Off-line Signature Verification Using Contour Features

Almudena Gilperez, Fernando Alonso-Fernandez, Susana Pecharroman, Julian Fierrez, Javier Ortega-Garcia
Biometric Recognition Group - ATVS
Escuela Politecnica Superior - Universidad Autonoma de Madrid
Avda. Francisco Tomas y Valiente, 11 - 28049 Madrid, Spain
{almudena.gilperez, fernando.alonso, julian.fierrez, javier.ortega}@uam.es
http://atvs.ii.uam.es

Abstract

An off-line signature verification system based on contour features is presented. It works at the local image level, and encodes directional properties of signature contours and the length of regions enclosed inside letters. Results obtained on a sub-corpus of the MCYT signature database shows that directional-based features work much better than length-based features. Results are comparable to existing approaches based on different features. It is also observed that combination of the proposed features does not provide improvements in performance, maybe to some existing correlation among them.

1. Introduction

The increasing interest on biometrics is related to the number of important applications where a correct assessment of identity is a crucial point [1]. In this paper, we address the problem of automatic verification of writers on scanned images of signatures, known as off-line signature verification. This is a long-established pattern classification problem [2], since signature is one of the most widely used authentication methods due to its acceptance in government, legal, financial and commercial transactions [3]. It is worth noting that even professional forensic examiners perform at about 70% of correct classification rate, and thus this is a challenging research area [4].

A machine expert for off-line signature verification has been built in this work. It is based on features proposed for writer identification and verification using images of handwriting documents [5]. We have selected a number of features to be used with handwritten signatures which are based on local image analysis. The features implemented work at the analysis of the contour level. The signature is seen as a texture described by some probability distributions computed from the image and capturing the distinctive visual appearance of the samples. User individuality is therefore encoded using probability distributions (PDF) extracted from signature images. The term "feature" is used to denote such a complete PDF, so we will obtain an entire vector of probabilities capturing the signature uniqueness.

The rest of this paper is organized as follows. A description of the machine expert implemented in this work is given in Section 2. The experimental framework used, including the database, protocol and results, is described in Section 3. Conclusions are finally drawn in Section 4.

2. Machine expert based on contour features

The signature verification system includes three main stages: i) signature preprocessing, ii) feature extraction, and iii) feature matching. These stages are described next.

2.1. Pre-processing Stage

The objective of this stage is to enhance the signature image and to adapt it to the feature extraction stage. The preprocessing stage is divided in four parts, as shown in Figure 1: binarization, noise removal, component detection and contour extraction.

In the first place, the scanned image is binarized using the Otsu's method [6]. This method consists in a histogram thresholding. It performs well when the image is characterized by a uniform background and similar objects, as it is the case of signature images, and it does not need human supervision or prior information before its execution. The next step is the elimination of noise of the binary image, which is done through a morphological opening plus a closing operation [7]. Then a connected component detection, using 8-connectivity, is carried out. In the last step, internal and external contours of the connected components are extracted using the Moore's algorithm [7]. Beginning from a contour pixel of a connected component, which is set as the starting pixel,

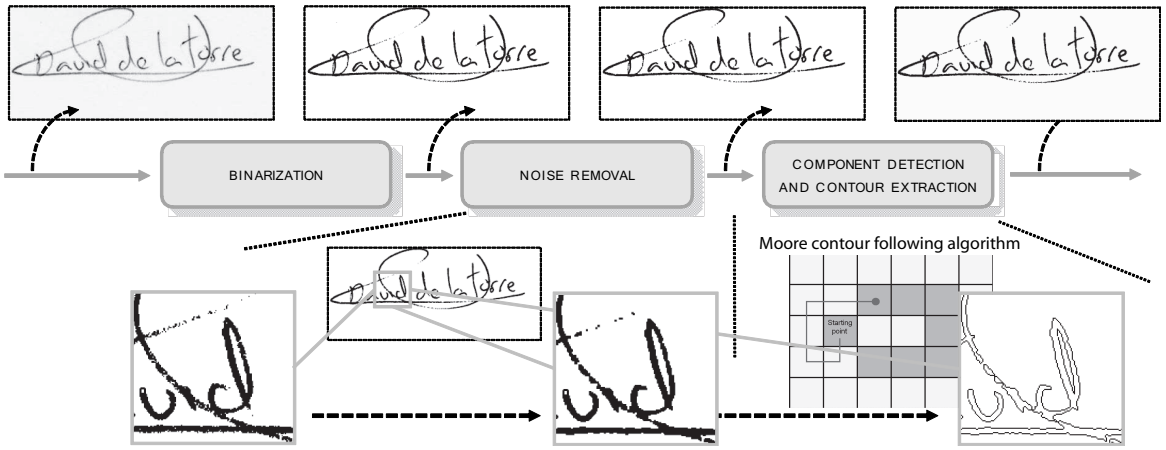

Figure 1. Preprocessing stage performed by the verification system.

this algorithm seeks a pixel boundary around it following the meaning clockwise, and repeats this process until the starting pixel is reached for the same position from which it was agreed to begin the algorithm. The result is a sequence with the pixels coordinates of the boundary of the component. This vectorial representation is very effective because it allows a rapid extraction of many of the features used later.

2.2. Feature Extraction Stage

Features are calculated from two representations of the signature extracted during the preprocessing stage: the binary image without noise and the contours of the connected components. The features used in this work are summarized in Table 1, including the signature representation used by each one. The signature is shaped like a texture that is described with probability distribution functions (PDFs). Probability distribution functions used here are grouped in two different categories: direction PDFs (features f1, f2, f3h, f3v) and length PDFs (features f5h, f5v). A graphical description of the extraction of direction PDFs is depicted in Figure 2. To be consistent with the work in which these features where proposed [5], we follow the same nomenclature used in it.

Contour-Direction PDF (f1)

This directional distribution is computed very fastly using the contour representation, with the additional advantage that the influence of the ink-trace width is eliminated. The contour-direction distribution f1 is extracted by considering the orientation of local contour fragments. A fragment is determined by two contour pixels (x_k,y_k) and ($x_{k+\epsilon}$,$y_{k+\epsilon}$) taken a certain distance ϵ apart. The angle that the fragment makes with the horizontal is computed using

$$\phi = \arctan(\frac{y_{k+\epsilon} - y_k}{x_{k+\epsilon} - x_k}) \quad (1)$$

As the algorithm runs over the contour, the histogram of angles is built. This angle histogram is then normalized to a probability distribution f1 which gives the probability of finding in the signature image a contour fragment oriented with each ϕ. The angle ϕ resides in the first two quadrants because, without online information, we do not know which inclination the writer signed with. The histogram is spanned in the interval 0°-180°, and is divided in $n = 12$ sections (bins). Therefore, each section spans 15°, which is a sufficiently detailed and robust description [5]. We also set $\epsilon = 5$. These settings will be used for all of the directional features presented in this paper.

Contour-Hinge PDF (f2)

In order to capture the curvature of the contour, as well as its orientation, the "hinge" feature f2 is used. The main idea is to consider two contour fragments attached at a common end pixel and compute the joint probability distribution of the orientations ϕ_1 and ϕ_2 of the two sides. A joint density function is obtained, which quantifies the chance of finding two "hinged" contour fragments with angles ϕ_1 and ϕ_2, respectively. It is spanned in the four quadrants (360°) and there are $2n$ sections for every side of the "contour-hinge", but only non-redundant combinations are considered (i.e. $\phi_2 \geq \phi_1$). For $n = 12$, the resulting contour-hinge feature vector has 300 dimensions [5].

Direction Co-Occurrence PDFs (f3h, f3v)

Based on the same idea of combining oriented contour fragments, the directional co-occurrence is used. For this

Table 1. Features used in this work.

	Feature	Explanation	Dimensions	Source
f1	$p(\phi)$	Contour-direction PDF	12	contours
f2	$p(\phi_1, \phi_2)$	Contour-hinge PDF	300	contours
f3h	$p(\phi_1, \phi_3)_h$	Direction co-occurrence PDF, horizontal run	144	contours
f3v	$p(\phi_1, \phi_3)_v$	Direction co-occurrence PDF, vertical run	144	contours
f5h	$p(rl)_h$	Run-length on background PDF, horizontal run	60	binary image
f5v	$p(rl)_v$	Run-length on background PDF, vertical run	60	binary image

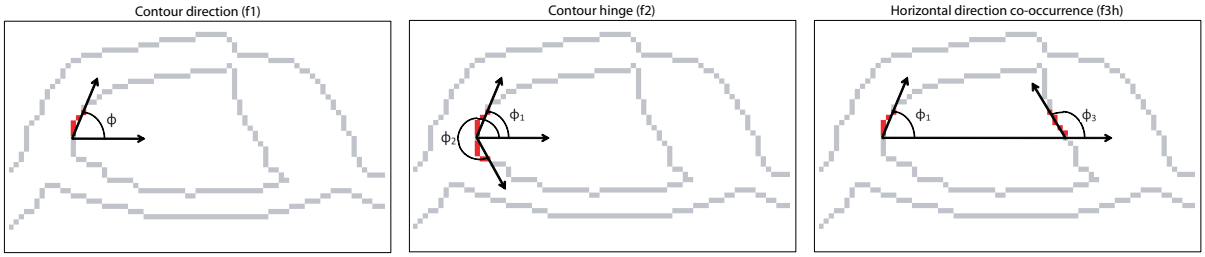

Figure 2. Graphical description of the feature extraction. From left to right: contour direction (f1), contour hinge (f2) and horizontal direction co-occurrence (f3h).

feature, the combination of contour-angles occurring at the ends of run-lengths on the background are used, see Figure 2. Horizontal runs along the rows of the image generate f3h and vertical runs along the columns generate f3v. They are also joint density functions, spanned in the two first quadrants, and divided into n^2 sections. These features give a measure of a roundness of the written characters and/or strokes.

Run-Length PDFs (f5h, f5v)

These features are computed from the binary image of the signature taking into consideration the pixels corresponding to the background. They capture the regions enclosed inside the letters and strokes and also the empty spaces between them. The probability distributions of horizontal and vertical lengths are used.

2.3. Feature Matching Stage

Each client of the system (enrolee) is represented by a PDF that is computed using an enrolment set of K signatures. For each feature, the histogram of the K signatures together is computed and then normalized to a probability distribution.

To compute the similarity between a claimed identity q and a given signature i, the χ^2 distance is used [5]:

$$\chi^2_{qi} = \sum_{n=1}^{N} \frac{(p_q[n] - p_i[n])^2}{p_q[n] + p_i[n]} \quad (2)$$

where p are entries in the PDF, n is the bin index, and N is the number of bins in the PDF (the dimensionality)

We also perform experiments combining the different features. The final distance in this case is computed as the mean value of the Hamming distances due to the individual features:

$$H_{qi} = \sum_{n=1}^{N} |p_q[n] - p_i[n]| \quad (3)$$

The χ^2 distance, due to the denominator, gives more weight to the low probability regions of the PDF and maximizes the performance of each individual feature. On the other hand, the Hamming distance provides comparable distance values for the individual features [5].

3. Experiments

3.1. Database and Experimental Protocol

We have used for the experiments a subcorpus of the MCYT database [8] which includes fingerprint and online signature data of 330 contributors from 4 different Spanish sites. Skilled forgeries are also available in the case of signature data. Forgers are provided the signature images of clients to be forged and, after training with them

Figure 3. Signature examples of the four types encountered in the MCYT corpus.

several times, they are asked to imitate the shape. Signature data were acquired with an inking pen and paper templates over a pen tablet. Therefore, signature images are also available on paper. Paper templates of 75 signers (and their associated skilled forgeries) have been digitized with a scanner at 600 dpi. The resulting subcorpus has 2250 images of signatures, with 15 genuine signatures and 15 forgeries per user (see Figure 3)[1].

The training set comprises either $K = 5$ or $K = 10$ genuine signatures (depending on the experiment under consideration). The remaining genuine signatures are used for testing. For a specific target user, casual impostor test scores are computed by using the genuine samples available from all the remaining targets. Real impostor test scores are computed by using the skilled forgeries of each target. As a result, we have $75 \times 10 = 750$ or $75 \times 5 = 375$ client similarity scores, $75 \times 15 = 1,125$ impostor scores from skilled forgeries, and $75 \times 74 \times 10 = 55,500$ or $75 \times 74 \times 5 = 27,750$ impostor scores from random forgeries.

In a verification context, two situations of error are possible: an impostor is accepted (false acceptance, FA) or the correct user is rejected (false rejection, FR). For error reporting, we use the graphical representations of Detection Error Trade-off (DET), which represent FA vs. FR rate. In order to have an indication of the level of performance with an ideal score alignment between users, we also report the EER when using *a posteriori* user-dependent score normalization [9]. The score normalization function is as follows $s' = s - s_\lambda$, where s is the raw similarity score computed by the signature matcher, s' is the normalized similarity score and s_λ is the user-dependent decision threshold at the EER obtained from a set of genuine and impostor scores of the user λ.

[1]This signature corpus is publicly available at http://atvs.ii.uam.es

3.2. Results

The system performance for *a posteriori* user-dependent score normalization is given in Table 2 (individual features) and Table 3 (combination of features). DET curves for the individual features without score normalization are plotted in Figure 4.

It is observed that the best individual feature is always the Contour-Hinge PDF f2, independently of the number of signatures used for training and both for random and skilled forgeries. This feature encodes simultaneously curvature and orientation of the signature contours. It is remarkable that the other features using two angles (f3h, f3v) perform worse than f2. Also worth noting, the feature using only one angle (f1) exhibits comparable performance to f3h and f3v, even outperforming them in some regions of the DET. It is interesting to point out the bad result obtained by the length PDFs (f5h and f5v). This suggests that the length of the regions enclosed inside the letters and strokes is not a good distinctive feature in offline signature verification (given a preprocessing stage similar to ours).

An important result also is that the combination of features does not result in performance improvement, as can be observed in Table 3, even for combinations that involve features of different categories (direction and length). Only the combination of f5h and f5v features has a significant improvement. An explanation is as follows. Although paired differently, the features based on directions involve the same set of angle values. As can be observed in Figure 2, the three examples depicted include the same value in one of the angles. As a result, there is some correlation between the features and therefore its combination does not result in improvement. For the features based on length, their bad performance could explain why they do not provide benefits in the fusion.

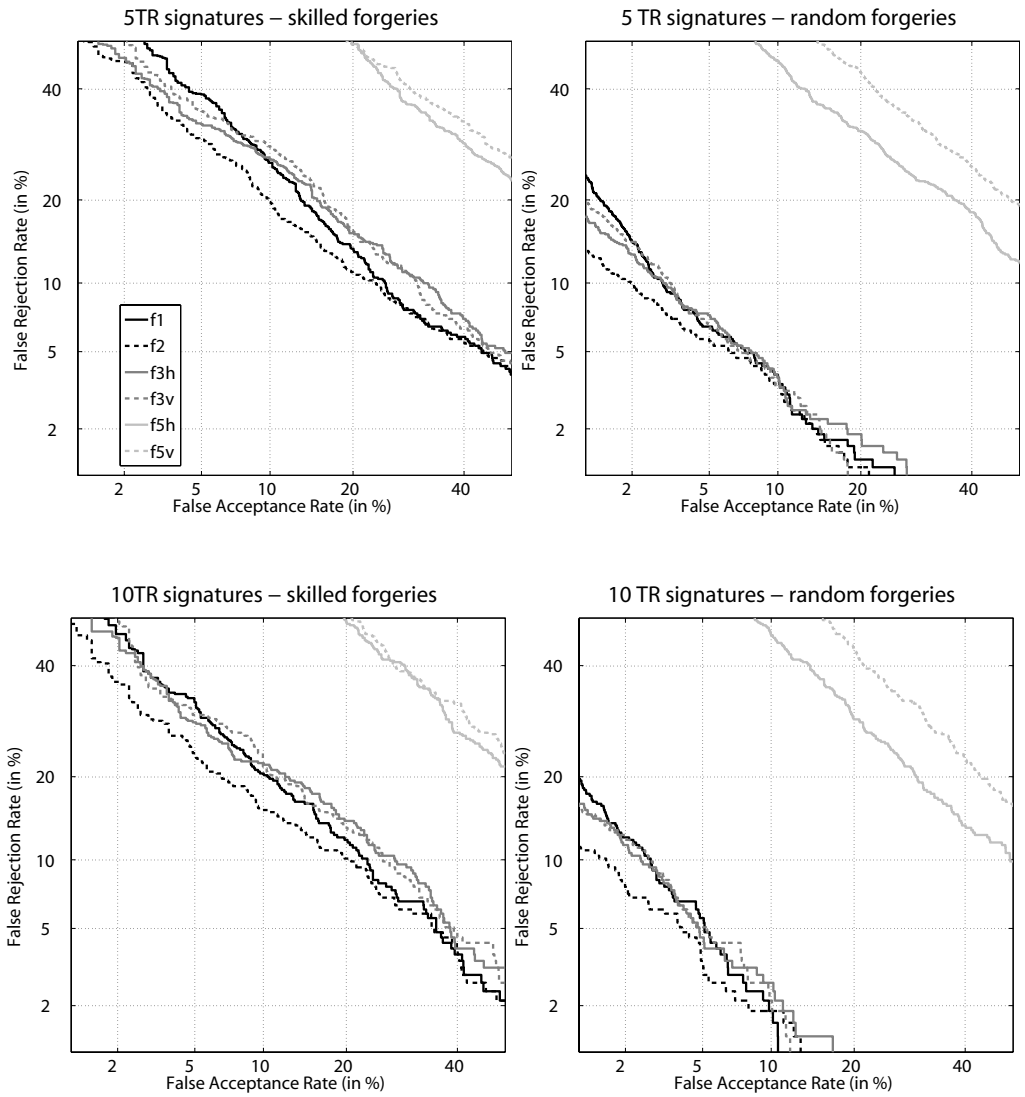

Figure 4. Verification performance without score normalization (user-independent decision thresholds).

4. Conclusions

A machine expert for off-line signature verification based on contour features has been presented. Writer individuality has been encoded using probability density functions (PDFs), grouped in two categories: direction PDFs and length PDFs. They work at the local level and encode several directional properties of contour fragments of the signature as well as the length of the regions enclosed inside letters.

Experimental results are given using 2250 different signature images of 75 contributors extracted from the MCYT signature database. Verification performance is reported for user-dependent and user-independent decision thresholds. Features based on direction work much better that those based on lengths, with best EERs of 6.44% and 1.18% for skilled and random forgeries, respectively (contour-hinge PDF, 10 training signatures, *a posteriori* score normalization). It is also remarkable that the combination of features does not result in performance improvement, maybe due to the correlation among them. We use the simple mean rule as fusion method. Considering the use of other complex fusion rules [12] is a source of future work.

Verification results are comparable to other existing approaches for off-line signature verification based on different features using the same experimental framework [10]. This encourages us to exploit their complementary information using different fusion strategies [11]. Another source of future work is to better analyze the information content in signature images in order to devise quality measures related to their utility for identity verification [13].

Table 2. System Performance in terms of EER (in %) of the **individual features** with *a posteriori* user-dependent score normalization.

SKILLED FORGERIES

	Direction PDFs				Length PDFs	
	f1	**f2**	**f3h**	**f3v**	**f5h**	**f5v**
5 TR Samples	12.71	10.18	11.40	12.31	30.33	31.78
10 TR Samples	10.00	6.44	7.78	9.16	28.89	33.78

RANDOM FORGERIES

Direction PDFs				Length PDFs	
f1	**f2**	**f3h**	**f3v**	**f5h**	**f5v**
3.31	2.18	3.09	3.21	22.18	28.03
1.96	1.18	1.40	1.49	20.46	28.58

Table 3. System Performance in terms of EER (in %) of the **combination of features** with *a posteriori* user-dependent score normalization. They are marked in bold the cases in which there is a performance improvement with respect to the best individual feature involved.

SKILLED FORGERIES

	f3=f3h+f3v	**f5=f5h+f5v**	**f1 & f5**	**f2 & f5**	**f3 & f5**	**f1 & f2**	**f1 & f3**	**f2 & f3**
5 TR Samples	12.40	**27.56**	16.69	15.56	13.33	13.11	12.38	11.40
10 TR Samples	8.93	**25.60**	13.64	12.13	9.64	9.87	9.16	8.40

RANDOM FORGERIES

	f3=f3h+f3v	**f5=f5h+f5v**	**f1 & f5**	**f2 & f5**	**f3 & f5**	**f1 & f2**	**f1 & f3**	**f2 & f3**
5 TR Samples	3.08	**21.00**	6.40	5.86	4.13	2.87	**2.95**	2.45
10 TR Samples	1.63	**17.86**	4.27	3.73	2.23	1.87	**1.43**	**1.06**

5. Acknowledgements

This work has been supported by Spanish project TEC2006-13141-C03-03, and by European Commission IST-2002-507634 Biosecure NoE. Author F. A.-F. thanks Consejeria de Educacion de la Comunidad de Madrid and Fondo Social Europeo for supporting his PhD studies. Author J. F. is supported by a Marie Curie Fellowship from the European Commission.

References

[1] A. Jain, A. Ross and S. Pankanti, "Biometrics: A Tool for Information Security", *IEEE Trans. on Information Forensics and Security*, 1:125–143, 2006.

[2] R. Plamondon and S. Srihari, "On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, 22(1):63–84, 2000.

[3] M. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", *Electronics and Communication Engineering Journal*, 9:273–280, December 1997.

[4] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Impact of signature legibility and signature type in off-line signature verification", *Proceedings of Biometric Symposium, Biometric Consortium Conference*, Baltimore, Maryland (USA), 1:1-6, September 2007.

[5] M. Bulacu and L. Schomaker, "Text-Independent Writer Identification and Verification Using Textural and Allographic Features", *IEEE Trans. on Pattern Analysis and Machine Inteligence*, 29(4):701–717, April 2007.

[6] N. Otsu, "A threshold selection method for gray-level histograms", *IEEE Trans. on Systems, Man and Cibernetics*, 9:62–66, December 1979.

[7] R. Gonzalez and R. Woods, *Digital Image Processing*, Addison-Wesley, 2002.

[8] J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon, J. Gonzalez, M. Faundez-Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. Igarza, C. Vivaracho, D. Escudero and Q. Moro, "MCYT baseline corpus: a bimodal biometric database", *IEE Proceedings on Vision, Image and Signal Processing*, 150(6):395–401, December 2003.

[9] J. Fierrez-Aguilar, J. Ortega-Garcia and J. Gonzalez-Rodriguez, "Target Dependent Score Normalization Techniques and Their Application to Signature Verification", *IEEE Trans. on Systems, Man and Cybernetics-Part C*, 35(3), 2005.

[10] J. Fierrez-Aguilar, N. Alonso-Hermira, G. Moreno-Marquez and J. Ortega-Garcia, "An off-line signature verification system based on fusion of local and global information", *Proc. Workshop on Biometric Authentication, BIOAW*, Springer LNCS-3087:295–306, 2004.

[11] J. Fierrez-Aguilar, J. Ortega-Garcia, J. Gonzalez-Rodriguez and J. Bigun, "Discriminative multimodal biometric authentication based on quality measures", *Pattern Recognition*, 38(5):777–779, 2005.

[12] A. Ross, P. Flynn and A. Jain, editors, *Handbook of Multibiometrics*, Springer, 2006.

[13] F. Alonso-Fernandez, M. Fairhurst, J. Fierrez and J. Ortega-Garcia, "Automatic measures for predicting performance in off-line signature", *Proc. International Conference on Image Processing, ICIP*, 1:369-372, San Antonio TX, USA, September 2007.