Sistema de Seguridad Basado en una Plataforma Heterogénea Distribuida

Diana Lora[+], Pablo Cerro[*], Alberto A. Del Barrio[+], Guillermo Botella[+]

Departamento de Arquitectura de Computadores y Automática, Facultad de Informática de la Universidad Complutense de Madrid
+{dlora, abarriog, gbotella}@ucm.es, * pablo.cerro.canizares@gmail.com

Resumen. Este trabajo presenta el proyecto "Ecosistema Digital de Seguridad", realizado en la asignatura Sistemas Empotrados Distribuidos, perteneciente a la titulación Máster en Ingeniería Informática de la Universidad Complutense de Madrid. En este trabajo se describe e implementa un sistema de seguridad por medio de una plataforma heterogénea, cuyo objetivo es la verificación de los usuarios autorizados. En concreto, la placa Raspberry Pi se encarga del reconocimiento de la imagen y la contraseña, mientras que la STM32F4 Discovery sirve de interfaz con el usuario, recibiendo la contraseña y enviándosela a la Raspberry a través de la interfaz RS-232.

Palabras Clave: Seguridad, Raspberry Pi, STM32F4 Discovery, Ecosistema de Seguridad, Sistemas Empotrados Distribuidos.

Abstract. This work presents the project entitled "Digital Security Ecosystem", carried out as a final project in the Distributed Embedded Systems subject, which belongs to the Computer Engineering Master, at the Complutense University of Madrid. In this work, a security system is described and implemented through a heterogeneous platform, whose objective consists of the authorized users' verification. Concretely, the Raspberry Pi board is responsible for identifying the image and the password, while the STM32F4 Discovery board acts as the user interface, receiving the password which will be sent to the Raspberry by using the RS-232 interface.

Keywords: Security, Rasberry Pi, STM32F4 Discovery, Security Ecosystem, Distributed Embedded Systems.

1 Introducción

En la actualidad, la globalización y la alta competitividad hacen que las organizaciones tengan mayor cuidado con la información vital que poseen. La necesidad de mantener el conocimiento de una organización en secreto ha traído el rápido desarrollo del sector de la seguridad, con el fin de evitar que información importante se encuentre accesible a la competencia.

Por tanto, son necesarias nuevas medidas de seguridad que vayan de la mano con las tendencias tecnológicas. Por ello, la biometría [2] ha tomado mayor fuerza en el mercado, ya que une la biología del ser humano con la seguridad. La biometría es una tecnología de reconocimiento de características físicas únicas de las personas, como por ejemplo el reconocimiento facial, reconocimiento del iris, la huella digital o tono de la voz. Los sistemas biométricos están compuestos de un dispositivo de captura y un software biométrico que interpreta la muestra y la transforma en una secuencia numérica. Debido a que los seres humanos tenemos características morfológicas únicas que nos diferencian de los demás, la biometría es considerada en la actualidad como el método mejor catalogado para la identificación humana [2].

El reconocimiento facial [3] es un tipo de aplicación de la biometría donde se puede identificar a una persona por medio de patrones del rostro. Este tipo de aplicaciones son comúnmente utilizadas en sistemas de seguridad por la gran fiabilidad y eficiencia que brindan. La mayor parte del software de reconocimiento facial está basado en códigos numéricos llamados *faceprints* [3]. Estos sistemas utilizan 80 puntos nodales del rostro humano para medir diferentes variables como son: ancho o alto de la nariz, la profundidad de las cuencas de los ojos y la forma de los pómulos, etc. Dichos puntos nodales son identificados en una imagen digital de la cara de un individuo, y posteriormente almacenados en forma de código numérico o faceprint. El faceprint se utiliza como base para la comparación con los datos capturados a partir de caras en imágenes o vídeos.

Gracias a la tecnología anteriormente descrita se hace más efectiva la autenticación y acceso del personal de una organización a un sistema o instalación. Previamente al desarrollo de la biometría, el acceso del personal a una instalación se hacía a través de una código secreto que cada individuo posee. Sin embargo, este método no es completamente fiable debido a que otra persona puede ingresar credenciales ajenas. Con la ayuda de la biometría se tiene la garantía de que la persona solicitando acceso a un sistema es en efecto quien dice ser.

Una de las necesidades principales de los sistemas de seguridad es la distribución de sus diferentes componentes y la interacción entre ellos. Por tanto, es un ejemplo de aplicación muy adecuado de los conceptos estudiados en la asignatura Sistemas Empotrados Distribuidos (SEDs) [9]. El sistema digital de seguridad es un SED que consta de dos componentes que interactúan entre sí, por medio de interfaz RS-232, con la finalidad común de verificar las credenciales del usuario.

El resto del artículo se organiza de la siguiente forma: la Sección 2 describe el diseño del sistema, mientras que la Sección 3 trata los detalles de implementación del mismo. En la Sección 4 se evalúa la plataforma por medio de varios experimentos y finalmente en la Sección 5 se presentan nuestras conclusiones, así como posibles líneas de trabajo futuro.

2 Diseño del Sistema Digital de Seguridad

Un ecosistema digital es cualquier sistema distribuido, con propiedades de auto-organización, de escalabilidad y sostenibilidad, que está inspirado en los ecosistemas naturales [1]. Dichos sistemas son entornos extendidos e interconectados, donde se intercambian datos entre sus componentes. Un ejemplo claro de ecosistema digital es la propia Internet.

El sistema digital de seguridad del presente proyecto está basado en dichos ecosistemas, y consta de dos componentes, como puede observarse en la Figura 1:

- El módulo de identificación de contraseñas. Este bloque será el encargado de recibir la clave introducida por el usuario, y enviarla al módulo reconocedor. Será implementado sobre la placa STM32F4 Discovery [11].
- El modulo reconocedor de usuarios. Este componente recibirá la clave del anterior módulo, y decidirá si pertenece al sistema o no. Además, realizará el reconocimiento facial del usuario. Combinando ambas informaciones, decidirá si el usuario puede acceder al sistema. Dicho bloque se implementará finalmente con la placa Raspberry Pi [10,12] y una cámara [6].

Estos dos componentes tienen su funcionalidad específica, pero existe una interacción entre ellos para la toma de decisiones y el funcionamiento correcto del sistema.

El flujo del sistema digital de seguridad es el siguiente:

1. Se identifica el usuario por medio de reconocimiento facial.
2. El usuario ingresa la contraseña en la plataforma STM32F4 Discovery.
3. La plataforma STM32F4 Discovery envía la contraseña a la Raspberry Pi.
4. La Raspberry Pi valida la contraseña con la que tiene almacenada en su base de datos.
5. La Raspberry Pi envía 1 para confirmar que el usuario tiene autorización y 0 para denegar acceso.
6. La plataforma STM32F4 Discovery le muestra al usuario el mensaje de “Bienvenido!” o “Denegado” de acuerdo a la respuesta recibida.

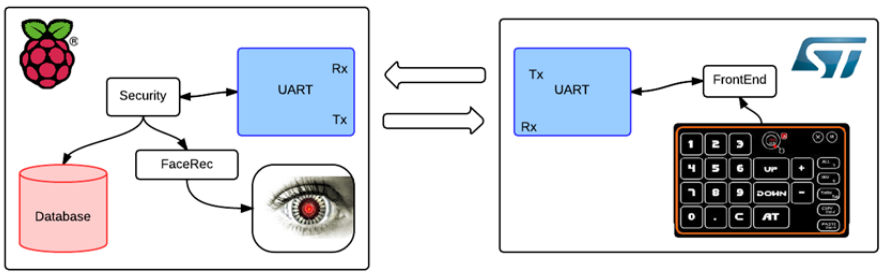

Figura 1. Diagrama de comunicación entre plataformas.

3 Implementación

En esta sección se describen los detalles de implementación del sistema. Primeramente hablaremos en profundidad de las funcionalidades realizadas por cada uno de los componentes, y posteriormente se explicará el proceso de envío de datos entre ambas placas.

3.1 STM32F4 Discovery

En el sistema digital de seguridad propuesto la plataforma STM32F4 Discovery es la encargada de recibir la contraseña ingresada por el usuario, enviarla a la Raspberry Pi y esperar respuesta de autenticación de usuario. La Figura 2 muestra un diagrama de bloques ilustrando estas ideas.

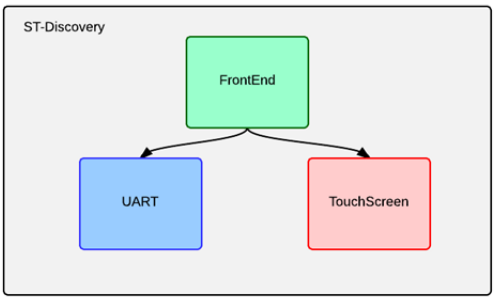

Figura 2. Funcionalidades realizadas por la plataforma STM32F4 Discovery.

Para la creación de la funcionalidad previamente descrita, se desarrolló una aplicación en el lenguaje de programación C# con acceso a los componentes necesarios de la STM32F4. En este caso, es preciso acceder a la pantalla táctil y la USART, que implementa la interfaz RS-232. La aplicación consiste en mostrar en pantalla un teclado numérico en el que el usuario ingresa su contraseña y cuando éste seleccione “Enviar”, la contraseña será enviada a la Raspberry Pi.

3.2 Raspberry Pi & Cámara

La Raspberry Pi implementa diferentes funcionalidades en el sistema. Por un lado, contiene la base de datos de contraseñas y realiza la autenticación de usuarios. Además, posee un sistema de reconocimiento facial, basado en la integración de una cámara y en el uso de las librerías OpenCV [5], que le permite detectar el rostro del usuario. La Raspberry Pi tiene un sistema de seguridad programado en C, el cual consulta en la base de datos de los usuarios registrados la validez de la información recibida. Finalmente, responde a la STM32F4 Discovery si la credencial recibida (clave+imagen) tiene acceso o no.

La Figura 3 muestra un diagrama con las funcionalidades principales implementadas por la Raspberry Pi.

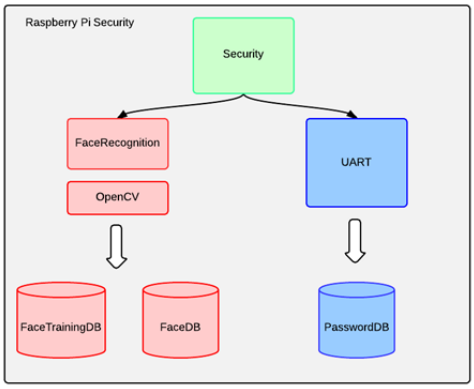

Figura 3. Funcionalidades realizadas por la plataforma Raspberry Pi.

Para realizar los cálculos referentes a la detección y reconocimiento facial se utilizan las librerías de código abierto OpenCV. Estas librerías son APIs sencillas, las cuales ofrecen diferentes funcionalidades como: machine learning, detección de objetos, efectos fotográficos, aceleración por GPU, y visión por computador. Ésta última es la utilizada en este proyecto. En [16] se muestran los pasos realizados para la configuración de las librerías SimpleCV y OpenCV en la Raspberry Pi. El algoritmo de reconocimiento de imagen es el *Haar Cascade Classifier*, capaz de obtener tasas de reconocimiento en torno al 95% y superiores [17,18].

3.3 Comunicación entre Plataformas

Para la comunicación entre las plataformas se utiliza la USART (Universal Synchronous/Asynchronous Receiver/Transmitter). Una USART es un dispositivo que permite la comunicación entre dispositivos por medio del puerto serie usando el protocolo RS-232C [4].

En el caso de la plataforma STM32F4 Discovery se utiliza la USART1, donde el pin PA10 sirve para recibir datos y el pin PA9 para enviar. Para la Rasberry Pi el pin 8 es el de envío de datos y el pin 6 es el encargado de la recepción de datos. En la Figura 4 se muestran la ubicación de los pines de la USART de la Raspberry Pi.

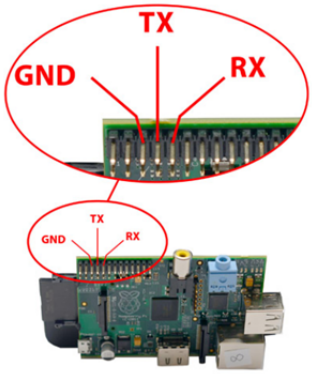

Figura 4. Identificación de pines en Raspberry Pi.

A continuación, debemos conectar los pines de transmisión y recepción de cada dispositivo de manera cruzada, es decir el pin USART-aRX del dispositivo A ha de conectarse al pin USART-bTX del dispositivo B (análogamente para USARTaTX USARTbRX). Además, es necesario que ambos compartan una toma de tierra (GND). La Figura 5 muestra la interconexión de ambas placas.

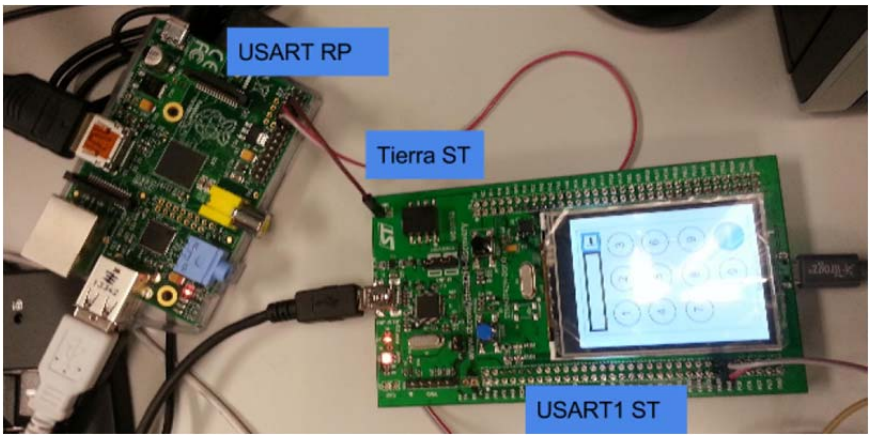

Figura 5. Configuración física del sistema.

4 Resultado

Para llegar a completar con éxito la construcción del sistema tras su modelado y configuración, se realizaron pruebas con las dos plataformas individualmente. Una vez probado que ambas plataformas funcionaban correctamente de manera individual, se procedió al ensamblaje final.

Para la realización de las pruebas se utilizó Termite [8]. Este programa es un terminal RS-232. Tiene una interfaz similar a una consola en la que se en la cual se muestra la información enviada por ambas plataformas.

A continuación se detallan en profundidad las pruebas realizadas para comprobar el funcionamiento del proyecto.

4.1 Análisis experimental con STM32Discovery

Para validar del correcto funcionamiento de la aplicación desarrollada sobre la plataforma STM32F4 Discovery, se conectó la placa al puerto serie de un PC y se probó la conectividad con el programa Termite. La prueba consistió en ingresar la contraseña en la placa de la plataforma STM32F4 Discovery, pulsar el botón enviar y comprobar que la información mostrada por Termite se correspondía a la ingresada en la Discovery.

4.2 Análisis experimental con Raspberry Pi

Al igual que las pruebas realizadas con la plataforma STM32F4 Discovery descritas en el apartado anterior, se decidió interconectar la Raspberry Pi con el puerto serie de un PC utilizando el programa Termite. Esta prueba fue realizada para comprobar la compatibilidad de la UART de RaspberryPi con una plataforma distinta.

Además, con el objetivo de comprobar el correcto funcionamiento de las librerías de visión artificial OpenCV, se realizaron pruebas inicialmente con imágenes estáticas proporcionadas por la librería de OpenCV y externas a ésta. Los resultados fueron favorables ya que el sistema reconocía exitosamente el rostro de la persona. La Figura 6 muestra un ejemplo de reconocimiento facial estático.

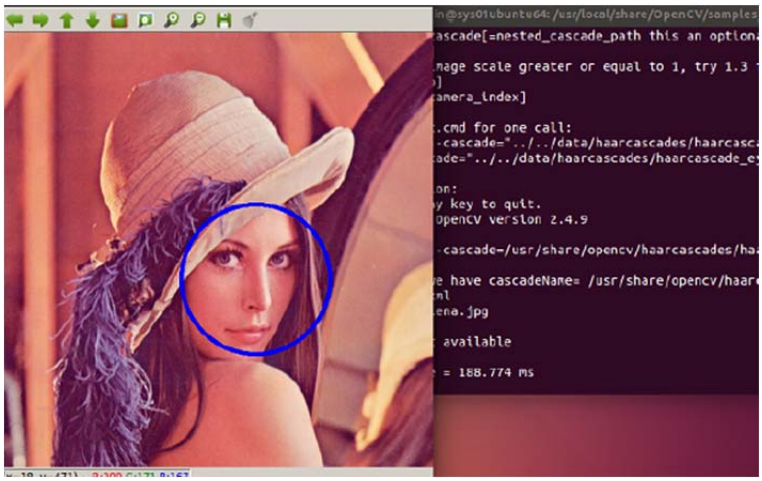

Figura 6. Pruebas OpenCV con imagen estática.

Posteriormente se realizaron pruebas con vídeos para validar que igualmente que con las imágenes, las librerías de OpenCV podían reconocer el rostro humano. La Figura 7 muestra un ejemplo de reconocimiento facial dinámico.

4.3 Análisis experimental con el sistema completo

Por último, se procedió a conectar las dos plataformas por puerto serie, como se mostró en la Figura 5. En la Sección 3.3 se encuentran los pines utilizados para la conexión entre la STM32F4 y la Raspberry Pi. Una vez conectado el sistema completo, el conjunto de pruebas realizadas en sistema digital fueron las mostradas en la Tabla I.

Además, se realizó un vídeo [13] en el que se puede observar el funcionamiento completo del sistema. La plataforma STM32F4 Discovery envía la contraseña introducida por el usuario a la Raspberry Pi. Ésta valida la contraseña en la base de datos, y si es correcta realiza el reconocimiento facial del individuo. La Rasberry Pi devuelve una variable validando o denegando el acceso de la persona.

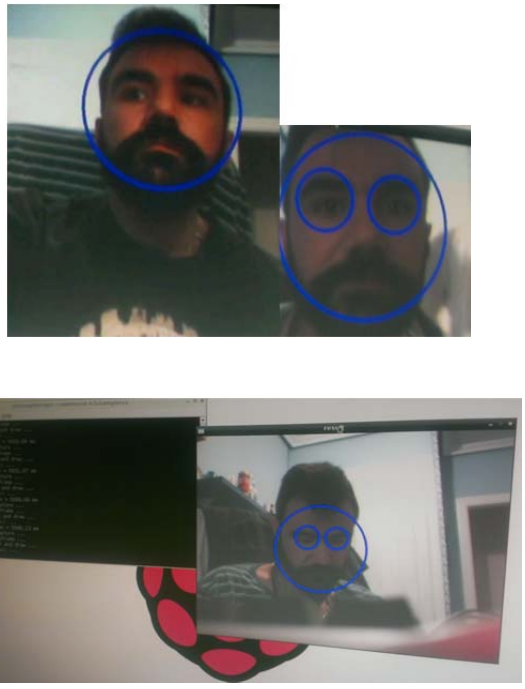

Figura 7. Proceso de identificación a través de cámara.

Tabla I. Casos probados para demostrar la funcionalidad del sistema

# Caso	Discovery	Raspberry Pi	Resultado
1	Contraseña correcta	Faceprint correcto	OK
2	Contraseña correcta	Faceprint incorrecto	Fallido
3	Contraseña incorrecta	Faceprint incorrecto	Fallido
4	Contraseña incorrecta	Faceprint correcto	Fallido

5 Conclusiones y Trabajo Futuro

En este artículo se ha presentado un sistema digital de seguridad. Dicho sistema trata de explotar tanto las virtudes de los sistemas empotrados distribuidos (bajo consumo, escalabilidad y tolerancia a fallos) como de la biometría. Por medio de dos placas de bajo consumo y coste, es posible implementar un sistema de alta seguridad basado en el reconocimiento de claves y el reconocimiento facial.

Como líneas futuras se podría refinar el sistema, siendo capaz de reconocer a diferentes personas y administrar distintos perfiles de seguridad para cada una de ellas. Por ejemplo, a partir de cierta hora únicamente dejar pasar a los directivos, denegar el acceso a personas despedidas, si se detecta a algún intruso comunicarse con la policía, etc.

Otra mejora interesante sería la sustitución de la comunicación serie por elementos wireless, como ZigBee, Bluetooth o incluso WiFi, y la aplicación de un protocolo de seguridad para el envío de claves, como RSA [19]. Usando una comunicación wireless, se podría escalar fácilmente el sistema y crear un sistema de cámaras distribuidas. De esta manera, podrían causar baja cualquiera de las cámaras vigilantes y el resto del sistema podría seguir funcionando, enviando una alarma por la baja causada.

Referencias

1. Santamaría, Fernando. (2010). Una introducción a los ecosistemas digitales. Recuperado de http://fernandosantamaria.com/blog/2010/07/unaintroduccionalosecosistemasdigitales/
2. Sánchez Calle, Ángel. (2008). Aplicaciones En La Visión Artificial Y La Biometría Informática, Dykinson S.L.
3. Harry Wechsler (1998). Face Recognition: From Theory to Applications, Springer.
4. Ben Cohen (2001). Component Design by Example … A Step-by-Step Process Using VHDL with UART as Vehicle, VhdlCohen Publishing.
5. Eben Upton (2013). Raspberry Pi User Guide, Wiley, 3rd edition.
6. Simon Monk (2014). Raspberry Pi Cookbook, O'Reilly Media.

7. Horne, M. (2014). Raspberry Jam Potton Pi & Pints. Recuperado de http://www.recantha.co.uk/blog/?p=5261
8. CompuPhase. (2015). Termite: a simple RS232 terminal. Recuperado de http://www.compuphase.com/software_termite.htm
9. Máster en Ingeniería Informática de la Universidad Complutense de Madrid, http://informatica.ucm.es/estudios/2014-15/master-ingenieriainformatica
10. C. Edwards, Not-so-humble raspberry pi gets big ideas, Engineering Technology 8 (3) (2013) pp. 30-33.
11. STM32F4. (2014). Discovery kit for STM32F407/417 line: Data Brief. Recuperado de http://www.st.com/st-web-ui/static/active/en/resource/technical/document/data_brief/DM00037955.pdf
12. Raspberry Pi Foundation. Setting up your RasberryPi. Recuperado de http://www.raspberrypi.org/help/quick-start-guide/
13. Ecosistema Digital de Seguridad. Pruebas de Validación. Recuperado de https://www.youtube.com/watch?v=ZUqM24PdnIw&feature=youtu.be
14. Crisan, C. (2014). Motion Eye with Raspberry Pi. Recuperado de http://www.howtoembed.com/projects/raspberrypi/95motioneyewithraspberrypi
15. Stan Z. Li, Anil K. Jain (2011). Handbook of Face Recognition, Springer, 2nd edition.
16. Araujo, M. (2013). RASPBERRY PI + SIMPLECV + OPENCV + RASPICAM CSI CAMERA. Recuperado de http://tothinkornottothink.com/post/59305587476/raspberry-pi-simplecv-opencv-raspicam-csi-camera
17. P. I. Wilson and J. Fernandez. 2006. “Facial feature detection using Haar classifiers”. *J. Comput. Sci. Coll.* 21, 4 (April 2006), 127-133.
18. Viola, P.; Jones, M., "Rapid object detection using a boosted cascade of simple features," Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2001, pp.I-511,I-518.
19. Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué. “El criptosistema RSA” RA-MA S.A. Editorial y Publicaciones, 2005.