Análisis de lectores biométricos de huella dactilar implementados en una Raspberry Pi

Conference Paper · September 2017

CITATIONS
0

READS
4,856

3 authors, including:

Antonio Alarcón-Paredes
Instituto Politécnico Nacional
41 PUBLICATIONS **265** CITATIONS
SEE PROFILE

Gustavo Adolfo Alonso Silverio
Universidad Autónoma de Guerrero
54 PUBLICATIONS **575** CITATIONS
SEE PROFILE

CICOM 2017
7° Congreso Internacional de computación
México - Colombia
XVII Jornada Académica en Inteligencia Artificial
Septiembre 28, 29 y 30 de 2017, Colombia

ANÁLISIS DE LECTORES BIOMÉTRICOS DE HUELLA DACTILAR IMPLEMENTADOS EN UNA RASPBERRY PI

MARCO ANTONIO BRUNO
Facultad de ingeniería, UAGro
mbruno@uagro.mx

ANTONIO ALARCÓN PAREDES
Facultad de ingeniería, UAGro
aalarcon@uagro.mx

GUSTAVO ALONSO SILVERIO
Facultad de ingeniería, UAGro
gsilverio@uagro.mx

RESUMEN

Los sistemas embebidos están tomando cada vez más importancia en nuestra vida cotidiana, pues contribuyen a elevar la productividad y competitividad en un mundo cada vez más globalizado. La reducción en los costos de los componentes electrónicos ha aumentado el número de plataformas de hardware que soportan el sistema operativo Linux, las cuales son muy comunes en productos comerciales; una de ellas es Raspberry Pi. En este documento se presenta un análisis de distintos lectores de huella dactilar que pueden ser implementados posteriormente en el desarrollo de sistemas de bajo costo basados en este indicador biométrico utilizando una Raspberry Pi.

PALABRAS CLAVE

Sistemas embebidos, biometría, huellas dactilares, Raspberry Pi.

ABSTRACT

Currently, embedded systems have an increasingly importance in our day lives, as they contribute to raising productivity and competitiveness in an increasingly globalized world. The reduction of the costs in electronic components has given the opportunity to develop a range of platforms supporting the Linux operating

system, which are very common in commercial products; an example of the latter is Raspberry Pi. In this paper, an analysis of different fingerprint readers that can be implemented in the development of low cost systems based on this biometric indicator on a Raspberry Pi, is presented.

KEYWORDS

Embedded Systems, biometric, fingerprint, Raspberry Pi

INTRODUCCIÓN

Un sistema embebido es un sistema computacional diseñado para realizar una o más funciones dedicadas, en donde la mayoría de los componentes están incluidos en la placa base (tarjeta de video, audio, microprocesador, etc.). En la actualidad, los sistemas embebidos se encuentran en auge, ya que pueden encontrarse en una múltiple gama de productos, *e.g.*, relojes, parquímetros, máquinas expendedoras o sistemas de control de acceso. Muchas veces los dispositivos resultantes no tienen el aspecto que se asocia normalmente a una computadora ya que están orientados a minimizar los costos económicos. El crecimiento en la industria electrónica se ha generado en parte por el aumento en los niveles de integración, es decir la cantidad de transistores que se tienen por mm^2 y el costo inversamente relacionado con dicha cantidad, los altos niveles de integración han permitido construir sistemas más veloces, con mayor cantidad de puertos de fácil interacción con otros dispositivos, permitiendo desarrollar diversos tipos de aplicaciones.

Por otra parte, el uso de métodos de identificación se ha convertido en parte de la seguridad en las organizaciones tanto públicas como privadas para evitar suplantaciones e infiltraciones que tiene como consecuencia robo de información o pérdida de recursos tangibles e intangibles, por lo tanto son cada vez más los desarrolladores de sistemas que buscan implementar nuevos mecanismos de seguridad, pero aún hay un reto por buscar soluciones de bajo costo y el uso de sistemas embebidos combinados con lectores biométricos los hacen una opción muy viable para resolver esa necesidad [1].

Los sistemas de identificación de personas se basan en el principio de identidad esto quiere decir que cada persona es idéntica solo a ella misma. En este sentido, la identidad es representada como un conjunto de elementos, perdurables e inmutables en el tiempo, que hacen única a esa persona.

Las tecnologías biométricas pueden clasificarse atendiendo a muy diversos criterios, por ejemplo: Las más actuales: iris, voz, geometría de la mano, rostro, huella dactilar. No muy utilizadas: medidas del cráneo, termografía facial, patrón de venas de las manos, lóbulos de la oreja, exploración de la retina, huella de la mano, firma manuscrita, dinámica de introducción de teclas sobre un teclado, pigmentación, reflectividad óptica de la piel, forma de andar o de gesticular. Casos especiales: ácidos nucleicos (DNA o ácido desoxirribonucleico y RNA o ácido ribonucleico) [2].

La identificación por huella dactilar es una de las biometrías más conocidas y publicitadas. Gracias a su unicidad y constancia en el tiempo, las huellas dactilares han sido usadas para la identificación por más de un siglo, siendo automatizadas más recientemente (Fig. 1) gracias a los avances en la computación.

Figura 1. Huella dactilar

La identificación por huellas dactilares es popular por su inherente comodidad de adquisición y las numerosas fuentes disponibles para recolección de datos (diez dedos).
Las huellas dactilares han sido uno de los métodos más usados para el reconocimiento humano por la amplia aceptación que tiene entre las personas; los sistemas biométricos automatizados han estado en crecimiento en estos últimos años debido a la determinación y compromiso de la industria, las evaluaciones y las necesidades de los gobiernos del mundo y así como la aportación de las organizaciones encargadas de los estándares de seguridad, esto ha conducido a la siguiente generación en reconocimiento de huellas dactilares, que promete dispositivos más rápidos y de más alta calidad de adquisición para mejorar la exactitud y la confiabilidad.
Sin embargo, el proceso de reconocimiento de huellas dactilares en sistemas embebidos continúa siendo poco explorado debido a la compatibilidad de hardware para realizar la lectura de este indicador biométrico. Por ello, este trabajo consiste en el estudio sobre la viabilidad de integración de lectores biométricos para el reconocimiento de huellas dactilares en una Raspberry Pi, que a la postre pueda ser utilizada para elaborar sistemas complejos diseñados para tener un desempeño competitivo. Asimismo puede ser la base para trabajos futuros ayudando a los desarrolladores de sistemas embebidos a crear proyectos donde sea necesario incluir un lector biométrico de huellas dactilares.

OBJETIVOS

El objetivo de este trabajo es presentar un análisis de lectores biométricos de bajo costo que puedan ser integrados con una Raspberry Pi, este trabajo pretende ser una guía para la toma de decisiones en trabajos futuros en donde implementar autentificación biométrica a un sistema embebido basado en una Raspberry Pi sea una necesidad.

METODOLOGÍA Y PROCESOS DE DESARROLLO

Problemas en la adquisición de huellas dactilares

El problema en la adquisición de las huellas dactilares en un sistema embebido se puede apreciar en diferentes escenarios por lo cual los desarrolladores siempre están en busca de optimizar los procesos y lograr resultados de calidad, a continuación, se mencionan algunos de los aspectos más relevantes:

- **Falta de documentación en la adquisición de datos crudos provenientes del lector biométrico:** La falta de documentación técnica sobre el funcionamiento de un lector biométrico produce muchas ineficiencias y problemas que podrían ser fácilmente evitados, cuando la única documentación se encuentra a través de la ayuda en foros de desarrolladores será una solución casi imposible de mantener y tendrá un alto índice de errores no esperados en la lectura de datos provenientes del lector, o en el peor de los casos quedar obsoleta en muy poco tiempo.
- **SDK desarrollado para un lenguaje de programación:** Cuando el SDK de desarrollo se encuentra orientado a un lenguaje de programación en particular es una limitación debido a que no todos los lenguajes de programación se pueden implementar con facilidad en un sistema embebido.
- **Tiempo de respuesta en la adquisición de datos:** En sistemas de producción el tiempo de respuesta es un factor muy importante, al trabajar con un sistema embebido estamos limitados a sus capacidades técnicas, y si el SDK utilizado es desarrollado por un tercero podría tenerse un bajo rendimiento en el funcionamiento del dispositivo.
- **Calidad de las imágenes de huellas dactilares:** En el caso de algunos lectores de huellas dactilares, se tiene que trabajar directamente con la imagen adquirida. En este sentido, la calidad de la imagen determina la cantidad de características que podemos extraer de ella.

Dispositivos analizados

Raspberry Pi

Raspberry Pi es una computadora del tamaño de una tarjeta de crédito que tiene muchas de las funcionalidades de una computadora personal, se ha convertido en un dispositivo ampliamente utilizado debido a su bajo costo y al continuo crecimiento de su comunidad de desarrolladores desde su creación, fue desarrollado en reino unido por la fundación Raspberry Pi, con el objeto de estimular la enseñanza de ciencias de la computación en las escuelas.

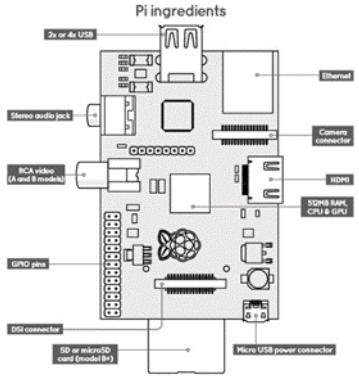

Figura 2. Componentes de una Raspberry Pi

La figura 2. muestra el hardware que integra a la Raspberry Pi cuenta con un chip Broadcom BCM2835, que contiene un procesador central (CPU) ARM1176JZF-S a 700 MHz, procesador gráfico (GPU) VideoCore IV, módulo de 512 MB de memoria RAM, Conector RJ45 a 10/10 Mbps, 2 lectores USB 2.0, salida analógica de audio por un jack de 3.5 mm, salida digital de video + audio HDMI, salida analógica de video RCA, pines I/O de propósito general, conector de alimentación por micro USB y lector de tarjetas SD.

La Raspberry Pi 3 (dispositivo seleccionado para este trabajo) está diseñada para ejecutar el sistema operativo GNU/Linux, varias distribuciones de Linux han sido portadas al chip Broadcom BCM2835 de la Raspberry Pi, por mencionar algunos ejemplos Debian, Fedora y Arch Linux. Las distribuciones atienden necesidades diferentes, pero tiene una característica en común son de código abierto, además por lo general el software desarrollado es compatible entre si, en este trabajo se utiliza la distribución Raspbian deribada de Debian Wheezy, se utilizó una versión precompilada para la Raspberry Pi.

DIGITAL PERSONA U ARE 4500

El lector biométrico U are 4500 (Fig. 3) es fabricado por la empresa DigitalPersona, está diseñado para la integración con equipos en los que la identificación o verificación de personas sea necesaria, cuenten con una interfaz de comunicación USB (Universal Serial Bus) 2.0, cuenta con un SDK compatible con en el sistema operativo Windows o cualquier distribución basada en el sistema operativo Linux incluso es un módulo muy confiable combinando con la distribución Raspbian orientada a la plataforma Raspberry Pi , además de esto cuenta con librerías diseñadas para algunos de los lenguajes de programación más utilizados como C, C++,C#, Java, VB .NET [3].

Figura 3. Lector de huella U.are.U. 4500

El lector utiliza una tecnología de escaneo óptica para capturar imágenes de alta calidad con una amplia área de captura, para usarlo el usuario deberá colocar su dedo en la ventana transparente y el lector de manera automática escaneara la huella, para más información, una luz roja indica que la imagen de la huella ha sido capturada, la transferencia y cifrado de los de datos se realiza de manera automática a través de la interfaz de comunicación USB gracias a los componentes electrónicos con los que cuenta, se alimenta con una entrada de 5V USB (Universal Serial Bus), las imágenes que se obtiene se encuentran en escala de gris, el peso del sensor es de 105 gramos y las dimensiones son de 36 x 65 x 15.56 mm.

FINGERPRINT SCANNER GT-511C3

El módulo Fingerprint Scanner – TTL (GT511C3) es un dispositivo de bajo costo producido por la SparkFun Electronics, está diseñado para tener una alta integración con Linux, provee de una rápida velocidad y precisión en la identificación de huellas dactilares utilizando el algoritmo SmackFinger 3.0. Cuenta con un CPU de 32 bits a 72 MHz (ARM Cortex M3) además incorpora una base de datos que puede almacenar hasta 200 plantillas de huellas dactilares, puede realizar el reconocimiento de la huella en cualquiera de los 360°. La carga y descarga de plantillas de huellas dactilares se realiza a través de una interfaz de comunicación serial RS-232 utilizando un conector UART acrónimo de (Universal Asynchronous Receiver-Transmiter) a una tasa de comunicación de 9600 baudios por segundo.

Figura 4. Lector de huellas dactilares GT-511C3

La comunicación con el módulo se realiza a través de un protocolo de envío de paquetes, existen tres tipos de paquetes:

- Paquetes de comandos: Se utilizan para indicarle al dispositivo que realice una operación por ejemplo verificar si un dedo está presionando el sensor, capturar una huella, crear una plantilla, obtener una imagen, entre otros.
- Paquetes de respuesta: Los paquetes de respuesta pueden ser de dos tipos y se identifican con el condigo ACK(0x30) y NACK(0x31), el primero indica que un comando se ejecutó correctamente y el

segundo cuando se produjo una falla, además en caso de falla el código del error también es proporcionado [6].

- Paquetes de datos: Los campos no tiene una longitud estática debido a que es se utiliza para extraer información como imágenes, plantillas, información referente al dispositivo, entre otros.

ADAFRUIT ZFM-206SA

El sensor biométrico ZFM-206SA (Fig. 5) es fabricado por Adafruit Industries, el sensor realiza procesamiento digital de imágenes interno ya que cuenta con un DSP (Digital Signal Processor), además incluye capacidades de almacenamiento de plantillas de huellas dactilares en su base de datos interna. El sensor funciona con el protocolo serial, por lo cual lo hace de fácil integración a cualquier microcontrolador o tarjeta de desarrollo la velocidad de comunicación por defecto es de 57600 baudios por segundo, siendo ajustable de 9600 a 115200 baudios por segundo.

Figura 5. Lector de huella Adafruit ZFM-206SA

El dispositivo puede almacenar hasta 162 huellas dactilares, el led del dispositivo se ilumina cuando se encuentra tomando imágenes en busca de huellas dactilares, para poder utilizar el dispositivo es necesario guardar las huellas en la base de datos interna a estas se les asigna un número de identificación, posteriormente se puede iniciar con la secuencia de lectura y comparación para verificar las huellas de los usuarios registrados y así poder ejecutar acciones en base al resultado.

La comunicación con el módulo se realiza a través de un protocolo de envío de paquetes, existen tres tipos de paquetes [7]:

- Paquetes de instrucciones: Se utilizan para indicarle al dispositivo que realice una instrucción por ejemplo comenzar a tomar imágenes, obtener las plantillas almacenas en su base de datos, obtener el número de usuarios almacenados, entre otros.
- Paquetes de confirmación de comunicación: Los paquetes de respuesta pueden ser de dos tipos y se identifican con el condigo 0x00 y 0x01, el primero indica que se la comunicación entre el microcontrolador o tarjeta se realizó correctamente y el segundo cuando se produjo una falla en la comunicación.
- Paquetes de datos: Las plantillas de huellas dactilares tiene un tamaño de 512 bytes.

Software

Python es uno de los lenguajes de programación que permite realizar la interacción entre la Raspberry Pi y los módulos de manera más natural. Para el sensor DIGITAL PERSONA U are U 4500 fue necesario realizar la comunicación a través del puerto USB (Universal Serial Bus) y se utilizó la librería Fprint desarrollada para sistemas operativos basados en Linux pero los desarrolladores recomiendan utilizarla solamente en fase experimental, debido a que se encuentra en desarrollo y podría causar conflictos a la hora de utilizarla en entornos de producción.
Para los sensores FINGERPRINT SCANNER GT-511C3 y ADAFRUIT ZFM -206SA se utilizó la librería de comunicación serial Pyserial [9] ya que comparten esta característica al ser sensores que trabajan a través de la comunicación de paquetes.

Evaluación de lectores biométricos

Para implementar un sistema automático de reconocimiento de personas se necesitan mecanismos que evalúen la bondad y capacidad del sistema. Cuantificar las capacidades que tienen los lectores biométricos para la captura de huellas dactilares ayudará a mejorarlo y a compararlo con otros ya implementados.
Un sistema de reconocimiento biométrico captura un indicador biométrico, extrae sus características y forma una plantilla que compara con otro u otros para evaluar si pertenecen o no a una misma persona. De esta forma se requiere que los indicadores biométricos sean distintos entre las personas a esto se le conoce como variación inter-clase, por otra parte se requiere que las plantillas generadas a partir de la adquisición de huellas dactilares de una misma persona sean idénticos o muy parecidos a esto se le denomina variación intra-clase. Sin embargo, existen factores que disminuyen la variación inter-clase y que aumentan la variación intra-clase, dando lugar a errores de reconocimiento. Por ejemplo, un usuario que interactúe con el sensor de forma distinta o que presente cambios fisiológicos puede hacer que el sistema genere plantillas muy distintas a partir del mismo indicador biométrico.
Para la evaluación de los lectores se determinaron algunos parámetros como la capacidad de almacenamiento, interfaz de comunicación, tipo de sensor, tasa de aceptación falsa y la capacidad de ajustar la clasificación de seguridad. El tipo de sensor determina el costo y el tamaño del lector biométrico así como la probabilidad de evitar la lectura de huellas dactilares falsas, la interfaz de comunicación aumenta la compatibilidad con el hardware a implementar, la tasa de aceptación falsa es cuando existe la posibilidad de identificar un registro erróneamente con otro registrado, la tasa de rechazo falso es la posibilidad de identificar un registro que no se encuentra registrado, en el caso de la capacidad de almacenamiento se debe a que algunos de los sensores analizados disponen de una base de datos interna, el tamaño de plantilla se refiere al tamaño máximo que puede tener el archivo que genera el sensor a partir de la extracción de las características de una huella dactilar, el tiempo de búsqueda es la cantidad máxima que puede tardar el sensor en retornar un resultado positivo o negativo sobre la existencia de una plantilla, el tamaño de la imagen es la cantidad de pixeles que mide una imagen capturada, el nivel de seguridad se traduce en la calidad de la imagen obtenida esto conlleva a un mayor tiempo de respuesta por parte del sensor, , los datos que se muestran en la Tabla 1 se obtuvieron de la hoja de especificaciones que proporciona el fabricante.

Tabla 1. Comparación de lectores biométricos

	DIGITAL PERSONA U ARE 4500	FINGERPRINT SCANNER GT-511C3	ADAFRUIT ZFM-260ª
Tipo de sensor	Óptico	Óptico	Óptico

Interfaz de comunicación	USB	Serial	Serial
Tasa de aceptación falsa	Depende del algoritmo implementado	0.001%	0.008%
Tasa de rechazo falsa	Depende del algoritmo implementado	0.1%	0.005%
Capacidad de almacenamiento	No disponible	200 plantillas	162 plantillas
Tamaño de plantilla	Depende del algoritmo implementado	256 bytes	512 bytes
Tiempo de búsqueda	Depende del algoritmo implementado	< 1 segundo	< 1 segundo
Tamaño de imagen	512x512 pixeles	202x258 pixeles	256x288 pixeles
Nivel de seguridad	5 no configurable	5 configurable desde 1	5 configurable desde 1

Los lectores biométricos analizados cuentan con diversas características (Tabla 1) que pueden ser aprovechadas para obtener una comparación confiable, a continuación, se presenta un resumen de las ventajas y limitaciones que presentan cada uno de estos:

1. **DIGITAL PERSONA U ARE 4500:** Al implementar este dispositivo tendremos que aplicar sofisticados algoritmos para extraer los datos, gestionar la memoria para tener una mínima ocupación de memoria, cifrar la plantilla para garantizar la seguridad, implementar mecanismos de inserción y búsqueda de datos para garantizar su uso en aplicaciones con alta demanda, la tasa de aceptación falsa y la tasa de rechazo falsa dependen totalmente de estos algoritmos. La comunicación por USB (Universal Serial Bus) lo convierte en un dispositivo con alta integración con la plataforma Raspberry Pi ya que es una de las interfaces de comunicación más utilizadas en el mundo, la cantidad de plantillas que se pueden almacenar está limitada por la capacidad de memoria disponible en el Raspberry Pi. Este lector ha sido utilizado en trabajos como [10].

2. **FINGERPRINT SCANNER GT-511C3:** Al implementar este dispositivo tenemos dos opciones extraer la imagen del lector y realizar el procesamiento por nuestra cuenta o utilizar el algoritmo SmackFinger 3.0 que viene incluido en el dispositivo lo cual es una ventaja ya que cuenta con instrucciones para la extracción, almacenamiento y comparación de huellas dactilares en tiempos menores a 1 segundo, el fabricante del dispositivo asegura una tasa de aceptación falsa de 0.001% y una tasa de rechazo falsa de 0.1%. La comunicación se realiza a través de los pines I/O de propósito general con los que cuenta la Raspberry Pi. Una de las principales desventajas es la capacidad de almacenamiento ya que está limitada a 200 plantillas de huellas dactilares. Este lector ha sido utilizado en trabajos como [11].
3. **ADAFRUIT ZFM-206SA:** Este lector tiene una forma muy similar de trabajar respecto al anterior, podemos extraer la imagen del lector y aplicar algoritmos para la extracción de las características de la huella dactilar o utilizar los algoritmos de extracción, almacenamiento y comparación con los que cuenta el lector, con un tiempo de respuesta menor a 1 segundo, la tasa de aceptación falsa que promete el fabricante es de 0.0008% mientras que para la tasa de rechazo falso tenemos la cantidad de 0.005%. La comunicación se realiza a través de los pines I/O de propósito general con los que cuenta la Raspberry Pi y la capacidad de almacenamiento está limitada a 162 plantillas de huellas dactilares. Este lector ha sido utilizado en trabajos como [12].

CONCLUSIONES

El trabajo mostrado en este artículo sirve como una guía para los desarrolladores de sistemas que tengan como necesidad implementar el reconocimiento de huellas dactilares a sus aplicaciones utilizando un sistema embebido en este caso Raspberry Pi, las particularidades de los sistemas embebidos como el bajo costo, bajo consumo de energía y el rápido crecimiento que se ha observado en la comunidad de desarrolladores conlleva a que cada vez existan más fabricantes interesados en crear hardware y software compatible con sistemas embebidos, esto ha propiciado a la búsqueda de mejores, métodos, técnicas, herramientas y procesos de desarrollo que garanticen productos de calidad y con una amplia gama de aplicaciones y desarrollos tecnológicos.

El reconocimiento de huellas dactilares es uno de los métodos más populares y precisos dentro de las tecnologías biométricas. Ésta es utilizada en aplicaciones en tiempo real, sin embargo, este método implementado en sistemas embebidos como Raspberry Py es una solución en fase de desarrollo. Después de analizar los atributos de los lectores biométricos se recomienda utilizar el FINGERPRINT SCANNER GT-511C3 porque es el lector más rápido a la hora de extraer, comparar y almacenar las plantillas de huellas dactilares, el tiempo es un factor fundamental en estos procesos. Además, aunque presenta un porcentaje de rechazo falso mayor respecto al lector ADAFRUIT ZFM-206SA se debe a que realiza comparaciones de 1:N en una base de datos de mayor tamaño para verificar la identidad de las personas, hay que tomar en cuenta que en la actualidad no existe un método de comparación que entregue una coincidencia exacta entre las características de la imagen de entrada y las almacenadas en la base de datos, la cual es interna, agregando una ventaja ya que la compresión y cifrado de los datos es operado por el dispositivo, por último no está de más mencionar que el dispositivo cuenta con amplia documentación por parte del fabricante [6] .

AGRADECIMIENTOS

Los autores reconocen en gran medida al Consejo Nacional de Ciencia y Tecnología (CONACYT, México) por su apoyo financiero.

REFERENCIAS

[29] Maya Bineteskaya, Pedro Tomé Gonzáles. 2013.Reconocimiento Facial en el Ámbito Forense. Universidad Autónoma de Madrid, Escuela Politécnica Superior.

[30] A. A. Ross et al. Handbook of Multibiometrics.2006. Springer.

[31] Obtenido de: https://www.crossmatch.com/wp- content/uploads/2017/05/20160125-DS-En-DigitalPersona- U.are_.U-SDK-for-Windows.pdf

[32] Obtenido de: http://micklord.com/foru/Raspberry%20Pi%20Pages%20from%20Computer%20Shopper%202015-02.pdf

[33] Obtenido de: http://histinf.blogs.upv.es/2013/12/18/raspberry-pi/

[34] Obtenido de:https://cdn.sparkfun.com/datasheets/Sensors/Biometric/GT-511C3_datasheet_V2.1_20161025.pdf

[35] Obtenido de: https://cdn learn.adafruit.com/downloads/pdf/adafruit-optical- fingerprint-sensor.pdf

[36] Obtenido de: https://github.com/dlech/fprint-demo

[37] Obtenido de: https://github.com/pyserial/pyserial

[38] Cristaldo, R., Cespedes, J., Villalba C., Mendez, E,. (2013). Un enfoque de integración entre fprint y sourceAFIS, Jornadas Argentinas de Software Libre.

[39] Sapes, J., Solsolna, F., (2016). FingerScanner: Embedding a Fingerprint Scanner in a Raspberry Pi, Department of Computer Science and INSPIRES, University of Lleid.

[40] Nhevera, Dickson., (2014). Fingerprint and NFC authentication Brick, Universiteit Stellenbosch University.