


---

**Chapter III
State of the Art in Off-Line Signature Verification**

Luana Batista
École de technologie supérieure, Canada

Dominique Rivard
École de technologie supérieure, Canada

Robert Sabourin
École de technologie supérieure, Canada

Eric Granger
École de technologie supérieure, Canada

Patrick Maupin
Defence Research and Development Canada (DRDC), Canada

---

**ABSTRACT**

Automatic signature verification is a biometric method that can be applied in all situations where handwritten signatures are used, such as cashing a check, signing a credit card, authenticating a document, and others. Over the last two decades, several innovative approaches for off-line signature verification have been introduced in literature. Therefore, this chapter presents a survey of the most important techniques used for feature extraction and verification in this field. The chapter also presents strategies used to face the problem of a limited amount of data, as well as important challenges and research directions.

Copyright © 2008, IGI Global. Distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

Biometrics refers to automated methods used to verify or recognize the identity of a person. In contrast to the conventional identification systems whose features such as ID cards or passwords can be forgotten, lost, or stolen, biometric systems are based on physiological or behavioral features that are difficult for another individual to reproduce, thereby reducing the possibility of forgery (Kung, Mak & Lin, 2004). Fingerprints, voice, iris, retina, hand, face, handwriting, keystroke, and finger shape are examples of popular features used in biometrics. The use of other biometric measures such as gait, ear shape, head resonance, optical skin reflectance, and body odor is still in an initial research phase (Wayman, Jain, Maltoni & Maio, 2005).

The handwritten signature has always been one of the most simple and accepted ways to authenticate an official document. It is easy to obtain, results from a spontaneous gesture, and is unique to each individual (Abdelghani & Amara, 2006). Automatic signature verification, therefore, can be applied in all situations where handwritten signatures are currently used, such as cashing a check, signing a credit card transaction, and authenticating a document (Griess & Jain, 2002).

The goal of a signature verification system is to verify the identity of an individual based on an analysis of his or her signature through a process that discriminates a genuine signature from a forgery (Plamondon, 1994). Figure 1 shows an example of a signature verification system. The process follows the classical pattern recognition model steps: that is, data acquisition, preprocessing, feature extraction, classification (generally called "verification" in the signature verification field), and performance evaluation.

Depending on the data acquisition mechanism, the process of signature verification can be classified online and off-line. In the online (or dynamic) approach, specialized hardware such as a digitizing tablet or a pressure-sensitive pen is used in order to capture the pen movements over the paper at the same time of the writing. In this case, a signature can be viewed as a space-time variant curve \( \gamma(t) = (x(t), y(t)) \), where \( x(t) \) is the curvilinear displacement, \( y(t) \) is the angular displacement, and \( \dot{\gamma}(t) \) is the torsion of its trajectory (Plamondon & Lorette, 1989). On the other hand, in the off-line (or static) approach, the signature is available on a sheet of paper, which is later scanned in order to obtain a digital representation composed of M x N pixels. Hence, the signature image is considered as a discrete 2D function \( f(x,y) \), where \( x = 0, 1, 2, ..., M \) and \( y = 0, 1, 2, ... \).

Figure 1. Block diagram of a generic signature verification system

\[ \begin{align*}
\text{Acquisition} & \rightarrow \text{Preprocessing} & \text{Feature Extraction} & \rightarrow \text{Verification} \\
\text{Raw signature} & \rightarrow \text{Preprocessed signature} & \text{Feature vector} & \rightarrow \text{genuine signature features} \\
\end{align*} \]
system. The reason is that, in practice, it is rarely possible to obtain samples of forgeries; and, when dealing with banking applications, for example, it becomes impracticable (Mursheed, Bortolozzi & Sabourin, 1995). On the other hand, all types of forgeries are used to evaluate the system's performance.

**FEATURE EXTRACTION TECHNIQUES**

Feature extraction is essential to the success of a signature verification system. In an off-line environment, signatures are acquired from a medium, usually paper, and preprocessed before the feature extraction begins. Off-line feature extraction is a fundamental problem because of a handwritten signature's variability and the lack of dynamic information about the signing process. An ideal feature extraction technique extracts a minimal feature set that maximizes interpersonal distance between signature examples of various persons while minimizing intrapersonal distance for those belonging to the same person.

There are two classes of features used in off-line signature verification: (1) static, related to the signature shape, and (2) pseudo-dynamic, related to the dynamics of the writing. These features can be extracted locally if the signature is viewed as a set of segmented regions, or globally if the signature is viewed as a whole. It is important to note that techniques used to extract global features also can be applied to specific regions of the signature in order to produce local features. In the same way, a local technique can be applied to the whole image to produce global features. Figure 4 presents a way to visualize the categories of features used in signature verification.

Moreover, local features can be classified as contextual and noncontextual. If the signature segmentation is performed in order to interpret the text (e.g., bars of "1" and dots of "0"), the analysis is considered contextual (Chuang, 1977). This type of analysis is not popular for two reasons: (1) it requires a complex segmentation process, and (2) it is not suitable to deal with graphical signatures. On the other hand, if the signature is viewed as a drawing composed by line segments (as it occurs in the majority of the works), the analysis is considered noncontextual.

Before describing some of these features, the many ways to represent a signature image are discussed.

**Representations of a Signature**

Some extraction techniques transform the signature image into another representation before extracting the features. The literature is quite extensive in signature representations.

Box and convex hull representations have been used to represent signatures (Frias-Martinez, Sanchez & Velez, 2006). The box representation is composed of the smallest rectangle fitting the signature. Its perimeter, area, and perimeter/area ratio can be used as features. The convex hull representation is composed of the smallest convex hull fitting the signature. Its area, roundness, compactness, and length and orientation of its maximum axis can be used as features.

The skeleton of the signature, its outline, directional frontiers, and ink distributions also have been used as signature representations (Huang & Yan, 1997). The skeleton (or core) representation is the pixel wide strokes resulting from the application of a thinning algorithm to a signature image. The skeleton can be used to identify the signature edge points (1-neighbor pixels) that mark the beginning and ending of strokes (Ozgunduz, Senturk & Karslioglu, 2005). Further, pseudo-Zernike moments also have been extracted from this kind of representation (Wen-Ming, Shao-Fa & Xian-Gui, 2004).

The outline representation is composed of every black pixel adjacent to at least one white pixel. Directional frontiers (also called shadow images) are obtained when keeping only the black pixels touching a white pixel in a given direction (there are 8 possible directions). To perform ink distribution representations, a virtual grid is posed on the signature image. The cells containing more than 50% of black pixels are completely filled while the others are emptied. Depending on the grid scale, the ink distributions can be coarser or more detailed. The number of filled cells can also be used as a global feature.

Upper and lower envelopes (or profiles) are also found in the literature. The upper envelope is obtained by selecting column-wise the upper pixels of a signature image, while the lower envelope is achieved by selecting the lower pixels. As global features, the number of turns and gaps in these representations have been extracted (Ramesh & Murty, 1999).

Mathematical transforms have been used to represent signature images. Nemcek and Lin (1974) chose the fast Hadamard transform in their feature extraction process as a tradeoff between computational complexity and representation accuracy, when compared to other transforms. Discrete Radon transform is used to extract an observation sequence of the signature, which is used as a feature set (Coetzer et al., 2004). Finally, signature images also can undergo a series of transformations before feature extraction. For example, Tang, Tao, and Lam (2002) used a central projection to reduce the signature image to a 1-D signal that is in turn transformed by a wavelet before fractal features are extracted from its fractal dimension.

**Geometrical Features**

Global geometric features measure the shape of a signature. The height, width (Armand, Blumenstein & Mudhukumarasamy, 2006) and area (or pixel density) (Abdelghani & Amara, 2006) of the signature are basic features pertaining to this category. The height and width can be combined to form the aspect ratio (or caliber) (Oliveira, Justino, Freitas & Sabourin, 2005).

More elaborate geometric features consist of proportion, spacing, and alignment to baseline. Proportion measures the height variations of the signature, while spacing describes the gaps in the signature (Oliveira et al., 2005). Alignment to baseline extracts the general orientation of the signature according to a baseline reference (Abdelghani & Amara, 2006; Armand et al., 2006; Frias-Martinez et al., 2006; Oliveira et al., 2005; Senol & Yildirim, 2005).

Connected components also can be extracted as global features, such as the number of 4-neighbors and 8-neighbors pixels in the signature image (Frias-Martinez et al., 2006).

**Statistical Features**

Many authors use projection representation. It consists of projecting every pixel on a given axis (usually horizontal or vertical), resulting in...
a pixel density distribution. Statistical features, such as the mean (or center of gravity), global, and local maxima, can be extracted from this distribution (Frias-Martinez et al., 2006; Ozgunduz et al., 2005; Senol & Yildirim, 2005).

Moments, which can include central moments (i.e., skewness and kurtosis) (Bajaj & Chaudhury, 1997; Frias-Martinez et al., 2006) and moment invariants (Al-Shoushan, 2006; Lv, Wang, Wang, & Zhao, 2005; Oz, 2005), are also extracted from the pixel distributions.

Moreover, other types of distributions can be extracted from a signature. Sabourin and Drouhard (1992) extracted directional PDF from the gradient intensity representation of the silhouette of a signature. Stroke direction distributions have been extracted using structural elements and morphologic operators (Frias-Martinez et al., 2006; Lv et al., 2005; Madasu, 2006; Ozgunduz et al., 2005). A similar technique is used to extract edge-lingo (strokes changing direction) distributions (Madasu, 2006). Based on an envelope representation of the signature, slope distributions are also extracted in this way (Fierrez-Aguilar, Alonso-Hermira, Moreno-Marguez & Ortega-Garcia, 2004; Lee, Lizarraga, Gomez & Koerich, 1997), whereas Madasu, Hannandulu, and Madasu (2003) extracted distributions of angles with respect to a reference point from a skeleton representation.

**Fixed Zoning**

Fixed zoning defines arbitrary regions and uses them for all signatures. To perform fixed zoning based on the pixels, all the pixels of a signature are sent to the classifier after a normalization of the signature image to a given size. Mateo, Martinez et al., 2006; Mateo, Travieso, Alonso & Ferrer, 2004; Mighell, Wilkinson & Goodman, 1989).

Otherwise, numerous fixed zoned methods are described in the literature. Usually, the signature is divided into strips (vertical or horizontal) or uses a layout like a grid or angular partitioning. Then geometric features (Abdelghani & Amara, 2006; Armand et al., 2006; Ferrer, Alonso, & Travieso, 2005; Huang & Yan, 1997; Justino, Borotolozi, & Sabourin, 2005; Martinez et al., 2004; Ozgunduz et al., 2005; Qi & Hunt, 1994; Santos, Justino, Borotolozi, & Sabourin, 2004; Senol & Yildirim, 2005), wavelet transform features (Abdelghani & Amara, 2006), and statistical features (Fierrez-Aguilar et al., 2004; Frias-Martinez et al., 2006; Hannandulu, Yusof & Madasu, 2005; Justino et al., 2005; Madasu, 2006) can be extracted.

Signal-dependent retinas have been used to describe local regions capturing best the intrapersonal similarities from the reference signatures of individual writers (Ando & Nakajima, 2003). A generic algorithm is used to optimize the location and size of these retinas before similarity features are extracted from the questioned signature and its reference set.

Connectivity analysis has been performed on a signature image to generate local regions before extracting geometric and position features from each region (Igarza, Hernaez, & Goirizzeila, 2005). Even more localized regions (signal-dependent) are achieved using stroke segmentation. Perez-Hernandez, Sanchez, and Velez (2004) achieved stroke segmentation by first finding the direction of each pixel of the skeleton of the
State of the Art in Off-Line Signature Verification

signature and then using a pixel tracking process. Then the orientation and endpoints of the strokes are extracted as features. Another technique is to erode the stroke segments into regions before extracting similarity features (Franke, Zhang & Koppen, 2002) from these elongated regions. Instead of focusing on the strokes, the segmentation can be done in other signature representations. Chen and Srikhari (2006) matched two signature contours using DTW before segmenting and extracting Zernike moments from the segments. Xiao and Leedham (2002) segmented upper and lower envelopes where their orientation changes sharply. After that, they extracted length, orientation, position, and pointers to the left and right neighbors of each segment.

**Pseudo-Dynamic Features**

The lack of dynamic information is a serious constraint for offline signature verification systems. The knowledge of the pen trajectory, along with speed and pressure, gives an edge to online systems. To overcome this difficulty, some approaches use dynamic signature references to develop individual stroke models that can be applied to offline signature verification. For instance, Guo, Doerrmann, and Rosenfeld (2001) used stroke-level models and heuristic methods to locally compare dynamic and static pen positions and stroke directions. Lau, Yuen, and Tang (2005) developed the universal writing model (UWM), which consists of a set of distribution functions constructed using the attributes extracted from online signature samples, whereas Nel, du Preez, and Herbst (2005) used a probabilistic model of the static signatures based on hidden Markov models (HMM). The HMM restricts the choice of possible pen trajectories describing the morphology of the signature. Then the optimal pen trajectory is calculated using a dynamic sample of the signature.

However, without resorting to online examples, it is possible to extract pseudo-dynamic features from static signatures. Pressure features can be extracted from pixel intensity (i.e., grey levels) (Huang & Yan, 1997; Lv et al., 2005; Santos et al., 2004; Wen-Ming et al., 2004) and stroke width (Lv et al., 2005; Oliveira et al., 2005), whereas speed information can be extrapolated from stroke curvature (Justino et al., 2005; Santos et al., 2004), stroke slant (Justino et al., 2005; Oliveira et al., 2005; Senol & Yildirim, 2005) progression (Oliveira et al., 2005; Santos et al., 2004), and form (Oliveira et al., 2005).

**Discussion**

This section presented important feature extraction techniques used to extract global and local information from signatures. The choice of using global or local features will depend mainly on the types of forgeries to be detected by the system. The global features are extracted at a low computational cost, and they have good noise resilience. However, they have less capacity to discriminate between genuine signatures and skilled forgeries. On the other hand, local features are more suitable to identify imitations, despite their dependence on the zoning process.

An issue that has received little attention in literature is the generally low quantity of available signature samples vs. the generally high number of extracted features. This issue may be solved by the following:

1. **Selecting the most discriminating features:** In the work of Xudha, Furuhashi, Obata, and Uchikawa (1996), for example, genetic algorithms were used to select the optimal set of partial curves from an online signature and the best features of each partial curve.
2. **Using regularization techniques to obtain a stable estimation of the covariance matrix** (Fang & Tang, 2005).
3. **Generating synthetic samples:** This can be done by adding noise or applying transformations to the real signatures (Fang et al., 2002; Fang & Tang, 2005; Huang & Yan, 1997; Velez, Sanchez, & Moreno, 2003).

**Using dissimilarity representation:** this technique makes it possible to reduce the number of classes as well as increase the quantity of feature vectors (Santos et al., 2004).

The two last points are discussed in more detail in the section entitled “Dealing with a Limited Amount of Data.”

**VERIFICATION STRATEGIES AND EXPERIMENTAL RESULTS**

This section categorizes some work in offline signature verification according to the technique used to perform verification; that is, distance classifiers, artificial neural networks, hidden Markov models, dynamic time warping, support vector machines, structural techniques, and Bayesian networks.

In signature verification, the verification strategy can also be categorized as writer-independent or writer-dependent (Srikhari et al., 2004). With writer-independent verification, an n-class classifier deals with the whole population of writers. In contrast, with the writer-dependent verification, a one-class or a two-class classifier is employed per writer. As the majority of the work presented in literature is designed to perform writer-dependent verification, this aspect is mentioned only when writer-dependent verification is considered.

The same procedure is taken regarding the type of forgeries used for training, since only random forgeries are generally used in this phase.

Before describing the work, some measures used to evaluate the performance of signature verification systems are presented. The section concludes with a discussion of the main challenges to be faced in this field.

**Performance Evaluation Measures**

In signature verification systems, the simplest way to report their performances is in terms of error rates. The false rejection rate (FRR) is related to genuine signatures that were rejected by the system; that is, classified as forgeries, whereas the false acceptance rate (FAR) is related to forgeries that were misclassified as genuine signatures. FRR and FAR are also known as type 1 and type 2 errors, respectively. Finally, the average error rate (AER) is related to the total error of the system; that is, type 1 and type 2 errors together.

On the other hand, if the decision threshold of a system is set to have the percentage of false rejections approximately equal to the percentage of false acceptances, the equal error rate (EER) is calculated.

**Distance Classifiers**

A simple distance classifier is a statistical technique that usually represents a pattern class with a Gaussian probability density function (PDF). Each PDF is uniquely defined by the mean vector and covariance matrix of the feature vectors belonging to a particular class. When the full covariance matrix is estimated for each class, the classification is based on Mahalanobis distance. On the other hand, when only the mean vector is estimated, classification is based on Euclidean distance (Coetzer, 2005).

Approaches based on distance classifiers are traditionally writer-dependent. The reference samples of a given author are used to compose the class of genuine signatures (w), and a subset of samples from each other writer is chosen randomly to compose the class of forgeries (w). Once the smallest distance between a reference signature and a questioned signature is found, the latter is classified according to the label of the reference signature (w or w'). If the classifier is designed to find a number of k nearest reference
signatures, a voting scheme is used to take the final decision.

Distance classifiers were one of the first classification techniques used in off-line signature verification. One of the earliest reported works was by Nenec and Lin (1974). By using a fast Hadamard transform extraction technique on genuine signatures and simple forgeries, a number of global and local features were extracted considering only the North American signature style. Using weighted distance classifiers, they obtained an FRR ranging from 8% to 12% and an FAR of 0.02%.

Some years later, skilled forgeries have begun to be considered in off-line signature verification. Besides proposing a method to separate the signatures from noisy backgrounds and to extract pseudo-dynamic features from static images, Ammar and colleagues (Ammar, 1991; Ammar, Yoshida, & Uchida, 1996, 1999) were the first to attempt to detect skilled forgeries in an off-line signature verification system. In their work, distance classifiers were used, combined with the leave-one-out, cross-validation method since the number of signatures examples was small. Qiu and Hunt (1994) presented a signature verification system based on global geometric features and local grid-based features. Different types of similarity measures such as Euclidean distance were used to discriminate between genuine signatures and forgeries (increasing simple and skilled). They achieved an FRR ranging from 3% to 11.3%, and an FAR ranging from 0% to 15%.

Sabourin and colleagues (Sabourin & Plamondon, 1986; Sabourin et al., 1993) have done extensive research in off-line signature verification since the mid-1980s. In one of their works (Sabourin et al., 1993), the Extended Shadow Code was used in order to extract local features from genuine signatures and random forgeries. The first experiment used a k-nearest neighbors (k-NN) classifier with voting schema, obtaining an AER of 0.01% when k = 1. The second experiment used a minimum distance classifier, obtaining an AER of 0.77% when the matching signatures were used for each writer. In another relevant work, Sabourin et al. (1997b) used granulometric size distributions as local features, also in order to eliminate random forgeries. By using k-nearest neighbors and threshold classifiers, they obtained an AER around 0.02% and 1.0%, respectively. Fang, Wang, Leung, and Tse (2001) developed a system based on the assumption that the curvature of a signature is generally less smooth than that of genuine signatures. Besides the utilization of global shape features, a crossing and fractal dimension methods were proposed to extract the smoothness features from the signature's segments. Using a simple distance classifier and the leave-one-out, cross-validation method, an FRR of 18.1% and an FAR of 16.4% were obtained. More recently, Fang et al. (2002) extracted a set of peripheral features in order to describe internal and external structures of the signatures. To discriminate between genuine signatures and skilled forgeries, they used a Mahalanobis distance classifier together with the leave-one-out, cross-validation method. The obtained AERs were in the range of 15.6% (without artificially generated samples) and 11.4% (with artificially generated samples).

Artificial Neural Networks

An artificial neural network (ANN) is a massively parallel distributed system composed of processing units capable of storing knowledge learned from experience (examples) and using it to solve complex problems (Haykin, 1998). Multilayer perceptron (MLP) trained with the error back propagation algorithm (Rumelhart, Hinton & William, 1986) has so far the most frequently ANN architecture used in pattern recognition.

Particularly in off-line signature verification, ANNs have been used extensively both in writer-independent and writer-dependent approaches. To perform writer-independent verification, the network is generally trained by using one class per writer. On the other hand, writer-dependent verification is generally performed by using two classes: one for the genuine signatures and another for the forgeries. Migello et al. (1989) were the first ones to apply ANNs for off-line signature verification. In order to eliminate simple forgeries, they used the raw images as input to an MLP. In the experiments, by using a training set composed by genuine signatures and forgeries, they achieved an EER of 2%. Sabourin and Drouhard (1992) used directional PDFs as global feature vectors and MLP as classifiers in order to eliminate random forgeries. Since their database was composed of few data, some signature samples were generated by rotating the directional PDFs. In the experiments, they obtained an FRR of 1.75% and an FAR of 9.0%.

Cardot, Revu, Victorri, and Revillet (1994) used outline and geometric measures of the signature images to compose two types of feature vectors. The most important contribution of their work was the proposal of a multilevel neural network architecture to eliminate random forgeries. The first level is composed of two Kohonen maps (one for each of features) in order to perform an initial classification and to choose the random forgeries to train the second level networks. As the number of writers was very large (more than 300), they had to limit the number of classes to fewer than 50. In the second level, two MLPs for each writer are used to perform writer-dependent verification. Finally, in the last level, an MLP accepts or rejects the signature. By using a dataset of signatures extracted from real postal checks, they achieved an FRR of 4% and an FAR of 2%.

Mursheed, et al. (1995) proposed a verification strategy based on fuzzy ARTMAPs in the context of random forgeries. Different from other neural networks types, the fuzzy ARTMAPs allow training by using examples of only one class. Therefore, in this approach, the genuine signatures are used for training and the random forgeries (as well as some unseen genuine signatures samples) for testing. In order to simulate different experts examining different regions of the signature, the image is divided in a number of overlapping squares according to the writer signature shape. After that, each signature region is reduced by applying an MLP network, and verified by a specialized fuzzy ARTMAP. Finally, based on the results given by each fuzzy ARTMAP, the final decision is taken. In the experiments, they obtained an AER of 9.14%.

Bajaj and Chaudhury (1997) used an ensemble of MLPs to perform writer-independent verification. In order to discriminate between genuine signatures and random forgeries, one MLP per feature vector (moments, upper envelope, and lower envelope) was trained. Moreover, each MLP was composed of 10 outputs (one for each writer). In the verification phase, the output of the three classifiers was combined to obtain a final decision. In the experiments, a substantial reduction of the error rate was obtained when using the three classifiers together (FRR=5%; FAR=3%).

Fadhel and Bhattacharya (1999) proposed a signature verification system based on Steerable Wavelet as feature extraction technique and MLP as classifier. In the first experiment, by selecting only the first two of the 16 coefficients, which represent each signature image, they obtained a classification rate of 85.4%, whereas in a second experiment, by using all 16 coefficients, the classification rate was improved to 93.8%.

Sansone and Vento (2000) proposed a three-stage, multi-expert system in order to deal with all types of forgeries. The first stage was designed to eliminate random and simple forgeries by using only the signature's outline as a feature. The
second stage receives the signatures accepted by the previous stage, which can be classified as genuine or as skilled forgery. The features used in this stage are the high-pressure regions. Finally, a third stage takes the final decision. Using MLP as classifiers, they obtained an FRR of 2.04% and FARs of 0.01%, 4.29%, and 19.80% with respect to random, simple, and skilled forgeries, respectively.

Blatzakis and Papamarkos (2001) used global geometric features, grid features, and texture features to represent the signatures. They proposed a two-stage system in order to eliminate random forgeries. In the first stage, three MLPs (one for each feature set) and the Euclidean distance metric perform a coarse classification. After that, an RBF (radial basis function) neural network, trained with samples that were not used in the first stage, takes the final decision. An FRR of 3% and an FAR of 9.8% were obtained in the experiments.

Quek and Zhou (2002) proposed a system based on fuzzy neural networks in order to eliminate skilled forgeries. To represent the signatures, they used reference pattern-based features, global baseline features, pressure features, and slant features. In the first set of experiments, using both genuine signatures and skilled forgeries to train the network, an average AER of 22.4% was obtained. Comparable results were obtained in the second set of experiments, in which only genuine signatures were used as training data.

Vélez, et al. (2003) performed signature verification by comparing subimages or positional cuttings of a test signature to the representations stored in compression neural networks. In this approach, neither image preprocessing nor feature extraction is performed. By using one signature per writer, together with a set of artificially generated samples, they obtained a classification rate of 97.8%.

In a recent work, Armand, et al. (2006) proposed the combination of the modified direction feature (MDF), extracted from the signature’s contour, with a set of geometric features. In the experiments, they compared RBF and resilient backpropagation (RBP) neural network performances. Both networks performed writer-independent verification and contained 40 classes—39 corresponding to each writer and one corresponding to the forgeries. In this case, skilled forgeries were used in the training phase. The best classification rates obtained were 91.21% and 88.0%, using RBF and RBP, respectively.

Hidden Markov Models

Hidden Markov models (Rubinov, 1989) are finite stochastic automata used to model sequences of observations. Although this technique is more suitable to model dynamic data (e.g., as speech and online signatures), it has also been applied in segmented off-line signatures. Generally, HMMs are used to perform writer-dependent verification by modeling only the genuine signatures of a writer. In this case, the forgeries are detected by thresholding.

Rigoll and Kosmala (1998) presented a comparison between online and off-line signature verification using discrete HMMs. To represent the signatures in the online model, they used both static and pseudo-dynamic features. In the first set of experiments, in which each feature was investigated separately, surprising results were obtained. The bitmap feature was the most important one, achieving a classification rate of 92.2%. The Fourier feature also supplied a high classification rate. Finally, another surprise was the low importance of the acceleration. As expected, good results were obtained using the velocity feature. Other experiments using several features together were performed in order to obtain high classification rates. The best result (99%) was obtained when only four features (bitmap, velocity, pressure, and Fourier feature) were combined.

To represent the signatures in the off-line model, they subdivided the signature image into several squares of 10x10 pixels. After that, the grey value of each square was computed and used as a feature. In the experiments, a classification rate of 98.1% was achieved. The small difference between the online and off-line classification rates is an important practical result, since off-line verification is simpler to implement.

El-Yacoubi, Justino, Sabourin, and Bortolozzi (2000) proposed an approach based on HMM and pixel density features in order to eliminate random forgeries. To perform training while choosing the optimal HMMs’ parameters, the Baum-Welch algorithm and the cross-validation method were used. In the experiments, each signature was analyzed under three resolutions (100x100, 40x40, and 16x16 pixels) by applying the Forward algorithm. Finally, a majority-vote rule took the final decision. An AER of 0.46% was obtained when both genuine and impostor spaces were modeled, and AER of 0.91% was obtained when only the genuine signatures were modeled.

Justino, Bortolozzi, and Sabourin (2001) used HMMs to detect random, simple, and skilled forgeries. Also using a grid-segmentation scheme, three features were extracted from the signatures: pixel density feature, Extended Shadow Code, and axial slant feature. They applied the cross-validation method in order to define the number of states for each HMM writer model. Using the Bakis model topology and the forward algorithm, they obtained an FRR of 2.83% and FARs of 1.44%, 2.50%, and 22.67% for random, simple, and skilled forgeries, respectively.

Coetzee, et al. (2004) used HMMs and discrete random transforms to detect simple and skilled forgeries. In this work, some strategies were proposed in order to obtain noise, shift, rotation, and scale invariances. By using a left-to-right ring model and the Viterbi algorithm, EERs of 4.5% and 18% were achieved for simple and skilled forgeries, respectively.

Dynamic Time Warping

Widely applied in speech recognition, dynamic time warping (DTW) is a template matching technique used for measuring similarity between two sequences of observations. The primary objective of DTW is to nonlinearly align the sequences before they are compared (matched) (Coetzee, 2005). Despite being more suitable to model data that may vary in time or speed, dynamic time warping has been used in off-line signature verification. As usually occurs in HMM-based approaches, a test signature is compared to the genuine ones of a writer (writer-dependent verification), and a forgery is detected by thresholding.

Wilkinson and Goodman (1990) used DTW to discriminate between genuine signatures and simple forgeries. Assuming that curvature, total length, and slant angle are constant among different signatures of a same writer, they used a slope histogram to represent each sample. In the experiments, they obtained an EER of 7%. Increases in the error rates were observed when the forgers had some prior knowledge about the signatures.

Deng, Liao, Ho, and Yuan (1999) proposed a Wavelet-based approach to eliminate simple and skilled forgeries. After applying a closed-contour tracing algorithm to the signatures, the curvature data obtained were decomposed into multiresolutional signals using wavelets. Then, DTW was used to match the corresponding zero-crossings. Experiments were performed using English and Chinese signature datasets. For the English dataset, an FRR of 5.6% and FARs of 21.2% (skilled forgeries) and 0% (simple forgeries) were obtained, whereas using the Chinese dataset, an FRR of 6.0% and FARs of 13.5% (skilled forgeries) and 0% (simple forgeries) were achieved.

Fang, et al. (2003) proposed a method based on DTW and one-dimensional projection profiles in order to deal with intraperssonal signature variations. To achieve discrimination between genuine signatures and skilled forgeries, nonlinear DTW was used in a different way. Instead of using the distance between a test signature and a reference sample to take a decision, the positional distortion at each point of the projection profile was
incorporated into a distance measure. Using the leave-one-out, cross-validation method and the Mahalanobis distance, they obtained AERs of 20.8% and 18.1%, when binary and grey level signatures were considered, respectively.

Support Vector Machines
Support vector machines (SVMs) (Vapnik, 1999) is a kernel-based learning technique that has shown successful results in applications of various domains (e.g., pattern recognition, regression estimation, density estimation, novelty detection, etc.).

Signature verification systems that use SVMs as classifiers are designed in a similar way to those that use neural networks. That is, in a writer-dependent approach, there is one class for the genuine signatures and another class for forgeries. In addition, by using one-class SVMs (Scholkopf, Platt, Taylor, Smola & Williamson, 2001), it is possible to perform training by using only genuine signatures. In the work of Srichari, et al. (2004), the authors tried to use it in the context of skilled forgeries. However, by using the traditional two-class approach, the AER decreased from 46.0% to 9.3%.

Martinez, et al. (2004) used SVM with RBF kernel in order to detect skilled forgeries. In the experiments, different types of geometrical features as well as raw signatures were tested. The best result—an FAR of 18.85%—was obtained when raw images with a scale of 0.4 were used. Justino, et al. (2005) performed a comparison between SVM and HMM classifiers in the detection of random, simple, and skilled forgeries. By using a grid-segmentation scheme, they extracted a set of static and pseudo-dynamic features. Under different experimental conditions (i.e., varying the size of the training set and the types of forgeries), the SVM with a linear kernel performed better than the HMM.

Ozgunduz, et al. (2005) used support vector machines in order to detect random and skilled forgeries. To represent the signatures, they extracted global geometric features, direction features, and grid features. In the experiments, a comparison between SVM and ANN was performed. Using an SVM with RBF kernel, an FRR of 0.02% and an FAR of 0.11% were obtained, whereas the ANN, trained with the backpropagation algorithm, provided an FRR of 0.22% and an FAR of 0.16. In both experiments, skilled forgeries were used to train the classifier.

Structural Techniques
In structural techniques, the patterns are organized hierarchically in a way that each level, they are viewed as being composed of simpler subpatterns. By using a small number of primitives (the most elementary subpatterns) and grammatical rules, it is possible to describe a large collection of complex patterns (Coetzer, 2005). Therefore, it is possible to interpret the scene both globally and locally.

Sabourin, Plamondon, and Beaumier (1994) were the first ones to propose a structural representation of handwritten signatures images. In their approach, a segmentation process breaks up the signature into a set of primitives. From these shape primitives, both static and pseudo-dynamic features are extracted. The comparison process is composed of two stages: Local interpretation of primitives (LIP) and global interpretation of the scene (GIS). In the LIP stage, a template match process is performed in which each primitive of the test signature image is labeled, taking into account the reference set. Finally, the GIS stage takes the final decision by computing a similarity measure between the test primitive set and the reference primitive set. The experiments were performed in order to eliminate random forgeries. By using a minimum distance classifier with two reference signatures, they obtained an AER of 1.43%.

Bastos, Bortolozzi, Sabourin, and Kaestner (1997) proposed a mathematical signature representation in terms of ellipses, parabolas, and hyperbolae. The goal of this approach is to allow a simplification of the signature tracing when detecting random forgeries. After performing a thinning process, junction and endpoints are found in the signatures. Next, an algorithm is applied in each part of the signature tracing (between an endpoint and a junction point) in order to obtain all necessary points for modeling a mathematical equation. Finally, the least square method of curve adjusting is applied to each set of tracing points, resulting in a number of equations of ellipses, parabola, and hyperbolae. Performing superpositions between the found equations and the respective signatures, they obtained similarity indices ranging from 86.3% and 97.3% with respect to different writers.

Huang and Yan (2002) proposed a two-stage signature verification system based on ANN and a structural approach. To represent the signatures, they used geometric and directional frontier features. In the first stage of the system, a neural network attributes to the signature three possible labels: pass (genuine signature), fail (random or less skilled forgery), and questionable (skilled forgery). For the questionable signatures, the second stage uses a structural feature verification algorithm to compare the detailed structural correlation between the test signature and the reference samples. In the experiments, the first classifier rejected 2.2% of the genuine signatures, accepted 3.6% of the forgeries, and was undecided on 32.7% of the signatures. The second classifier rejected 32.1% of the questionable genuine signatures and accepted 23.2% of the questionable forgeries. Therefore, for the combined classifier, an FRR of 6.3% and an FAR of 8.2% were obtained.

Discussion
This section presents some verification strategies proposed in the field of off-line signature verification. Even though the error rates are reported, it is very difficult to compare the performances of different verification strategies, since each work uses different feature extraction techniques, experimentation protocols, and signature databases (see Tables 1 and 2). Despite the great recognition rates obtained by using classifiers, which learn from examples (e.g., ANNs, HMMs, and SVMs), there are some difficulties to be faced. The first one is the large number of examples required to ensure that the classifier will, in fact, learn (Lecerf & Plamondon, 1994). On the other hand, classifiers that do not require many reference samples, since there is no explicit training phase (e.g., distance classifiers), have a low generalization capability.

Another difficulty, which occurs mainly with ANNs and SVMs, is the necessity of using forgeries in the training phase in order to allow class separation by the classifier. However, the authors have already been dealing with this problem by using one-class classifiers (Mursched et al., 1995; Srichari et al., 2004), computer-generated forgeries (Miguel et al., 1989), and a subset of genuine signatures from other writers (random forgeries).

The utilization of multiple classifiers has improved the recognition performance in difficult classification problems. Using just one optimal classifier, it is possible to lose valuable information contained in the other suboptimal classifiers. It has been shown that when a set of R classifiers is averaged, the variance contribution in the bias-variance decomposition decreases by 1/R, resulting in a smaller expected error (Tax, 2001).

In a multistage approach, each classification level receives the results of the previous one, reducing the complexity of the problem (Blatzies & Papamarkos, 2001; Huang & Yan, 2002;Sansone & Vento, 2000). Particularly in signature verification, the complexity can be reduced even further if the system combines both writer-independent verification (to eliminate random and simple forgeries) and writer-dependent verification (to eliminate the skilled forgeries). However, few systems (Cardot et al., 1994) use this strategy to improve their performances.

Moreover, ensemble of classifiers has been less explored in this field (Bajaj & Chaudhary, 2005).
Finally, one aspect that has not been discussed in the signature verification literature is the use of incremental learning. As a signature varies according to psychological and physical state, it is very difficult to get all possible variations during the training phase. Besides, the signature may change over time. Thus, updating the classifier as new examples are available may be useful in real signature verification systems.

DEALING WITH A LIMITED AMOUNT OF DATA

Mainly for practical reasons, a limited number of signatures by writers is available to train a classifier for signature verification. However, by using a small training set, the class statistics estimation errors may be significant, resulting in unsatisfactory verification performance (Fang & Tang, 2005).

Huang and Yan (1997) applied small transformations to the genuine signatures in order to generate additional training samples, and heavy transformations, also to the genuine signatures, in order to generate forgeries. In the two cases, the transformations were slant distortions, scalings in horizontal and vertical directions, rotations, and perspective view distortions; whereas Vélez et al. (2003) tried to reproduce intrapersonal variability by using only one signature per writer. To generate additional training samples, they applied rotations (in the range of ±35°), scalings (in the range of ±20%), horizontal and vertical displacements (in the range of ±20%), and various types of noise for each original signature.

By using a different approach, Fang and Tang (2005) proposed the generation of additional samples in the following way:

1. Two samples are selected from the set of genuine signatures.
2. Then anelastic matching algorithm is applied to the pair of signatures in order to estab-

Table 1. Signature verification databases (I = Individual; G = Genuine; F = forgeries; S = Samples)

<table>
<thead>
<tr>
<th>References</th>
<th>Images</th>
<th>Signatures</th>
<th>Forgeries Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Netney &amp; Lin, 1974)</td>
<td>128x256 pixels binary</td>
<td>600G / 151 120F / 46</td>
<td>Simple</td>
</tr>
<tr>
<td>(Nagel &amp; Rosseifeld, 1977)</td>
<td>500 dpi 64 grey levels</td>
<td>110 / 21 14F / 21</td>
<td>Simple</td>
</tr>
<tr>
<td>(Ammar et al., 1982)</td>
<td>256x1024 pixels 256 grey levels</td>
<td>200G / 101 20F / 101</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Qi &amp; Huan, 1994)</td>
<td>300 dpi 256 grey levels</td>
<td>300F / 151 15F / 101</td>
<td>Simple and Skilled</td>
</tr>
<tr>
<td>(Subourin et al., 1993) (Subourin et al., 1993b) (Subourin et al., 1992) (Subourin et al., 1994)</td>
<td>128x512 pixels 256 grey levels</td>
<td>800G / 201</td>
<td>Random</td>
</tr>
<tr>
<td>(Fang et al., 2002) (Fang et al., 2003)</td>
<td>300 dpi 256 grey levels</td>
<td>1320G / 551 1220F / 121</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Michell et al., 1989)</td>
<td>128x64 pixels binary</td>
<td>80G / 11 6F / 6F</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Cardon et al., 1994)</td>
<td>1024x512 pixels 256 grey levels</td>
<td>6000G / 900</td>
<td>Random</td>
</tr>
<tr>
<td>(Munsh et al., 1995)</td>
<td>128x512 pixels 256 grey levels</td>
<td>200G / 51</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Bajaj &amp; Chaudhury, 1997)</td>
<td>200 dpi binary</td>
<td>150G / 101</td>
<td>Random</td>
</tr>
<tr>
<td>(Fidwel &amp; Bhattacharya, 1999)</td>
<td>340 dpi 256 grey levels</td>
<td>306S / 301</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Serrone &amp; Venti, 2000)</td>
<td>300 dpi 256 grey levels</td>
<td>980G / 491 980F / 491</td>
<td>Simple and Skilled</td>
</tr>
</tbody>
</table>

Table 2. Signature verification databases (continuation) (I = Individual; G = Genuine; F = forgeries; S = Samples)

<table>
<thead>
<tr>
<th>References</th>
<th>Images</th>
<th>Signatures</th>
<th>Forgeries Types</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Blumak &amp; Papamarkos, 2001)</td>
<td>binary</td>
<td>2000G / 1111</td>
<td>Random</td>
</tr>
<tr>
<td>(Quck &amp; Zhou, 2002)</td>
<td>316x184 pixels 256 grey levels</td>
<td>555G / 250 15-200 F x S</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Vélez et al., 2003)</td>
<td>350 dpi 256 grey levels</td>
<td>125G / 125</td>
<td>not specified</td>
</tr>
<tr>
<td>(Armand et al., 2006)</td>
<td>not specified</td>
<td>306G / 301</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Bajaj &amp; Chaudhury, 1997)</td>
<td>300 dpi binary</td>
<td>300G / 141 66F</td>
<td>Simple and Skilled</td>
</tr>
<tr>
<td>(El-Yacoubi et al., 2000)</td>
<td>300 dpi binary</td>
<td>400G / 101</td>
<td>Random</td>
</tr>
<tr>
<td>(Jasino et al., 2004)</td>
<td>300 dpi 256 grey levels</td>
<td>400G / 100 1220F / 10</td>
<td>Simple and Skilled</td>
</tr>
<tr>
<td>(Coster, 2005)</td>
<td>300 dpi binary</td>
<td>600G / 221 264F / 49</td>
<td>Simple and Skilled</td>
</tr>
<tr>
<td>(Ding et al., 1999)</td>
<td>600 dpi 256 grey levels</td>
<td>100G / 501 250G / 50</td>
<td>Simple and Skilled</td>
</tr>
<tr>
<td>(Srinithi et al., 2004)</td>
<td>300 dpi 256 grey levels</td>
<td>1320G / 551</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Martinez et al., 2004)</td>
<td>not specified</td>
<td>384G / 160 68G / 160</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Ogundipe et al., 2003)</td>
<td>256 grey levels</td>
<td>1320F / 701</td>
<td>Skilled</td>
</tr>
<tr>
<td>(Bustos et al., 1997)</td>
<td>not specified</td>
<td>120G / 64</td>
<td>Random</td>
</tr>
<tr>
<td>(Huang &amp; Yan, 2002)</td>
<td>150 dpi 256 grey levels</td>
<td>1272G / 531 763G / 531</td>
<td>Skilled</td>
</tr>
</tbody>
</table>
lish correspondences between individual strokes.
3. Next, corresponding stroke segments are linked up by displacement vectors.
4. Finally, these displacement vectors are used to perform an interpolation between the two signatures, thus to produce a new training sample.

Based on the dissimilarity representation approach (Bicego, Murino, & Figueiredo, 2004; Cha, 2001; Pekalska & Duin, 2000) in which an object is described by its distances with respect to a predetermined set of prototypes, Santos, et al. (2004) solved the problem of having a limited number of samples to perform signature verification. Instead of using one class per writer to train a global classifier, only two classes are used: genuine and forgery. After the usual feature extraction phase, new feature vectors are generated in the following way:

1. Compute the Euclidean distance vector between each pair of signatures.
2. If the pair of signatures belongs to the same writer, set the feature vector to 1; otherwise, set the feature vector to 0.
3. Finally, train the classifier by using these vectors.

In the verification phase, the distance vectors are computed between the input signature and the reference vectors of its probable class and sent as input to the classifier. The final decision is taken by combining all classifier outputs in voting schema.

Similar signature verification approaches have also been developed by Srihari and colleagues (Kalera et al., 2004; Srihari et al., 2004).

CONCLUSION

This chapter presented a survey of techniques developed in the field of off-line signature verifica-
tion over the last 20 years. As we could observe, despite the vast amount of work performed in order to solve this problem, there are still many challenges to be faced due to the investigation of the trade-off between the quantity of available training samples and the number of extracted features to proposals of powerful verification strategies to deal with all the types of forgeries and dynamic environments. Moreover, for security reasons, it is not easy to make a signature dataset available in the signature verification community, mainly if the signatures come from a real situation (e.g., banking documents). However, the availability of datasets could make it possible to define a common experimentation protocol in order to perform comparative studies in this field.

Dissimilarity representation is an interesting approach because although it copes with the problem of having a reduced training set, it also solves the problem of having many classes in a writer-independent verification. Thus, the combination of this approach with SVM (to perform writer-independent verification) and with HMM (to perform writer-dependent verification) may be an interesting choice of a multistage system. Moreover, the utilization of SVMs facilitates the implementation of a reject mechanism based on ROC (receiver operating characteristic) curves (Fawcett, 2006; Tortorella, 2005).

Finally, regarding feature extraction techniques, the ESC (Sabourin et al., 1993) appears to be a good trade-off between global and local features since it permits the projection of the handwriting at several resolutions.

REFERENCES


ENDNOTE

In real situations (e.g., banking transactions), a client is asked to supply from three to five signature samples at the time of subscription.

Chapter IV

An Automatic Off-Line Signature Verification and Forgery Detection System

Vamsi Krishna Madasu
Queensland University of Technology, Australia

Brian C. Lovell
NICTA Limited (Queensland Laboratory), and University of Queensland, Australia

ABSTRACT

This chapter presents an off-line signature verification and forgery detection system based on fuzzy modeling. The various handwritten signature characteristics and features are first studied and encapsulated to devise a robust verification system. The verification of genuine signatures and detection of forgeries is achieved via angle features extracted using a grid method. The derived features are fuzzified by an exponential membership function, which is modified to include two structural parameters. The structural parameters are devised to account of possible variations due to handwriting styles and to reflect other factors affecting the scripting of a signature. The efficacy of the proposed system is tested on a large database of signatures comprising more than 1,200 signature images obtained from 40 volunteers.

INTRODUCTION

A handwritten signature can be defined as the scripted name or legal mark of an individual, executed by hand for the purpose of authenticating writing in a permanent form. The acts of signing with a writing or marking instrument such as a pen or stylus is sealed on the paper. The scripted name or legal mark, while conventionally applied on paper, may also be accomplished using other devices that capture the signature process in digital format.

Hilton (1992) discusses what a signature is and how it is produced. He notes that the signature...