CHAPTER 9
EMERGING ISSUES FOR STATIC HANDWRITTEN SIGNATURE BIOMETRICS

Moises Diaz-Cabrera, Aythami Morales, Miguel A. Ferrer

IDetIC. University of Las Palmas de Gran Canaria Campus de Tafira s/n, E35017, Las Palmas de Gran Canaria, Spain
E-mail: mdiaz@idetic.eu, amorales@gi.ulpgc.es, mferrer@dsc.ulpgc.es

This paper presents a review of the most recent advances in static/off-line signature recognition using Computer Vision and also identifies some new trends and research opportunities such as the generation of synthetic signatures, time drifting, forger and disguise identification and multilingual scenarios. We conclude that the increasing collaboration between the Pattern Recognition community and Forensic Handwriting Experts will lead to future static handwriting signature milestones.

1. Introduction

Signing is a well-accepted method to authenticate the identity of people and has been carried out for centuries. Law enforcement agencies, governments, financial institutions or forensic units use the signature as identity proof in their daily activities. Traditionally, signature analysis is frequently performed by experienced Forensic Handwriting Experts (FHE). They search for individual characteristics of the owner using common protocols and methods. This analysis is a time consuming task and depends on many factors such as the expert background, available data, and sample quality, among others.

Interest in the development of automatic signature recognition methods from the pattern recognition community began few decades ago. The aim of these systems is to provide a quantitative similarity measure
of signatures using an efficient and accurate automatic process. The state-of-the-art of automatic signature recognition is still distant from the results provided by skilled forensics in terms of performance. In fact, there is a large gap between the demands of FHE and the solutions provided by the Pattern Recognition community (PRc). An explanation for this difference is because most of the contributions made by PRc have focused on finding novel methods which outperform previous proposals in terms of quantitative measures, thereby leaving forensic requirements aside.

Several reviews have been published on automatic signature verification, e.g. Plamondon and Shirahi in 2000\textsuperscript{1} and Impedovo and Pirlo in 2008.\textsuperscript{2} This paper surveys some of the recent advances in automatic signature recognition since then, and identifies emerging trends and new challenges. These areas include: novel feature approaches, available public databases, international competitions, synthetic generation of samples, aging and its influence on signature processing, forger identification, disguised signature detection, and multilingual signature processing, among others.

This chapter is organized as follows: Section 2 surveys the last five years in static signature recognition; Section 3 focuses on the latest performance evaluation developments; Section 4 gathers some current trends and challenges while the conclusions of this paper are discussed in Section 5.

2. State of the Art: Automatic Signature Recognition

Most recent automatic signature recognition developments carried out by PRc are divided among the three main steps of the classical pattern recognition diagram: 1) Signature Preprocessing, 2) Signature Template and 3) Classification.

2.1. Signature pre-processing

Signature preprocessing in operative schemes involves signature detection, segmentation and enhancement. Unfortunately, these problems have attracted the attention of only a few researchers. Regarding
signature preprocessing, there are three general stages which directly affect the performance of an automatic verification system: find a signature in a document, locate it precisely and extract an accurate image of the signature strokes. Some work has been done in this subject with the Tobacco800 database.

The sheet used for the signature and its influence is another aspect that has scarcely been taken into account in the literature. Paper texture sometimes hinders the extraction of the inked signature, especially when verifying the signature authorship of ancient manuscripts. Ink type should also be taken into account for the segmentation process: A solid ink is usually more distinguishable than viscous or liquid ink.

Additional segmentation challenges arise when the signature image is blended with text or with official stamps commonly found in government forms, bank checks or thin sheets written on both sides. Some proposals to alleviate this problem have been put forth by Douglas and Peucker using a polygonal approximation algorithm and skeleton junction points to remove the text part on the signature in. Other authors take advantage of nonlinear statics methods. A post processing to smooth the signature strokes has also been proposed, especially when proposed texture features are more sensitive to spurious pixels in the stroke.

2.2. Feature extraction

Traditionally, features can be classified as global or local. Another kind of classical feature division is the geometrical signature features, statistical features or pseudo dynamic features. Global parameters mean information of the whole signature and local parameters refers to specific information in parts of the signature. Geometrical information refers to the height and the width of the signature as well as their ratio, the area of the signature or the number of points such as loops, end-points, cross-points, etc. A fusion for probability-based directional transitions features such as signature stroke, angles and arcs are also considered. The statistical features model several signature characteristics according to the averages and probability density functions, e.g., pixel density. Pseudo dynamic parameters estimate dynamic parameters from the static signature,
e.g. estimating the pressure from ink intensity or pen speed by the stroke curvature.

In the area of pseudo dynamic features, recent advances have been observed in trying to infer the signature trajectory. A novel proposal involves a statistical feature containing local descriptors and ink deposition information based on well-known texture parameters such as Local Patterns. Texture-based descriptors are becoming more and more popular due to their good performance. Moreover, in Ref. 9 the authors propose combining geometrical and pseudo dynamic information with texture descriptors. Concisely, they combine co-occurrence matrices, shape matrices and gray-level intensity, looking for vestiges of the pressure signal with multi-scale verification functions.

Popular robust local features detector such as the Scale Invariant Feature Transform (SIFT) or Speeded Up Robust Features (SURF) has also been applied to static signatures, for instance in10. In Ref. 11 the authors use Gabor filter-based features combined with SURF features (G-SURF). Recently, optical flow to estimate local stability among signatures is used in Ref. 12 with promising performances.

2.3 Classification

The verifier models work with user signatures’ features. It usually gives a score which is used to accept or reject the query signature as belonging to the claimed identity. Usual classifiers in pattern recognition are also used in signature verifications, i.e. K-Nearest neighbours, Neural Networks (NN), Hidden Markov Models (HMM) and Support Vector Machines (SVM) among others are well accepted strategies. Recently, the Alternating Decision Tree (ADT) based on decision nodes and prediction nodes achieved encouraging recognition results. An assembly of the above classifiers usually improves performance.

An issue arises when comparing the verifier procedure with FHE work. In pattern recognition the verifier provides a score from which the decision is taken. Meanwhile a forensic expert gives a Likelihood Ratio (LR) of the prosecutor hypothesis (a certain signature was done by a suspected signer) and the defence trial (a certain signature was done by
another different signer). A Bayesian analysis is often the key to get a likelihood ratio. This gap remains open although recent efforts suggest that it will be filled in the next years.

3. Performance Evaluation Problem

Performance evaluation of automatic signature verifiers is an important issue to fully appreciate and determine the real reach of this technology. Performance usually is given in terms of ROC (Receiver Operating Characteristic) or DET (Detection Error Tradeoff) plot, in which the False Rejection Rate (FRR) versus FAR (False Acceptance Rate) is depicted for all possible decision thresholds. Often a single number such as the EER (Equal Error Rate) is given as a simplified measure. These statistical measures are usually worked out with signature databases.

The MCYT and the GPDS databases have become popular for pattern recognition. The MCYT database contains 75 users, 15 genuine signatures and 15 skilled forgeries per user. The GPDS includes 881 users, 24 genuine and 30 imitations per user. More signature databases freely released can be found at Ref. 13–19. These database samples are used for both some of the genuine ones to train the models and the other genuine and the forgeries to evaluate their performance.

Table 1 summarizes some of the recent developments and their evaluation provided by the authors. Clearly it is difficult to compare the quality of the different proposals due to the different evaluation procedures.

One approach to limit this drawback is to conduct several international signature competitions with the purpose of comparing different systems on the same databases and with the same evaluation protocols. Some of them are: The BioSecure Signature Evaluation Campaign 2009\textsuperscript{20} and 2011;\textsuperscript{21} 4NSigComp 2010\textsuperscript{22} and 2012;\textsuperscript{23} The SigComp2011\textsuperscript{24} and SigWiComp2013.\textsuperscript{25}

The major problem of the existing databases and competition is that they only include a few aspects of the real world and fail to reflect complex reality. Therefore the validity of the results obtained in the evaluation is limited. Some aspects are difficult to consider in the reduced databases, and they follow: performance with hundreds of
Table 1. Performances of some novel proposed schemes.

<table>
<thead>
<tr>
<th>Authors</th>
<th>Technique</th>
<th>Database</th>
<th>Results (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>K. Tselios, 2011</td>
<td>Directional Transitional Features + SVM</td>
<td>GPDS 300 users</td>
<td>EER: 3.80</td>
</tr>
<tr>
<td>Luana Batista et al. 2012</td>
<td>HMM + SVM</td>
<td>BrazilianSV 168 users</td>
<td>AER: 5.46</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GPDS 300 users</td>
<td>FRR with RF: 4.50</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FAR with RF: 5.19</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FRR with SF: 16.81</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FAR with SF: 16.88</td>
</tr>
<tr>
<td>M.A. Ferrer et al. 2012</td>
<td>Texture features + SVM</td>
<td>GPDS 800 users</td>
<td>EER with RF: 1.64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MCYT75 users</td>
<td>EER with SF: 16.85</td>
</tr>
<tr>
<td>S. Pal et al., 2012</td>
<td>Gabor filter + SURF features + SVM</td>
<td>GPDS 50 users</td>
<td>RR: 97.05</td>
</tr>
<tr>
<td>G. Pirlo et al. 2013</td>
<td>Optical flow + ADT</td>
<td>GPDS 300 users</td>
<td>EER with SF: 4.0</td>
</tr>
</tbody>
</table>

EER: equal error rate, AER: average error rate, FRR false rejection rate, FAR: false acceptance rate, RF: random forgeries, SF: skilled forgeries and RR: recognition rate.

of users, temporal drift, signer neuronal degeneration and aging effect, multilingua signatures (western, Hindi, Bangla, Japanese, Chinese, etc.), writer pose influence on the signature, pencil, inks and sheet influence, ability to detect disguised samples, etc. Additionally, the free distribution of real database compromises the legal identity of users hampering its distribution.

4. New Trends in Static Signature Recognition

In this paper the new challenges faced by researchers is broken down into five topics.

4.1. Generation of Synthetic Signatures Samples

The inclusion of real variability in a signature database requires a costly international cooperation in terms of time and money. A current,
apparently effective solution is the synthetic generation of databases. This procedure presents the following advantages: (i) it is effortless to produce (once the generation algorithm has been developed), (ii) there is no size restriction (in terms of subjects and samples per subject) since it is automatically produced from a computer, (iii) it is not subject to legal aspects because it does not comprise the data of any real user, and (iv) it eliminates human mistakes such as labeling the data which bias the performance evaluation of the algorithms.

The generation of a new synthetic handwritten signature has emerged as an attractive alternative for researchers during the last years. In fact several proposals have been published. Firstly, a novel methodology was developed by Galbally et al.\textsuperscript{28,29} to generate on-line signatures based on flourish and some isolated characters. Later, a static synthetic signature method is related to,\textsuperscript{30} which are based on flourish. A trend in this area is to include the diverse variability of real sceneries in the database.

4.2. \textit{Temporal drifting on automatic signature recognition}

The signature, as a behavioral biometric, is sensible to long-term variations which can be related to multiple session acquisitions,\textsuperscript{31} aging\textsuperscript{32} or neuromotor degenerations,\textsuperscript{33} among others. The main effect of aging in signature processing applications is the degradation of intraclass variability. Hence, distinguishing between genuine and forged signatures is a rather complex.

The literature about the effects of time on static handwritten signature recognition is scarce.\textsuperscript{32} However, the evaluation of aging in handwriting can be analyzed to extrapolate conclusions. In Ref. 34, researchers identify seven handwriting factors which are affected by aging: legibility, speed, pen grip, pressure, handwriting movements, styles and error corrections. All these factors influence the way a person sign and therefore the performance of automatic signature processing. Recent works study the relevance of aging in handwriting\textsuperscript{35} and dynamic signature\textsuperscript{31,32} recognition. Therefore, the development of technologies for static signature recognition adaptable to aging effects is a research line to be explored.
4.3. Forger identification

Most automatic signature recognition systems try to answer this question: is this signature made by its real owner? In the case of a forged signature, this classification scheme avoids an obvious second question which is relevant for FHE: who has forged the signature? The identification of forgers is a daily task for skilled forensics. However it has not attracted any noticeable role in the pattern recognition research community. In,36 the researchers evaluate the probability density function of different recognition systems obtained from the forger’s signature, the forged signature and the original owner. Their results establish a baseline but do not allow the forger to be identified. Traditional automatic signature recognition systems are mainly based on the global aspect of the signature and the forensics techniques for forger identification. They are focused on local individual characteristics of the strokes or even the analysis of furrows made by the writing tool on the paper. The development of automatic identification techniques based on these local features and its application to forger identification are open topics.

4.4. Disguised signature recognition

When a questioned signature is analyzed by a FHE, the analysis is done under the assumption of two possible hypotheses (see section 2.3). In the defense hypotheses there are two possible scenarios: i) the signature was made by a writer different from the original owner; ii) the signature was made by its original owner but it was disguised. Although FHE have faced this problem for a long time,37,38 the development of an automatic recognition system of disguised signatures is an open challenge. The inclusion of a disguised signature in performance benchmarks is relatively new. As an example, eleven state-of-the-art systems were evaluated to detect disguised signatures during the last two Forensic signature verification competition 4NSigComp2010 and 4NSigComp2012. The results obtained during the second evaluation23 clearly outperform the previous ones with EER under 30%. A promising performance based on local descriptors was achieved in Ref. 39 with a similar performance to the winners of 4NSigComp2012. This result encourages exploring deeply the feature approaches based on local information, as is proposed by FHE protocols. Again, this is an open
challenge and the inclusion of disguised signatures will be more standard in future experimental benchmarks.

4.5. Multiscript signature recognition

The signatures are commonly composed by letters and/or flourish and the letters can be written using different scripts. Despite the large number of works dealing with the script-based text recognition and the static signature recognition, most of them study the isolate problem. Some open questions related to multiscript scenarios are: What is the influence of the script in the recognition accuracy? The performance of a system proposed for the script A will be the same for the script B? In Ref. 41, Bangla, Devanagari and Roman script signatures were evaluated by using signature recognition systems. The most common errors occur with the misclassification of Hindi and Devanagari signatures. The signature is a behavioral biometric trait and it can be influenced by cultural aspects. The analysis of the influence of multiethnic characteristics in the signature identification systems is another unexplored topic for automatic signature recognition systems.

5. Conclusions

In terms of performance, state-of-the-art automatic signature recognition seems to be stopped in a performance around EER = 9% if the signature model is trained with genuine and tested with forgeries using the actual databases. Obviously, results vary depending on the database and the forger ability. In search of improvements, the pattern recognition research community is moving to the parameters used in FHE evaluations. This migration opens up a new scenario of applications and research opportunities. This paper offers a survey of some of these new issues but nowadays more and more proposals appear to be trying to bridge the Forensics Handwriting Experts demands and the Pattern Recognition community developments.

New acquisition devices, development of commercial applications, cancelable templates, gender and age estimation are some examples of new trends which have not been included in this work but may be important in the coming years.
References

Emerging Issues for Static Handwritten Signature Biometrics


