Expert Systems with Applications 37 (2010) 3676–3684

Contents lists available at ScienceDirect

Expert Systems with Applications

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

Combining local, regional and global matchers for a template protected on-line signature verification system

Loris Nanni [a,*], Emanuele Maiorana [b], Alessandra Lumini [a], Patrizio Campisi [b]

[a] DEIS, Università di Bologna, Viale Risorgimento 2, 40136 Bologna, Italy
[b] Università degli Studi "Roma Tre", Via della Vasca Navale 84, 00146, Roma, Italy

ARTICLE INFO

Keywords:
On-line signature
Ensemble of classifiers
Dynamic Time Warping
Hidden Markov Models
Linear Programming Descriptor
BioHashing
Template protection

ABSTRACT

In this work an on-line signature authentication system based on an ensemble of local, regional, and global matchers is presented. Specifically, the following matching approaches are taken into account: the fusion of two local methods employing Dynamic Time Warping, a Hidden Markov Model based approach where each signature is described by means of its regional properties, and a Linear Programming Descriptor classifier trained by global features.

Moreover, a template protection scheme employing the BioHashing and the BioConvolving approaches, two well known template protection techniques for biometric recognition, is discussed.

The reported experimental results, evaluated on the public MCYT signature database, show that our best ensemble obtains an impressive Equal Error Rate of 3%, when only five genuine signatures are acquired for each user during enrollment. Moreover, when the proposed protected system is taken into account, the Equal Error Rate achieved in the worst case scenario, that is,when an "impostor" is able to steal the hash keys, is equal to 4.51%, whereas an Equal Error Rate ~0 can be obtained when nobody steals the hash keys.

1. Introduction

People recognition based on signatures is one of the most commonly employed biometric based authentication methods. In a signature verification system, the individuals can be recognized by measuring and analyzing the activity of signing, which includes information regarding the stroke order, the pressure applied by the pen or its speed, in addition to the visual aspect of the signatures. Being part of everyday life, signature based authentication is perceived as a non-invasive and non-threatening process by the majority of the users. Furthermore, the written signature has a high legal value. On the other hand, the signature can be influenced by physical and emotional conditions, and therefore exhibits a significant variability which must be taken into account in the authentication process.

Several interesting reviews (Dimauro, Impedovo, Lucchese, Modugno, & Pirlo, 2004; Fierrez & Ortega-Garcia, 2008; Impedovo & Pirlo, 2008; Leclerc & Plamondon, 1994) of the state-of-the-art on signature recognition have been proposed during the last years. Basically, signature based authentication can be either *static* or *dynamic*. In the static mode, also referred to as *off-line*, only the written image of the signature, typically acquired through a camera or an optical scanner, is employed. In the dynamic mode, also called *on-line*, signatures are acquired by means of a graphic tablet or a pen-sensitive computer display, which can provide temporal information about the signature, such as the pressure, the velocity, the pen tilt signals versus time, and so on.

The on-line signature verification methods proposed in literature (Jain, Griess, & Connell, 2002; Ortega-Garcia, Fierrez-Aguilar, Martin-Rello, & Gonzalez-Rodriguez, 2003; Ortega-Garcia, Fierrez-Aguilar, & Simon, 2003; Plamondon & Lorette, 1989; Sakamoto et al., 2005) can be distinguished into three main categories, which differ in the information extracted from the available data:

(a) *global approaches*, where a set of global parametric features (i.e. signature total duration, number of pen-ups, and so on) are extracted from the acquired signatures, and used to train a classifier (Fierrez-Aguilar, Ortega-Garcia, & Gonzalez-Rodriguez, 2005). Some recent works (Nanni & Lumini, 2005; Nanni, 2006) demonstrate that a Random Subspace ensemble of one-class classifiers allows a considerable performance improvement, with respect to a stand-alone one-class classifier.
(b) *local function based approaches*, where the time functions extracted from different signatures are directly matched by using elastic distance measures, such as Dynamic Time Warping (DTW) (Jain et al., 2002), instead to be used as features for a classifier. During the comparative studies performed for the Signature Verification Competition of 2004

* Corresponding author.
E-mail address: lnanni@deis.unibo.it (L. Nanni).

0957-4174/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.eswa.2009.10.023

(SVC 2004) (Yeung et al., 2004), the on-line signature recognition algorithm proposed in Kholmatov and Yanikoglu (2005), employing DTW matching, gave the lowest average Equal Error Rate (EER) values, when tested with skilled forgeries. In Piyush Shanker and Rajagopalan (2007) a modified DTW algorithm is presented, which is based on the stability of the components of the signature and outperforms the standard DTW;

(c) *regional function based approaches*, where the acquired signatures are analyzed by estimating some regional properties, which are then employed to train a given classifier. The best regional approaches model on-line signatures with Hidden Markov Models (HMMs) (Fierrez-Aguilar, Ortega-Garcia et al., 2005; Fierrez-Aguilar et al., 2005). Moreover, in Nanni and Lumini (2008b) signatures are decomposed employing wavelet transforms, and the Discrete Cosine Transform (DCT) is applied to the resulting approximation coefficients. A Linear Programming Descriptor (LPD) classifier is then trained using the obtained DCT coefficients.

According to some recently published results (Yeung et al., 2004), the most promising approaches belong to the category of local function based methods. However, one of the major research trends in on-line signature verification is to combine different systems, in order to build an ensemble of classifiers (Fierrez-Aguilar, Nanni, Lopez-Penalba, Ortega-Garcia, & Maltoni, 2005; Van, Garcia-Salicetti, & Dorizzi, 2007).

In this work, an ensemble of matchers belonging to different categories is presented. The ensemble is built by combining:

- a local function based matcher, obtained from the fusion of two variants of the Kholmatov's DTW algorithm (Kholmatov & Yanikoglu, 2005);
- a regional function based matcher, where each signature is represented by a sequence of vectors describing regional properties, and HMMs are employed as classifiers;
- a global approach employing a LPD classifier, trained by global parametric features.

Moreover, the security of a signature based authentication system is also considered. The use of biometric data in an automatic recognition system involves the possibility of identity theft, with the risk of improper use of the stolen information and, even worse, the impossibility to replace the stolen data. When designing a biometric system, several measures have then to be carefully considered, in order to enhance biometric data resilience against attacks (Ratha, Connell, & Bolle, 2001). The state-of-the-art on biometric template protection is discussed in details in Section 2.

In this paper, a protected signature based authentication system is build as an ensemble of already presented approaches. Specifically, two different solutions for template protection are implemented: the Improved BioHashing (Lumini & Nanni, 2007) and the BioConvolving method proposed in Maiorana, Martinez-Diaz, Campisi, Ortega-Garcia, and Neri (2008).

The experimental results, reported in Section 4, are obtained using the public SUBCORPUS-100 MCYT Bimodal Biometric Database (Ortega-Garcia et al., 2003; Ortega-Garcia, Fierrez-Aguilar, Simon, et al., 2003), which comprises signatures taken from 100 subjects, and confirm the effectiveness of the proposed ensembles of classifiers.

2. Biometric template protection

In the recent past, many solutions have been investigated to secure biometric templates. Among them, the most promising approaches consist in the implementation of *cancelable biometrics* (Ratha et al., 2001), which can be roughly described as the application of an intentional and repeatable modification to the original biometric templates. Typically, a properly defined cancelable biometrics should satisfy the properties of *renewability* (it should be possible to revoke a compromised template and issue a new one based on the same biometric data) and *security* (it should be impossible or computationally unfeasible to obtain the original biometric template from the modified one). Moreover, it should grant that the recognition performance of the protected system does not degrade significantly with respect to an unprotected system.

A classification of the proposed protection methods has been presented in Jain, Nandakumar, and Nagar (2008), where two macro-categories, referred to as *Biometric Cryptosystems* and *Feature Transformation* approaches, are considered. Biometric cryptosystems typically employ binary keys to secure the biometric templates, and during the process some public information, usually referred to as *helper data*, is used. This category can be further divided in *key binding* systems, where the helper data are obtained by binding a key with the biometric template (Juels & Wattenberg, 1999; Juels & Sudan, 2006), and *key generating* systems, where both the helper data and the cryptographic key are directly generated from the biometric template (Sutcu, Lia, & Memon, 2007). In a feature transformation approach a transformation function, typically governed by random parameters employed as keys, is applied to the biometric template, thus generating the desired cancelable biometrics. It is possible to distinguish between *salting* approaches, where the employed transforms are invertible (Teoh, Ngo, & Goh, 2006), and *non-invertible transform* approaches, where a one-way function is applied to the considered templates (Ratha, Chikkerur, Connell, & Bolle, 2007). The security of salting approaches relies in the secure storage of the transform parameters, whereas when the latter approaches are considered, their security relies in the difficulty to invert the transformation, even if its defining parameters are known. When a feature transformation approach is employed, the transformed templates can remain in the same (feature) space of the original ones, being then possible to employ, in the authentication stage, the matchers designed for the original biometric templates. This allows to guarantee performance which is similar to that of an unprotected approach. Moreover, having the possibility of employing dedicated matchers, a score can be obtained as the output of a recognition process, even if it has been performed in a transformed domain: secure multibiometric systems can therefore be implemented through score-level fusion techniques (Ross, Nandakumar, & Jain, 2006).

Signature template protection have been first considered in Vielhauer, Steinmetza, and Mayerhofer (2002) with a key generation approach, where a set of parametric features was extracted from the acquired dynamic signatures, and a hash function was applied to the feature binary representation, obtained exploiting some statistical properties of the enrollment signatures. In Freire-Santos, Fierrez-Aguilara, and Ortega-Garcia (2006) an adaptation of the fuzzy vault to signature protection has been proposed, employing a quantized set of maxima and minima of the temporal functions mixed with chaff points in order to provide security. Also the fuzzy commitment (Juels & Wattenberg, 1999) (more specifically, its practical implementation known as *Helper Data System* (Van der Veen, Kevenaar, Schrijen, Akkermans, & Zuo, 2006) has been employed to provide security for the features extracted from an on-line signature, as proposed in Maiorana et al. (2008), Campisi, Maiorana, & Neri (2008), where a user-adaptive error correcting code selection was also introduced. A salting approach has been proposed in Yip, Goh, Ngo, & Teoh (2006), as an adaptation of the *BioHashing* method (Teoh et al., 2006) to signature templates. Moreover, in Lumini & Nanni (2007)) an improved version of the