Servicio Web de identificación biométrica sobre FPGA para dispositivos móviles Wi-Fi

David Rodríguez [1], Juan M. Sánchez [1], Arturo Duran[1]

[1] Área de Arquitectura y Tecnología de los Computadores
Esuela Politécnica, Universidad de Extremadura
Campus Universitario S/N 10071 Cáceres
{drlozano, sanperez, aduran}@unex.es
http://atc.unex.es

Abstract. En el presente artículo proponemos una arquitectura completa que cumple el estándar BioAPI, basada en un servicio Web XML y hardware reconfigurable, para la identificación y verificación biométrica móvil de individuos mediante el uso de su huella dactilar. Se plantea un sistema cliente servidor, en el que se utiliza como cliente Web biométrico un Asistente Digital Personal (PDA) provisto de un sensor biométrico y de tecnología inalámbrica WiFi, y de un servidor de aplicación biométrica, soportado sobre un Proveedor de Servicios Biométricos (BSP) parcialmente implementado sobre un dispositivo hardware reconfigurable. BioAPI da acceso a las funciones de *enrolment*, *identification* y *verification* mediante un BSP acelerado por lógica reconfigurable (FPGA).

1 Introducción

La identificación biométrica es la autentificación y/o verificación de la identidad de una persona basado en características de su cuerpo o de su comportamiento, utilizando por ejemplo el iris de su ojo, su voz o su huella dactilar. Los métodos de identificación biométrica son una herramienta eficaz para identificar personas. Las huellas dactilares están reconocidas como prueba fidedigna de identidad, siendo un sistema de autenticación efectivo, cómodo y rápido de aplicar.

Las nuevas tecnologías permiten en la actualidad disponer de dispositivos móviles en forma de ordenadores de mano o PDAs con sensores biométricos para la captura y procesamiento de huellas dactilares. Esto unido a las emergentes tecnologías inalámbricas, permiten desarrollar aplicaciones para la identificación o verificación de individuos en espacios públicos o abiertos, como los aeropuertos, zonas de ocio, centros de enseñanza, etc.

Las PDAs y los nuevos *Smart Phones* (teléfonos con microprocesador, memoria, pantalla y sistema operativo), tienen limitaciones computacionales y de almacenamiento grandes, con lo que se requiere de una arquitectura cliente servidor para poder realizar identificaciones rápidas y fiables de un individuo contra una población grande de huellas, identificación 1:N.

Por otro lado, los servicios Web XML proveen un modelo basado en estándares simples y flexibles, para la interconexión de aplicaciones sobre Internet, aprovechando las infraestructuras existentes, siendo la evolución natural de las arquitecturas distribuidas en Internet [1][2].

Por último, el hardware reconfigurable ha sido utilizado con éxito en múltiples ocasiones para la realización de tareas de cifrado, reconocimiento de patrones, criptografía, etc., que son por naturaleza problemas intratables y de complejidad computacional muy elevada, bien como sistemas embebidos o servidores dedicados [4].

A la vista de estas consideraciones, proponemos el diseño de un sistema completo de autentificación/verificación biométrica de huellas dactilares, basado en una aplicación cliente-servidor para dispositivos móviles (PDA o *Smart Phone*), utilizando servicios Web XML y un BSP acelerado mediante hardware reconfigurable. Las ideas clave del presente trabajo son:

- Introducir la biometría dactilar y el estándar BioAPI, secciones 2 y 3.
- Identificar los elementos que componen la arquitectura propuesta, sección 4.
- Definir la arquitectura y funcionalidades de la aplicación cliente, sección 5.
- Por último, descripción del servicio Web XML de identificación biométrica sobre FPGA, sección 6.

2 Biometría basada en huellas dactilar

La identificación vía huellas dactilares se lleva a cabo mediante la comparación de ciertas características que se extraen de las mismas llamadas minutiaes. Y que son el resultado del análisis de las crestas de fricción (*ridge*) y de los valles (*valley*) que se visualizan en las imágenes de las huellas. Estos minutiaes son clasificados en 18 tipos por algunos métodos, si bien como muestra la figura 1, son combinación de dos tipos básicos: final de cresta (*ending*) y bifurcación de cresta (*bifurcation*) [5].

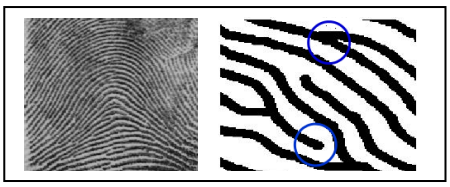

Fig. 1. Huella y detalle de los dos tipos de minutiaes

Los algoritmos de identificación tradicionales están basados en la utilización de funciones de reconocimiento de patrones de puntos para la comparación de minutiaes, y por tanto, los sistemas implementados que los utilizan suelen almacenar únicamente para cada individuo los minutiaes que caracterizan su huella dactilar.

La aplicación a los minutiaes de algoritmos de reconocimiento de patrones de puntos o locales, ofrece problemas en determinados casos, como son imágenes de huellas

de baja calidad de las que se extraen un número pequeño de minutiaes, alteración de las condiciones de humedad o temperatura en la que se capturaron las imágenes, atenuación de los ridge o modificaciones no lineales de las huellas. Todos estos factores hacen que la identificación de individuos basada en este tipo de algoritmos sea tratada como un problema computacionalmente complejo [6].

Este tipo de algoritmos pueden mejorar su efectividad utilizando métodos de reconocimiento de patrones de subáreas o globales, que utilizan la comparación de áreas de especial interés en lugar de puntos. Estas áreas se seleccionan de alrededor de los minutiaes, de áreas que cuenten con ridges que tengan baja curvatura o combinaciones de ridges poco usuales [7].

3 BioAPI

La utilización de todas estas técnicas para desarrollar sistemas automáticos de identificación de individuos, supone problemas de interoperabilidad. La huella de un usuario digitalizada y tratada por uno de los procesos desarrollados, puede no ser útil para su utilización con cualquiera de los algoritmos planteados.

Para solucionar estos problemas, desde diferentes comités internacionales se han desarrollado estándares para diferentes aspectos de la utilización de la biometría, como son: el formato para el intercambio de datos, estructuras de datos, protocolos de comunicación, etc. Uno de ellos es BioAPI y su objetivo es estandarizar el interfaz entre los componentes software y la arquitectura, ocultando en la medida de lo posible los detalles de la tecnología de biometría, facilitando así el desarrollo de aplicaciones que usen esta tecnología.

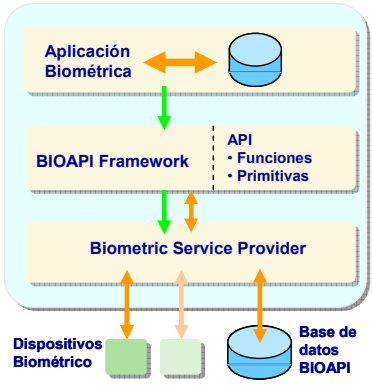

Fig. 2. Arquitectura del estándar BioAPI

La API propuesta por BioAPI ofrece a las aplicaciones funciones de alto nivel como *enrollment*, *verification* e *identification*. Mientras que el proveedor de servicios biométricos o BSP ofrece un conjunto de funciones de bajo nivel como son: *capture*,

process, createtemplate, *verifymatch*, e *identifymatch* orientadas directamente a la tecnología biométrica.

4 Arquitectura XML-BioAPI para entornos móviles

El sistema ha sido diseñado siguiendo una arquitectura de capas como la mostrada en la figura 3, utilizando un esquema cliente servidor, y una red de acceso y tránsito basada en tecnologías IP (red inalámbrica WiFi + Internet/Intranet). Se utiliza tecnología Web estándar para la comunicación entre la aplicación cliente y el servidor, siendo las funciones principales de cada elemento las siguientes:

- Aplicación cliente: se trata de una aplicación basada en un navegador Web y sus extensiones (ActiveX, Applets y JavaScript) la cual actúa como interfaz entre el usuario y el proveedor de servicios biométricos BSP.
- Servidor de aplicación y BSP: consiste en un servicio Web XML con las extensiones software y hardware necesarios para implementar las primitivas propuestas en BioAPI. El BSP diseñado implementa un subconjunto de sus funciones sobre hardware reconfigurable, utilizando una FPGA Virtex de Xillinx sobre una placa de prototipos RC1000 de Celoxica.
- Base de Datos: es compatible con el estándar ISO CBEFF (NISTIR 6529).

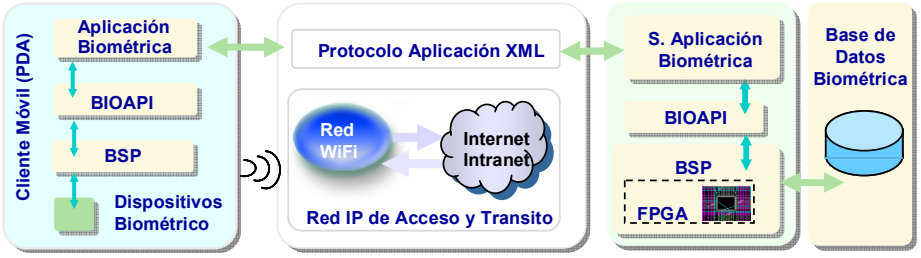

Fig. 3. Visión global de la arquitectura propuesta

Las ventajas de utilizar una arquitectura cliente servidor basada en tecnologías Web sobre una red IP son varias:

- Permite independizar la arquitectura cliente hardware y software del medio de acceso (WiFi, Ethernet, Bluetooth, GPRS/UMTS) y de la la red de transito IP (ATM, Frame Relay, SONET).
- El mantenimiento y distribución de la aplicación cliente se facilita utilizando un servidor Web, la aplicación modificada se descarga de forma automática desde el servidor a los clientes.

5 Aplicación cliente

En el diseño de la aplicación cliente, se ha buscado una arquitectura flexible que permita cubrir tanto un escenario como el propuesto PDA y WiFi, como otros modelos de acceso y aplicaciones, como por ejemplo, un *Smart Phone* y UMTS o un PC con ADSL. También, se ha buscado emplear un interfaz grafico de usuario amigable y sencillo de utilizar, por lo que se decidió utilizar una aplicación basada en un navegador Web estándar.

Para la aplicación cliente, se plantearon dos posibles implementaciones, ambas debían poder utilizar las funciones proporcionadas por las librerías de BioAPI y gestionar la información auxiliar necesaria (nombre, sexo, edad, fotografía…) para realizar el proceso de identificación biométrica de un individuo, las opciones estudiadas han sido:

- Applet Java: utilizando como host un navegador Web equipado con una Maquina Virtual Java (JVM) y como herramientas de desarrollo el *Java Development Kit* (JDK) y el *Abstract Window Toolkit* (AWT). Tiene como ventaja la interoperabilidad entre distintos sistemas operativos y plataformas. Por el contrario es más lento que el código nativo y hay menos soporte y drivers para el acceso al hardware biométrico.
- Control ActiveX: el host es también un navegador Web, que soporte bien de forma nativa o mediante el uso de un *plug-in* controles ActiveX. Tiene como ventaja una ejecución nativa más rápida, más librerías y mayor soporte para el acceso al hardware. En contra una menor interoperabilidad entre sistemas operativos y al requerir Windows o un plug-in compatible.

5.1 Prototipado de la aplicación cliente

El dispositivo seleccionado para soportar la aplicación cliente, es una PDA Ipaq H5550 de Hewlett-Packard, con un microprocesador Intel PXA255 a 400Mhz con tecnología Xscale, 128Mb de memoria SDRAM y 48Mb de memoria Flash ROM, pantalla TFT de 240x320 y 65.000 colores.

Dispone de tecnologías inalámbricas Bluetooth y WLAN 802.11b, así como de un sensor *biométrico* para la lectura de huellas dactilares. La figura 4 muestra la PDA Ipaq H5550 solicitando la identificación del propietario del dispositivo para poder iniciar sesión.

La versión de la PDA es Pocket PC 2003 con sistema operativo Windows CE 4.20. Se ha utilizado el Pack de encriptación de 128 bits para cifrar la transmisión de la información a través de *Internet* o la intranet, añadiendo una capa adicional de seguridad al cifrado WEP.

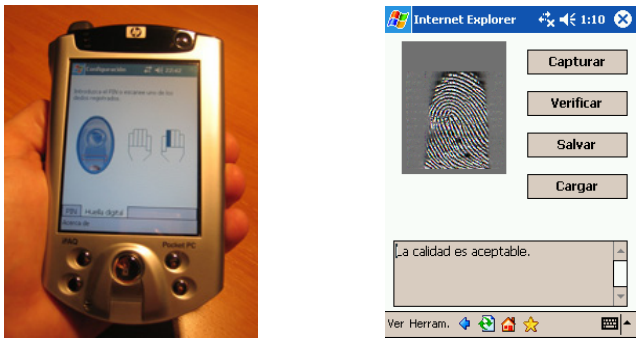

Fig. 4. PDA interfaz gráfico de la aplicación cliente ejecutándose sobre IExplorer

El sensor biométrico AT77C101B instalado en la PDA H5550, denominado FingerChip, es un sensor desarrollado por Atmel Corporation y cuyas características principales son:

- Sensor térmico CMOS.
- Area de escaneado de 0,4 mm x 14 mm.
- Array de la imagen: 8 x 280 = 2240 pixels
- Tamaño de pixel: 50 µm x 50 µm = 500 dpi

El software biométrico de preprocesamiento e identificación local esta desarrollado por Cogent Systems, Inc.

Para realizar una prueba de la arquitectura propuesta, se ha optado por utilizar un cliente basado en una aplicación Windows en forma de un control ActiveX, el cual es invocado desde el navegador Web Internet Explorer para Pocket PC. Para dar soporte a la aplicación biométrica, ha sido necesario instalar en la PDA las librerías:

- HP Ipaq Biometric Toolkit.
- BioAPI Consortium Framework.
- Microsoft .Net Compact Framework

6 Servicio Web XML de identificación biométrica

El servicio Web RC1000_BIOAPI implementa y soporta la conectividad de los clientes remotos a las funciones de alto nivel del estándar BioAPI *enrolment*, *identification* y *verification.*

Las llamadas a las funciones anteriores se traducen en llamadas de bajo nivel soportadas por el BSP. El BSP del prototipo cuenta con parte de estas funciones implementadas sobre la FPGA VIRTEX de la tarjeta RC1000 de Celoxica.

Los clientes inalámbricos pueden consumir los servicios del servidor de aplicación biométrico de dos formas distintas como muestra la figura 5, y descritas en los apartados 6.1 y 6.2.

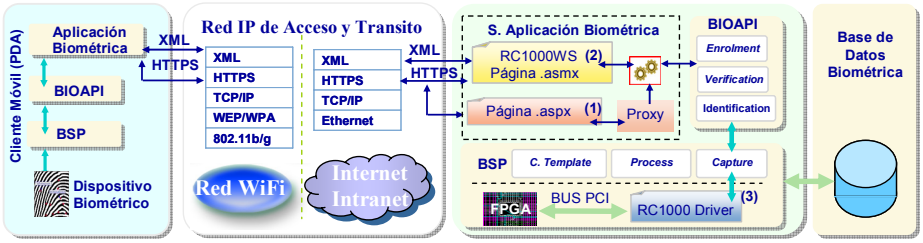

Fig. 5. Arquitectura, protocolos y dispositivos empleados en el prototipo

6.1 Acceso mediante servidor de aplicación

El servidor de aplicación, identificado con un (1) en la figura 5, publica sus recursos mediante páginas Web dinámicas con extensión .aspx, en las cuales se crea una instancia del Proxy que sirve de intermediario entre la página .aspx y el servicio Web que invocará las funciones de BioAPI. El resultado de las operaciones biométricas solicitadas, son devueltos al cliente desde la página .aspx del servidor de aplicación.

El servidor de aplicación controla el acceso a los recursos y puede implementar las funciones de *accounting* de los usuarios. Los protocolos utilizados en el caso (1) son HTTPS para el intercambio entre el Cliente Web y el Servidor de Aplicación, y XML-SOAP entre el Proxy y el Servicio Web.

6.2 Acceso directo al servicio RC1000_BIOAPI

La segunda opción, identificada con un (2) en la figura 5, se basa en la utilización de páginas .asmx de ASP.NET, que permiten un acceso directo al servicio Web. En la página asmx se describen: el espacio de nombres, las clases, propiedades y métodos del servicio Web XML. Para este escenario existen dos posibilidades:

- Primera, la aplicación cliente tipo ActiveX o Java Applet, la cual se comunica directamente mediante SOAP con el servicio Web sin necesidad de utilizar peticiones HTTPS.
- Segunda opción, la aplicación cliente interactúa con el navegador Web que la hospeda mediante JavaScript o VB Script. Siendo el código de la página Web el que se comunica con el servicio Web mediante peticiones HTTPS-GET y HTTPS-POST de páginas .asmx. Las peticiones de los clientes son interceptadas por el servidor Web IIS mediante un filtro ISAPI (Internet Server Application Programming Interface) que inicia un *runtime* que compila y ejecuta el código del servicio Web y devuelve el resultado en XML.

6.3 BSP basado en Hardware Reconfigurable

El BSP implementado en el servidor de aplicación biométrica está parcialmente soportado por algoritmos acelerados por una placa de prototipos RC1000 con una FPGA Virtex. El BSP propuesto en la arquitectura de BioAPI cuenta con cuatro funciones de bajo nivel que son susceptibles de ser implementadas en la FPGA. Estas funciones son: *process*, *createtemplate*, *verifymatch* e *identifymatch*.

La función *capture*, si bien es mantenida en el BSP, no tiene sentido en el lado del servidor si éste no cuenta con un sensor biométrico instalado.

Para el prototipo, se han implementado las funciones de la primitiva *process* del BSP, la cual se encarga del preprocesamiento y extracción de los minutiaes tomando como entrada la imagen de la huella dactilar capturada por el sensor de la aplicación cliente. En estos procesos se aplican algoritmos de tratamiento de imágenes como, filtros, umbralizaciones, adelgazamientos y operaciones morfológicas. Estos algoritmos se han implementado en Handel-C con éxito sobre la plataforma RC1000 en trabajos anteriormente [3].

Respecto a las funciones *verifymatch* e *identifymatch*, su implementación está ligada a la elección de un algoritmo de comparación de minutiaes. Para realizar este tipo de tareas se han utilizado normalmente algoritmos de pattern matching, bien de puntos o de zonas, o ambos simultáneamente.

La función *verifymatch* se encarga de la comparación 1:1 de huellas dactilares. Es decir, se comprueba que una huella (*sample*) coincide con una ya almacenada (*template*).

La función *identifymatch* realiza comparaciones 1:N de huellas dactilares. Comprueba si una determinada huella (*sample*) coincide con alguna de las huellas ya almacenadas en la base de datos biométrica.

Los algoritmos de pattern matching son algoritmos que pueden ser fácilmente pararelizables, existen implementaciones sobre FPGA que desmuestran la viabilidad y mejora en rendiemiento de una solución hardware-software sobre una solución software pura [8].

6.4 Acceso al hardware reconfigurable

Para los métodos de acceso descritos en 6.1 y 6.2 el acceso a los funciones del BSP implementadas en la FPGA, identificado con un (3) en la figura 5, se realiza a través del bus PCI mediante la utilización de las librerías de la tarjeta RC1000 (PP1000.lib) y del driver de la tarjeta.

7 Conclusiones y trabajos futuros

Hemos diseñado e implementado con éxito un prototipo que permite la identificación y verificación biométrica móvil de un individuo mediante un dispositivo PDA con tecnología WiFi y un servidor de aplicación Web XML biométrico acelerado con una FPGA.

Los puntos fuertes de nuestro trabajo incluyen: la utilización de una arquitectura que cumple con BioAPI como interfaz entre la aplicación cliente y la implementación hardware-software de las funciones del BSP, lo cual permite modificar fácilmente y de forma transparente los algoritmos de matching o la lógica reconfigurable. Permitiendo utilizar de forma dinámica componentes IP (Intelelectual Property) ya desarrollados. Otra ventaja es la utilización de tecnologías Web estándar, lo cual permite integrar el sistema diseñado en un gran número de entornos de explotación con mínimas modificaciones.

Los trabajos actuales y futuros incluyen el diseño y programación de la versión Java del cliente biométrico, y la implementación completa y estudio de rendimiento de las funciones *verifymatch* e *identifymatch* sobre la plataforma RC2000 de Celoxica.

Agradecimientos

El presente trabajo ha sido soportado parcialmente por el proyecto coordinado OPLINK TIN2005-08818-C04-03.

Referencias

1. Newcomer E.: Understanding Web Services: XML, WSDL, SOAP, and UDDI. Addison-Wesley (2002).
2. Kaye D.: Loosely Coupled: The Missing Pieces of Web Services. RDS Press (2003).
3. Rodríguez, D., Sánchez J.M., Gómez J.A.: Reconfigurable Hybrid Architecture for web Applications. Proceedings Field-Programmable Logic and Applications, 13th International Conference, FPL'03 (2003) pág. 1091-1094.
4. V.K. Prasanna and A. Dandalis, "FPGA-based Cryptography for Internet Security". Online Symposium for Electronic Engineers. (2000).
5. R.M. Bolle, A.W. Senior, N. K. Ratha and S. Pankanti, "Fingerprint Minutiae: A Constructuive Definition". Lecture Notes in Computer Science.
6. Ying HAO, Tieniu TAN, Yunhong WANG, "An effective Algorithm For Fingerprint Matching".
7. O. Svedin, M. Öbrink, J. Bergenek, "Precise BioMatch™ FingerPrint Technology". White Paper April 2004.
8. Fons M., Fons F., Canyellas N., Lopez M., Cantó E., "Codiseño Hardware-software de un Algoritmo de Matching Biométrico", JCRA 2003, pag. 399-406.