

Handwritten Signatures Authentication Using Artificial Neural Networks Committee Machines

Milton R. Heinen and Paulo M. Engel

UFRGS, Informatics Institute,
Porto Alegre, RS, Brazil, 91501-970
mrheinen@inf.ufrgs.br, engel@inf.ufrgs.br

and

Fernando S. Osório

UNISINOS, Applied Computing,
São Leopoldo, RS, Brazil, 93022-000
fosorio@unisinós.br

Abstract

The main goal of this paper is to describe our study, research and implementation of a handwritten signatures authentication system based on a committee of artificial neural networks. This system is composed of three modules, the data acquisition module, responsible for on-line users' signatures data input through a pen tablet device, the preprocessing module, responsible for the extraction of representative signature features, and the neural module, that learns how to recognize users' signatures, classified as authentic or not, through the use of an artificial neural network. Several experiments were accomplished using a 2440 real signatures database, and the obtained results were very satisfactory.

1 Introduction

Nowadays, one of main problems in computer security systems is the users' authentication, that is, how to assure that the one is trying to access a system is really the legitimate user. In many information systems, the users' authentication is assured through the use of alphanumeric passwords, which need to be memorized by the users and maintained safe from other people. Even if this is the most used users' authentication method, password authentication has some important security vulnerabilities, mainly because passwords can be easily stolen by someone else.

In order to overcome this password related security problem, biometric authentication techniques based on physiological characteristics, like fingerprint identification, iris and retina recognition were also adopted to guarantee users' authenticity [21]. These techniques are much more secure and effective than passwords, but there were some disadvantages, mainly because they are very intrusive [3, 11]. For example, fingerprint identification have a negative connotation, because this procedure is related to criminal investigations [10].

Beyond the human physiological biometric features, we can also adopt behavioral biometric characteristics for users' authentication, as for example handwritten signatures [11, 24]. Behavioral biometric methods have several advantages related to other techniques. The first advantage is directly related to the security level, because in opposition to passwords, even if someone knows the user signature, usually it is not possible to reproduce easily this signature. The reproduction of a signature is more difficult as, besides the final signature shape, we include behavioral parameters related to user pen movements. The other advantage come from the user's comfort, because users have the habit of use handwritten signatures in business transactions, and they feel secure regarding this authentication method. The degree of intrusion presented in signature authentication systems is very low, and the necessary hardware has a low cost too (usually costing from U\$30 to U\$100).

Although it has the described advantages, the handwritten signatures authentication is a problem difficult to solve. This is due to the large variability that exists between signatures of different people and even in

the signatures of a single person [9]. This variability leads to the use of solutions based on machine learning techniques, like artificial neural networks, to achieve better results compared to other solutions [2].

This paper describes our research relative to the handwritten signatures authentication using artificial neural networks (ANN). In our previous works [5, 6, 7, 8], the authentication process was accomplished by an only neural network. In this paper, a committee of neural networks [4] were used for to improve the readability of the authentication process. It is structured as follows: initially we present some concepts associated to signature authentication and artificial neural networks, describing the main ideas related to the authentication method adopted in this work; after this, the proposed model is detailed, describing the system modules (data acquisition module, preprocessing module, and neural module), and to conclude we show our experiments results, obtained using the system prototype, presenting some final remarks and future research perspectives.

2 Handwritten signature authentication

A signature authentication system is a software responsible for validating signatures, indicating if a signature is authentic or not. When a signature is not authentic, probably it can be categorized in one of these three different forgeries [1, 5]:

- Random forgeries: these forgeries are accomplished by people that ignore the design of the original signatures, or don't have the ability to correctly reproduce it;
- Traced forgeries: these forgeries are accomplished following the original signature outline available in a printed form, resulting in a forgery with a shape quite close to the original signature shape;
- Skilled forgeries: these forgeries are accomplished by expert people that possesses the ability to reproduce signatures in a very satisfactory way [15].

The signatures data acquisition and authentication can be implemented in two different ways: on-line and offline [1]. The offline authentication method uses previously drawn signatures in paper sheets, which are digitalized later using a scanner. After that, they are treated by the signature authentication system. The on-line signature authentication systems use a special hardware device to directly input the signature drawn to the system, like a Pen Tablet (Figure 1).



Figure 1: Example of a digitalizing tablet

The on-line signature authentication has several advantages related to the offline authentication [5, 7]:

- Captures more information: besides the visual signature features, it is also possible to obtain temporal and dynamical signature information (user behavioral information);
- Captures better information: a scanner digitalized signature can have a high level of noise (image artifacts and distortions), what hinders the authentication process. Pen tablet devices can provide better signature data.
- Popularization of tablet based input devices (e.g. palmtops, handhelds and tablets), simplify data acquisition.

In this work, we chose to use on-line signatures' authentication due to these main advantages, and also because we consider this method more effective and well adapted to electronic transactions.

3 Machine learning

According to Mitchell [14], a program is capable to learn when its performance is improved with the experience in a certain task. So, to define a machine learning problem, we should identify three fundamental characteristics: the task to be learned, the performance measure and the experience source. It is also necessary that the knowledge to be learned through the experience, called objective function, must be well defined. In the case of signatures authentication, the knowledge that must be learned is a signature database composed of previously well classified as authentic or not signatures. This kind of application problem adopts supervised machine learning methods. Therefore, the task to be learned is the signature classification, the experience source is the signatures database and the performance measure is the evaluation of the correct answers rate in the overall signature authentication task. Nowadays, several machine learning techniques can be used for signatures' authentication, as for example, induction of decision trees, fuzzy inference systems, genetic algorithms and artificial neural networks.

3.1 Artificial neural networks

Through the use of an abstract and simplified model of human neurons, is possible to develop a neural simulator capable to classify, to generalize and to learn how to classify and approximate functions [18, 19]. One of the most used neural learning models is the so called multi-layer Perceptron (MLP) with back-propagation learning algorithm [22, 19, 4]. Some improved versions of the original back-propagation algorithm were developed in the few past years, and the RPROP algorithm [20] become an interesting choice among them.

The RPROP algorithm performs a direct adaptation of the weight step (learning rate) based on local gradient information. To achieve this, each weight has its individual update value Δ_{ij} , which solely determines the size of the weight update. This adaptive update-value evolves during the learning process based on its local sight of the error function E , according to the following learning-rule [20]:

$$\Delta_{ij}^{(t)} = \begin{cases} \eta^+ * \Delta_{ij}^{(t-1)}, & \text{if } \frac{\partial E}{\partial w_{ij}}^{(t-1)} * \frac{\partial E}{\partial w_{ij}}^{(t)} > 0 \\ \eta^- * \Delta_{ij}^{(t-1)}, & \text{if } \frac{\partial E}{\partial w_{ij}}^{(t-1)} * \frac{\partial E}{\partial w_{ij}}^{(t)} < 0 \\ \Delta_{ij}^{(t-1)}, & \text{else} \end{cases} \quad (1)$$

where $0 < \eta^- < 1 < \eta^+$, $\frac{\partial E}{\partial w_{ij}}$ is the partial derivative of the error function for the weight w_{ij} , and $\Delta_{ij}^{(t-1)}$ is the last weight update.

In order to learn a specific task, it is necessary a database containing training examples with input patterns and expected answers (patterns and their corresponding classes). This learning database is presented to the artificial neural network, which can learn how to answer in a similar way to the database examples, classifying the patterns. It can also be used a second database for learning validation (evaluation of generalization level), that is only used to evaluate the ANN performance (it is not used to adjust the ANN parameters and weights). This second database is different from the one used in the learning task [18]. This type of learning is known as supervised learning with cross-validation [4].

Through an iterative process, learning database examples are presented to the artificial neural network, adapting the neural network connection weights. These weights simulate the reinforcement and inhibition of synaptic connections present in real neurons. The neural learning occurs from this weights adaptation. The weights' optimizations are responsible to do the neural network learn how to answer correctly to the input data, accordingly to the examples contained in the learning database.

3.2 Committee machines

Second [4], a committee machine as defined as a combination of various specialist neural networks, that in the case of supervised learning divide the classification task to each other. Those machines can be divided in two main categories: static structures or dynamic structures. In the static structures, the several specialists' answers are combined by a mechanism that does not depend of the input signals. In this category the ensemble average method are included, where the different specialists' outputs are lineally combined to produce the global exit. Using these method, the obtained performance will be at least the same, and possibly better to the best specialist acting individually [4].

4 Proposed system: NeuralSignX

The main goal of this paper is to propose a methodology for on-line handwritten signature authentication based on artificial neural networks. To validate our approach, a practical system was proposed and implemented in a prototype¹. In the proposed system, the signature authentication is accomplished in the following way:

- The signatures are collected and stored in a database;
- Some position and scale adjustments are accomplished over the signatures;
- Relevant features used in the authentication process are extracted from the signatures;
- The signatures' authentication is accomplished using neural networks.

The proposed system, called NeuralSignX System, is composed of three modules: data acquisition module, preprocessing module and neural classification module (learning and recognition).

4.1 Data acquisition module

In order to validate the proposed system, it was necessary the creation of a signatures database. Thus, it was developed a module of the system called data acquisition module. This module is responsible for read the signature data from the tablet and to save these data. This module generates a signature description file, where each signature is composed by a sequence of pen coordinates (x, y), state (1 or 0: drawing or pen lifted up) and time stamp for each captured point (in milliseconds). The pen tablet we used in the experiments with our system was a SuperPen WP4030, manufactured by UC-Logic². The Figure 2 shows an example of a typical signature (the captured points were highlighted).



Figure 2: Example of a typical signature

The signatures' database used in our experiments was collected during one year, and each user contributed with several signatures picked up in different moments, so typical variations that happen along the time in a signature are also present in the database. The composition of the 2440 signatures database was the following:

- 1800 authentic signatures, accomplished by 60 different users (30 signatures per user);
- 320 traced forgeries;
- 320 skilled forgeries;

In our initial experiments it was determined that about 10 signatures per user would be enough for an adequate neural network learning. Since the learning validation process needs more different signatures (cross-validation), we decided to collect up to 30 signatures per user, so we were able to learn and to test properly the authentication task. The traced forgeries [12]. were accomplished following the original signature outline available in a printed form, and the skilled forgeries were accomplished by expert people that practiced for some time until to be able to reproduce the authentic signatures in a very satisfactory way.

¹NeuralSignX – <http://www.inf.unisinos.br/~osorio/neuralsignx/>

²UC-Logic SuperPen – <http://www.superpen.com/>

4.2 Preprocessing module

The preprocessing module is subdivided in two stages. In the first stage, general position and scale adjustments are applied to the signatures, and in the second stage features are extracted from the signatures. These features are obtained from each signature allowing to differentiate signatures from one user from the signatures of other users. The adjustments implemented in the first stage are position adjustment, that minimizes the variations in the signature position, and scale adjustment, that resize the signatures to a standard size.

In the second stage of the preprocessing module, the signature features extraction is accomplished. Some techniques of signature features extraction used in NeuralSignX System were found in the literature [13, 25, 23], and many other features extraction techniques were created or specifically adapted by the authors, where a detailed description of them can be found in [17, 5, 8]. After the study and implementation of the signature features extraction methods, a new study was accomplished in order to verify the relevance of each feature, using the Principal Components Analysis [16]. The main signature features we selected to use in this work are:

Signature elapsed time: the signature time duration from the start until the end of the drawing (1 entry);

Quantity of pen lifts: the number of times that the pen leave the tablet during the drawing (1 entry);

Medium and maximum pen velocity: the overall medium speed and the maximum speed of pen movements (2 entries);

Cardinal points measure: the number of pseudo-vectors (simplified structural shape) that are pointing to each cardinal point section (N, S, E, W, NE, NW, SE, SW). The Figure 3 shows the cardinal point sections defined and some signature pseudo-vectors (8 entries);

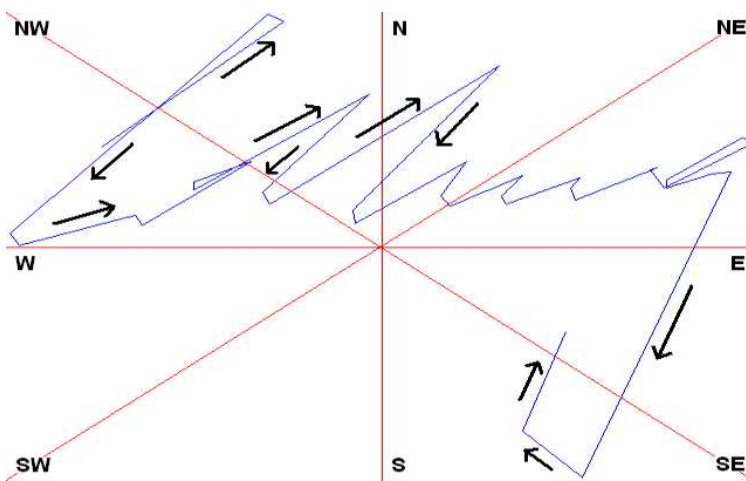


Figure 3: Cardinal sections

Signature density grid: the signature is divided in several cells, and for each cell the density (number of points falling into this cell) is calculated [2]. The Figure 4 demonstrates the use of this feature. In this figure, the high density cells in the grid are darker, and the less dense the cells are the brighter is the cell filling color. This feature is composed by several attribute values, one value for each cell of the grid (48 entries);

Vertical and horizontal line intersections: the bitmap containing the signature is intersected by virtual lines that cut the signature in fixed intervals, and for each virtual line we count how many times this line intersects the signature drawing. In the Figure 5, several vertical and horizontal lines, used to count the intersections, are shown over a signature. This feature is also composed by several attribute values, one for each line intersection counter (26 entries).

4.3 Neural module

The neural module receives the signature features, obtained by the preprocessing module, and uses them to classify the signatures as authentic or not. This module is composed by a committee of three specialists, as it illustrates Figure 6. Each specialist was implemented using a MLP neural network with three layers,

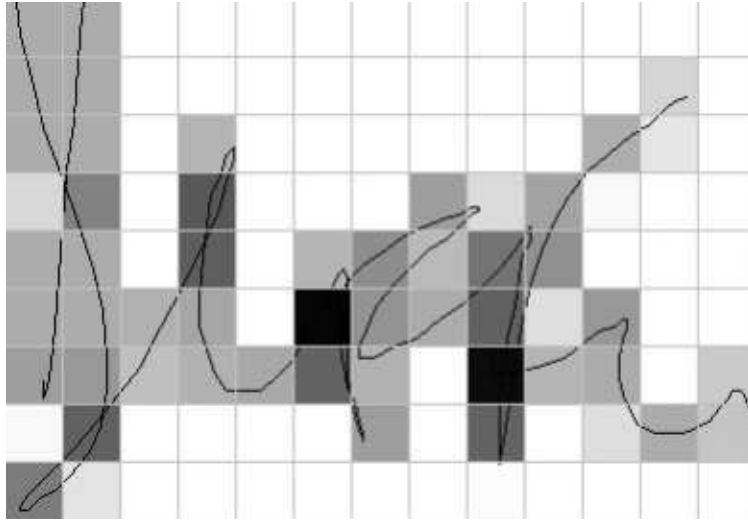


Figure 4: Signature density grid

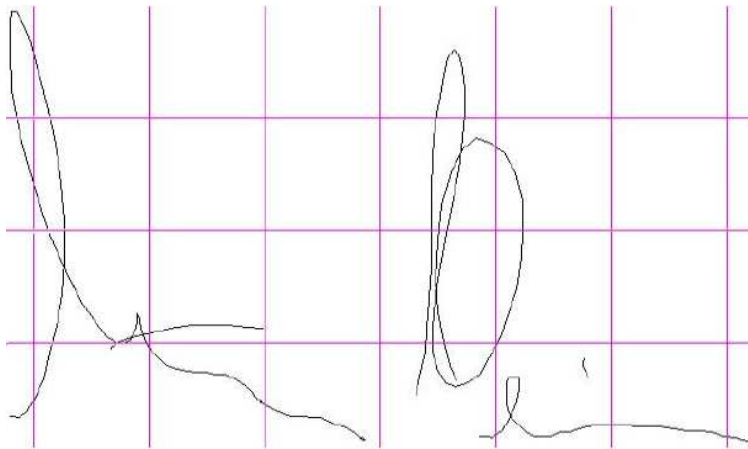


Figure 5: Line intersections

structured in the following way:

- **Esp A:** receives in the input layer only the *signature density grid* feature. It has 48 inputs, 2 hidden neurons and 1 output (101 synaptic weights);
- **Esp B:** receives in the input layer only the *Vertical and horizontal line intersections* feature. It has 2 inputs, 3 hidden neurons and 1 output (85 synaptic weights);
- **Esp C:** receives in the input all the other features. It has 12 inputs, 4 hidden neurons and 1 output (57 synaptic weights);

Thus, instead of a single neural network with 86 inputs, the classification task is accomplished using three smaller neural networks, reducing the computational complexity and the overfitting risk, due to the smaller amount of synaptic weights [4]. Besides, each specialist is composed by a committee of 5 identical neural networks initialized with different synaptic weights. The output values were calculated using the ensemble averaging method [4].

The artificial neural network simulator adopted was the Stuttgart Neural Network Simulator - SNNS³, it is a free software, and a quite complete neural network simulator that have several additional tools that

³SNNS – <http://www-ra.informatik.uni-tuebingen.de/SNNS/>

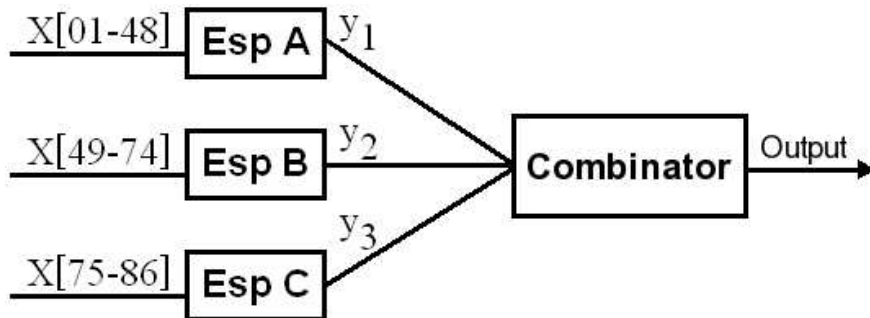


Figure 6: Specialists committee

allow us to create scripts and execute learning and simulation tasks in batch mode. The SNNS facilities also simplify the analysis of the obtained results and creation of graphic plots.

The learning algorithm used for weights optimization was the algorithm RPROP [20]. This algorithm was selected because it is more efficient, making the learning process much more fast. Second order methods, based on the Hessian matrix approximation, were discarded due to the amount of synaptic weights, that turns those methods slower than gradient descend methods [4]. The main ANN parameters we configured to use with the SNNS simulator are:

- Initial learning rate: 0.1
- Maximum learning rate: 1.0
- Weights initialization: [-0.001, 0.001]
- Number of generations: 1000

The Score threshold was fixed in 0.4, and the the activation function used was the sigmoid. The value 1.0 obtained in the output represents an authentic signature of a specific user, and the value 0.0 represents a non authentic signature of this user. In order to make the experiments statistically valid, the simulations were accomplished using a ten-fold cross-validation method. For each individual fold we also repeated 10 times the simulation using exactly the same data and parameters, with only different initializations of the weights. The obtained results are described in the Section 5 below.

5 Results

This section describes the main results obtained in the experiments accomplished using our system prototype. For to compare the performance of committee machine in relation to a single neural network, initially we performed experiments using a single neural network, composed of 86 inputs, 5 hidden neurons and 1 output (441 synaptic weights). Table 1 shows the results obtained in these experiments for 10 users randomly selected. For secure subjects, the users' identity was preserved. The values in Table 1 show the mean and the standard deviation of the 10 folds of each user, and for each fold were accomplished 10 distinct experiments, totalizing 1000 experiments.

The first column (U) shows the user identification number. The following columns show, respectively, the mean and standard deviation values of the following measures: correct authentication rate (HIT), false positive rate (FPR) and false negative rate (FNR). False positive (FP) authentications occur when a false signature is classified as authentic, and false negative (FN) authentications occur when an original signature is classified as not authentic. The last row of the table (μ) shows the general mean of each column. All the values presented in the Table 1 are expressed in percentages, excluding the user identification number. The false positive rate (FPR) and false negative rate (FNR), that are calculated through the following equations:

$$FPR = \frac{N_{FP}}{N_{cl0}} \times 100 \quad (2)$$

$$FNR = \frac{N_{FN}}{N_{cl1}} \times 100 \quad (3)$$

Table 1: Results using a single ANN

U	HIT		FPR		FNR	
	μ	σ	μ	σ	μ	σ
01	99.94	0.19	0.00	0.01	5.00	15.81
02	99.77	0.20	0.05	0.12	15.33	16.57
03	99.84	0.15	0.07	0.09	8.00	13.54
04	99.59	0.30	0.14	0.17	23.00	28.69
05	99.85	0.21	0.07	0.13	7.00	8.95
06	99.83	0.14	0.07	0.08	8.33	11.57
07	99.84	0.21	0.03	0.04	11.00	16.03
08	99.97	0.06	0.01	0.04	1.33	3.22
09	99.98	0.07	0.02	0.08	0.00	0.00
10	99.96	0.05	0.02	0.04	1.33	3.22
μ	99.86	0.16	0.05	0.08	8.03	11.76

where N_{FP} is the number of false positives, N_{FN} is the number of false negatives, N_{C10} is the number of patterns of the class 0 and P_{C11} is the number of patterns of the class 1.

Observing the results in Table 1, it is noticed that the correct authentication rate (HIT) are quite high, what demonstrates that the system performance is reasonably satisfactory. In relation to the false positive rate (FPR), although they are very small (0.05% in mean), nevertheless they are preoccupying in a signatures authentication system. Already false negative rate (FNR), this is very high (8.03% in mean), whats may cause a certain users' rejection of the system. Thus, we hoped that using the committee machine these results may be significantly improved.

Table 2 shows the results obtained in the experiments accomplished using the committee machine described in the Section 4.3 The values in Table 2 shows the mean and the standard deviation of the 10 folds of each user, and for each fold were accomplished 10 distinct experiments, totalizing 1000 experiments.

Table 2: Results using a committee machine

U	HIT		FPR		FNR	
	μ	σ	μ	σ	μ	σ
01	100.0	0.00	0.00	0.00	0.00	0.00
02	99.84	0.20	0.00	0.00	13.33	17.21
03	99.96	0.12	0.00	0.00	3.33	10.54
04	99.96	0.12	0.00	0.00	3.33	10.54
05	99.96	0.12	0.00	0.00	3.33	10.54
06	99.92	0.17	0.00	0.00	6.67	14.05
07	100.0	0.00	0.00	0.00	0.00	0.00
08	99.92	0.17	0.00	0.00	6.67	14.05
09	100.0	0.00	0.00	0.00	0.00	0.00
10	99.96	0.12	0.00	0.00	3.33	10.54
μ	99.95	0.10	0.00	0.00	4.00	8.75

Table 2 results shows that there was an improvement in the correct authentication rate (HIT) to 99.95% in mean. The result more aimfull are the false positive rate (FPR), that were reduced to zero in all the accomplished experiments. In relation to the false negative rate (FNR), this was also reduced for 4% in mean.

Figures 7(a) and 7(b) shows, respectively, boxplot graphs for the false positive rate (FPR) and the false negative rate (FNR) in relation to the experiments of table 1 (bars "ANN" in the graphs) and table 2 (bars "Committee" in the graphs). Observing these graphs, it can be noticed that the results obtained with the committee machine are superior to the results of a single neural network. Thus, it is possible to affirm that the committee machines improves the security to signatures authentication process.

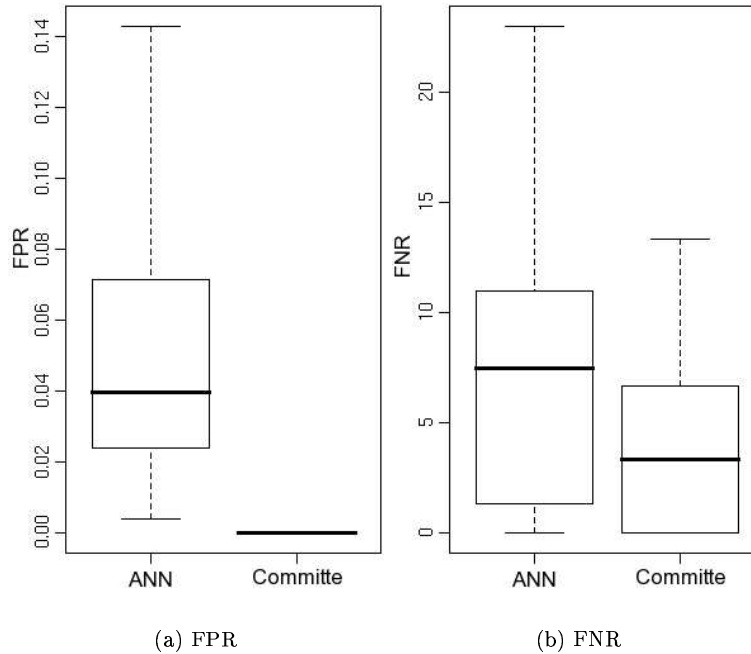


Figure 7: Boxplot graphics

6 Conclusions

The main goal of this work was the study, research and development of a signature authentication system that should be able to authenticate users based on handwritten signatures. In order to reach this objective an extensive study of several topics related to pattern recognition, signatures authentication, machine learning, artificial neural networks and committee machines, was accomplished. Our approach to deal with this problem was described and we implemented an on-line signature authentication system, called NeuralSignX. Our prototype implementation of the proposed signature authentication system is composed of three modules that implement the different process stages related to this task: on-line signature acquisition, preprocessing (signature positioning, scaling, feature extraction and selection), and signature training and recognition using a committee of artificial neural networks. The system prototype is complete and operational, and it was used to validate our approach and to evaluate the authentication system performance.

The results obtained in the simulations using our system prototype showed that this kind of on-line signature authentication system is not only viable, but it is also a very good solution to improve authentication security in information systems. The obtained results also proved that the artificial neural networks are very suitable to be used in signature authentication tasks. The signature features we proposed and selected were very effective allowing to obtain a proper signature classification system. The selected input features allowed the neural network to obtain high learning rates and a very good generalization level, resulting in low incorrect signature authentications rates. This high accuracy presented by the NeuralSignX system is fundamental to provide a really secure signature authentication system.

Our future research work is being directed to hybrid authentication systems. The hybrid systems, through the combination of different techniques (e.g. signatures, fingerprints, eye scanning, passwords, face recognition and voice), can improve authentication systems performance to a virtually unbreakable level of security.

References

- [1] ABBAS, R. Backpropagation networks prototype for off-line signature verification. Minor thesis, RMIT – Department of Computer Science, Melbourne, Australia, Mar. 1994.
- [2] BALTZAKIS, H., AND PAPAMARKOS, N. A new signature verification technique based on a two stage neural network classifier. *Engineering applications of Artificial intelligence* 14 (Sept. 2000), 95–103.

- [3] GUPTA, G., AND MCCABE, A. A review of dynamic handwritten signature verification. Technical report, James Cook Univ., Townsville, Australia, Nov. 1997.
- [4] HAYKIN, S. *Neural Networks: A Comprehensive Foundation*, 2 ed. Prentice-Hall, Upper Saddle River, NJ, 1999.
- [5] HEINEN, M. R. Autenticação on-line de assinaturas utilizando redes neurais. Final undergraduate dissertation, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, RS, Brazil, 2002.
- [6] HEINEN, M. R., AND OSÓRIO, F. S. Biometria comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas. *Infocomp: Revista de Ciência da Computação* 3, 2 (Nov. 2004), 32–37.
- [7] HEINEN, M. R., AND OSÓRIO, F. S. Autenticação de assinaturas utilizando algoritmos de aprendizado de máquina. In *Anais do V ENIA* (São Leopoldo, RS, Brazil, July 2005).
- [8] HEINEN, M. R., AND OSÓRIO, F. S. Handwritten signatures authentication using artificial neural networks. In *Proc. IEEE Int. Joint Conf. Neural Networks (IJCNN)* (Vancouver, Canada, July 2006).
- [9] HUANG, K., AND YAN, H. Off-line signature verification based on geometric feature extraction and neural network classification. *Pattern Recognition, V30, N1* (1997), 9–17.
- [10] JAIN, A. K., GRIESS, F. D., AND CONNELL, S. D. On-line signature verification. *Pattern Recognition* (Jan. 2002).
- [11] KHOLMATOV, A., AND YANIKOGLU, B. Identity authentication using improved online signature verification method. *Pattern Recognition Letters* 26, 15 (Nov. 2005), 2400–2408.
- [12] LAU, K. K., YUEN, P. C., AND TANG, Y. Y. Directed connection measurement for evaluating reconstructed stroke sequence in handwriting images. *Pattern Recognition* 38, 3 (Mar. 2005), 323–339.
- [13] LEI, H., AND GOVINDARAJU, V. A comparative study on the consistency of features in on-line signature verification. *Pattern Recognition Letters* 26, 15 (Nov. 2005), 2483–2489.
- [14] MITCHELL, T. *Machine Learning*. McGraw-Hill, New York, 1997.
- [15] NAMBOODIRI, A. M., SAINI, S., LU, X., AND JAIN, A. K. Skilled forgery detection in on-line signatures: A multimodal approach. In *Proc. 1st Int. Conf. Biometric Authentication (ICBA)* (Hong Kong, China, July 2004), vol. 3072 of *LNCS*, Springer-Verlag, pp. 505–511.
- [16] OJA, E. Principal components, minor components and linear neural networks. *Neural Networks* 5 (Mar. 1992), 927–935.
- [17] OSÓRIO, F. S. Um estudo sobre reconhecimento visual de caracteres através de redes neurais. Master’s thesis, Univeridade Federal do Rio Grande do Sul (UFRGS), Porto Alegre, RS, Brazil, 1991.
- [18] OSÓRIO, F. S. *INSS: Un Système Hybride Neuro-Symbolique pour l’Apprentissage Automatique Constructif*. Doctoral thesis, INPG/IMAG, Grenoble, France, 1998.
- [19] OSÓRIO, F. S., AND AMY, B. Inss: A hybrid system for constructive machine learning. *Neurocomputing* 28 (1999), 191–205.
- [20] RIEDMILLER, M., AND BRAUN, H. A direct adaptive method for faster backpropagation learning: The RPROP algorithm. In *Proc. IEEE Int. Conf. Neural Networks (ICNN)* (San Francisco, CA, Mar. 1993), pp. 586–591.
- [21] RIHA, Z., AND MATYAS, V. Biometric authentication systems. Technical Report RS-2000-08, FI MU Report Series, Nov. 2000.
- [22] RUMELHART, D. E., HINTON, G. E., AND WILLIAMS, R. J. *Learning Internal Representations by Error Propagation*. MIT Press, Cambridge, MA, 1986.

- [23] WIROTIUS, M., RAMEL, J. Y., AND VINCENT, N. New features for authentication by on-line handwritten signatures. In *Proc. 1st Int. Conf. Biometric Authentication (ICBA)* (Hong Kong, China, July 2004), vol. 3072 of *LNCS*, Springer-Verlag, pp. 577–584.
- [24] YEUNG, D. Y., CHANG, H., XIONG, Y., GEORGE, S., KASHI, R., MATSUMOTO, T., AND RIGOLL, G. Svc2004: First int. signature verification competition. In *Proc. 1st Int. Conf. Biometric Authentication (ICBA)* (Hong Kong, China, July 2004), vol. 3072 of *LNCS*, Springer-Verlag, pp. 16–22.
- [25] YU, K., WANG, Y., AND TAN, T. Writer identification using dynamic features. In *Proc. 1st Int. Conf. Biometric Authentication (ICBA)* (Hong Kong, China, July 2004), vol. 3072 of *LNCS*, Springer-Verlag, pp. 512–518.