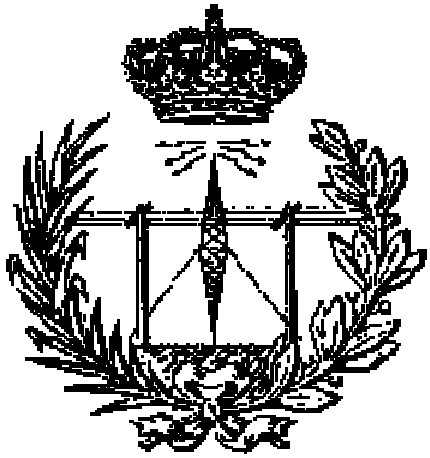
UNIVERSIDAD DE LAS PALMAS DE GRAN CANARIA

ESCUELA TÉCNICA SUPERIOR DE
INGENIEROS DE TELECOMUNICACIÓN



RESUMEN

MODELADO DE UN VERIFICADOR DE FIRMAS MANUSCRITAS PARA TARJETAS INTELIGENTES

Autor: David Hernández Casañas
Tutor: Dr. Miguel Ángel Ferrer Ballester
Fecha: Febrero 2004

INTRODUCCIÓN

El propósito de este proyecto es el modelado, diseño y evaluación de una aplicación para Tarjetas de Crédito Inteligentes, capaz de verificar por si misma la firma manuscrita que realiza el usuario en el resguardo.

(a) (b)

Figura 1 (a) Tarjeta de Crédito Inteligente y (b) firma de usuario en resguardo.

La necesidad de este proyecto nace de la gran importancia que tiene, en la economía moderna, la certera identificación personal, que posibilite el uso eficiente de los medios de pago a través de tarjetas de crédito. Dado que el fraude realizado en la Unión Europea con tarjetas de crédito durante el año 2001 ascendía a 600 millones de euros, con un incremento del 50% respecto al año anterior [1], la *Comisión Europea* recomendó la completa sustitución de las tarjetas de crédito de banda magnética por Tarjetas Inteligentes para el año 2005 [1], recomendación que ya ha sido asumida por Visa y Europay/Mastercard.

Figura 2 Visa y MasterCard.

Los métodos de verificación automática de firmas manuscritas, como área relevante de las técnicas de identificación biométricas, combinados con la seguridad de las Tarjetas Inteligentes [2, 3, 4], pueden proporcionar unos medios de pago eficientes, y al mismo tiempo, ampliamente aceptados, fiables, seguros y disponibles a un bajo coste relativo.

La firma manuscrita, frente a otras técnicas de identificación biométrica, aporta el hecho de que por si es aceptada por leyes y transacciones comerciales como un

método de autenticación personal, es un método no invasivo, no provoca recelo pues la gente está acostumbrada a firmar, es rápido y efectivo, siempre se lleva consigo, no puede perderse y no hay necesidad de esconderla ni de memorizarla, al contrario de lo que ocurre con el PIN.

Sin embargo el uso de las firmas como sistema de verificación presenta dos desventajas. En primer lugar, las falsificaciones, que pueden, no obstante, ser detectadas en la mayor parte de los casos con las precauciones adecuadas. En segundo lugar, la alta variabilidad de las firmas constituye un importante obstáculo para su empleo en un sistema automático de verificación.

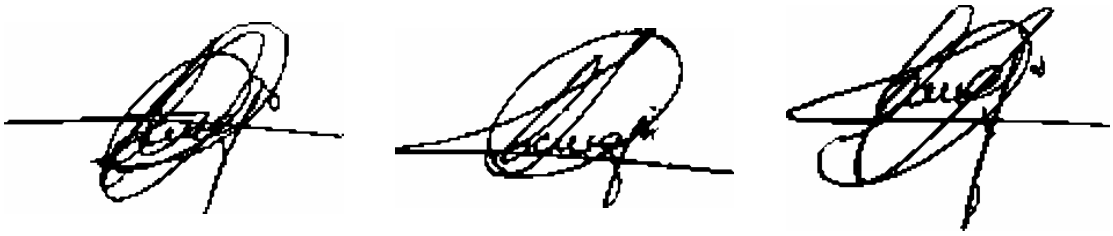


Figura 3 Ejemplo de variabilidad de las firmas de un mismo firmante.

OBJETIVOS

Nuestro proyecto pretende ir un paso más allá en la línea de investigación emprendida por el Grupo de Procesado Digital (GPDS en adelante) de esta universidad sobre la verificación estática de firmas manuscritas, basada en la caracterización de sus estructuras geométricas y desarrollada hasta entonces mediante Redes Neuronales y Cadenas Ocultas de Markov (HMM) [5, 6, 7, 8]. Con dicho fin, se plantearon los siguientes objetivos:

- Rediseñar y optimizar los parámetros de anteriores investigaciones para adaptarlos a los requisitos de las Tarjetas Inteligentes [9, 10, 11, 12, 13].

- Diseñar nuevos y eficientes algoritmos de verificación y mínimo coste computacional que puedan ser implementados en Tarjetas Inteligentes.

- Definir los requisitos mínimos de la Tarjeta Inteligente, siempre buscando el mínimo coste económico que permita su uso masivo como tarjeta de crédito.

VISIÓN GENERAL DEL SISTEMA

El sistema consistirá, por consiguiente, en diseñar una aplicación de valor añadido para las Tarjetas Inteligentes usadas como tarjetas de crédito, que posibilite la verificación de la firma realizada por el comprador en el resguardo. Debido a que el sistema caracterizará la firma estáticamente, requerirá que un operador, en este caso el comerciante, compruebe que la persona que realiza la compra con la tarjeta estampe su firma en el resguardo, para capturar posteriormente su imagen.

El sistema se encargará entonces de preprocesar la imagen capturada y de extraer de ella los parámetros de la firma. Una vez transmitidos los parámetros cifrados a la Tarjeta Inteligente inserta en el lector, ésta comparará dichos parámetros con los que tiene almacenado como prototipos característicos del firmante. Si la firma testada cae dentro del margen de variabilidad tolerado, definido por un umbral almacenado también en ella, se validará la firma como auténtica (ver figura 4).

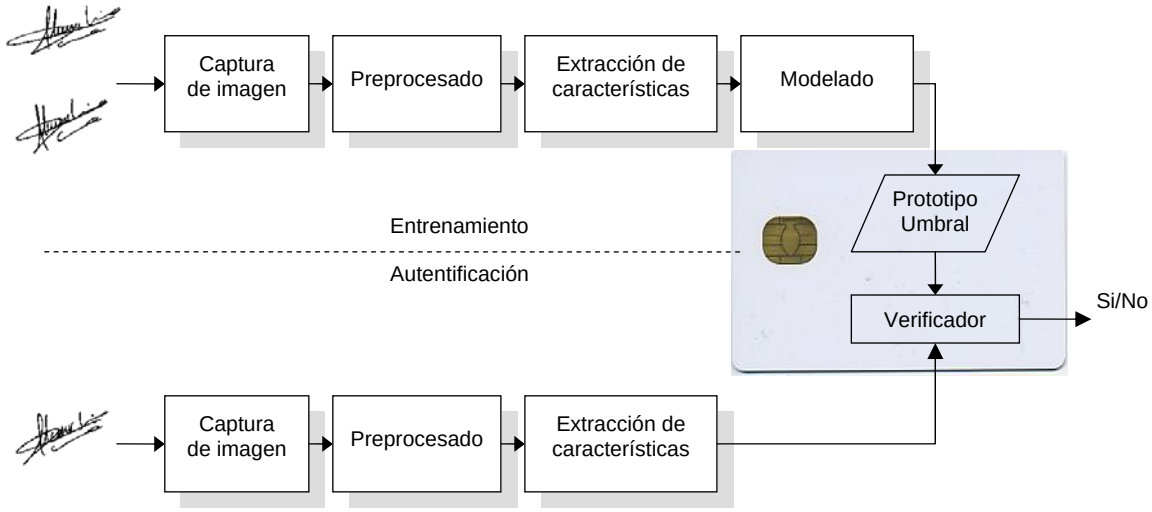


Figura 4 Componentes del sistema de verificación de firmas.

Antes de que el comprador pueda hacer uso de la tarjeta, deberá darse de alta (entrenarse) en el sistema, facilitando al banco un conjunto de firmas de las cuales poder extraer unos parámetros prototipo de sus firmas y de los umbrales representativos de la variabilidad tolerada, personalizándose así la tarjeta del usuario al grabar dichos datos en ella.

Debido al empleo de las firmas como medida de mejora de la seguridad, será necesario manejar dichos datos también de forma segura. Dicha necesidad se ve intensificada por el hecho de que los usuarios están acostumbrados a firmar de una determinada manera y les sería difícil tener que cambiar de firma si ésta se viera comprometida. No obstante, las Tarjetas Inteligentes ofrecen la plataforma ideal para almacenar y procesar estos tipos de datos de forma segura. Por ello, el proceso de verificación se realizará dentro de la tarjeta; con esta verificación interior, los prototipos de los usuarios nunca abandonarán el ambiente seguro de la tarjeta.

Para manejar eficientemente las demandas de verificación con los recursos limitados de las Tarjetas Inteligentes, la implementación será austera en consumo de memoria y deberá usar de forma eficiente la capacidad del procesador. De los distintos tipos de verificadores existentes (Redes Neuronales [14], Modelos Ocultos de Markov [15],…), los basados en métricas de similitud son los que mejor se adaptan a dicha austeridad y bajo coste computacional.

DESARROLLO DEL PROYECTO

En primer lugar se analizaron las técnicas de caracterización estática de firmas manuscritas desarrolladas por el GPDS, optimizando el coste computacional de su obtención, haciéndolas invariante a la traslación y al escalado de la firma, adaptándolas a las limitaciones computacionales de los verificadores implementables en Tarjetas Inteligentes y mejorando el rendimiento obtenido por los parámetros anteriores.

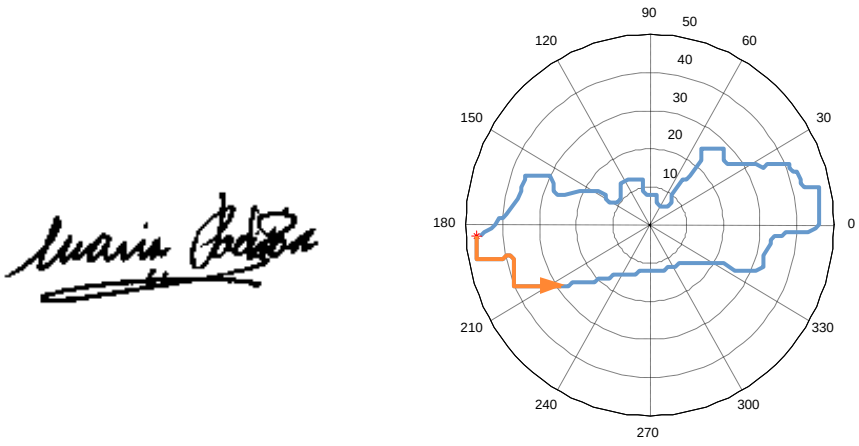


Figura 5 Firma original y envolvente morfológica en ejes polares.

En el desarrollo de dichas técnicas se confirmó, como ya se había adelantado en otras investigaciones del GPDS, que la envolvente de la firma es un buen descriptor de la misma, permitiendo caracterizarla con un bajo coste computacional al combinarla con otras características.

En segundo lugar, se diseñaron diversos verificadores implementables en una Tarjeta Inteligente, empleándose varias técnicas y combinación de técnicas de parametrización, adaptando distintas métricas de similitud entre parámetros a las limitaciones computacionales de las tarjetas [16, 17], planteando unos cuantos métodos de prototipado de los firmantes mediante aprendizajes competitivos y no competitivos [18], e introduciendo varios procedimientos de determinación de la variabilidad del firmante que nos permitiera optimizar su determinación para la etapa de verificación.

Con dichos diseños se realizaron diversos experimentos sobre una base de datos de 3840 firmas genuinas y 4800 firmas falsificadas pertenecientes a 160 usuarios, obteniéndose una tasa de verificación del 95.03% para impostores y del 83.43% para falsificadores con el verificador que mejor relación entre tasa de verificación y coste computacional presentó, siendo éste el que parametrizaba la firma por Medición de su Envolvente, la modelaba mediante Prototipos Promedios y la verificaba mediante Distancia Euclídea Ponderada y umbrales de variabilidad definidos por Desviaciones Típicas.

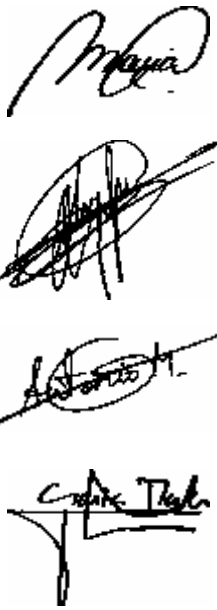
Genuinas	Falsificadas
	

Tabla 1 Muestra de la Base de Datos de firmas genuinas y falsificadas.

Como nuestro proyecto hacía uso de la misma Base de Datos que las investigaciones anteriores del GPDS, pudimos comparar los resultados obtenidos por ambas en las mismas condiciones.

	Nº usuarios	***Tasa de Verificación***	
		Impostores	*Falsificadores*
Anteriores investigaciones	160	94.48%	78.17%
Este proyecto	160	95.03%	83.43%

Como se observa, no sólo se mejoró la tasa de verificación de falsificadores en más de un 5%, sino que se realizó mediante un algoritmo más rápido y sencillo que los Modelos Ocultos de Harkov usados por las investigaciones anteriores, con un coste computacional mucho más reducido, posibilitando la implementación del verificador dentro de una Tarjeta Inteligente.

No obstante, y aunque los resultados en la verificación de impostores son bastantes elevados, la verificación de falsificadores demanda un refinamiento posterior en venideras investigaciones, siendo los resultados iniciales muy prometedores. Sin embargo, hay que hacer notar que el rendimiento de cualquier sistema de verificación de firmas se verá obviamente limitado por el cuidado que ponga el usuario en la realización de la misma.

Así mismo, una inspección visual de las firmas de la base de datos indicó que aquellas para las cuales el sistema presentaba un pobre rendimiento de verificación, no eran discriminables fácilmente por el ojo humano. Además, es conocido que la efectividad de verificación del ojo se ve afectada por el cansancio físico que repercute en el resultado de su decisión, mientras que un sistema automático mantiene un nivel constante en sus decisiones.

En tercer lugar, para una mejor determinación de los requisitos mínimos de la Tarjeta Inteligente, se diseñó una aplicación applet de JavaCard capaz de procesar los comandos de personalización de la tarjeta y verificación de la firma.

Los requisitos mínimos exigidos por el verificador diseñado permitirán emplear la gama más baja de las Tarjetas Inteligentes multi-aplicación JavaCard, con precios unitarios entre 3 y 4 dólares.

CONCLUSIONES

En este proyecto se ha optimizado las técnicas de caracterización de las firmas manuscritas mediante sus estructuras geométricas, se ha diseñado y evaluado diversos algoritmos de verificación y se ha desarrollado una aplicación para Tarjetas Inteligentes que ha mejorado notablemente los resultados obtenidos por investigaciones anteriores, consiguiéndose unas tasas de verificación del 95.03% para impostores y del 83.43% para falsificadores, resultados obtenidos al evaluar el sistema con 3840 firmas genuinas y 4800 firmas falsificadas.

Dicha aplicación se ha desarrollado como applet de JavaCard para su integración dentro de una Tarjeta Inteligente multi-aplicación. Además del gran valor añadido de esta aplicación, la misma se ha diseñado con unos requisitos mínimos, posibilitándose su integración en Tarjetas Inteligentes multi-aplicación de la gama más baja y menor coste económico [9, 10, 11, 12], cumpliendo así el objetivo de poder ser usada masivamente como tarjeta de crédito.

Figura 6 Tarjeta Inteligente JavaCard.

Prueba del manejó eficientemente de las demandas de verificación con los recursos limitados de las Tarjetas Inteligentes es que el tiempo de ejecución de la aplicación dentro de la tarjeta no sobrepasó los 15 ms, para un total estimado de medio segundo en el proceso de verificación de la firma.

REFERENCIAS

[1] Comisión Europea (2001, Feb.) Prevención del fraude y la falsificación de los medios de pago distintos del efectivo. Bruselas, Bélgica. [Online]. Available: http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/com11es.pdf

[2] International Organization for Standardization, "Integrated circuit(s) cards with contacts," ISO 7816, 1996-2002. [Online]. Available: http://www.iso.org

[3] EMVCo, LLC, "Integrated Circuit Card Specification for Payment Systems," EMV2000, Dec. 2000. [Online]. Available: http://www.emvco.com

[4] Sun Microsystems, Inc. (2003, May.) Java Card Technology. [Online]. Available: http://java.sun.com/products/javacard

[5] J. L. Camino, C. M. Travieso, C. R. Morales and M. A. Ferrer, "Signature Classification by Hidden Markov Models", *in 33rd Annual 1999 International Conference on Security Technology*, Madrid, pp. 481-484, Oct. 1999.

[6] J. A. Sánchez, C. M. Travieso, I. G. Alonso and M. A. Ferrer, "Handwritten signature recognizer by its envelope and strokes layout using HMM" *IEEE International Carnahan Conference on security Technology*, London, pp. 267-271, Oct. 2001.

[7] J. L. Camino, C. M. Travieso, C. R. Morales and M. A. Ferrer. (2002, Jun.) Multilabeled discrete hidden Markov model for handwritten signatures recognition. Grupo de Investigación de Procesado de Señales Biológicas, Universidad de Las Palmas de Gran Canaria. [Online]. Available e-mail: mferrer@dsc.ulpgc.es

[8] C. M. Travieso, J. C. Briceño y M. A. Ferrer. (Jul. 2002) Verificación Automática de Firmas Manuscritas mediante Modelos Ocultos de Markov. Grupo de Investigación de Procesado de Señales Biológicas, Universidad de Las Palmas de Gran Canaria. [Online]. Available e-mail: mferrer@dsc.ulpgc.es

[9] Aspects Software Ltd. (2003, May.) Operating System Aspects OS755. [Online]. Available: http://www.aspectssoftware.com/os/

[10] IBM Corporation. (2003, May.) IBM's Java Card Open Platform (JCOP). [Online]. Available: http://www.zurich.ibm.com/jcop/products/cards.html

[11] Atmel Corporation. (2003, May.) AVR-based Secure Microcontrollers. [Online]. Available: http://www.atmel.com/products/SecureAVR

[12] Philips Electronics. (2003, May.) Philips Semiconductors – Identification. [Online]. Available: http://www.semiconductors.philips.com/markets/identification/datasheets

[13] ST Microelectronics Ltd. (2003, May.). ST - Smartcards. [Online]. Available: http://www.st.com/smartcard

[14] C. M. Bishop, *Neuronal Networks for Pattern Recognition.* New York: Oxford University Press, 1995, pp. 1-112.

[15] L. Rabiner, "A tutorial on Hidden Markov models and Selected Applications in Speech Recognition", *in Proceedings of the IEEE*, vol. 77, n.2, pp. 257-286, 1989.

[16] J. C. Machado, M. R. A. Almeida, G. G. S. Tannus and R. Q. Feitosa, "Off-Line Signature Verification Using Hausdorff Distance", *Proceedings of the SCI 2001/ISAS 2001 World Multiconference on Systemics, Cybernetics and Informatics,* 2001, vol. 6.

[17] S. N. Wrigley. (1998, Apr.). Speech Recognition By Dynamic Time Warping. Department of Computer Ciencie, University of Sheffield. [Online]. Available: http://www.dcs.shef.ac.uk/~stu/com326

[18] F. J. Cortijo Bon. (2001, Oct.). Reconocimiento de formas. Departamento de Ciencias de la Computación e Inteligencia Artificial, Universidad de Granada. [Online]. Available: http://www-etsi2.ugr.es/depar/ccia/rf/material.html