2009 10th International Conference on Document Analysis and Recognition

On-Line Signature Verification: Directional Analysis of a Signature Using Weighted Relative Angle Partitions for Exploitation of Inter-Feature Dependencies

Muhammad Talal Ibrahim[1], Matthew Kyan[2],M. Aurangzeb Khan[3],
Khurram Saleem Alimgeer[4], Ling Guan[5]
[1,2,5]Ryerson Multimedia Research Lab, Ryerson University, Toronto, Canada.
[3,4]Dept. of Electrical Engineering, COMSATS Institute of Information Technology, Islamabad, Pakistan.
[1]muhammadtalal.ibrahi@ryerson.ca, [2]mkyan@ee.ryerson.ca, [3]aurangzeb_niazi@comsats.edu.pk,
[4]khurram_saleem@comsats.edu.pk, [5]lguan@ee.ryerson.ca

Abstract

In this paper, we propose a new directional analysis tool for On-line signatures that decomposes the given input signature into directional bands on the basis of relative angles. Our directional analysis tool takes the independent trajectories (horizontal and vertical) as an input and then decomposes them into directional bands on the basis of relative angles. We have used both user-dependent and user-independent thresholds for selecting an optimal number of partitions for each signer. By decomposing signature trajectories based upon relative angles of an individual's signature, the resulting process can be thought of as one that exploits inter-feature dependencies . In the verification phase, distances of each partitioned trajectory of a test signature are calculated against a similarly partitioned template trajectory for a known signer. Each partition is then weighted based on its quality and quantity. Experimental results demonstrate the superiority of our approach to On-line signature verification in comparison with other techniques.

1 Introduction

Biometrics can be classified into two main classes: *physical* and *behavioral* based on the type of biometric trait used. Signature is a behavioral biometric that is likely to change over a period of time. Behavioral biometric systems have higher error rate than the those based on physical traits. This paper deals with the On-line signature verification where each signature is represented by time varying signals acquired from a wacom tablet or similar and verification is based on extracted dynamic features such as such as velocity, acceleration, curvature, pressure, total signature time, RMS speed, Average writing speed, etc. [13], [9], [10], [1], [7] in addition to overall shape. The availability of more unique behavioural traits thus offers the potential to achieve much lower error rates than that in Off-line signature verification where verification is based on only the shape of the signature.

In this paper, we have provided a novel approach to On-line signature verification whereby directional analysis of a signature is performed by calculating the relative angles between the sample points along its trajectory. Partitioning into *N* groups based on relative angles futher exploits natural dependencies between individual directional trajectories. For the verification purpose, we also present a new weighted partition criteria that allows each partition to play a varying role in the verification process according to a data-dependant weight.

The paper is organized as follows. The second section deals with the acquisition of signature data and preprocessing steps. The third section is dedicated to the design and structure of our proposed system and the final section presents experimental results and concluding remarks.

2 Data Acquisition and Preprocessing

For the experimental process, we have used a database of 25 different signers, and for each signer 600 genuine signatures, and 250 highly skilled forgeries were collected over a period of three months in order to capture different nuances of each signer [5], [4]. However, we have also used a subset of this database consisting of 25 genuine and 25 forgery signatures for each signer which reflects a more realistic number of signatures typically available for training. In addition, one public database (MCYT [2]) is used to draw comparison with existing methods.

To account for likely variances in the size and orientation of signatures as imparted through a digitising interface such as a tablet, we have followed a number of preprocessing steps as suggested in [5], [4] to make all the signatures of the ith signer to be translation, rotation and scale invariant. Details of each preprocessing step is given below.

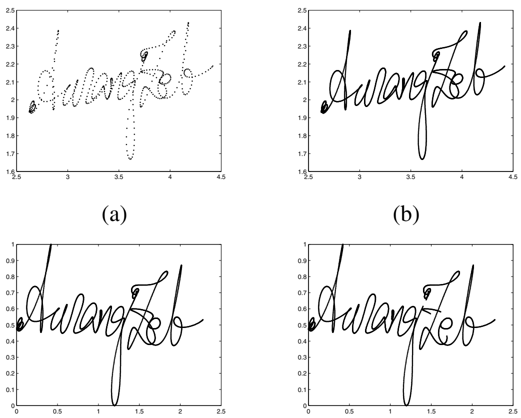
2.1 Smoothing using Cubic Spline

Due to the low sampling rate of the data acquisition device (100 samples/sec), there is a need to smooth the resulting jagged trajectories [3]. For this purpose, we have used cubic spline which not only helps in smoothing the trajectories independently but also provides us another dynamic feature (i.e velocity) which is the first derivative of cubic spline [3, 5]. Fig. 1(a-b) shows a signature before and after smoothing.

2.2 Translation, Rotation and Scaling

All of the signatures of ith signer are made translation invariant by subtracting the mean of each independent trajectory (horizontal,vertical) from its respective trajectory. In this way, the mean of each signature will be shifted to zero. Now, the next step is to make the signatures rotation invariant which is achieved by rotating the principal component (PC) of the jth signature of the ith signer to the angle of the PC of the base-signature b^i of the ith signer. PCs are calculated by using principal component analysis (PCA) [4]. Now the need of making all the signatures of ith signer scale invariant is achieved by

978-0-7695-3725-2/09 $25.00 © 2009 IEEE
DOI 10.1109/ICDAR.2009.113



(a) (b) (c) (d)

Figure 1. a) shape of the signatures before smoothing; b) shape of the signature obtained by plotting the smoothed horizontal trajectory against the smoothed vertical trajectory; c) signature after translation, rotation and scale invariance; d) signature after zero pressure removal

using the following pair of equations:

$$\begin{aligned} Ratio_j^i &= \frac{max(x_j^i)}{max(y_j^i)} \\ y_j^i &= \frac{y_j^i - min(y_j^i)}{max(y_j^i) - min(y_j^i)} \\ x_j^i &= \left(\frac{x_j^i - min(x_j^i)}{max(x_j^i) - min(x_j^i)}\right) \times Ratio_j^i \end{aligned} \quad (1)$$

After making all the signature scale invariant, the vertical trajectories of each signature will be scaled from 0 to one and the horizontal trajectories will be scaled from zero to the $Ratio_j^i$. Fig. 1 (c) shows the result after translation and scaling.

2.3 Zero Pressure Removal

In On-line signature acquisition, tablet samples are captured even when the pen tip is close to the surface of the tablet without touching the surface. The spatial areas, velocity and pressure of signature corresponding to such regions (captured between the pen-up and pen-down) are named zero pressure regions. Authors in [4] proposed a method of removing spatial areas corresponding to zero pressure regions. Their method was used to calculate a threshold value $zero_j^i$ based on the pressure profile of each signature of ith signer by using the following pair of equation:

$$\begin{aligned} std_j^i &= \sqrt{\frac{1}{M}\sum_{m=1}^{M}(z_j^i(m) - \frac{1}{M}\sum_{m=1}^{M} z_j^i(m))^2}, \\ zero_j^i &= \frac{1}{M}\sum_{m=1}^{M} z_j^i(m) - std_j^i, \end{aligned} \quad (2)$$

where M is total number of samples in a pressure profile z_j^i of jth signature of ith signer. The spatial areas, pressure and time corresponding to the pressure profile below this threshold value was then considered as zero pressure region and hence were removed, as shown in Fig. 1 (d).

2.4 Dynamic Time Warping

The last step of our preprocessing module is Dynamic time Warping (DTW), which helps to establish a point to point correspondence between the base-signature b^i and all the signatures including genuine and forgeries of the ith signer. Since the velocity profile is richer in detail than the pressure profile [9], we perform DTW between the base velocity v_b^i and velocity profiles v_j^i of jth signature of signer i as described in [5]. After the DTW transformation, any one-to-many relationships present in warping path are eliminated [5], so that the length of warping path becomes equal to the length of base vector (v_b^i). By discarding all the repeated values in the warping path of v_b^i, corresponding indices may then be used to retrieve x_j^i and y_j^i for all signatures of ith signer.

3 Proposed System

Normally, each Biometric identification system can be decomposed into two major stages: $Training$ and $Verification$. For the training purpose, we have used only 3 and 5 genuine signatures from each signer to construct a template of relative angle content. This content is partitioned and assessed through an associated weighting scheme that attempts to place importance on more informative partitions during verification. A fusion process considered across partitions then governs the ultimate decision of whether or not a test signature is considered genuine or forgery, as outlined in the following.

3.1 Training

3.1.1 Relative Angle Calculations

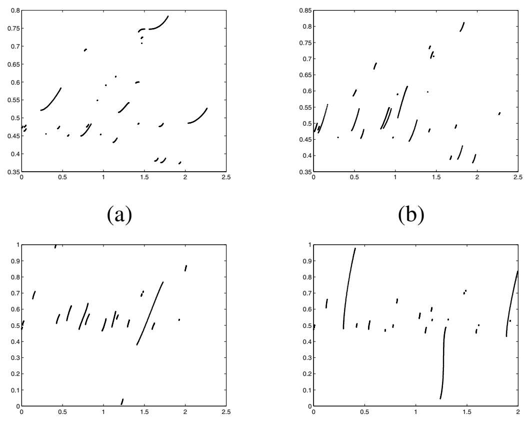
As the idea behind our proposed system is directional analysis of signatures, so we have calculated relative angles. Relative angle is formed by taking the angle between the slope of two consecutive points in the shape of signature. All the calculations are done for the base-signature b^i for ith signer. Mathematically, relative angles can be calculated as:

$$Ar_b^i(m) = tan^{-1}\left(\frac{y_{m+1} - y_m}{x_{m+1} - x_m}\right), m = 1, 2, 3, \cdots, M. \quad (3)$$

where $\mathbf{Ar_b^i}$ is a vector of M relative angles for base-signature b^i of ith signer and M is total sample points in signature shape.

3.1.2 Creation of Angle Partitions

In this block we created N different partitions based on relative angles. Now the next step is to decompose the signature into its partitions based on our proposed partitioning method. Now the question rises that in how many partitions a signature should be decomposed? So we have to select the number of partitions which gives the most optimum results in the verification phase. We have used both user-dependent and user-independent thresholds to select the number of relative angle partitions. In case of our database, empirical results show that sixteen partitions are most feasible for the verification purpose. In case of user-independent, if we reduce the number of partitions from sixteen then the size of the discriminating feature increases that can negatively effects the reliability of our verification system and if we increase the number of partitions greater than sixteen, the size of the discriminating



(a) (b) (c) (d)

Figure 2. a) Spatial areas corresponding to relative angles from $0 - 22.5$, b) Spatial areas corresponding to relative angles from $22.5 - 45$, c) Spatial areas corresponding to relative angles from $247.5 - 270$, d) Spatial areas corresponding to relative angles from $270 - 292.5$.

feature reduces which poorly effect the overall recognition rate of verification process. For decomposing relative angles into partitions, each angle of Ar_b^i is scanned for the criteria:

$$ind_n^i = (n-1) \times (\frac{360}{N}) \leq \mathbf{Ar_b^i} \leq (n) \times (\frac{360}{N}) \quad (4)$$

where $n = 1, 2, 3, \cdots, N$ and ind_n^i is an index vector containing indices of relative angles for nth partition of ith signer.

3.1.3 Angle based Signature Partitioning

After creation of sixteen index vectors for the base-signature b^i of ith signer, we decompose all the horizontal and vertical trajectories into partitions based on these index vectors. Basically each partition in horizontal and vertical trajectory is created by taking sample points of trajectory corresponding to indices of each index vector ind_n^i. Mathematically it can be given as:

$$xpart_{nj}^i = x_j^i(ind_n^i); \quad ypart_{nj}^i = y_j^i(ind_n^i) \quad (5)$$

where $xpart_{jn}^i$ and $ypart_{jn}^i$ represent nth partition in horizontal trajectory (x_j^i) and vertical trajectory (y_j^i), respectively, corresponding to jth signature of signer i. At this point we have "N" angle based partitions of all signatures. Fig. 2 shows some of the partitions of a randomly selected signature from the signature database.

3.1.4 Mean based Template Generation

In our proposed system we have generated sixteen templates of horizontal trajectory (x_j^i) and vertical trajectory (y_j^i) each. Templates are created by taking mean of nth partition of all the jth signatures of signer i as given by the equation below:

$$txpart_n^i = \frac{1}{J}\sum_{j=1}^{J} xpart_{nj}^i; \; typart_n^i = \frac{1}{J}\sum_{j=1}^{J} ypart_{nj}^i \quad (6)$$

where $txpart_n^i$ and $typart_n^i$ are the nth horizontal template trajectories and vertical template trajectories of signer i respectively and J represents total number of signatures of that ith signer used for the training purpose.

3.1.5 Threshold Criteria

The main task of this block is to deduce a threshold criteria that presents a strong separation between the genuine and forgery signature of ith signer. Intuitively, this decision should be based on the distance between a test signature ($test^i$) and its respective template. To achieve this purpose we calculate threshold values th_n^i for all N partitions of a signer i. Firstly, we create N two dimensional $2D$ distance spaces by plotting normalized distances of horizontal trajectories $dxpart_{nj}^i$ against normalized distances of vertical trajectories $dypart_{nj}^i$ as calculated in equation given below:

$$\begin{aligned}
dxpart_{nj}^i &= \sqrt{\sum_{k=1}^{K_n}(txpart_n^i - xpart_{nj}^i)^2}, \\
dypart_{nj}^i &= \sqrt{\sum_{k=1}^{K_n}(typart_n^i - ypart_{nj}^i)^2}, \\
dxpart_{nj}^i &= \tfrac{dxpart_{nj}^i}{max(dxpart_n^i)} \\
dypart_{nj}^i &= \tfrac{dypart_{nj}^i}{max(dypart_n^i)}
\end{aligned} \quad (7)$$

Secondly, magnitudes $\mathbf{dt_n^i}$ of all J distance vectors are plotted in each n two dimensional $2D$ space according to:

$$dt_{nj}^i = \sqrt{(dxpart_{nj}^i)^2 + (dypart_{nj}^i)^2}. \quad (8)$$

Finally, a percentage of the maximum scatter of training dataset corresponding to ith signer (th_n^i) in each of the N two dimensional $2D$ distance spaces is calculated.

$$th_n^i = max(\mathbf{dt_n^i}) + (max(\mathbf{dt_n^i}) \times c), \quad (9)$$

where c is a controlling parameter that can be used to tune False Rejection Rate (FRR) and False Acceptance Rate (FAR) during the verification stage. For selecting the value of c, we have to take into account the security level that we need. There is tradeoff between FRR and FAR, meaning that reducing one of these values will increase the other. Normally, we want a security system with almost zero FAR. In our system where we wanted to have zero FAR, initially the value of c was selected very small, so that the boundary between genuine and forgery remains tight. The value of c is then increased such that the system maintains zero FAR and yields the minimum FRR possible for each signer.

3.1.6 Weighting Factor for Partitions

From above discussion it is obvious that each partition partially influences the decision of whether the test signature is genuine or forgery, in N partial decisions for a test signature. Fusion of all these decisions into one, is achieved using a weighted majority rule that accounts for both "Quantity" and "Quality"of each partition. Here quantity refers to the number of sample points contained by a partition, which reflects the proportion of related relative angles in a signature. Quality of a partition refers to the scatter of signature trajectories around its respective template. The ultimate decision then, weights each partition based on its number of sample points as well as scattering.

It is intuitive that a partition having larger number of sample

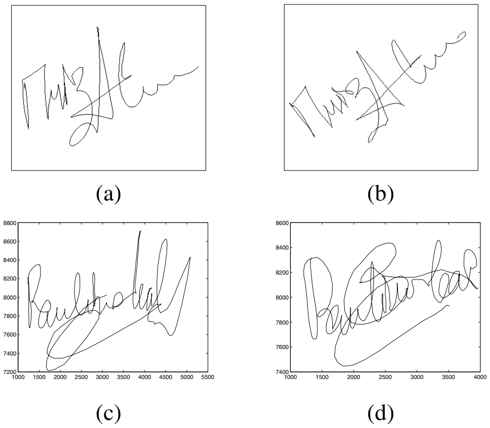


Figure 3. Sample signatures: a) genuine signature from database used in [5], [4], [6]; c) genuine signature from MCYT database; b) forgery from database used in [5], [4], [6]; d) forgery from MCYT database. Here we see that skilled forgeries are quite close in shape to their genuine counterparts. The need of dynamic features like angle, velocity and pressure are evident for proper discrimination.

points must contribute more in decision making. Our proposed quantity-based weighting criteria is given by:

$$wsp_n = \frac{K_n}{M}, \tag{10}$$

where wsp_n is the weight factor for nth partition, K_n represents number of sample points in nth partition and M is the total number of sample points in all partitions.

Secondly, our proposed quality-based weighting criteria wst_n is calculated for each partition, where wst_n caters for scattering of a partition around its respective template. This scattering is indicative of the more stable and consistent angles unique to a signature profile, thus partitions with small scatter are more reliable for use in any decision process that ensues. Mathematically, wst_n represents the normalized ratio of maximum separation from all partitions to separation of nth partition, and is defined by:

$$\begin{aligned} stdxy_n^i &= \sqrt{\frac{\sum_{j=1}^{J}(dt_{nj}^i - (\frac{\sum_{j=1}^{J} dt_{nj}^i}{J}))^2}{J}} \\ wst_n^i &= \frac{max(\mathbf{stdxy^i})}{stdxy_n^i} \\ wst_n^i &= \frac{wst_n^i}{\sum_{n=1}^{N} wst_n^i} \end{aligned} \tag{11}$$

where $\mathbf{stdxy^i}$ is a vector containing sixteen elements each representing standard deviation for each nth partition.

Finally, the combination of weight factors wsp_n^i and wst_n^i is ultimately used to obtain a single fused weight wt_n^i for the nth partition of the ith signer:

$$wt_n^i = \frac{wsp_n^i + wst_n^i}{2} \tag{12}$$

Table 1. Equal Error Rates (EER) for 25 signers belonging to our signature database.

Signer No.	EER of [5] using 200 Training Signatures	EER of our proposed using 200 Training user dependent
1	0.090	0.090
2	0.015	0.009
3	0.020	0.003
4	0.018	0.010
5	0.025	0.019
6	0.013	0.013
7	0.015	0.009
8	0.013	0.012
9	0.029	0.015
10	0.023	0.000
11	0.019	0.000
12	0.030	0.024
13	0.022	0.017
14	0.027	0.019
15	0.019	0.000
16	0.012	0.012
17	0.015	0.014
18	0.024	0.018
19	0.026	0.000
20	0.019	0.012
21	0.017	0.009
22	0.022	0.018
23	0.026	0.010
24	0.029	0.000
25	0.030	0.027

3.2 Verification

To verify a test signature ($test^i$) of ith signer, it is passed through all necessary preprocessing steps to ensure a suitable correspondence for comparison with trained templates. The test signature is then decomposed into N partitions based on relative angles as discussed in case of training signatures. All partitions are then used independently to calculate distances d_n^i from their respective templates. On the basis of these distances, a test signature $test^i$ is declared as genuine or forgery by the following criteria:

$$D_n^i = \begin{cases} 1 & d_n^i \leq th_n^i \\ -1 & \text{otherwise.} \end{cases} \tag{13}$$

where D_n^i is a decision vector containing N elements each representing a partial decision for nth partition. Elements of D_n^i is either 1 or -1, where 1 represents that signature is genuine and -1 represents that it is a forgery. Finally, these partial decisions are combined on the basis of weights (Eq. 12), to form an overall decision about test signature $test^i$:.

$$Decision = \begin{cases} Genuine & (\sum_{n=1}^{N}(wt_n^i \times D_n^i)) \geq 0 \\ Forgery & \text{otherwise.} \end{cases} \tag{14}$$

4 Experimental Results and Conclusion

To check the authenticity of our proposed system, we have used our own private database (reported in [4], [5]), containing 600 genuine and 200 forgery signatures for 25 signers.

Verification systems are largely compared through Equal Error Rate (EER), which represents the point on the Receiver Operating Characteristics (ROC) where False Acceptance Rate (FAR) is equal to False Rejection Rate (FRR). FAR represents the probability that a false match occurs, while FRR represents the probability that a false rejection occurs. Table. 1 shows EER for 25 signers belonging to our database. The average EER for our proposed system is 0.0128, where as average EER in [6], [5], [12] and [13] are 0.0220, 0.0239, 0.059 and 0.061 respectively while using our own database.

Researchers of online signature verification are trying to improve the performance under the constraint that only a few genuine signatures are available for training. In order to show the validity of our proposed algorithm, same experiments were also performed on the subset of our database containing 25 signers and for each signer 25 genuine and 25 forgeries were selected. In this experiment, training was done by using only 3 and 5 genuine signatures. The results are given in Table. 2. One of the most famous public databases (MCYT [2]) was also used to validate our system. Again, training of our system uses only 3 and 5 genuine signatures (the de-facto standard for training On-line Signature Verification Systems). Fig. 3 (c) shows genuine signature from MCYT [2] along with its respective skilled forgery.

This paper presents a novel approach to exploit inter feature dependencies in a signature by decomposing the base-signature of ith signer into N partitions based on relative angles of sample points and further weighting each partition according to its importance in decision making. Here, we have not used the conventional majority rule for the decision fusion process, as the majority rule gives equal weights to all the decisions and does not account for correlation among features [7]. We have tested our algorithm by using both user-dependent and user-independent for the selection of number of partitions. For the user-independent, we have used 16 partitions for both databases. To verify the validity of our proposed system, we have compared the average Equal Error Rate (EER) of our proposed system with some of the existing techniques [5], [4] using our own and MCYT database. Table 2 and Table 3 shows that our proposed system has outperformed the systems proposed in [5], [4] and moreover user-dependent threshold gives better results than the user-independent thresholds. The results on the MCYT database are also satisfactory where we have achieved an EER of 0.0364 when only 3 genuine signatures were used for training and EER of 0.0120 when only 5 genuine signatures were used, where as average EER in [11] and [8] are 0.0120, 0.0375 respectively while using only 5 genuine signatures for training.

Table 2. Avg. Equal Error Rates (EER) in percent for 25 signers belonging to our signature database.

No. of Training Signatures	Avg. EER of [5]	Avg. EER of [4]	Avg. EER of our proposed System user-dependent	Avg. EER of our proposed System 16 partitions
3	1.400	0.880	0.658	0.788
5	0.940	0.580	0.410	0.534

Table 3. Avg. Equal Error Rates (EER) in percent for 100 signers belonging to MCYT signature database.

No. of Training Signatures	Avg. EER of [5]	Avg. EER of [4]	Avg. EER of our proposed System user-dependent	Avg. EER of our proposed System 16 partitions
3	8.680	6.800	3.640	5.480
5	7.200	5.600	1.200	1.810

References

[1] G. Dimauro, S. Impedovo, M. G. Luccchese, R. Modugno, and G. Pirlo. Recent advancement in automatic signature verification. In *IEEE. 9th International Workshop on Frontiers in Handwriting Recognition*, pages 179–184, Oct. 2004.

[2] J. O. Garcia, J. F. Aguilar, D. Simon, J. Gonzalez, M. F. Zanuy, V. Espinosa, A. Satue, I. Hernaez, J. J. Igarza, C. Vivaracho, D. Escudero, and Q. Moro. Mcyt baseline corpus: a bimodal biometric database. *VISP*, 150:395–401, Dec. 2003.

[3] T. Hastie, E. Kishon, M. Clark, and J. Fan. A model for signature verification. In *IEEE. International Conference on Systems, Man and Cybernetics*, volume 1, pages 600–604, July 1991.

[4] M. Ibrahim, K. S. Alimgeer, M. A. Khan, and I. A. Taj. Creation and selection of most stable discriminating features for on-line signature verification. In *IEEE. International Conference on Machine Vision*, volume 3, pages 97–101, Dec. 2007.

[5] M. A. U. Khan, M. K. Khan, and M. A. Khan. Velocity-image model for online signature verification. *IEEE Trans. Image Processing*, 15(11):3540–3549, Nov. 2006.

[6] M. K. Khan, M. A. Khan, M. A. U. Khan, and I. Ahmad. On-line signature verification by exploiting inter-feature dependencies. In *18th International Conference on Pattern Recognition*, volume 2, pages 796–799, 2006.

[7] L. L. Lee, T. Berger, and E. Aviczer. Reliable on-line human signature verification systems. *IEEE. Trans. on Pattern Analysis and Machine Intelligence*, 18:643–647, Jun. 1996.

[8] O. Miguel-Hurtado, L. Mengibar-Pozo, M. G. Lorenz, and J. Liu-Jimenez. On-line signature verification by dynamic time warping and gaussian mixture models. In *IEEE 41st Annual Carnahan Conference on Security Technology*, pages 23–29, Oct. 2007.

[9] W. Nelson and E. Kishon. Use of dynamic features for signature verification. In *IEEE International Conference on Systems, Man and Cybernetics*, pages 201–205, Oct. 1991.

[10] T. Qu, A. E. Saddik, and A. Adler. A stroke based algorithm for dynamic signature verification. In *Canadian Conference on Electrical and Computer Engineering*, volume 1, pages 461–464, May 2004.

[11] Z.-H. Quan and K.-H. Liu. Online signature verification based on the hybrid hmm/ann model. *International Journal of Computer Science and Network Security*, 7:313–322, March. 2007.

[12] M. Wrioutius, J. Y. Ramel, and N. Vincent. Selection of points for on-line signature comparison. In *Ninth International Workshop on Frontiers in Handwriting Recognition*, pages 503–508, Oct. 2004.

[13] J. Yi, C. Lee, and J. Kim. Online signature verification using temporal shift estimated by phase of gabor filter. *IEEE. Trans. on Signal Processing*, 53:776–783, Feb. 2005.