Off-line Signature Verification Based on Forensic Questioned Document Examination Approach

Cesar R. Santos, Flávio Bortolozzi, Luiz S. Oliveira, Edson Justino

Pontifical Catholic University of Parana
Rua Imaculada Conceição, 1155 – Curitiba PR, Brazil – 80215910
{cesar, fborto, soares, justino @ ppgia.pucpr.br}

ABSTRACT

There are different methods for signature verification proposed in the literature. Most of them, take into account a personal model, i.e., they need a considerable number of genuine signatures of the same writer to correctly train the model. This is the main drawback of this kind of approach, since in real applications we have small number of samples available for training. In this paper we propose an off-line signature verification method based on Forensic Questioned Document Examination approach. This kind of strategy reduces any classification problem to a 2-class problem, hence, makes it possible to build robust signature verification systems even when few signatures per writer are available. Comprehensive results on a database composed of 240 writers (40 samples per writer) demonstrate the efficiency of the proposed method.

1. INTRODUCTION

In the last few decades many methods have been developed in pattern recognition area, regarding the off-line signature verification problem. Approaches based on personal model are extensively used. However, in a real application, we have a limited number of samples available to produce the pattern models (4 to 6 samples in general). The personal approach is based on two different pattern classes, W_1 and W_2. W_1 represents the genuine signature set, for a specific writer while W_2 represents the forgery signatures set. The W_2 set is divided into other three different subsets (random, simple, and simulated forgeries) [2].

The main purpose of the training phase is to obtain a robust personal model M. The main drawbacks of this kind of approach are the need of learning the model each time a new writer should be included in the system and the great number of genuine signatures necessary to build a reliable model.

In this paper we propose an off-line signature verification method based on Forensic Questioned Document Examination approach. This kind of strategy uses a global model, which reduces the pattern recognition problem to a 2-class problem, hence, makes it possible to build robust signature verification systems even when few signatures per writer are available. To implement this global model, we have used the concept of dissimilarity [3] to build the feature vectors. Comprehensive results on a database composed of 240 writers (40 samples per writer) and Support Vector Machines demonstrate the efficiency of the proposed method.

SAC'07, March 11-15, 2007, Seoul, Korea.

2. FORENSIC APPROACH

The Forensic Questioned Document Examination approach classify a handwriting sample, in terms of authenticity, into genuine and not genuine [2], which means that any pattern recognition problem can be reduced to a 2-class problem. In the case of signature verification, the experts use a set of n genuine signature samples Sk_i (i=1,2,3,…,n) as references and then compare Sk with a questioned sample Sq. The idea is to verify the discrepancies among Sk and Sq. For this purpose, a set of F graphometric features is extracted from both Sk and Sq for further comparison. Let V_{ij}, (i=1,2,...,n) and (j=1,2,…,F) be the set of graphometric features extracted from the genuine signatures and Q_j (j=1,2,…,F) the set of graphometric features extracted from the questioned signatures. After feature extraction, the differences among features are computed and the experts provide a partial decision R_i (i=1,2,3,…,n). The final decision D depends on the sum of the partial decisions, obtained through these comparisons. Very often, majority vote rule is used to support the final decision.

3. DATABASE

The signature database is composed of 240 writers (40 samples per writer) and it has been divided into training and testing databases. The training set contains 180 writers with 4 genuine and one random forgery per writer. Computing the distance feature vector among the 4 genuine samples of each author gives us 1080 positive samples. The negative samples are found by computing the distance feature vector among the random forgery of each author with the 4 genuine samples of the 180 writes, which gives us 720 negative samples. These 1800 samples make then our training set, which is used during the SVM learning.

The testing set is composed of the remaining 60 writers with 20 samples per writers. These 20 samples contain 5 genuine signatures, 5 random forgeries, 5 simple forgeries, and 5 simulated forgeries. This approach must consider a reference set, which we have defined as Sk. In our experiments, Sk is composed of 5 genuine samples per writer.

4. SIGNATURE VERIFICATION METHOD

The proposed method works as follows. First the image is segmented using a grid and then the graphometric features are extracted from each cell to form the feature vector. This process is applied to the questioned (*Sq*) and reference (*Sk.*) images as well. This produces the aforementioned graphometric feature vectors V_{ij} e Q_j. Once those vectors are generated, the next step consists in computing the distance feature vector $R_i = (V_{ij} - Q_j)$, which will feed the classifier. Finally, the final decision is taken based on the majority vote rule. Since we have 5 reference images, the questioned image *Sq* will be compared 5 times, yielding 5 votes. The following subsections present details of each module of the proposed system.

4.1 Segmentation

In order to segment the image of signature, we have used a grid-segmentation. A set of different grid resolutions was tried in the experiments, but a grid with square cells of medium resolution (50x50 pixels), showed better results

4.2 Graphometric Features

As discussed before, after segmentation, the next step consists in extracting the graphometric features, which will be used to compute the distance feature vector. Four different subsets of features have been considered in this work: Density of Pixels, Proportion of Pixels, Progression, and Slant. For more details, please refer to [1].

4.3 Distance Features

The distance features used here are based on the concept of dissimilarity [3]. The idea behind this is that similar signatures will have small distances, which is equivalent to large similarity (or small dissimilarity). Once the four graphometric features sets have been extracted ($F = 4$), the Euclidean distances among then are calculated, producing the distance features vector (Equation 1).

$$R_i = \bigcup_{j=1}^{F} \sqrt{(V_i^j - Q^j)^2}, i = (1,2,...,n) \quad (1)$$

Considering that each graphometric feature vector has 160 components (8 × 20 cells), the distance feature vector R_i has 160 × 4 components.

4.4 Comparison and Decision

The comparison stage introduced in Section 2 is computationally implemented by means of a SVM. In the training stage, the feature distances R_i are computed using a pair of signatures samples. If the signatures belong to the same writer, the distance feature vector is set to +1 (authorship), otherwise it is set to -1 (no authorship). The SVM is then trained to discriminate small feature distances (similar signatures) from large feature distances (dissimilar signatures). In the verification stage, the SVM will assign a given distance feature vector to one of the two mentioned classes. After the questioned image has been compared with all references images through the SVM, the decision is taking based on the majority vote rule, i.e, if the majority of the votes are given to the authorship class, then the system decides that the questioned signatures *Sq* are similar to the reference set *Sk*, otherwise, it decides that they are dissimilar.

5. EXPERIMENTAL RESULTS

The experiments were conducted using the svmLight library . The training set used during these experiments contains 1800 samples. In order to estimate the parameters of the SVM kernels (*C* and *d*), we have used a grid search and k-fold cross validation. Table 1 shows the results obtained using the linear and polynomial kernels. Both linear and polynomial kernels achieve about the same overall results. However, we have observed that the model generated by the linear kernel absorbs better the intra-personal variability. On the other hand, it seems that it is also susceptive to accept different forgery types.

Table 1. Comparative results

Kernel	False	False Acceptance (%)			Total
	Reject. (%)	Random	Simple	Simul.	Error
Linear	10.67	3.73	0.33	20.07	8.70
Polyn.	11.33	3.39	0.00	16.72	7.86

The model build with the polynomial kernel detects more Type II Errors (False Acceptance), but consequently increases the false rejection (Type I Error). This phenomenon occurs because the polynomial kernel produces a model more adapted to non-separable signature classes. In practice, frauds in banking industry are related in about 95% of the time with simple forgeries. In light of this, the results achieved by the proposed system are very interesting.

6. CONCLUSIONS

In this paper we demonstrate that even using few samples per writer to build train the machine learning model, it is possible to achieve very low error rates for simple forgeries. One advantage of this approach lies in the fact that it allows the inclusion of new writers in the system without the necessity of retraining the model. The proposed methodology compares favorably regarding the error rates for simples and simulated forgeries, but there is a lot of room for improvement for false rejection.

7. ACKNOWLEDGMENTS

This research has been support by The National Council for Scientific and Technological Development (CNPq), grant 475645/2004-9

8. REFERENCES

[1] Oliveira L. S., Justino, E., Freitas, C., and Sabourin, R. *The Graphology Applied to Signature Verification*, 12th Conference of the International Graphonomics Society (IGS 2005), pages 286-290, 2005.

[2] Justino, E., Bortolozzi, F., Sabourin R., *An Off-line Signature Verification Method Based on SVM Classifier and Graphometric Features*, 5th ICAPR, 2003,

[3] Pekalska E., Duin R. P. W., *Dissimilarity representations allow for building good classifiers*. Pattern Recognition, 23:943-956, 2002