World of Computer Science and Information Technology Journal (WCSIT)
ISSN: 2221-0741
Vol. 2, No. 2, 46-50, 2012

Multiple Classifiers to verify the Online Signature

Dr. Mohammed J. Alhaddad
Department of Information Technology
Computer Science & Information Technology Collage
King Abdulaziz University
Saudi Arabia

Abstract—Nowadays biometric increasingly used in many applications that has strong relation to our live; it's a reliable mean as an alternative to the traditional methods of personal identification. As a behavioral biometric, an online signature still has some shortcomings because of that nature. Furthermore, features in online signature verification system can be either global or local; the techniques that can be used also variety. In this paper both global and local features were used. To classify the mentioned features; the back-propagation neural network (BPNN) technique was used to classify the local features, whereas, the global features was classified by the probabilistic model. Once the results obtained from the local classifier and global classifier, the "AND" fusion was used to combine the two classifiers for final decision. SVC2004 dataset was used to evaluate the proposed method in term of False Rejection Rate (FRR) and False Acceptance Rate (FAR). The obtained results for FRR and FAR were 0.3% and 0.5% respectively. These results are encouraging when compared with related existing studies.

Keywords- Online Signature; Probabilistic Modeling; Back-propagation Neural Network (BPNN).

I. INTRODUCTION

Generally, biometric automatic recognition of people based on their distinctive physiological (face, fingerprint, iris, etc.) and behavioral (online/offline signature, voice, etc.) characteristics. Depending on the available data in the input, signature can be classified into two categories: offline (static) signature [1, 2, 3] takes the image as an input of a signature and it is useful in bank check and document, online (dynamic) signature [4, 5, 6, 7, and 8] uses signatures that are captured by pressure-sensitive tablets that extract dynamic properties of a signature in addion to its shape.

In an online or an offline signature system, two steps are required before the final decision is made; first, a user is registered by providing samples of signature (reference signatures), then, when a user presents a signature (test signature) claiming to be a particular individual, the test signature is then compared with reference signatures for that user. If the similarity is very near to a certain threshold, the user is accepted otherwise rejected.

The common steps involved in signature verification include: data acquisition, preprocessing, features extraction, and verification. In each step after getting data there are many methods and techniques that can be applied individually or by combining two or more techniques to get a better results.

Features can be separated into two categories: global and local features. Global features describe properties of the whole signature. Examples of the global features including: total writing time, bounding box, or the number of the strokes. Local features are properties which refer to a position within the signature. Distance or curvature change between consecutive points on the signature trajectory is also considered as local feature [4]. Features may also be classified as spatial (related to shape) or temporal (related to dynamic) [9].

In this paper, global features are classified by the probabilistic features modeling which is similar to [10] with some differences in the features, threshold, reference signatures number, and dataset used. BPNN is used to classify the local features; the results that came from both technique are combined by "AND" fusion.

II. RELATED WORK

Handwriting is very complex in nature. It is a biomechanical process that includes the movements of fingers, wrist, and forearm. It has been shown that humans generate handwriting through controlling the magnitude and direction of speed [11]. Therefore, many techniques and models are proposed and applied for online signature verification system using one type of feature or both.

Dynamic features that are derived from velocity and acceleration of the pen together with other global features by fitting the probability density function (PDF) are modeled by [10] as follows: in the training phase the mean and variance of each feature is estimated. A quantity called the threshold is estimated. To estimate the threshold, the specimen signatures are treated as test signatures and the features are then substituted into (1).

$$P(X_i) = \exp\left[-(X_i-\mu_i)^2/(2Var_i)\right]/\sqrt{2\mu_i Var_i} \qquad (1)$$

where P(Xi) is the score of particular feature Xi, µi is the mean, Vari is the variance, and i is an index of current feature.

The probability score (PS) is calculated over all the features using (2).

$$PS = \sum_{i=1}^{i=n} P(X_i) \qquad (2)$$

where *n* is the number of features. This is repeated over the whole set of sample signatures; probability score is used to serve as a threshold value.

In [4] the similarity between an input signature and the reference signatures is computed using string matching and the similarity value is computed to a threshold; both spatial and temporal features were used. Local spatial features that are extracted and studied are: (i) the x and y coordinates differences between two consecutive points, Δx, Δy, (ii) the absolute y-coordinate with reference to the center of the signature, y, (iii) the sine and cosine of the angle with the x-axis, sine x and cosine x, (iv) the curvature, B and (v) the grey values in a 9x9 pixel neighborhood.

A novel approach to the on-line signature verification using local shape Analysis has been presented by [12]. First, they segmented the input signature into several segments using HMM (Hidden Markov Model). Then, they combined two adjacent segments to form a long segment and its spectral and tremor information are calculated using the Fast Fourier Transformation (FFT). Finally, the decision of accepting it or rejecting it, is based on the similarity between the spectral and its prototype.

Two-class pattern recognition problem for online signature verification has been proposed by [13]. First, they experimented with Bayes classifier on the original data, as well as a linear classifier used in conjunction with Principle Component Analysis (PCA). The BPNN used by [14] per each signer with parameters as follows: (i) 72 signatures for recognition, (ii) 251 neural BIAS in the input layer, (iii) 11 neural BIAS in the hidden layer, (iv) 2 neurals in the output layer, (v) 60 patterns in train stage.

Online signature verification based on Parzen Window Classifier (PWC) and Hiden Markov Model (HMM) have been developed by [15]; the application of HMM to time sequences directly based on the dynamic functions.

Reference [16] multiple classifiers (neural network, support vector machine and Pearson correlation) were used to develop an on-line signature verification system. Then, they fused them by applying a different fusion technique.

A new technique for online signature verification has been presented by [17]. The technique integrates a longest common subsequences (LCSS) detection algorithm which measures the similarity of signature time series into a kernel function for support vector machines (SVM). The SVC 2004 (40 users) benchmark database is used to show the properties of the new SVM-LCSS beside signatures of 153 test persons.

SVC 2004 has been used also by [18] with dynamic time warping (DTW) approach, the obtained result is shown in Table 7.

III. Proposed Methodology

Basically, there are well known steps involved in online signature verification as mentioned in section 1 and detailed in [4, 9, 10, 16]. Researchers are focusing on selecting powerful features [4, 12, 13] and a hybrid method [15, 16, 17] to guarantee a higher accuracy of verifying identity of persons via signature.

In this paper, two classifiers have been used. First one is used to classify the global features that are chosen; the second one is used to classify the local features. The results of two classifiers are combined to get the final decision. Figure 1 depicts the proposed method used in this paper

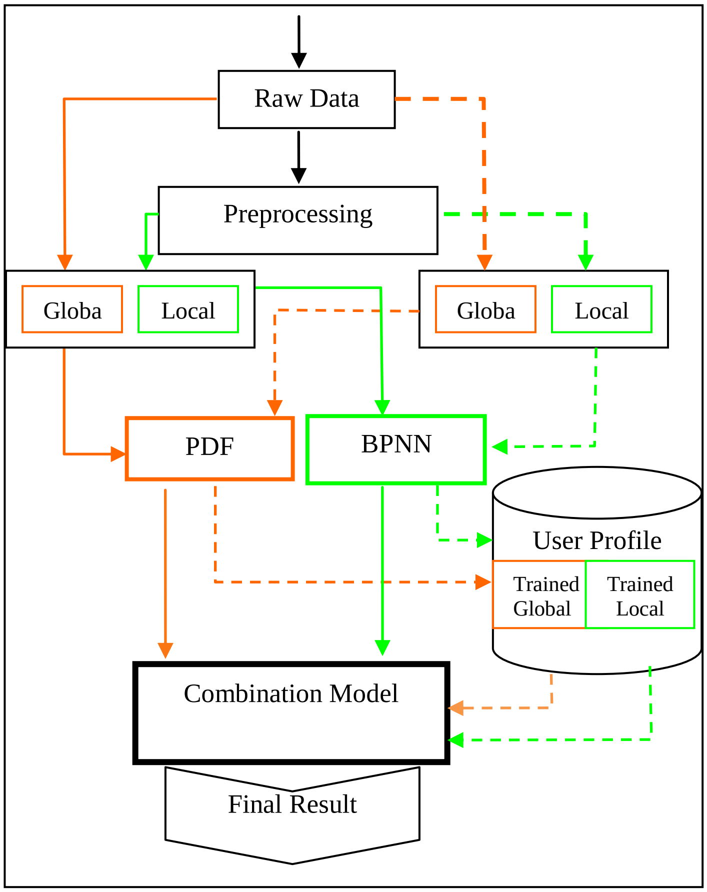

Figure 1. the proposed method.

Where the dotted lines indicate to the train phase, whereas, the solid indicates to the test phase.

A. Global Classifier

Eight global features are selected to be classified by this model which are: (1) Total time of signature, (2) Max Azimuth, (3) Average Azimuth, (4) Number of zeros in the velocity in X direction, (5) Number of zeros in the velocity in Y direction, (6) Number of zeros in the acceleration in X direction, (7) Number of zeros in the acceleration in Y direction, (8) Total distance traveled by the pen. This is the sum of all the Euclidean distances between all the points.

First, getting all features values of all reference signatures as shown in Table 1, then, the mean and variance are calculated as shown in Table 2.

TABLE1. FEATURES' VALUES OF 5 REFERENCE SIGNATURES FOR A USER

Features/ signature	Sig1	Sig2	Sig3	Sig4	Sig5
F1	2063	2083	2113	1923	1951
F2	1350	1350	1190	1180	1210
F3	1200.119	1178.093	1145.594	1119.33	1150.7
F4	70	85	92	77	86
F5	105	114	127	111	113
F6	81	83	110	90	96
F7	81	83	95	85	91
F8	29530.5	29277.23	29444.15	29077.46	27564.6

TABLE 2. MEAN AND VARIANCE OF REFERENCE SIGNATURES FOR A USER

Features	µ	Var
F1	2026.6	7104.8
F2	1256	7480
F3	1158.774	969.2111
F4	82	73.5
F5	114	65
F6	92	136.5
F7	87	34
F8	28978.79	654912.9

In order to obtain the threshold of the global features classifier for a specific user, the probability score of the reference signatures is calculated as shown in Table 3.

TABLE 3. PORBABILITY SCORE (PS) OF REFERENCE SIGNATURES FOR A USER

signature	PS Value
Sig1	0.1187635
Si2	0.1900374
Sig3	9.253134E-02
Sig4	0.1951401
Sig5	0.1967456

Threshold of a specific user is the minimum values among all reference signatures, and it is kept in his profile. In the test phase, all steps are repeated until getting the PS value; if the current PS value is greater than or equal to the threshold value stored in the user profile, the user is accepted as genuine, otherwise is rejected as a forgery.

B. Local Classifier

The local features which are selected for signature verification using back-propagations neural network are determined as follows: (1) the collection of X-coordinates from the start to end, (2) the collection of Y-coordinates from the start to end, (3) the collection of Azimuth values from the start to end.

A three-layer MLP is designed to recognize the signatures based on 2-dimensional features x, y as the input and Azimuth as the output. The same network can be applied for the rest of features.

The neural network parameters used in this paper are set as follows: (1) train function='learnlm'; is a network training function that updates weight and bias values according to Levenberg-Marquardt optimization. It is the fastest method for training moderate-sized feed-forward neural networks (up to several hundred weights), (2) train show=20; is the number of epochs between showing the progress, (3) train epochs=100; is the maximum number of iteration, (4) train goal=0.0001; is the performance goal, (5) train lr=0.2; is the learning rate, (6) train lr_inc=1.05; is the learning rate increase multiplier, (7) train lr_dec=0.7; is the learning rate decrease multiplier.

Test signature passes through the four trained forward network only to obtain the test error for comparing with train error. This will give the clue of how much the error is closed to each other. Table 4 shows the test errors of a genuine signature with its associated trained error.

TABLE 4. TRAIN ERRORS AND TEST ERRORS OF GENUINE

No/Error	Train	Test
1	0.000914246	0.0066
2	0.000870961	0.0075
3	0.000720229	0.0063
4	0.000235909	0.0016

Fig. 2 shows how much the test errors are closed to the train errors. The value of the threshold used in this technique is 0.50. So, test signature is considered as a genuine if it satisfies (3):

$$\text{Verifier} = \sum_{i=1}^{N} Tr_i / Ts_i \geq 0.50 \qquad (3)$$

where i=1…N, N is the number of trains; Tr is the train errors and Ts is the test errors. The above test gained the value of 0.5139 which is greater than 0.50, so it is considered as a genuine signature.

The errors of forged test signature and the errors of the trained network are shown in Table 5. While, the relation between the test error and train errors of forged signature are shown in Fig. 3.

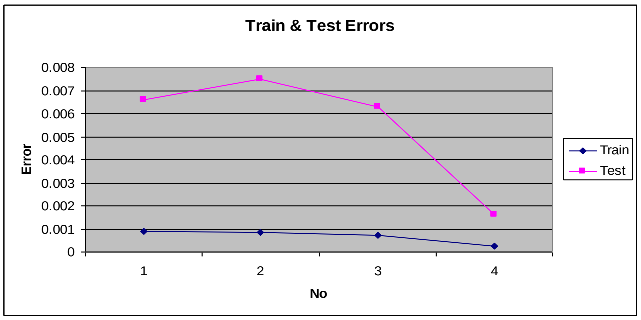

Figure 2. Train Errors and Test Errors of Genuine.

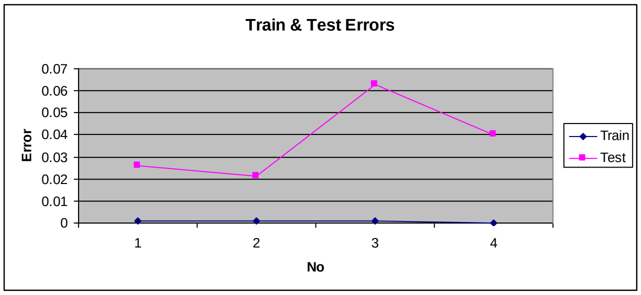

Figure 3. Train Errors and Test Errors of Forgery.

TABLE 5. TRAIN ERRORS AND TEST ERRORS OF FORGERY

No/Error	Train	Test
1	0.000914246	0.0261
2	0.000870961	0.0213
3	0.000720229	0.0627
4	0.000235909	0.0402

The result of the above test is 0.0934 which is not closed to 0.50, which means that the signature is considered as a forged signature.

Fig. 4 shows the differences in the errors between genuine signature and forgery signature comparing to the errors of train.

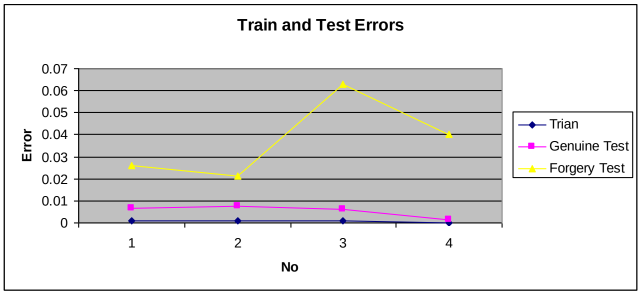

Figure 4. Train Errors and Test Errors of Gennuine and Forgery.

C. *Combiniation*

In general, both two classifiers, i.e. the probabilistic model classifier and neural network classifier yielded different accuracies. In order to get the benefit from both classifiers, an “AND” Logical Gate fusion is used at the decision-making score level among these two classifiers. Each one of the proposed classifier modules is characterized by its own characteristics. A user is considered as a genuine if he passes in both classifiers, otherwise, he is considered as a forgery.

IV. EXPERIMENTAL RESULTS

The performance of proposed online signature verification system in this paper is evaluated based on SVC2004 Task2 [19]. This dataset is very famous in this research’s community to benchmark their work. The number of persons and signatures that were used are shown in Table 6.

TABLE 6. THE DETAILS OF THE DATASET USED

Dataset	**Phase**	**User's Type**	**No. of signs**	**Total of 40 user**
SVC2004	Train	Genuine	5	200
	Test	Genuine	5	200
		Skilled	5	200

There are two measures to evaluate the performance of the online signature verification, False Rejection Rate (FRR) and the False Acceptance Rate (FAR). However, some researchers prefer to use the Equal Error Rate (EER) which is the intersection between FRR and FAR. The results of global features classifier, local features classifier, and the combination model are shown in Table 7.

TABLE 7. THE FRR AND FAR OF THE CLASSIFIERS

Classifier	**FRR**	**FAR**
Global Features Classifier	27%	9%
Local Features Classifier	14%	37 %
Proposed Combined	3%	5%

Making a fair comparison among researchers sometimes is not quite accurate. The reasons behind that are: using a different dataset, different type of forgery (random, skilled, etc) to test the system, different number of reference and test signatures, and the way of experiments are being conducted.

Performance of online signature verification system for some existing studies according to date are shown in Table 8.

TABLE 8. PERFORMANCE OF SOME EXISTING STUDIES

Method	Dataset	Error%	
	Users/sig.	FRR	FAR
PDF calssifier [10]	5/25	-	5
String matching [4]	102 /1232	2.8	1.6
HMM [12]	2/120	6.67	0.0
	40/1440	9.94	0.5
	2/1100	11.3	2.0
Bayes classifier [13]	94/1247	2.19	3.5
Bp ANN [14]	-/150	1.8	2

PWC,HMM [15]	MCYT	EER= 6.67
		EER= 2.12	

Neural Network and SVM [16]	20/600	21.5	3.5
		3.5	0.0
SVM-LCSS [17]	SVC2004	EER=6.84	
DTW [18]	SVC2004	5.5	4.13

V. Conclusion

In this paper, the probability model and BPNN have been combined using "AND" fusion. The combination model overcomes the drawbacks of using each model individually. The obtained result is very encouraging. Generally, using different dataset yield different result of FRR and FAR even if the same approach is used.

References

[1] M. K. Kalera, S. Srihari, and A. Xu, "Offline signature verification and identification using distance statistics," Int. J. Pattern Recognit. Artif.Intell. (IJPRAI), vol. 18, no. 6, pp. 1339–1360, 2004.

[2] R. Sabourin, M. Cheriet, and G. Genest, "An extended-shadow-code based approach for offline signature verification," in Proc. 2nd Int. Conf. Doc. Anal. Recognit. (ICDAR-2), Tsukuba Science City, Japan, Oct.1993, pp. 1–5.

[3] J. Pan and S. Lee," Offline Tracing and Representation of Signatures," Proc. CVPR, pp. 679–680, 1991.

[4] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," Pattern Recognit., vol. 35, no. 12, pp. 2963–2972, Dec. 2002.

[5] V. S. Nalwa, "Automatic on-line signature verification," Proc. IEEE, vol. 85, no. 2, pp. 215–239, Feb. 1997.

[6] R. S. Kashi, J. Hu, W. L. Nelson, and W. L. Turin, "A hidden Markov model approach to online handwritten signature verification," Int. J. Doc. Anal. Recognit. (IJDAR), vol. 1, no. 2, pp. 102–109, 1998.

[7] M. E. Munich and P. Perona, "Visual identification by signature tracking," IEEE Trans. Pattern Anal.Mach. Intell. (T-PAMI), vol. 25, no. 2, pp. 200–217, Feb. 2003.

[8] T. Hastie, E. Kishon, M. Clark, and J. Fan, "A model for signature verification", Proc. 1991 IEEE Int. Conf. on Syst., Man, Cybern., vol. 1, pp.191 - 196 , 1991.

[9] A. Kholmatov," Biometric Identity Verification Using on-line & off-line signature Verification," Master's thesis, Turkey. Sabanic University, p. 17, 2003.

[10] G. V. Kiran, R. S. Kunte, and S. Samuel, "On-line signature verification system using probablistic feature modeling," in Proc. 6th Int. Symp. Signal Process. Appl., Kuala Lampur, Malaysia, 2001, vol. 1, pp. 355–358.

[11] R. Plamondon and G. Lorette, "Automatic signature verification and writer identification—The state of the art," Pattern Recognit., vol. 22, no. 2, pp. 107–131, Jan. 1989.

[12] Mingfu Zou, Jianjun Tong, Changping Liu and Zhengliang Lou," On-line Signature Verification Using Local Shape Analysis," Proceedings of the Seventh International Conference on Document Analysis and Recognition (ICDAR 7), vol. 1, Edinburgh, U.K., Aug. 2003, pp. 314–318.

[13] Kholmatov A. and Yanikoglu B," Biometric Authentication using Online Signatures," Berlin, Springer, 3280, 2004.

[14] Rioja F. R., Mariko N. M., Hector P. M. and Karina T. M, "Dynamic features Extraction for on-line signature verification," Preceeding of the 14th international conference on electronic, communication and computers. IEEE, 156-161, 2004.

[15] Julian Fierrez-Aguilar, Loris Nanni, Jaime Lopez-Pe˜nalba, Javier Ortega-Garcia1 and Davide Maltoni,"An On-Line Signature Verification System Based on Fusion of Local and Global Information," Springer Berlin / Heidelberg, vol: 3546/2005, pp. 523-532.

[16] Marzuki Khalid, Hamam Mokayed, Rubiyah Yusof and Osamu Ono,"Online Signature Verification with Neural Networks Classifier and Fuzzy Inference," Third Asia International Conference on Modelling & Simulation. IEEE, 236-241, 2009.

[17] Christian Gruber, Thiemo Gruber, Sebastian Krinninger, and Bernhard Sick," Online Signature Verification with Support Vector Machines Based on LCSS Kernel Functions," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART B: CYBERNETICS, VOL. 40, and NO. 4, pp. 1088-1100, 2010.

[18] Ahmed Galib Reza, Hyotaek Lim, and Md Jahangir Alam," An Efficient Online Signature Verification Scheme Using Dynamic Programming of String Matching, "Springer, LNCS, vol: 6935, pp. 590–597, 2011.

[19] SVC2004 dataset that held on the "First International Signature Verification Competition," http://www.cse.ust.hk/svc2004/.

AUTHORS PROFILE

Dr. Mohammed J. Alhaddad received his Master from Essex University in 2001, and he obtained PhD from the school of Computer Science and Electronic Engineering, University of Essex in 2006, UK. He became Chairman of Information Technology Department at King Abdul-Aziz University. His research interests include Working on the development of E-Government in Saudi Arabia.

and working to use the latest technologies that may help to improve the quality of services provided by government agencies, Beside studying the ways of linking the data of associated government agencies with each other to insure a maximum integration for the concept of E-Government, Also studying the ways of developing the human element, which oversees the functioning of the procedures automation and ensure the efficiency of the systems used, With continuously development to be up-to-dated in this field of work, Also Data Extraction from web pages, Information Retrieval from the Web, and various uses of rules in database system implementation, for example in Active Databases, Expert Databases, Semantic Query Optimisation, co-operative query answering, Distributed databases and Deductive databases.

He also interested in distributing Data Server Workload over multiple workstations in Local Area Networks. Previous work has included the design and construction of parallel processor hardware for fast processing of bulk data; the use of a commercially-available multiprocessor platform for deductive query processing; and other exploitations of the Active Memory concept where processing power is associated with stored data.

Current research interests are Network Security, Artificial Intelligence, Robots, Fuzzy System, Brain Computer Interface BCI, and Radio Frequency Identification RFID