AUTOMATIC SIGNATURE VERIFICATION:

FRANCK LECLERC and RÉJEAN PLAMONDON
Laboratoire SRCFSE, 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 summarises 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 techniques, neural networks.

I. 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.67,73,74 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.91,75,76 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 summarises 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.
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 and M. Ammar, Y. Yoshida and T. Fukumura 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 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 are evaluating a shade-coding method to eliminate random forgeries. In the same context, R. Sabourin and R. Plamondon 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, 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, 69, for example, F. Nouhoud and M. J. Reville apply dynamic programming to the envelope of the signature image, and V. A. Shapiro 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 propose the use of slope histograms to detect forgeries. With a database of 500 true signatures and 506 simple forgeries, the authors obtained an equal error rate of 7% (type I and II).

D. Randolph and G. Krishnan, 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 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.

Thus it is clear that since research in 1980 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. 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. Fuji 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,25–28,33,45 and can be modified as required.

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. 65, 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, \textsuperscript{21,20} or to describe the process of generating a handwritten stroke. In the research of F. Leclerc\textsuperscript{48} and F. Leclerc and R. Plamondon, \textsuperscript{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\textsuperscript{71} and the work of A. Alimi and R. Plamondon\textsuperscript{47} have enabled the model to evolve, which led R. Plamondon to develop the delta lognormal law for the generation of rapid movements.\textsuperscript{69,67,83,72} Finally, a knowledge of the handwriting generation process facilitates decision-making in the design of a signature verification system.\textsuperscript{68}

Another way to approach the problem is to analyze the signature to determine which points are perceptually important in the segmentation process.\textsuperscript{71} Segmentation is an important step in the realization of a signature verification system,\textsuperscript{19,23,37,38,39,59,66,77} so important in fact that it may warrant special consideration. G. Dimaro, S. Impedovo and G. Pirlo,\textsuperscript{24} 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\textsuperscript{46,66} or by means of neural networks (M. Lalonde and J. J. Brault\textsuperscript{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.\textsuperscript{43} 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\textsuperscript{52} designed a parallel card based on the TM5820CM0 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\textsuperscript{20,31} 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 few sometimes reveal stable signature of a signer's signature have proposed signature approach (which parameter approach).

Although no solution, there are E. Kishon invest based on a digital pressure exertedgross forgeries, elastic remnants and their approx derivative pressus 37, 38, 40, 50, 51 Researchers n systems. The 141 of counterfeit sig often involves as signature, howe and K. Fujii,\textsuperscript{19} the system, C. F. I. 25% type II err signer and 19 fo have previously domain by consi a complex num. G. Dimaro\textsuperscript{47} to verify signatures true signatures f and 434 forgeries More recently, to identifying signe in generating a.
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 and J. J. Brault and R. Plamondon have proposed an index to measure the complexity inherent in imitating a signature.

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

Although some venues of action have become established in signature verification, there are many left to explore. In Ref. 50, 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. 36, 37, 38, 40, 45, 46, 48, 49, 50, 55, 59, 62, 64, 66, 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, 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 genuine 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 have achieved a 2% 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, K. Dar and A. Kunz 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. Dimarotto 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. Garzolo and L. Bruzzone 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. Prasad23 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. Khalid have applied a nonstationary autoregressive model for signature verification. On a database of 328 signatures (58 signatures from 18 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. Law86 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, Dimarco et al.26 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. Mjelnes and G. Sæberg23 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. Yoshimura27 and M. Yoshimura28 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 systems16 and are now used in signature segmentation,41 static verification,20,21,23,24,31,44

The advantages of signatures and their signatures as genuine-based on recent signal of specimens required

4.1. Dynamic Signatures

Table 1 shows the dy results are derived frc networks. J. Higashin verification system, w neural network is ach pressure and speed sig.

For a signature vi signatures and forgery Forged signatures are ers, which is why Hj instead. The author a networks are trained

function of time. The 256 points remain. P. H. M. Suen,76 on the the J. Minot use the sign by a special sensor a define four measures: difference and the rat identical signatures t to train the network. Ref. 25, E. Desgardin linear speed) to iden compression.

Like K. P. Zimmer have decided to use o The aim of their work of Zimmermann and verification systems. Syntactic recognition. For some as similar. Thus, S. M. can infer a grammar
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, 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 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 and H. D. Chang, J. F. Wang and H. M. Suen on the other hand, use the parameter approach. Thus, P. Gentric and J. Minot use the signals $x(t)$, $y(t)$ and $z(t)$ (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. Desjardins, 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, L. Y. Tseng, and T. H. Huang have decided to use one bit quantized pressure, but this time with a neural network. The aim of their work 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 use a syntactic neural network that can infer a grammar. Their alphabet is composed of eight directions plus a null...
<table>
<thead>
<tr>
<th>Authors</th>
<th>Signals used</th>
<th>Set of signatures</th>
<th>Networks</th>
<th>Errors</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>H. D. Chang</td>
<td>Parameters</td>
<td>800 trues (80 W x 10 S)</td>
<td>Bayesian</td>
<td>type I: 2%</td>
<td>10 S for learning incremental learning with true S</td>
</tr>
<tr>
<td>J. F. Wang</td>
<td>produced by $u_4(t)$, $u_5(t)$</td>
<td>200 simple forgeries</td>
<td>type II: 2.3%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>H. M. Suen</td>
<td></td>
<td>200 skilled forgeries</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>J. Higashin</td>
<td>Pressure $u_6(t)$ + speed $u_7(t)$</td>
<td>527 specimens from 70 W</td>
<td>2 hidden layers</td>
<td>type I: 7.07%</td>
<td>half registered S for learning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>786 input neural</td>
<td>type II: 0.61%</td>
<td>all S for test</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>output neural</td>
<td></td>
<td></td>
</tr>
<tr>
<td>J. Minout</td>
<td>$u_1(t)$, $u_2(t)$, pressure $u_3(t)$</td>
<td>120 trues (12 W x 10 S)</td>
<td>Specific</td>
<td>type I: 2%</td>
<td>5 S learning</td>
</tr>
<tr>
<td>P. Genric</td>
<td></td>
<td>48 skilled forgeries</td>
<td>type II: 4%</td>
<td></td>
<td>5 S + 4 F for test</td>
</tr>
<tr>
<td>E. Nenjardin</td>
<td>Speed $u_4(t)$</td>
<td>195 trues (13 W x 15 S)</td>
<td>Diablo</td>
<td>type I: 0%</td>
<td>10 S learning</td>
</tr>
<tr>
<td>A. C. Doux</td>
<td></td>
<td>340 forgeries</td>
<td>type II: 0.36%</td>
<td></td>
<td>5 S for test + 340 F</td>
</tr>
<tr>
<td>M. Milgram</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>S. M. Lucas,</td>
<td>$u_6(t)$, $u_7(t)$</td>
<td>400 S from 40 W</td>
<td>Synaptic neural</td>
<td>type I: 6.6%</td>
<td>Network infer grammar</td>
</tr>
<tr>
<td>R. F. Dampan</td>
<td></td>
<td></td>
<td>network</td>
<td>type II: 4.5%</td>
<td></td>
</tr>
<tr>
<td>L. Y. Tseng,</td>
<td>one bit pressure</td>
<td>90 trues (9 W x 10 S)</td>
<td>ART1 neural</td>
<td>type I: 12.5-28.5%</td>
<td>use to screen forgeries</td>
</tr>
<tr>
<td>T. H. Huang</td>
<td>$u_9(t)$</td>
<td>10 forgeries</td>
<td>network</td>
<td>type II: 5.0-12.5%</td>
<td>10 S or 5 S for learning</td>
</tr>
</tbody>
</table>

Table 1. Dynamic signature verification systems with neural (S = Specimen, W = Writer, F = Forger).
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 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, Minot and Gentric did not want to create forgeries artificially. Instead, they designed a neural network adapted to the monochrom 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 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. Reveux, B. Victorri, and M. J. Revillet 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.
In another study, S. Baru is presented in between 90% because his art signatures but D. A. Migh of rapidly eliminating backpropagation forgers to end during the trough genuine during computer-generated.

Generally, in the 1989 art of learning to authors is these are not able to use random. Another difficult to 20 (see Tal traditional system is still in its end in the future.

5. CONCLUSION
As we have mentioned that has been and multifaceted. Given the many consequences will be maintained. Our hope is the field and the issue.

6. ACKNOWLEGEMENTS
This work was supported by 000915 from...
In another article, S. Barua explored 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 x 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 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


21. R. M. Charing IEEE Int.

22. H. D. Cras signature v.

23. H. D. Cras force-sensitive


25. E. Desjardins par recherches 1993, pp. 1

26. K. Dhar an Carnahan

27. G. Dimarco verification eds. S. Im pp. 371-38

28. G. Dimarco dynamical in HANDWRITING

29. E. P. Eerins signature vi

30. M. C. Fairl written sign Ang.-Sept.

31. M. C. Fairl selection for

32. P. Frichette pour la con pp. 128-134

33. G. Gazolo identificatio Oct. 1993, j

34. P. Gestric eceurones", /

35. R. Gzime am IBM Tech.

36. I. Graham, Computers

37. W. Haberm and signatu Conf. on C

38. W. J. Hale on signature pp. 121-125.


25. E. Desjardins, A. C. Dox, and M. Milgram, "Identification de signataires, en ligne, par reseaux diabolos", in Proc. 6th Int. Conf. on Handwriting and Drawing, Paris, July 1993, pp. 144-146.


41. J. Higashi, "Signature verification system on neuro-computer", in Proc. 11th IAPR Int. Conf. on Pattern Recognition, Aug.–Sept. 1992, pp. 517–521.


65. G. Pollo, "Algorithms for signature verification", in Fundamentals in Handwriting Recognition, Château de Bonas, France, June-July 1993, pp. 139-152.


68. R. Plamondon, "A model-based dynamic signature verification system", in Fundamentals in Handwriting Recognition, Château de Bonas, France, June-July 1993, pp. 75-93.


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.


90. Y. Sato and K. Kogure, “Online 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.


Received 31 October 1993; revised 6 November 1993.