Autenticação de Assinaturas utilizando Análise de Componentes Principais e Redes Neurais Artificiais

Milton Roberto Heinen e Fernando Santos Osório
Universidade do Vale do Rio dos Sinos (UNISINOS) - Computação Aplicada
mheinen@turing.unisinos.br, fosorio@unisinos.br

Abstract— **The main goal of this paper is to describe our research and implementation of a handwritten signature authentication system based on artificial neural networks. In this system the authentication process occurs in the following way: firstly, the users' signatures are read using a pen tablet device and then stored; after that some adjustments in position and scale are accomplished; representative signature features are extracted; the input space dimensionality is reduced using principal component analysis; and finally, the users' signatures are classified as authentic or not, through the use of a neural network. Several experiments were accomplished using a 2440 real signatures database, and the obtained results were very satisfactory.**

I. Introdução

Um dos maiores problemas enfrentados hoje em dia em termos de segurança em informática é a autenticação de usuários, que implica em garantir que uma pessoa que está tentando acessar um sistema seja quem ela realmente diz ser. Na maioria dos sistemas de informação, a autenticidade dos usuários é garantida através do uso de senhas alfanuméricas, que devem ser memorizadas e mantidas a salvo de outras pessoas. Apesar de ser a forma de autenticação mais difundida da atualidade, a autenticação de usuários baseada em senhas alfanuméricas apresenta diversas vulnerabilidades em termos de segurança[1], [2].

Devido a estes problemas, técnicas de autenticação baseadas em características biométricas físicas, como impressões digitais, exames de retina e da palma das mãos vêm sendo utilizadas para garantir a autenticidade dos usuários[3], [4]. Estas técnicas são muito mais seguras do que as senhas alfanuméricas, mas apresentam algumas desvantagens, como o custo elevado dos equipamentos e o alto grau de intrusão[1].

Além das características biométricas físicas, também podem ser utilizadas para a autenticação de usuários características biométricas comportamentais, como as assinaturas manuscritas[1], [5], pois estas apresentam diversas vantagens em relação as outras técnicas de autenticação. A primeira vantagem é a segurança, pois ao contrário das senhas, mesmo que alguém conheça a assinatura de um usuário, usualmente não é possível reproduzir esta assinatura de forma trivial. Outra vantagem é que os usuários estão acostumados a utilizar assinaturas como uma forma de autenticação em transações financeiras, e assim sentem-se mais seguros e confortáveis em relação ao seu uso. O grau de intrusão apresentado pelos sistemas de autenticação de assinaturas é baixo, e o hardware necessário tem um custo bastante acessível (entre U$ 15.00 e U$ 80.00).

Mas apesar das diversas vantagens, a autenticação de assinaturas é um problema de difícil solução do ponto de vista computacional, devido a grande variabilidade existente entre assinaturas de uma mesma pessoa[6]. Esta variabilidade faz com que soluções baseadas em técnicas de Inteligência Artificial e Aprendizado de Máquinas apresentem melhores resultados do que soluções puramente algorítmicas[7], [5].

Neste trabalho foi desenvolvida uma metodologia, bem como a sua implementação em um protótipo[8], [9], [10], que permite a autenticação de usuários através do uso de assinaturas manuscritas. Este artigo está estruturado da seguinte forma: a seção II apresenta diversos conceitos relativos à autenticação de assinaturas; as seções III e IV descrevem, respectivamente, as Redes Neurais Artificiais (RNA) e a Análise de Componentes Principais (*Principal Component Analysis* – PCA); a seção V descreve o sistema proposto e a sua implementação em um protótipo; a seção VI descreve os resultados obtidos nos experimentos; e a seção VII apresenta as conclusões finais e as perspectivas futuras.

II. Autenticação de Assinaturas

Um sistema de autenticação de assinaturas é responsável por validar assinaturas, dizendo se elas são autênticas ou não. Do ponto de vista da obtenção dos dados, a autenticação de assinaturas pode ser realizada de duas formas diferentes, que são as formas *on-line* e *off-line*[11]. Na autenticação *off-line*, a assinatura é desenhada pelo usuário em uma folha de papel, que é posteriormente digitalizada e enviada para o sistema que faz a autenticação. Já na autenticação *on-line*, a assinatura é desenhada diretamente em um dispositivo especial de hardware, como um *tablet* (Figura 1).

Fig. 1. Exemplo de um *tablet*

A autenticação *on-line* de assinaturas apresenta diversas vantagens em relação a autenticação *off-line*, dentre as quais é possível destacar uma maior riqueza de informações, pois além das características visuais da assinatura, é possível obter informações temporais e dinâmicas[6], [9]. Neste trabalho optou-se por realizar a autenticação de assinaturas de forma *on-line*.

III. Redes Neurais Artificiais

Através de um modelo abstrato e simplificado dos neurônios humanos é possível desenvolver um simulador que seja capaz de classificar, generalizar e aprender funções desconhecidas. Um dos modelos de aprendizado neural mais utilizados na atualidade é o modelo denominado *back-propagation*[12].

Após o desenvolvimento do algoritmo *back-propagation*, vários algoritmos sugerindo melhorias no modelo original foram desenvolvidos de forma a tornar o aprendizado em uma Rede Neural mais rápido e eficiente. Dentre as melhorias sugeridas, pode ser destacado o algoritmo *Resilient Propagation* (RPROP)[13], que realizada uma adaptação direta da taxa de aprendizado η baseado em informações do gradiente local. Para conseguir isto, cada peso tem seu valor de atualização individual Δ_{ij}, que determina a intensidade do ajuste deste peso. O valor de adaptação Δ_{ij} evolui durante o processo de aprendizado baseado no sinal da função de erro E, de acordo com a seguinte regra[13]:

$$\Delta_{ij}^{(t)} = \begin{cases} \eta^+ \times \Delta_{ij}^{(t-1)} , & \text{se } \frac{\partial E}{\partial w_{ij}}^{(t-1)} \times \frac{\partial E}{\partial w_{ij}}^{(t)} > 0 \\ \eta^- \times \Delta_{ij}^{(t-1)} , & \text{se } \frac{\partial E}{\partial w_{ij}}^{(t-1)} \times \frac{\partial E}{\partial w_{ij}}^{(t)} < 0 \\ \Delta_{ij}^{(t-1)} , & \text{senão} \end{cases} \tag{1}$$

onde $0 < \eta^- < 1 < \eta^+$, $\frac{\partial E}{\partial w_{ij}}$ é a derivada parcial da função de erro E para o peso w_{ij}, e $\Delta_{ij}^{(t-1)}$ é a taxa atualização dos pesos anterior. Além de acelerar o processo de aprendizado, o algoritmo RPROP faz com que a Rede Neural seja mais facilmente configurada.

Para que ocorra o aprendizado, é utilizado um conjunto de dados de exemplos de padrões com as respostas esperadas (padrões e classes correspondentes), que é dividido em uma base de aprendizado e uma base de validação (avaliação da generalização). Este tipo de aprendizado é conhecido como aprendizado supervisionado com validação cruzada[14].

IV. Análise de Componentes Principais

A Análise de Componentes Principais (*Principal Component Analysis* – PCA)[15] é uma técnica essencial em compressão de dados e na extração e seleção de atributos. Métodos para a redução da dimensionalidade do espaço de entrada, como a PCA, são usados para descartar as combinações lineares das variáveis de entrada que possuem pequenas variâncias e preservar somente aquelas que possuem as maiores variâncias[16].

Em termos matemáticos, a PCA pode ser definida da seguinte forma: assuma que x é um vetor de dados de entrada n-dimensional que foi ajustado de forma a ter a média igual a zero. O propósito da PCA é encontrar as $p\,(p \leq n)$ combinações lineares $w_1^T x, w_2^T x, \cdots, w_p^T x$ dos elementos de x que maximizem

$$E\{(w_i^T x)^2\}, \;\; i = 1, \cdots, p \,, \tag{2}$$

sob as restrições

$$w_i^T w_j = \delta_{ij}, \;\; j < i \,. \tag{3}$$

A solução para os vetores $w_1, \cdots, w_p$ são os p *eigenvectors* da matriz de covariância

$$C = E\{xx^T\} \,. \tag{4}$$

Estes são os p vetores ortogonais unitários $c_1, \cdots, c_p$ dados por:

$$Cc_i = \lambda_i c_i \,, \tag{5}$$

onde $\lambda_1, \cdots, \lambda_p$ são p os maiores *eigenvalues* da matriz C em ordem decrescente de magnitude. A primeira combinação linear $c_1^T x$ é chamada primeira componente principal, a segunda combinação linear $c_2^T x$ é a segunda componente, e assim por diante[16].

Desta forma, a PCA pode ser utilizada para reduzir a dimensionalidade do espaço de entradas, descartando as combinações lineares que possuem pequenas variâncias, e mantendo apenas aquelas que possuem grandes variâncias[14].

V. Sistema Proposto

O objetivo deste artigo é propor uma metodologia para a autenticação *on-line* de assinaturas utilizando Análise de Componentes Principais (PCA) e Redes Neurais Artificiais (RNA). Para validar esta metodologia, um modelo de sistema de autenticação de assinaturas foi proposto e implementado em um protótipo completo e funcional[1]. No sistema proposto, a autenticação de assinaturas é realizada da seguinte forma:

[1]NeuralSignX – http://www.inf.unisinos.br/~osorio/neuralsignx/

- As assinaturas são coletadas e armazenadas;
- São realizados ajustes de posição e escala;
- Diversos atributos utilizados no processo de autenticação são extraídos a partir das assinaturas;
- A dimensionalidade dos dados de entrada (valores dos atributos) é reduzida através do uso da PCA;
- A autenticação das assinaturas é realizada através do uso de Redes Neurais Artificiais.

A. Aquisição das assinaturas

Para a validação do modelo proposto, foi necessária a criação de uma base de dados de assinaturas. Assim, foi desenvolvido um módulo do sistema, chamado de Módulo de Aquisição de Assinaturas, que é responsável por ler as assinaturas a partir de um *tablet* e salvar as assinaturas em um arquivo. O arquivo gerado contém uma descrição das assinaturas, onde cada uma delas é composta por uma seqüência de coordenadas da caneta em relação ao *tablet* (x, y), um estado (0 ou 1: caneta levantada ou em contato com o *tablet*) e o instante de tempo em que cada amostra foi coletada (em milisegundos). O *tablet* utilizado nos experimentos foi o UC-Logic SuperPen WP4030[2].

A base de dados de assinaturas utilizada nos experimentos possui atualmente 2440 assinaturas, distribuídas da seguinte forma:

- 1800 assinaturas de 60 usuários reais (30 assinaturas por usuário);
- 400 assinaturas pictográficas, representando 40 modelos de desenhos diferentes (10 exemplos de cada modelo);
- 240 assinaturas falsificadas (120 falsificações traçadas e 120 falsificações especializadas).

A coleta das assinaturas aconteceu de forma que cada usuário contribuiu com no máximo cinco assinaturas de cada vez, de forma que as assinaturas coletadas refletissem as diferenças que ocorrem nas assinaturas reais devido ao estado físico e emocional do usuário. As assinaturas pictográficas representam desenhos variados, que não possuem uma relação direta com o nome do usuário[17]. As falsificações traçadas foram desenhadas percorrendo-se a trajetória de assinaturas reais registradas em papel, e as falsificações especializadas foram desenhadas por pessoas que praticaram por algum tempo até que conseguissem reproduzir as assinaturas originais de forma satisfatória.

Após a coleta das assinaturas, foram realizados ajustes de posição e escala, de forma que o processo de autenticação se tornasse mais robusto[10].

[2]UC-Logic SuperPen - http://www.superpen.com/

B. Extração dos atributos

Após da criação base de dados de assinaturas e dos ajustes de posição e escala, a extração dos atributos foi realizada. Os atributos utilizados no sistema proposto foram baseados em algumas técnicas de pré-processamento encontradas na literatura[7], [18], [2], [19], somados a outras técnicas propostas e/ou adaptadas pelos próprios autores[20], [6], [9], [10]. Após o levantamento e a elaboração dos diversos atributos, foi realizado um estudo para verificar a importância de cada um deles, e os atributos que se mostraram mais eficientes foram:

Tempo de duração da assinatura: é o tempo que o usuário utilizou para a desenhar a assinatura (1 entrada);

Número de vezes em que a caneta foi levantada: conta-se quantas vezes a caneta se afastou do *tablet* durante a assinatura[6] (1 entrada);

Comprimento total da assinatura: é a distância total percorrida pela caneta durante o traçado (1 entrada);

Velocidade média e máxima da assinatura: é a velocidade de deslocamento da caneta em relação ao *tablet*[6] (2 entradas);

Número de trocas de sentido nos eixos x ***e*** y***:*** conta-se quantas vezes a caneta trocou de direção em relação aos eixos x e y. Uma troca de direção é quando o valor de uma coordenada que estava em crescimento começou a decrescer, e vice-versa[9] (2 entradas);

Contagem por pontos cardeais: este atributo extrai a forma estrutural da assinatura, e depois verifica quantos pseudo-vetores apontam para as coordenadas geográficas (N, S, E, W, NW, SW, NE, SE)[10]. A Figura 2 demonstra o uso desta técnica (8 entradas);

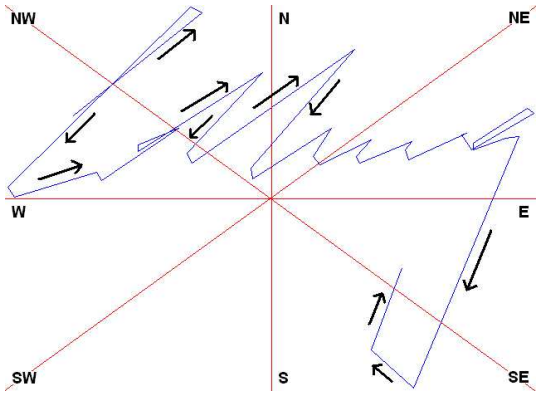


Fig. 2. Contagem por pontos cardeais

Comprimento total dos pseudo-vetores: é o resultado da soma de todos os pseudo-vetores que apontam para cada um dos oito quadrantes (8 entradas);

Densidade com informações de grade: divide-se a assinatura em diversas células, e para cada célula é

calculada a densidade de pontos da assinatura (técnica adaptada de [7]). Para uma determinada célula i, a densidade D_i é calculada através da fórmula:

$$D_i = \frac{np_i - np_{min}}{np_{max} - np_{min}}, \quad (6)$$

onde np_i é o número de pontos da assinatura que se situam dentro da célula i, np_{min} é o número de pontos da célula menos densa, e np_{max} é o número de pontos da célula mais densa. A Figura 3 é demonstra o uso desta técnica. As células com maior densidade são representadas por tons mais escuros (48 entradas);

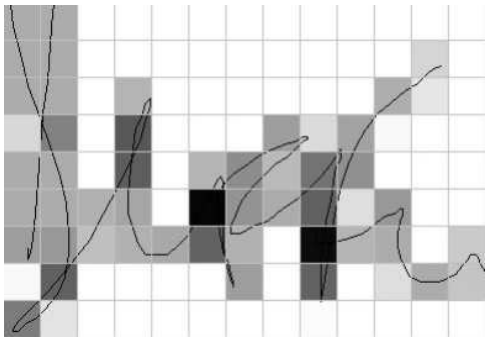


Fig. 3. Densidade com informações de grade

Intersecções de linhas verticais e horizontais: a partir de uma assinatura digitalizada, são traçadas linhas imaginárias cortando a assinatura em intervalos fixos, e para cada linha imaginária são contadas quantas vezes esta intersecciona a assinatura[20]. Na Figura 4 são mostradas diversas linhas verticais e horizontais interseccionando uma assinatura (26 entradas);

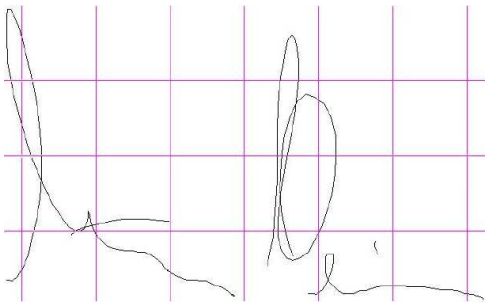


Fig. 4. Intersecções de linhas verticais e horizontais

Amostragem seqüencial: permite que a trajetória da assinatura seja representada por um número reduzido de pontos amostrados. A Figura 5 mostra a amostragem seqüencial de uma assinatura (16 entradas);

Simetria: mede o grau de simetria da assinatura com relação aos eixos x e y (2 entradas).

Os números entre parênteses representam o número de entradas para cada atributo. No total, os 11 atributos necessitariam de 115 entradas na RNA.

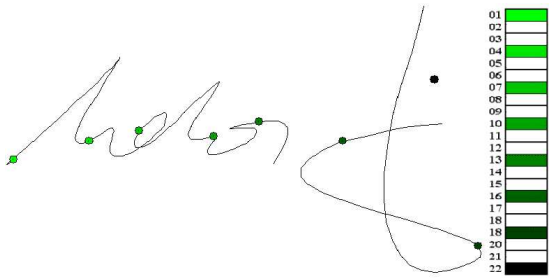


Fig. 5. Amostragem seqüencial

C. Redução do espaço de entradas

Para reduzir o número de entradas da Rede Neural, e evitar os problemas que geralmente ocorrem quando este número é muito elevado[14], os atributos (01) *Contagem por pontos cardeais*, (02) *Comprimento total dos pseudo-vetores*, (03) *Intersecções de linhas verticais e horizontais*, (04) *Amostragem seqüencial* e (05) *Densidade com informações de grade* tiveram o número de entradas reduzido através do uso da Análise de Componentes Principais (PCA). Assim, apenas as componentes mais importantes de cada atributo foram utilizadas no processo de autenticação, possibilitando a redução do número de entradas com uma perda mínima de informação.

Para cada um dos atributos listados acima, foi calculada a variância explicada pelas componentes principais. A Tabela I mostra a variância acumulada nas seis primeiras componentes dos atributos listados acima. A

TABLE I
VARIÂNCIA ACUMULADA

Atributo	C1	C2	C3	C4	C5	C6	NF
01	56.8	68.9	77.5	85.7	91.0	95.3	3
02	25.6	44.9	59.9	71.7	80.7	89.4	3
03	29.5	44.5	52.0	57.3	61.4	65.2	5
04	21.5	32.5	42.6	51.7	59.1	65.8	6
05	19.8	27.6	32.8	37.1	41.4	45.2	12

primeira coluna (Atributo) mostra o identificador de cada atributo, as colunas entre C1 e C6, inclusive, mostram os percentuais da variância acumulada explicada pelas seis primeiras componentes, e a coluna NF mostra a quantidade de fatores selecionada para ser utilizada na autenticação de assinaturas.

Procurou-se utilizar uma quantidade de fatores (componentes) que explicasse no mínimo 60% da variância do conjunto de dados. Embora não conste na Tabela I, a variância acumulada das 12 primeiras componetes do atributo 05 (*Densidade com informações de grade*) é 62.37%. Com a utilização da PCA, o número de entradas da Rede Neural foi reduzido de 115 para 38, com um mínimo de perdas em termos de variabilidade

do conjunto de entradas.

D. Processamento neural

O módulo de processamento neural recebe o valor dos atributos fornecidos pelo módulo anterior e realiza a classificação, dizendo se as assinaturas são autênticas ou não. Para a classificação, foi adotado um modelo de RNA baseado em *Multi Layer Perceptron* (MLP), com um algoritmo de aprendizado mais otimizado do que o *back-propagation* tradicional, o algoritmo RPROP[13]. Este algoritmo foi selecionado ser mais eficiente que o *back-propagation* tradicional, tornando o aprendizado muito mais rápido e eficiente.

O simulador de Redes Neurais Artificiais selecionado para ser utilizado neste trabalho foi o Stuttgart Neural Network Simulator - SNNS[3], que é um simulador de Redes Neurais Artificiais gratuito e completo, e que possui diversas ferramentas adicionais que permitem a geração de *scripts* e a análise dos resultados.

Os valores dos principais parâmetros utilizados na RNA são mostrados na Tabela II. Uma descrição completa destes parâmetros pode ser encontrada na documentação do SNNS. O passo inicial de aprendizado utilizado foi 0.1, e passo máximo de aprendizado foi fixado em 1.0. Através da realização de diversos experimentos preliminares, foi constatado que não era necessária a utilização de neurônios na camada oculta (os padrões são linearmente separáveis). O *Score threshold* foi fixado em 0.4, o que significa que saídas maiores que 0.6 representam assinaturas autênticas, e saídas menores que 0.4 representam assinaturas não autênticas. A função de ativação utilizada foi a *sigmoid*.

TABLE II
PARÂMETROS DA REDE NEURAL

Parâmetro	Valor
Número de entradas	38
Número de saídas	1
Número de neurônios ocultos	0
Taxa de aprendizado inicial	0.1
Taxa máxima de aprendizado	1.0
Número máximo de gerações	1000
Weight decay	1.0×10^{-38}
Score threshold	0.4

Para tornar os experimentos estatisticamente válidos, as simulações foram realizadas utilizando o método de validação cruzada conhecido por *10-fold cross-validation*. Para cada um dos folds, foram realizados 10 experimentos distintos utilizando sementes aleatórias diferentes, totalizando 100 experimentos por usuário. A divisão dos padrões procurou respeitar a proporção dentro de cada fold entre os exemplos da classe 0 (assinaturas não autênticas) e 1 (assinaturas autênticas).

[3]SNNS – http://www-ra.informatik.uni-tuebingen.de/SNNS/

VI. RESULTADOS

A Tabela III mostra a média e o desvio padrão dos resultados obtidos nos experimentos realizados para 10 usuários selecionados ao acaso. Por questões de sigilo, a identidade dos usuários foi preservada. Os valores presentes na tabela III mostram a média e o desvio padrão dos 10 folds de cada usuário. No total foram realizados 1000 experimentos (100 por usuário).

TABLE III
RESULTADOS OBTIDOS

	MSE	TAC		TFP		TFN	
U	μ	μ	σ	μ	σ	μ	σ
01	7.68e-04	99.92	0.12	0.07	0.13	0.33	1.0
02	1.63e-03	99.82	0.25	0.10	0.21	6.33	11.0
03	1.47e-03	99.83	0.19	0.14	0.18	3.00	6.2
04	1.37e-03	99.85	0.23	0.06	0.09	7.33	13.8
05	7.52e-04	99.92	0.12	0.04	0.08	3.33	5.9
06	1.47e-03	99.84	0.29	0.06	0.13	8.00	15.3
07	1.04e-03	99.88	0.18	0.06	0.08	5.00	9.7
08	4.09e-05	100.0	0.01	0.00	0.01	0.00	0.0
09	5.33e-04	99.94	0.12	0.03	0.09	2.33	7.4
10	4.21e-04	99.95	0.10	0.04	0.10	0.67	1.4

A primeira coluna (U) mostra o número de identificação do usuário, a segunda coluna mostra o erro médio quadrado (mean square error - MSE). As colunas seguintes mostram, respectivamente, a média (μ) e o desvio padrão (σ) da taxa de acertos (classificações realizadas corretamente - TAC), da taxa de falsos positivos (TFP) e da taxa de falsos negativos (TFN). Um falso positivo é quando uma assinatura que não pertence ao usuário (falsa) é identificada como se fosse verdadeira, e um falso negativo ocorre quando uma assinatura que pertence ao usuário (verdadeira) é identificada como não se não pertencesse este.

Em um sistema de autenticação de assinaturas, o essencial é que a taxa de falsos positivos seja a menor possível. Já a taxa de falsos negativos não é tão crítica, pois pode-se pedir que o usuário assine novamente quando uma assinatura for classificada como falsa.

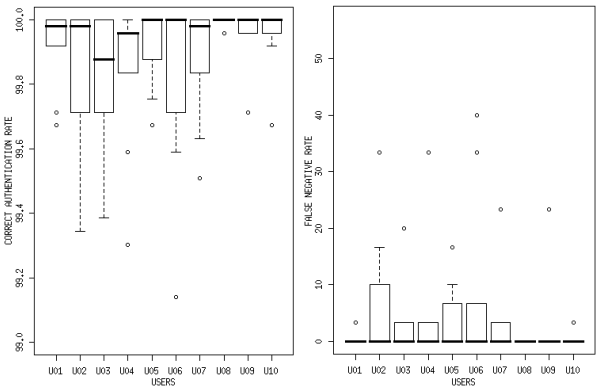
Observando os resultados da tabela III, nota-se que a taxa de acertos (TAC) é bastante elevada, o que demonstra que o desempenho do sistema é bastante satisfatório. A taxa de falsos positivos (TFP) e a taxa de falsos negativos (TFN) foram calculadas utilizando as equações:

$$TFP = \frac{N_{FP}}{N_{Cl0}} \times 100 \quad (7)$$

$$TFN = \frac{N_{FN}}{N_{Cl1}} \times 100 \quad (8)$$

onde N_{FP} é o número de falsos positivos, N_{FN} é o número de falsos negativos, N_{Cl0} é o número de padrões da classe 0 e P_{Cl1} é o número de padrões da classe 1.

A Figura 6(a) mostra um gráfico de *boxplot* da taxa de acertos (TAC), e a Figura 6(b) mostra um gráfico de *boxplot* para a taxa de falsos negativos (TFN). Observando estes gráficos, pode-se notar que o desempenho do sistema é bastante satisfatório para todos os usuários selecionados.



(a) TAC (b) TFN

Fig. 6. Gráfico de *boxplot*

VII. Conclusões e Perspectivas

Este trabalho teve por objetivo o estudo, a pesquisa e o desenvolvimento de um sistema de autenticação de usuários através de assinaturas manuscritas. Para atingir tal objetivo foram estudados tópicos referentes à autenticação de assinaturas, a Análise de Componentes Principais, e as Redes Neurais Artificiais. Também foi apresentada uma proposta de solução, bem como a sua implementação em um protótipo, de um sistema de autenticação *on-line* de assinaturas.

Os resultados obtidos nas simulações realizadas com o protótipo comprovam que um sistema de autenticação de assinaturas não é apenas viável, mas também representa uma ótima solução para a autenticação *on-line* de usuários em sistemas de informação. Também se comprova a partir dos resultados obtidos que as Redes Neurais Artificiais são muito adequadas para o processo de autenticação de assinaturas, e que os atributos selecionados foram muito eficazes no processo de classificação, pois permitiram que a Rede Neural conseguisse não apenas obter elevadas taxas de aprendizado e de generalização, mantendo baixos os índices de falsos positivos, o que é fundamental em um sistema de autenticação de assinaturas.

Como trabalhos futuros podem ser desenvolvidos sistemas multimodais de autenticação de usuários baseados em características biométricas múltiplas (e.g. assinatura, face e íris).

References

[1] A. Kholmatov and B. Yanikoglu, "Identity authentication using improved online signature verification method," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2400–2408, Nov. 2005.

[2] K. Yu, Y. Wang, and T. Tan, "Writer identification using dynamic features," in *Proc. 1st Int. Conf. Biometric Authentication (ICBA)*, ser. LNCS, vol. 3072. Hong Kong, China: Springer, July 2004, pp. 512–518.

[3] Z. Riha and V. Matyas, "Biometric authentication systems," FI MU Report Series, Technical Report RS-2000-08, Nov. 2000.

[4] A. M. Namboodiri, S. Saini, X. Lu, and A. K. Jain, "Skilled forgery detection in on-line signatures: A multimodal approach," in *Proc. 1st Int. Conf. Biometric Authentication (ICBA)*, ser. LNCS, vol. 3072. Hong Kong, China: Springer, July 2004, pp. 505–511.

[5] D. Y. Yeung, H. Chang, Y. Xiong, S. George, R. Kashi, T. Matsumoto, and G. Rigoll, "Svc2004: First int. signature verification competition," in *Proc. 1st Int. Conf. Biometric Authentication (ICBA)*, ser. LNCS, vol. 3072. Hong Kong, China: Springer, July 2004, pp. 16–22.

[6] M. R. Heinen, "Autenticação on-line de assinaturas utilizando redes neurais," Final Undergraduate Dissertation, Universidade do Vale do Rio dos Sinos (UNISINOS), São Leopoldo, RS, Brazil, 2002.

[7] H. Baltzakis and N. Papamarkos, "A new signature verification technique based on a two stage neural network classifier," *Engineering applications of Artificial intelligence 14*, pp. 95–103, Sept. 2000.

[8] M. R. Heinen and F. S. Osório, "Biometria comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas," *Infocomp: Revista de Ciência da Computação*, vol. 3, no. 2, pp. 32–37, Nov. 2004.

[9] ——, "Autenticação de assinaturas utilizando algoritmos de aprendizado de maquina," in *Anais do V ENIA*, São Leopoldo, RS, Brazil, July 2005.

[10] ——, "Handwritten signatures authentication using artificial neural networks," in *Proc. IEEE Int. Joint Conf. Neural Networks (IJCNN)*, Vancouver, Canada, July 2006.

[11] R. Abbas, "Backpropagation networks prototype for off-line signature verification," Minor Thesis, RMIT – Department of Computer Science, Melbourne, Australia, Mar. 1994.

[12] D. Rumelhart, G. Hinton, and R. Williams, *Learning Internal Representations by Error Propagation*. Cambridge, MA: MIT Press, 1986.

[13] M. Riedmiller and H. Braun, "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.

[14] S. Haykin, *Redes Neurais: Princípios e Prática*, 2nd ed. Porto Alegre, RS, Brazil: Bookman, 2001.

[15] R. Cattell, *Factor Analysis*. New York: Harper Books, 1952.

[16] E. Oja, "Principal components, minor components and linear neural networks," *Neural Networks*, vol. 5, pp. 927–935, Mar. 1992.

[17] K. K. Lau, P. C. Yuen, and Y. Y. Tang, "Directed connection measurement for evaluating reconstructed stroke sequence in handwriting images," *Pattern Recognition*, vol. 38, no. 3, pp. 323–339, Mar. 2005.

[18] H. Lei and V. Govindaraju, "A comparative study on the consistency of features in on-line signature verification," *Pattern Recognition Letters*, vol. 26, no. 15, pp. 2483–2489, Nov. 2005.

[19] M. Wirotius, J. Y. Ramel, and N. Vincent, "New features for authentication by on-line handwritten signatures," in *Proc. 1st Int. Conf. Biometric Authentication (ICBA)*, ser. LNCS, vol. 3072. Hong Kong, China: Springer, July 2004, pp. 577–584.

[20] F. S. Osório, "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.