NeuralSignX: Sistema Neural para a Autenticação de Assinaturas

Milton Roberto Heinen[1]

Fernando Santos Osório[2]

Resumo *–Este artigo apresenta nosso trabalho relacionado com a pesquisa e implementação de um sistema para a o reconhecimento (autenticação) de assinaturas manuscritas, através de um processo de reconhecimento on-line, baseado no uso de Redes Neurais. Neste trabalho são descritos os conceitos básicos da área de autenticação de assinaturas e os procedimentos necessários, e por nós implementados, que irão conduzir a uma autenticação robusta e confiável de assinaturas. O sistema NeuralSignX é apresentado, onde seus módulos são descritos e os resultados práticos do uso deste sistema são analisados onde é feita uma avaliação de seu desempenho usando uma base de dados de assinaturas reais.*

Palavras Chave *–- Autenticação de Assinaturas, Redes Neurais Artificiais, Recohnecimento de Padrões.*

I. INTRODUÇÃO

Nos dias atuais, o uso cada vez mais freqüente de sistemas de informação e a premente necessidade de aumento da segurança, traz a necessidade de se identificar, autenticar e controlar os usuários de forma segura. 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 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 (muitos usuários não aceitam se sujeitar a um exame biométrico). Neste trabalho foi desenvolvida uma metodologia, bem como a sua implementação em um protótipo [4,5], que permite realizar a autenticação de usuários através do uso de assinaturas manuscritas – biometria comportamental [4]. A autenticação das assinaturas é implementada neste trabalho através do uso de um hardware de baixo custo e do uso de Redes Neurais Artificiais. Este processo é considerado pouco intrusivo, pois as pessoas já possuem o hábito de usar assinaturas para autenticar documentos diversos, e não precisam sofrer um processo, algumas vezes considerado incômodo, de leitura de suas características biométricas físicas (e.g. digitais, retina ou íris).

II. AUTENTICAÇÃO DE ASSINATURAS

O uso de assinaturas é correntemente aplicado em nossa sociedade para autenticar documentos e referendar transações. A autenticação de assinaturas pode ser realizada de duas formas: **off-line** [1] e **on-line** [2]. Na autenticação off-line, a assinatura realizada no papel, sendo digitalizada e depois analisada. Este é um processo que só pode se basear em atributos estáticos. Na autenticação on-line a assinatura é lida diretamente por um dispositivo de digitalização, como por exemplo um conjunto *caneta-tablet*, do tipo apresentado na Figura 1. Este tipo de dispositivo permite capturar informações da dinâmica do movimento (modo de assinar). Um dos principais objetivos ao se buscar a *autenticação on-line* de assinaturas é a extração de atributos comportamentais que sejam caracterizadores das assinaturas dos usuários, de modo a identificá-la de forma única. Esta identificação usualmente baseia-se em técnicas de aprendizado de máquina [14], que são usualmente bastante adequadas para realizar este reconhecimento de padrões, permitindo desenvolver sistemas de alta performance.

Fig. 1. "Tablet" utilizado para coleta de assinaturas

A. Reconhecimento de Padrões

[1] Milton Heinen, Bminds – Pólo de Informática / Unisinos, Av. Unisinos 950 – São Leopoldo/RS, E-Mail: *miltonrh@ig.com.br*.

[2] Fernando Osório, Programa de Pós-Graduação em Computação Aplicada – PIPCA / Unisinos, Av. Unisinos 950 – São Leopoldo/RS – CEP. 93022-000. Tel. (51) 5908161, Fax: (51) 590-8162, E-mail: *osorio@exatas.unisinos.br* .

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: (i) Uso de um conjunto de exemplos de assinaturas de um usuário, mas de tamanho limitado; (ii) 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; (iii) Aprendizado focado na obtenção de um baixíssimo nível de falsos aceites (é bastante desejável que este índice seja *zero*); (iv) 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 [14]: 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.

B. Redes Neurais Artificiais

Através de um modelo abstrato e simplificado dos neurônios humanos é possível desenvolver um simulador neural que seja capaz de classificar, generalizar e aprender a reconhecer padrões. Um dos modelos de aprendizado Neural mais utilizados na atualidade é o modelo denominado Multi-Layer Perceptron (MLP), com aprendizado do tipo Back-propagation [3].

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 (RNA) de modo que esta possa aprender a responder de forma similar as 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. Este tipo de aprendizado é conhecido como aprendizado supervisionado com validação cruzada [3,8].

O sistema de autenticação on-line de assinaturas que desenvolvemos usou Redes Neurais para a criação do classificador, que identifica se uma assinatura é ou não de um determinado usuário (aceita/rejeita). Assim, cada usuário terá uma Rede Neural especificamente treinada para o reconhecimento de sua assinatura, onde para cada novo usuário basta criar uma nova Rede Neural e adicionar ao sistema (sistema expansível).

III. O SISTEMA NEURALSIGNX

O Sistema NeuralSignX [4,5] é um sistema de autenticação on-line de assinaturas baseado em Redes Neurais, composto de três módulos (fig.2). O primeiro módulo é o módulo de entrada, responsável pela leitura *on-line* dos dados das assinaturas provenientes de um *tablet*.

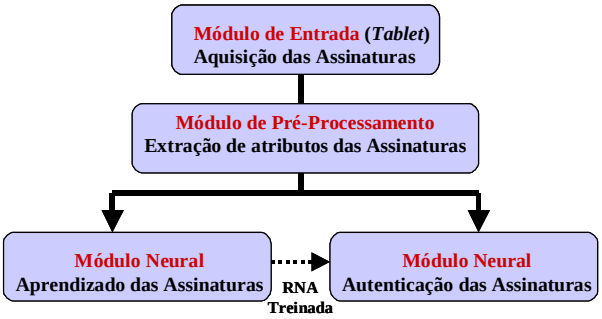

Fig. 2. Módulos do Sistema NeuralSignX

O **módulo de entrada** gera um arquivo contendo uma descrição das assinaturas, onde cada assinatura é composta por uma seqüência de coordenadas da caneta (X, Y: adotou-se uma área útil de desenho de 800x600 pontos), 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. Um exemplo dos dados coletados pelo módulo de entrada é apresentado abaixo:

```
LOGIN=OSORIO
93 309 1 21:55:13:150
96 309 1 21:55:13:210
99 309 1 21:55:13:260
102 309 1 21:55:13:260
111 309 1 21:55:13:320
117 309 1 21:55:13:320
126 309 1 21:55:13:320
132 309 1 21:55:13:370
...
```

O segundo **módulo** é o **de pré-processamento**, responsável pelos ajustes de posição e escala e pela extração dos atributos caracterizadores das assinaturas. Os atributos são informações obtidas a partir das assinaturas que permitem diferenciá-las umas das outras, como por exemplo: a velocidade média da caneta, o tempo de duração da assinatura, a densidade de pontos por regiões, entre outros. A Fig. 3 apresenta uma tela da interface do módulo de pré-processamento do sistema NeuralSignX.

Os atributos que usamos na implementação do sistema foram baseados em técnicas de pré-processamento encontradas na literatura [1,2,11,12,13], somados a outros que foram propostos e/ou adaptados pelos próprios autores [4,7]. Cabe destacar que foram estudados diversos atributos, onde alguns deles (a exemplo dos baseados em pressão e inclinação da caneta, descritos em [12]), acabaram não sendo utilizados. Um estudo sobre os atributos mais relevantes foi feito com o auxílio da aplicação da análise dos componentes principais – ACP [15] e também analisado-se os atributos mais relevantes selecionados durante a construção de árvores de decisão, usando o algoritmo C4.5 [14].

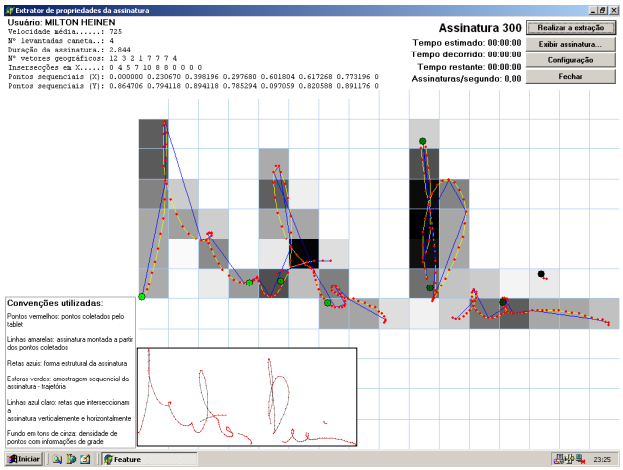

Fig. 3. Módulos do Sistema NeuralSignX

Entretanto, constatou-se que a eliminação de certos atributos, aparentemente menos relevantes ou já representados em outros atributos, nem sempre resultava em um bom desempenho. Certos atributos podiam ser considerados irrelevantes em assinaturas de diversos usuários (estatisticamente pouco significativos), mas talvez de grande importância apenas para um ou outro usuário. Sendo assim, optou-se por usar um conjunto de atributos, que mesmo tendo alguma redundância, demonstrou em experimentos preliminares (descritos em [4]) ter bons resultados. Os atributos adotados nos experimentos descritos a seguir foram os seguintes [4]:

· Densidade (quantidade) de pontos na grade dividida em células de 100x100 pontos – 48 atribs.;

· Interseções entre o traçado da assinatura e linhas verticais e horizontais em uma grade virtual composta de 23 linhas e 31 colunas - 54 atribs.;

· Amostragem de ‘n’ pontos originais (X e Y) distribuídos ao longo da seqüência de traçado da assinatura. O primeiro e último correspondem ao ponto de início e término da assinatura – 16 atribs.;

· Tempo de duração total da assinatura – 1 atrib.;

· Número de vezes que a caneta foi levantada durante o traçado da assinatura – 1 atributo;

· Velocidade média da caneta (permite detectar facilmente as falsificações) – 1 atributo;

· Velocidade máxima da caneta – 1 atributo;

· Contagem da quantidade de pseudo-vetores apontando para cada um dos 8 quadrantes (N, S, L,

O, NO, SO, NE, SE), gerados a partir do traçado original da assinatura – 8 atributos;

· Soma total do comprimento de cada um destes pseudo-vetores – 8 atributos;

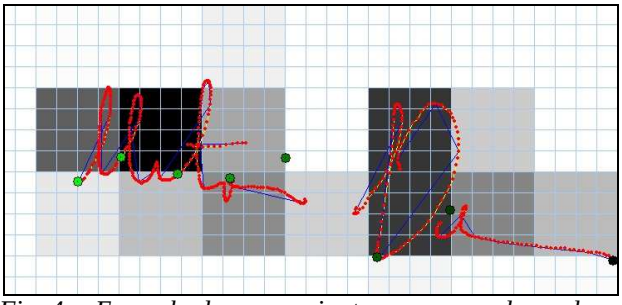

Fig. 4. Exemplo de uma assinatura processada, onde as zonas em tons escuros tem uma alta densidade de pontos

As Figuras 4 e 5 apresentam um exemplo de uma assinatura que foi analisada pelo modulo de pré-processa-mento e o respectivo resultado obtido na extração dos atributos descritos anteriormente. O total de atributos de entrada adotado nas redes neurais foi portanto fixado em 138 entradas numéricas, sendo obtidas de forma automática, para cada assinatura, pelo módulo de pré-processamento. As Redes Neurais possuem também 2 saídas binárias, codificadas da seguinte maneira: 10 (assinatura válida) e 01 (assinatura rejeitada).

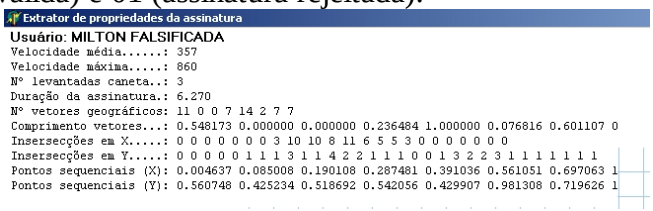

Fig. 5. Atributos extraídos de uma assinatura

O terceiro módulo, o **módulo neural**, realiza duas tarefas: (i) aprendizado das assinaturas e (ii) a classificação das assinaturas em 2 classes - aceitas/rejeitadas. A Rede Neural aprende e classifica as assinaturas a partir dos 138 valores dos atributos extraídos das assinaturas. Na implementação do Sistema NeuralSignX foi adotado um modelo de RNA baseado em MLP, entretanto, optou-se pelo uso de um algoritmo de aprendizado mais otimizado do que o *Back-Propagation*, o algoritmo *Cascade-Correlation* desenvolvido por Fahlman [6]. O módulo neural do sistema implementado adotou um simulador de RNAs baseadas no algoritmo Cascade-Correlation desenvolvido por Osório, o NeuSim [8]. Este simulador pode ser facilmente integrado a diferentes aplicações, e customizado de acordo com as necessidades de cada aplicação.

O módulo de aprendizado neural, recebe uma base de aprendizado e uma base de validação, realiza o treinamento da rede (validação cruzada) e gera um arquivo contendo os pesos e a topologia final da rede treinada. Estes arquivos que descrevem a rede podem então ser carregados pelo módulo neural de autenticação para realizar o teste sobre uma assinatura qualquer. O módulo de autenticação permite que sejam realizadas de forma integrada e automática as 3 etapas do processamento das assinaturas: entrada, pré-procesamento e autenticação.

Diversas RNAs foram treinadas com conjuntos diferentes de exemplos de assinaturas reais, coletados com o auxílio do *tablet*. Também foram criadas bases de assinaturas, para fins de teste de robustez, contendo assinaturas fictícias (desenhos feitos a mão), assinaturas falsificadas (tentativas de um usuário forjar uma assinatura já existente na base) e "*nuvem de pontos*" (geração automática de assinaturas fictícias). Estas bases foram usadas em uma série de experimentos, onde na seção seguinte iremos descrever alguns dos principais resultados obtidos, que permitem observar o bom desempenho obtido pelo NeuralSignX na autenticação *on-line* de assinaturas.

IV. RESULTADOS EXPERIMENTAIS

Nesta seção serão apresentados os resultados obtidos em dois experimentos principais, um primeiro usando uma base composta apenas de assinaturas reais (sem falsificações ou adição de assinaturas fictícias), compondo uma base com um total de 1350 assinaturas, e um segundo experimento usando assinaturas reais, falsificações e assinaturas fictícias, compondo uma base com um total de 29.999 assinaturas.

No primeiro experimento realizado para a autenticação de assinaturas, foi utilizada uma base de dados estruturada da seguinte forma:

- Total de 1350 assinaturas de 46 usuários diferentes;
- Base de dados total dividida de forma equilibrada em 2 partes: 675 assinaturas para o treinamento da rede (base de aprendizado) e 675 assinaturas para a validação da rede (base de teste);
- A base de dados total era composta por uma média de 30 assinaturas por usuário, com exceção do Usuário1, que possuía 70 assinaturas na base de aprendizado e na de teste;

- As assinaturas foram pré-processadas gerando um total de 138 entradas numéricas, e tendo como resposta duas saídas binárias assumindo uma das duas configurações: 01 ou 10.

TABELA I
RESULTADOS DA AUTENTICAÇÃO DO USUÁRIO1 (EXPER. 1)

Simulação	Teste 1	Teste 2	Teste 3	Teste 4	Teste 5
Dados Aprendizado	100%	100%	100%	100%	100%
Dados Validação	100%	99,85%	100%	99,85%	100%
No. Aceites Indevidos (FP)	0	0	0	0	0
No. Rejeições Indevidas (FN)	0	1	0	1	0
Média	Aprend.	100%	Média	Valid.	99,94%

Os resultados obtidos na autenticação das assinaturas de um usuário de teste são mostrados na Tabela 1. Nesta tabela são apresentados os resultados da autenticação da assinatura do Usuário1, que possuía um número maior de assinaturas na base de dados. Foram realizadas apenas cinco simulações, pois o algoritmo cascade-correlation apresenta uma pequena variabilidade dos resultados entre diferentes simulações. Nestas simulações foram computadas: a taxa de acerto para os Dados de Aprendizado, a taxa de acerto para os Dados de Validação, o número de Aceites Indevidos (FP – Falsos Positivos) e o número de Rejeições Indevidas (FN – Falsos Negativos). Constata-se que o desempenho da rede, considerando os dados da base de teste (validação) atingiu um índice médio de 99,94% de respostas corretas.

Foram realizados testes também com dados dos outros 46 usuários, obtendo resultados similares aos do experimento 1, conforme apresentado na Tabela 2, que contêm os resultados finais obtidos para 5 usuários diferentes. A Tabela 2 possui indicados os resultados médios obtidos com a base de validação (5 simulações) para os índices: Acertos na autenticação, Aceites Indevidos, Rejeições Indevidas e Quantidade de Assinaturas deste usuário que estavam presentes na base de assinaturas de teste. A média final de acertos se manteve próxima de 100% (99,86% de acertos).

TABELA II
AUTENTICAÇÃO DE DIFERENTES USUÁRIOS (EXPER. 1)

Usuário	Média do Total de Acertos	Média Aceites Indevidos	Média Rejeições Indevidas	Quantidade de Assinaturas de Teste
Usuário1	674,6 - 99,94%	0	0,4	70
Usuário2	673 - 99,70%	0	2	10
Usuário3	674 – 99,85%	1	0	25
Usuário4	675 – 100%	0	0	15
Usuário5	673,8 – 99,82%	0	1,2	15
Média	674,08 – 99,86%	0,2	0,72	32,4

No segundo experimento, o sistema foi submetido a uma base de 29.999 assinaturas para treino e para teste, composta por: assinaturas reais; assinaturas fictícias traçadas a mão; assinaturas fictícias geradas automaticamente; falsificações simples (usuário não especialista faz uma cópia de uma assinatura); e falsificações precisas (usuário treinado na reprodução de uma assinatura). Destas 29.999 assinaturas, 2550 eram assinaturas feitas por pessoas, sendo que foram divididas em 2 conjuntos, 1275 para aprendizado e 1275 para validação.

TABELA III
RESULTADOS DA AUTENTICAÇÃO DO USUÁRIO1 (EXPER.2)

Simulação	**Teste 1**	**Teste 2**	**Teste 3**	**Teste 4**	**Teste 5**
Dados Aprendizado	100%	100%	100%	100%	100%
Dados Validação	99,98%	99,99%	99,98%	99,98%	99,99%
N.º Aceites Indevidos FP	0	0	0	0	0
N.º Rejeições Indevidas FN	4	2	3	4	2
Média	100%	aprendizado		99,98%	teste

As assinaturas geradas de “modo automático” compunham a chamada “nuvem de pontos”, sendo que a base total de assinaturas possuía 28.724 assinaturas deste tipo inseridas na base de aprendizado e na base de validação. O uso da “nuvem de pontos” visa melhorar o processo de reconhecimento das assinaturas, delimitando de forma mais precisa a classe de interesse [4, 9, 10]. Este problema de delimitar a classe é usualmente resultante do fato de que em certos tipos de aplicações de classificação possuímos um número razoável de exemplos da classe a ser reconhecida, e o número de exemplos que não pertence a esta classe é praticamente ilimitado. A obtenção manual dos exemplos que não pertencem a 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 o mais possível todo o espaço de valores de entrada. Esta técnica é conhecida como geração de NNC – **Nuvem** de pontos **Não** pertencentes a **Classe** alvo [4,9]. O uso da geração de NNC visou refinar a rede de modo que esta ficasse mais robusta e pudesse inclusive evitar um aceite indevido de uma assinatura falsificada.

O NeuralSignX obteve no experimento 2 uma taxa média de aprendizado de 100% e de validação de 99,98%, conforme os resultados apresentados na Tabela 3, para o Usuário1. Este usuário em particu-

lar possuía 265 assinaturas, distribuídas em 140 assinaturas originais e 125 assinaturas com algum traço similar, mas que não deveriam ser aceitas como assinaturas destes usuário. Estas 265 assinaturas foram distribuídas de forma equilibrada entre as bases de aprendizado e de teste.

TABELA IV
AUTENTICAÇÃO DE DIFERENTES USUÁRIOS (EXPER. 2)

Usuário	Média do Total de Acertos	Média Aceites Indevidos	Média Rejeições Indevidas	Quantidade de Assinaturas de Teste
Usuário1	29.996 (99,98%)	0	3	70
Usuário2	29.997,4	0,6	1	40
Usuário3	29.997	1,8	0,2	15
Usuário4	29.996,4	1,6	1	15
Usuário5	29.998,2	0,2	0,6	15
Média	29.997 (99,99%)	0,84	1,16	32,4

É importante destacar que o número de assinaturas, que incluem as geradas automaticamente, era bastante grande, e mesmo assim o sistema foi robusto o suficiente para alcançar altas taxas de reconhecimento correto (autenticação). Este bom desempenho também pode ser observado quando foram realizados testes com outros usuários, onde os resultados obtidos para 5 usuários de teste são apresentados na Tabela 4. Constata-se um pequeno índice de aceites indevidos, mas acreditamos que este índice seja o reflexo do reduzido número de exemplos de assinaturas destes usuários presentes na base de dados. A adição de um número maior de assinaturas para estes usuários na base de aprendizado, a exemplo do que foi feito e constatado com os dados do Usuário1, poderia reduzir ainda mais este índice de aceitações indevidas.

Concluindo esta seção sobre os experimentos, devemos destacar que o Sistema NeuralSignX apresentou um desempenho adequado em relação as exigências impostas para um sistema de autenticação por biometria: nível de falsos aceites próximo a zero (em muitos casos igual a 0) e número de falsas rejeições bastante baixo. Estes resultados práticos nos levam a crer que sistemas baseados na metodologia proposta pelos autores, e posteriormente implementada e validada junto ao protótipo do sistema, podem ser usados de forma adequada em aplicações práticas (e.g. sistemas bancários, controle de acesso e autenticação on-line de documentos).

V. CONCLUSÕES E PERSPECTIVAS

Este artigo teve por objetivo apresentar uma descrição geral do sistema NeuralSignX. Concluímos que o sistema foi capaz de realizar a autenticação on-line de assinaturas, tendo sido testado com dados reais de assinaturas de um número expressivo de usuários, e obtendo índices de desempenho bastante satisfatórios.

Como trabalhos futuros podemos vislumbrar sistemas multimodais de autenticação de usuários baseados em características biométricas múltiplas (e.g. assinatura, face e íris) e o aperfeiçoamento das técnicas de pré-processa-mento e extração de atributos das assinaturas.

REFERÊNCIAS

[1] 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.

[2] Gupta, Gopal; McCabe, Alan. A Review of Dynamic Handwritten Signature Verification. Technical Report - James Cook University, Townsville, Australia, 1997.

[3] Haykin, Simon. Redes Neurais: Princípios e Prática, 2a. ed. Bookman. 2001.

[4] Heinen, Milton. Autenticação On-Line de Assinaturas utilizando Redes Neurais. TCC – Unisinos – Curso de Informática. Novembro 2002. 92p. Disponível no site: http://inf.unisinos.br/~osorio/NeuralSignX

[5] Heinen, Milton e Osório, Fernando. Autenticação On-line de assinaturas utilizando Redes Neurais. SIRC 2002, Simpósio de Informática. Santa Maria, RS. 2002.

[6] Fahlman, Scott e Lebiére Christian. The Cascade-Correlation Learning Architecture. Technical Report – CMU-CS-90-100, Carnegie-Mellon University. Feb.1990.

[7] Osório, Fernando S. Um estudo sobre reconhecimento visual de caracteres através de Redes Neurais. UFRGS, CPGCC. Dissertação de mestrado, 1991.

[8] Osório, F. INSS: Un Système Hybride Neuro-Symbolique pour l'Apprentissage Automatique Cons-tructif. Tese de Doutorado. INPG/IMAG - Grenoble, França. 1998.

[9] Bender, Túlio. Classificação e Recuperação de Imagens por Cor Utilizando Técnicas de Inteligência Artificial. Mestrado em Computação Aplicada – UNISINOS, Junho de 2003.

[10] Bender, T. e Osório, F.. 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/

[11] Pacut, Andrzej; Czajka, Adam. Recognition of Human Signatures. Proceedings IJCNN'01 - International Joint Conference on NN Vol.2 pp1560-1564. 2001.

[12] Sakamoto, D.; Morita, H.; Ohishi, T.; Komiya, Y.; Matsumoto, T. On-line Signature Verification Algorithm Incorporating Pen Position, Pen Pressure and Pen Inclination Trajectories. Proceedings of the IEEE International Conference on Acoustic, Speech and Signal Processing 2001. pp993-996 vol. 2.

[13] Jain, Anil K.; Griess, Friederike D.; Connell, Scott D. On-line signature verification. Pattern Recognition. Elsevier Press. 2002.

[14] Mitchell, Tom. Machine Learning, McGraw-Hill – Computer Science Series. Boston, MA. 1997.

[15] Cattell, Raymond. Factor Analysis. New York. Harper Books, 1952.