AUTOMATIC SIGNATURE VERIFICATION: THE STATE OF THE ART—1989–1993

FRANCK LECLERC and RÉJEAN PLAMONDON

Laboratoire Scribens, École Polytechnique de Montréal
Département de Génie Électrique, C. P. 6079, Succ. Centre Ville
Montréal (QC), H3C 3A7, Canada

This paper is a follow up to an article published in 1989 by R. Plamondon and G. Lorette on the state of the art in automatic signature verification and writer identification. It summarizes the activity from year 1989 to 1993 in automatic signature verification. For this purpose, we report on the different projects dealing with dynamic, static and neural network approaches. In each section, a brief description of the major investigations is given.

Keywords: Automatic signature verification, handwriting models, static and dynamic technique, neural networks.

1. INTRODUCTION

Research is very actively under way in the signature verification domain. In their indepth article on this subject published in 1989,[72] R. Plamondon and G. Lorette reflect this high level of activity in their description of the numerous verification methods available and by classifying the strengths and weaknesses of these techniques.

A great deal has been done in the domain since this article was published. Researchers have applied new technologies, such as neural networks and parallel processing, to the problem of signature verification and they are continually introducing new ideas, concepts and algorithms. Signature verification is a real challenge for researchers because of the many difficulties that can arise during the process of creating such a system.[65,73,74] Two approaches are used in signature verification, one based on the static image of the signature (the result of the action of signing) and the other on the dynamic processes involved (the action of signing itself). The static approach has always been considered more problematic because the results obtained, in terms of type I and type II errors, are not as good as those obtained using the dynamic approach.[51,75,76] However the dynamic approach, too, poses numerous difficulties.[64] In this introductory paper, we propose to provide a comprehensive overview of the work that has been carried out since Ref. 72 appeared in 1989. This overview is presented in three sections: the first summarizes recent activity in static signature verification, the second describes developments in dynamic signature verification, both by conventional symbolic methods, and the third is devoted to verification by neural networks, whatever the approach, whether static or dynamic.

International Journal of Pattern Recognition and Artificial Intelligence Vol. 8 No. 3 (1994) 643–660

2. STATIC SIGNATURE VERIFICATION

As stated previously, static signature verification has always been considered by researchers to be the more difficult approach and to give worse results than dynamic signature verification.

Since 1989, M. Ammar[2–5] and M. Ammar, Y. Yoshida and T. Fukumura[6,7] have continued their work and have been quite active in this domain. In Ref. 5, for example, M. Ammar introduces a new technique for static signature verification which he calls AMT (Ammar Matching Technique). His approach is based on knowledge drawn from reference signature images, and on AMT, which enables similarity measurement. With this technique, M. Ammar reports elimination of skilled forgeries with a very low rate of false rejections, and with a mean error of 2% using a database of 200 genuine signatures from 20 writers and 200 skilled forgeries from 20 forgers.

The research of J. C. Pan and S. Lee[49,61] centers on representing the signature image. Using base heuristics, the authors represent a signature as a series of elements that simulate the process of generating a handwritten stroke by a human.

In a similar vein, as part of a long-term project aimed at creating a complete automated handwritten signature verification system, R. Sabourin, M. Cheriet and G. Genest[83] are evaluating a shade-coding method to eliminate random forgeries. In the same context, R. Sabourin and R. Plamondon[88] are defining and evaluating a number of relational similarity measures taken between relational vectors representing spatial distances between the reference profile and pairs of test primitives. In static signature verification, it is difficult to eliminate forgeries created by tracing or by photocopying. In four articles by the same group,[81,86,87,89] a solution is proposed for this problem based on grey-level comparison.

Dynamic programming is a technique that is widely used in dynamic signature verification to compare functions, such as the variation of a measure over time (pressure, speed, acceleration, etc.). This technique is also used in static signature verification. In Refs. 60, 80, for example, F. Nouboud and M. J. Revillet apply dynamic programming to the envelope of the signature image, and V. A. Shapiro[91] uses it in conjunction with an idea inspired by the field of tomography. In this project, Shapiro uses the projections under various different angles of the signature image, on the basis that the signature image can be retrieved from these projections.

Based on the fact that the properties of curvature, total length and slant angle of a signature are constant among different samples, T. S. Wilkinson and J. W. Goodman[95] propose the use of slope histograms to detect forgeries. With a database of 500 true signatures and 306 simple forgeries, the authors obtained an equal error rate of 7% (type I and II).

D. Randolph and G. Krishnan,[79] emulating techniques employed by signature verification experts, have developed a system with heuristics that learns to recognize signatures by accepting 92.5% of genuine signatures (7.5 type I error rate) and by rejecting 94.5% of forgeries (5.5% type II error rate). These rates are evaluated with a database of 120 true signatures and 36 simple imitations (imitations realized without examining the genuine signatures).

Finally, G. Krishnan and D. Jones[43] have introduced an algorithm to detect tracing forgeries by suggesting that the ink dispersion along the pen tip trace of someone who is forging by tracing is different from that of someone signing naturally. In designing their system, the authors use the gradient of the edges of the signature, because this gradient is significantly different in an original signature from that in a signature forged by tracing. For the test, the authors use 120 signatures from twelve subjects and fifteen different forgers who produce 7 tracing imitations for the twelve subjects. The rejection rates obtained in this way for tracing forgeries are in the neighborhood of 85%. Others works with gradient are also reported in the article.[85]

Thus it is clear that since research in 1989 static signature verification continues to be of great interest to the scientific community, especially considering the enormous financial impact of the automated verification of cheque signatures and signatures on official documents.

3. DYNAMIC SIGNATURE VERIFICATION

A signature verification system is designed in a number of stages, as follows: acquisition, preprocessing, comparison and evaluation. The acquisition process is very important because the quality of the signals is critical to optimizing the comparison process. Also, if the signals are of good quality, then the execution time associated with preprocessing is minimized, since the role of preprocessing is sometimes to correct faults in the acquisition system. In dynamic signature verification, the choice of signals that can be processed is fairly large (the x and y coordinates of a pen tip as a function of time, speed, acceleration, pressure, etc.). That is why some researchers focus on this problem in particular and propose data processing equipment designed exclusively for the acquisition step. R. Baron and R. Plamondon, for example, have evaluated an instrumented pen to measure acceleration.[8] Similarly, P. de Bruyne and R. Korolnik have developed hardware, which is presented in Ref. 24, to measure static and dynamic calligraphic characteristics. Finally, in Ref. 93, H. Taguchi, K. Kiriyama, E. Tanaka, and K. Fujii propose an instrumented pen capable of measuring the angle of the pen and the force exerted on it, which they are testing for use in a signature verification system. Although there is no consensus on the ideal acquisition tool for signature verification, the hardware currently available on the market—the digitizer—is without question the most widely used,[26–28,33,45] and can be modified as required.[93]

Many signals can be used in a signature verification system, the question is, which one do we choose? R. Plamondon and M. Parizeau compare the different types of signals in Ref. 77: the horizontal and vertical positions, the horizontal and vertical speeds and the horizontal and vertical accelerations. In this study, it was shown that the vertical signals are the most discriminating and that speed is the best representation for a 2D signature. Similarly, we may ask which combination of handwritten strokes (handwritten word, initial or signature) is the best one to use? In Ref. 62, M. Parizeau and R. Plamondon conclude that the signature is the best way of identifying an individual.

As in static signature verification, there are many ways to approach the problem of creating a dynamic signature verification system. This great diversity is reflected in the R. Plamondon and G. Lorette articles 51, 72–74, 76 and in this post-1989 update. One way of approaching the problem is to use a model as a base, for example to describe the signature[21,39] or to describe the process of generating a handwritten stroke. In the research of F. Leclerc[46] and F. Leclerc and R. Plamondon,[47] the validity of a model of the process of generating handwritten strokes was verified on signatures. More recently, a comparison of various models carried out by R. Plamondon, A. Alimi, P. Yergeau and F. Leclerc[71] and the work of A. Alimi and R. Plamondon[1] have enabled the model to evolve, which led R. Plamondon to develop the delta lognormal law for the generation of rapid movements.[66,67,69,70] Finally, a knowledge of the handwriting generation process facilitates decision-making in the design of a signature verification system.[68]

Another way to approach the problem is to analyze the signature to determine which points are perceptually important in the segmentation process.[11] Segmentation is an important step in the realization of a signature verification system,[13,21,27,28,39,59,66,78] so important in fact that it may warrant special consideration. G. Dimauro, S. Impedovo and G. Pirlo,[28] for example, segment a signature to be verified by matching it with the reference signatures so that only an optimal set of segmentation points is retained. With this type of segmentation, it is then possible to perform local comparisons rather than global ones. This results in a reduction in processing time and provides the opportunity to retrieve local information that may be fundamental for accurate verification of the signature. This segmentation may also be carried out using the knowledge of a model[48,66] or by means of neural networks (M. Lalonde and J. J. Brault[44]).

Whether segmented or not, the test signature must then be compared with the reference signature(s). There are many comparison algorithms currently available. A comparative study of three comparison techniques that are very widely used in signature verification (regional correlation, elastic matching and tree matching) has not shown the superiority of any one of them. The choice of technique depends on criteria like processing time, the signals used and the sensitivity of the adjustable parameters of the technique.[63] The problem is that the algorithms proposed for signature verification are often complex and frequently involve a great deal of repetitive calculation. This often requires very considerable processing time and may be cumbersome for on-line systems. For this reason, it would be of significant benefit to implement these algorithms in parallel. To explore this possibility, P. Fréchette and R. Plamondon[32] designed a parallel card based on the *TMS320C30* digital processor and have compared the performances of two signal comparison algorithms: regional correlation and dynamic programming. M. C. Fairhurst, P. S. Brittan and K. D. Cowley[30,31] have also suggested that the parallel approach is sometimes unavoidable—for example, to optimize a characteristic vector on a reference population of signers.

Even if very good comparison algorithms are available, the verification system sometimes reveals weaknesses with respect to particular signers who have an unstable signature that may be easy to forge. As a means of evaluating the quality of a signer's signature, J. J. Brault[10] and J. J. Brault and R. Plamondon[12,14,15] have proposed an index to measure the complexity inherent in imitating a signature.

In order to avoid time-consuming processing, some researchers propose a multilevel approach, the object of which is to rapidly eliminate gross forgeries by following simple processing steps.[28,59,78] This is particularly efficient when using the function approach (which is costly in terms of calculation time) in conjunction with the parameter approach.[78]

Although some avenues of action have become established in signature verification, there are many left to explore. In Ref. 59, for example, W. Nelson and E. Kishon investigate the possibility of creating a signature verification system based on a digitizer that produces the x, y coordinates of the pen tip and the pressure exerted on the pen tip simultaneously. This system rapidly eliminates gross forgeries, segments the signatures and uses dynamic programming to perform elastic rematching. In this study, the authors investigate the validity of their choice and their approach. If you are interested by previous work using pressure, force or derivative pressure you are referred to the following articles in Refs. 22, 23, 29, 35, 37, 38, 40, 50, 55, 90, 92, 96, 98, 101.

Researchers usually use the type I and type II error rates to evaluate verification systems. The type II error rate is very important because it expresses the percentage of counterfeit signatures (forgeries) that have been accepted. Minimizing this rate often involves an increase in the number of type I errors (rejections of a genuine signature), however. The system devised by H. Taguchi, K. Kiriyama, E. Tanaka and K. Fujii,[93] which is based on a commercial digitizer and a specially designed pen, has achieved a 6.7% type I error rate and a 0% type II error rate using a database of 105 genuines and 105 forgeries. In testing the validity of using spectral analysis in conjunction with discriminant analysis to build a signature verification system, C. F. Lam and D. Karnins[45] have achieved a 0% type I error rate for 2.5% type II errors with 8 genuine signatures and 152 forgeries produced by one signer and 19 forgers. Like C. F. Lam and D. Karnins,[45] K. Dar and A. Kunz[26] have previously explored the possibility of representing signatures in the frequency domain by considering the coordinates x and y as the real and imaginary part of a complex number. In the same vein, S. Impedovo, M. Castellano, G. Pirlo, and G. Dimauro[42] use spectral analysis of strokes with a structured knowledge database to verify signatures. In the first attempt, a knowledge database was built with 1000 true signatures from one writer. Tests were conducted with 232 genuine signatures and 434 forgeries. They obtained 3.5% type I error rate and 4.2% type II error rate. More recently, G. Gazzolo and L. Bruzzone[33] have proposed a methodology for identifying signers based on geometric, dynamic and graphological characteristics in generating a reference vector.

Researchers have also applied new techniques inspired from speech recognition to signature verification. L. Yang, B. K. Widjaja, and R. Prased[97] have used with success hidden Markov models. For a first attempt with 496 signatures from 31 subjects, the authors obtained 4.44% type I and 1.79% type II error rates using random forgeries. In the same way, N. Mohankrishnan, M. J. Paulik and M. Khalil[58] have applied a nonstationary autoregressive model for signature verification. On a database of 928 signatures (58 signatures from 16 writers), they have obtained an equal error rate of approximately 8%, using random forgeries.

A great deal of work is currently being done in the development of software, but little on hardware, although some researchers are developing more substantial hardware designs. For example, with an instrumented pen and a design for a dedicated microprocessor-based system that extracts the dynamic characteristics of a signature, D. P. Mital and K. T. Lau[56] have obtained a 2% type I error rate and a 5% type II error rate (the size of the database is unknown).

Finally, with a two-level strategy that aims at the rapid elimination of gross forgeries and the accurate verification of skilled forgeries, Dimauro *et al.*[28] have proposed signature segmentation tests based on reference signatures with a view to performing a local rather than a global comparison through elastic matching. In this way, the authors obtain type I and type II error rates of less than 4% on 15 signatures.

In signature verification, as in many shape recognition domains, it is very difficult to compare the results of different systems. Even if researchers express system performance in terms of type I and type II error rates (which unfortunately is not always the case!), these rates are measured under very different conditions (number of signers, types of signatures, types of forgeries used, etc.), and comparison is therefore very difficult. One way this can be done is to compare different systems by taking two of the systems available on the market and testing them under the same conditions, as S. F. Mjølsnes and G. Søberg[57] have done. It would be a laborious task to test twenty or so systems (cost of operation, mobilization of equipment and personnel, etc.), but would certainly be feasible, and very useful in making a final decision among two or three prototypes. Another approach is to use a public-domain database, as I. Yoshimura[99] and M. Yoshimura[100] have done and determine the error rates on this group of signatures. For example, with a dissimilarity measure incorporating the direction of pen movements, these authors obtained error rates of as little as 1% with the CADIX database.

This has been a brief survey of recent activity in dynamic signature verification. In the next section, we examine a new direction in the signature verification domain, the application of the neural network technique.

4. NEURAL NETWORKS

One of the greatest advances in signature verification since the 1989 article is the increasingly frequent use of neural networks. Neural networks have found their way into identity verification systems[36] and are now used in signature segmentation,[44] static signature verification[9,17–19,53,82,84] and dynamic signature verification.[16,20,25,34,41,54]

The advantages of neural networks are that they can be trained to recognize signatures and their characteristics are such that they could be used to classify signatures as genuine or forged as a function of time through a retraining process based on recent signatures. Their primary disadvantage is often the large number of specimens required to ensure that the network does in fact learn.

4.1. Dynamic Signature Verification using Neural Networks

Table 1 shows the dynamic signature verification results of four systems. These results are derived from the use of various strategies and several types of neural networks. J. Higashino,[41] for example, uses a four-layer network in his signature verification system, with two (2) hidden layers and an output neural. The output neural yields a measure of the degree of signature similarity. The training of the neural network is achieved through backpropagation of the error, calculated from pressure and speed signals.

For a signature verification system to learn to distinguish between genuine signatures and forgeries, samples of two types of signatures must be provided. Forged signatures are difficult to obtain and it is hard to define a class of forgers, which is why Higashino[41] uses genuine signatures that have been deformed instead. The author also uses what is known as the function approach. The neural networks are trained to recognize pressure, horizontal speed and vertical speed as a function of time. The signals of these parameters are then resampled so that only 256 points remain. P. Gentric and J. Minot[34,54] and H. D. Chang, J. F. Wang and H. M. Suen,[20] on the other hand, use the parameter approach. Thus, P. Gentric and J. Minot use the signals $x(t)$, $y(t)$ and $p(t)$ (the coordinates and pressure obtained by a special sensor) and elastic matching combined with dynamic programming to define four measures: mean pressure distortion, written shape distortion, dynamic difference and the ratio of signature durations. These measures are taken from N identical signatures that are considered in pairs. These signatures are then used to train the network, which has been specially designed for their application. In Ref. 25, E. Desjardin, A. C. Doux and M. Milgram use the speed module (curvilinear speed) to identify signers with a diabolo network normally used for signal compression.

Like K. P. Zimmermann and M. J. Varady,[101] L. Y. Tseng, and T. H. Huang[94] have decided to use one bit quantized pressure, but this time with a neural network. The aim of their works is to screen gross forgeries. Results are quite similar to those of Zimmermann and Varady; they are not really good as compared with dynamic verification systems.

Syntactic recognition is popular in handwritten applications and pattern recognition. For some aspects handwritten recognition and signature verification are similar. Thus, S. M. Lucas and R. I. Damper[52] use a syntactic neural network that can infer a grammar. Their alphabet is composed of eight directions plus a nul

Table 1. Dynamic signature verification systems with neurals (S = Specimen, W = Writer, F = Forgery.)

Authors	Signals used	Set of signatures	Networks	Errors	Comments
H. D. Chang J. F. Wang H. M. Suen[20]	Parameters produced by $u_x(t)\,u_y(t)$	800 trues (80 W × 10 S) 200 simple forgeries 200 skilled forgeries	Bayesian	type I: 2% type II: 2.5%	10 S for learning incremental learning with true S
J. Higashino[41]	Pressure $u_p(t)$ + speed $u_v(t)$	527 specimens from 70 W	2 hidden layers 768 input neurals 1 output neurals	type I: 7.97% type II: 0.61%	half registered S for learning all S for test
J. Minot[54] P. Gentric[34]	$u_x(t)$, $u_y(t)$ pressure $u_p(t)$	120 trues (12 W × 10 S) 48 skilled forgeries	Specific	type I: 2% type II: 4%	5 S learning 5 S + 4 F for test
E. Desjardin A. C. Doux M. Milgram[25]	Speed $u_v(t)$	195 trues (13 W × 15 S) 340 forgeries	Diabolo	type I: 0% type II: 0.38%	10 S learning 5 S for test + 340 F
S. M. Lucas, R. I. Damper[52]	$u_x(t)$, $u_y(t)$	400 S from 40 W	Syntactic neural network	type I: 5.6% type II: 4.5%	Network infer grammar
L. Y. Tseng, T. H. Huang[94]	one bit pressure $u_p(t)$	90 trues (9 W × 10 S) 10 forgeries	ART1 neural network	type I: 12.5–28.8% type II: 5.0–12.5%	use to screen forgeries 10 S or 5 S for learning

vector for no movement. In the learning mode, the neural network builds the grammar. In test mode, the network acts like a parser that verifies the test signatures.

Finally, J. Bromley, J. W. Bentz, L. Botton, I. Guyon, L. Jackel, Y. Le Cun, C. Moore, E. Sackinger, and R. Shah[16] introduced a "siamese" neural network for a signature verification system that incorporates some constraints. For this system, the authors tested various combinations of characteristics (a total of eight (8) based on speed, acceleration, the direction of the tangent relative to the trajectory, etc.). These results are not included in Table 1 because the system did not comply with one of the constraints, which was to achieve a 99.5% acceptance rate of genuine signatures for an 80% detection rate of forgeries.

In Ref. 54, J. Minot and P. Gentric raise the problem of modeling "realistic forgeries", in other words, how to devise good forgeries for training neural networks. Unlike J. Higashino,[41] J. Minot and P. Gentric did not want to create forgeries artificially. Instead, they designed a neural network adapted to the monoclass problem. This network estimates the similarity of different signatures and is connected to a decision network, a perceptron with a hidden layer, which is trained by backpropagation of the error gradient. H. D. Chang *et al.*[20] also use the parameter approach by extracting 15 measures based on the position signal, but in this case using a bayesian neural network. The network is trained with genuine signatures. During the verification process, the vector of the signature characteristics is evaluated to check whether or not the signature corresponds sufficiently well to the learned specimens. The neural network then acts as a bayesian classifier.

This has been a summary of recent activity in dynamic signature verification using neural networks. In the next section, we discuss the use of this new technique in static signature verification.

4.2. Static Signature Verification using Neural Networks

In addition to using neural networks for dynamic signature verification, researchers have also used these networks for static signature verification. Table 2 shows the static signature verification results of four systems. R. Sabourin and J. P. Drouhard in Ref. 84, for example, use neural networks to classify signature images, with the probability density function of the stroke directions serving as a global characteristics vector. The authors use this approach to rapidly eliminate gross forgeries, such as random forgeries. The network described in this article is a propagation classifier network used prior to and with backpropagation for the training process. During training, the authors use genuine signatures and random forgeries. In other work, R. Sabourin[82] has evaluated a Kohonen LVQ-type classifier. The results obtained are close to those of a conventional classifier of the type "k nearest neighbors with vote".

H. Cardot, M. Revenu, B. Victorri, and M. J. Revillet[17,18,19] also use neural networks to eliminate gross forgeries. For this they chose a global approach for which they use geometric parameters (mean stroke direction, moments of inertia, size of the signature) and the envelope of the signature.

Table 2. Static signature verification systems with neurals (S = Specimen, W = Writer, F = Forgery.)

Authors	Images	Set of signatures	Networks	Errors	Comments
S. Barua[9]	5 x 35 binary	27 patterns	Perceptron multilayers	90 to 95%	3 h learning
H. Cardot *et al.*[19]	512 x 512 binary	6000 signatures	Several types	Type I: 5% Type II: 2%	Size of training set unknown. Use gross imitations
D. A. Mighell[53]	128 x 64 binary	80 trues S x 1 W 66 forgeries	33 in 32 hid. neur. 1 out	Type I: 2% Type II: 2%	20 learn. = 10 S + 10 F 126 test = 70 S + 56 F
R. Sabourin and J. P. Drouard[84]	128 x 512 in 256 grey levels	800 trues (20 W x 40 S)	Feed-forward classifier	Type I: 1.75% Type II: 9.0%	20 S learning test = 20 S + 140 random F

In another article, S. Barua[9] explores the possibility of using neural networks to identify individuals in the context of protecting information systems. In his study, S. Barua uses a multilayer perceptron with one hidden layer. The signature is presented in a 5×35 binary image. The recognition rates of the models were between 90% and 95%. The author does not provide much detail on these results because his article was a feasibility study and the signals used were not from genuine signatures but from quite unrealistic models.

D. A. Mighell, T. S. Wilkinson, and J. W. Goodman[53] approached the problem of rapidly eliminating gross forgeries by using a neural network that learns through backpropagation. Once again, the authors had to confront the problem of using forgers to enhance the performances of their system. If no forgers are revealed during the training phase, then the network will recognize all the signatures as genuine during the test phase. The solution proposed by the authors is to use computer-generated forgeries. The results of their study are summarized in Table 2.

Generally speaking, neural networks obtain results comparable to those presented in the 1989 article. The great advantage of neural networks is that they are capable of learning to perform class separation. The principal difficulty raised by the various authors is the necessity of introducing forgers during the training phase. Forgers are not readily available and the class of forgers is difficult to define. Suggested solutions to the problem are to use networks designated for one class of signers, to use random forgeries or computer-generated forgeries from genuine signatures. Another difficulty is the number of signatures needed for the enrollment, around 10 to 20 (see Tables 1 and 2), which is greater than the number of references used in traditional systems (see Ref. 72). The development of the neural network approach is still in its early stages, however, and research in this domain will probably intensify in the future.

5. CONCLUSIONS

As we have attempted to demonstrate by providing a brief review of the work that has been done in the field since 1989, signature verification is a very active and multifaceted domain that continues to attract the attention of researchers. Given the complexity of the subject and of the financial interests involved as a consequence of signature fraud, it is more than likely that this level of enthusiasm will be maintained for many years to come.

Our hope is that this report on the state of the art will be useful to researchers in the field and will serve as a good introduction to the work published in this special issue.

6. ACKNOWLEDGEMENTS

This work was supported by grant ER-1220-1220 from FCAR and grant OGP-000915 from NSERC.

REFERENCES

1. A. Alimi and R. Plamondon, "Performance analysis of handwritten stroke generation models", in *Proc. of IWFHR 3th Int. Workshop on Frontiers in Handwriting Recognition*, Buffalo, May 1993, pp. 272–283.
2. M. Ammar, "Performance of parametric and reference pattern based features in static signature verification: A comparative study", in *Proc. Int. Conf. on Pattern Recognition*, 1990, pp. 646–648.
3. M. Ammar, "Identification of fraudulent Japanese signature from actual handwritten documents: A case study", in *Proc. of Int. Workshop on Frontiers in Handwriting Recognition*, Château de Bonas, France, Sept. 1991, pp. 369–374.
4. M. Ammar, "Progress in verification of skillfully simulated handwritten signature images", *Int. J. of Pattern Recogn. Artif. Intell.* **5**, 1 & 2 (1991) 337–351.
5. M. Ammar, "Elimination of skilled forgeries in off-line systems: A breakthrough", in *Proc. 11th IAPR Int. Conf. on Pattern Recognition*, Aug.–Sept. 1992, pp. 415–418.
6. M. Ammar, Y. Yoshida, and T. Fukumura, "Off-line preprocessing and verification of signatures", *Int. J. of Pattern Recogn. Artif. Intell.* **2**, 4 (1988) 589–602.
7. M. Ammar, Y. Yoshida, and T. Fukumura, "Structural description and classification of signature images", *Pattern Recogn.* **23**, 7 (1990) 697–710.
8. R. Baron and R. Plamondon, "Acceleration measurement with an instrumented pen for signature verification and handwriting analysis", *IEEE Trans. Instrum. Measurement* **38**, 6 (1989) 1132–1138.
9. S. Barua, "Neural networks and their applications to computer security", in *Proc. SPIE — Int. Society for Optical Engineering*, San Diego, July 1992, pp. 735–742.
10. J. J. Brault, "Proposition et vérification d'un coefficient de difficulté d'imitation des signatures manuscrites", Ph.D. thesis, École Polytechnique de Montréal, 1988.
11. J. J. Brault and R. Plamondon, "Segmenting handwritten signatures at their perceptually important points", *IEEE Trans. Pattern Anal. Mach. Int.* **15**, 9 (1986) 953–957.
12. J. J. Brault and R. Plamondon, "How to detect problematic signers for automatic signature verification", in *Int. Carnahan Conf. on Security Technology: Electronic Crime Countermeasures*, Oct. 1989, pp. 127–132.
13. J. J. Brault and R. Plamondon, "Segmentation des signatures manuscrites", in *Proc. of Vision Interface'89*, 1989, pp. 110–116.
14. J. J. Brault and R. Plamondon, "Can we measure the intrinsic complexity of signatures to be imitated?" in *Proc. 5th Handwriting Conf.*, Tempe, Arizona, 1991, pp. 169–171.
15. J. J. Brault and R. Plamondon, "A complexity measure of handwritten curves: Modeling of dynamic signature forgeries", *IEEE Tran. Syst. Man Cybern.* **23**, 2 (1993) 400–412.
16. J. Bromley, J. W. Bentz, L. Bottou, I. Guyon, L. Jackel, Y. Le Cun, C. Moore, E. Sackinger, and R. Shah, "Signature verification using a siamese time delay neural network", *Int. J. Pattern Recogn. Artif. Intell.* **7** (1993) 669.
17. H. Cardot, M. Revenu, B. Victorri, and M. J. Revillet, "Des réseaux neuronaux pour l'authentification de signatures manuscrites", in *Proc. CNED'92: Colloque National sur l'Écrit et le Document*, Nancy, July 1992, pp. 250–255.
18. H. Cardot, M. Revenu, B. Victorri, and M. J. Revillet, "Coopération de réseaux neuronaux pour l'authentification de signatures manuscrites", in *Proc. 6th Int. Conf. on Handwriting and Drawing*, Paris, July 1993, pp. 225–227.
19. H. Cardot, M. Revenu, B. Victorri, and M. J. Revillet, "L'authentification de signatures manuscrites: une approche globale par réseaux de neurones", in *Proc. 6th Int. Conf. on Handwriting and Drawing*, Paris, July 1993, pp. 225–227.

20. H. D. Chang, J. F. Wang, and H. M. Suen, "Dynamic handwritten Chinese signature verification", in *Proc. of ICDAR 93: Int. Conf. on Document Analysis and Recognition*, Oct. 1993, pp. 258–261.

21. R. M. Clark, T. Hastie, and E. Kishon, "A model for comparing signatures", in *Proc. IEEE Int. Conf. on Systems Man Cybern.*, 1990, pp. 326–330.

22. H. D. Crane and J. S. Ostrem, "Automatic signature verification using a three-axis force-sensitive pen", *IEEE Trans. Syst. Man Cybern.* **13**, 3 (1983) 329–337.

23. H. D. Crane, D. E. Wolf, and J. S. Ostrem, "The SRI pen system for automatic signature verification", in *Proc. NBS Trends and Applications*, Gaithersburg, 1977.

24. P. De Bruyne and R. Korolnik, "Measurement of static and dynamic calligraphic features", in *Int. Carnahan Conf. on Security Technology: Crime Countermeasures*, 1991, pp. 110–115.

25. E. Desjardin, A. C. Doux, and M. Milgram, "Identification de signataires, en ligne, par reseaux diabolo", in *Proc. 6th Int. Conf. on Handwriting and Drawing*, Paris, July 1993, pp. 144–146.

26. K. Dhar and A. Kunz, "Digital techniques to analyse handwritten signatures", in *Int. Carnahan Conf. on Security Technology: Crime Countermeasures*, 1988, pp. 9–13.

27. G. Dimauro, S. Impedovo, and G. Pirlo, "A stroke-oriented approach to signature verification", in *From Pixels to Features III: Frontiers in Handwriting Recognition*, eds. S. Impedovo and J. C. Simon, Elsevier Science Publishers B. V., 1992, pp. 371–384.

28. G. Dimauro, S. Impedovo, and G. Pirlo, "A signature verification system based on a dynamical segmentation technique", in *Proc. IWFHR 3th Int. Workshop on Frontiers in Handwriting Recognition*, Buffalo, May 1993, pp. 262–271.

29. E. P. Eernisse, C. E. Land, and J. B. Snelling, "Piezoelectric sensor pen for dynamic signature verification", in *Proc. IEEE Int. Electron. Devices Meeting*, 1977.

30. M. C. Fairhurst and P. S. Brittan, "A parallel approach to individually optimised handwritten signature verification", in *Proc. 11th IAPR Int. Conf. on Pattern Recognition*, Aug.–Sept. 1992, 685–688.

31. M. C. Fairhurst, P. S. Brittan, and K. D. Cowley, "Parallel realisation of feature selection for a high performance signature verification system", in *PACTA*, Barcelona, 1992.

32. P. Fréchette and R. Plamondon, "Architecture parallèle basée sur des TMS320C30 pour la comparaison de signaux", in *Proc. Vision Interface'90*, Calgary, June 1991, pp. 128–134.

33. G. Gazzolo and L. Bruzzone, "Real time signature recognition: A method for personal identification", in *Proc. ICDAR 93: Int. Conf. on Document Analysis and Recognition*, Oct. 1993, pp. 707–709.

34. P. Gentric and J. Minot, "Authentification dynamique de signatures par réseaux de neurones", *Revue Annuelle LEP*, 1990, pp. 34–36.

35. R. Gjøne and J. Miraglia, "Pen for signature verification by acceleration and pressure", *IBM Tech. Disclosure Bulletin*, **24**, 2 (1981).

36. I. Graham, "Neural network technique in client authentication", in *Proc. Conf. on Computers in the City 88*, Nov. 1988, pp. 207–228.

37. W. Haberman and A. Fejfar, "Automatic identification of personnel through speaker and signature verification — system description and testing", in *Proc. 1976 Carnahan Conf. on Crime Countermeasures*, 1976, pp. 23–30.

38. W. J. Hale and B. J. Paganini, "An automatic personal verification system based on signature writing habits", in *Carnahan Conf. on Crime Countermeasures*, 1980, pp. 121–125.

39. T. Hastie, E. Kishon, M. Clark, and J. Fan, "A model for signature verification", in *Proc. IEEE Int. Conf. on Systems, Man Cybern.*, Oct. 1991, pp. 191–196.
40. N. M. Herbst and C. N. Liu, 'Automatic signature verification based on accelerometry", *IBM J. Res. Develop.*, **21**, 3 (1977) pp. 245–253.
41. J. Higashino, "Signature verification system on neuro-computer", in *Proc. 11th IAPR Int. Conf. on Pattern Recognition*, Aug.–Sept. 1992, pp. 517–521.
42. S. Impedovo, M. Castellano, G. Pirlo, and G. Dimauro, "On-line signature verification system through stroke analysis", in *Proc. AFCET Int. Conf. on New Concepts in Computer Science*, 1990, pp. 47–53.
43. G. Krishnan and D. Jones, "Machine verification of traced signatures", in *Proc. SPIE — Int. Society for Optical Engineering*, 1991, pp. 563–572.
44. M. Lalonde and J. J. Brault, "A neural network approach to handwritten curve partitioning", in *Proc. of Vision Interface'93*, 1989, pp.136–141.
45. C. F. Lam and D. Kamins, "Signature recognition through spectral analysis", *Pattern Recogn.* **22**, 1 (1989) 39–44.
46. F. Leclerc, "Validation d'un modèle générateur de vitesse à profil gaussien sur des signatures manuscrites", Master's thesis, École Polytechnique de Montréal, Nov. 1989.
47. F. Leclerc and R. Plamondon, "Validation d'un modèle de la fonction de transfert du bras sur des signatures manuscrites"., in *Proc. of Vision Interface'90*, Halifax, May 1990, pp. 105–111.
48. F. Leclerc, R. Plamondon, and G. Lorette, "Des gaussiennes pour la modélisation des signatures et la segmentation de tracés manuscrits", *Traitement du signal* **9**, 4 (1992) 347–358.
49. S. Lee and J. C. Pan, "Offline tracing and representation of signatures", *IEEE Trans. Syst. Man Cybern.* **22**, 4 (1992) 755–771.
50. C. N. Liu, N. M. Herbst, and N. J. Anthony, "Automatic signature verification: System description and field test results", *IEEE Trans. Syst. Man Cybern.* **9**, 1 (1979) 35–38.
51. G. Lorette and R. Plamondon, "Dynamic approaches to handwritten signature verification", in *Computer Processing of Handwriting*, eds. R. Plamondon and C. G. Leedham, World Scientific Publ., 1990, pp. 21–47.
52. S. M. Lucas and R. I. Damper, "Signature verification with a syntactic neural net", in *Int. Joint Conf. on Neural Networks*, 1990, pp. 373–378.
53. D. A. Mighell, T. S. Wilkinson, and J. W. Goodman, "Backpropagation and its application to handwritten signature verification", in *Advances in Neural Information Processing Systems I*, ed. D. S. Touretzky, Morgan Kaufman, 1989, pp. 340–347.
54. J. Minot and P. Gentric, "Authentification dynamique de signatures par réseaux de neurones", *Traitement du signal* **8** (1990) 423–430.
55. D. P. Mital, C. P. Hin, and W. K. Long, "An on-line signature verification system", in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, 1987, pp. 837–841.
56. D. P. Mital and K. T. Lau, "A microprocessor-based signature verification system", *IEEE Trans. Consumer Electron.* **35**, 4 (1989) 845–851.
57. S. F. Mjølsnes and G. Soberg, "A comparative performance experiment of dynamic signature verification devices", in *Computer Recognition and Human Production of Handwriting*, eds. R. Plamondon, C. Y. Suen, and M. L. Simmer, World Scientific Publ., 1989, pp. 91–102.
58. N. Mohankrishnan, M. J. Paulik, and M. Khalil, "On-line signature verification using a nonstationary autoregressive model representation", *IEEE Int. Symp. on Circuits Systems*, Vol. 4, Chicago, USA, 1993, pp. 2303–2306.
59. W. Nelson and E. Kishon, "Use of dynamic features for signature verification", in *Proc. IEEE Int. Conf. on Systems, Man, and Cybernetics*, Oct. 1991.

60. F. Nouboud, "Contribution à l'étude et à la mise au point d'un système d'authentification de signatures manuscrites", Ph.D. thesis, Université de Caen, 1988.
61. J. C. Pan and S. Lee, "Off-line tracing and representation of signatures", in *Proc. IEEE Computer Society Conf. on Computer Vision and Pattern Recognition*, 1991, pp. 679–680.
62. M. Parizeau and R. Plamondon, "What types of scripts can be used for personal identity verification?" in *Computer Recognition and Human Production of Handwriting*, eds. R. Plamondon, C. Y. Suen, and M. L. Simmer, World Scientific Publ., 1989, pp. 77–90.
63. M. Parizeau and R. Plamondon, "A comparative analysis of regional correlation, dynamic time warping, and skeletal tree matching for signature verification", *IEEE Trans. Pattern Anal. Mach. Intell.* **12**, 7 (1990), 710–717.
64. J. R. Parks, "Automatic identification of people. Improving the performance of dynamic signature verification", in *IEE Colloq. Dig.*, (1990) 4.1–4.5.
65. G. Pirlo, "Algorithms for signature verification", in *Fundamentals in Handwriting Recognition*, Château de Bonas, France, June–July 1993, pp. 139–152.
66. R. Plamondon, "A model-based segmentation framework for computer processing of handwriting", in *Proc. 11th Int. Conf. on Pattern Recognition*, The Hague, 1992, pp. 303–307.
67. R. Plamondon, "A theory of rapid movements", in *Tutorial in Motor Behavior II*, eds. G. E. Stelmach and J. Requin, Elsevier Science Publ. B. V., 1992, pp. 55–69.
68. R. Plamondon, "A model-based dynamic signature verification system", in *Fundamentals in Handwriting Recognition*, Chateau de Bonas, France, June–July 1993, pp. 75–93.
69. R. Plamondon, *The Generation of Rapid Human Movements: Part I: A Δ Log-Normal Law*, Laboratoire Scribens, École Polytechnique edition, 1993.
70. R. Plamondon, *The Generation of Rapid Human Movements: Part II: A Quadratic and Power Laws*, Laboratoire Scribens, École Polytechnique edition, 1993.
71. R. Plamondon, A. Alimi, P. Yergeau, and F. Leclerc, "Modeling velocity profiles of rapid movements: A comparative study", *Biolog. Cybern.* **69** (1993) 119–128.
72. R. Plamondon and G. Lorette, "Automatic signature verification and writer identification — The state of the art", *Pattern Recogn.*, **22**, 2 (1989) 107–131.
73. R. Plamondon and G. Lorette, "On-line signature verification: How many countries are in the race?" in *Proc. Int. Carnahan Conf. on Security Technology*, 1989, pp. 183–189.
74. R. Plamondon and G. Lorette, "Designing an automatic signature verifier: Problem definition and system description", in *Computer Processing of Handwriting*, eds. R. Plamondon and C. G. Leedham, World Scientific Publ., 1990, pp. 3–20.
75. R. Plamondon, G. Lorette, and R. Sabourin, "Identity verification from automatic processing of signatures: IV static techniques and methods", in *Handwriting Pattern Recognition*, eds. R. Plamondon *et al.*, World Scientific Publ., 1989.
76. R. Plamondon, G. Lorette, and R. Sabourin, "Automatic processing of signature images: Static techniques and methods", in *Computer Processing of Handwriting*, eds. R. Plamondon and C. G. Leedham, World Scientific Publ., 1990, pp. 49–63.
77. R. Plamondon and M. Parizeau, "Signature verification from position, velocity and acceleration signals: A comparative study", in *Proc. 9th Int. Conf. on Pattern Recognition*, 1988.
78. R. Plamondon, P. Yergeau, and J. J. Brault, "A multilevel signature verification system", in *From Pixels to Features III: Frontiers in Handwriting Recognition*, eds. S. Impedovo and J. C. Simon, Elsevier Science Publishers B. V., 1992, pp. 363–370.

79. D. Randolph and G. Krishnan, "Off-line machine recognition of forgeries", in *Proc. of SPIE – Int. Soc. for Optical Engineering*, San Diego, Nov. 1990, pp. 255–264.
80. M. J. Revillet, "Signature verification on postal cheques", in *Proc. ICDAR 91: Int. Conf. on Document Analysis and Recognition*, Saint-Malo, Sept.–Oct. 1991, 767–773.
81. R. Sabourin, "Une approche de type compréhension de scène appliquée au problème de la vérification automatique de l'identité par l'image de la signature manuscrite", Ph.D. thesis, École Polytechnique de Montréal, 1990.
82. R. Sabourin, "Évaluation d'un classificateur de type LVQ de kohonen pour la vérification automatique de l'identité", in *Proc. CNED'92: Colloque National sur l'Écrit et le Document*, Nancy, July 1992, pp. 160–167.
83. R. Sabourin, M. Cheriet, and G. Genest, "An extended-shadow-code based approach for off-line signature verification", in *Proc. ICDAR 93: Int. Conf. on Document Analysis and Recognition*, Oct. 1993, pp. 1–5.
84. R. Sabourin and J. P. Drouhard, "Off-line signature verification using directional PDF and neural networks", in *Proc. 11th IAPR Int. Conf. on Pattern Recognition*, Aug.–Sept. 1992, pp. 321–325.
85. R. Sabourin and R. Plamondon, "Preprocessing of handwritten signatures from image gradient analysis", in *Proc. 8th Int. Conf. on Pattern Recognition*, Paris, Oct. 1986, pp. 576–579.
86. R. Sabourin and R. Plamondon, "Progress in the field of automatic handwritten signature verification systems using grey-level images", in *Proc. of IWFHR — Int. Workshop on Frontiers in Handwriting Recognition*, Montréal, Apr. 1990.
87. R. Sabourin and R. Plamondon, "Steps toward efficient processing of handwritten signatures images", in *Proc. Vision Interface'90*, Halifax, May 1990, pp. 94–104.
88. R. Sabourin and R. Plamondon, "Observability and similarity in spatial relations in the structural interpretation of handwritten signature images", in *Proc. 7th Scandinavian Conf. on Image Analysis*, Arlborg, Aug. 1991, pp. 477–485.
89. R. Sabourin, R. Plamondon, and G. Lorette, "Off-line identification with handwritten signatures image: Survey and perspectives", in *Proc. SSPR'90: Syntactic and Structural Pattern Recognition*, Murray Hill, June 1990, pp. 377–391.
90. Y. Sato and K. Kogure, "On-line signature verification based on shape, motion, and writing pressure", in *Proc. 6th Int. Conf. on Pattern Recognition*, 1982, pp. 823–826.
91. V. A. Shapiro and I. S. Bakalov, "Static signature verification as a dynamic programming problem", in *Proc. 6th Int. Conf. on Handwriting and Drawing*, Paris, Jul. 1993, pp. 219–221.
92. J. Sternberg, "Automated signature verification using handwriting pressure", Tech. Rep., Wescon, 1975.
93. H. Taguchi, K. Kiriyama, E. Tanaka, and K. Fujii, "On-line recognition of handwritten signatures by feature extraction of pen movements", *Syst. Computers Jpn.*, **20**, 10 (1989) 1–14.
94. L. Y. Tseng and T. H. Huang, "An on-line Chinese signature verification scheme based on the ART1 neural network", in *Int. Joint Conf. on Neural Networks*, Baltimore, Maryland, Jun. 1992, pp. 624–630.
95. T. S Wilkinson and J. W Goodman, "Slope histogram detection of forged handwritten signatures", in *Proc. SPIE — Int. Society for Optical Engineering*, Boston, 1990, pp. 293–304.
96. T. K. Worthington, T. J. Chainer, J. D. Williford, and S. C. Gundersen, "IBM dynamic signature verification", in *Computer Security, IFIP 1985*, eds. J. B. Grimson and H. J. Kugler, Elsevier Science Publ. B. V., 1095, pp. 129–154.

97. L. Yang, B. K
Markov mod
Norway, 1993
98. M. Yasuhara
alignment: A
99. I. Yoshimura
direction of
From Pixels
and J. C. Sin
100. M. Yoshimur
fication incoı
2083–2092.
101. K. P. Zimme
tized pressur

Received 31 Octo

97. L. Yang, B. K. Widjaja, and R. Prasad, "On-line signature verification applying hidden Markov models", in *Proc. of 8th Scandinavian Conf. on Image Analysis*, Tromso, Norway, 1993, pp. 1311–1316.
98. M. Yasuhara and M. Oka, "Signature verification experiment based on nonlinear time alignment: A feasibility study", *IEEE Trans. Syst. Man Cybern.* **7** (1977) 212–216.
99. I. Yoshimura and M. Yoshimura, "On-line signature verification incorporating the direction of pen movement: An experimental examination of the effectiveness", in *From Pixels to Features III: Frontiers in Handwriting Recognition*, eds. S. Impedovo and J. C. Simon, Elsevier Science Publ. B. V., 1992, pp. 353–362.
100. M. Yoshimura, Y. Kato, S. I. Matsuda, and I. Yashimura, "On-line signature verification incoporating the direction of pen movement", *IEICE Trans.* **74**, 7 (1991) 2083–2092.
101. K. P. Zimmermann and M. J. Varady, "Handwritten identification from one-bit quantized pressure patterns", *Pattern Recogn.* **18**, 1 (1985) 63–72.

Received 31 October 1993; revised 6 November 1993.