Validación de Firmas Ológrafas

Tamara D. Blum
Universidad de Palermo, AI-Group,
Ciudad de Buenos Aires, Argentina, C1175ABT
tdblum@hotmail.com, aigroup@palermo.edu

Ariel J. Sztern
Universidad de Palermo, AI-Group,
Ciudad de Buenos Aires, Argentina, C1175ABT
asztern@mail.com, aigroup@palermo.edu

y

Daniela López De Luise
Universidad de Palermo, Directora del Proyecto, Directora del AI-Group,
Ciudad de Buenos Aires, Argentina, C1175ABT
aigroup@palermo.edu

Abstract

The purpose of this paper is to present a prototype from recent research about new biometrics techniques for validating handwriting signatures. During this research it has been studied existent methods. It has been found enough data to discard those alternatives that are not efficient for a massive, portable and secure solution. This paper describes a prototype of an informatics solution named *PI-1*. This prototype has been designed to fulfill the following researched issues: portability, security, massiveness and functionality with low-cost hardware. Part of the project goals includes on-line and off-line processing for signatures, getting images from several devices such as cell phones, digital cameras, scanners or drawing tablets.

Keywords: Signature validation, Handwriting signature, Holograph, Biometric, Cryptography.

Resumen

El presente trabajo pretende dar a conocer la investigación realizada acerca de nuevos métodos de validación biométrica. Durante la misma se han estudiado los métodos existentes al día de hoy y se han encontrado motivos suficientes como para que los descartemos al analizar una solución masiva, portable y segura. Se describe la arquitectura general del prototipo de solución informática denominada *PI-1*. Este responde a los puntos investigados tomando como base que la solución sea portable, segura, masiva y funcional utilizando hardware económico. A su vez, parte de los objetivos incluyen el procesamiento on-line de las firmas, así como el off-line, obteniendo las imágenes desde diversos dispositivos al alcance de la mano, como pueden serlo teléfonos celulares, cámaras de fotos digitales, escáners o tabletas de diseño.

Palabras claves: Validación de firmas, Firmas manuscritas, Firmas ológrafas, Biometría, Criptografía.

INTRODUCTION

Aún hoy, en plena evolución informática y cuando las distancias se ven acortadas en muchos aspectos, se puede observar que esos mismos avances no han podido ayudar demasiado en otras áreas. Trámites que requieren de la presencia física del individuo, dado que no pueden ser realizados de otra forma, personas que deben presenciar y dar fe de actos que se llevan a cabo y se rubrican con la firma como por ejemplo las escrituras de compra-venta inmobiliaria, autorizaciones, cesiones de poder, y tantos otros. La firma manuscrita sigue siendo la forma elegida para dar validez a los documentos, presentaciones, etc. [1].

Si bien existen otros mecanismos para validar la identidad de una persona, la firma manuscrita es la forma más natural y la que menos somete al individuo a situaciones incómodas. Es un mecanismo no invasivo y tiene menor margen de error que la validación a través de huellas dactilares, otro de los mecanismos no invasivos existentes.

No sería insensato pensar en una base de datos administrada por un ente confiable, que permita validar que la persona que firma un documento es quien dice ser.

Aún si se encontrara una solución adecuada, como la que se propone en el presente trabajo, hay algunos temas con los que será inevitable lidiar y nada tienen que ver con la tecnología, ni con lo que ella puede ofrecer; o la forma en que puede ayudar: profesionales e instituciones que tienen establecida una metodología para realizar este tipo de tareas. La implementación de estas soluciones requiere no sólo la recapacitación del personal involucrado sino también el rediseño de la operatoria completa.

La validación ológrafa automatizada es de gran utilidad no sólo para acotados ámbitos.

A continuación se presentan las principales consideraciones que motivan el presente trabajo.

1.1 ¿ Por qué validar basándose en la firma manuscrita ?

En la actualidad se encuentran diferentes dispositivos biométricos de validación o identificación de personas. Entre ellos se encuentran los de lectura de huella dactilar, reconocimiento facial o escaneo del iris, retina, etc. Sin embargo, la utilización de firma manuscrita propone un mecanismo simple, que no se ve alterado por factores externos, como en el caso de otros métodos como ser la huella dactilar [2]. Por otro lado, no depende ni requiere de dispositivos costosos, lo cual facilita la difusión y aplicación del sistema en ámbitos en los que no se desee realizar una gran inversión.

1.2 Pericias Caligráficas

Ya sea en una firma, como en cualquier otro tipo de escritura, el individuo deja sus propias características de personalidad plasmadas en la muestra. Dichas características o automatismos (gestos inconscientes e involuntarios realizados por cada individuo en forma constante), pueden ser analizadas dividiendo el área de escritura en 4 zonas, las cuales reflejan diferentes aspectos de la personalidad. Ello se grafica en la figura 6.

Fig. 6. División de las zonas de escritura.

Las personas expresan por medio de la escritura. La mayor parte de los escritos provienen de las emociones y estados afectivos. Aún si se intentara falsificar o fingir en el acto de la escritura, los razgos particulares surgirían tarde o temprano.

Existen 3 leyes acerca de la disciplina pericial:

Primera Ley: asegura que es el cerebro quien guía al órgano escritor, y que éste último no produce ningún tipo de modificación en la escritura. Dicha Ley fue comprobada en personas mutiladas que pudieron reproducir el mismo tipo de escritura con otros órganos luego de un período de aprendizaje.

Segunda Ley: expresa que el “Yo” que se encuentra en acción en el momento de la escritua, alterna continuamente la intensidad de atención. El máximo pico de atención del Yo consciente se da en el comienzo y el mínimo al final.

Tercera Ley: dice que no es posible modificar a propósito la propia escritura y que ello pase desapercibido. En el escrito aparecerán huellas que demuestren el esfuerzo realizado para reprimir el propio modo escritural. Algunos ejemplos de las huellas pueden ser presiones, desviaciones, interrupciones, rupturas, trazos indecisos, defectos, temblores o retoques.

El deterioro de las firmas esta relacionado con la edad o la situación de salud de las personas. Se pueden ver signos de cansancio, lentitud, temblores, etc. Incluso puede profundizarse con casos de incapacidad total para expresar ideas por escrito.

1.3 Principios que avalan la Firma

Existen dos principios que debe cumplir una firma para ser válida: *ad solemnitatem* y *ad probationem* [3]. Estos principios que rigen a las firmas, establecen que las mismas deben determinar la existencia o validez de un acto jurídico (*ad solemnitatem*) y la admisibilidad y valoración de pruebas en un juicio (*ad probationem*).
Un sistema de validación de firmas ológrafas debe preservar su sentido legal, facilitando la identificación del firmante.

1.4 Ley de Firma Digital

El 14 de Diciembre de 2001 se publicó en el Boletín Oficial de la Nación Argentina la Ley Nacional 25.506 de Firma Digital [4], cuya aplicación es regulada por el Decreto Nacional Nº 2.628/02 [4]. El Artículo 3 de la nombrada norma establece que cuando la Ley requiera una firma manuscrita, esa exigencia podrá ser satisfecha por la firma digital. Esto se aplica para los casos en que se requiere la presencia de la firma, como para aquellos en los que se establezcan penas por la ausencia de la misma. La Ley también establece que la exigencia legal de conservar documentos queda satisfecha con la conservación de los documentos digitales firmados digitalmente, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente la fecha y hora, así como también el origen y destino de generación, envío o recepción.
El Estado Argentino invita a los gobiernos provinciales a sumarse y legislar a favor de la Firma Digital, a la vez que promete promoverla. Hasta el momento se han adherido los gobiernos de las provincias de Santa Fe [5] [4], que extiende a los gobiernos municipales la invitación; Tierra del Fuego [6] [4]; La Pampa [7] [4]; Chubut [8] [4]; Buenos Aires [9] [4].
A pesar de la iniciativa de uso de la firma digital, hay ciertos casos en los cuales no puede ser aplicada:

a) Disposiciones por causa de muerte;
b) Actos jurídicos del derecho de familia;
c) Actos personalísimos en general;
d) Actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o acuerdo de partes.

1.5 Fraudes

El Estado Argentino ha tenido que pronunciarse reiteradas veces por fraudes cometidos con firmas falsificadas en cheques. Los bancos, que debieran ser responsables y preocuparse por los bienes que les son confiados, no cuentan con todo lo necesario para cumplir con esa responsabilidad y la delegan en un empleado, dejando que sea éste quien con su mejor buena voluntad y su experiencia controle y decida acerca los documentos a pagar.
Algunos claros ejemplos son el Dictamen Nº 184 de la Procuración del Tesoro de la Nación (de fecha 11 de Noviembre de 1999) [4], que desliga de responsabilidad alguna al Banco de la Nación Argentina, por el pago efectuado de cheques extraviados, dado que no se hallaron características de falsificación visiblemente manifiestas entre las firmas de los cheques y las del registro del banco en el informe pericial-caligráfico; y los Dictámenes Nº 192 (de fecha 27 de Diciembre de 1993) [4] y R00022 (de fecha 19 de Noviembre de 1996) [4], donde se hace a lugar a los reclamos planteados por el pago de cheques apócrifos, aduciendo que la confrontación que realiza un empleado bancario no debe realizarse con un criterio técnico-caligráfico pero tampoco debe reducirse a un control superficial, ya que la entidad bancaria es responsable de poner celo y preocupación por los bienes confiados. Se toma en cuenta que al comparar las rúbricas, se detectaron notables diferencias entre las firmas de los habilitados y las de los cheques falsificados, sin necesidad de utilizar elementos específicamente diseñados para la verificación.
Según la Ley Argentina, los bancos responden por las consecuencias de los pagos de los cheques cuando las firmas de éstos difieren visiblemente respecto de las registradas (Ley de Cheques, Ley Nacional Nº 24.452, Anexo I, Artículo 35 [4]). La falsificación se considerará visible cuando se pueda apreciar a simple vista, dentro de la rapidez y prudencia impuestas por el normal movimiento bancario (Ley de Cheques, Ley Nacional Nº 24.452, Anexo I, Artículo 36 [4]).

El resto de este trabajo se organiza de la siguiente forma: sección II presenta el escenario actual de los sistemas de software dedicados a la validación automatizada de firmas ológrafas, la sección III describe el prototipo PI-1 base de la presente propuesta, sección IV consideraciones de seguridad, sección V acerca del tratamiento de imágenes, sección VI identificación de patrones, sección VII conclusiones y trabajo a futuro.

SISTEMAS DE SOFTWARE EXISTENTES

No se cuenta actualmente con gran cantidad de software que permita verificar firmas manuscritas.
Muchas empresas que se dedican a la seguridad, han optado por otro tipo de soluciones biométricas como la validación de la palma de la mano o el escaneo del iris y/o la retina.

IBM de Israel tiene un producto **¡Error! No se encuentra el origen de la referencia.** desarrollado para la validación on-line de las firmas, sin embargo el producto no se encuentra disponible para equipos móviles y no prevé cargas masivas ni off-line.
SoftPro **¡Error! No se encuentra el origen de la referencia.** es una alternativa diseñada pensando en los fraudes con cheques. Los desarrolladores han lanzado al mercado varios productos que abarcan diferentes aspectos y necesidades para con las firmas ológrafas, pero no lo han hecho para equipos móviles. Por otro lado, los requerimientos de dichas soluciones hacen que no sean productos para múltiples plataformas.
Por otro lado, existen productos diseñados para dar mayor seguridad a sistemas o redes que realizan la validación a través de firmas manuscritas entre otros métodos biométricos **¡Error! No se encuentra el origen de la referencia.**. Sin embargo, fueron realizados para un fin completamente diferente y las necesidades también los son.

PROTOTIPO DE LA PROPUESTA

A continuación se detalla el prototipo de la propuesta del presente trabajo.

3.1 Arquitectura general

Como se mencionó al comenzar el escrito, la propuesta contempla el procesamiento de firmas ológrafas utilizando como fuente de información diferentes alternativas. Dependiendo del dispositivo de entrada se obtendrán resultados con mayor o menor índice de coincidencia. Las posibilidades que brindan los dispositivos de lectura on-line son mayores, motivo por el cual se puede ofrecer un mejor resultado mediante este tipo de procesamiento. No obstante, mediante la lectura off-line también se ofrecen resultados con un bajo índice de error.
Como se ve en la figura 1, la solución que se plantea permite que se incorporen firmas tanto para almacenar en la base de datos, como para la validación a partir de diferentes formatos: dispositivo de lectura on-line, archivo de firmas (escaneado o fotocopiado), o webcams. A su vez, esos datos pueden ser utilizados como fuente de datos de los diferentes procesadores (móviles o de escritorio). El desarrollo admite ser invocado a través de Internet como un servicio web.

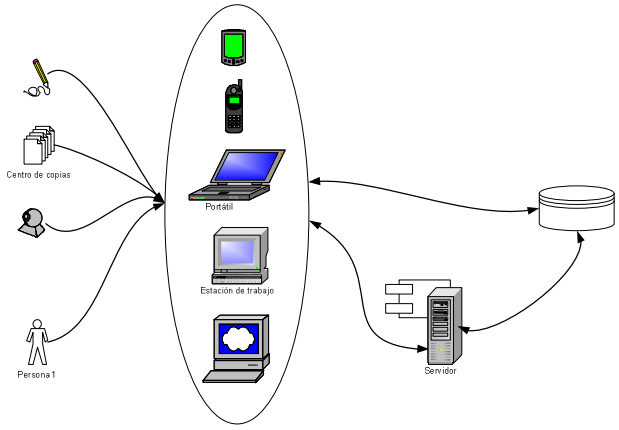

Fig. 1. Arquitectura general del sistema de validación.

El procesador analiza la firma y la registra en la base de datos o bien la valida dependiendo del caso.
Previo a todo proceso de validación es imprescindible que se cargue una serie de muestras de cada individuo contra las cuales validar. Dichos registros deben ser actualizados periódicamente de modo de contemplar los cambios que va sufriendo el ser humano en su manera de escribir y de firmar.
La base de datos se almacena en formato XML (Extensible Markup Language). Esto permite tener un mejor control a nivel seguridad, siendo totalmente portable ya que no requiere motores específicos para el acceso.

3.2 Flujo de datos

A continuación se diagrama la manera en que fluyen los datos a lo largo de los procesos.

La figura 2.1 ilustra desde el momento en que se inicia el proceso de registración por pedido de un actor hasta el momento en que se almacena la información en la base de datos. La captura realizada se produce en un cliente externo[1] , transfiriéndose posteriormente los datos del firmante y las muestras obtenidas de la firma, al servidor para su posterior limpieza, vectorización y almacenamiento. Se puede ver que los datos son procesados en distintos hilos de ejecución, siendo encriptados en diferentes etapas a modo de poder ofrecer un mayor nivel de seguridad junto con un mejor tiempo de respuesta. Luego de finalizar su procesamiento, los hilos generados deberán volver a acoplarse, para almacenar la información obtenida en forma conjunta.

[1] Los clientes externos pueden ser celulares, PDAs (asistentes de datos personales), otro sistema, etc.

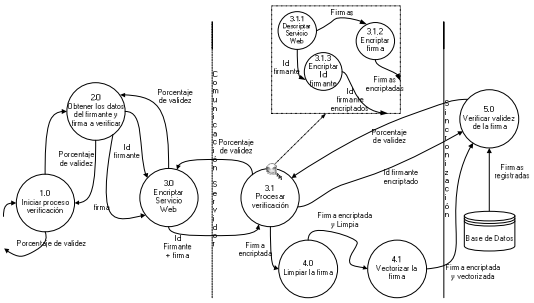

Fig. 2.1. Procedimiento de registración de firmantes.

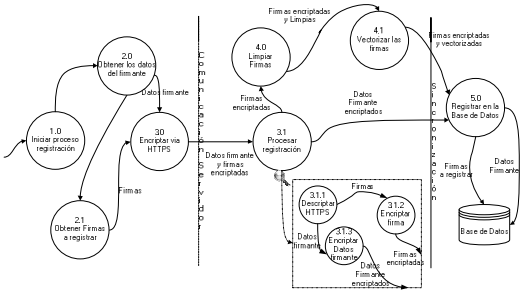

Fig. 2.2. Proceso de verificación de firmas.

El diagrama 2.2, por otra parte, da cuenta del modo en que se procesa un pedido de validación de firma. A este nivel no es importante si la firma proviene de un archivo almacenado (off-line) o de un dispositivo de captura (on-line). En este caso, también se trabaja con distintos hilos que se encargan de diferentes tareas y ayudan a tener una mayor independencia entre los datos de la firma y del firmante a validar.
Esto ayudará a dificultar el robo de información si los datos son interceptados.

3.3 Interfaces

Las interfaces gráficas tienen diseños simples e intuitivos; lo que facilita el uso de la solución.
La figura 3.0 muestra la pantalla de registración de un nuevo firmante a partir de la utilización de un teléfono celular. Se registran los datos y luego se obtienen las muestras de las firmas utilizando la cámara del teléfono. Esta información es transmitida al servidor para su procesamiento, permitiendo la posterior validación.

Fig. 3.0. Formulario para captura de datos del firmante y muestras de firmas desde teléfono celular.

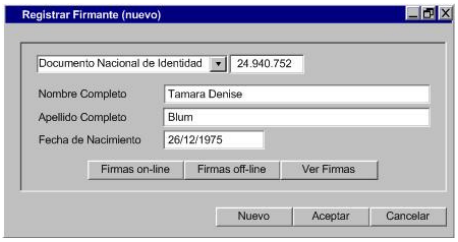

Fig. 3.1. Formulario para registrar un nuevo firmante desde una computadora personal.

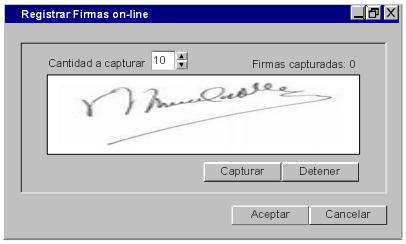

Fig. 3.2. Formulario para registrar firmas utilizando un dispositivo de captura (on-line) desde una computadora personal.

La figura 3.1 es un ejemplo de la forma en que se registran los nuevos datos por medio de una computadora personal. La operatoria es similar. En el caso de la captura de firmas off-.line, se solicita una cantidad de archivos de firmas. En el caso de la captura on-line, se toman las muestras de las firmas de a una (figura 3.2) utilizando un dispositivo de captura on-line. Las firmas serán almacenadas en la base de datos, formando la muestra.
Las figuras 3.3 y 3.4 ilustran la forma en que se validan las firmas de los individuos de los que ya se poseen muestras. Como se puede ver en la figura 3.3, se identifica a la persona a través de su documento de identidad y se visualizan los datos principales. Acto seguido, se solicita la firma a validar y se carga la misma en el visor. Si la firma a validar es capturada on-line, se solicita mediante un formulario como el que se muestra en la figura 3.2. En el caso de que la firma a validar sea off-line, se permitirá elegir el archivo que la contenga utilizando un formulario como el que se puede ver en la figura 3.4.

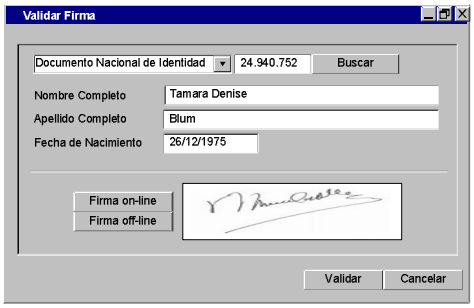

Fig. 3.3. Formulario para verificar el grado de acercamiento entre la firma a validar y la registrada en el sistema (on-line y off-line).

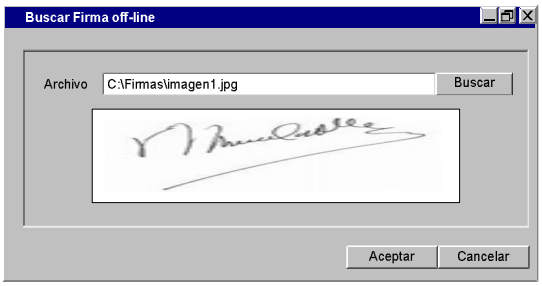

Fig. 3.4. Formulario para seleccionar una firma desde un archivo (off-line).

3.4 Almacenamiento de datos

Ya se ha mencionado anteriormente que dentro de los objetivos de la propuesta se encuentra el obtener un producto capaz de funcionar en diferentes dispositivos y/o plataformas. Por lo tanto, no se puede dejar de tener en cuenta que motores de bases de datos existentes podrían llegar a ser un inconveniente en este aspecto. Se profundiza aún más si requiere de costos adicionales en concepto de licencia. Es por ese motivo que se ha decidido trabajar con una base de datos XML. Otra opción evaluada es el almacenamiento mediante la utilización de archivos planos, sin embargo, este trabajo presupone una carga de datos lo suficientemente importante como para caer en la necesidad de que sean administrados en forma mas eficiente.

Las bases de datos XML son del tipo árbol, donde los nodos son los atributos y cada una de las subdivisiones son las raíces jerárquicas. Existen actualmente diferentes alternativas para acceder a la información desde distintos lenguajes de programación. Y no necesariamente hay una forma que sea la más conveniente. Los requisitos para validar no son los mismos que para la registración. Uno de los métodos de acceso es DOM (Document Object Model), el cual tiene una contra importante dado que carga toda la base de datos en memoria. Ello puede implicar problemas cuando los recursos sean limitados o la base de datos contenga demasiada información por lo que se lo descarta para esta propuesta. Otro de los métodos es SAX. Este método lee el documento XML en forma secuencial, disparándose eventos a medida que se abren y cierran nuevos tags. Este método trae como inconveniente que no es posible volver atrás una vez que se avanza con la lectura del documento o base de datos. Para subsanarlo se puede ir almacenando la información en objetos a medida que se lee. Ambos métodos forman parte del estándar de la W3C (World Wide Web Consortium).

También existen motores de bases de datos. Algunos de ellos son productos gratuitos y otros se comercializan por tipo de licencia. Algunas de las grandes empresas como Oracle también promueven sus propias bases de datos XML. Por otro lado, hay algunas bases de datos que son XML-enabled: admiten el formato, pero no fueron pensadas ni creadas como XML.

Después de evaluar las distintas alternativas, se optó por desarrollar una interfaz de acceso a los datos e implementarla utilizando SAX, dejando la información al resguardo en archivos de texto con formato XML. Esto permite intercambiar la forma de acceder a los datos en un futuro, si se encontrara una mejor alternativa, con sólo implementar en una nueva clave la misma interfaz.

Los datos se guardarán encriptados para dificultar la interpretación de los mismos e impedir el “robo” de información.

CONSIDERACIONES DE SEGURIDAD

Esta sección describe aspectos relativos a la seguridad que deben ser considerados al momento de desarrollar un software de autenticación como el planteado en este trabajo.

Teniendo en cuenta que los ataques pueden ser de distintos tipos de acuerdo no sólo a la arquitectura de la aplicación, sino también a sus componentes externos, y el tipo y ubicación del atacante [16], dentro del presente esquema, se trabaja no sólo a nivel interno como en el caso de la seguridad referida a los threads (hilos), sino también sobre la base de datos que almacena las firmas, la comunicación con dispositivos clientes, tales como teléfonos celulares, páginas web seguras y servicios web utilizados para el proceso de validación.

4.1 Encripción GSM

La tecnología GSM (Global System for Mobile Communications) esta compuesta por servicios anexos, como ser GPRS (General Packet Radio Service), los cuales ofrecen características de valor agregado. Transmisión de datos a altas velocidades, navegación en Internet a color, e-mail, son algunos de estos ejemplos.

Este apartado, se focaliza en los mecanismos de encripción utilizados por esta tecnología, la cual se ha convertido en un estándar masivamente aceptado por el mercado.

Este estándar, se basa en la implementación de tres algoritmos, los cuales comprenden los procesos de autenticación y encripción de datos y voz [14] [15].

El primero de ellos, el A3, se encarga de autenticar la tarjeta SIM (Subscriber Identity Module) del equipo móvil, con la Central de Autenticación. Se logra por medio de la utilización de un esquema de "desafío-respuesta". El segundo algoritmo, genera la clave de cifrado a ser utilizada durante la encripción / desencripción. Esto se logra por medio del algoritmo A8, el cual recibe los mismos parámetros que el punto anterior. Esta clave también es calculada por la Central de Autenticación. El último algoritmo, el A5, se encarga de encriptar / desencriptar la comunicación (datos y voz) utilizando la clave obtenida en el punto anterior.
La encripción GPRS utiliza los mismos algoritmos y clave de identificación, pero con un "desafío" distinto. En ningún momento se transmite la clave de identificación. Para mayor seguridad, los algoritmos expuestos, son procesados dentro de la tarjeta SIM y no en el teléfono.
Si bien este protocolo permite obtener mayor seguridad ante un hacker eventual, el mismo ha sido violado en distintas oportunidades, siendo la propuesta por Elad Barkan, Eli Biham y Nathan Keller en 2003, la de mayor éxito [15]. Su trabajo se basa en el criptoanálisis de los algoritmos A5/1 (fuerte), A5/2 (débil) y A5/3 (similar al algoritmo KASUMI utilizado por UMTS).

4.2 Páginas Web Seguras

Uno de los puntos validados en el desarrollo del prototipo se encuentra relacionado con la comunicación entre los dispositivos móviles basados en J2ME y su servidor web. Para el presente trabajo se han estudiado distintas formas de comunicación, identificando beneficios e inconvenientes en cada una. Este análisis se muestra en la figura 4.0.
En lo referido a la comunicación del registro de firmas, se ha podido verificar que el empleo de servicios web no es apropiado para grandes volúmenes de datos, ya que el tamaño de las firmas supera la cantidad máxima de bytes que pueden ser direccionados por la memoria de los dispositivos móviles (teléfonos, PDAs, etc.) basados en J2ME [28]. Se ha concluido que la forma más natural y práctica para enviar grandes volúmenes de información, es por medio de mensajes del tipo *Post*[2] sobre páginas web.

FIG. 4.0
BENEFICIOS E INCONVENIENTES DE LAS TECNOLOGÍAS DE COMUNICACIÓN ANALIZADAS

Tecnología	Beneficios	Inconvenientes
Web Services	Utilización de interfases simples y estandarizadas	Limitaciones en el tamaño de los mensajes Implementación de seguridad mas compleja
Implementación de Protocolo propietario	No posee limitaciones en el tamaño de los mensajes Adaptable a necesidades actuales y futuras	Interfases no estandarizadas Implementación de seguridad propietaria Mayor complejidad en el desarrollo del cliente y el servidor
Paginas Web Seguras	Implementación simple de No posee limitaciones en el tamaño de los mensajes	Interfases no estandarizadas

Considerando los inconvenientes de seguridad presentes en este tipo de documentos, (envío de información no encriptada, posibilidad de alterar mensajes, suplantación de identidad, etc.) se ha optado por la implementación del estándar HTTPS (Hyper Text Transfer Protocol Secure). Este estándar se encuentra implementado en dispositivos móviles bajo el nombre de kSSL (Kilobyte Secure Sockets Layer) [27] y se encuentra disponible a partir de la versión 1.0.3 de MIDP (Mobile Information Device Profile). El mismo permite autenticar el servidor por medio de un certificado, estableciendo a partir de dicha etapa, una comunicación basada en un canal seguro de 128 bits. Esto permite que tanto las firmas como los datos del firmante, puedan viajar por el mismo medio, sin las falencias que puedan desencadenar en fallas de seguridad, aprovechables por terceros.

4.3 Encripción en Servicios Web

Una parte importante de la seguridad se encuentra relacionada con las interfaces. Aquí se exponen los posibles tipos de vulnerabilidades y se plantea una solución a los mismos, sobre la que se basa el prototipo desarrollado.
Teniendo en cuenta las limitaciones enunciadas en el punto anterior (restricciones en el tamaño de los mensajes, implementación compleja de la seguridad, etc.), se ha restringido la utilización de los servicios web únicamente para la validación de las firmas.
Un servicio web, básicamente, permite exponer una funcionalidad encapsulada, que puede ser consumida por un cliente para resolver un requerimiento específico [27]. La seguridad aplicada a los servicios web, plantea distintos aspectos como ser la autenticación, el acceso en base a roles, mensajería y seguridad de datos.
Los principales tipos de ataques se producen por intentar o concretar un acceso no autorizado; introducir código malicioso; ataques por denegación de servicio; o modificación de mensajes (Man in the Middle) [16].
El estándar denominado WS-Security 1.0 o WSS (Web Service Security) [17] que determina un protocolo de comunicación actúa a nivel mensaje y no sobre los protocolos de transferencias o conexión, lo cual garantiza que

[2] Método utilizado para el envío de información a una página web en forma interna, no exponiendo los parámetros transmitidos en la barra de direcciones.

dicho proceso sea más eficiente [18]. El estándar WSS define aspectos relativos a la integridad, confidencialidad y autenticación aplicada sobre los mensajes SOAP (Simple Object Application Protocol) [18]. WSS implementa tokens (comandos reservados) de seguridad para el proceso de autenticación, los cuales mantienen dicha información por medio del encabezado de seguridad del mensaje SOAP. En cuanto a la integridad de la información transmitida, WSS implementa firmas digitales XML, lo cual provee seguridad para que el mensaje no sea alterado durante la comunicación.Por último, la confidencialidad del mensaje es implementada por medio de la especificación XML Encryption y permite asegurar que el mensaje solo pueda ser leído por el destinatario, evitando de esta forma que un tercero pueda descifrarlo [18].
Dado que el estándar WSS no plantea una plataforma concreta, el mismo puede ser implementado en distintos lenguajes y ambientes. Actualmente existen implementaciones de WSS en .NET, Java y PHP entre otros.

4.4 Seguridad en Threads

Un punto fundamental en el esquema de la propuesta, se focaliza en la seguridad de su arquitectura concurrente. Se pueden establecer dos principios básicos, del desarrollo concurrente: la comunicación y la sincronización [19].

4.4.1 Comunicación entre Procesos:

Uno de los puntos a tener en cuenta es que en una arquitectura multi-threading, es fundamental que exista una comunicación entre los threads para evitar que uno afecte el desarrollo de otro.
Existen varias alternativas para supervisar o coordinar esto:

a) Utilización de semáforos:

Por un lado es posible señalizar determinados comportamientos mediante la utilización de semáforos, los cuales son implementados en áreas de memoria compartidas [20].

b) Envío de Mensajes / Monitoreo / Sincronización

Existen situaciones en las cuales dos o más threads requieren acceder a un mismo recurso en forma exclusiva. En este punto, es fundamental coordinar un acceso ordenado, que asegure que un único thread tiene control del recurso. Esto se logra mediante la sincronización de los threads, con respecto al recurso que se intenta acceder [21]. Java utiliza mecanismos de alto-nivel denominados Monitores [22], los cuales se encargan de bloquear el acceso a una porción determinada de código, la cual puede ser accedida de a un thread por vez.
Una vez que el thread ha finalizado la operación requerida, el Monitor se encarga de liberar el recurso, para que otro thread tome control del mismo.

c) Implementación de Canales

La implementación de canales en Java, permite establecer y controlar conexiones entre distintos procesos, relevando al programador de la complejidad de esta tarea [23]. Los canales, trabajan en un único sentido y poseen características de auto-sincronización basadas en la primitiva de sincronización asimétrica rendezvous [24]. Esta primitiva permite que dos procesos concurrentes, se comuniquen en forma coordinada, a partir de un punto de encuentro. Si un proceso A requiere comunicarse con otro B, se establece un punto de encuentro en donde A queda a la espera de B. Si B llega primero, entonces el proceso se queda a la espera de A.
Dado que la comunicación se realiza mediante un proceso sincrónico, la transferencia de datos entre ambos procesos se produce sin necesidad de utilizar de un buffer intermedio. Si se requiere que la comunicación se realice en ambos sentidos, es necesario implementar dos canales independientes.

4.4.2 Seguridad en Java

Uno de los puntos centrales en cuanto a la seguridad de aplicaciones, tiene que ver con la implementación de políticas de acceso. Esto permite realizar validaciones o controles sobre operaciones críticas que, de otra forma, pueden generar comportamientos no seguros.
Java implementa la seguridad basada en políticas por medio de la clase *java.lang.SecurityManager*, lo que permite que cualquier clase que derive de ella, pueda implementar una política de seguridad personalizada según sus requerimientos. Ante un requerimiento sobre una tarea que puede ser potencialmente peligrosa, el API (Application Programming Interface) de Java, consulta internamente al Security Manager para validar si puede proceder o no con la solicitud, de acuerdo al contexto del solicitante [25].

d) Existen dos tipo de acciones que permiten generar comportamientos “no seguros”, los cuales no se encuentran soportados por el Security Manager y permiten realizar un ataque del tipo “denegación de servicio”. Estos ataques se producen particularmente por reservar memoria hasta agotarla o generar threads hasta que colapse el sistema.

TRATAMIENTO DE IMÁGENES

El análisis de las características y patrones comprendidos en las firmas ológrafas, propone un desafío complejo, dado que el mismo, varía dependiendo de la calidad de la muestra obtenida.
Teniendo en cuenta que los dispositivos utilizados para la captura de firmas, son variados y con características diferentes (celulares, PDAs, archivos, etc.), es necesario realizar un proceso que permita normalizar y eliminar aspectos que dificulten el procesamiento de las imágenes en la red neuronal.

Se han analizado distintas alternativas que tienden a mejorar la calidad de los registros de firmas obtenidos, enfocándose principalmente en los siguientes aspectos:
a) Ruido: comprende cualquier alteración producida antes o durante la captura, que incorpore trazos, marcas, manchas o sombras, externas a la firma. Puede generar problemas en la identificación de las características.
b) Centrado: teniendo en cuenta que el método para captura de las firmas no se encuentra estandarizado, es altamente probable que las imágenes obtenidas no se encuentren centradas. Esto distorsiona el reconocimiento de los patrones, entre firmas de una misma persona.
c) Tamaño: las muestras obtenidas, al no ser uniformes, pueden responder a distintas escalas. Esto dificulta no solo la comprensión de los patrones de la firma, sino también ocasiona un mayor tiempo de procesamiento por parte de la red neuronal, ya que las imágenes contienen mayor información. Para ello, es fundamental reducir el tamaño de la muestra, generando condiciones similares para el procesamiento de todas las firmas.
d) Color: se ha considerado para el presente trabajo, la estandarización de los colores correspondientes a la firma, con el fin de normalizarla y reducir su volumen. Por ello, se determino utilizar imágenes en blanco y negro, lo que permite simplificar la obtención del vector de características y agilizar el procesamiento.

IDENTIFICACIÓN DE PATRONES

El punto mas critico de la investigación, se ha focalizado en la identificación de los patrones característicos de una firma ológrafa. Estos patrones son los que identifican aquellas particularidades que vuelven única a la firma.
Se han estudiado distintas aproximaciones utilizadas en campos similares, como ser:
a) Reconocimiento de rostros: en este punto se ha analizado la propuesta introducida por Sirovich y M. Kirby, conocida como Eigenfaces [29]. A diferencia de un rostro, la identificación de firmas, es una tarea que requiere mayor exactitud, ya que al validar una firma se debe desestimar aquellas que correspondan a falsificaciones. En el caso de los rostros, si dos personas poseen facciones muy similares, es probable se deseen obtener ambos resultados como validos.
b) Redes neuronales de Clasificación: estas redes responden a patrones mas específicos, pudiendo clasificar una determinada entrada, en un conjunto de salidas ya conocidas. El resultado es una clase especifica, previamente establecida durante el entrenamiento de la red. La complejidad presentada por las firmas, hace que la identificación concreta de una salida, puede desembocar en falso positivo, al catalogar como valida una falsificación, por poseer mayor afinidad con la firma real que con el resto del universo de firmas.
c) Redes neuronales de Retropropagación: hemos considerado este tipo de redes, como la aproximacion mas concreta sobre la problemática planteada, dado que es capaz de ajustar sus pesos en forma automatica a partir de los valores obtenidos. Esto contribuye a mejorar la comprensión de los razgos que componen la firma, obtenidose como resultado un vector que representa los patrones significativos de la firma procesada.

CONCLUSIONES Y TRABAJO A FUTURO

Entidades bancarias, mercado inmobiliario, autorizaciones o poderes, juzgados, compras con tarjetas de crédito y registros de conducta del ciudadano son algunos de los ámbitos mas importantes en los que se delega la validación del individuo en personas con mayor o menor especialización en este tipo de tareas (y en algunos casos ninguna), o sistemas biométricos con un alto margen de error.
La solución que se propone, se intenta ajustar a las necesidades de diferentes tipos de usuarios: personas físicas o jurídicas. También a diferentes plataformas e incluso servicios. Es por esto que se determinó almacenar la información en archivos con formato XML.
Se establece un esquema de seguridad en el cual la información viaja encriptada y a través de distintos hilos de ejecución a fin de mantener por separado a los datos que en su conjunto podrían permitir el acceso no deseado, en caso de ser “robados” por terceros.
El trabajo a futuro constará de poner en práctica las cuestiones analizadas y establecer, a medida que se desarrolle la solución, si cada uno de los puntos definidos continúa siendo la mejor alternativa dentro de las existentes. Una vez revalidado cada uno de ellos, se podrá obtener el sistema en su conjunto.
Asimismo, una vez concluida la implementación completa, podría complementarse el sistema con el análisis on-line (dinámico) de firmas manuscritas.
Respecto al diseño de la base de datos, queda pendiente terminar de definir si la mejor alternativa es que los datos se guarden en su conjunto dentro del mismo archivo o guardarlos estilo “cabecera-detalle”.
Las ventajas de guardar el conjunto de datos en diferentes archivos es que ante el hecho de corromperse alguno de ellos, se puede rearmar la base de datos con sólo tomar nuevamente las muestras que corresponden al firmante que tiene sus firmas corruptas. Sin embargo, el resguardo de la información puede verse afectado si el archivo que se corrompe es el que actúa de “cabecera”. El mismo grado de dificultad existe ante la corrupción del archivo que contendría a la base de datos completa,
Aunque el almacenamiento de la información utilizando varios archivos es ventajoso por su disposición, este sistema podría traer como consecuencia alguna desventaja en la seguridad, ya que permitiría un rastreo más simple del contenido y las muestras de las firmas por parte de usuarios locales del sistema.

Referencias

[1] Trevathan, J. and McCabe, A. *Remote Handwritten Signature Authentication.* In Proceedings of the 2nd International Conference on EBusiness and Telecommunication Networks (ICETE '05), pp 335--339, 2005. http://citeseer.ist.psu.edu/trevathan05remote.html.

[2] Gupta, J and McCabe, A. *A Review of Dynamic Handwritten Signature Verification*. James Cook University, Australia (1997). http://citeseer.ist.psu.edu/gupta97review.html.

[3] G. Rodríguez, "*De la firma autógrafa a la firma digital*", Facultad de ciencias jurídicas y políticas, Universidad de Zulia [Disertación sobre firma ológrafa y digital; y la implementación de ésta última como medio de autenticación y confirmación para documentos electrónicos].

[4] Información consultada en http://www.saij.jus.gov.ar, Sistema Argentino de Informática Jurídica - Ministerio de Justicia, Seguridad y Derechos Humanos

[5] La Ley Provincial Nº 12.491, del 24 de Noviembre de 2005 dispone de un plazo de hasta 5 (cinco) años para la implementación de la tecnología necesaria para la Firma Digital en el ámbito normativo.

[6] Ley Provincial Nº 633, del 6 de Julio de 2004.

[7] Ley Provincial Nº 2.073, del 9 de Octubre de 2003.

[8] Ley Provincial Nº 5.366, del 5 de Julio de 2005. Autoriza el empleo de la Firma Digital en todas las dependencias de los tres poderes del Gobierno Provincial y se compromete a promover el uso de la Firma Digital en expedientes y búsquedas, control y seguimiento de información.

[9] Ley Provincial Nº 13.666, del 12 de Abril de 2007.

[10] http://www.haifa.il.ibm.com/projects/image/sv/index.html.

[11] http://www.signplus.com/en/products/signplus/.

[12] http://www.iwsinc.com/Biometrics/IWSDesktopSecurity.cfm.

[13] Información consultada en http://www.gsmworld.com, GSM Facts and Figures - GSM Association.

[14] U. Meyer y S. Wetzel, "*On the impact of GSM Encryption and Man-In-The-Middle attacks on the Security of Interoperating GSM / UMTS Networks*", Dept. of Comput. Sci., Darmstadt Univ. of Technol., Germany. Septiembre 2004.

[15] E. Barkan, E. Biham y Nathan Keller, "*Instant Ciphertext Only Cryptanalysis of GSM Encrypted Communication*", Computer Science Department Technion Israel Institute of Technology. Mayo 2003.

[16] Shivaram Mysore, "*Securing Web Services - Concepts, Standards and Requirements*", Sun Microsystems. Octubre 2003.

[17] OASIS, "*Web Services Security: SOAP Message Security 1.1 (WS-Security 2004), OASIS Standard Specification*". Febrero 2006.

[18] Microsoft, "*¿Por qué WSE?*". Información consultada en http://www.microsoft.com/spanish/msdn/articulos/archivo/030505/voices/whywse.mspx. Julio de 2005.

[19] Alberto Pacheco, "*Programa Concurrente*", División de Estudios de Posgrado e Investigación - Instituto Tecnológico de Chihuahua.

[20] Edsger Dijkstra, "*The Structure of the "The" Multiprogramming System*". 1968

[21] Brinch Hansen, "*Structured Multiprogramming*". California Institute of Technology. Julio 1972.

[22] Sun Microsystems, "*Java Language Specification - Second Edition*". 2000.

[23] Gerald Hilderink, Jan Broenink, Wiek Vervoort y Andre Bakkers, "*Communicating Java Threads*". University of Twente, dept. EE, Control Laboratory. 1997.

[24] E.J. Anderson y R.R. Weber, "*The rendezvous problem on discrete locations*". University of Cambridge. 1990

[25] Bill Venners, "*Java security: How to install the security manager and customize your security policy*". JavaWorld.com. Enero de 1997.

[26] Carla King, "*Securing the Wireless Internet Using "Kilobyte" SSL*". Sun Microsystems. Julio 2001. Información consultada en http://www.sun.com/bigadmin/content/developer/howtos/kssl.html.

[27] "*Guía Breve de Servicios Web*". World Wide Web Consortium. Enero 2008. Información consultada en

http://www.w3c.es/Divulgacion/GuiasBreves/ServiciosWeb

[28] Eric Giguere , "*Java 2 Micro Edition - Programming Strategies for Small Devices*". Publicado por John Wiley & Sons. Febrero 2001.

[29] L. Sirovich and M. Kirby, "*Low-dimensional procedure for the characterization of human faces*", Journal of Optical Society of America. 1987.