Pattern Recognition 42 (2009) 2117–2126

Contents lists available at ScienceDirect

Pattern Recognition

journal homepage: www.elsevier.com/locate/pr

On-line signature verification system with failure to enrol management

Joan Fàbregas, Marcos Faundez-Zanuy*

Escola Universitària Politècnica de Mataró, Avda. Puig i Cadafalch 101-111, 08303 Mataro, Barcelona, Spain

ARTICLE INFO

Article history:
Received 16 July 2008
Received in revised form 9 December 2008
Accepted 18 January 2009

Keywords:
On-line signatures
Biometric authentication
Feature extraction
Individual threshold
Failure to acquire
Failure to enrol

ABSTRACT

In this paper we introduce a new biometric verification system based on on-line signatures and simulate its operation. For this purpose we have split the MCYT signature database in three subsets: one for classifier training, another for system adjustment and a third one for system testing simulating enrolment and verification. This context corresponds to a real operation, where a new user tries to enrol an existing system and must be automatically guided by the system in order to detect the failure to enrol (FTE) situations. The main contribution of this work is the management of FTE situations by means of a new proposal, called intelligent enrolment, which consists of consistency checking in order to automatically reject low quality samples. This strategy enhances the performance of the system to 22% when 8% of the users are left out. In this situation 8% of the people cannot be enroled in the system and must be verified by other biometrics or by human abilities. These people are identified with intelligent enrolment and the situation can be thus managed. In addition we also propose a DCT-based feature extractor with threshold coding and discriminability criteria.

1. Introduction

Handwritten signatures have a long tradition in commonly encountered verification tasks like, for example, financial transactions and document authentication. They are normally used and well accepted by the general public, and signatures are easily obtained with relatively cheap devices. These are important advantages of signature recognition over other biometrics. Yet, signature recognition has also some drawbacks: it is a difficult pattern recognition problem due to large possible variations between signatures of the same person. These variations may be originated by instabilities, emotions, environmental changes, etc, and are person dependant. In addition, signatures can be forged more easily than other biometrics.

Signature recognition can be split into two categories depending on the data acquisition method:

- *Off-line* (*static*): The signature is scanned from a document and the system recognizes the signature analysing its shape.
- *On-line* (*dynamic*): The signature is acquired in real time by a digitizing tablet and the system analyses shape and the dynamics of writing, like for example: positions in the x and y axis, pressure applied by the pen, etc.

Using the dynamic data, further information can be inferred, such as accelerations, velocity, curvature radius, etc. [1]. In this paper, we will focus on this approach.

For a signature verification system, depending on testing conditions and environment, three types of forgeries can be established [2]:

- Simple forgery, where the forger makes no attempt to simulate or trace a genuine signature.
- Substitution or random forgery, where the forger uses his/her own signature as a forgery.
- Freehand or skilled forgery, where the forger tries and practices imitating as closely as possible the static and dynamic information of the signature to be forged.

From the point of view of security, the last one is the most damaging; for this reason, some databases suitable for system development include some trained forgeries [3,4].

A comprehensive survey of signature verification can be found in [1,2,5]. The existing methods differ both in feature selection and in decision techniques and they can be divided into two classes [6]:

- *Feature-based*: In which a set of global features is derived from the signature trajectories. Some authors take measures such as total duration of the signature or the number of pen ups, etc. [7,8]. Others compute the Fourier descriptors of the signature

* Corresponding author.
E-mail address: faundez@eupmt.es (M. Faundez-Zanuy).

0031-3203/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.patcog.2009.01.019

trajectory [9–11]. Once the features are obtained, the decision method is some kind of distance [12], a statistical model [8], or a neural network [13].

- *Function-based*: In which the time sequences describing the local properties of the signature are used for recognition [14–16]. The most usual ones are position, velocity and acceleration of the trajectory, but also the pressure and the pen inclination [17]. Time sequences are then matched by using elastic distance measures such as dynamic time warping [18–20] or converted into a sequence of vectors and modelled with hidden Markov models [6,21,22].

There are also systems that combine the confidences provided by the two approaches [8,22] and/or use user-dependant decisions, with score normalization techniques [37] or user-dependant thresholds [15], and yield better verification results.

The evaluation of a verification system requires the analysis of two types of errors [24]: Type I error or false reject rate (FRR), which is the percentage of genuine signatures incorrectly rejected by the system. Type II error or false acceptance rate (FAR), which is the percentage of forgeries incorrectly accepted by the system. These two types of errors usually have different associated costs depending on security requirements. The performance of a system may be measured by the value of the detection cost function (DCF) defined as [25]:

$$DCF = C_{FR} \cdot FRR \cdot P(C) + C_{FA} \cdot FAR \cdot P(I) \quad (1)$$

where C_{FR} is the cost of a false reject, C_{FA} is the cost of a false acceptance, $P(C)$ is the prior probability of a client (genuine signature) and $P(I)$ is the prior probability of an impostor (forgery). In this paper, in order to facilitate the comparison with other papers, $C_{FE} = C_{FA} = 1$ and $P(C) = P(I) = \frac{1}{2}$ will be assumed. DCF represents the expected cost of making a detection decision based on a weighted sum of False Rejections and False Acceptance error probabilities. A more meaningful performance measure is the error trade-off curve (DET) [25], which shows how one error changes with respect to the other for several threshold values.

Another measure of a system's performance, often used in biometrics literature, is the equal error rate (EER) [24], which is the point where the FAR and FRR are the same. In order to facilitate comparison with state-of-the-art performances we have also computed the EER where possible. To obtain the EER value, once the tests have been performed, the threshold is trimmed-up in order to balance FAR and FRR. State-of-the-art EER results for skilled forgeries vary around 6% and 3% [4].

In addition to FAR and FRR there are also two other kind of errors that are usually neglected in laboratory conditions, although they are crucial for real world applications [24]. They are named failure to acquire (FTA) and failure to enrol (FTE), and are defined as follows:

Failure to enrol (*FTE*) *rate*: FTE rate is the expected proportion of the population for whom the system is unable to generate repeatable templates. This will include those unable to present the required biometric feature, those unable to produce an image of sufficient quality at enrolment, and those who cannot reliably match their template in attempts to confirm that the enrolment is usable.

Failure to acquire (FTA) rate: FTA denotes the proportion of times the biometric device fails to capture a sample when the biometric characteristic is presented to it.

1.1. Motivation of this work

Normally the literature on biometrics deals with the ideal situation where the set of known users is predefined in advance and no new users are added after the initial set up of the system. In some cases, the problem is even more restricted and it is limited to what is known as closed world problems [23]. In this paper, we go one step further because we deal with the more real situation using two operation steps. First, we adjust a biometric signature recognition system by means of a predefined set of initial users. Second, we study the situation where new users try to enrol in an automatic fashion and the system must be able to detect and manage the FTE situations. That is, the system automatically detects training samples which are unstable to create a consistent model and asks the user for a new biometric sample, we call this procedure 'intelligent enrolment'. This situation is not new in biometrics; ~4% of people cannot be enroled in a fingerprint system due to the poor quality of their fingerprints. In a signature verification system, due to the large variability among signatures of the same person, this percentage is expected to be bigger. This is a challenging problem that has been neglected in the on-line signature recognition literature.

1.2. Paper organization

This paper is organized as follows: Section 2 provides an overview of the initial system setup. Section 3 explains the system operation. Section 4 presents the experimental results using the MCYT database and Section 5 summarizes the main conclusions.

2. Initial system design

In this section we will discuss the initial set up for the on-line signature verification system, considering a database of genuine and impostor users. Usually, a pattern recognition system consists of two main blocks: feature extraction and classifier. Fig. 1 summarizes this scheme for our on-line signature recognition problem. Given a set of measurements provided by a digitizing tablet, we try to obtain the most relevant features for classification and then a classifier is used to compare with a reference.

2.1. Feature extraction

We use a spectral method [9–11], but replacing the usual Fast Fourier Transform by the one dimensional discrete cosine transform (DCT) to perform a low-frequency filtering of temporal variables. The same approach has been previously used for face recognition [26] with spatial variables. This method characterizes the dynamic and global behaviour of the signature by taking some of the first terms of the DCT which is due to the excellent energy compaction of the DCT and the fact that it is a near optimal substitute for the Karhunen–Loeve transform [29]. It does not require pre-processing (re-sampling and smoothing) as other commonly used methods do [15,27].

Another difference with the usual spectral methods (including [28]) is that, with the help of the classifier (see next section), we perform a threshold coding with discriminability criterion and not the usual zonal or threshold coding with representability criterion, commonly used for image compression [29].

The digitizing tablet provides the horizontal and vertical position of the pen over time in equally spaced intervals: $x(n)$ and $y(n)$, $n = 1, \ldots, N_s$. It also provides the pressure $p(n)$, the azimuth angle $\gamma(n)$, and the altitude angle $\phi(n)$, of the pen at the same intervals [3] (see Fig. 2). N_s stands for signature time durations in time samples. We complete these five discrete measures with other two calculated discrete functions: the displacement $\delta s(n) = \sqrt{(\delta x)^2 + (\delta y)^2}$, $n = 1, \ldots, N_{s-1}$; where $\delta x = x(n) - x(n-1)$ and $\delta y = y(n) - y(n-1)$ are the coordinate differences between two consecutive points; and the curvature angle $\theta(n) = \alpha(n) - \alpha(n-1)$, $n = 1, \ldots, N_{s-2}$; where $\alpha(n) = \arctan(\delta y / \delta x)$, $n = 1, \ldots, N_{s-1}$.

The feature extraction performs the DCT of each variable (see Fig. 1) and initially takes the first 30 terms (this number will be