Dynamic Signature Verification System Using Stroked Based Features

Tong Qu, Abdulmotaleb El Saddik, Andy Adler
MCRLab, VIVA Lab, University of Ottawa,
Ottawa, Ontario, Canada
[tqu, elsaddik, adler]@site.uottawa.ca

Abstract

This paper presents a novel feature-based dynamic signature verification system. Data is acquired from a Patriot digital pad, using the Windows Pen API. The signatures are analyzed dynamically by considering their spatial and time domain characteristics. A stroke-based feature extraction method is studied, in which strokes are separated by the zero pressure points. Between each pair of signatures, the correlation comparisons are conducted for strokes. A significant stroke is discriminated by the maximum correlation with respect to the reference signatures. The correlation value and stroke length for the significant strokes are extracted as features for identifying genuine signatures against forgeries. The membership function and classifier are modeled based on the probabilistic distribution of selected features. Experimental results were obtained for signatures from 20 volunteers. The current 6- feature based signature verification system was calculated to have a false accept rate of 1.67% and false reject rate of 6.67%.

1. Introduction and related work

Automatic signature verification is electronic analysis of a person's signature is used to determine if that person is who they claim to be. There are two types of signature verification – static and dynamic. Static verification methods are based on the limited information available solely from the basic shape and structural characteristics of the signature represented as a two-dimensional image (2-D image as input from a camera or scanner). A dynamic signature verification system gets its input from a digitizer or other, usually pen-based, dynamic input device. The signature is then represented as one or several time-varying signals. Dynamic verification not only looks at how the appearance of the signature, but also the process an individual uses to form the signature. This method relies on features, which define the pattern of execution of the signature (for examples, pen motion, pen velocity, stroke sequencing, and so on). So they consequently are able to exploit information, which is not available in the image, but could be characteristic of an individual signer, and therefore offer the potential for greater accuracy.

Many projects have been carried out on dynamic signature verification with varying degrees of success. Plamondon et al. summarized a comprehensive survey [1] with its accompanying bibliography [2,3,4]. However, an overview of recent publications since 1993 does not show a clear breakthrough either in signature verification techniques or in the kind of analysis and characteristic selection process [1]. A variety of new techniques suggests either adjustments or combinations of known methods and has been used with more or less success. Various dynamic verification techniques have been tested based on different conditions. These can be classified as: time warping or dynamic matching [5,6], signal correlation [7], probabilistic classifiers [8], neural network [9,10], hidden Markov models [11], Euclidian or other distance measure [12], and hierarchical approach combining a few methods [13].

This paper presents a novel signature verification algorithm based on extracted features by locating significant strokes. Data is acquired using the Patriot digital pad (figure 1); however, this pad uses the standard Windows Tablet input API [14], and our results can be straightforwardly extended to other similar devices. We extracted features based on locating significant strokes. Not only stroke-based features, but also for features such as signing time duration and average writing speed were used in current verification system. The membership function and classifier are modeled based on the feature's probabilistic characteristics. When evaluating a test signature, its corresponding feature values are calculated and sent to a probabilistic classifier, which compared the feature value with those of previously obtained reference signatures.

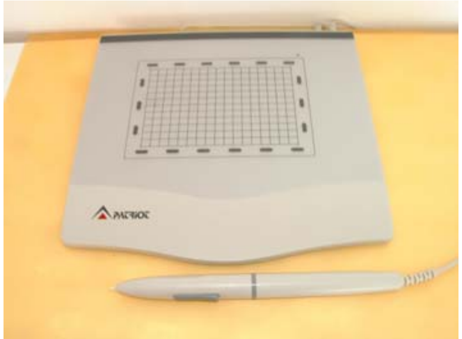

Figure1. Patriot digital pad

2. Data acquisition and signature processing

In the proposed system, each user is required to construct his (or her) signature template at first. Users must repeat their specimen signature several times in the "same" manner, which means using the "same" speed, pressure, strokes, timing sequence etc. Before recording the signatures, users should practice the signing process until they feel they can recreate their signature easily and comfortably on the digital pad. In order to obtain a signature template, which can reflect the long-term manner of a user's signing process, a set of this user's signatures is recorded at different time and different situations (when he feel happy, sad, excited, or tired, etc). 20 volunteers took part in the data acquisition and their signatures were collected over a period of three months. All the collected genuine signatures were classified into two classes. One is used for training signature template and the other is used for signature verification. In order to study the effect of the number of training signatures, a few volunteers signed as many as 60 signatures, while others only recorded 15 signatures. Some volunteers were asked to forge other's genuine signatures. They were asked to study not only the 2-D structures of the genuine signature but also the dynamic signing process. 5 or 8 forgeries were obtained for each signature template.

Repetitions of signatures assist the algorithm to account for variability of the signature with respect to time and other variations. Later, when the same user (or someone claiming to be that particular user) presents for authentication, the features extracted from his test signature are compared with that of the features in the reference set belonging to that particular person under test. If the signature has indeed come from the original user, then the comparison process should yield an approval output, while an attempt at forgery should be blocked by the system.

In this system, the Patriot digital pad is connected with a personal computer through a standard serial port. The digital pad enables recording the pen tip coordinates and pen tip pressure. The raw data are measured at the serial port and the measurements are registered every millisecond. The signature's spatial and pressure information can be obtained directly, using the windows tablet API [14]. They represent the horizontal (x) & vertical (y) coordinates of the pen tip and the pressure applied during signing process. In addition, by taking the sampling rate into account, we can relate this spatial information to the time domain. These generated signals present the information for the pen tip speed, acceleration and azimuth angle. These components constitute the dynamic signature.

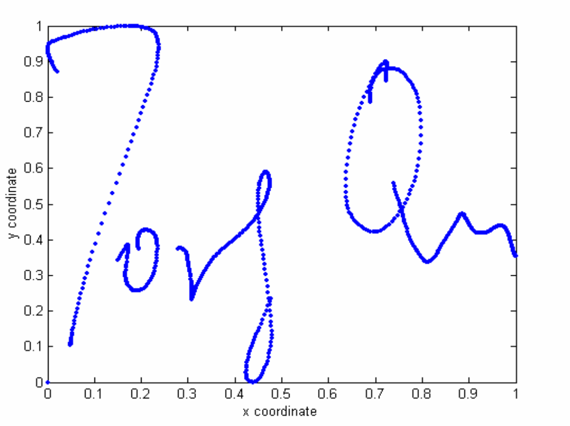

Figure2. A sample signature

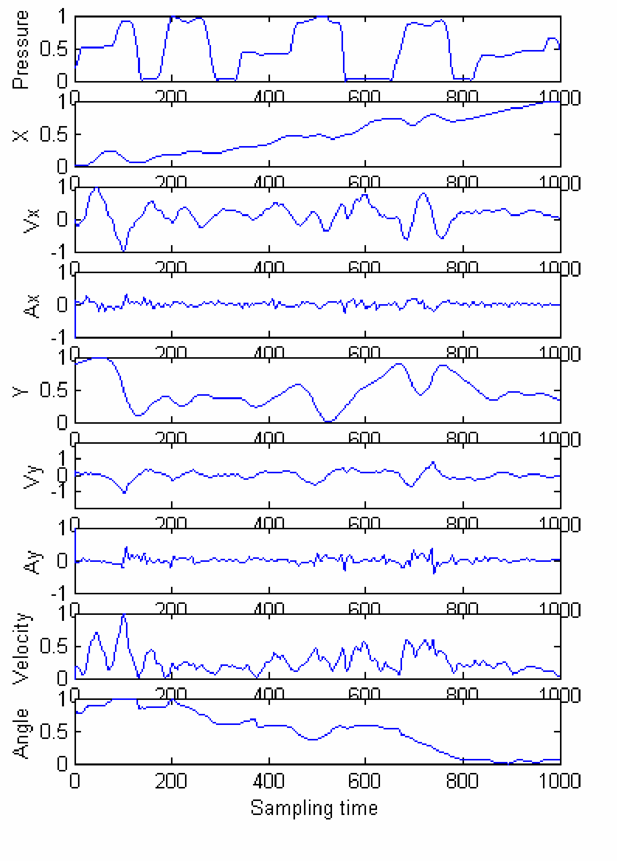

Figure3. Dynamic signatures representation

Pre-processing of raw dynamic signature data uses a filter to remove hardware noise. Then, the starting location, size, and total duration of the signature are normalized, so the signature verification is independent of these characteristics. The normalization process for a coordinate point in the signature is according to the formula:

$$Norm\_Value = \frac{Current\_Value - Origin\_Value}{\left| End\_Value - Origin\_Value \right|}.$$

Where $Norm\_Value$ represents the normalized value; $Current\_Value$, the current coordinate value; $Origin\_Value$, the first coordinate of the signature; and End_Value is the last coordinate point of the signature.

For a sample signature shown in Figure 2, the force, position, and velocity signals are normalized and plotted in Figure 3. Pressure is the pressure signal. X , V_x , and A_x are the pen tip displacement, speed, and acceleration in the horizontal (x) coordinate Y , V_y , and A_y represent the pen tip displacement, speed, and acceleration in the vertical (y) coordinate. Velocity is calculated from V_x and V_y . Angle represents the dynamic instantaneous azimuth angle of the pen tip movement.

3. Feature extraction

Features are symbolic or numeric entities that describe a pattern. For example, a feature for a static signature is the number of loops in the 2-D image, while a feature for a dynamic signature is the average writing speed. The complete signals (i.e., position, pressure, velocity, acceleration vs. time, etc.) can be represented by time domain functions whose values directly constitute the feature set. In addition, those parameters (such signing time, peak number, stroke sequencing, etc.) computed from the measured signals are another source of features.

The following features are calculated from the dynamic signature data:

- Total time during the signing process
- Average writing speed
- Pen-up time
- Maximum forward velocity
- Average velocity over x and over y
- Number of strokes
- Variance of pressure signal (or in 10 sliding window)
- Pressure changing in 10 sliding windows
- Number of pen ups and downs
- Direction at first pen down, first pen up
- Signature length
- Time of second pen down
- Number of sign changes in the x and y velocities and x and y accelerations
- Number of zero values in the x and y accelerations
- Total path length
- Mean or variance of the x and y displacement signal in 10 or 100 sliding windows

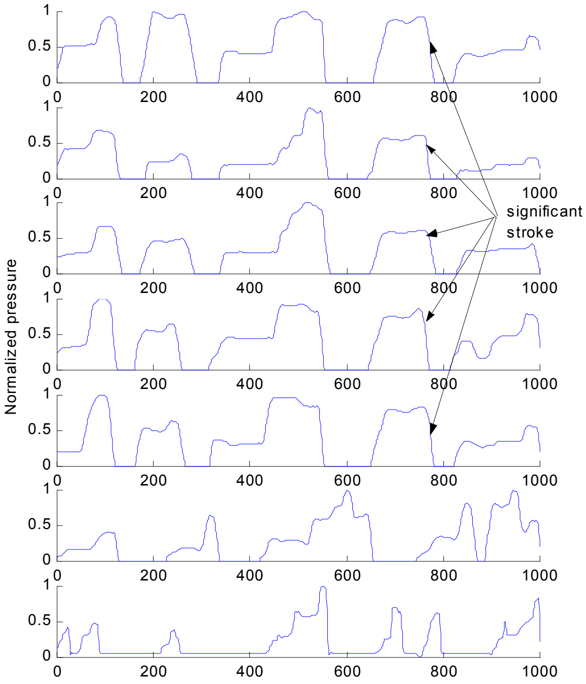

Figure 4. Stroke-based normalized pressure versus time of five genuine signatures and two forgeries. The 4th stroke in each genuine signature is the significant stroke.

In addition to these global features, we calculate a set of local features based on individual strokes. During signing, individual strokes can be distinguished by finding the points where there is a 1) decrease in pen tip pressure, 2) decrease in pen velocity, and 3) rapid change in pen angle. These points imply some internal characteristic of the pressure sequencing. Therefore, they can be used to locate the strokes for the dynamic signature. Visually, there often exists high similarity between the corresponding strokes of reference signatures, but much lower similarity between the strokes of genuine signatures and that of forgeries. Between each pair of signatures, the correlation comparisons are conducted for strokes. A significant stroke is discriminated by the maximum correlation between the reference signatures. Thus, the correlation value and stroke length for the significant stroke are extracted as features for identifying genuine signatures against forgeries.

In figure 4, the stroke-based pressure signals are compared between five genuine signatures and two forgeries. The same user signed the 5 genuine signatures, and others imitated the 2 forgeries. Even for the 5 references, different strokes exhibit different variations among the repetitions. The correlation coefficients between the strokes for all 5 genuine references were calculated for the data of figure 4. In this example, the 4th–4th stroke pairs have the highest correlation. This suggests the 4th stroke reflects the signer's internal characteristic, and it should have better ability to keep such characteristic than other strokes when this signer repeats his signing. It is convenient to name such kind of stroke as a significant stroke for a signature template. Different individuals maybe have different significant strokes for their dynamic signatures. In the example in figure 4, the 4th stroke is the significant stroke and its correlation values are listed (in table 1) not only for the genuine-genuine pairs, but also for the forgery-genuine pairs. For the genuine-genuine pairs, the significant stroke's correlation values (e.g. 0.9199 for G1-G2 pair) are higher than those of genuine-forgery pairs (e.g. 0.5561 for G1-F1 pair). Furthermore, the significant stroke's average correlation value for all the genuine-genuine pairs should be higher than those of the genuine-forgery pairs. In this case, for all the genuine-genuine pairs, the significant stroke's average correlation value is 0.9670. It is higher than that of genuine-forgery pairs. We select the mean significant stroke of all the references as a feature in the template. If F1 is a test signature, the 4th stroke's average correlation value between F1 and all the references is only 0.6302 (0.1706 for F2, both are far from the 0.9670).

In addition, we also use other features related to significant strokes such as stroke length, and stroke duration time. Note here, different signals (e.g. velocity signal) may have different significant strokes for the same user.

Table 1. 4th stroke's correlation between the signatures in figure 3

	G1	G2	G3	G4	G5
G1	1	0.9199	0.9830	0.9575	0.9846
G2	0.9199	1	0.9595	0.9678	0.9643
G3	0.9830	0.9595	1	0.9612	0.9834
G4	0.9575	0.9678	0.9612	1	0.9889
G5	0.9846	0.9643	0.9834	0.9889	1
F1	0.5561	0.6729	0.5573	0.7267	0.6379
F2	0.1508	0.1454	0.0815	0.2807	0.1946

4. Feature distribution for signature classifier

Based on our observations that most of the feature values tend to be clustered about a mean value with a certain variance that is characteristic to a certain user, we use Gaussian density to model the distributions of these features. Figure 5 shows the average writing speed for 40 signatures by same user, illustrating this effect. Since N signatures give us N values of a particular feature (e.g. N average writing speed), we fit a Gaussian density function to these values. The unbiased estimator for the mean and variance [15] are,

$$\mu_i = \sum_{j=1}^{N} \frac{X_j}{N} \text{ and } Var_i = \sum_{j=1}^{N} \frac{(X_j - \mu)^2}{N-1},$$

respectively. Where the X_j are the feature values, and i varies from 1 to N. Thus, for a given user, the (μ_i, Var_i) is a mean and variance which describe the behavior of a feature. For a M-feature system we have: (μ_1, Var_1), (μ_2, Var_2), $(\mu_3, Var_3), \ldots, (\mu_M, Var_M)$. Value s are computed for each user. When a user's authenticity is to be verified, the set of mean and variance reference values corresponding to the user in test is used.

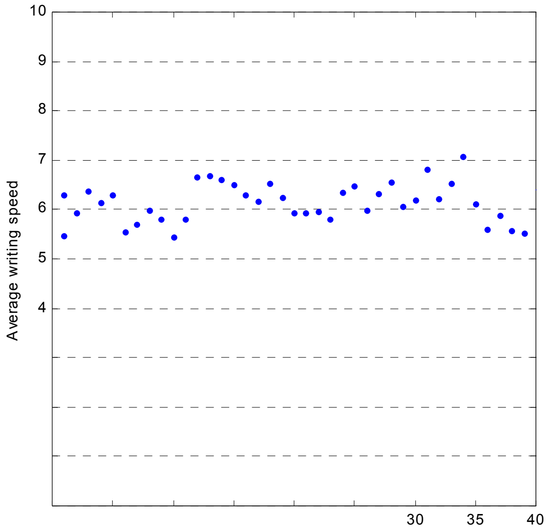

Figure5.Average writing speed vs. number of signatures

Signature verifications accounts for the similarity in signatures produced by the same user, but need to allow for a certain variability. The amount of variation allowed varies by user and for each feature. According to the equation of above, an unbiased estimator for the mean and variance, by adding the number of reference signatures (N), the experimental mean (μ_i) and experimental variance (Var_i) will converge to the true mean and variance of a feature. There is a trade off between N and accuracy of the experimental mean and variance. μ_i reflects the mean value of a corresponding feature i. Var_i introduces a threshold value, which is illustrated in figure 6. This value is selected independently for each given user and feature. For a person whose signature is very constant, the threshold can be kept low, and the variations of subsequent signatures are expected to be small. For higher variations among repetitions for a user, a higher threshold is required.

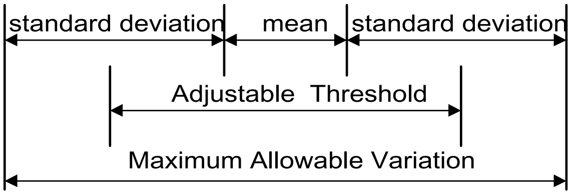

Figure 6. Diagram of threshold adjustment

We need an optimal N, which allows us to maintain certain accuracy without large signature training set. For example, for the average writing speed feature, table 1 shows the (μ_i, Var_i) by increasing N for the current system. Since (μ_i, Var_i) doesn't exhibit significant changing when increasing N, so we select $(\mu_i, Var_i) \approx$ (6.0439,0.1020) to approximate the unbiased estimators for the mean and variance. We set $N = 5$ for most users in the current verification system.

Table 2. Comparison of (μ_i, Var_i) versus N

N	5	10	20	30	50
μ_i	6.0439	5.8694	6.1056	6.1234	6.1280
Var_i	0.1020	0.0989	0.1472	0.1176	0.1568

Finally, to verify the identity of an unknown user, the following processing is implemented: for each feature value of the test signature, the system checks to see if it lies within the allowed range of that reference feature. The variance estimator determines the allowed variation range, and the threshold assigned limits it. If the test feature value falls within this range, the test is assigned a weight (e.g. 1 or 0 for inside or outside the threshold, respectively). The signature classifier discriminates the genuine signature against the forgeries by evaluating the entire accumulated value in the assignment of a percent match of the test signature compared to the signature template.

5. Signature verification experiment

An experiment was performed to evaluate the current 6-feature verification system based on their probabilistic classifier. The features used are: correlation value of the significant stroke in pressure signal; the duration of the significant strokes; average writing speed, total time during the signing process, variance of pressure signal in 10 sliding windows, mean of the x displacement signal in 100 sliding windows. False rejection rate (FRR) and false acceptance rate (FAR) are measured to evaluate the performance of the system [16].

A total of 240 signatures, split into 130 reference and 110 test signatures, from 10 volunteers were used in this experiment. In order to study the training effect by the number of signatures, the first volunteer signed 60 signatures and the second recorded 10 signatures. For the rest 8 volunteers, each performed 5 signatures to train their signature template (we set $N = 5$ described above). In addition, the other 20 training signatures are used to adjust the threshold. For a feature i, the basic threshold is set to be $2\sqrt{Var_i}$. Furthermore, it was adjusted by additional 2 references, if needed, until either signature was accepted, or the maximum threshold value was reached. Thus, there were three training sets of sizes 60, 10 and 5 training signatures. In addition, each set has 2 signatures to adjust the threshold value.

Forgery signatures were created several volunteers asked to try to forge others signatures. They began to create forgeries by studying the 2-D structures of the genuine signature. The genuine signers also showed them the dynamic signing process of the genuine signature. For each volunteer, his signature was forged 5 times by other volunteers.

Signatures vary to a degree among repetitions. It is possible that a given signature, even though authentic, varies so much from the template signature that it is judged by the system as a forgery, resulting in a false rejection. An ideal signature verification system would never reject an authentic signature. In practice, the false rejection rate (FRR) of a system is to be reduced to the smallest possible. In our experiment, 60 sample authentic signatures were obtained. The system then compared these authentic signatures to the template, 56 of the 60 authentic signatures were correctly approved by the system, giving a FRR of 6.67%For the template trained by 60 signatures, and all the 6 test genuine signatures were approved. This result suggests that a large training set should improve the algorithm performance. Since one genuine signature was rejected by the template which is trained by 10 references, which suggests that a 10-signature reference set does not have a better training effect over a 5-signatures reference set, so it is reasonable for us to choose $N = 5$ as the training signatures.

To study the system performance on identifying the forgeries, 50 forgeries by other volunteers and 10 randomly forgeries were applied to check the system. Fifty-nine forgeries were accurately rejected by the system. The only one accepted forgery is for a user whose signatures are not constant. This results in a false acceptance rate of 1.67%.

The system's performance throughout the experiment was quite well. This degree of accuracy demonstrates that some features are constant for every signer. It also shows that they do not necessarily have to be the same for everyone, so the template signature should be weighted differently for each signer.

6. Conclusions and future work

A signature verification system was successfully designed, developed, and tested. It is compact enough to fit in a small microprocessor based package, yet accurate enough to effectively approve authentic signature and deny forged signatures. A stroke-based feature extraction approach is studied and significant strokes features are extracted from the force, pressure, and velocity signals. Strokes are separated by the zero pressure points. Between pair of signatures, the correlation comparisons are conducted for strokes. A significant stroke is discriminated by the maximum correlation between the reference signatures. Thus, the correlation values for the significant stroke are extracted as features for identifying genuine signatures against forgeries. This method was proved to be effective for current 6-feature based verification system. Experimental results indicate a false reject rate of 6.67% and false accept rate of 1.67%. In current system, fixed threshold is used, so only fixed FAR and FRR values were obtained. In the future, a variable threshold will be used to calculate the FAR and FRR data for the detection error tradeoff curve. In addition, more features will be evaluated and implemented in the updated systems.

7. References

[1] R. Plamondon and S. Srihari, "On-line and off-line handwriting recognition: a comprehensive survey", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol 22, No. 1, Jan. 2000

[2] R. Plamondon and G. Lorette, "Identity verification from automatic processing of signatures: Bibliography," in *Computer Processing of Handwriting*, R. Plamondon and C.G. Ledham Eds, Singapore: world Sccientific, pp. 65-85, 1990

[3] R. Plamondon, *Patten Recognition*, *special issue on automatic signature verification*. Vol. 31, No. 11, pp. 1589-1600, Nov. 1998

[4] F. Leclerc and R. Plamondon, "Automatic signature verification: The state of the art: 1989-1993," *Int'l Journal of Pattern Recognition and Artificial Intelligence*, Vol.8, No.3, pp. 643-660, June 1994

[5] R. Martens and L. Claesen, "On-line signature verification by dynamic time-wrapping", *Proceedings 13th Int'l Conf. Pattern Recognition*, pp. 38-42, Vienna, 1996

[6] B. Wirtz, "Stroke-based time warping for signature verification", *Proceedings of Third Int'l Conf. Document Analysis and Recognition (ICDAR'95*), pp.179-182, Montreal, Canada, Aug. 1995

[7] V.S. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE*, Vol. 85, No.2, pp. 215-240, 1997

[8] L.L, Lee, T. Berger, and E. Aviczer, " Reliable on-line signature verification systems," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, Vol. 28, No. 6, pp. 643-647, June 1996

[9] C.G. Wolf, and P. Morrel-Samuels, "The use of hand-drawn gestures for text editing", *Proc. of Int'l Journal of Man-Machine Studies*, Vol.27, pp. 91-102, 1987

[10] L.L. Lee, "Neural approaches for human signature verification", *Third Int'l Conf. on Document Analysis and Recognition,* Vol. 2, pp.1055-1058, Montreal, Aug. 1995

[11] J.G.A. Dolfing, E.H.L. Aarts, and J.J.G.M. Van Oosterhout, "On-line verification signature with hidden Markov models", *Proceedings of 14th Int'l Conf. Pattern Recognition,* pp. 1309-1312, Brisbane, Australia, Aug. 1998

[12] T. Matsuura and T.S. Yu, "On-line signature verification by IIR system", *Proceedings of 5th Int'l Workshop Frontiers in Handwriting Recognition (IWFHRV),* Colchester, England, pp. 413-416, Sep. 1996

[13] X. -H, Xiao and R. -W. Dai, "On-line Chinese signature verification by matching dynamic and structural features with a quasi-relaxation approach", Proceedings *of 5th Int'l Workshop Frontiers in Handwriting Recognition (IWFHRV),* Colchester, England, pp. 475-478, Sep. 1996

[14] Windows tablet API, www.lcs-telegraphics.com

[15] A. Leon-Garcia, *Probability and random processes for electrical engineering* to signal processing, Addison-Wesley, 1989

[16] Biometrics Working Group, "Best practices in testing and reporting performance of biometric devices", version 1.0, Jan. 2000, www.cesg.gov.uk