# Biometria Comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas

Milton Roberto Heinen[1]
Fernando Santos Osório[2]

UNISINOS - Universidade do Vale do Rio dos Sinos
Ciências Exatas e Tecnológicas – Computação Aplicada
CEP 93022-000 São Leopoldo (RS)
[1]milton_heinen@yahoo.com.br
[2]osorio@exatas.unisinos.br

**Resumo.** O objetivo do presente trabalho é descrever o desenvolvimento da pesquisa e implementação de um sistema que realiza a autenticação de usuários através do uso 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 do sistema proposto, e os resultados obtidos foram da ordem de 99,99% de acertos.

**Palavras-Chave:** Autenticação de Assinaturas, Reconhecimento de Padrões, Inteligência Artificial, Aprendizado de Máquina, Redes Neurais Artificiais.

## 1 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 a pessoa que está tentando acessar um sistema é quem ela realmente diz ser. Na maioria dos sistemas de informação, a autenticidade dos usuários é garantida através de senhas alfanuméricas, que devem ser memorizadas pelos usuários e mantidas a salvo de outras pessoas. Apesar de ser a forma de autenticação mais difundida na atualidade, a autenticação por senhas apresenta diversas vulnerabilidades em termos de segurança, pois se elas caírem em mãos erradas, toda a segurança de um sistema é ameaçada.

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 se garantir a autenticidade dos usuários [Riha et al. (2000)]. Estas técnicas são muito mais seguras que as senhas, mas apresentam algumas desvantagens, como o custo elevado do equipamento de hardware necessário para a autenticação e o alto grau de intrusão, que gera desconfortos aos usuários [Heinen (2002)]. Em relação às impressões digitais, seu uso possui uma conotação negativa devido ao fato de estarem ligadas a delitos e investigações criminais [Jain et al. (2002)].

Além das características biométricas físicas, também podem ser utilizadas para a autenticação de usuários características biométricas comportamentais, como as assinaturas manuscritas, que apresentam diversas vantagens em relação às demais 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$ 25,00 e U$ 100,00).

Mas apesar das diversas vantagens que esta técnica apresenta, a autenticação de assinaturas é um problema de difícil solução do ponto de vista computacional, devido a grande variabilidade que ocorre entre assinaturas de uma mesma pessoa [Huang et al.

(1997)]. Esta variabilidade faz com que soluções baseadas em técnicas de Inteligência Artificial e Aprendizado de Máquinas apresentem melhores resultados do que soluções puramente algorítmicas [Baltzakis et al. (2000)].

Neste trabalho foi desenvolvida uma metodologia, bem como a sua implementação em um protótipo [Milton (2002)], que permite realizar a autenticação de usuários através do uso de assinaturas manuscritas. As principais contribuições deste trabalho são: a elaboração e o teste de um conjunto significativo de atributos relativos às assinaturas, a aplicação de um modelo de Rede Neural (*Cascade-Correlation*) que permite otimizar o processo de aprendizado e a performance da rede, e o desenvolvimento de uma técnica de melhoria do aprendizado através da geração automática de contra-exemplos (Nuvem de Pontos).

Este artigo está estruturado da seguinte forma: Inicialmente serão apresentados diversos conceitos relativos à autenticação de assinaturas e as Redes Neurais Artificiais, que são o método escolhido para se realizar a autenticação das assinaturas neste sistema. Em seguida será apresentado o modelo proposto, descrevendo o funcionamento de seus diversos módulos, e por último serão apresentados os resultados obtidos nas simulações realizadas com o sistema.

## 2 Reconhecimento de assinaturas

A autenticação de assinaturas 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 e enviada para o sistema que realiza a autenticação. Na autenticação *on-line*, a assinatura é feita diretamente sobre um dispositivo de hardware, como uma mesa digitalizadora ou um *tablet* (Figura 1). Além destes dispositivos, podem ser utilizados para a autenticação *on-line* de assinaturas computadores do tipo *Handheld*, que permitem a escrita diretamente sobre uma tela sensível.

**Figura 1:** Exemplo de um *tablet*

O reconhecimento *on-line* de assinaturas permite que sejam utilizadas diversas informações temporais e dinâmicas relativas à assinatura, como a velocidade da caneta e a trajetória, que permitem que se obtenham melhores resultados no processo de autenticação. Neste sistema 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.

## 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. Para existir um problema de Aprendizado de Máquina bem definido devem-se identificar três características fundamentais: a tarefa a ser aprendida, a medida de performance e a fonte de experiência. Também é necessário que se defina o conhecimento que será aprendido através da experiência, também chamado de função alvo. No caso do reconhecimento de assinaturas, o conhecimento que deve ser aprendido é como classificar de forma correta uma assinatura: autêntica ou não. A tarefa é a classificação das assinaturas, a fonte é a base de dados de assinaturas e a medida é a avaliação feita sobre a taxa de acertos na autenticação das assinaturas. Existem diversas técnicas de Aprendizado de Máquina que podem ser utilizadas para a autenticação de assinaturas, como as Árvores de Decisão, os Sistemas *Fuzzi*, os Algoritmos Genéticos e as 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 necessário um conjunto de dados com exemplos de padrões e as respostas esperadas (padrões e classes correspondentes). Esta base de dados de aprendizado é apresentada para a Rede Neural Artificial (RNA) de modo que esta possa aprender a responder de forma similar às respostas informadas na base de dados, passando a reconhecer os padrões. Utiliza-se também uma segunda base de dados, a base de validação (avaliação da generalização), que é usada unicamente para medir o desempenho do aprendizado (não é usada no ajuste da rede), sendo esta

base um conjunto de dados diferente do usado no aprendizado [Osório (1998)]. Este tipo de aprendizado é conhecido como aprendizado supervisionado com validação cruzada [Haykin (2001)].

Através de um processo iterativo, são apresentados à Rede Neural diversos exemplos contidos na base de dados de aprendizado, para que ocorra a adaptação dos pesos, que simulam o reforço e a inibição das conexões sinápticas existentes entre os neurônios reais. Desta adaptação de pesos surge o aprendizado, que fará com que a Rede Neural aprenda a responder aos estímulos de entrada de acordo com as respostas desejadas contidas nos exemplos apresentados.

## 4 Sistema proposto: NeuralSignX

O sistema proposto, denominado Sistema NeuralSignX[1], é constituído de três módulos, como é mostrado na Figura 2.

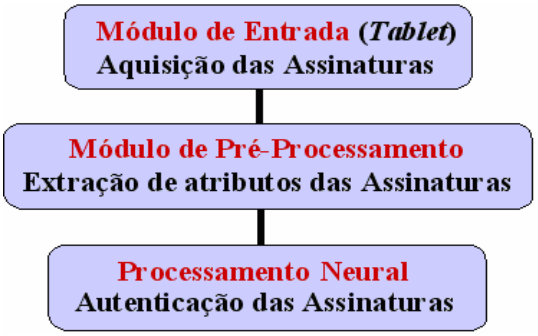


**Figura 2:** Módulos do sistema de autenticação de assinaturas proposto

### 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 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 técnicas como Matrizes de Correlação, Análise de Componentes Principais [Cattell (1952)] e Árvores de Decisão [Mitchell (1997)]. Alguns dos 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

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

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

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 3 demonstra o uso desta técnica;

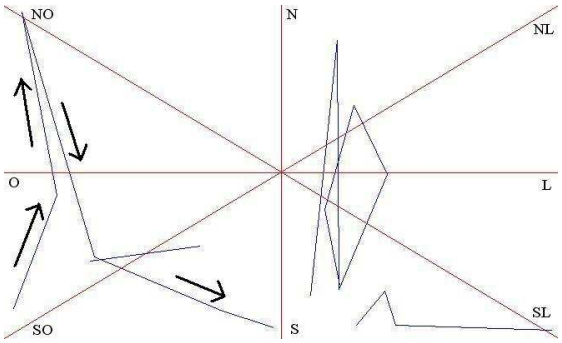


**Figura 3:** Pseudovetores apontando para os oito quadrantes

- 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 4 é demonstra o uso desta técnica. As células com maior densidade de pontos são representadas por tons mais escuros.

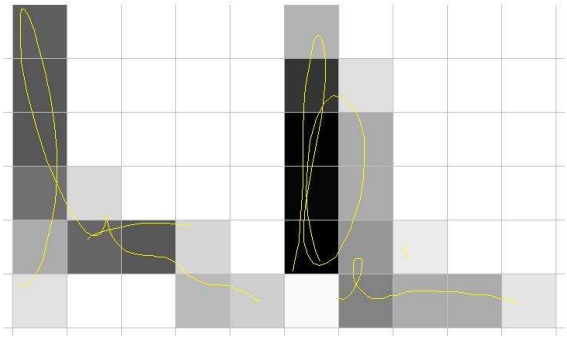

**Figura 4:** Densidade de pontos da assinatura

- 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)]. Na Figura 5 são mostradas diversas linhas verticais e horizontais interseccionando uma assinatura.

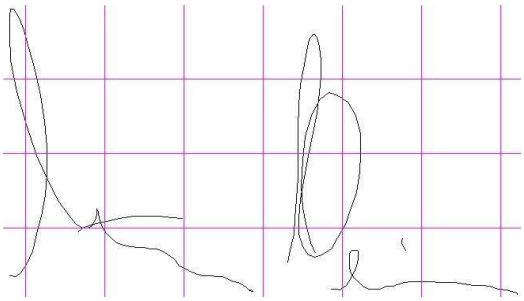

**Figura 5:** Interseções de linhas verticais e horizontais em relação à assinatura

O sistema permite que o usuário selecione os atributos que serão utilizados no processo de autenticação, e também vários parâmetros de simulação e aprendizado. A Figura 6 mostra uma das telas do módulo de pré-processamento do sistema NeuralSignX. À medida que as assinaturas vão sendo analisadas pelo sistema, são mostradas na tela diversas informações visuais relativas aos atributos das assinaturas.

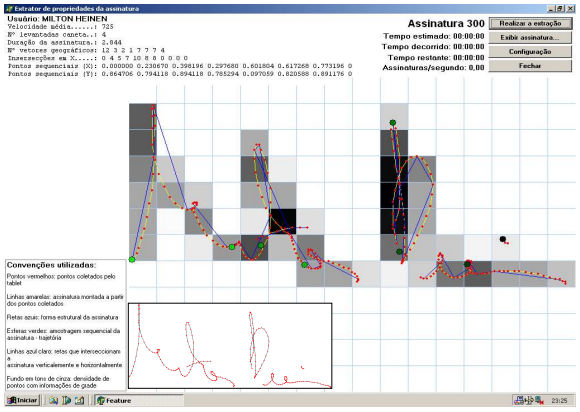


**Figura 6:** Tela principal do módulo de pré-processamento

### 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* [Fahlman (1990)]. Este algoritmo foi selecionado ser mais eficiente que o *Backpropagation* em tarefas de classificação, e também pelo fato de não haverem sido encontrados na literatura outros trabalhos que utilizassem este algoritmo de aprendizado para a autenticação de assinaturas. 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.

## 5 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.

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 presentes na base de testes foi de 675 assinaturas.

**Tabela 1:** Somente assinaturas autênticas

| **Usuário** | Média do Total de Acertos | Média AI | Média RI | Nº assinaturas do 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 rejeições indevidas (RI), e 0,2 casos de aceites indevidos (AI). Um aceite indevido é quando uma assinatura que não pertence a determinado usuário é classificada como se fosse dele, e uma rejeição indevida é quando uma assinatura que pertence ao usuário é classificada como se não fosse dele. 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 rejeições indevidas e 0,84 casos de aceites indevidos. 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.

**Tabela 2:** Assinaturas autênticas e falsificadas

| **Usuário** | Média do Total de Acertos | Média AI | Média RI | Nº assinaturas do 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 aceites indevidos seja baixa, pois é menos prejudicial ao sistema pedir para que o usuário assine novamente do que aceitar uma assinatura falsificada como verdadeira.

## 6 Conclusão

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 e as Redes Neurais Artificiais, e foi descrita uma proposta de solução e implementação de um sistema de autenticação *on-line* de assinaturas. Para validar esta proposta de implementação, foram desenvolvidas diversas ferramentas que implementam as diversas operações e etapas estudadas neste trabalho, criando assim um protótipo completo e operacional do sistema.

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 do tipo *Cascade-Correlation* são muito adequadas ao processo de autenticação de assinaturas, e que os atributos selecionados foram muito eficazes na classificação das assinaturas, pois permitiram que a Rede Neural conseguisse não apenas obter elevadas taxas de aprendizado, como também de generalização, mantendo baixos os índices de aceites indevidos, o que é fundamental em um sistema de autenticação de assinaturas. Cabe salientar que não são encontrados no mercado atualmente sistemas similares ao desenvolvido, que permitam a autenticação de assinaturas com o mesmo grau de segurança, o que torna o sistema NeuralSignX uma ferramenta de grande potencial do ponto de vista comercial.

## 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 Utilizando 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, Gopal; Mccabe, Alan. *A review of dynamic handwritten signature verification.* Technical Report - James Cook University, Townsville, Australia, 1997.

[Haykin (2001)] Haykin, Simon. *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/ ou http://inf.unisinos.br/~osorio/NeuralSignX/nsx.html

[Huang et al. (1997)] Huang, Kai; Yan, Hong. *Off-line signature verification based on geometric feature extraction and neural network classification.* Pattern Recognition, V30, N1. pp-9-17. Elsevier Press, 1997.

[Jain et al. (2002)] Jain, Anil K.; Griess, Friederike D.; Connell, Scott 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/

[Osorio (1998)] Osorio, Fernando S. *INSS: Un Système Hybride Neuro-Symbolique pour l'Apprentissage Automatique Cons-tructif.* Tese de Doutorado. INPG/IMAG - Grenoble, França. 1998.

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

[Riha et al. (2000)] Riha, Zdenek; Matyas, Vaclav. *Biometric authentication systems.* FI MU Report Series, RS-2000-08, November 2000.

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