Neural Networks on Handwritten Signature Verification

J. Francisco Vargas
University of Las Palmas de Gran Canaria, Spain & Universidad de Antioquia, Colombia

Miguel A. Ferrer
University of Las Palmas de Gran Canaria, Spain

INTRODUCTION

Biometric offers potential for automatic personal identification and verification, differently from other means for personal verification; biometric means are not based on the possession of anything (as cards) or the knowledge of some information (as passwords). There is considerable interest in biometric authentication based on automatic signature verification (ASV) systems because ASV has demonstrated to be superior to many other biometric authentication techniques e.g. finger prints or retinal patterns, which are reliable but much more intrusive and expensive. An ASV system is a system capable of efficiently addressing the task of make a decision whether a signature is genuine or forger. Numerous pattern recognition methods have been applied to signature verification. Among the methods that have been proposed for pattern recognition on ASV, two broad categories can be identified: memory-based and parameter-based methods as a neural network. The Major approaches to ASV systems are the template matching approach, spectrum approach, spectrum analysis approach, neural networks approach, cognitive approach and fractal approach.

The proposed article reviews ASV techniques corresponding with approaches that have so far been proposed in the literature. An attempt is made to describe important techniques especially those involving ANNs and assess their performance based on published literature. The paper also discusses possible future areas for research using ASV.

BACKGROUND

As any human production, handwriting is subject to many variations from very diverse origins: Historic, geographic, ethnic, social, psychological, etc (Bou-letreau, 1998). ASV is a difficult problem because signature samples from the same person are similar but not identical. In addition, a person signature often changes radically during their lifetime (Hou, 2004). Although these factors can affect a given instance of a person writing, writing style develops as the writer learns to write, as do consistencies which are typically retained (Guo, 1997). One of the methods used by expert document examiners is to try to exploit these consistencies and identify ones which are both stable and difficult to imitate. In general, ASV systems can be categorized into two kinds: The On-line and Off-line systems. For On-line, the use of electronic devices to capture dynamics from signature permits to register more information about the signing process while improving the system performance, in the case of Off-line approaches for ASV, this dynamic information is lost and only a static image is available. This makes it quit difficult to define effective global or local features for the verification purpose.

Three different types of forgeries are usually take into account on ASV system: random forgeries, produced without knowing either the name of the signer nor the shape of his signature; simple forgeries, produced knowing the name of the signer but without having an example of his signature; and skilled forgeries, produced by people who, looking at an original instance of the signature, attempt to imitate it as closely as possible. The problem of signature verification become more difficult when passing from random to simple and skilled forgeries, the later being so difficult a task that even human beings make errors in several cases. It is pointing out that several systems proposed up to now, while performing reasonably well on a single category of forgeries, decrease in performance when working with all the categories simultaneously, and generally this decrement is bigger than one would expect.(Abuhaiba,2007; Ferrer,2005).
Numerous pattern recognition methods have been applied to signature verification (Plamondon, 1989). Among the methods that have been proposed for pattern recognition, two broad categories can be identified: memory-based techniques in which incoming patterns are matched to a (usually large) dictionary of templates, and parameter-based methods in which pre-processed patterns are sent to a trainable classifier such as a neural network (Lippmann, 1987). Memory-based recognition methods require a large memory space to store the templates, while a neural network is a parameter-based approach which just requires a small amount of memory space to store the linking weights among neurons. Mighell et al (Mighell, 1989) were apparently the first to work in applying NNs for off-line signature classification. Sabourin and Drouhard (Sabourin,1992) presented an method based on directional probability density functions together with a BackPropagation neural networks (BPN) to detect random forgery. Qi and Hunt (Qi, 1996) used global and grid features with a simple Euclidean distance classifier. Sansone and Vento (Sansone,2000) proposed a sequential three-stage multi-expert system, in which the first expert eliminates random and simple forgeries, the second isolates skilled forgeries, and the third gives the final decision by combining decisions of the previous stages together with reliability estimations. Baltzakis and Papamarkos (Baltzakis,2001) developed a two-stage neural network, in which the first stage gets the decisions from neural networks and Euclidean distance classifiers supplied by the global, grid and texture features, and the second combines the four decisions using a radial-base function (RBF) neural network.

MAIN FOCUS OF THE CHAPTER

As mentioned above, the major approaches to signature verification systems are the template matching approach, spectrum approach, spectrum analysis approach, neural networks approach, cognitive approach and fractal approach. The rigid template matching, the simplest and earliest approach to pattern recognition, can detect random forgeries from genuine signatures successfully, but cannot detect skilled forgeries effectively. The statistical approach, including HHMs, Bayesian and so on, can detect random forgeries as well as skilled forgeries from genuine ones. Structural approach shows good performance when detecting genuine signatures and forgeries. But this approach may yield a combinatorial explosion of possibilities to be investigated, demanding large training sets and very large computational efforts. The spectrum analysis approach can be applied to different languages, including English and Chinese. Moreover it can be applied to either on-line or off-line verification systems.

Neural networks approach offers several advantages such as, unified approaches for feature extraction and classification and flexible procedures for finding good, moderately nonlinear solutions. When it is used in either on-line or off-line signature verification, it also shows reasonable performance.

Neural Networks on ASV

Multi-layer perceptron (MLP) neural networks are among the most commonly used classifiers for pattern recognition problems. Despite their advantages, they suffer from some very serious limitations that make their use, for some problems, impossible. The first limitation is the size of the neural network. It is very difficult, for very large neural networks, to get trained. As the amount of the training data increases, this difficulty becomes a serious obstacle for the training process. The second difficulty is that the geometry, the size of the network, the training method used and the training parameters depend substantially on the amount of the training data. Also, in order to specify the structure and the size of the neural network, it is necessary to know a priori the number of the classes that the neural network will have to deal with. Unfortunately, when talking about a useful ASV, a priori knowledge about the number of signatures and the number of the signature owners is not available (Baltzakis,2001).

For the BPN case, a learning law is used to modify weight values based on an output error signal propagated back through the network. From random initial values, the weights are changed according to this learning law that uses a learning rate and a smoothing rate which sometimes allows a faster convergence of the training phase. The training phase is critical, especially when the data to be classified are not clearly distinguishable and when there are not enough examples to conduct training. In this case, the training phase can be very long and it may even be impossible to obtain an acceptable performance. Usually a criterion for stopping the training phase is defined. After that, several rejection methods are evaluated to improve the decision taken by