Optimal Threshold Selection for Online Verification of Signature

A. Alizadeh, T. Alizadeh, Z. Daei

Abstract: **In this paper an innovative method for [1]verification of signature using parametric features based on optimal threshold selection is proposed. For each signature, 62 parametric feature are derived from horizontal place, x(t), vertical place, y(t) and pen down and up signals which are obtained from a digitizer plane. The weighted distance between each feature of a signatories and the related reference features is compared to a suitable threshold value and then the feature is accepted or not. The number of the accepted features for a person is then compared to another threshold, which has a suitable value for each signature, and then the signature will be verified or rejected. In this research, 1500 original signatures from 30 person and 600 forgery signatures are used. For each person, 30 genuine and 10 forgery signatures are considered for training of the algorithm and the rest are used in testing and validation. It is shown in the results that there is 0.67% false rejection ratio and 0.67% false acceptation ratio for the training set and a 2.68% and 1.99% for the testing set, respectively.**

Index Terms— **Online signature verification – feature extraction – parametric features – weighted Euclidean distance**

1. Introduction

Biometric authentication is researched widely in many scientific fields recently [1]. Biometric features include attributes like fingerprints, handwriting, iris, retina, DNA, face, blood vessel, lip movements, body movements and signature [2]. Among so many features, signature is a form of behavioral biometrics. Due to its distinctiveness and stability, signature-based personal identification systems are used and accepted widely [1]. An important advantage of the signature over other biometrics is its long standing tradition in many commonly encountered verification tasks. It has been used for decades in civilian applications while other methods (e.g., fingerprints) still have the stigma of being associated with criminal investigation. In other words, signature verification is already accepted by the general public [3]. The signature verification generally is divided into two vast areas: off-line methods that assume no time-related information and on-line ones with time-related information available in the form of multidimensional function of time [4]. There are several implementations for signature recognition and verification [5]. Justino, Bortolozzi and Sabourin proposed an off-line signature verification system using Hidden Markov Model [6]. Zhang, Fu and Yan proposed handwritten signature verification system based on Neural 'Gas' based Vector Quantization [7]. Vélez, Sánchez and Moreno proposed robust off-line signature verification system using compression networks and positional cuttings [8]. Arif and Vincent concerned data fusion and its methods for an off-line signature verification problem which are Dempster-Shafer evidence theory, Possibility theory and Borda count method [9]. Chalechale and Mertins used line segment distribution of sketches for Persian signature recognition [10]. Sansone and Vento increased performance of signature verification system by a serial three stage multi-expert system [11].Dynamic features include the number and order of the strokes, the overall speed of the signature, the pen pressure at each point etc. and make the signature more unique and more difficult to forge. As a result, online signature verification is more reliable than offline ones. Application areas of online signature verification include protection of small personal devices (e.g. PDA, laptop), authorization of computer

Manuscript received December 8, 2009.
A. Alizadeh is with the Electrical Engineering Department, University of Bonab, Iran. (phone: +98-412-7243801; fax: +98-412-7240800; e-mail: a_alizadeh@tabrizu.ac.ir).
T. Alizadeh is with University of the Electrical Engineering Department, Bonab, Iran. (e-mail: Alizadeh_tohid@yahoo.com).
Z. Daei is with the Electrical Engineering Department, University of Tabriz, Tabriz, Iran (e-mail: z.daei@tabrizu.ac.ir).

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

users for accessing sensitive data or programs, and authentication of individuals for access to physical devices or buildings [12].A typical signature verification algorithm is consisted of four steps: 1. Data acquisition, 2. Feature extraction, 3. Feature selection and 4. Decision making and final validation [13, 14, and 15].For training phase of the signature verification, a combination of genuine and forgery signatures [13,15] or just genuine signatures [16] are used. In this paper, forgery signatures are used just for obtaining threshold values and in the rest of the training, genuine signatures are used. The rest of the paper is organized as follows: signature acquisition is considered in the second sect. and the third section is about feature extraction. In the next section the proposed algorithm is presented and finally the results and some suggestions for further works are given in the last section.

2. ACQUISITION OF GENUINE AND FORGERY SIGNATURES

In this paper signatures from 30 persons are collected. From each person, 50 true signatures in two or three phases, with a time interval of about one week are gathered. For gathering signatures, a digitizer plane with a resolution of 125 point in inch and a sampling rate of 333 samples per second is used. The mean age of the signatories is 25 years, 90% is male and 10% is female. For each genuine signature, five persons forged it ten times. The forgers had enough time to practice signature on the paper and digitizer. From the ten signatures of each forger, four signatures that were more similar to original ones, have been selected for train and test sets, using a pre-compare stage. This forgery is named statically skilled forgery [13]. For each subject 50 genuine and 20 forgery signatures were collected. 30 genuine and 10 forgery signatures from this set were used for training and the rest were used for testing. Signature features, used in this paper, are sensitive to angle and the large size variation of the signature, so it is asked from the signatories to sign in a same angle and size. In addition to the shape of the signature, the direction and path of the original signature was shown to the forgers. Samples of the genuine and forgery signatures are shown in Figs. 1 and 2. After acquiring x(t) and y(t) signals, velocity functions, $v_x(t)$, $v_y(t)$ and $|v(t)|$ are calculated. Then, all of these functions are filtered using a low pass filter prior to feature extraction stage. As an illustrating example, a genuine and its forgery signatures and their x(t), y(t), $v_x(t)$ and $v_y(t)$ signals are shown in Figs. 3 to 7, respectively.

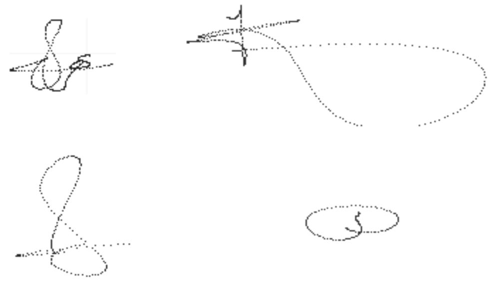

Fig. 1. Samples of genuine signatures

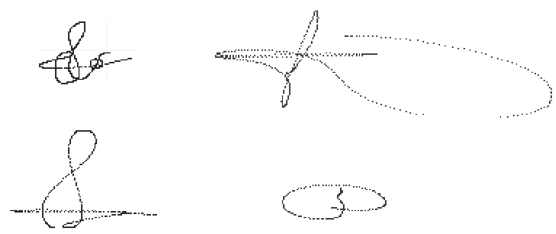

Fig. 2. Samples of forgery signatures

3. FEATURE EXTRACTION

In this paper parametric features have been used. This features are obtained from x(t), y(t), $v_x(t)$, $v_y(t)$, $|v(t)|$ functions and pen up and down and contain spatial features like the mean, maximum and minimum of the x(t) and y(t), time features like the signature time, minimum and maximum time of the x(t), y(t), $v_x(t)$, $v_y(t)$ functions and velocity related features like mean, maximum and minimum of the velocity in the x and y directions [13]. Investigating the importance of these features showed that the spatial features of the forgery signatures have a little distance from their similar features of the genuine signatures while the time features and velocity related features of the forgery signatures have a significant difference with their similar features of the genuine signatures. Ts, Vy_{min} and $t(y_{min})$ became the most important features in the mentioned order. The features used in this paper are explained in the Table1.

4. VERIFICATION ALGORITHM

After feature extraction of the genuine signatures in the training set, the mean and variance values for each signatory calculated and saved as reference

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

features. For a signature to be verified or rejected, its features will be compared to its reference features. The weighted Euclidean distance of each feature with the mean reference feature is obtained from the following relation:

$$d_{ij} = \frac{|x_i - m_{ij}|}{\delta_{ij}} \quad (1)$$

Where m_{ij} is the mean value, and δ_{ij} is the variance of the ith feature for the jth signatory and x_i is the ith feature of the signature which should be verified for the jth signatory.

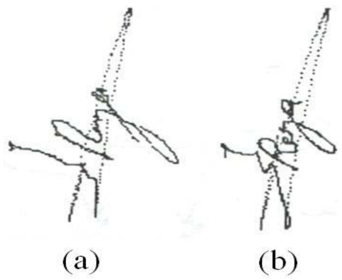

Fig. 3. An example of a genuine and forgery signature

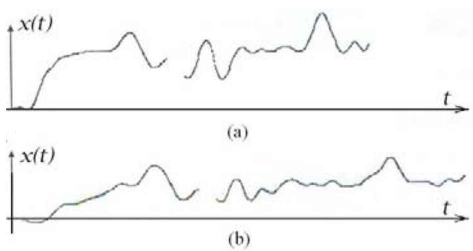

Fig. 4. x(t) signals for (a) genuine and (b) forgery signature

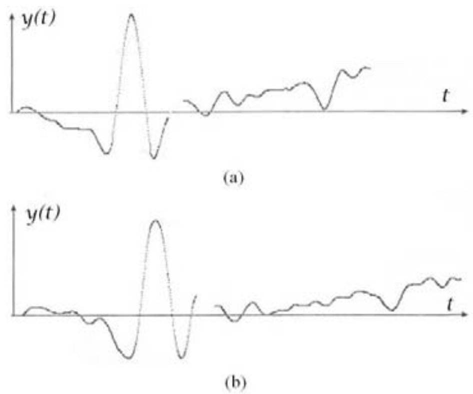

Fig. 5. y(t) signals for (a) genuine and (b) forgery signature

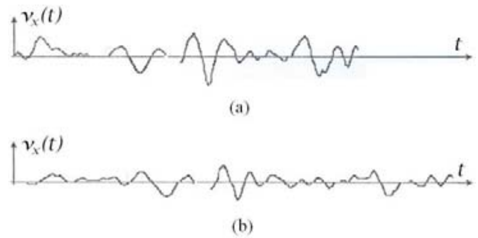

Fig. 6. v_x(t) signals for (a) genuine and (b) forgery signature

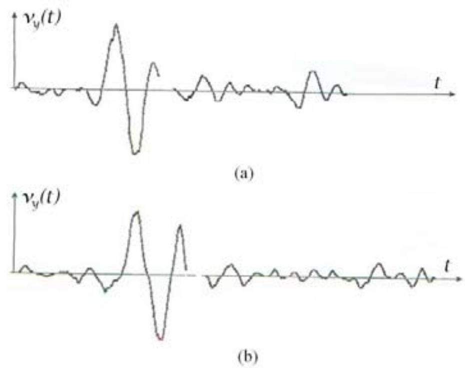

Fig. 7. v_y(t) signals for (a) genuine and (b) forgery signature

In the conventional methods, such as weighted Euclidean distance, the distance between the features vector and average features vector is calculated and after comparing this value with a suitable threshold, the signature will be verified or rejected. In this paper, the weighted distance of each feature, d_{ij}, is calculated and is compared to the first threshold value, T_{1j} . Then, the number of the accepted features is compared to the second threshold value, T_{2j}, and finally the signature will be verified or not. For more skilled signatories, T_{1j} has lower values, and for whom with unstable signatures, it takes a higher values. For obtaining optimal values for T_{1j} and T_{2j} for each individual, at first the FAR (False Accepting Ratio) and FRR (False Rejection Ratio) diagrams for constant T_{2j} and varying T_{1j} are drawn. The diagrams for two different values of T_{2j} are shown in Fig. 8. The suitable value of T_{1j} for the given T_{2j} is then the intersection of the two diagrams, where the summation of the error values are minimum. For different values of T_{2j} , different values for T_{1j} are obtained. These two values are called (T_1, T_2) pair for jth signatory.

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Table. 1. List of Features

1. (T_s)	Total signing duration
2. (T_p)	Total pen down duration
3. (Seg)	Number of segment
4. (X_{max})	Maximum value of x(t)
5.t(x_{max})	Time of Feature 4
6. (X_{min})	Minimum value of x(t)
7. t(x_{min})	Time of Feature 6
8. (Y_{max})	Maximum value of y(t)
9. t(y_{max})	Time of Feature 8
10. (Y_{min})	Minimum value of y(t)
11. t(y_{min})	Time of Feature 10
12. X_{avr}	Mean value of x(t) function
13. Y_{avr}	Mean value of y(t) function
14. Vx_{max}	Max horiz. writing speed
15. t(Vx_{max})	Time of Feature 14
16. Vx_{min}	Min horiz. writing speed
17. t(Vx_{min})	Time of Feature 16
18. Vy_{max}	Max vertic. writing speed
19. t(Vy_{max})	Time of Feature 18
20.Vy_{min}	Min vertic. writing speed
21. t(Vy_{min})	Time of Feature 20
22.S(v_x)	Integral of v_x(t) curve
23.S(v_y)	Integral of v_y(t) curve
24.xend	x of end point
25.yend	y of end point
26.L	Total dots recorded or signature length
27.A	Signature frame area
28.L/A	Length per frame area
29.D	Signature frame width
30.H	Signature frame height
31.H/D	
32.σ_x	Standard deviation of x(t)
33.σ_y	Standard deviation of y(t)
34.V_{avr}	Average writing speed
35. V_{max}	Max. writing speed
36.t(V_{max})	Time of max speed
37.S(V)	Integral of v(t) curve
38.T_{Vxp}	Duration of Vx(t)>0
39. T_{Vxn}	Duration of Vx(t)<0
40. T_{Vyp}	Duration of Vy(t)>0
41. T_{Vyn}	Duration of Vy(t)<0
42. S(Vxp)	Integral of positive v_x(t) curve
43. S(Vxn)	Integral of negetive v_x(t) curve
44. S(Vyp)	Integral of positive v_y(t) curve
45. S(Vyn)	Integral of negetive v_y(t) curve
46. N(Vxz)	Number of point that V(x)=0
47. N(Vyz)	Number of point that V(y)=0
48. Vst	Start speed
49. Vend	End point speed
50. Ang_{st}	Start angle with x axis
51. Ang_{st-end}	Star point to end point line angle with x axis
52. Ang_{st-end}	Star point to end point line angle with x axis
53. Ang_{12}	Start point to 2nd segment start point angle with x axis
54. Tp/Ts	
55. T(seg2)	
56. t(V_{max})/Ts	
57. V_{avr}/V_{max}	
58. T_{Vxn}/Ts	
59. T_{Vxn}/Ts	
60. T_{Vxn}/Ts	
61. T_{Vxn}/Ts	
62. T(seg2)/Ts	Time of 2nd segment if exist if 2nd exist segment

For choosing the best pair, T_2 is calculated according to the following procedure. For each value of T_1, the minimum number of the accepted features for genuine signatures, m_{gj}, and the maximum number of the accepted features for forgery signatures, M_{fj}, in the training set are calculated. The optimal value of the T_2 for this T_1 is given by the following equation:

$$T_{2j} = \frac{m_{gj}+M_{fj}}{2} \tag{2}$$

By using this method, the FAR and FRR error diagrams and their summation will be as the Fig. 9.

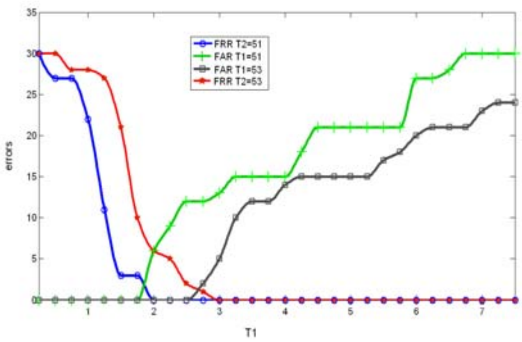

Fig. 8. FAR and FRR ratios for two values of T_{2j}

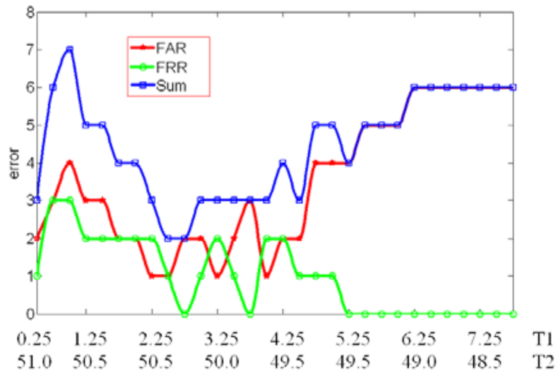

Fig. 9. The FRR, FAR and their summation diagrams for (T_1, T_1) pair

The optimal (T_1, T_2) pair will be the pair for which the summation error has the minimum value. For the example diagrams of the Fig. 1 and Fig. 2, T_1 and T_2 values are 2.25 and 50.5, respectively. The (T_1, T_2) pair together with the reference features are saved for each signature.

ISBN: 978-988-17012-8-2
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

5. RESULTS AND CONCLUSION

Using the proposed algorithm, for the training set containing 30 genuine and 10 forgery signatures, FRR and FAR errors achieved 0.67% and 0.67%, respectively. For the test set, containing 20 genuine and 10 forgery signatures, FRR and FAR errors achieved 2.68% and 1.99%, respectively. For comparing purposes, an experiment using conventional weighted Euclidean distance was done. For training set, FRR and FAR errors become 0.67% and 1.33%, respectively, and for test set, FRR and FAR errors become 2.5% and 3%, respectively.

Investigating the effects of the each feature on the verification of the signature shows that some features haven't considerable difference for genuine and forgery signatures, and others have great difference. It seems that the first class of the features hasn't considerable effect on the verification of the signature, while the second class features have somehow great effect. So, better results could be achieved if a parameter such as weight for features is used.

REFERENCES

[1] Zhang, J., Kamata, S. "Online Signature Verification Using Segment-to-Segment Matching", Int. Conf. on Frontiers in Handwriting Recognition ICFHR (2008), August 19-21, 2008 ,Montréal, Québec

[2] T.Ohishi,Y .Komiya,T.Matsumoto, "On-line Signature Verification using Pen-Position, Pen-Pressure and Pen-Inclination Trajectories", International Conference on Pattern Recognition (ICPR'00), September 3-8, 2000, Barcelona, Spain,

[3] Maryam Moghadam Fard, Mehdi Moghadam Fard, Nasser Mozayani, "A New On-line Signature Verification by Spatio-Temporal Neural Network", ISI 2008, June 17-20, 2008, Taipei, Taiwan, pp. 233-235

[4] Ningning Liu, Yunhong Wang, "Template Selection for On-line Signature Verification", International Conference on Pattern Recognition (ICPR 2008), December 8-11, 2008, Tampa, Florida, USA

[5] Emre Özgündüz,Tülin Şentürk and M. Elif Karslıgil, "OFF-LINE SIGNATURE VERIFICATION AND RECOGNITION BY SUPPORT VECTOR MACHINE", 13th European Signal Processing Conference (EUSIPCO 2005), 4-8 September 2005, Antalya, Turkey

[6] E. J. R. Justino, F. Bortolozzi and R. Sabourin, "Off-line Signature Verification Using HMM for Random, Simple and Skilled Forgeries", ICDAR 2001, International Conference on Document Analysis and Recognition, vol. 1, pp. 105--110. 2001

[7] B. Zhang, M. Fu and H. Yan, "Handwritten Signature Verification based on Neural 'Gas' Based Vector Quantiza-tion", IEEE International Joint Conference on Neural Net-works, pp. 1862-1864, May 1998.

[8] J. F. Vélez, Á. Sánchez , and A. B. Moreno, "Robust Off-Line Signature Verification Using Compression Networks And Positional Cuttings", Proc. 2003 IEEE Workshop on Neural Networks for Signal Processing, vol. 1, pp. 627-636, 2003.

[9] M. Arif and N. Vincent, "Comparison of Three Data Fu-sion Methods For An Off-Line Signature Verification Prob-lem", Laboratoire d'Informatique, Université de François Rabelais, 2003

[10] A. Chalechale and A. Mertins, "Line Segment Distribu-tion of Sketches for Persian Signature Recognition", IEEE Proc. TENCON, vol. 1, pp. 11–15, Oct. 2003

[11] Sansone and Vento, "Signature Verification: Increasing Performance by a Multi-Stage System", Pattern Analysis & Applications, vol. 3, pp. 169–181, 2000.

[12] Alisher Kholmatov, Berrin Yanikoglu, "Identity authentication using improved on-line signature verification method", Pattern Recognition Letters 26(15): pp. 2400-2408 (2005)

[13] Luan L. Lee, Toby Berger, and Erez Aviczer, "Reliable On-Line Human Signature Verification Systems", IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 18, NO. 6, JUNE 1996

[14] R. Plamondon and G. Lorette, "Designing and automatic signature verifier: problem definition nad system description", Computer Processing of Hand Writing, World scientific Publishing Co., 1990, pp. 3-20

[15] R. Plamondon and G. Lorette, "automatic signature verification and writer identification-the state of the art", pattern Recognition, Vol. 22, No. 02, pp. 107-131, 1989

[16] Jaihie Kim, J.R. Yu, S.H. Kim, "Learning of prototypes and decision boundaries for a verification problem having only positive samples", Pattern Recognition Letters 17 (1996) 691-697