2009 10th International Conference on Document Analysis and Recognition

Offline Signature Verification Based on Pseudo-Cepstral Coefficients

Jesus F. Vargas
Universidad de Antioquia
Dpto de Ingeniería Electronica
Medellin, Colombia
jfvargas@udea.edu.co

Miguel A. Ferrer, Carlos M. Travieso, Jesus B. Alonso
Universidad de Las Palmas de Gran Canaria
CETIC
Las Palmas 35017, Spain.
{mferrer, ctravieso, jalonso}@dsc.ulpgc.es

Abstract

Features representing information about pressure distribution from a static image of a handwritten signature are analyzed for an offline verification system. From gray-scale images, its histogram is calculated and used as "spectrum" for calculation of pseudo-cepstral coefficients. Finally, the unique minimum-phase sequence is estimated and used as feature vector for signature verification. The optimal number of pseudo-coefficients is estimated for best system performance. Experiments were carried out using a database containing signatures from 100 individuals. The robustness of the analyzed system for simple forgeries is tested out with a LS-SVM model. For the sake of completeness, a comparison of the results obtained by the proposed approach with similar works published using pseudo-dynamic feature for offline signature verification is presented.

1. Introduction

The security requirements of the today's society have placed biometrics at the center of a large debate, as it become a key aspect in multitude of applications [2],[29],[23]. Biometrics measure individuals' unique physical or behavioral characteristics to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait. Of this class of biometrics, technologies for signature and voice are the most developed [17].

Handwritten signature is one of the most widely accepted personal attributes for identity verification. As a symbol of consent and authorization, specially in the prevalence of credit cards and bank cheques, handwritten signature has long been the target of fraudulence. Forging a signature is deemed to be more difficult than a fingerprint given the availability of sophisticated analyses [10]. Unfortunately, signature verification is a difficult discrimination problem since a handwritten signature is the result of a complex process depending on physical and psychological conditions of the signer, as well as on the conditions of the signing process[14]. The net result is that a signature is a strongly variable entity and its verification is not trivial, even for human experts. In this sense, signature verification has attracted many researchers from universities and companies, which are interested to the scientific challenges and to the valuable applications of this field, since no doubts automatic signature verification has a very important role in the set of biometric techniques for personal verification [21, 6].

In the present work, we focus on pseudo-dynamic characteristics. Features representing information of pressure distribution of a handwritten signature contained in a gray-scale image are analyzed. It is possible to say that pixels representing shapes written with high pressure may appear as darker zones, in this way, different values for pressure corresponds with variation of gray levels conforming histogram. The area and position of these zones appear to be distinctly different for genuine and forgery samples [1]. In this work, calculation of pseudo-cepstral coefficients as new approach for signature parametrization is presented. The optimal number of pseudo-coefficients is estimated for best system performance.

The paper is organized as follows: Section 2 presents a background of offline signature verification. Section 3 describes the approach proposed. Section 4 discusses about the Database. Section 5 is devoted to the classifiers. Section 6 presents the evaluation protocol and reports the experimental results, and the paper ends with concluding remarks.

2 Background

There are two major methods of signature verification. One is an on-line method to measure the sequential data such as handwriting speed and pen pressure with a special device. The other is an off-line method that uses an op-

978-0-7695-3725-2/09 $25.00 © 2009 IEEE
DOI 10.1109/ICDAR.2009.68

tical scanner to obtain handwriting data written on paper. There are two main approaches for off-line signature verification: static approaches and pseudo-dynamic approaches. The static one involves geometric measures of the signature while pseudo-dynamic one tries to estimate dynamic information from the static image[8]. When compared with online systems which uses special input devices such as tablets, offline approaches are much more difficult because the only available information is a static two-dimensional image obtained by scanning pre-written signatures on a paper; the dynamic information of the pen-tip (stylus) movement such as pen-tip coordinates, pressure, velocity, acceleration, and pen-up and pen-down can be captured by a tablet in real time but not by an image scanner. The offline method, therefore, needs to apply complex image processing techniques to segment and analyze signature shape for feature extraction [15]. Hence, online signature verification is generally more successful. Nevertheless, off-line systems have a significant advantage in that they do not require access to special processing devices when the signatures are produced. In fact, if the accuracy of the verification promoted greatly, the off-line method has much more practical application areas than that of the on-line one. Consequently more and more researches have looked into the feature-extraction methodology of offline signature recognition and verification [16].

On the other hand, track of the pen shows a great deal of variability. No two genuine signatures are ever precisely the same. Two identical signatures constitute legal evidence of forgery by tracing. The normal variability of signatures constitutes the greatest obstacle to be met in achieving automatic verification. Signatures vary in their complexity, duration, and vulnerability to forgery. Signers vary in their coordination and consistency. Thus, the security of the system varies from user to user. A short, common name is no doubt easier to forge than a long, carefully written name, no matter what technique is employed. Therefore, the system must be capable of "degrading" gracefully when supplied with inconsistent signatures, and the security risks must be kept to acceptable levels [12].

Generally, the problem of signature verification is faced by taking into account three different types of forgeries: random forgeries, produced without knowing either the name of the signer nor the shape of its signature; simple forgeries, produced knowing the name of the signer but without having an example of his signature; and skilled forgeries, produced by people who, looking at an original instance of the signature, attempt to imitate it as closely as possible. It is obvious that the problem of signature verification becomes more and more difficult when passing from random to simple and skilled forgeries, the latter being so difficult a task that even human beings make errors in several cases. In fact, exercises in imitating a signature often allow us to produce forgeries so similar to the originals that discrimination is practically impossible; in many cases, the distinction is complicated even more by the large variability introduced by some signers when writing their own signatures [26]. In relation to this, studies on signature shape found that North American signatures are typically more stylistic in contrast to the highly personalized and ''variable in shape" European ones [3].

2.1 Offline signature verification based on pseudo-dynamic features

For static signature images, we cannot derive dynamic information directly. What we can do is to derive some features that can partly represent the dynamic information. These special characteristics are referred to as pseudo-dynamic information. The term "pseudo-dynamic" is used to distinguish real dynamic data recorded during writing process from the information, which can be reconstructed from the static image [3].

There are different approaches to the reconstruction of the dynamic information from static handwriting records. Techniques from the field of forensic document examination mainly base on the microscopic inspection of the writing trace and assumptions about the underlying writing process [9]. Approaches from the field of image processing and pattern recognition can be divided in mathematical methods estimating the temporal order of stroke production [24, 5]; in method inspired by motor control theory recovering temporal features on the base of stroke geometries such as curvature [25]; and finally, in methods analyzing stroke thickness and/or stroke intensity variations [1, 4, 11, 20, 7]. From last group, we considerate mainly gray level distribution. When we analyze a gray-scale image containing a scanned handwritten signature, it is possible to say that pixels representing shapes written with high pressure appear as darker zones. In this way, High Pressure Points (HPPs) are those signature pixels which have gray level values upper than a suitable threshold. High pressure feature was proposed by Ammar et al. [1] to indicate regions where more emphasis has been made by the signer. This idea of calculate a threshold to find the HPPs was adopted and developed for others researchers [13, 26]. In order to analyze not only HPPs but Low Pressure Points (LPP) too, a complementary threshold has been proposed [19]. A local analysis, using Radial and Angular Partition (RAP) to determine the ratio, over each cell, between HPPs and all points conforming the binary version of image , has been proposed [28].

3 Our approach

From the gray scale image the histogram is calculated. With that information, the levels corresponding with back-

ground are detected and removed from histogram.

3.1 Gray-scale histogram preprocessing

Equalizing is done by using Eq. 1 [1],

$$I'(i,j) = I(i,j) - \frac{1}{M}\sum_{l=1}^{M} I(l,j) \tag{1}$$

where $(1 \leq i \leq M)$ and $(1 \leq j \leq N)$, with MxN size of original gray-scale image $I(i,j)$. Background reduction is done by clipping the negative of the equalized image according to,

$$I''(i,j) = \begin{cases} I'(i,j), & \text{if} I'(i,j) > 0 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

3.2 pseudo-Cepstral coefficients of gray-scale histogram

One of the more important properties of the Cepstrum is that it is a homomorphic transformation.
The cepstrum of an image g(x,y) is defined as follows:

$$C_g(p,q) = F^{-1}\{\log|G(u,v)|\} \tag{3}$$

where $G(u,v)$ is the Fourier transform of $g(x,y)$, and F^{-1} is the inverse Fourier transform. As Eq. 3 shows, the image in cepstrum-domain is the inverse Fourier transform of the logarithm power spectrum of the original image. In this approach, despite of we analyze an image, only its gray-scale histogram is taked into account. In this way, the cepstrum is defined for an array vector, as:

$$C_h(p) = F^{-1}\{\log|H(u)|\} \tag{4}$$

where $H(u)$ is replaced with the gray-scale histogram representing the "spectrum" of the signature image, this is

$$C_h(p) = F^{-1}\{\log|hisI(u)|\} \tag{5}$$

Finally, the unique minimum-phase sequence $\hat{y}$ is estimated and used as feature vector for signature verification.

$$\begin{array}{l} \hat{x} = \mathrm{Re}(F^{-1}(\log|hisI|)) \\ \hat{y} = \mathrm{Re}\left(F^{-1}\left(e^{F(\hat{x})}\right)\right) \end{array} \tag{6}$$

4 Database construction

The GPDS-100 signature corpus contains 24 genuine signatures and 24 forgeries of 100 individual [7]. So, there are 100 x 24 = 2400 genuine signatures and the same for forgeries. The genuine signatures were taken in just one session. To organize so many people in different session was a lost fight. The repetitions of each genuine signature and forgery specimen were collected using black or blue ink on white A4 sheets of paper featuring two different box sizes: the first box is 5 cm wide and 1.8 cm high and the second box is 4.5 cm wide and 2.5 cm high. Half of the genuine and forgery specimens were written in each type of boxes. The forgeries were collected by form with 15 boxes. Each forger form contains 5 images of different genuine signatures chosen randomly. The forger imitated 3 times each one of the 5 signs. They taken as long as they like to learn the signature and perform the forgeries. As the forgers are not expert people, these forgeries are simple forgeries. Once the signature forms were collected, each form was scanned with a Canon device using 256 level gray scale and 600dpi resolution. All the signature images were saved in PNG format.

5 Classification

Once the feature vectors are estimated, we need to solve a two-class classification (genuine or forgery) problem. Here we provide a brief description of the classification technique used in the verification stage.

5.1 Least Squares Support Vector Machines

Least Squares Support Vector Machines (LS-SVM) are reformulations to standard SVMs which lead to solving linear KKT systems [27]. Only solving linear equation is needed in the optimization process, which not only simplifies the process, but also avoids the problem of local minima in SVM. The LS-SVM model is defined in its primal weight space by,

$$\hat{y}(x) = \omega^T \varphi(x) + b \tag{7}$$

where $\varphi(x)$ is a function which maps the input space into a higher dimensional feature space, x is the M-dimensional vector of inputs x_j, and ω and b the parameters of the model. Given N input-output learning pairs (x^i, y^i). $R^M xR$, Least Squares Support Vector Machines for function estimation formulate the following optimization:

$$\min_{\omega,b,e} J(\omega,e) = \frac{1}{2}\omega^T\omega + \gamma\frac{1}{2}\sum_{i=1}^{N} e_i^2 \tag{8}$$

subject to

$$y^i = \omega^T\varphi\left(x^i\right) + b + e^i, i = 1,\ldots,N \tag{9}$$

The parameter set θ consists of vector ω and scalar b. Solving this optimization problem in dual space leads to finding

the α_i and b coefficients in the following solution:

$$h(x) = \sum_{i=1}^{N} \alpha_i K\left(x, x^i\right) + b \qquad (10)$$

Function $K\left(x, x^i\right)$ is the kernel defined as the dot product between the $\varphi(x)^T$ and $\varphi(x)$ mappings. The meta-parameters of the LS-SVM model are the width of the Gaussian kernels (taken identical for all kernels) and the γ regularization factor. The training method for the estimation of ω and b can be found in [27]. For this work, a RBF kernel with $\gamma = 10$ and $\sigma = 1$ as parameters was used.

6 Evaluation Protocol

6.1 Experiments

The genuine and forgery training samples has been randomly divided in two subsets of the same size (12 genuine and 12 forgeries). The first subset will be use for training purposes, and the second one will be use for testing. Remaining samples were used for verification. In order to obtain reliable results, the training and test procedure has been repeated 5 times with different training and test subsets. Results presented here were obtained taking into account "simple" type forgeries.

6.2 Results

Figure 1 shows results obtained for different number of pseudo-coeffecient N_c used as feature vector for signature verification. As can be seen, with $N_c = 14$ a good value for Equal Error Rate (EER = 6.20%) is obtained.

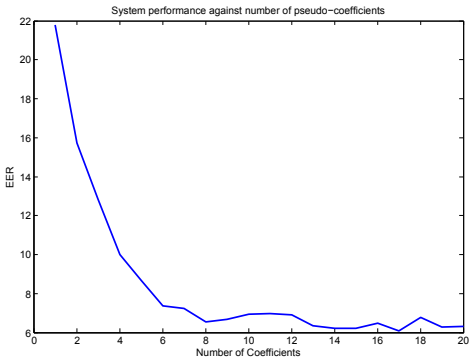

Figure 1. Selection of feature vector length.

6.3 Comparison with other published methods

We have to say that it is difficult to compare the performance of different signature verification systems since each author constructs own signature datasets. The lack of a standard international signature database is still being a big problem for performance comparison. For the sake of completeness, in Tables 1 and 2 we present a comparison of the results obtained by the proposed approach with similar works published which include features based on pseudo-dynamic information. Works taking into account for this challenge present results in terms of Type I and Type II errors for simple forgeries. The average error has been calculated too as mean value between False Acceptance Rate (FAR) and False Rejection Rate (FRR) values.

Table 1. Datasets used by other authors

	# Signers	Genuines Samples	Forgeries Samples
Ammar et al. [1]	20	10	10
Lv et al.[18]	20	25	30
Huang et al. [13]	21	24	24
Sansone et al [26]	49	20	10
Mitra et al. [19]	20	10	10
Ferrer et al. [7]	160	24	24
Vargas et al. [28]	160	24	24
Proposed	100	24	24

Table 2. Comparison of proposed approach with other published methods.

	(%)FAR	(%)FRR	(%)EER
Ammar et al. [1]	6.5	4	5.25
Lv et al.(A)[18]	32.00	30.00	31.00
Lv et al.(B)[18]	28.3	27.5	27.90
Huang et al. [13]	11.80	11.10	11.45
Sansone et al [26]	12.45	12.04	12.24
Mitra et al. [19]	2.50	4.00	3.25
Ferrer et al. [7]	12.60	14.10	13.35
Vargas et al. [28]	14.66	10.01	12.33
Proposed	7.35	5.05	6.20

In Table 2, Lv et al.(A) refers to results for gray distribution as feature set, and Lv et al.(B) refers to results for stroke width distribution as feature set.

7 Conclusions

A new off-line signature verification method based on pseudo-cepstral coefficients from histogram of grayscale images is described.

The performance of the system have been presented with reference to a experimental signature database containing samples from 100 individual including simple

forgeries. The experimental results show that using pseudo-coefficients achieves acceptable system performance EER=6.20% when compared with similar systems.

Acknowledgments

This work has been funded with the Spanish project MEC TEC2006-13141-C03/TCM.; F. Vargas is supported by the high level scholarships program, *Programme Alβan* No. E05D049748CO.

References

[1] M. Ammar, Y. Yoshida, and T. Fukumura. A new effective approach for automatic off-line verification of signatures by using pressure features. In *in Proceedings 8th International Conference on Pattern Recognition*, pages 566–569, 1986.

[2] K. Bowyer, V. Govindaraju, and N. Ratha. Introduction to the special issue on recent advances in biometric systems. *IEEE Trans. Systems, Man and Cybernetics - B*, 37(5):1091–1095, October 2007.

[3] H. Cardot, M. Revenu, B. Victorri, and M. Revillet. A static signature verification system based on a cooperative neural network architecture. *International Journal on Pattern Recognition and Artificial Intelligence*, 8(3):679–692, 1994.

[4] D. Doermann and A. Rosenfeld. Recovery of temporal information from static images of handwriting. *Int. J. Comput. Vision*, 15(1-2):143–164, 1995.

[5] A. El-Baati, A. M. Alimi, M. Charfi, and A. Ennaji. Recovery of temporal information from off-line arabic handwritten. In *AICCSA '05: Proceedings of the ACS/IEEE 2005 International Conference on Computer Systems and Applications*, pages 127–vii, Washington, DC, USA, 2005. IEEE Computer Society.

[6] M. Fairhurst. New perspectives in automatic signature verification. Technical Report 1, Information Security Technical Repor, 1998.

[7] M. Ferrer, J. Alonso, and C. Travieso. Offline geometric parameters for automatic signature verification using fixed-point arithmetic. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 27(6):993–997, 2005.

[8] 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. In *Workshop on Biometric Authentication, Springer LNCS-3087*, pages 298–306, May 2004.

[9] K. Franke, O. Bünnemeyer, and T. Sy. Ink texture analysis for writer identification. In *IWFHR '02: Proceedings of the Eighth International Workshop on Frontiers in Handwriting Recognition (IWFHR'02)*, page 268, Washington, DC, USA, 2002. IEEE Computer Society.

[10] K. Franke, J. R. del Solar, and M. Köpen. Soft-biometrics: Soft computing for biometric-applications. Technical report, IPK, 2003.

[11] J. Guo, D. Doermann, and A. Rosenfeld. Forgery detection by local correspondence. *International Journal of Pattern Recognition and Artificial Intelligence*, 15(579–641):4, 2001.

[12] N. Herbst and C. Liu. Automatic signature verification based on accelerometry. Technical report, IBM J.Res.Dev., 1977.

[13] K. Huang and H. Yan. Off-line signature verification based on geometric feature extraction and neural network classification. *Pattern Recognition, Elsevier Science*, 30(1):9–17, 1997.

[14] S. Impedovo and G. Pirlo. Verification of handwritten signatures: an overview. In *ICIAP '07: Proceedings of the 14th International Conference on Image Analysis and Processing*, pages 191–196, Washington, DC, USA, 2007. IEEE Computer Society.

[15] Y. Kato and M. Yasuhara. Recovery of drawing order from single-stroke handwriting images. *IEEE Transaction on Pattern Analysis and Machine Intelligence*, 22(9), 2000.

[16] S. Lee and J. Pan. Offline tracking and representation of signatures. *IEEE Transactions on Systems, Man and Cybernetics*, 22(4):755–771, 1992.

[17] S. Liu and M. Silverman. A practical guide to biometric security technology. *IEEE IT Professional*, 3(1):27–32, 2001.

[18] H. Lv, W. Wang, C. Wang, and Q. Zhuo. Off-line chinese signature verification based on support vector machine. *Pattern Recognition Letters, Elsevier*, 26:2390–2399, 2005.

[19] A. Mitra, P. Kumar, and C. Ardil. Automatic authentification of handwritten documents via low density pixel measurements. *International Journal of Computational Inteligence*, 2(4):219–223, 2005.

[20] L. Oliveira, E. Justino, C. Freitas, and R. Sabourin. The graphology applied to signature verification. In *12th Conference of the International Graphonomics Society*, pages 286–290, 2005.

[21] R. Plamondon. *Progress in Automatic Signature Verification*. World Scientific Publ., 1994.

[22] R. Plamondon and S. Srihari. On-line and off-line handwriting recognition: A comprehensive survey. *IEEE Trans. Pattern Anal. Mach. Intell.*, 22(1):63–84, 2000.

[23] S. Prabhakar, J. Kittler, D. Maltoni, L. O'Gorman, and T. Tan. Introduction to the special issue on biometrics: Progress and directions. *PAMI*, 29(4):513–516, April 2007.

[24] Y. Qiao and M. Yasuhara. Recovering dynamic information from static handwritten images. In *FHR04*, pages 118–123, 2004.

[25] P. R. and G. W. The 2/3 power law: When and why? *Acta Psychologica*, 100:85–96(12), November 1998.

[26] C. Sansone and M. Vento. Signature verification: Increasing performance by a multi-stage system. *Pattern analysis & Applications, Springer*, 3:169–181, 2000.

[27] J. A. K. Suykens, T. Van Gestel, J. De Brabanter, B. De Moor, and J. Vandewalle. *Least Squares Support Vector Machines*. World Scientific Publishing Co., Pte, Ltd, 2002.

[28] J. Vargas, M. Ferrer, C. Travieso, and J. Alonso. Off-line signature verification based on high pressure polar distribution. In *ICFHR08. Montereal.*, August 2008.

[29] D. Zhang, J. Campbell, D. Maltoni, and R. Bolle. Special issue on biometric systems. *IEEE Trans. Systems, Man and Cybernetics - C*, 35(3):273–275, August 2005.