A Novel Approach for Online Signature Verification Using Fisher Based Probabilistic Neural Network

Souham Meshoul
Center of Excellence in Information Assurance
IT Department, CCIS – King Saud University
Riyadh, Saudi Arabia
batouche@ksu.edu.sa

Mohamed Batouche
Center of Excellence in Information Assurance
Dept. of Software Engineering, CCIS – KSU
Riyadh, Saudi Arabia
smeshoul@ksu.edu.sa

Abstract—**The rapid advancements in communication, networking and mobility have entailed an urgency to further develop basic biometric capabilities to face security challenges. Online signature authentication is increasingly gaining interest thanks to the advent of high quality signature devices. In this paper, we propose a new approach for automatic authentication using dynamic signature. The key features consist in using a powerful combination of linear discriminant analysis (LDA) and probabibilistic neural network (PNN) model together with an appropriate decision making process. LDA is used to reduce the dimensionality of the feature space while maintining discrimination between users. Based on its results, a PNN model is constructed and used for matching purposes. Then a decision making process relying on an appropriate decision rule is performed to accept or reject a claimed identity. Data sets from SVC 2004 have been used to assess the performance of the proposed system. The results show that the proposed method competes with and even outperforms existing methods.**

Keywords-Online Signature Verification, Probabilistic Neural Network, Linear Discriminant Analysis.

I. INTRODUCTION

Biometric technology is becoming one of the most important supports providing security [1]. It is mainly required for authentication purposes. Biometrics is usually used in conjunction with other security alternatives like passwords and tokens to further improve security provided by the authentication system. The motivations that encouraged the use of biometrics are their reliability and also the difficulty to steal, to copy or relatively to forge biometric information. Biometric authentication consists in establishing identity using human traits like physiological characteristics (fingerprint, hand geometry, iris patterns…etc.) and behavioural ones (signature, keystroke,voice..etc). Selecting a particular biometric depends upon the targeted application, user preference and attitude, practicality issues, accuracy and also technological issues and level of security required. With the advent of high quality signature capture devices, signature is attracting more attention as a biometric to develop practical applications. Targeted applications are numerous and include banking, e-commerce, access control and e-government among others. The challenge is to develop an authentication system that is trustworthy and accurate enough. The difficulties inherent to signature based authentication are related to the great variability of signatures. Furthermore, forgers can reproduce signatures with high resemblance to the user's signatures. Forgeries range from simple to skilled. Generally, signature based authentication systems address two issues: signature verification and signature recognition. Signature verification refers to the process of accepting or rejecting a claimed identity given an input signature. Depending on the way signatures are represented and more precisely on the availability of time related information, methods for automatic signature based authentication (ASA) fall into two broad categories namely off-line methods and on-line methods [2]. In the first case, a signature is represented by an image obtained once the writing process is over by digitizing the signature written on a paper. In another way, an off-line process deals with a signature as a static two dimensional image that's why it is also known as static process in the literature [3]. On-line methods operate on dynamic features that are captured during the writing process using a specialized device. In this case a signature is viewed as an ordered list of points defined each by a list of features like x and y point coordinates, pen pressure, azimuth angle of the pen with the digitizing tablet and the altitude of the pen with the device. Other local and global features can be derived from these basic features such as velocity, acceleration, center of gravity…etc.

In quest of effective methods for online signature verification, we describe in this paper a method that relies on the following ideas. First signatures are represented by normalized dynamic features related to pressure, azimuth, altitude and distance to center of gravity which is a derived feature. Second, a linear discriminant analysis (LDA) is used to reduce the dimensionality of the feature space while maintaining discrimination between classes. LDA has been largely investigated with Principal Component Analysis (PCA) in the context of appearance-based object recognition and especially face recognition [4]. LDA focuses on the discrimination between classes whereas PCA describes data without paying any attention to the underlying class structure. PCA has been investigated for off-line signature recognition and verification in [5]. The third and core idea underlying our work consists in the use of a Probabilistic Neural Network (PNN) for effective verification. A PNN

978-1-4244-7755-5/10/$26.00 ©2010 IEEE

model is derived during an offline step using the projected reference signatures on the Fisher space. It is used during an online step to perform the matching task that helps in accepting or rejecting a claimed identity given a projected input signature. Then the output of the PNN is analyzed through a decision making process to deliver the final decision. For this purpose, we define a specific decision rule.

The rest of the paper is organized as follows. Section 2 provides an overview of the concepts and research work related to ASA. Section 3 emphasizes the processes used for feature extraction. Sections 4 and 5 are devoted to the description of the off-line and on-line process respectively. In section 6, we report on the conducted experiments and the obtained results. Finally, conclusions and perspectives are drawn.

II. Related Work

Like any other biometric system, a signature based system encompasses components for data acquisition and preprocessing, feature extraction, matching and decision making. A method for ASA can be viewed as a combination of the following choices: the feature space, the enrollment representation and the matching strategy. Feature space choice deals with the kind of features used (local vs global) upon which the related method is known to be function based or feature based respectively. Some methods suggest a fusion of both kinds of features [6]. The enrollment representation consists in defining the way a user is viewed in the database. Two alternatives are possible. Either a template is assigned to each signature in the training set or a statistical model is derived for each user using its set of genuine signatures. The first alternative is the essence of reference-based methods whereas the second is related to model-based methods. The matching strategy choice refers to the method used to compute a matching score between signatures in order to assess similarity between them. This choice is largely influenced by the kind of features used. Function-based methods use generally strategies like Dynamic Time Warping [7-9] and Hidden Markov Models [10, 11] whereas feature-based methods rely on statistical techniques like Mahalanobis distance [12]. Most of these methods make use of a decision threshold to accept or reject the matching results. Determining the value of this threshold is challenging.

III. Feature Extraction

Feature extraction is one of the critical parts of any signature based system. In our work, we make use of dataset available at SVC2004 online signature database [13]. For each signature, the provided dynamic features are x-coordinate, y-coordinate, Time stamp, Button status, Azimuth, Altitude, and Pressure. Figure 1 shows one of the existing signatures with a plot of some related features.

In order to obtain features which are rotation, shift and scale invariant with fixed size, a preprocessing on the original data which consists in data normalization and sampling was performed. Data normalization [9] aims to scale the values of the pressure, azimuth and altitude to the range [0, 1]. For each signature point with coordinates (*x*,*y*), the distance to the center of gravity has been derived as suggested in [14]. Distance values have been normalized with regard to the highest distance. This new dynamic parameter is denoted by *G*. Figure 2 illustrates the derived dynamic parameter *G* for the above signature example.

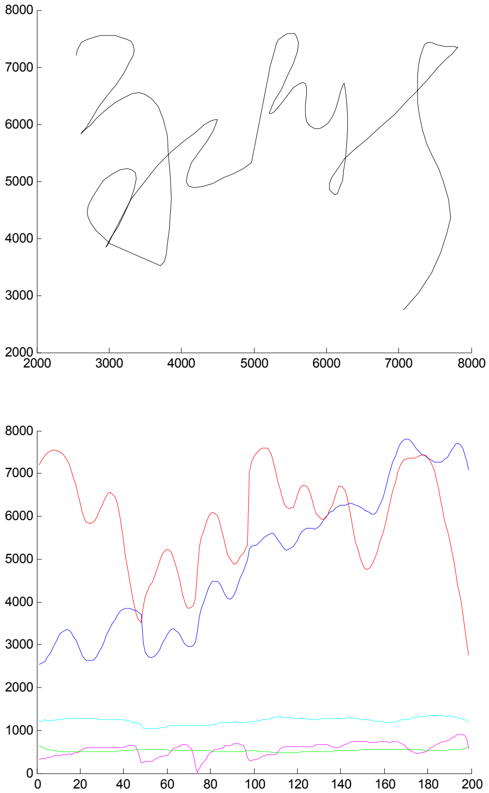

Figure 1. An online signature and its related dynamic parameters (SVC 2004 dataset – user 7).

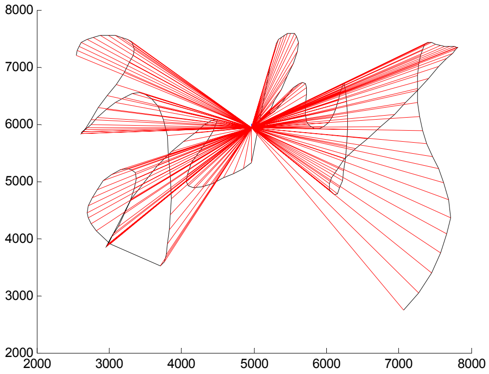

Figure 2. Dynamic parameter *G*: distances of signature points to the center of gravity.

Finally, data sampling has been used to reduce the number of signature points in a way to get a fixed number of equidistant points while keeping critical points given by button status (pen ups). Figures 3 and 4 show the principle of such sampling process.

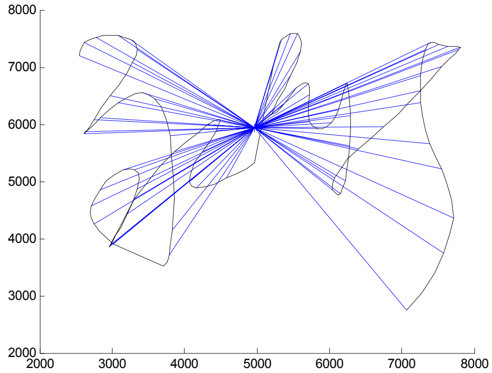

Figure 3. Distances from center of gravity after sampling and inclusion of critical points.

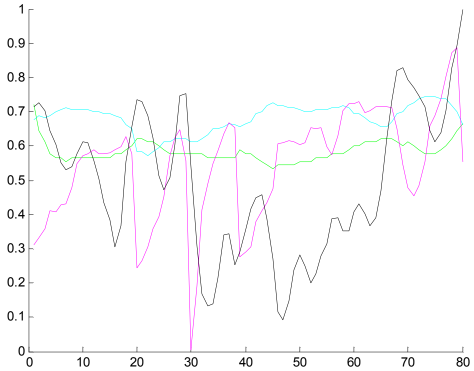

Figure 4. Dynamic parameters after normalization and sampling: *G*, Pressure, Azimuth and Altitude.

IV. THE OFF-LINE PROCESS: PNN MODEL CONSTRUCTION

The off-line process aims to construct the PNN model using the enrolled signatures in the database. As shown in figure 5 this process encompasses several steps: feature extraction as described in section above, feature space reduction using Linear Discriminant Analysis (LDA), signature projection on the obtained Fisher space and finally PNN model generation.

During this step, all the training signatures are used. First, they are processed as explained in section 2. For every signature, the dynamic parameters after sampling and normalization G (distances to the center of gravity), pressure (P), azimuth (Az) and altitude (Al) are recorded. Then the whole dataset is used as input to linear discriminant analysis (LDA) component. Every signature is represented by the vector of all selected features. Operating in the manner described in section III.A, LDA provides Fisher discriminants which are linear combination of original signatures features. These ones allow to best discriminate between users by grouping signatures of the same user and separating signatures of different users. The training signatures are then projected onto Fisher space leading to a set of features vectors which are used to train PNN in order to derive its model as outlined in section III.B.

In the following, more emphasis on feature space reduction and PNN model construction is given.

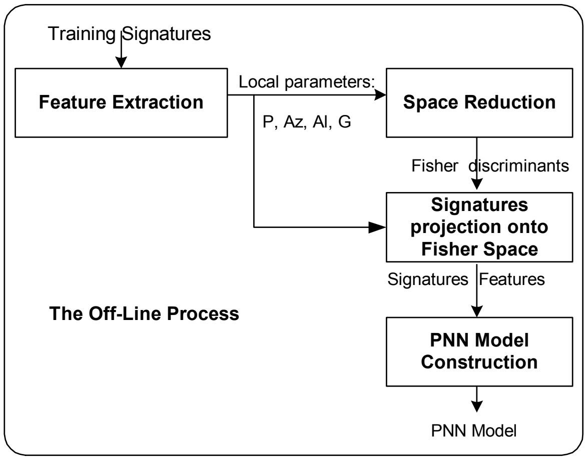

Figure 5. Training Fisher-based PNN for signature verification.

A. LDA for Feature Space Reduction

The goal of Linear Discriminant Analysis (LDA) also called Fisher Discriminant Analysis is to find an efficient way for maximum discrimination between classes in addition to dimensionality reduction. Emphasizing the theoretical background of LDA is beyond the scope of this work. In the following, we explain its use in our context; one can refer to [4, 15, 16] for an in-depth study. LDA searches for Fisher discriminant vectors which group signatures of the same user and separates signatures of different users. Signatures are projected from N-dimensional space (*N* is the number of feature vector) to *C*-1 dimensional space (*C* corresponds to the number of users). More formally, the basic idea of LDA is to determine those vectors so that the Fisher Index det|S_b|/det|S_w| is maximized. For this purpose, for all signatures of all users, two measures are defined:

- The within class scatter matrix S_w which measures the amount of scatter between signatures of the same user and is given by:

$$S_w = \sum_{j=1}^{C} \sum_{i=1}^{N_j} \left(x_i^j - \mu_j\right)\left(x_i^j - \mu_j\right)^T \qquad (1)$$

where N_j is the number of signatures for user j, x is a signature vector, i denotes the i-th signature vector for user j, and μ_j refers to the mean vector of class j.

- The between class scatter matrix S_b which measures the amount of scatter between different users and is given by:

$$S_b = \sum_{j=1}^{C} (\mu_j - \mu)(\mu_j - \mu)^T \tag{2}$$

where μ refers to the mean vector of all signatures.

LDA produces an optimal linear transformation which maps the input space to the projection space. Assuming that S_w is non-singular, the basis vectors of this function correspond to the first (C–1) eigenvectors with the largest eigenvalues of $S_w^{-1}S_b$.

B. Probabilistic Neural Network Construction

Probabilistic Neural Networks (PNN) introduced by Donald Specht in 1988 [17, 18] are a kind of radial basis network suitable for classification problems. They are the neural network implementation of kernel discriminant analysis and produce outputs with Bayes posterior probabilities. Contrary to backpropagation, the PNN training process is very fast (many orders of magnitude faster) and converges to a global optimum (no local minima issues).

PNNs are based upon the Bayes strategy for decision making and Parzen window estimation [18]. Using the latter technique, the probability density functions (PDF) required by Bayes' theory can be easily determined. Suppose n is the number of training samples, m is the feature space dimension, and x_i is the i-th training sample for a certain class (user 1 for example), then the Parzen estimate of the PDF for class 1 is [19,20]

$$F_1(x) = \frac{1}{(2\pi)^{m/2}\sigma^m n}\sum_{i=1}^{n}\exp[-\frac{(x-x_i)^T(x-x_i)}{2\sigma^2}] \tag{3}$$

The σ is the ‘‘smoothing parameter’’ which represents the single free parameter for this algorithm. This parameter is determined experimentally by comparing the results obtained for different values of this parameter σ.

As shown in figure 6, PNN architecture is like multilayered feedforward network with four layers: an input layer, a pattern layer, a summation layer, and an output layer.

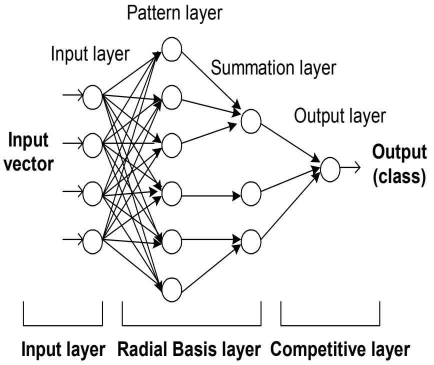

Figure 6. Probabilistic neural network architecture.

The input layer merely distributes features of input vector (input signature) to the pattern layer. The latter, with one neuron for each training sample (training signature), is fully connected to the input layer. The weights w_i for these connections are set equal to the different training patterns. After the input pattern (input signature) x and the weights w_i are normalized to unit, the pattern layer computes distances from the input vector to the training samples and produces a vector whose elements indicate how close the input is to a training sample. Each neuron j performs a radial transfer function which can be simplified as follows:

$$\exp\left(\frac{x^T w_j - 1}{\sigma^2}\right) \tag{4}$$

The pattern layer neurons representing the same class are connected to the same summation unit. The summation layer, with one neuron for each class (user), sums the outputs of pattern layer for each class and produces outputs which represent the probabilities that the vector (signature) belongs to each class (user). Finally, the output layer picks the maximum of these probabilities, and provides the target class (target user) for the input vector (signature) given by:

$$\text{targetclass}(x) = \arg\max(\frac{1}{n_i}\sum_i \exp((x^T.w_i - 1)/\sigma^2)) \tag{5}$$

where n_i is the number of patterns (training samples) of the i-th class.

V. The On-line process: Signature Verification

Given an input signature x and a claimed identity id, signature verification aims to accept or reject the claim. In other words, the process consists to check whether the input signature can be part of the class of genuine signatures or the class of forgeries related to the claimed person. As shown in figure 7, during the on-line process, features are first extracted using the input signature x. Then it is projected onto the Fisher to derive discriminant features used as input to the constructed PNN. PNN acts as a matcher. It identifies the user class to which the input signature x is more related. The PNN output denoted by *idout* along with the claimed identity *id* are the principal ingredients of the decision making process. Accepting or rejecting the claimed identity is determined by the following decision rule:

```
if ( idout = id) & (strength(idout) ≥ threshold)
  accept the claimed identity id (genuine)
else
  reject the claimed identity id (forgery)
end
```

Strength(*idout*) is the matching score implicitly provided by PNN. It is derived from eq. 5 as follows:

$$Strength\,(idout) = \frac{1}{n_i}\sum_i \exp((x^T.w_i - 1)/\sigma^2) \qquad (6)$$

n_i and w_i are respectively the number of patterns (training signatures) and their corresponding weights related to the output class *idout*.

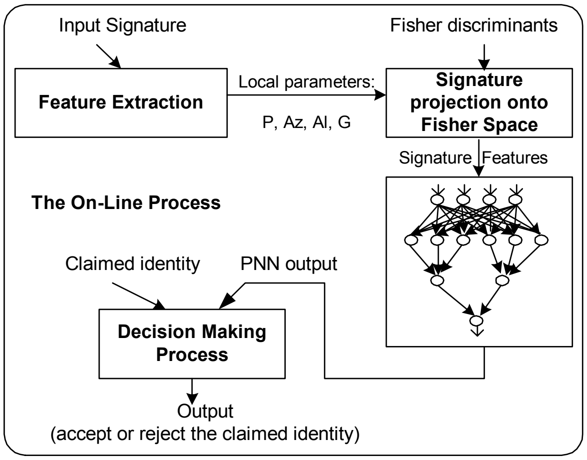

Figure 7. Flowchart of verification process.

The key idea underlying the decision making process is that the decision to accept or reject a claim is not only based on the output of the PNN but also on the strength of such output.

VI. Results and Discussion

Several experiments have been conducted to assess the performance of the proposed approach. The 40 sets of signature data provided in SVC2004 task2 have been used. Every set corresponds to a user and includes 20 genuine signatures and 20 skilled forgeries. 80% of genuine signatures are used for training and the rest of genuine and all of forgery signatures (skilled forgeries) are used for testing purposes. The experimental protocol has been carried out to study the significance of the different combination of features for verification purposes and to set tunable parameters.

Some kind of feature selection has been performed and EER (Equal Error Rate) has been recorded for each combination of local parameters. Results has been gathered in Table 1. An EER of 6.44% has been achieved when using the combination of parameters: Altitude and Pressure.

Table 1. Obtained results for different subsets of features.

Subset of parameters	Obtained EER using Fisher based PNN
Pressure, Azimuth	8.19%
Pressure, Altitude	**6.44**%
Altitude, Azimuth	8.37%
G, Pressure	10%
G, Azimuth	6.88%
G, Altitude	10.06%
Pressure, Altitude, Azimuth	7.50%
Pressure, Azimuth, G	10.75%
Pressure, Altitude, G	8.87%
Altitude, Azimuth, G	12.06%
G, Pressure, Altitude, Azimuth	9.94%

The EER corresponds to the value of threshold where the False Acceptance Rate (FAR) is equal to the False Rejection Rate (FRR) as shown on figure 8. In our experiments, only three parameters need to be set: the smoothing parameter used in PNN, the number of Fisher discriminants (from 1 to 39), and the preset threshold. Best results were obtained with the smoothing parameter set to 0.1, the number of Fisher discriminants set to 20, and the threshold set to the value corresponding to an EER equal to 6.64.

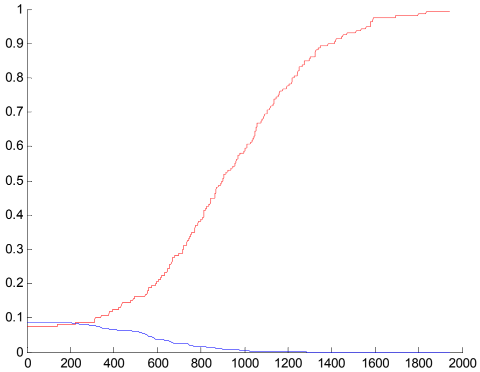

Figure 8. Plot of FAR and FRR rates for diffent values of threshold.

For sake of comparison, the obtained results were compared against those of other systems like the best SVC2004 system and Neural Nets based system [21]. As shown on table 2, our system competes with these systems.

Table 2. Comparison with other systems using skilled forgeries.

	Best SVC2004 system	Spatio-Temporal Neural Networks	Fisher Based PNN
FAR %	6.90	7.50	6.64
FRR %	6.90	12.81	**6.64**
EER %	6.90	-	**6.64**

VII. Conclusions and Future Work

In this paper, we described an effective method for on-line signature verification. This method can be abstracted as a combination of the following choices:

- Use of a set of local parameters namely pressure, azimuth, altitude and distance to center of gravity.

- Reduction of the feature space while keeping separation between users through linear discriminant analysis.

- Use of PNN model to find a match to the input signature.

- Use of an appropriate rule for decision making that takes into account the matching score.

The method has been assessed using datasets from SVC2004 database. The obtained results are very encouraging and show the effectiveness of the proposed method.

As future work, we plan to investigate other features and carry out an in-depth study of the impact of sets of features on the method.

References

[1] Jain, A. K., Ross, A. and Pankanti, S. Biometrics: A Tool for Information Security. IEEE Transactions on Information Forensics and Security, 1(2) (2006) 125-143.

[2] D. Kalenova, “Personal Authentication Using Signature Recognition”, Department of Information Technology, Laboratory of Information Processing, Lappeenranta University of Technology, 2003.

[3] R. Sabourin. “Off-line signature verification: recent advances and perspectives”, volume 1339, chapter Lecture Notes in Computer Science, LNCS, pages 84–98. Springer, 1997.

[4] A. M. Martinez, A. C. Kak, PCA versus LDA, IEEE Trans. On PAMI, 23(2): 228-233, 2001.

[5] A. Ismail, M. A. Ramadan, T. El Danf, A. H. Samak, Automatic signature recognition and verification using principal components analysis, Proceedings of 5^{th} International Conference on Computer Graphics, Imaging and Visualization, pp. 356-361, 2008.

[6] Fierrez-Aguilar, L. Nanni, J. Lopez-Penalba, J. Ortega-Garcia, and D. Maltoni. An online signature verification system based on fusion of local and global information. In Proc. of IAPR Intl. Conf. on Audio- and Video-Based Biometric Person Authentication, AVBPA, pages 523–532. Springer LNCS-3546, 2005.

[7] M. Yasuhara and M. Oka. Signature verification experiment based on nonlinear time alignment: a feasibility study. IEEE Trans. on Systems, Man and Cybernetics, part C, 12(3):212–216, 1977.

[8] A. Kholmatov and B. Yanikoglu. Identity authentication using improved online signature verification method. Pattern Recognition Letters, 26(15):2400–2408, 2005.

[9] Marcin Adamski and Khalid Saeed, **“**Online Signature Classification and its Verification System”, in proceedings of the 7th Computer Information Systems and Industrial Management Applications – CISIM, pp. 189-194, 2008.

[10] D. Muramatsu and T. Matsumoto. An HMM signature verifier incorporating signature trajectories. In Proc. of Intl. Conf. on Document Analysis and Recognition, ICDAR, volume 1, pages 438–442. IEEE Press, 2003.

[11] M. Fundez – Zanuy, “Signature recognition state-of-the-art”, IEEE Aerospace and Electronic Systems Magazine, pp. 28-32, July 2005.

[12] J. Galbally, J. Fierrez, M. R. Freire, and J. Ortega-Garcia. Feature selection based on genetic algorithms for on-line signature verification. In Proc. of IEEE Workshop on Automatic Identification Advanced Technologies, AutoID, pages 198–203, 2007

[13] Yeung D., Chang H., Xiong Y., George S., Kashi R., Matsumoto T. and Rigoll G., “SVC2004: First International Signature Verification Competition,” Proceedings of the International Conference on Biometric Authentication, Hong Kong, 2004, pp. 16-22.

[14] P. Moallem, K. Faez, “On Line Signature Pattern Recognition using Feature String and Neural Network”, Proceedings of HC-200 Conference, Japan, Sept. 6-9 2000, pp. 143-146.

[15] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, “Eigenfaces vs. fisherfaces: Recognition using class specific linear projection,” IEEE Trans. Pattern Anal. Machine Intell., vol. 19, no. 7, pp. 711–720, Jul. 1997.

[16] K. Fukunaga, Introduction to Statistical Pattern Recognition, 2nd Edition, Academic Press, New York, 1990.

[17] D. F. Specht, Probabilistic neural networks, Neural Networks 1 (3) (1990) 109–118.

[18] D. F. Specht and P. D. Shapiro, "Generalization Accuracy of Probabilistic Neural Networks compared with Back-Propagation Networks," Proceedinns of the International Joint Conference on Neural Networks, Vol. 1, pp. 887-892, Seattle, Washington, July 1991.

[19] D. F. Specht, “Enhancements to Probabilistic Neural Networks”, International Joint Conference on Neural Networks, vol. I, pp. 761-768, June 1992.

[20] G.M. Sun, X.Y. Dong, G.D. Xu. Tumor tissue identification based on gene expression data using DWT feature extraction and PNN classifier. Neurocomputing, 69:387-402, January 2006.

[21] M.M. Fard, M.M. Fard, N. Mozayani. A New On-line Signature Verification by Spatio-Temporal Neural Network. ISI 2008, Taipeo, Tawan, pp. 233-235, , June 2008.