque interpretativo en los sistemas biométricos, para definir así su confiabilidad. *Cortes, O. et.al. (2010).*

Metodología empleada para la obtención de datos biométricos en distintas instituciones

En primera instancia se tiene que:

Tanto las instituciones públicas como privadas hacen uso de la información que nosotros proporcionamos, datos que son confidenciales donde las dependencias públicas nos toman la delantera, al tramitar algún servicio que vaya de acuerdo a nuestra identidad hacen cumplir una serie de requisitos, los cuales van desde tomar fotos para credenciales, firmas e incluso dejar, huellas dactilares. *Díaz, V. (2013).*

Por ultimo se dice que:

Lo que se crea es un archivo histórico como ciudadano de nacionalidad mexicana, empezando a aparecer en el sistema, entre ellos hospitales y jefaturas del estado que son los únicos facultados para tomar información que está en la base datos para ser usada de manera segura y confiable. Habrá quienes pregunten de donde es que sacan toda nuestra información, no hay más que voltear al pasado, recordar cuando se proporciona una foto, firma o huellas dactilares, identificando de esta manera que todo registro es analizado y guardad *Díaz, V. (2013).*

Métodos de reconocimiento biométrico

Reconocimiento Facial o Rostro.

Los sistemas de biometría facial permiten identificar a una persona analizando las características de su rostro. La extracción de esta información está actualmente ligada a sofisticados procesos matemáticos y algoritmos de coincidencia. El reconocimiento facial clasifica la apariencia de personas y medir puntos nodales del rostro como distancia entre los ojos, ancho en nariz, ojos a boca, o la longitud de la línea de la mandíbula. *Moctezuma, O. (2016).*

Reconocimiento de Firmas.

Se trata de firma biométrica manuscrita, aquella que realizamos sobre tabletas o smartphones que puedan recoger aspectos biométricos, como son el trazo, presión o velocidad, que juntos hacen que esta sea una firma única, asociada inequívocamente a solo un usuario. Este tipo de tecnología permite garantizar la integridad del contenido firmado, puesto que asegura que este no ha sufrido ninguna alteración o cambio posterior al momento en que se realizó. Es la tecnología biométrica menos problemática, en la actualidad resulta la más difundida en el mundo, entre otras ventajas, es muy económica si se requiere implementar. *Diaz, V. (2013).*

Reconocimiento o Patrón de Iris

El reconocimiento por iris pertenece a la biometría estática, medición de características físicas en personas, es un método seguro, con una tasa de fiabilidad del 95% considerado alto. Es de los sistemas biométricos más confiables debido a que posee alrededor de 266 puntos únicos, mientras que la mayoría de sistemas biométricos poseen alrededor de 13 a 60 características distintas. Cada ojo es único permaneciendo estable con el paso del tiempo y en diferentes ambientes climáticos. *Cortes, O. et. al. (2010).*

Método de reconocimiento biométrico

Reconocimiento de Huella Dactilar.

El reconocimiento de huella dactilar es el método en identificación biométrica por excelencia debido a que es fácil de adquirir, usar y por ende goza de gran aceptación por parte de los usuarios. El uso de huellas dactilares para establecer la identidad de una persona tuvo su origen a mediados del siglo XIX, siendo pionero en esta área sir William Herschel.

La identificación con huellas dactilares está basada principalmente en la ubicación y dirección de terminaciones, crestas, bifurcaciones, deltas, valles y crestas. La huella dactilar es de los métodos más utilizados para desencriptar un dispositivo, sirve como método de apertura y cierre en cualquier sistema donde se necesite su instalación, por ello es de los más utilizados en cuestiones de seguridad. *Cortes, O. et. al. (2010).*

Estructura de un Sistema Biométrico

Los dispositivos biométricos poseen tres componentes básicos. El primero se encarga de la adquisición análoga o digital destacando algún indicador biométrico en una persona, como, por ejemplo, la adquisición de imágenes para huellas dactilares mediante un escáner. El segundo maneja la compresión, procesamiento, almacenamiento. comparación, con datos adquiridos y los almacenados. El tercer componente establece una interfaz con aplicaciones ubicadas en el mismo u otro sistema. *Cortés, O et.al. (2010)*

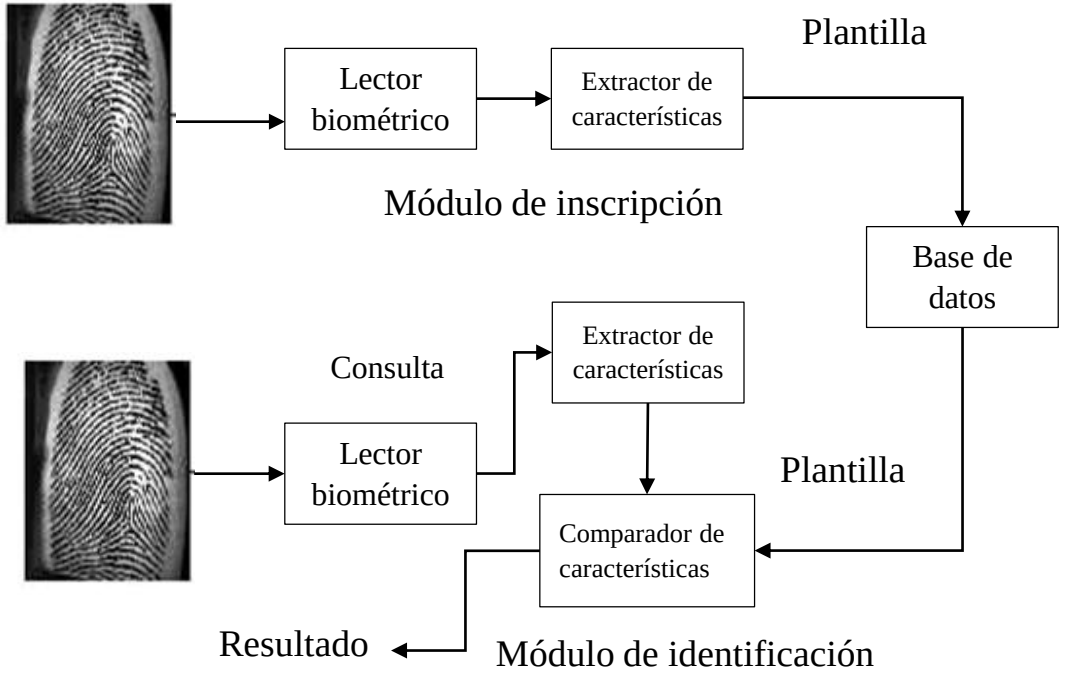

Figura 1 Estructura de registro de dato.
Fuente: Cortés, O et.al. (2010)

IMPLEMENTACIÓN DE UN LECTOR DE HUELLA UTILIZANDO VISUAL STUDIO

Para la implementación del lector biométrico se usó un lector de huella dactilar (modelo No. URU2S-U). Este dispositivo se conecta al computador vía puerto USB y es compatible con una gran serie de versiones del sistema operativo Windows. Este resulta sencillo de instalar y posee un diseño compacto y moderno que facilita su uso. *Cortes, O. et.al. (2010)*

Figura 2 Fingerprint reader U.are.U2000
Fuente: Windows SDK .NET, Digital Person base de datos

Desarrollo del Software

El programa implementado realiza los siguientes procesos y funcionalidades:

- Inscripción. Este punto captura la huella dactilar de una persona cuatro veces. Después de capturada la huella realizará su extracción en las características a los rasgos dactilares digitales; posteriormente se crea una plantilla para huella dactilar capturada, y por último realiza el almacenamiento en la plantilla (template) para la comparación posterior.

- Verificación. Es el proceso de comparación de una huella digital capturada con una plantilla(template) de huellas dactilares para determinar si ambas coinciden.

- Desmatriculación de una huella. Es la eliminación de una plantilla (template) de huella digital asociada a una previamente inscrita.

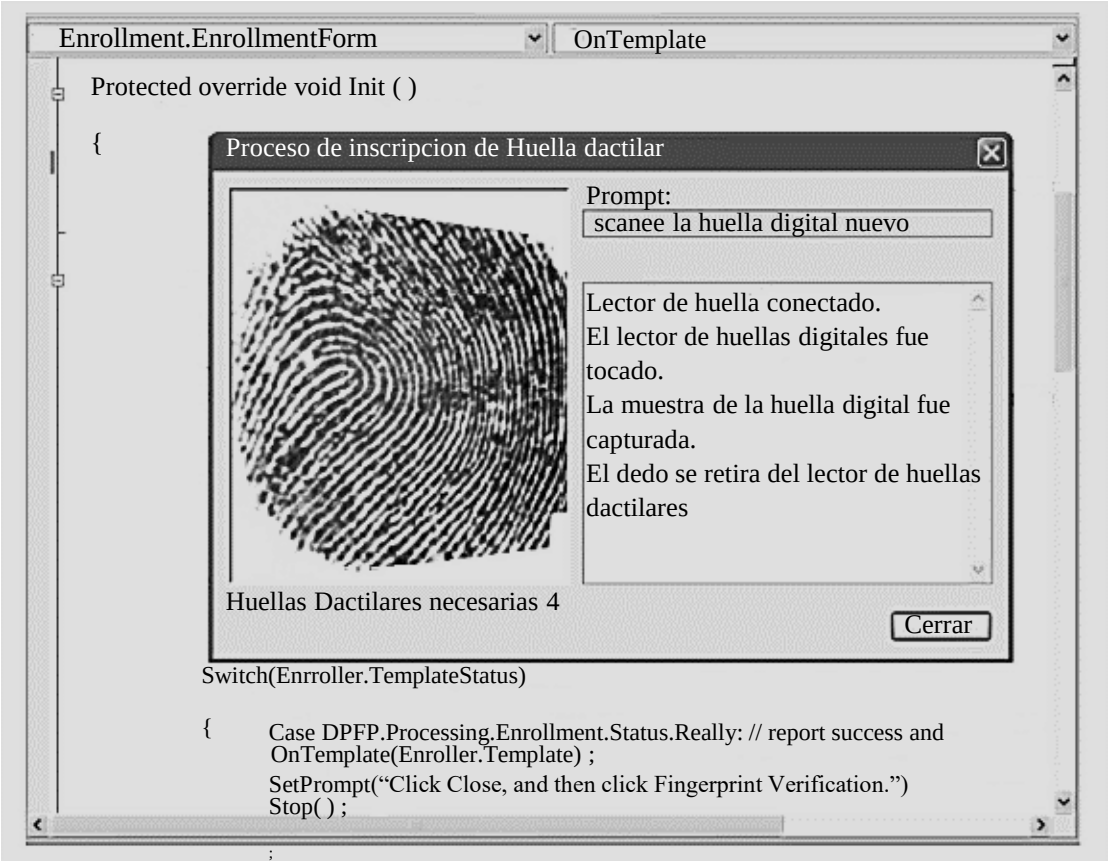

Figura 3 Proceso de inscripción de una huella dactilar,
Fuente: Visual Studio Versión 1.6 (2021)

Conclusión

La tecnología biométrica es y a demostrado ser un sistema confiable de igual manera eficiente, por ello en cuestiones de seguridad, protección de datos e identidad será tecnológicamente algo que va a revolucionar el mundo en cuanto a resguardo para la información, pero también como método de identificación, tan solo debemos mirar nuestro teléfono celular envuelto en una serie de ingeniería de alta gama encontrando a primera vista desbloqueo por reconocimiento dactilar siendo el usuario dueño de su información y con tenido, dando así una prueba en como un sistema biométrico es cada vez más una realidad por ello desde el punto de vista ingenieril, donde se puntualiza la investigación se identifica que los factores de seguridad realmente cumplen con el desarrollo sustentable y ayudan a la seguridad internacional, cultural, social, política y decisiones geopolíticas sin dejar vulnerable a ningún individuo.

Referencias

- Cortés Osorio, Jimy Alexander; Medina Aguirre, Francisco Alejandro; Muriel Escobar, José A. Sistemas de Seguridad Basados en Biometría Scientia Et Technica, Universidad Tecnológica de Pereira Pereira, Colombia diciembre, 2010, pp. 98-102.
- Moctezuma-Ochoa, Daniela Alejandra. Re-identificación de personas a través de sus características soft-biométricas en un entorno multi-cámara de video vigilancia. *Ingeniería Investigación y Tecnología*, XVII, 02 (2016): 257-271.
- Díaz Rodríguez, Vanessa, Sistemas biométricos en materia criminal, Instituto de Ciencias Jurídicas de Puebla A. C. Puebla, México, un estudio comparado enero-junio, 2013, pp. 28-47.
- Hernández, R, Fernández, C, & Baptista, P. (2010.). Metodología de la Investigación. México D.F.: Mc Graw Hill. p.p.1-275.
- One Touch® for Windows® SDK .NET Edition Visual Studio Versión 1.6 One Touch for Windows-SDK One Touch for
- Moncada-Jiménez, J., Salicetti-Fonseca, A., Carazo-Vargas, P., & Morera-Siércovich, P. L. (2021). La recolección, utilización y almacenamiento de datos biométricos sensibles en deportistas: insumos para la carrera de Educación Física. Revista Educación, 45(1), 640-652.
- Ponce Hernández, W. (2021). Mecanismos de protección de la privacidad de los ciudadanos aplicados a la firma manuscrita biométrica.
- Utreras Logacho, P. L. (2021). Gestión de identidad digital de usuarios en servicios web para la protección de la privacidad de la información (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).
- Mendoza García, M. P. (2021). Protección de datos y herramientas tecnológicas para la prevención del Covid-19: análisis a la luz de dos modelos contrapuestos (España vs Emiratos Árabes Unidos).

ECORFAN®