Reliable On-Line Human Signature Verification Systems

Luan L. Lee, Toby Berger, and Erez Aviczer

Abstract—On-line dynamic signature verification systems were designed and tested. A data base of more than 10,000 signatures in ($x(t)$, $y(t)$)-form was acquired using a graphics tablet. We extracted a 42-parameter feature set at first, and advanced to a set of 49 normalized features that tolerate inconsistencies in genuine signatures while retaining the power to discriminate against forgeries. We studied algorithms for selecting and perhaps orthogonalizing features in accordance with the availability of training data and the level of system complexity. For decision making we studied several classifiers types. A modified version of our majority classifier yielded 2.5% equal error rate and, more importantly, an asymptotic performance of 7% false acceptance rate at zero false rejection rate, was robust to the speed of genuine signatures, and used only 15 parameter features.

Index Terms—Signature verification, human signature verification, dynamic signature verification, on-line signature verification, point-of-sale, point-of-delivery, forgery.

1 Introduction

THE design and implementation of an on-line dynamic signature verification system involves data acquisition, feature extraction, feature selection, decision making and performance evaluation. Such problems have been discussed both in the by-now classic survey paper of Plamondon and Lorette [1] and, more recently, in the sequel thereto by Leclerc and Plamondon [2].

In this correspondence we describe an approach to designing reliable and effective on-line signature verification which includes: construction of a reliable data base, selection of optimum feature sets with or without forgery data available, finding classifier-independent feature selection procedures, obtaining reliable asymptotic global and individual performance, obtaining a suitable statistical model for signatures, minimizing the effects both of the inconsistency of genuine signatures and of the variety of forgeries, and adapting to practical limitations such as on-line response and limited memory size. We introduce new techniques for on-line human signature verification that are responsive to all these issues and yield performance satisfactory for point-of-sale (POS) applications. Among articles that have appeared subsequent to the submission of this correspondence that overlap somewhat with our results are works by Dimauro et al. [3], Plamandon [4], Nelson et al. [5], Fairhurst and Brittan [6], and Yang et al. [7].

2 Data Acquisition

A total of 5,603 genuine signatures were collected from a population of 105 human subjects which included 22 women and five left-handed writers. Some subjects contributed as few as 13 genuine signatures; one subject wrote his signature more than 1,000 times. About 90% of the genuine signatures were collected under "normal" writing conditions. Because a signature verification system must be robust with respect to variations in writing speed, we also collected a set of 240 *"fast"* signatures from nine subjects who were asked to write their genuine signatures as fast as possible. The percentage reduction in writing time from normal to fast signing ranged from 10% to 50%. With respect to the size of signatures, the smallest rectangles that fit the largest and smallest signatures, respectively, measured 10 cm by 13 cm and 2 cm by 0.5 cm. Signature writing times ranged from 1 s to 14 s.

The construction of a meaningful forgery data base requires careful planning. We employed three kinds of forgeries, namely: **simple** [1], **statically skilled**, and **timed forgeries**. Although other kinds of forgeries have been suggested in the literature [1], we believe that the three kinds forgeries we used are the sorts most likely to be encountered in POS applications. In simple forgery, we assumed that forgers know how to spell the genuine signatures. A total of 1,148 simple forgeries were collected. A forgery is considered statically skilled when, in addition to possessing all spatial information about the genuine signature, the forger is allowed to practice imitations both on paper and on the tablet. A total of 3,466 statically skilled forgeries were collected. For timed forgery, in addition to the static information about genuine signatures, the forger is provided during practice with information about the average genuine writing time. A total of 1,148 timed forgeries were collected.

Additionally we collected 248 Chinese signatures from 23 subjects, 26 Arabic signatures from two subjects, 13 Tamil signatures from one subject, 13 Korean signatures from one subject, and 13 Hebrew signatures from one subject.

3 Feature Extraction

The first feature set consists of 42 personalized parameter features —13 static and 29 dynamic—as described in Appendix A. Some of the 42 features were inspired by the literature of handwriting verification [8], [9], [10], [15], after being appropriately adapted to our signature verification application. Others of the 42-feature set are our own contributions based on experience acquired form the signature collection procedure. The only preprocessing required here is to minimize the effect of the spatial resolution of the graphics tablet by eliminating one of any two consecutive sample points that were separated by only one or two basic spatial resolution units. Spatial resolution of the tablet can seriously affect instantaneous features which involve only a few sample points. We eliminated the problem of signature rotation and shifting by providing a horizontal line on paper taped over the tablet surface as reference for writing.

Preliminary experiments showed that the 42-feature set is highly sensitive to variations in size and speed of genuine signatures. Therefore, a second set consisting of 49 normalized features was constructed with the objective of rectifying these deficiencies [13]. The feature normalization procedure can be as complex as that proposed in [11], [16] or as simple as linear normalization. The effectiveness of the linear normalization procedure we employed depends on the extent to which the temporal assumption and the spatial assumption below are valid. We did not directly examine the degree of validity of these assumption, but our positive verification results strongly suggest that reality conforms well to these assumptions. **Temporal Assumption:** an instance of an event will occur at roughly the same fraction of time of the writing duration of a signature regardless of the overall signing speed. **Spatial Assumption:** linear scaling of the horizontal and vertical displacements, by possibly different scaling constants, will restore genuine signatures written larger or smaller than usual to the standard shape.

Virtually no additional time or effort is needed to obtain the linearly normalized features from their nonnormalized versions

- *L.L. Lee is with the Faculty of Electrical Engineering, DECOM-FEE-UNICAMP, Campinas, SP, 13081-970, BRAZIL.*
- *T. Berger is with Cornell University, School of Electrical Engineering, Engineering and Theory Center Building, Ithaca NY 14853.*
  E-mail: berger@ee.cornell.edu.
- *E. Aviczer is with AT&T Bell Laboratories, Holmdel, NJ 17733.*

Manuscript received Oct. 20, 1994; revised Jan. 9, 1996. Recommended for acceptance by M. Mohuiddin.
For information on obtaining reprints of this article, please send e-mail to: transactions@computer.org, and reference IEEECS Log Number P96007.

0162-8828/96$05.00 ©1996 IEEE

since the normalization factors—total writing time, total horizontal displacement, and total vertical displacement—were in the original 42-feature set. A detailed description of the normalized feature set appears in Appendix B.

4 Feature Selection

Relatively few attempts have been made to select an optimal subset of features from a larger feature set for automatic human signature verification [8], [10]. Moreover, these approaches either depended on the classifier being used or were not effectively tested by forgery data. Three feature selection algorithms are now described. The first selects features assuming availability of genuine signatures only. Let $m(a, i)$ and $\sigma^2(a, i)$ be the sample mean and the sample variance of feature i computed from the reference data base of subject a. Then the distance measure for feature i between subject a and subject b is defined as

$$d_i(a, b) = \frac{|m(a, i) - m(b, i)|}{\sqrt{\sigma^2(a, i) + \sigma^2(b, i)}}. \qquad (1)$$

We say that feature i has a higher order, or degree, of importance for subject a than does feature j in population P if

$$d_i(a) = \min_{b \in P, b \neq a} d_i(a,b) > \min_{b \in P, b \neq a} d_j(a,b) = d_j(a).$$

In other words, we order features for subject a in terms of their *"maximin"* distance from the rest of the entire population P. Selection of the k best features is equivalent to selection of those k features (i.e., those k values of i) for which the distances $d_i(a)$ defined by (1) are largest.

When both genuine and forgery data are available, we replace (1) by

$$d_i(a) = \frac{|m(a, i) - m(f, i)|}{\sqrt{\sigma^2(a, i) + \sigma^2(f, i)}}. \qquad (2)$$

Here $m(f, i)$ and $\sigma^2(f, i)$ are, respectively, the sample mean and the sample covariance of feature i computed from the data base of forgeries of subject a's signature. When forgery data are available feature i is considered more important than feature j if $d_i(a) > d_j(a)$. An extensive list of the individually ordered 42 features for each of 22 subjects is available in [13]. Features should be selected for incorporation in a classifier not just on the basis of such orderings but also with regard to how they are correlated with one another; see Section 4.2.

Test results confirm that better performance can be achieved by using an optimum individualized subset of features instead of using the whole feature set. However, individually optimized subsets may be precluded by limitation of fast response time and memory size. A feasible suboptimal alternative to the problem of finding an ideal feature set is to identify a so-called *common feature set* consisting of features that are good for most persons in the population. A common feature set is attractive if the procedure for finding it is simple and the degradation in performance is small enough relative to employing individualized feature sets. Our m-feature common set consists of those m features with the highest relative frequencies of appearances in the subjects' lists of m best individualized features. Table 1 shows the selected common set of 10 feature frequencies of appearances and the order of preference among them for the population of 22 subjects.

TABLE 1
COMMON 10 FEATURES SETS

	Preference	1	2	3	4	5	6	7	8	9	10
The 42 Feature Set	Feature #	1	22	24	5	23	6	25	7	29	32
	Frequency	20	19	14	12	12	11	11	9	9	8
The 49 Feature Set	Feature #	48	5	4	6	7	30	35	39	1	44
	Frequency	17	11	10	10	10	9	8	8	7	6

4.1 Classifier Designs

The main task in classifier design is to deduce a distance measure between signatures that effects strong separation between the class of forgeries and the class of genuine signatures for each subject. However, the joint probability distribution of the features usually is unknown and difficult to estimate. Accordingly, many popular methods which involve probabilistic distance measures cannot be used and all approaches are more or less ad hoc. Majority classifiers, which implement the majority decision rule described below, have the advantage of being simple to implement while providing performance satisfactory for POS applications.

Let m_i and σ_i, represent, respectively, the sample average and sample standard deviation of feature i in the ensemble of an individual's genuine signatures. Let n denote the total number of features used in decision process, let α be a fixed threshold, and t_i be the value of feature i for the candidate signature (T) being tested. Define

$$N_\alpha = \left| \left\{ i : \frac{|t_i - m_i|}{\sigma_i} \leq \alpha \right\} \right|. \qquad (3)$$

The majority decision rule is "T is declared a genuine signature if $N_\alpha \geq n/2$ and a forgery if $N_\alpha < n/2$." Note that the majority rule is highly nonlinear, the decision region in the n-dimensional normalized feature space for accepting a signature as genuine being unbounded and, roughly speaking, consisting of n noncircular infinite cylinders centered in the origin, each with its axis parallel to one of n feature coordinate axes.

The problem of inconsistency of genuine signatures can be attacked by using normalized features. This reduces the false rejection rate of the majority classifier for fixed α and a fixed set of n features but also reduces the forgery rejection rate. Accordingly, tradeoffs must be studied carefully to assess the utility of normalization. Intuition suggests that, if we do not altogether destroy the information that normalization removes from the raw signature data, we may be able to use it to make the majority classifier perform better than when it uses only normalized features. Two such modified decision procedures, designed to work in conjunction with time-normalized features, called *"presoft majority decision"* and *"prehard majority decision,"* are described below.

The presoft majority decision procedure consists of comparing the writing time, t_w, of the signature being tested to the average writing time, $\bar{t}_w$, computed from the subject's genuine reference set. If $|t_w - \bar{t}_w| > \beta\bar{t}_w$, where a nominal value for parameter β is 0.2, do not normalize the dynamic features in the 49-feature set; otherwise, normalize them as usual. Finally, execute the conventional majority decision rule using the resulting 49 features.

The presoft majority classifier penalizes signatures possessing highly deviant writing time by removing the normalization factor of signature writing time from the dynamic features. This is justified because considerable consistency in signature writing time was observed among genuine signatures. However, there still is hope for a genuine signature with an anomalous t_w to be classified correctly if enough features in the 49-feature set behave satisfactorily. Similarly, some forgeries might escape detection even if they fail to pass the predecision procedure.

The prehard majority classifier penalizes signatures with large $|t_w - \bar{t}_w| > \beta\bar{t}_w$ more heavily by declaring a signature to be a forgery if $|t_w - \bar{t}_w| > \beta\bar{t}_w$.

4.2 Accounting for Feature Covariances

Two shortcomings of the majority classifier are that it weights each feature equally and does not account for correlations among features. One approach to dealing with correlation is to employ a

Karhunen-Loeve (K-L) representation. Toward this end we first diagonized the sample covariance matrix of the feature set for the training sample of genuine signatures; usually only five or six of the resulting uncorrelated linear combination of features were needed to account for most (80% to 95%) of the overall variance in individuals' genuine signatures. Next, we did the same for the training ensembles of "forgeries," finding that we usually needed about 20 K-L features to account for the bulk of the variance. Detailed description of extensive experiments on K-L features and their results can be found in [12].

We have also attacked the feature selection problem via neural nets and jackknife statistics. A single-neuron classifier yields an improvement in performance [17]; more general nets naturally yield further improvement [18]. Also, a bottom-up jackknife feature selection algorithm can design majority classifiers with small feature sets and good Type I vs Type II tradeoffs [19].

5 Statistical Model

A good statistical model for signatures would advance signature technology by quantifying interclass and intraclass variability among signatures [1]; forgery classes are particularly difficult to characterize. In attempts to address this problem, Hastie et al. [11] recently proposed a statistical model for signature verification by computer which provides good results for relatively consistent signatures. We make no attempt to solve the complex and fundamental problem of developing a statistical model for human signatures. However, by introducing a statistical model for the parameter feature sets of genuine signatures, we were able to generate enough simulated feature vectors to estimate the asymptotic performance of our signature verification systems and to check the estimate using data from the subject who signed 1,000 times. We postulated an additive model, $X = M + N$, where $X = (X_1, X_2, .., X_n)$ is an n-dimensional random vector representing the signature's parameter feature set, M is an n-dimensional constant vector and N is an n-dimensional Gaussian vector with zero mean and covariance matrix C.

6 Experimental Results and Conclusion

Type I error (false rejection) and Type II error (false acceptance) are used to evaluate the performance of a signature verification system [1]. The key performance requirement for POS applications is that the Type II error must stay small (say, ≤ 25%) as the decision threshold is adjusted to drive the Type I error to zero. We now present experimental results on majority classifiers which show their suitability for POS applications. Additional results can be found in [13].

Fig. 1a shows the performance measure of majority classifiers which employ four different 10-feature sets and the 13 static features set, all selected from the 42-feature set. The solid line and dash-dotted line are for subsets of 10 best individualized features selected, respectively, with and without reference forgery data available. The solid line with * is for the set of 13 static features. The dashed line is the case of the common 10-feature set selected from the reference data base, i.e., the Basic Data Base of six genuine signatures and eight statically skilled forgeries for each subject. The performance curve was obtained by evaluating the testing data base which has five genuine signatures and 22 statically skilled forgeries for each subject. Finally the dotted line shows the performance of the same common 10-feature set when not only the six genuine reference signatures but also the five genuine testing signatures were included in the procedure to search for a common feature set, and simultaneously the genuine testing data base also consists of the same 11 genuine signatures.

We conclude from Fig. 1a: 1) that using a large genuine data base when selecting common feature results in better classifier performance, 2) that our common feature sets achieve performance satisfactory for POS application, 3) that our feature selection algorithms provide optimum individualized subsets of 10 features that yield excellent discrimination, and 4) on-line signature verification systems that include dynamic features are superior, especially in POS applications where near-zero Type I error is needed.

The majority classifier with the optimal individualized 34-feature set provided the overall optimum performance relative to any size n of the subset of features selected from our 42 features when the feature selection algorithm used only genuine signatures. When both genuine and forgery data are available, the performance of subsets of 24 individually selected features is the best among subsets of features of any dimension selected from our 42 feature set. These results shows that forgery data are desirable but not essential for feature selection; forgery data avail us of improved performance and simpler verifier structure.

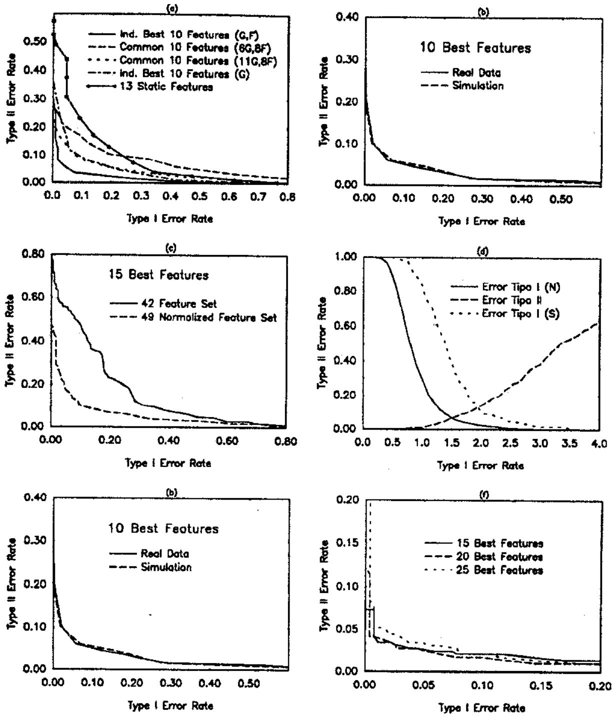

Fig. 1. Performance comparison of the majority classifiers. (a) some individual and common majority classifiers; (b) real vs. simulated data; (c) 42 and 49 feature sets; (d) error rate vs. threshold; (e) presoft majority classifiers; (f) prehard majority classifiers.

In order to validate the efficacy of our statistical model, the performance of a majority classifier based on simulated data generated by the model described in Section 5 was compared to that obtained from the real data. As shown in Fig. 1b, for the optimal 10 feature set the simulated results closely match those of the real data. Similar results were observed on most subsets of different orders, except for cases of subsets with very small order, say five features, and that with very large order, say 42 features. However, the largest discrepancy in equal-error-rate performance only barely exceeded 5%. A possible explanation for this is that some features, such as the number of pen-ups and the number of dots, cannot be well-approximated by Gaussians. The performance curve of real data in Fig. 1b was obtained from testing 1,000 genuine signatures all collected from the same subject and 325 statically skilled forgeries collected from 13 forgers. By comparing Fig. 1b with Fig. 1a, we conclude that our statistical model is a feasible tool not only for computing individual asymptotic performance but also for testing new classifier designs and reducing the burden of collecting extensive samples of raw signatures.

Fig. 1c shows the performance of the majority classifier using subsets of 15 best features selected from the 42 and 49 feature sets, and tested by the fast genuine signatures. The comparison strongly suggests that reliable signature verification systems require normalized features in order to provide satisfactory performance in the presence of significant variations in writing speed. Perhaps most importantly, the performance curves in Fig. 1c support the validity of the assumptions made in Section 3 when we introduced the normalized feature set.

Fig. 1d shows the performance of a majority classifier versus decision threshold for the Fast Data Base and the Global Data Base using the best individualized 15 features selected from the 49-feature set. For POS applications we choose a decision threshold of 2.5; this yielded a Type I error of less than 1% for the normal speed signatures(N) and a Type II error of 20%. Note that the **same** decision threshold results in 5% Type I error(S) for the fast signatures. It is worth mentioning that in practice we would have a degradation much smaller than 4% because subjects write their signatures fast relatively rarely. Also, we expect that they will be willing to tolerate a somewhat higher rate of rejection of signatures they scrawl in great haste. We conclude from Fig. 1d that using a threshold in the interval from 2.5 to 3.0 for the best 15 features from the set of 49 normalized features results in a majority classifier that yields Type I and Type II errors suitable for POS applications robustly with respect to the speed of genuine signature.

The experimental results reveal that only 0.5% of the genuine signatures had writing durations that deviated from the subject's average writing time by more than 18% ($\beta = 0.18$). Under normal conditions few if any people have signature writing times that deviate from their nominal value by more than 20%. Fig. 1e and-Fig. 1f show, respectively, the performance of the presoft and prehard majority classifier of Section 4.1. Comparing Fig. 1e and Fig 1f to Fig 1c shows that notable improvements are achieved using modified majority decision rules. The prehard majority classifier provides the best performance among those studied in this work: 2.5% equal error rate and, more importantly for POS, an asymptotic performance of 7% false acceptance rate at "zero" false rejection rate using only 15 individualized parameter features selected from the 49-feature set. Moreover, this was achieved despite the unrealistically demanding condition that many of the forgers were permitted to produce imitations that matched almost perfectly in signing time in addition to being given the opportunity to practice static forgeries extensively. In particular, the presoft majority classifier detected about 50% of the timed forgeries while successfully classifying 99% of the genuine signatures as shown by the performance curve in Fig. 2.

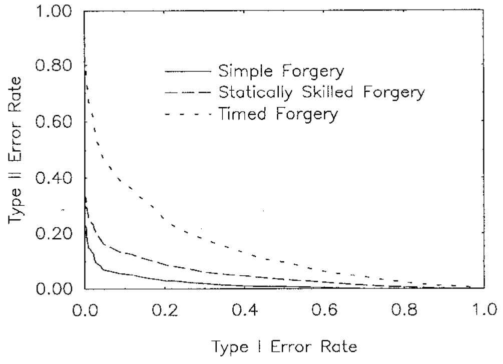

Fig. 2. Error rates vs. types of forgeries.

Our findings provide the basis for an adaptive method and system for real time verification of dynamic human signature [14] suitable for POS applications in regard to performance, memory and cost; the mean genuine feature values are easily adapted to changes in the signature of an individual with time. Tests on our verification system show that it is suitable for on-line implementation. Using a PC with a 486-processor, the verification algorithms require less than 1.5 s verification time, even without any effort at optimizing the algorithm code. Chip-based special purpose hardware in a commercial realization of the system would run considerably faster. A smart card implementation also appears feasible.

Appendix A – 42 Feature Set

Before listing the 42 and 49 feature sets for convenience we introduce the following definition and notations:

$$\begin{aligned}
x_0 &= x(\text{1st pen down})\\
y_{end} &= y(\text{last pen up})\\
y_{max} &= \text{maximum } y\\
d_x &= \left|x_{\max} - x_{\min}\right|\\
y_0 &= y(\text{1st pen down})\\
x_{max} &= \text{maximum } x\\
y_{\min} &= \text{minimum } y\\
d_y &= \left|y_{\max} - y_{\min}\right|\\
x_{end} &= x(\text{last pen up})\\
x_{min} &= \text{minimum } x\\
\Delta_x &= \textit{total shift of } (x) \text{ in pen downs}\\
\Delta_y &= \text{total shift of } (y) \text{ in pen downs}
\end{aligned}$$

1. Avg. writing speed ($\overline{v}$)
2. Max. writing speed (v_{max})
3. Time of max speed ($t(v_{max}$)
4. t(1st pen move) - t(1st pen down)
5. Total signing duration (T_s)
6. Total pen down duration (T_w)
7. Min horiz. writing speed
8. Time of Feature 7
9. Total dots recorded
10. Average dot execution time
11. Number pen ups
12. Time of 2nd pen down
13. Initial direction
14. Dir. from 1st to 2nd pen down
15. Dir. of 1st pen down to 2nd pen up
16. Init. dir. after 2nd pen down
17. Dir. from 1st pen down to last pen up
18. Duration of $v_x > 0$
19. Duration of $v_x < 0$
20. Duration of $v_y > 0$
21. Duration of $v_y < 0$
22. Average positive v_x
23. Average negative v_x
24. Average positive v_y
25. Average negative v_y
26. Total $v_x = 0$ events recorded
27. Total $v_y = 0$ events recorded
28. Max v_x — avg v_x
29. Max v_y – avg v_y
30. Max v_x – min v_x
31. Max v_x – min v_y

32. Max v_y — min v_y
33. t(x_{max}) T_w
34. t(x_{min})/T_w
35. $(x_{max} - x_{min}) \times (y_{max} - y_{min}) = A_{min}$
36. Signature length/A_{min}
37. $x_0 - x_{min}$
38. $x_{end} - x_{max}$
39. $x_{end} - x_{min}$
40. $(x_{max} - x_{min})/(y_{max} - y_{min})$
41. Standard deviation of x
42. Standard deviation of y

Appendix B– 49 Normalized Feature Set

1. T_w/T_s
2. Time of max v/T_w
3. Average v/maximum v
4. Duration of $v_x > 0)/T_w$
5. Duration of $v_x < 0)/T_w$
6. Duration of $v_y > 0)/T_w$
7. Duration of $v_y < 0)/T_w$
8. Duration of $v_x > 0$ in pen ups $(T_s - T_w)$
9. Duration of $v_x < 0$ in pen ups/$(T_s - T_w)$
10. Duration of $v_y > 0$ in pen ups/$(T_s - T_w)$
11. Duration of $v_y < 0$ in pen ups)/$(T_s - T_w)$
12. Normalized initial direction (d_x/d_y)
13. Dir. from 1st to 2nd pen down/(d_x/d_y)
14. Dir. 1st pen down to 2nd pen up/(d_x/d_y)
15. Dir. after 2nd pen down/(d_x/d_y)
16. Dir. before last pen up/(d_x/d_y)
17. Dir. 1st pen down to last pen up/(d_x/d_y)
18. Total dots recorded.
19. Number of pen ups
20. Time of 2nd pen down/T_s
21. Total dot execution time/T_w
22. Time of max v_y/T_w
23. Time of min v_y/T_w
24. Time of max v_x/T_w
25. Time of min v_x/T_w
26. Total $v_x = 0$ events recorded
27. Total $v_y = 0$ events recorded
28. Number of quadrant slope changes
29. $\overline{v}$ /max v_x
30. $\overline{v}$ /max v_y
31. Min. $v_x/\overline{v}_x$
32. Min. $v_y/\overline{v}_y$
33. First time instance of $v \neq 0$
34. $A_{min}/(\Delta_x{*}\Delta_y)$
35. Signature length/A_{min}
36. $(x_0 - x_{max})/\Delta_x$
37. $(x_0 - x_{min})/\Delta_x$
38. $(x_{end} - x_{max})\ \Delta$
39. $(x_{end} - x_{min})/\Delta_x$
40. $(y_0 - y_{max})/\Delta_y$
41. $(y_0 - y_{min})/\Delta_y$
42. $(y_{end} - y_{max})/\Delta$
43. $(y_{end} - y_{min})/\Delta$
44. $[(x_{max} - x_{min})/(y_{max} - y_{min})]/[\Delta_x/\Delta_y]$
45. Standard deviation of x/Δ_x
46. Standard deviation of y/Δ_y
47. Duration pos. slopes/durat. neg. slopes
48. Writ. Dist. in quad. 1 & 3/that in 2 & 4
49. Duration of high curvature time/T_w

Acknowledgment

This work was supported in part by the Brazilian Science Agency (CNPq), the State University of Campinas (UNICAMP), and the National Science Foundation under grant NCR-8903288.

References

[1] R. Plamondon and G. Lorette, "Automatic Sgnature Verification and Writer Identification—The State of The Art," *Pattern Recognition,* vol. 22, no. 2, pp. 107-131, 1989.

[2] F. Leclerc and R. Plamondon, "Automatic Signature Verification: the State of The Art," *Int'l J. Pattern Recognition and Artificial Intelligence,* vol. 8, no. 3, pp. 643-660, 1994.

[3] G. Dimauro, S. Impedovo, and G. Pirlo, "Component-Oriented Algorithms for Signature Verification," *Int'l J. Pattern Recognition and Artificial Intelligence,* vol. 8, no. 3, pp. 771-793, 1994.

[4] R. Plamondon, "The Design of an On-Line Signature Verification System: From Theory to Practice," *Int'l J. Pattern Recognition and Artificial Intelligence,* vol. 8, no. 3, pp. 795-811, 1994.

[5] W. Nelson, W. Turin, and T. Hastie, "Statistical Methods for On-Line Signature Verification," *Int'l J. Pattern Recognition and Artificial Intelligence,* vol. 8, no. 3, pp. 749-770, 1994.

[6] M.C. Fairhurst and P. Brittan, "An Evaluation of Parallel Strategies for Feature Vector Construction in Automatic Signature Verification Systems," *Int'l J. Pattern Recognition and Artificial Intelligence,* vol. 8, no. 3, pp. 661-678, 1994.

[7] L. Yang, B.K. Widjaja, and R. Prasad, "Application of Hidden Markov Model for Signature Verification," *Pattern Recognition,* vol. 28, no. 2, pp. 161-170, 1995.

[8] M. Achemlal, M. Mourier, G. Lorette, and J.P. Bonnefoy, "Dynamic Signature Verification" *Security and Protection in Information Systems,* A. Grissonnanche ed., pp. 381-389, B. V. (North-Holland), *IFIP,* Elsevier Science, 1989.

[9] J.P. Bonnefoy, P. Jounet, G. Lorette, and M. Gaudaire, "Reconnaissance automatique, en temps reel de signatures manuscrites: definition et mise en oeuvre dune methodologie generale," *Proc. Third Congres Rec. des Formes et Intel. Artif.,* pp. 267-275, Nancy, 1981.

[10] H.D. Crane and J.S. Ostrem, "Automatic Signature Verification Using a Three-Axis-Force-Sensitive Pen," *IEEE Trans. Systems Man, and Cybernetics,* vol. 12, pp. 329-337, 1983.

[11] E. Kishon, T. Hastie, M. Clark, and J. Fan, "A Statistical Model for Signature Verification," *Proc. IEEE Conf. Systems, Man, and Cybernetics,* Charlottesville, Va., 1991.

[12] E. Aviczer, "On-Line Signature Verification Model," M Eng Project Report, Cornell Univ. School of Electrical Engineering, May 1991.

[13] L.L. Lee, "On-Line Systems for Human Signature Verification," PhD thesis, Cornell Univ. School of Electrical Engineering, Jan. 1992.

[14] L.L. Lee and T. Berger, "Adaptive Method and System for Real Time Verification of Dynamic Human Signatures," U.S. Patent Application No. 07/790, 965 allowed Feb. 8, 1996.

[15] G. Lorette, "On-Line Handwritten Signature Recognition Based on Data Analysis and Clustering," *Proc. Seventh Int'l Conf. Pattern Recognition,* vol. 2, pp. 1,284-1,287, Montreal, 1984.

[16] Y. Sato and K. Kogure, "On-Line Signature Verification Based on Shape, Motion, and Writing Pressure," *IEEE Proc. Sixth Int'l Conf. on Pattern Recognition,* pp. 823-826, Munich 1982.

[17] L.L. Lee and T. Berger "Optimization of a Signature Verification System Using a Neural Network," *Proc. Int'l Conf. Artificial Neural Net—ICANN,* Amsterdam, Sept. 13-16, 1993.

[18] L.L. Lee and T. Berger "On Two-Pattern Classification Using Neural Networks," *Proc. Int'l Conf. Signal Process—ICSP'93,* Beijing, China, Oct. 26-30, 1993.

[19] Y.J. Chiu, "On-Line Signature Verification," Master of Engineering Report, Cornell Univ. School of Electrical Engineering, Jan. 1992.