# Chapter 14
# Automatic Signature Verification on Handheld Devices

**Marcos Martinez-Diaz**
*Universidad Autonoma de Madrid, Spain*

**Julian Fierrez**
*Universidad Autonoma de Madrid, Spain*

**Javier Ortega-Garcia**
*Universidad Autonoma de Madrid, Spain*

## ABSTRACT

*Automatic signature verification on handheld devices can be seen as a means to improve usability in consumer applications and a way to reduce costs in corporate environments. It can be easily integrated in touchscreen devices, for example, as a part of combined handwriting and keypad-based multimodal interfaces. In the last few decades, several approaches to the problem of signature verification have been proposed. However, most research has been carried out considering signatures captured with digitizing tables, in which the quality of the captured data is much higher than in handheld devices. Signature verification on handheld devices represents a new scenario both for researchers and vendors. In this chapter, we introduce automatic signature verification as a component of multimodal interfaces; we analyze the applications and challenges of signature verification and overview available resources and research directions. A case study is also given, in which a state-of-the-art signature verification system adapted to handheld devices is presented.*

## INTRODUCTION

The current proliferation and ubiquity of electronic applications and services has motivated the need for user authentication means, which must be convenient and reliable at the same time. Nowadays, access control and user authentication are common tasks that are usually performed with tokens or passwords. In the case of handheld devices, user authentication is performed in most cases with passwords that are provided through keypad-based monomodal interfaces. Biometric-based systems represent an alternative to traditional user validation methods, as they rely on anatomical (e.g. fingerprint, iris) or behavioral (e.g. voice, signature) traits to authenticate a user (Jain, Ross & Pankanti, 2006).

DOI: 10.4018/978-1-60566-978-6.ch014

These traits cannot be in general forgotten or stolen without severe consequences for the user. As an example, it is now common to observe fingerprint verification systems in handheld and portable electronic devices (e.g. laptops). Due to the enhanced convenience provided to the users compared to the use of passwords, biometrics such as voice, fingerprint or signature can improve the usability of mobile user authentication applications.

Among biometric traits, signature is one of the most socially accepted as it has been used in financial and legal transactions for centuries. Despite its acceptance, automatic signature verification is a challenging task per se, as it must face at the same time the variability among genuine signatures from an individual (high *intra-class* variability) and the possibility of skilled forgers, which can imitate a signature with high accuracy (low *inter-class* variability). Moreover, forgers are not always possible to model during the design of a verification system due to their unknown nature. Consequently, reliable automatic signature verification is still an open issue, which can be corroborated by the notable variety of research works conducted on this subject in the last decades (Plamondon & Lorette, 1989; Fierrez & Ortega-Garcia, 2007).

Two main types of signature verification systems exist, depending on the nature of the information they use to perform verification. *Off-line* systems use static signature images, which may have been scanned or acquired using a camera. *On-line* or *dynamic* systems use captured signature time-functions, extracted from the pen motion. These functions can be obtained using digitizer tablets or touchscreen-enabled devices such as Tablet-PCs and smartphones. Traditionally, dynamic systems have presented a better performance than off-line systems as more information levels (e.g. pen speed, pen pressure, etc.) than the signature static image are available to perform verification (Plamondon & Lorette, 1989).

In this context, touchscreen-enabled handheld devices represent an appropriate computing platform for the deployment of dynamic signature verification systems as they provide both a pen-based input and reasonable computing power. These devices are already prepared for multimodal interaction, usually based on the combination of keypad, handwriting or speech modalities. As a matter of fact, commercial devices already provide handwritten character recognition as a text input alternative for years. Touchscreen-enabled smartphones have recently experienced an outstanding technological evolution, representing many new promising scenarios and applications for ubiquitous user interfaces and, specifically, for signature verification. They have gathered an increasing interest among the scientific and industrial communities as they provide multimodal capabilities (Oviatt & Lunsford, 2003) and a convenient way of interfacing with other systems; being thus able to host a wide range of user-centric applications (Ballagas, Borchers, Rohs, Sheridan, 2006). Verification of signatures or graphical passwords on handheld devices provides a convenient method for ubiquitous user authentication in commercial payments or financial transactions among other applications.

In this chapter we consider dynamic signature verification on handheld devices and overview its major applications and challenges. The chapter is focused on the handwritten signature modality, which can be integrated in multimodal interfaces for mobile devices based on touchscreens and keypads or speech. Signature may be used as an optional (and more natural) validation means instead of typed passwords or as a mandatory step in electronic transactions. The chapter is organized as follows. First, the typical architecture of a dynamic signature verification system is outlined. Applications, a market overview and challenges are then presented, which are followed by a summary of available resources and standards. We present as a case study a state-of-the-art signature verification system based on local and global features that has been specifically adapted to handheld devices. The system is tested using a signature database