Pattern Recognition 60 (2016) 998–1014

Contents lists available at ScienceDirect

Pattern Recognition

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

Signatures verification based on PNN classifier optimised by PSO algorithm

Piotr Porwik *, Rafal Doroz, Tomasz Orczyk

Institute of Computer Science, University of Silesia, ul. Bedzinska 39, 41-200 Sosnowiec, Poland

ARTICLE INFO

Article history:
Received 28 February 2015
Received in revised form
22 April 2016
Accepted 30 June 2016
Available online 2 July 2016

Keywords:
Hotelling's statistics
Classification
PNN
PSO
Signature verification

ABSTRACT

In this paper, we propose a new biometric pattern recognition method. In classical techniques only features of raw objects are compared. In our approach we will use composed signatures' features. Features of a signature are associated with appropriate similarity coefficients and individually matched to a given signature. If it is necessary, composed features can be reduced. In the proposed study the most promising results are obtained from Hotelling's approach. Data comprising the composed features allow to achieve higher signature recognition level, compared to unprocessed (raw) data. It is the greatest novelty of the paper—the proposed method of data reduction together with a new type of similarity measure gives a high signature recognition level for various classes of classifiers.

Leaning on investigations carried out, the classifier based on the Probabilistic Neural Network (PNN) has been introduced. Optimal parameters of the PNN have been determined by means of the Particle Swarm Optimization (PSO) procedure. The two class PNN classifier demonstrates high efficiency, compared to other classifiers. The described signature verification system consists of three units where features are captured, composed features are prepared, data are reduced and verified. The results of the study carried on signatures of the SVC2004 and MCYT databases and demonstrate the effectiveness of the proposed approach in comparison with other methods from the literature.

1. Introduction

The automatic recognition of users, based on biometrics, has been widely investigated by many researchers in recent years. Additionally, verification of individuals by their signature is a widely accepted technique in everyday life, particularly in banking and commercial transactions. It is a very old document authentication technique; hence it is very popular, and socially acceptable [1–7]. An individual's verification on the basis of a signature, except in trivial cases, is not easy and requires an analysis of many special cases. For example, some users can consciously change their signature. Some people exhibit great variability in the way they write their signature because of some diseases, temporary influence of emotional condition, or due to lack of habit. It should also be noted that genuine signature can be falsified either by random or professional forgers. The difficulties mentioned above can be overcome by using different verification methods including voting [8], fuzzy approach [9], multi-modal systems [10–12], different classifiers' fusion [13] or signature partitioning [14,15,7]. Signature recognition techniques can be split into two categories: static and dynamic techniques. In the static mode, the user puts a signature on paper and then an optical scanner digitizes the image. It is a so-called *off-line* technique, where only the shape of the signature is recognized. In the dynamic mode, the user puts a signature on a digitizing tablet. This device samples the features of a signature in a real time. Dynamic recognition is very attractive because it allows features of behavioral biometrics to be registered. This technique is also known as the *on-line* technique [1,16–18]. Various *on-line* methods use up to 40 different features (i.e. relative position, speed, acceleration, pen pressure, pen angle, etc.), which can be divided into local and global signature features [19–21]. "Local features" refer to features within a single sample (point) of a signature trace (i.e. point position, local speed, pen pressure, etc.) whereas "global features" use the whole signature trace (i.e. trace length, signature area, etc.). A specially designed tablet to capture digital signatures can transmit data directly to a computer, helping to construct classification algorithms operating in the *on-line* mode. A handwritten signature is the most widely accepted biometric verification method. For this reason, different techniques have been developed and adopted in order to construct reliable handwritten signature verification systems: Hidden Markov Models (HMMs) [22–24], Support Vector Machines (SVMs) [25,6], Dynamic Time Wrapping (DTW) [1,26–28], Principal

* Corresponding author.
E-mail addresses: piotr.porwik@us.edu.pl (P. Porwik), rafal.doroz@us.edu.pl (R. Doroz), tomasz.orczyk@us.edu.pl (T. Orczyk).

http://dx.doi.org/10.1016/j.patcog.2016.06.032
0031-3203/

Component Analysis (PCA) [29], fuzzy systems [9], ensemble based classifiers for accuracy signature improvement [13,17] and others. The importance of the problem is significantly noticeable: since 2004, various competitions have been devoted to signature verification and recognition. In these competitions, various teams or individual contestants present different algorithms. These algorithms are a valuable source of knowledge because the description of these algorithms and preprocessing techniques are published and accessible [7]. In recent years, there have been more competitions such as SigComp2011 [30], 4NSigComp2012 [31], and SigWiComp2013 [32]. The organizers of these competitions publish benchmark databases that allow one to compare obtained results. Authors of this paper have also reported on signature verification [33,19], where they have described a novel similarity measure for signature comparison and an innovative feature selection method. In our previous papers signature features were compared in the windows area [19] or points of a signature were divided into subsets [33]. The similarity between corresponding subsets was compared. Unfortunately, dynamic features were separately analyzed. For this reason we have introduced a technique where signature dataset have been simultaneously analyzed and in reduction process dataset were minimized [34,35]. Finally, an optimal number of features was processed by the *k*-NN classifier. We noticed that feature selection procedure can be improved and linked with various similarity measures. Ultimately, dynamic features are related to similarity measures. It has improved a machine-learning method of data classification, which is presented in this paper.

Verification methods can also be categorized into other basic groups:

1. *Global and local feature based methods*: Global features treat patterns as a whole, while local features are extracted from a limited area of a pattern. In this feature extraction method, for example, the vertical and horizontal projections are analyzed together with the height and width of a signature. These approaches are also called the parameter based methods [20,36]. The wide survey of methods that utilize objects with both global and local features is presented in the work [10]. In [20], an individual's signature feature discriminative power is determined and then fusion of Principal Component Analysis method and a Parzen window classifier are used in the classification process. In [6] an off line signature datasets were used and only genuine signatures were taken into consideration. The images are processed by Curvelet transform, decision functions, and adjusting differently. Finally, a signature is categorized by means of a one-class SVM classifier.
2. *Time function based methods*: In this approach, signature dynamic features are registered as a time series that contains information about changes of signature features over time. It is the so-called behavioral technique analysis of a signature. Corresponding time series of different signatures are compared and classified using the Dynamic Time Warping (DTW) technique [28]. As a classification result, the DTW matching path cost is calculated. In [1] the vector quantization and DTW methods are combined to build a fusion based classifier. Score fusion is a classification indicator. In [34], the authors have proposed a verification approach based on a multidimensional set of features computed for each discrete signature point. This set contains measured dynamic features which describe shape (*x*, *y* coordinates), local pressure, velocities and accelerations. Finally, by means of the *k*-NN classifier, the similarity between the corresponding dynamic features is calculated. In [37] feature combinations associated with the most commonly used time functions related to the signing process are analyzed. Based on the defined consistency factor, the most consistent feature combinations were determined,
3. *Region based methods*: In [16] the authors have proposed a method of signature verification, based on dynamic features. The signature of each person is split into sections. For every section, a codebook is prepared. Signature features together with appropriate codebooks improve classification results. Other approaches have been proposed in [14], where values of velocity and pressure signals partitioning of signature waveforms have been formed. The classification process is performed on the basis of distance between the template and the sample signature in the partitions. In this step, a signature is classified as a genuine one or a forgery. A similar approach is proposed in [15,38]. In that method, instead of horizontal partitions, vertical partitions are extracted. In [14,15], a short survey of different signature recognition methods have also been stated. In [33], a set of signature discrete points is divided into some subsets. Signature points are assigned to a given subset on the basis of an analysis of the dynamic feature values registered in these points. The similarity of signatures is evaluated by determining the similarity between the corresponding subsets in the signatures being compared. Partitioning of features is also proposed in [13].
4. *Combined* (*hybrid*) *based methods*: This approach is based on a combination of different methods as mentioned above. In [21], a biometric system of dynamic signature verification has been proposed, where an ensemble of local, global, and regional matchers was applied. The Hidden Markov Model approach has been used for analysis of the regional properties of a signature, and the Linear Programming Descriptor classifier trained on global features was employed. In [39], the authors have presented a biometric system where combination of global features and function based methods was employed. The feature based module calculates the distance between multi-dimensional vectors and a reference signature. The function based module calculates the accumulated distance between input time of a reference signature and a test signature. Finally, the calculated distances are combined and the similarity coefficient between the signatures is computed. In [3] biometric bimodal system based on speech and an *on-line* signature is presented. In this model, wavelet energy coefficients and traditional signature's features (azimuth, altitude, pressure, coordinates and time stamp) form a combined non-homogeneous vector of features. A feature selection procedure is then applied to reduce the feature vector dimension.

In this paper, we propose a new approach for signature verification based on signature time functions (*x*, *y*), trajectories, similarity coefficients, and Hotelling statistics [40,41], allowing us to reduce the amount of data needed for classification. The Hotelling procedure gives two advantages: it allows to reduce data and selects similarity coefficients with the greatest discriminant power. Our proposition has an important advantage over other available methods that use hybrid-based methods for dynamic signature verification. These advantages, among others, include the use of the special kind of dynamic features preparation and selection in the classification process. We propose using the Probabilistic Neural Networks (PNN) [42–44] as a classifier which offers high signature verification accuracy. The PNN is used as it is faster than the perceptron network, and insensitive to outliers. Primary characteristics of this method can be summarized as follows:

- In our experiments, a great number of existing dynamic features of a signature have been taken into consideration. These kinds of features are very difficult to forge and are changeable for each user. Even a single dynamic feature is difficult to translate into a