Signature Dynamics on a Mobile Electronic Signature Platform

Miroslav Skrbek

Institut Sichere Telekooperation
Fraunhofer Gesellschaft
Rheinstraße 75
64295 Darmstadt
skrbek@sit.fraunhofer.de
skrbek@fel.cvut.cz

Abstract: This article is focused on signature dynamics that is used for protection of qualified electronic signature functions and personal data on mobile platforms. The article presents a concept of the Trusted Pocket Signer (trustworthy PDA with integrated SmartCard used as Secure Signature Creation Device (SSCD)), role of biometrics within this concept, and major handwritten signature algorithm strategies. The handwritten signature algorithm was tested on a large signature database that has been created. The structure of the database reflects various forging techniques and different quality of forgeries. This article also includes technical issues considering integration of biometric functions into the embedded Trusted Pocket Signer software.

1 Introduction

Importance of trustworthy signature platforms grows since the electronic signature has the same legal status as a handwritten signature on a paper document. Present operating systems running on PCs connected to the Internet are too open, with limited security options, and their security settings are mostly under control of users with insufficient knowledge, so that threat of virus attacks persists and manipulations influencing the electronic signature process cannot be completely excluded. A solution of this problem is an embedded, sufficiently closed, secure platform combining trusted viewer functionality (What you see is what you sign - WYSIWYS) with the electronic signature creation on basis of an evaluated SmartCard. A mobile version of a trustworthy signature platform has been developed within the TruPoSign project and it is called Trusted Pocked Signer (TPS) [TPS03].

The Trusted Pocket Signer has a wide range of application areas, typically e-business and e-government, but also in professional areas like health care (prescriptions, medical documents). The health care applications are in focus of the TruPoSign project for their specific usage requirements. Applications in professional areas require very simple usage and short responses of embedded functions because a lot of documents are signed per day. Usage of biometrics (instead of a PIN) is faster and more comfortable solution for these applications.

2 TPS: an Overview

The TPS is a PDA sized handheld computer with colored LCD display, touch screen, and Linux operating system (see Figure 13). Java and C, C++ based software embedded in the TPS creates a trustworthy environment able to receive a document over the wireless (IrDA or Bluetooth) interface and present it to the user in a trusted viewer. A SmartCard inserted in the TPS provides electronic signature creation functions. When an electronic document (electronic order, prescription. etc.) is ready on the PC side, it is sent to the TPS (steps 1,2 in Figure 13) and shown in a viewer (step 3). As soon as the user comes to a resolution to sign the received document, he may invoke the electronic signature creation process. After the document is electronically signed, the signature is sent back over the wireless interface and processed by a PC application.

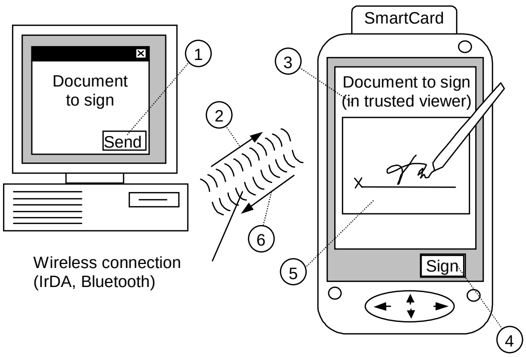


Figure 13: Trusted Pocket Signer Concept

As shown in Figure 13, the signature dynamics replaces the PIN input in step 5. A drawing area is shown instead of a numerical keyboard and the user is asked for a handwritten signature. If the signature is accepted (i.e. recognized as a genuine signature), an electronic signature creation process is started. If it is recognized as a forgery, the electronic signature creation process is canceled. The biometrics is not an alternative of the PIN for enabling the signature creation in the SmartCard. Only if the SmartCard requires one PIN authentication before producing any number of signatures, the signature creation is protected by biometrics ("willful act").

6 Handwritten Signature Verification Algorithm

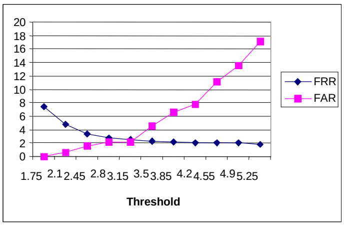
The handwritten signature verification algorithm, which has been developed within the TruPoSign project, is based on a physiologically motivated model of handwriting. The signature is considered as a sequence of aimed movements (horizontal or vertical lines are examples of simple aimed movements). Each movement is described by a set of static and dynamic features. A sequence of movement features composes a spatiotemporal signature representation.

The handwritten signature verification algorithm consists of the preprocessing, feature extraction, matching, and decision stages. The most critical stage is preprocessing because the touch screen data contains a lot of noise that must be filtered out prior the feature extraction phase. The B-spline smoothing filter [BI93] was used because it combines high filtration ability with low corruption of the original signal. The B-spline smoothing filters are simple enough to fit the limited computational resources of mobile devices.

The matching stage based on the dynamic warping method [TW95] compares segment sequences of the signature sample and signature template and establishes correspondences between segments. Features of corresponding segments are compared; excluding segments from comparison is strongly penalized. The segment comparison provides the distance consisting of the feature differences and penalties. The segment distances are summed to a single stroke distance. The total (signature related) distance is calculated as a sum of stroke distances and inter-stroke space distances. The total distance is compared to the threshold value which is derived from the six enrolled signatures.

7 Testing of the Algorithm

For testing of the verification algorithm, we have created a large database of handwritten signatures containing about 55000 signatures collected from 36 test persons. The database is structured into genuine signatures and four kinds of forgeries. The genuine signatures were collected for sitting, standing, and walking positions and also for different collection time. Forgeries in the database reflect typical forging techniques and also the quality of a forgery. For example: tracing of a signature, making forgery with and without a visual contact with the genuine signature.



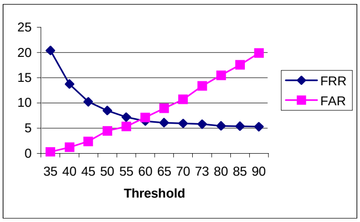


Figure 14: False Acceptance Rate and False Rejection Rate [%]
(short signatures – left, long signatures – right)

Figure 14 shows the false acceptance and false rejection rates of the algorithm for short signatures (2-3 letters) and long signature (complete word). The curves are printed as a function of the threshold. The figures show that the equal error rate less than 5% can be reached for short signatures and less than 10% for longer signatures.

8 Integration of Biometric Functions to the TPS Software

The TPS applications are written in Java and low-level services and computationally extensive modules are written in C, and C++. The biometric algorithm, which is written in C++, is encapsulated into a BioAPI specification compliant biometric service provider (BSP). The BSP is attached to BioAPI Framework implementing the BioAPI interface for native modules. Since the BioAPI specification is available for the C programming language only, we have developed a Java counterpart of the BioAPI interface and a JNI wrapper translating Java BioAPI calls to native BioAPI calls. This approach allows to integrate and to combine signature dynamics with other biometric methods (fingerprint for example) because new biometric methods are installed as new BSPs.

9 Acknowledgement

The TruPoSign project is a project funded within the Federal Ministry of Economics and Labour of Germany (BMWA) program "VERNET – Secure & Reliable Transactions in Open Communication Network" under leadership of the Fraunhofer-Insitute SIT.

This research has been supported by ERCIM (ERCIM Fellowship Program).

Literature

[API01] BioAPI Specification 1.1. BioAPI Consortium. March 2001. http://www.bioapi.org

[BI93] Unser, M., Aldroubi, A., Eden, M: B-Spline Signal Processing: Part I – Theory. IEEE Transactions on Signal Processing, Vol. 41, No. 2, February 1993.

[PLA93] Plamondon, R: The design of an on-line signature verification system: from theory to practice. International Journal of Pattern Recognition and Artificial Inteligence. 1994, Vol. 8, No. 3, 795-811.

[SDC96] Kashi, R.S., Turin, W., Nelson, L. W.: On-line handwritten signature verification using stroke direction coding. Optical Engineering, Vol. 35 No. 9, pp. 2526-2533, September 1996.

[TW95] Wirtz, B.: Stroke-based time warping for signature verification. IEEE Computer Society Press, 1995. ISBN 0-8186-7128-9.

[TPS03] Trusted Pocket Signer. Project WWW pages. http://www.sit.fraunhofer.de/english/SICA/sica_projects/TruPoSign/english.html