Autenticação de assinaturas utilizando algoritmos de Aprendizado de Máquina

Milton Roberto Heinen[1], Fernando Santos Osório[1]

[1]Computação Aplicada – Universidade do Vale do Rio dos Sinos (UNISINOS)
CEP 93.022-000 – São Leopoldo – RS – Brazil

mheinen@unisinos.br, fosorio@unisinos.br

Abstract. *The main goal of this paper is to describe our study, research and implementation of a handwritten signatures authentication system. This system is composed of three modules, the Data Acquisition Module, responsible for the on-line users' signatures reading through a pen tablet, the Pre-processing 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 simulations were accomplished using a proposed system, and the obtained results were 99.96% of correct recognition.*

Resumo. *O objetivo do presente trabalho é descrever a pesquisa e a implementação de um sistema de autenticação de assinaturas manuscritas. O sistema proposto é composto de três módulos, o módulo de entrada, responsável pela obtenção das assinaturas através de um tablet, o módulo de pré-processamento, responsável pelos ajustes visuais e pela extração dos atributos representativos das assinaturas, e o módulo de processamento, que realiza a autenticação das assinaturas através do uso de Redes Neurais Artificiais. Diversas simulações foram realizadas utilizando o sistema proposto, e os resultados obtidos foram da ordem de 99,96% de acertos.*

1. Introdução

Nos dias atuais, o uso cada vez mais freqüente de sistemas de informação e a premente necessidade de aumento da segurança, trazem a necessidade de se identificar, autenticar e controlar os usuários de forma segura [Jain et al. (2002)]. Na maioria dos sistemas computacionais, a autenticação de usuários ocorre através de senhas alfanuméricas, que representam um sério problema de segurança quando acabam parando em mãos erradas. Para evitar este problema, várias formas de autenticação de usuários baseadas em características biométricas físicas vem sendo desenvolvidas. Entretanto, usualmente estas técnicas implicam em um custo elevado ligado a aquisição dos equipamentos de hardware usados e em um alto grau de intrusão, que gera desconfortos aos usuários [Gupta et al. (1997)]. Em relação às impressões digitais, seu uso possui uma conotação negativa devido ao fato delas estarem ligadas a delitos e investigações criminais [Jain et al. (2002)]. Neste trabalho foi desenvolvida a proposta de uma metodologia, bem como a sua implementação em um protótipo [Heinen (2002)], que permite realizar a autenticação de usuários através do uso de assinaturas manuscritas. A autenticação das assinaturas é implementada neste trabalho através do uso de um hardware de baixo custo e do uso de Redes Neurais Artificiais do tipo *Cascade-Correlation*, sendo este processo considerado pouco intrusivo.

2. Autenticação de assinaturas

Um sistema de autenticação de assinaturas é um sistema responsável por validar assinaturas, dizendo se as mesmas são autênticas ou não. A autenticação pode ser realizada de duas formas diferentes, que são as formas *on-line* e *off-line* [Abbas (1994)]. Na autenticação *off-line*, a assinatura é feita pelo usuário em uma folha de papel, que é posteriormente digitalizada em um *scanner* e em seguida é enviada para o sistema que faz a autenticação. Já na autenticação *on-line*, a assinatura é feita diretamente sobre um dispositivo especial de *hardware*, como um *tablet* (Figura 1).

Figura 1. Exemplo de um tablet

Do ponto de vista técnico, o reconhecimento *on-line* de assinaturas apresenta diversas vantagens em relação ao *off-line*, dentre as quais é possível destacar [Heinen 2002]:

- Maior riqueza de informações: além das características visuais da assinatura, é possível obter informações temporais e dinâmicas;
- Pureza da imagem: uma assinatura *off-line* costuma apresentar distorções provenientes do processo de digitalização, o que dificulta o processo de autenticação.

Neste trabalho optou-se por utilizar o reconhecimento *on-line* de assinaturas devido a estas vantagens, e também por ser um método mais prático e adequado de ser utilizado em transações eletrônicas.

2.1 Reconhecimento de Padrões

As características biométricas de uma pessoa podem ser reconhecidas através do emprego de técnicas de aprendizado de máquina. Para isto, usualmente, é construída uma base de dados contendo exemplos de dados obtidos a partir da leitura (e processamento) destas características. Esta base de dados é posteriormente processada pelo algoritmo de aprendizado de máquina, de modo a construir um modelo das propriedades biométricas de cada pessoa. Um bom sistema de aprendizado de máquina, que possa ser usado no reconhecimento de padrões biométricos, deve ser robusto de modo a aceitar um certo grau de variabilidade (ou ruído) nos dados, mas mesmo assim espera-se que mantenha uma boa performance (taxa de respostas corretas).

O processo de autenticação de assinaturas é um tipo específico de reconhecimento de padrões, onde a resposta do sistema deve indicar apenas se o padrão apresentado pertence ou não a classe (assinatura verdadeira/falsa de um determinado usuário). Um sistema de reconhecimento de padrões mais sofisticado pode buscar obter a partir de

uma assinatura qualquer, qual foi o usuário (entre *'n'* possíveis usuários) que realizou esta assinatura.

Neste trabalho buscou-se realizar a autenticação de assinaturas, visto que este tipo de aplicação é a que mais interessa em sistemas de controle de segurança. Esta opção implicou também em algumas exigências para um bom desempenho de nosso sistema: a) Uso de um conjunto de exemplos de assinaturas de um usuário, mas de tamanho limitado; b) Uso de um conjunto de contra-exemplos de assinaturas de outros usuários que não sejam o usuário que se deseja autenticar. Este conjunto deve ser o mais variado possível; c) Aprendizado focado na obtenção de um baixíssimo nível de falsos aceites (é bastante desejável que este índice seja *zero*); d) Falsas rejeições podem ocorrer em pequeno número, pois podemos solicitar ao usuário que proceda uma nova tentativa de identificação. Onde considera-se: ***Falso Aceite***: Uma assinatura que não é do usuário (falsa) é identificada como sendo deste usuário (aceita) - FP (falso positivo); ***Falsa Rejeição***: Uma assinatura que é do usuário (verdadeira) é identificada como não sendo deste usuário (rejeitada) - FN (falso negativo).

Em nossas pesquisas foi estudada a aplicação de dois tipos de métodos de aprendizado supervisionado [Mitchell (1997)]: Redes Neurais Artificiais (RNA) e Árvores de Decisão. Optou-se pela utilização das Redes Neurais, onde as Árvores de Decisão contribuíram também para o estudo e seleção dos atributos a serem adotados no sistema.

3. Inteligência Artificial e Aprendizado de Máquina

Segundo Mitchell [Mitchell (1997)], um programa aprende quando a sua performance melhora com a experiência em uma determinada tarefa. Dentre as diversas técnicas de Aprendizado de Máquina que podem ser utilizadas para a autenticação de assinaturas, se optou neste trabalho pelo aprendizado supervisionado, utilizando Árvores de Decisão e Redes Neurais Artificiais.

3.1. 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 *Backpropagation* [Rumelhart et al. (1986)]. 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 [Haykin (2001)].

3.2. Cascade-Correlation

O *Cascade-Correlation* é um modelo otimizado de MLP (*Multi Layer Perceptron*), desenvolvido por [Fahlman (1990)] com a finalidade de solucionar a maioria dos problemas levantados anteriormente no algoritmo do *Backpropagation*. As principais vantagens que o *Cascade-Correlation* apresenta em relação aos demais modelos de Redes Neurais são:

- Definição da arquitetura: o algoritmo do *Cascade-Correlation* determina de forma automática a melhor topologia de rede possível para solucionar um problema;
- Menos parâmetros: alguns parâmetros, como o *passo* e o *momentum*, são ajustados automaticamente pelo simulador, não necessitando serem ajustados manualmente;
- Velocidade de aprendizado: o *Cascade-Correlation* converge mais rapidamente para um ponto mínimo da curva de erro, reduzindo o tempo de aprendizado.

Todas estas vantagens fazem com que o *Cascade-Correlation* seja muito simples de ser utilizado em comparação a outros modelos de Redes Neurais, além de ser extremamente eficaz em termos de aprendizado. Uma das limitações que o *Cascade-Correlation* apresenta é que ele só pode ser utilizado para problemas de classificação, e não para aproximação de funções. Uma vez que o *Cascade-Correlation* é muito adequado para resolver problemas de classificação, isto permite o seu uso em sistemas de autenticação de assinaturas.

A topologia do *Cascade-Correlation* é um pouco diferente da topologia do *Backpropagation* tradicional, como pode ser visto na Figura 2. Os neurônios da camada oculta não são posicionados lado a lado, mas sim em cascata, com a saída de um neurônio alimentado a entrada do outro.

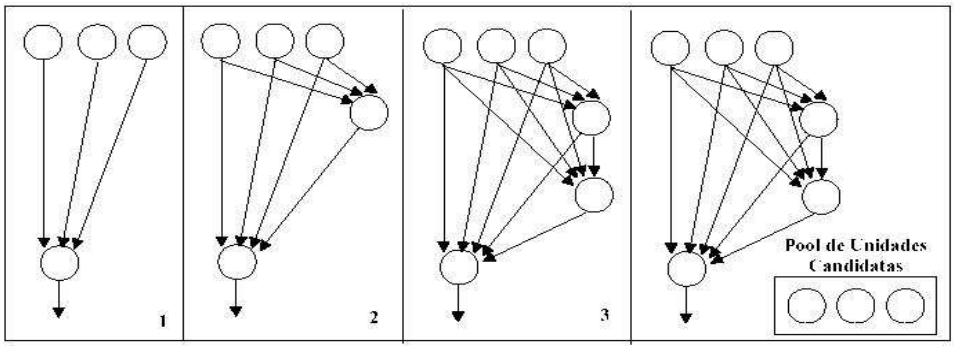

Figura 2. Topologia incremental do Cascade-Correlation

3.3. Árvores de Decisão

Uma das principais desvantagens das Redes Neurais é que elas não permitem que se visualize de forma trivial o conhecimento adquirido no processo de aprendizado. Quando se deseja saber quais as regras que levaram a tomada de uma certa decisão, outras técnicas de Aprendizado de Máquinas são mais adequadas, como por exemplo as Árvores de Decisão [Quinlan (1993)]. As Árvores de Decisão, construídas de modo automático utilizando aprendizado supervisionado, resultam em um conjunto de regras booleanas do tipo se/então/senão, que formam uma árvore onde os nodos mais elevados correspondem as entradas mais relevantes na classificação dos dados de entrada. No Sistema NeuralSignX, foi utilizado o algoritmo C4.5, proposto por [Quinlan (1993)].

Para que fosse possível verificar a importância dos atributos na autenticação das assinaturas de diversos usuários, foram geradas Árvores de Decisão para alguns usuários da base de dados. As informações enviadas para as Árvores de Decisão são as mesmas envidas para a Rede Neural, sendo necessário apenas alterar o formato dos arquivos para que sejam aceitos pelo software C4.5. Na Figura 3 é mostrada a árvore de decisão gerada com as assinaturas de um determinado usuário.

```
Decision Tree:

Interseccao_Y_3 <= 0 :
|   Soma_comprimento_vetores_Norte > 30 : FALSIFICATION (225.0/1.0)
|   Soma_comprimento_vetores_Norte <= 30 :
|   |   Ponto_amostrado_Y_1 <= 84 : FALSIFICATION (22.0/1.0)
|   |   Ponto_amostrado_Y_1 > 84 : ARNO_JOSE_HEINEN (14.0)
Interseccao_Y_3 > 0 :
|   Interseccao_Y_2 > 0 : FALSIFICATION (2153.0)
|   Interseccao_Y_2 <= 0 :
|   |   Ponto_amostrado_Y_5 <= 15 :
|   |   |   Velocidade_media <= 235 : ARNO_JOSE_HEINEN (2.0)
|   |   |   Velocidade_media > 235 : FALSIFICATION (5.0)
|   |   Ponto_amostrado_Y_5 > 15 :
|   |   |   Interseccao_Y_4 <= 3 : FALSIFICATION (116.0)
|   |   |   Interseccao_Y_4 > 3 :
|   |   |   |   Soma_comprimento_vetores_Noroeste <= 0 : ARNO_JOSE_HEINEN (2.0)
|   |   |   |   Soma_comprimento_vetores_Noroeste > 0 : FALSIFICATION (11.0)
```

Figura 3. Árvore de decisão para as assinaturas de um usuário

Pela análise das árvores pôde-se perceber que alguns atributos são mais importantes para a autenticação de determinadas assinaturas do que outros, e ***estes atributos variam de usuário para usuário***. Também foi possível perceber através da análise das Árvores de Decisão que para usuários diferentes existem atributos diferentes que melhor os identificam. Assim, foi possível identificar a importância da maioria dos atributos selecionados, e também se pode constatar que quanto mais atributos forem utilizados nas simulações, melhor é o desempenho do sistema.

4. Sistema proposto: NeuralSignX

O sistema proposto, denominado Sistema NeuralSignX[1], é constituído de três módulos, como é mostrado na Figura 4.

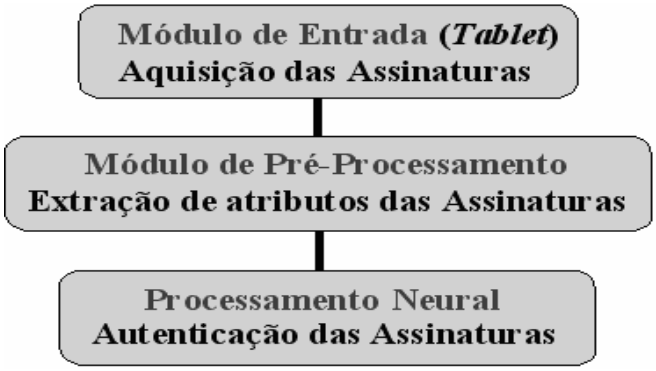

Figura 4. Módulos do sistema de autenticação de assinaturas proposto

4.1. Módulo de entrada

O módulo de entrada é responsável pela leitura dos dados provenientes do *tablet* e o armazenamento destes dados em disco. Este módulo gera um arquivo contendo uma descrição das assinaturas, onde cada assinatura é composta por uma seqüência de coordenadas da caneta (x, y), seu estado (1 ou 0: desenhando ou caneta levemente levantada) e um registro do momento em que cada ponto foi lido, com precisão na ordem de centésimos de segundo. O *tablet* utilizado no desenvolvimento do sistema

[1] O sistema proposto está documentado e disponibilizado no *site* http://www.bminds.com.br/~milton/

proposto é o PenTablet SuperPen WP4030, fabricado pela UC-Logic[2]. Um exemplo dos dados coletados pelo módulo de entrada é apresentado abaixo:

```
LOGIN=MILTON
116 478 0 21:42:23:821
116 478 1 21:42:23:831
125 467 1 21:42:23:842
134 456 1 21:42:23:852
145 441 1 21:42:23:873
168 445 0 21:42:23:883
175 493 0 21:42:23:894
189 517 1 21:42:23:907
```

4.2. Pré-processamento

O módulo de pré-processamento é sub-dividido em duas etapas. Na primeira etapa são realizados ajustes visuais na assinatura, e na segunda etapa são extraídos os atributos, que são informações obtidas a partir das assinaturas que permitem diferenciar as assinaturas de determinado usuário em relação às demais. Os ajustes realizados na primeira etapa são:

- Ajuste de posição: este ajuste minimiza as variações posicionais que ocorrem entre assinaturas de uma mesma pessoa. O Ajuste pode ser realizado pelo canto superior esquerdo ou pelo centro de massa da assinatura;
- Ajuste de escala: este ajuste redimensiona as assinaturas para um tamanho padrão, de forma que as diferenças de escala entre as assinaturas sejam minimizadas;

Na segunda etapa do módulo de pré-processamento é realizada a extração de atributos. Os atributos utilizados pelo do sistema foram baseados em técnicas de pré-processamento encontradas na literatura, somados a outros atributos que foram propostos e/ou adaptados pelos próprios autores em [Osório (1991)] e [Heinen (2002)]. Após o levantamento e a elaboração dos atributos, foi realizado um estudo para se verificar a relevância de cada atributo, utilizando Árvores de Decisão [Mitchell (1997)]. Os atributos que se mostraram mais eficientes foram:

- Tempo de duração da assinatura: é o tempo que o usuário utilizou para a realização da assinatura [Gupta et al. (1997)];
- Número de vezes em que a caneta foi levantada: conta-se quantas vezes a caneta se afastou do *tablet* durante a assinatura [Heinen (2002)];
- Velocidade média e máxima da assinatura: é a velocidade de deslocamento da caneta sobre o *tablet* [Heinen (2002)];
- Número de trocas de sentido da caneta 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 [Heinen (2002)];
- Contagem da quantidade de pseudovetores apontando para cada um dos oito quadrantes: este atributo extrai a forma estrutural da assinatura e depois verifica quantos pseudovetores apontam para as coordenadas (N, S, L, O, NO, SO, NL, SL) [Heinen (2002)]. A Figura 5 demonstra o uso desta técnica;

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

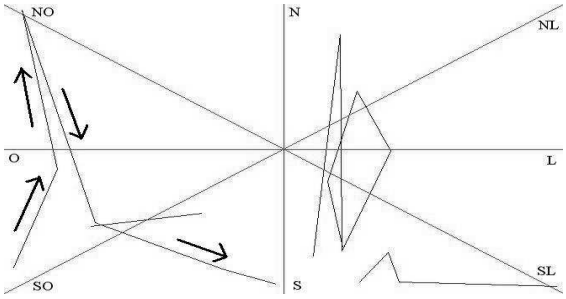

Figura 5. Pseudovetores apontando para os quadrantes

- Densidade da assinatura com informações de grade: divide-se a assinatura em diversas células, e para cada célula é calculada a densidade de pontos [Baltzakis et al. (2000)]. A Figura 6 é demonstra o uso desta técnica. As células com maior densidade de pontos são representadas por tons mais escuros.

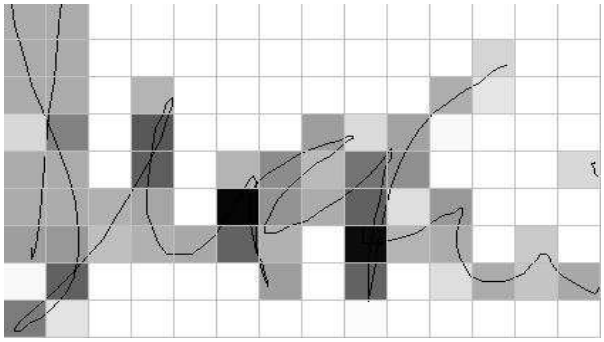

Figura 6. Densidade de pontos da assinatura

- Interseções de linhas verticais e horizontais em relação à assinatura: a partir de uma assinatura desenhada em um *bitmap*, são traçadas linhas imaginárias cortando a assinatura em intervalos fixos, e para cada linha imaginária, são contadas quantas vezes esta linha intersecciona a assinatura [Osório (1991)];
- Amostragem seqüencial da assinatura: permite a obtenção da trajetória da assinatura por amostragem (Figura 7);

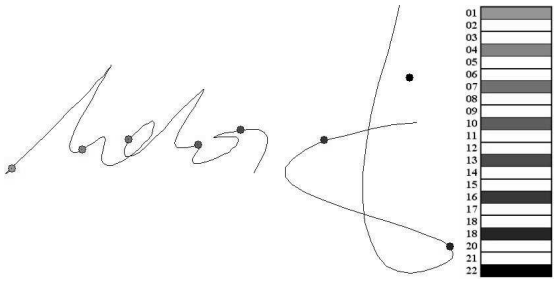

Figura 7. Amostragem seqüencial da assinatura

O sistema permite que o usuário selecione os atributos que serão utilizados no processo de autenticação, e também vários parâmetros de simulação e aprendizado.

4.3. Processamento neural

O módulo de processamento neural recebe o valor dos atributos fornecidos pelo módulo de pré-processamento e realiza a classificação, dizendo se uma assinatura é verdadeira 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 *Backpropagation*, o algoritmo *Cascade-Correlation*. Este algoritmo foi selecionado ser mais eficiente que o *Backpropagation* em tarefas de classificação [Fahlman (1990)]. O simulador de Redes Neurais Artificiais utilizado foi o Neusim [Osório (1999)], que é um simulador que pode ser facilmente integrado e customizado em diferentes aplicações.

O módulo de Processamento Neural possui duas fases, a fase de aprendizado e a fase de execução. Na fase de aprendizado, a base de dados de assinaturas é submetida ao simulador Neusim, que realiza o treinamento de forma que o sistema aprenda como classificar as assinaturas de forma correta. Na fase de execução, é realizada a autenticação de assinaturas propriamente dita, onde uma assinatura é submetida ao sistema, e baseado no conhecimento que a Rede Neural adquiriu durante a fase de aprendizado, é realizada a classificação, informando se a assinatura analisada é autêntica ou não.

6. Resultados

A base de dados de assinaturas utilizada nas simulações foi coletada ao longo de um ano, e cada usuário contribuiu com diversas assinaturas recolhidas em diferentes épocas, de forma que as variações que ocorrem ao longo do tempo em uma assinatura estivessem presentes na base de dados. Nos experimentos realizados contatou-se que cerca de 10 assinaturas por usuário seriam suficientes para o aprendizado da Rede Neural, mas para a validação do modelo proposto foram utilizadas mais assinaturas (até 80 por usuário), de forma a verificar se a autenticação está ocorrendo de forma satisfatória. A composição da base de dados de assinaturas ficou da seguinte forma:

- 2300 assinaturas autênticas, recolhidas de 67 usuários (média de 30 assinaturas por usuário);
- 250 assinaturas falsificadas, realizadas por 12 pessoas diferentes, que reproduzem as assinaturas de 30 usuários presentes na base de dados;
- 27449 assinaturas geradas de forma aleatória.

As assinaturas geradas aleatoriamente compunham a chamada “Nuvem de Pontos”, que visa melhorar o processo de reconhecimento das assinaturas, delimitando de forma mais precisa a classe de interesse [Heinen (2002)]. Este problema de delimitar a classe é usualmente resultante do fato de que em certos tipos de aplicações de classificação existe um número razoável de exemplos da classe a ser reconhecida, e o número de exemplos que não pertence a esta classe é praticamente ilimitado [Bender et al. (2003)]. A obtenção manual dos exemplos que não pertencem à classe pode ser difícil e custosa, por isto foi proposta a geração automática de contra-exemplos, que formam uma “Nuvem de Pontos” (ruído), que visa cobrir da melhor forma possível o espaço de valores de entrada. Isto também se deve ao fato de o número de atributos utilizados é grande, e as árvores de decisão terem demonstrado a importância de todos os atributos para a classificação das assinaturas.

Quando se trabalha com Aprendizado de Máquina, são necessárias diversas simulações, pois os resultados obtidos podem variar entre uma simulação e outra. Por isso foram realizados dez testes para cada usuário, e ao final foram calculadas as médias obtidas

por usuário. A Tabela 1 mostra os resultados obtidos nos primeiros testes, que foram realizados utilizando apenas assinaturas autênticas. O total de assinaturas utilizadas foi de 1300, sendo 675 utilizadas na base de treino e 675 na base de testes.

Tabela 1. Somente assinaturas autênticas

Usuário	Média do Total de Acertos	Média FP	Média FN	Nº assinaturas usuário
Usuário 1	674,6 - 99,94%	0	0,4	70
Usuário 2	673 - 99,70%	0	2	10
Usuário 3	674 - 99,85%	1	0	25
Usuário 4	675 – 100%	0	0	15
Usuário 5	673,8 - 99,82%	0	1,2	15
Média	**674,1 - 99,86%**	**0,2**	**0,72**	**32,4**

A média geral (para todos usuários testados) ficou em torno de 0,72 casos de falsas rejeições (FN), e 0,2 casos de falsos aceites (FP). A média de acertos ficou em torno de 99,86%.

Utilizando assinaturas falsificadas juntamente com as assinaturas verdadeiras, foram realizados testes com assinaturas de 30 usuários diferentes, e a média dos resultados ficou em torno de 1,16 casos de falsas rejeições e 0,84 casos de falsos aceites. A média de acertos na base de testes ficou em torno de 99,99%. A Tabela 2 mostra os resultados deste segundo experimento para cinco usuários. O número total de assinaturas presentes na base de testes foi de 29999 assinaturas, o que permitiu verificar que a classe a ser reconhecida estava realmente bem delimitada.

Tabela 2. Assinaturas autênticas e falsificadas

Usuário	Média do Total de Acertos	Média FP	Média FN	Nº assinaturas usuário
Usuário 1	29.996 (99,98%)	0	3	70
Usuário 2	29.997,4	0,6	1	40
Usuário 3	29.997	1,8	0,2	15
Usuário 4	29.996,4	1,6	1	15
Usuário 5	29.998,2	0,2	0,6	15
Média	**29.997 (99,99%)**	**0,84**	**1,16**	**32,4**

Em um sistema de autenticação on-line de assinaturas, o importante é que a taxa de falsos aceites seja baixa, pois é menos prejudicial ao sistema pedir para que o usuário assine novamente do que aceitar uma assinatura falsificada como verdadeira.

7. Conclusão

Este trabalho teve por objetivo o estudo da autenticação de usuários através de assinaturas manuscritas, utilizando Redes Neurais Artificiais. Para atingir tal objetivo foram estudados diversos tópicos referentes à autenticação de assinaturas, como a definição de métodos de pré-processamento, o levantamento dos atributos a serem utilizados, a análise destes atributos usando árvores de decisão, e a classificação das assinaturas utilizando Redes Neurais Artificiais. Também foi criada a proposta de solução e implementação de um sistema de autenticação *on-line* de assinaturas, e para validar esta proposta de implementação foi desenvolvido o protótipo completo e operacional do sistema, e também foi coletada uma base de dados de assinaturas reais. A partir dos resultados obtidos foi possível comprovar que as Redes Neurais Artificiais são muito adequadas ao processo de autenticação, e que os atributos selecionados foram

muito eficazes na autenticação de assinaturas, pois permitiram que a Rede Neural conseguisse obter taxas elevadas de aprendizado e de generalização, mantendo baixos índices de falsos aceites, 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) e o aperfeiçoamento das técnicas de pré-processamento e extração de atributos das assinaturas.

8. Referências

[Abbas (1994)] Abbas, Rasha. *Backpropagation Networks prototype for off-line signature verification.* Minor thesis, RMIT, Department of Computer Science, Melbourne, March 1994.

[Baltzakis et al. (2000)] Baltzakis, H.; Papamarkos, N. *A new signature verification technique based on a two stage neural network classifier.* Engineering applications of Artificial intelligence 14(2001), pp.95-103, September 2000.

[Bender et al. 2003)] Bender, T.; Osório, Fernando S. *Reconhecimento e Recuperação de Imagens Utili-zando Redes Neurais Artificiais do Tipo MLP*. IV ENIA – Congresso da SBC 2003. Campinas, Agosto 2003. http://inf.unisinos.br/~tulio/

[Cattell (1952)] Cattell, Raymond. *Factor Analysis.* New York. Harper Books, 1952.

[Fahlman (1990)] Fahlman, Scott E.; Lebiere, C. *The Cascade-Correlation learning architecture.* Carnegie Mellon University – CMU. Computer Science Technical Report CMU-CS-90-100. February 1990.

[Gupta et al. (1997)] Gupta, G.; Mccabe, A. *A review of dynamic handwritten signature verification.* Technical Report - James Cook University, Australia, 1997.

[Haykin (2001)] Haykin, S. *Redes Neurais: Princípios e Prática.* 2ª ed. Bookman. 2001.

[Heinen (2002)] Heinen, Milton Roberto. *Autenticação On-line de assinaturas utilizando Redes Neurais.* UNISINOS. Trabalho de Conclusão. 92p, 2002. http://www.bminds.com.br/~milton/

[Jain et al. (2002)] Jain, A. K.; Griess, F. D.; Connell, S. D. *On-line signature verification.* Pattern Recognition (In Press, Uncorrected Proof). Elsevier Press. Jan. 2002.

[Mitchell (1997)] Mitchell, Tom. *Machine Learning.* WCB / McGrall-Hill – Computer Science Series. Boston, MA. 1997.

[Osório (1991)] Osório, Fernando S. *Um estudo sobre reconhecimento visual de caracteres através de Redes Neurais.* UFRGS, CPGCC. Dissertação de mestrado, 1991. http://inf.unisinos.br/~osorio/

[Osório (1999)] Osório, Fernando S. *INSS: A hybrid system for constructive machine learning.* Neurocomputing 28 (1999) 191-205. Elsevier Press 1999.

[Quinlan (1993)] Quinlan, J. R. *C4.5- Programs for Machine Learning*. Morgan Kauffman Publishers. San Mateo, CA. 1993.

[Rumelhart et al. (1986)] Rumelhart, D.; Hinton, G.; Williams, R. *Learning Internal Representations by Error Propagation.* Parallel Distributed Processing: Explorations in the Microstructure of Cognition - Vol. 1. Cambridge: MIT Press, 1986.