Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

Tipo de artículo: Artículo original
Temática: Reconocimiento de patrones
Recibido: 01/11/2017 | Aceptado: 17/09/2018

Reconocimiento de impresiones dactilares sobre la plataforma Raspberry Pi

Fingerprints recognition on Raspberry Pi platform

Emilio Rodríguez Hernández*, **José Hernández Palancar, Alfredo Muñoz Briseño**

Centro de Aplicaciones de Tecnologías de Avanzada. C.P. 12200, Siboney, Playa. La Habana, Cuba

***Autor para correspondencia:** erodriguez@cenatav.co.cu

Resumen
El reconocimiento de impresiones dactilares es una técnica ampliamente utilizada para la identificación de individuos, debido a su invarianza en el tiempo y a su singularidad. El presente trabajo se propuso implementar un sistema de reconocimiento de personas por sus impresiones dactilares sobre la plataforma Raspberry Pi. Esta investigación incluye la fundamentación de la selección del hardware, compuesto por la placa de desarrollo Raspberry Pi y el escáner DigitalPersona, así como la implementación del software, mediante la utilización de la biblioteca Libfprint. Como resultado principal se obtuvo un sistema con la capacidad de identificar en tiempo real a un sujeto mediante la adquisición de su impresión dactilar a través de un escáner. Con la materialización de esta investigación se mostró la capacidad que poseen las placas de desarrollo para ser empleadas en sistemas biométricos enfocados al cumplimiento de diversas tareas.

Palabras claves: impresiones dactilares, Raspberry Pi, sistemas biométricos, sistema de reconocimiento

Abstract
Fingerprints recognition is a widely used technique for people identification, due to its time invariance and singularity. This work proposed the implementation of a recognition system of subjects by their fingerprints over Raspberry Pi platform. This research highlight the details of hardware selection, which is composed by the Raspberry Pi development board and DigitalPersona scanner, as well as the software implementation, through the Libfrpint library. The main result was a system with the ability to identify in real time a subject by acquiring his fingerprint through a scanner. This work showed the capability of development boards for being used on biometric systems in several tasks.

Keywords: *biometric systems, fingerprints, Raspberry Pi, recognition system*

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

Introducción

Las impresiones dactilares constituyen el primer rasgo biométrico utilizado en la historia. En 1893, las autoridades del Reino Unido aceptaron a partir de los estudios realizados, que dos personas no presentan las mismas impresiones dactilares Maltoni et al. (2009). Partiendo de este descubrimiento, se comenzaron a extraer de las escenas del crimen para ser analizadas por expertos que se especializaron en esta nueva ciencia. Con la información proporcionada por el análisis de estas, se pudieron esclarecer diversos crímenes a lo largo de la historia.

Estos fueron los primeros pasos en el reconocimiento de las impresiones dactilares, pero los avances de la ciencia y la tecnología siempre fueron en ascenso y sus aplicaciones se expandieron hacia otras áreas de la sociedad. La seguridad y los fraudes de identidad constituyeron las principales razones que originaron sus nuevas aplicaciones. La inserción de los rasgos biométricos en sistemas destinados para diversos fines originan los llamados Sistemas Biométricos, que al utilizar dichas características intrínsecas de la identidad corporal del individuo, no pueden ser perdidos, ni descifrados, como ocurre con una contraseña o una tarjeta de identificación.

La necesidad de aumentar la seguridad y mejorar los métodos de identificación de individuos para varios procesos de la cotidianidad, ha incrementado la utilización de los Sistemas Biométricos en diversas aplicaciones. Este término comienza a tomar popularidad con la implementación de los AFIS[1], los cuales ejecutan de forma automática el reconocimiento de las impresiones dactilares para la identificación de personas Bifari and Elrefaei (2014).

Los sistemas de reconocimiento de impresiones dactilares se han implementado sobre diferentes plataformas paralelamente a los avances tecnológicos. La literatura muestra soluciones realizadas sobre hardware programable mediante lenguajes de descripción de hardware (HDL[2]). Los FPGAs pertenecen a esta clasificación con una gran capacidad de cómputo, un elevado precio y la necesidad de un determinado grado de especialización para explotar sus funcionalidades. Fons et al. (2012) describen la implementación de un sistema de reconocimiento de impresiones dactilares mediante el empleo de un FPGA. El sistema se encuentra basado en dos técnicas simultáneamente: el co-diseño hardware-software, principalmente orientado a la aceleración del procesamiento para aplicaciones en tiempo real, y el hardware flexible, para disminuir el costo y poder utilizar dispositivos lógicos dinámicamente reconfigurables de capacidad reducida.

Una aplicación automatizada para el control de asistencia se muestra en la solución descrita por Shegokar et al. (2015), la cual se centra en la utilización de la micro-computadora de placa única, Raspberry Pi, y la

[1] *Automatic Fingerprints Identification System*, significado de sus siglas en inglés.
[2] *Hardware Description Language*, significado de sus siglas en inglés.

tecnología de comunicación inalámbrica NFC para la implementación de un sistema de reconocimiento facial. Se basa en la utilización del módulo de cámara de la placa y la incorporación de una etiqueta NFC propia para cada individuo. Las imágenes recogidas por la cámara son procesadas por medio de la utilización de la biblioteca OpenCV, para efectuar el reconocimiento facial.

Los autores Shah et al. (2015) implementaron un sistema de enrolamiento remoto que fusiona dos métodos de reconocimiento biométrico, las impresiones dactilares y el reconocimiento facial. El nodo remoto de autenticación se realiza sobre una Raspberry Pi, y se establece una conexión encriptada a través de la nube para enviar los datos recogidos a una base de datos que se encuentra en el servidor. El análisis de la portabilidad incorporó al diseño una pequeña batería, pues la Raspberry Pi presenta un bajo consumo de energía lo cual constituye una fortaleza. El flujo de la solución comienza con la captura de las imágenes por la Raspberry Pi, tanto por el módulo de cámara como por el escáner de impresiones dactilares. Luego estas imágenes son encriptadas con la utilización del protocolo AES256 para ser enviadas a través de una conexión inalámbrica *end-to-end* hasta el servidor remoto.

Sapes and Solsona (2016) desarrollaron un sistema de seguridad de bajo costo, basado en el reconocimiento de impresiones dactilares. Para ello utilizaron un escáner modelo GT(511C1R) y la placa de desarrollo Raspberry Pi con la distribución de GNU Linux, Raspbian. La herramienta *FingerScanner* se ofrece como resultado de esta investigación, la cual es un sistema de seguridad que posibilita la validación de los usuarios por medio de la utilización de un escáner de impresiones dactilares. La solución utiliza el paradigma cliente-servidor, donde el servidor se encuentra corriendo en la Raspberry (implementado con *Node.js*). La comunicación entre el escáner y la plataforma se realiza a través del protocolo UART[3], y la conexión entre los dispositivos se efectúa por medio de los pines del GPIO.

El presente trabajo brinda un acercamiento a la conformación de un sistema biométrico, soportado sobre una tecnología de hardware de placa única y bajo costo como la Raspberry Pi. Durante el transcurso de la investigación se abordan temas de relevancia como la selección de los componentes que se utilizan en la implementación tanto del hardware como el software, la descripción de los algoritmos utilizados para el procesamiento de las impresiones dactilares, y la discusión de los resultados obtenidos.

Descripción del sistema propuesto

El sistema propuesto se encarga de realizar el reconocimiento de impresiones dactilares en tiempo real, lo que incide directamente en la selección de las herramientas que se deben emplear. En un sistema biométrico basado

[3] *Universal Asyncronus Reception Transmission*, significado de sus siglas en inglés.

en impresiones dactilares que funcione en tiempo real no puede faltar un escáner biométrico para la obtención de la imagen digitalizada de la huella. Luego, para la extracción de la información de interés, se debe contar con una unidad de procesamiento que implemente los métodos necesarios para una correcta extracción de los rasgos.

La selección de los componentes de hardware para el montaje del sistema se realizó a partir de un análisis sobre los recursos mínimos necesarios para satisfacer los objetivos de la investigación. El principal propósito de esta, sienta sus bases en la implementación de un sistema de reconocimiento de personas basado en las impresiones dactilares sobre una tecnología de hardware de placa única y bajo costo. Por tanto, se procedió a la búsqueda de información acerca de estos tipos de tecnologías. Los resultados del análisis señalan hacia la utilización de las placas de desarrollo que fusionan una excelente capacidad de cómputo, un tamaño compacto y un precio relativamente bajo para todas las bondades que ofrecen.

El sistema implementado en este trabajo adopta la Raspberry Pi como unidad de procesamiento, la cual presenta excelentes capacidades de hardware que maximizan su relación costo-prestaciones. Su amplia comunidad de usuarios que la emplean a nivel mundial se alza como otra de sus claras ventajas, lo que permite encontrar gran cantidad de documentación acerca de su funcionamiento e instalación. La figura 1 muestra la placa de desarrollo con sus interfaces y componentes.

Figura 1. Placa de desarrollo Raspberry Pi 3.

El escáner biométrico utilizado es el DigitalPersona UareU 4500, el cual es compatible con la Raspberry Pi. Este presenta una resolución de 512 dpi y puede ser utilizado en cualquier sistema operativo. La figura 2 muestra el esquema del sistema implementado y sus conexiones.

Los datos recolectados durante el proceso de enrolamiento fueron serializados y almacenados en la base de datos

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

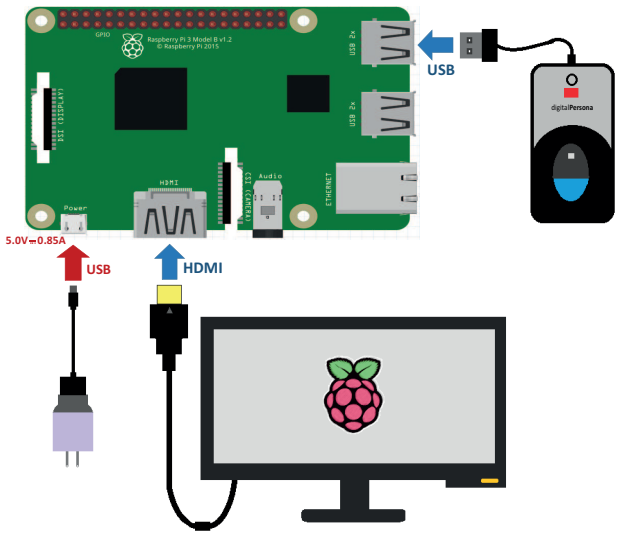

Figura 2. Hardware del sistema biométrico implementado.

"No SQL" con el empleo del gestor *Tokyo-Cabinet* Database. La ventajas esenciales de este gestor radican en sus rápidos accesos, debido a que presenta el patrón de diseño "llave-valor" (*key-value*) y a su simplicidad para guardar datos no estructurados. Se conformaron dos bases de datos de este tipo, una se utilizó para almacenar los vectores de rasgos y la otra para guardar la información demográfica del usuario.

Durante la etapa de revisión bibliográfica se detectó que la biblioteca Libfprint ha sido utilizada en varias investigaciones que presentan puntos de contacto con la presente. Esto despertó el interés por descubrir cómo se establecía su funcionamiento y qué posibilidades podía brindar. Uno de los motivos que propiciaron el primer acercamiento a esta biblioteca fue su condición de abarcar varios de los módulos necesarios para realizar el correcto funcionamiento del sistema de reconocimiento. Cuenta además con la implementación de drivers para el manejo de lectores biométricos de diferentes marcas Drake (2008).

Algoritmos de procesamiento de imágenes

Se hace importante señalar que para la realización de las pruebas sobre el funcionamiento de la biblioteca Libfprint fue necesario, por parte de su diseñador, incluir la posibilidad de realizar las actividades básicas del reconocimiento como la extracción de rasgos y la comparación de vectores de rasgos. Para esto utilizaron los métodos del NBIS[4] estandarizados por el Instituto Nacional de Normas y Tecnologías (NIST[5]).

[4] *NIST Biometric Image Software*, significado de sus siglas en inglés.
[5] *National Institute of Standards and Technology*, significado de sus siglas en inglés.

Estos métodos de procesamiento de impresiones dactilares se denominan MINDTCT y Bozorth3. Estos métodos emplean el análisis de las minucias de la impresión dactilar, que son los puntos donde las crestas se bifurcan o se terminan. Ambos algoritmos son utilizados para la detección automática de las bifurcaciones y terminaciones de las crestas, y para el cotejo entre las impresiones dactilares respectivamente Watson et al. (2007). Estas herramientas fueron desarrolladas por el FBI[6] y el DHS[7] con el objetivo de facilitar y soportar la manipulación y el procesamiento automático de las impresiones dactilares.

Detección de minucias

El detector de minucias MINDTCT extrae de cada minucia cuatro elementos fundamentales, su localización, orientación, tipo y calidad. El diagrama de la figura 3 muestra las ocho etapas presentes en su funcionamiento. A partir de la imagen de entrada de la impresión dactilar, el método genera un mapa representativo de las zonas de calidad. En este se representan las áreas de inestabilidad, donde la detección de minucias no es confiable. La generación de un mapa de orientación de las crestas forma parte del proceso, pues es necesario para la asignación de los valores binarios en la etapa de binarización de la imagen. Con la obtención de la imagen binarizada, comienza la etapa de detección de minucias mediante la realización de varios escaneos simples en busca de patrones de píxeles predefinidos Watson et al. (2007). La etapa que le precede se encarga de eliminar las falsas minucias, utilizando el mapa de calidad construido en la segunda fase. Luego se realiza un conteo de las crestas existente entre un punto de minucia y sus vecinos más cercanos. La séptima etapa lleva a cabo una evaluación de la calidad de las minucias para finalizar con la creación del archivo que contiene todos los puntos detectados.

Cotejo de minucias

El algoritmo de cotejo Bozorth presenta la característica de ser invariante a la traslación y a la rotación. Se encarga de calcular un coeficiente similitud entre dos impresiones dactilares, utilizando para ello la posición de las minucias $(x; y)$ y la orientación θ. Con estos datos se construyen dos tipos de tablas denominadas:

1. Tabla de comparación de minucias de la impresión dactilar.
2. Tabla de compatibilidad entre impresiones dactilares.

[6] *Federal Bureau of Investigation*, significado de sus siglas en inglés.
[7] *Department of Homeland Security*, significado de sus siglas en inglés.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

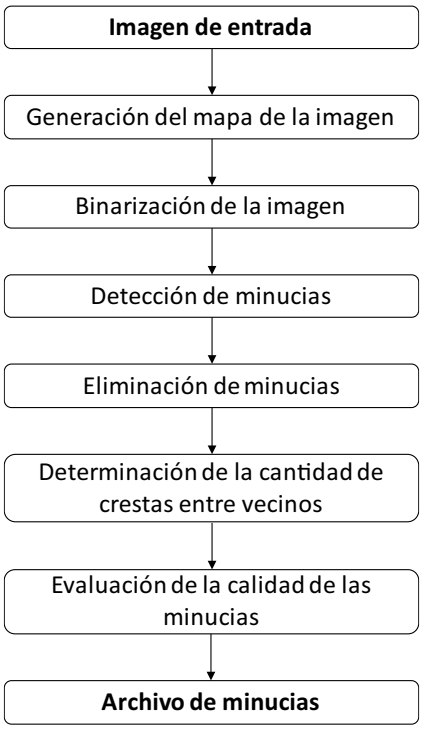

Figura 3. Etapas del algoritmo MINDTCT.

La primera etapa se encarga de crear una tabla del tipo 1 por cada impresión a comparar, denotadas como T y Q, en las cuales se almacenan un vector de rasgos $(m_j, m_k, d_m, \beta_j, \beta_k)$ por cada par de minucias que estén a una distancia menor que un umbral preestablecido, donde d_m representa la distancia euclidiana entre el par de minucias m_j, m_k, y β_j, β_k representan los ángulos existentes entre el segmento que une a las minucias m_j, m_k y la orientación de estas. Las tablas de tipo 1 son las almacenadas en la base de datos de tokyo cabinet, cuando se realiza una inserción en el sistema. En la figura 4 puede verse una representación gráfica de los rasgos extraídos.

En un segundo momento se compara cada elemento de T con cada elemento de Q. De esta manera, se almacenan en una tabla de tipo 2, denotada por F, los pares de vectores de rasgos compatibles. Dos vectores de rasgos $(m_i, mj, d_{m1}, \beta_i, \beta_j)$ y $(m_k, m_l, d_{m2}, \beta_k, \beta_l)$ son compatibles si: $|d_{m1} - d_{m2}| < th_d$, $|\beta_i - \beta_k| < th_{b1}$ y $|\beta_j - \beta_l| < th_{b2}$, donde th_d, th_{b1} y th_{b2} son umbrales preestablecidos. De esta forma se encuentra el mayor subconjunto de entradas de F que sea coherente geométricamente. A partir de dichas entradas se calcula un coeficiente de similitud global Mayoue (2008). Este coeficiente, es utilizado para decidir si dos impresiones fueron originadas por un mismo dedo o no.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

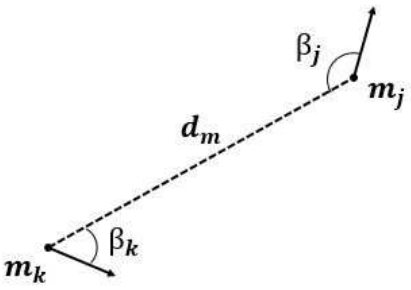

Figura 4. Representación del par de minucias analizadas por el algoritmo Bozorth.

Discusión de los resultados

En esta sección se realiza el análisis de los resultados obtenidos durante la implementación y la ejecución de las diferentes pruebas a las que se sometió el sistema propuesto. Con el fin de lograr una mayor comprensión esta discusión se divide en dos partes: el análisis de eficacia y el análisis de eficiencia.

Análisis de eficacia

Durante la realización de los experimentos para analizar la eficacia del sistema propuesto se utilizó la base de datos de competencia FVC2004[8] Cappelli et al. (2004). Esta es generada por una competencia internacional que somete a pruebas los algoritmos de verificación de impresiones dactilares.

El conjunto de impresiones utilizado fue el FVC2004 DB2_A, el cual cuenta con 100 sujetos distintas y 8 tomas de cada uno de ellos, para formar un total de 800 impresiones. Las impresiones que pertenecen a este grupo fueron recogidas por medio de la utilización del escáner DigitalPersona U.are.U 4000, con una resolución de 500 dpi y las imágenes presentan una dimensión de 328x364 píxeles. La razón que fundamenta la selección de este conjunto se debe a que la adquisición se realizó con el mismo tipo de sensor utilizado en la implementación del sistema propuesto. En la figura 5 se muestra una de las imágenes que forma parte de estas plantillas.

El protocolo estándar definifo por Cappelli et al. (2006) para evaluar la eficacia en esta base de datos se define como sigue:

1. Del conjunto de plantillas se eligen las imágenes que constituyen las primeras tomas de cada impresión. Este grupo se le conoce como las impostoras porque todas las impresiones que lo forman son diferentes. Entonces, la prueba consiste en extraer los falsos positivos que se puedan encontrar debido a que ninguna

[8] *Fingerprint Verification Competition in 2004*, significado de sus siglas en inglés.

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

Figura 5. Imagen perteneciente al grupo de impresiones FVC2004 DB2_A.

de ellas presenta coincidencias con otra. Para realizar esto se aplica un todos contra todos completando 4950 comparaciones.

2. Del conjunto se toman todas las impresiones que la componen y se procede a realizar un C_2^8 con cada conjunto de las 8 tomas de cada impresión que equivales a 2800 comparaciones. A este grupo se les denominan las genuinas porque cada impresión contiene en la base de datos 7 impresiones coincidentes. Por tanto, la prueba se encarga de extraer los falsos negativos.

Como resultado de la aplicación de los métodos del NBIS empleados para la detección de las minucias (MINDTCT) y para el cotejo de impresiones (Bozorth3), se computaron las curvas FMR[9] y FNMR[10] recogidas en la figura 6.

En aplicaciones que requieran una elevada seguridad se necesita suprimir al máximo la aceptación de impostores, lo que conlleva a modificar los umbrales de aceptación y aumentar los rechazos de impresiones genuinas. Los parámetros FMR100 y FMR1000 constituyen los puntos de operación de la FNMR para valores de FMR= 1/100 y FMR= 1/1000 respectivamente, los cuales describen la exactitud de los sistemas biométricos en escenarios de acceso restringido Cappelli et al. (2002). Esta forma de evaluación surge debido a que existen métodos que reportan altos valores de EER en comparación con otros, y sin embargo, sus puntos de operación FMR100 y FMR1000 pueden presentar mejores resultados. El análisis de estos parámetros resultó en un EER=0.24, el cual se muestra en la gráfica de la figura 6, un FMR100=0.74 y un FMR1000=0.85. Se observó que el extractor de rasgos utilizado falla en localizar algunas minucias, por lo que el uso de otro método de extracción puede mejorar grandemente los resultados obtenidos.

[9] *False Match Rate*, significado de sus siglas en inglés
[10] *False Non-Match Rate*, significado de sus siglas en inglés

Revista Cubana de Ciencias Informáticas
Vol. 12, No. 4, Octubre-Diciembre, 2018
ISSN: 2227-1899 | RNPS: 2301
Pág. 91-102
http://rcci.uci.cu

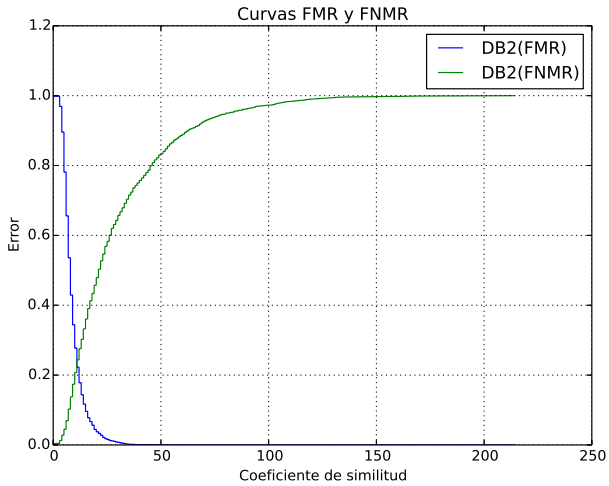

Figura 6. Curvas FMR y FNMR para el conjunto de plantillas FVC2004 DB2_A.

Análisis de eficiencia

El análisis de la eficiencia del sistema se ha realizado a partir de la medición del tiempo consumido por el proceso de identificación de una persona para diferentes números de individuos enrolados. Estos tiempos se comienzan a medir desde la lectura del escáner hasta la devolución del coeficiente de similitud por parte del algoritmo de comparación (Bozorth3 para este caso).

Con el fin de estimar los tiempos de identificación se introdujo en el código fuente de la aplicación algunas sentencias que permiten medir estos intervalos de tiempo. Se incluyen en la estimación, las iteraciones por la base de datos y la comparación con cada uno de los vectores de rasgos hasta el reconocimiento de la impresión por el sistema. Para poder ilustrar estas mediciones y evaluar su comportamiento, se realizaron varias salvas a la base de datos en diferentes momentos con una cantidad de impresiones variable con diferencia de 50 entre cada una, para contar con un total de 250 impresiones. La figura 7 muestra los tiempos que el sistema tarda en realizar comparaciones con todas las tablas de rasgos almacenadas en la base de datos.

Siendo el Bozorth un algoritmo costoso se muestra que los tiempos de búsqueda son aceptables para aplicaciones ligeras. No obstante, en el sistema propuesto es posible implementar otros algoritmos más eficientes y eficaces.

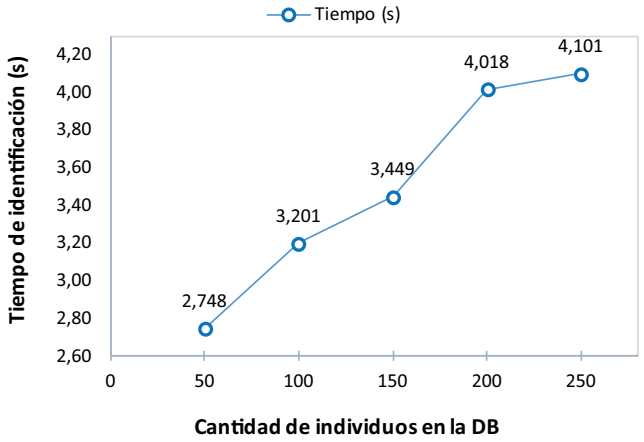

Figura 7. Tiempos de identificación.

Conclusiones y trabajos futuros

En este trabajo se implementó y analizó un sistema de identificación de personas por medio de sus impresiones dactilares, realizando todo el procesamiento en una Raspberry Pi. Esto permitió mostrar la capacidad que presentan estas placas de desarrollo para ser utilizadas en aplicaciones de este tipo. Los sistemas que cuentan con este hardware como unidad principal de procesamiento logran disminuir el costo del despliegue de las soluciones, aumentar la portabilidad de estas y reducir el tamaño físico junto al consumo de energía. El sistema que se describe en esta investigación utiliza los algoritmos de NBIS para la detección y cotejo de minucias, siendo este fue un caso de prueba. La aplicación es capaz de trabajar con otros algoritmos que ejecuten estas mismas funciones, por lo que para futuras investigaciones se desarrollarán otros algoritmos que mejoren los valores de EER, FMR100 y FMR1000 alcanzados por los métodos del NBIS. Para trabajos posteriores se propone utilizar otras placas de desarrollo para evaluar en ellas el funcionamiento del sistema propuesto.

Referencias

Ezdihar N. Bifari and Lamiaa A. Elrefaei. Automated Fingerprint Identification System based on weighted feature points matching algorithm. In *2014 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, pages 2212–2217. IEEE, September 2014.

Raffaele Cappelli, Dario Maio, Davide Maltoni, James L. Wayman, and Anil K. Jain. FVC2002: Second Fingerprint Verification Competition. *Object recognition supported by user interaction for service robots*, 3: 811–814, August 2002.

Raffaele Cappelli, Dario Maio, Davide Maltoni, James L. Wayman, and Anil K. Jain. FVC2004: Third Fingerprint Verification Competition. *Biometric Authentication*, 24(3):1–7, 2004.

Raffaele Cappelli, Dario Maio, Davide Maltoni, James L. Wayman, and Anil K. Jain. Performance evaluation of fingerprint verification systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 28(1): 3–18, January 2006.

Tokyo-Cabinet Database. http://hammerprinciple.com/databases/items/tokyo-cabinet.

Daniel Drake. Fingerprint Abstraction Layer for Linux, April 2008.

Mariano Fons, Francisco Fons, Enrique Canto, and Mariano Lopez. FPGA-based Personal Authentication Using Fingerprints. *J Sign Process Syst, Springer Science*, pages 153–189, 2012.

Davide Maltoni, Dario Maio, Anil K. Jain, and Salil Prabhakar. *Handbook of Fingerprint Recognition*. Springer, 2da edition, 2009.

Aurelién Mayoue. A biometric reference system for fingerprint NIST Fingerprint Image Software 2, 2008.

Jordi Sapes and Francesc Solsona. FingerScanner:Embedding a Fingerprint Scanner in a Raspberry Pi. *Sensors*, 2016.

Dhvani K. Shah, Vinayak A. Bharadi, V.J. Kaul, and Sameer Amrutia. End-to-End Encryption Based Biometric SaaS: Using Raspberry Pi as a Remote Authentication Node. In *2015 International Conference on Computing Communication Control and Automation (ICCUBEA)*, pages 52–59. IEEE, February 2015.

Nikhil P. Shegokar, Kaustubh S. Jaipuria, and Amitkumar Manekar. Review automated students attendance Management System using Raspberry-Pi and NFC. *International Journal of Research in Computer & Information Technology (IJRCIT)*, 1(1):90–92, 2015. ISSN 2455-3743.

Craig I. Watson, Michael D. Garris, Elham Tabassi, Charles L. Wilson, R. Michael Mccabe, Stanley Janet, and Kenneth Ko. Users guide to NIST biometric image software (NBIS), 2007.