

# Uso de Combinação de Reservoir para Verificação de Assinaturas Manuscritas Off-line

Saulo Henrique L. de M. Nápoles, Cleber Zanchettin

<sup>1</sup>Centro de Informática – Universidade Federal de Pernambuco (UFPE)  
Av. Jornalista Anibal Fernandes, s/n - Cidade Universitária – Recife – PE – Brazil

{shlmn, cz}@cin.ufpe.br

**Abstract.** *The handwritten signature is present in all important documents. In law, if the signature on a document is false, this document is also considered a fraud. To automate the task of verification of signatures, many classifiers have been tested, often with few practical results promising. This work proposed uses a combination of Reservoir Computings for handwritten signature verification, for their recurrent characteristics and training facility. The experiments with this promising technique are performed in a public database used in the competition for ICDAR 2009 and their results compared to the competitors.*

**Resumo.** *A assinatura manuscrita é marca presente em todos os documentos importantes. Perante a lei, se a assinatura em um documento é falsa, esse documento também é considerado uma fraude. Para automatizar a tarefa de verificação de assinaturas, muitos classificadores já foram testados, muitas vezes com resultados práticos pouco promissores. Neste trabalho é proposta a utilização da combinação de Reservoir Computings para verificação de assinaturas manuscritas, devido as suas características recorrentes e facilidade de treinamento. Os experimentos com esta promissora técnica são realizados em uma base de dados pública utilizada na competição do ICDAR 2009 e seus resultados comparados aos dos competidores.*

## 1. Introdução

Ao longo da história os documentos e as assinaturas apostas neles sempre necessitaram da garantia de sua autenticidade. Na Idade Média, a documentação régia sempre vinha com o selo real garantindo sua autenticidade. No Sistema Jurídico Visigótico, o mais intelectualizado ramo do direito germânico, existia a confirmação do documento pelas testemunhas que o tocavam, assinavam e sobrescreviam. Os documentos privados eram, em ocasiões, confirmados por documentos reais [Freitas *et al* 2007].

A assinatura é marca presente em todos os documentos importantes, desde pagamentos em cheques ou cartões de crédito, processos judiciais, até contratos e compromissos de negócios dos mais variados. Em um documento, ela prova que o assinante está de acordo com o que está escrito anteriormente, portanto, a identificação e autenticação dos documentos digitais é um dos principais aspectos a serem considerados para garantir a segurança e autenticidade das suas informações, visto que o atual aumento das informações no mundo digital vem exigindo meios mais seguros para a proteção uma vez que, a falsidade documental e o estelionato, em todos seus aspectos, constituem crime e se a assinatura em um documento é falsa, este documento também é considerado inválido [Huang e Yan 1997].

Uma das maneiras de validar uma assinatura é utilizando Sistemas de Verificação que visa examinar a autenticidade da assinatura manuscrita através de métodos que possam discriminá-la de uma falsificação [Heinen e Osório 2004]. Estes sistemas podem examinar a assinatura de maneira *on-line* ou *off-line*. Na abordagem *on-line* é necessário um hardware específico, que pode ser uma mesa digitalizadora ou uma caneta sensível e um tablet, para o indivíduo assinar, sendo assim, características dinâmicas também são observadas como: velocidade, força, pressão. Na abordagem *off-line*, a assinatura é realizada em papel e posteriormente digitalizada para serem extraídas as características estáticas, e, em seguida, fazer a verificação semelhante à verificação de imagens [Sisodia e Anand 2009].

As falsificações são classificadas em três subconjuntos: aleatórias, simples e simuladas. A falsificação aleatória é normalmente uma amostra genuína de outro autor. A falsificação simples ocorre quando o falsificador conhece o nome do autor, mas não possui um exemplo da assinatura a qual ele planeja falsificar. Por fim, a falsificação simulada ocorre quando o falsificador possui um exemplo da assinatura e faz uma imitação da assinatura genuína [Gonçalves 2008].

A verificação de assinatura consiste em, a partir de um exemplar da assinatura, verificar se ela pertence ou não ao autor. Em outras palavras, se ela foi ou não grafada pelo suposto autor. Este tipo de verificação encontra duas dificuldades: as variações interpessoal e intrapessoal. A primeira ocorrência parte de que duas pessoas não possuem a mesma escrita, já o segundo considera que ninguém escreve duas vezes exatamente igual como pode-se observar na Figura 1 com duas assinaturas genuínas sobrepostas [Freitas *et al* 2007].



**Figura 1: Variação intrapessoal de assinaturas genuínas (extraído de [Freitas *et al* 2007])**

O objetivo desse trabalho é desenvolver uma técnica de classificação baseada na combinação de redes *Reservoir Computing* para verificação de assinaturas manuscritas *off-line* que ofereça bons resultados práticos utilizando uma base de dados reais e pública. O restante do material se organiza da seguinte maneira: na seção 2 é realizado um levantamento bibliográfico dos sistemas de verificação de assinatura e classificadores relacionados com este trabalho. Na seção 3 é descrito como o modelo de classificação, baseado em *Reservoir*, foi construído e são apresentadas as características dos experimentos realizados. Na seção 4 são apresentados os resultados dos experimentos e uma discussão sobre os mesmos. Por fim, as conclusões e as indicações de trabalhos futuros são apresentadas na seção 5.

## **2. Trabalhos Relacionados**

Um número considerável de trabalhos relacionados com a verificação de assinaturas *off-line* vem sendo realizados recentemente [Batista *et al* 2007] [Impedovo e Pirlo 2008] [Dimauro ET AL 2004] [Prakash e Guru 2009] [Shankar e Rajagopalan 2007] [Justino *et al* 2005]. Conforme esses estudos, o primeiro trabalho na área de verificação de assinaturas *off-line* fazendo uso de sistemas conexionistas foi proposto por Mighell *et*

al. (1989), utilizando 80 assinaturas genuínas e 66 falsificações simuladas produzidas por um mesmo indivíduo.

Atualmente os trabalhos que envolvem Sistema de Verificação de Assinaturas utilizam como características para discriminação das assinaturas a área da imagem, altura e largura, razão do tamanho, características de direção, orientação e inclinação, contornos, texturas [Dimauro *et al* 2004]. Também podem ser usados dados simbólicos como proporção contínua, intervalo discreto ou multivalorado, multivalorado com tamanho, quantitativos, categóricos, etc [Prakash e Guru 2009].

Os classificadores mais utilizados na verificação são Redes Neurais Artificiais [Bajal e Chaudhary 1997], Dynamic Time Warping (DTW) [Shankar e Rajagopalan 2007], Cadeias Escondidas de Markov (HMM) e Máquinas de Vetor de Suporte (SVM) [Justino *et al* 2005]. Algumas abordagens utilizam uma combinação dessas técnicas formando um novo método híbrido. Pode ser utilizado um Algoritmo Genético para escolha das características a serem utilizadas numa rede neural [Xuhua *et al* 1997], combinação de SVMs utilizando Algoritmo Genético [Bertolini *et al* 2010], entre outras formas e obtêm resultados satisfatórios.

As redes neurais *feed-forward* são muito utilizadas em problemas não temporais, porém para problemas temporais, como previsão do tempo e financeiro, sistemas de identificação, sistemas de visão e fala, é necessário acrescentar conexões recorrentes para obter resultados melhores. Desta forma, uma assinatura manuscrita também pode ser considerada um padrão temporal, principalmente em sistemas de verificação *on-line*. Em sistemas de verificação *off-line*, várias destas características temporais estão presentes, como variações de traços, posição de escrita e linha, e principalmente a variação da assinatura de um mesmo assinante com o passar do tempo.

Em contrapartida às vantagens dos classificadores que trabalham estas características, ao acrescentar essas conexões recorrentes, o treinamento da rede se torna mais difícil, pois o classificador é transformado num sistema dinâmico bastante complexo [Holzmann 2009]. Para minimizar essa complexidade, três estudos independentes propuseram uma solução que tinha muito em comum: *Liquid State Machine* [Maass *et al* 2002], *Echo State Machine* [Jaeger e Haas 2004] e *Backpropagation Decorrelation* (BPDC) [Steil 2004]. Cada uma dessas técnicas propostas busca evitar o problema da formação de uma rede neural recorrente enquanto continuam a ser capazes de usar sua poderosa capacidade de processamento temporal. O *Reservoir Computing* utiliza a rede como um reservatório, cujos pesos não são alterados no treinamento e são escolhidos de forma espaça e aleatória. A resposta do reservatório é observada a partir da camada de saída por uma classificação simples utilizando uma função de avaliação linear [Schrauwen *et at* 2007].

Esta abordagem combina convenientemente a memória de curto prazo do reservatório com a facilidade do treinamento e da rápida convergência de uma função simples e linear. O reservatório funciona como um complexo *kernel* que filtra e calcula as combinações aleatórias das entradas atuais e passadas, com uma memória finita. A camada de saída, então, é capaz de combinar linearmente a informação do *Reservoir* com a saída [Embretchts 2009]. O modelo do *Reservoir* pode ser vista na Figura 2. A circunferência no centro representa o *Reservoir*, na qual os pesos entre suas conexões são inseridos aleatoriamente. O retângulo representa a camada de saída. A saída do *Reservoir* é função da entrada, do bias, do próprio *Reservoir* e da camada de saída como

pode ser visto na Equação (1). A resposta da camada de saída é dada pelo somatório da atualização do *Reservoir*, da camada de entrada, da própria camada de saída e do bias, como pode ser observado na Equação (2). Dessa forma, por ter poucos parâmetros para serem otimizados, não usar gradiente descendente, a atualização dos pesos não acontecer em toda a rede, o *Reservoir Computing* apresenta uma redução no tempo e garantia de convergência da rede, além de um controle maior em outras propriedades como: raio espectral, dispersão, conexões, diferentemente das redes neurais recorrentes.

$$(1) \quad x(t + 1) = f(W_{res}^{res} x(t) + W_{inp}^{res} u(t) + W_{out}^{res} y(t) + W_{bias}^{res})$$

$$(2) \quad \hat{y}(t + 1) = W_{res}^{out} x(t) + W_{inp}^{out} u(t) + W_{out}^{out} y(t) + W_{bias}^{out}$$

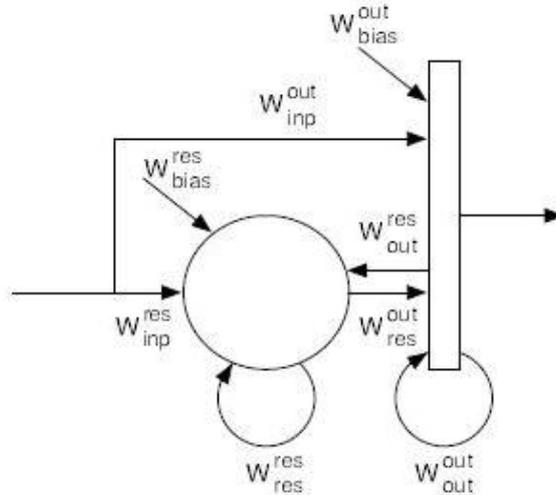


Figura 2. Topologia do *Reservoir Computing* (adaptado de [Schrauwen *et al* 2007])

### 3. Método Proposto

O modelo proposto neste trabalho é uma combinação de *Reservoirs Computing*. A idéia é combinar as saídas de vários classificadores com base *Reservoir* e diminuir as chances de um classificador isolado fazer uma escolha errada, em nosso caso, uma validação de uma assinatura falsa. Porém, combinar as saídas de classificadores só é útil quando estes classificadores produzem saídas distintas [Kuncheva 2004]. Apesar do método proposto utilizar diferentes instâncias do mesmo classificador, pelo fato do *Reservoir Computing* apresentar um caráter randômico nas suas ligações, é esperado que eles apresentem saídas diferentes ou que representem diferentes pontos da superfície de resposta do problema [Verstraeten *et al* 2006]. A combinação das saídas dos classificadores utilizada neste trabalho é bem simples, realizada através do voto majoritário, sendo escolhida como saída final, a resposta que mais apareceu individualmente nos classificadores *Reservoir* isolados.

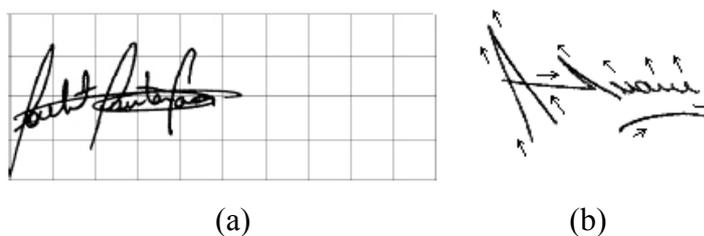
A base de dados utilizada nos experimentos foi a mesma utilizada na competição de verificação de assinaturas *off-line* do *International Conference on Document Analysis and Recognition (ICDAR) 2009*. O ICDAR é uma conferência internacional para pesquisadores e profissionais da área de reconhecimento de documentos que

acontece bienalmente. Esta conferência objetiva a identificação, o incentivo e a troca de ideias sobre o estado da arte na análise de documentos, compreensão, recuperação e avaliação de desempenho, incluindo várias formas de documentos multimídia [ICDAR 2011]. Paralela as atividades da conferência, existem várias competições, dentre as quais a competição de verificação de assinaturas *on-line e off-line*. No ano de 2009, participaram desta competição 8 equipes de pesquisadores da Espanha, França, Alemanha e Estados Unidos.

A base de dados disponibilizada na competição de 2009 é composta por 1.920 imagens sendo 60 assinaturas genuínas de 12 escritores e 1.860 falsificações do tipo simuladas, sendo 31 escritores falsos e 5 falsificações para cada assinatura genuína. As imagens foram segmentadas, visualmente inspecionadas e, em seguida, pré-processadas em tons de cinza e binarizadas (limiarizadas) com 300 e 600 dpi [Blankers 2010].

Para a extração das características das imagens foi construído um grid 4x10 na imagem, subdividindo a imagem da assinatura em 40 sub-imagens (Figura 3a). Destas sub-imagens foram extraídas as densidade dos pixels que é a relação entre a quantidade total de pixels sobre os pixels de assinatura. De acordo com os estudos de Justino (2001) esta característica incorpora um descritor estático, o qual propicia uma insensibilidade às variações intrapessoais.

Também foi extraída a inclinação axial de cada sub-imagem, pois esta característica descreve aspectos dinâmicos do traçado da assinatura. Esta tarefa realiza uma análise local sobre os segmentos mais significativos, extraíndo a direção através do segmento que produziu a máxima projeção. Cada segmento é representado segundo o *chain-code* com 8-vizinhos. Pode-se observar exemplos de inclinações axiais na Figura 3b. Desta forma, o algoritmo de extração de características se utiliza de características estáticas e características que descrevem o aspecto dinâmico da assinatura.



**Figura 3: (a) grid 4x10 subdividindo a imagem (b) Exemplo de inclinações axiais**

O método de classificação proposto utiliza 6 classificadores do tipo *Reservoir Computing*. A primeira camada possui 40 nodos correspondentes às características extraídas das assinaturas, onde cada nó de entrada recebe um par que representam as duas informações. A segunda camada é o bias, que é utilizado para aumentar o grau de liberdade, permitindo uma melhor adaptação do aprendizado. A terceira camada, o reservatório propriamente dito, tem tamanho fixo e é composto por 300 nós inseridos e conectados aleatoriamente. Foram feitos alguns testes iniciais para determinar o número de nós e este número foi escolhido por apresentar um melhor resultado no menor espaço de tempo entre 150, 200, 250, 350, 400, 450 e 500. Esta camada é treinada de forma *off-line* e utiliza como função de ativação a tangente hiperbólica por ser considerada a melhor função dentre as utilizadas na literatura.

No treinamento dos *Reservoir Computing* e análise dos resultados foi utilizada a validação cruzada. Na validação cruzada, os dados empregados na etapa do treinamento não são utilizados na etapa de teste. Neste procedimento foi realizada a paginação em 5 *folds*, onde os dados são divididos em 5 subconjuntos, nos quais é realizado o treinamento com cada subconjunto e o teste feito com os dados restantes. Ao final das execuções, a taxa de erro global é calculada pela média dos 5 desempenhos obtidos com cada subconjunto.

#### 4. Resultados e Discussão

A análise do desempenho do método proposto foi realizada de forma análoga a realizada na competição ICDAR 2009, que é baseada apenas na taxa de erro global computado a partir da base de dados testada.

Após executar o algoritmo 60 vezes, devido às características estocásticas do modelo, observou-se que a média da taxa de erro foi de 13,47% e desvio padrão de 1,63. A taxa de erro de cada execução pode ser observada na Figura 4, na qual o eixo horizontal indica o número da execução do algoritmo e o eixo vertical a taxa de erro naquele instante. Comparado estes resultados com os resultados dos algoritmos que competiram no ICDAR 2009, a combinação de *Reservoir* proposta perdeu em desempenho apenas para o algoritmo do *Centre de Morphologie Mathématique* que obteve uma taxa de erro médio de 9,15%. O desempenho dos competidores e do método proposto no trabalho pode ser observado na Tabela 1 que está ordenada pela taxa de erro médio. É importante observar que apenas a comparação entre as taxas de erro não é uma boa estatística paramétrica para comparar o desempenho de classificadores. É importante destacar também que apesar deste trabalho seguir todos os procedimentos destacados na competição ICDAR 2009, os resultados não podem ser comparados diretamente (ou pelo menos as análises precisam considerar), pois foram desenvolvidos em ambientes diferentes. Para tentar minimizar esta dificuldade foi realizado um teste de hipóteses com variância desconhecida utilizando a distribuição *t-Student*.

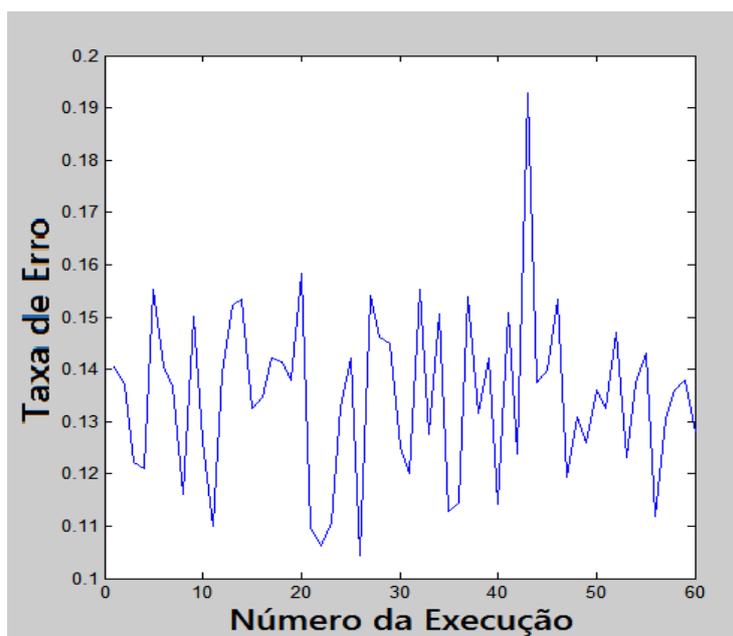


Figura 4. Taxa de erro médio no teste

**Tabela 1. Taxa de Erro Médio dos competidores**

<b>Instituto de Pesquisa</b>	<b>País</b>	<b>Taxa de Erro (%)</b>
Centre de Morphologie Mathématique	França	9,15
<b>Comitê de Reservoir (CIN-UFPE)</b>	<b>Brasil</b>	<b>13,47</b>
German Research Center for Artificial Intelligence	Alemanha	15,92
Biometric Recognition Group - ATVS	Espanha	18,27
Center of Excellence for Document Analysis and Recognition (CEDAR)	EUA	23,00
Computer Vision Center	Espanha	41,12

Para realizar o teste de hipótese de cada resultado dos competidores e o algoritmo desenvolvido, iremos adotar a hipótese nula  $H_0$  como sendo  $\mu_0 = \mu$  e a hipótese alternativa  $H_1$  como sendo  $\mu_0 < \mu$  onde  $\mu$  é a média do competidor, e  $\mu_0$  a média do algoritmo proposto. Foi observada a distribuição com nível de significância de 99%. O resultado pode ser conferido na Tabela 2, que confirma apenas o algoritmo francês como sendo melhor do que o algoritmo proposto.

Porém, por não se ter encontrado referência aos métodos dos competidores, fica difícil fazer mais comparações entre as técnicas confrontadas. Não se pode dizer qual técnica é melhor para ser utilizada com verificação de assinaturas, pois não foram encontradas informações de como os métodos foram construídos para esta competição ou que tenham utilizados esta mesma base de dados, isso dificulta a agregação de melhorias nas técnicas atuais porque não se sabe onde um algoritmo foi melhor do que o outro e poder juntar essas duas técnicas em apenas uma que tenha um desempenho superior as demais.

Esta dificuldade em encontrar referências formais às técnicas se deve ao fato da maioria delas serem soluções estratégicas, com aplicações comerciais. Desta forma a maioria das instituições mantém em segredo como são constituídos seus classificadores para verificação de assinaturas.

**Tabela 2. Resultado dos Testes de hipóteses**

<b>Instituto</b>	<b>País</b>	<b>Erro Médio</b>	<b><math>t_{cal}</math></b>	<b>Resultado</b>
<b>C. de Morphologie Mathématique</b>	<b>França</b>	<b>9,15</b>	<b>9,81</b>	<b>Não Rejeita <math>H_0</math></b>
German Research Center for A.I.	Alemanha	15,92	-5,21	Rejeita $H_0$
ATVS	Espanha	18,27	-10,21	Rejeita $H_0$
CEDAR	EUA	23,00	-35,46	Rejeita $H_0$
Computer Vision Center	Espanha	41,12	-74,02	Rejeita $H_0$

## 5. Conclusões e Trabalhos Futuros

Neste trabalho foi desenvolvida uma técnica conexionista, baseada em *Reservoir Computing*, para verificação de assinaturas manuscritas *off-line*, que se mostrou promissora quando comparada com diferentes técnicas de classificação de assinaturas utilizadas na atualidade. O *Reservoir Computing* usa do recurso de conexões recorrentes, sem se tornar um sistema complexo, podendo ser utilizado em problemas de difícil resolução com abordagens clássicas.

Na avaliação do modelo, foi usada uma base de imagens de assinatura pública adotada na competição de verificação de assinaturas da ICDAR 2009. As imagens foram subdivididas com um *grid* 4x10 e a partir de cada um desses, foram extraídas as características densidade de pixels e inclinação de axiomas, que denotam peculiaridades estáticas e dinâmicas da assinatura. Em seguida foi submetido aos classificadores, utilizando validação cruzada com *5-fold*. As saídas dos classificadores eram combinadas em uma única a partir do voto majoritário.

A medida de desempenho utilizada foi a taxa média de erro, que também foi usada na competição ICDAR 2009. Comparado com os demais competidores, o algoritmo proposto obteve um ótimo desempenho, perdeu apenas para um método, e o teste de hipótese realizado com os resultados dos experimentos ratifica essa conclusão.

A partir dos resultados dos experimentos realizados pode ser verificada a capacidade desta nova rede neural artificial e sua aplicabilidade no sistema de verificação de assinaturas manuscritas *off-line*, que também pode ser estendido para outros problemas, como de previsão por exemplo, devido a existência das mesmas características temporais, existente no problema abordado.

Entretanto, melhorias podem ser realizadas para que o método proposto tenha um desempenho ainda melhor, tais como: (i) mesclar com outras técnicas de classificação ou adicionar um procedimento para explorar a topologia da rede, (ii) incluir mais classificadores no comitê desenvolvido; (iii) utilizar uma regra de combinação diferente, com o tamanho do reservatório variável; (iv) pode também ser adicionado um *grid* que gere um maior número de sub-imagens e até mesmo outras características da assinatura ou acrescentar novas baseadas nos exames grafotécnicos.. Inserir, mesclar ou modificar a combinação dos classificadores pode melhorar o desempenho visto que outros pontos do espaço de soluções podem ser explorados. Modificar o *grid* e/ou aumentar o número de características exploradas facilitará na discriminação observada entre assinaturas genuínas e falsificações.

Outro trabalho futuro a ser investigado é utilizar uma base de dados com a presença de dados simbólicos, além dos dados que já são utilizados tradicionalmente para obter mais informações sobre as assinaturas.

## Agradecimentos

Este trabalho recebeu apoio financeiro da Fundação de Amparo à Ciência e Tecnologia do Estado de Pernambuco (FACEPE).

## Referências

Freitas, C. O. A., Justino, E. J. R., Oliveira, L. E. S. (2007) “Reconhecimento de firmas por semelhança no Brasil”. In: *Âmbito Jurídico*, Rio Grande, v 40, Disponível em

[http://www.ambito-juridico.com.br/site/index.php?n\\_link=revista\\_artigos\\_leitura&artigo\\_id=3895](http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=3895).  
Acesso em 07/04/2011.

- Huang K. e Yan, Hong. (1997) “Off-line Signature Verification based on Geometric Feature Extration and Neural Network Classification”. *Pattern Recognition*, Vol 30, No. 1, pp. 9-17.
- Heinen, M. R., Osorio, F. S. (2004) “Biometria Comportamental: Pesquisa e desenvolvimento de um sistema de autenticação de usuários utilizando assinaturas manuscritas”. *INFOCOMP (UFLA. Impresso) Lavras, MG, Brasil*, v. 3, n. 2, p. 31-37, 2004.
- Sisodia, K. e Anand, M. (2009) “Off-line Handwritten Signature Verification using Artificial Neural Network Classifier”. *International Journal of Recent Trends in Engineering*, Vol 2, no. 2, Novembro.
- Gonçalves, D. B. (2008) “Agrupamento de Classificadores na Verificação de Assinaturas *off-line*”. Setembro de 2008.86p. Dissertação (Mestrado em Informática) – Programa de Pós-Graduação em Informática, Pontifícia Universidade Católica do Paraná, Curitiba.
- Batista, L., Rivard, D., Sabourin, R., Granger, E., Maupin, P. (2007) “State Of The Art In Off-Line Signature Verification”. *Pattern Recognition Technologies and Applications: Recent Advances*.
- Impedovo, D. e Pirlo, G. (2008) “Automatic Signature Verification: The State of the Art”. *IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, Vol 38, pp. 609–635.
- Mighell, D. A., Wilkinson, T. S., Goodman, J. W. (1989) “Backpropagation and Its Application to Handwritten Signature Verification”. *Advances in Neural Information Processing Systems 1*, pp. 340–347.
- Dimauro, G., Impedovo, S., Lucchese, M. G., Modugno, R., Pirlo, G. (2004) “Recent Advancement in Automatic Signature Verification”. *Proceedings of 9<sup>th</sup> International Workshop on Frontiers in Handwriting Recognition (IWFHR)*, pp. 179-184. Tóquio, Japão
- Prakash, H. N. e Guru, D. S. (2009) “Relative Orientations of Geometrics Centroids for Off-line Signature Verification”. *International Conference on Advanced Pattern Recognition (ICAPR-2009)*, ISI, Kolkata, India pp. 201-204.
- Bajaj, R. e Chaudhary, S. (1997) “Signature Verification using mutiple neural classifiers”. *Pattern Recognition*, Vol 30, pp. 1-87.
- Shankar, A. P. e Rajagopalan (2007) “Off-line Signature Verification using DWT”. *Pattern Recognition Letters*, Vol 28, PP. 1407-1414.
- Justino, E. J. R. Bortolazzi, F. e Sabourin, R. (2005) “A Comparasion of SVM and HMM classifiers in the Off-line Signature Verification”. *Pattern Recognition Letters*, Vol 26, Issue 9, pp. 1377-1385.
- Xuhua, Y., Furuhashi, T., Obata, K., Uchikawa, Y. (1997) “Selection of Features for Signature Verification Using the Genetic Algorithm”. *Computers & Industrial Engineering* Vol. 30, No. 4, pp. 1037-1045.

- Bertolini, D., Oliveira, L. S., Justino, E., Sabourin, R. (2010) "Reducing Forgeries in Writer-independent Off-line Signature Verification Through Ensemble of Classifier". *Pattern Recognition*, Vol 43, pp. 387-396.
- Holzmann G. (2009) "Reservoir Computing: A Powerful Black-Box Framework for Nonlinear Audio Processing". *Proceedings of the 12<sup>th</sup> International Conference on Digital Audio Effects (DAFx-09)*, Como, Italy, 2009.
- W. Maass, T. Natschläger, and H. Markram. (2002) "Realtime computing without stable states: A new framework for neural computation based on perturbations". *Neural Computation*, Vol 14 No.11 pp.2531–2560.
- H. Jaeger and H. Haas. (2004) "Harnessing nonlinearity: predicting chaotic systems and saving energy in wireless telecommunication". *Science*, No. 308 pp. 78–80.
- J. J. Steil. (2004) "Backpropagation-Decorrelation: Online recurrent learning with  $O(N)$  complexity." In *Proceedings of International Joint Conference on Neural Network 2004 Budapest Hungria*, volume 1, pp 843–848.
- Schrauwen, B. Verstraeten, D. Campenhout, J. V.(2007) "An overview of reservoir computing: theory, applications and implementations". *Proceedings of the 15<sup>th</sup> European Symposium on Artificial Neural Networks (2007)* pp. 471-482. Bruges, Bélgica.
- Embrechts, M. J. Alexandre, L.A. Linton, J. D. (2009) "Reservoir computing for static pattern recognition". *17<sup>th</sup> European Symposium on Artificial Neural Networks - ESANN 2009*, Bruges, Bélgica. pp 245-250.
- Kuncheva, L. (2004) "Combining Pattern Classifier, Methods and Algorithms" Wiley, New York.
- Verstraeten, D. Schrauwen, B. D'Haene, M. Stroobandt, D. (2006) "The unified Reservoir Computing concept and its digital hardware implementations". *Proceedings of the 2006 EPFL LATSIS Symposium*. Lausanne, Suíça
- Blankers V.L., Heuvel C.E. van den., Franke K.Y., Vuurpijl L.G.(2010) "The ICDAR 2009 Signature Verification Competition". *10th International Conference on Document Analysis and Recognition*. Barcelona, Espanha
- Justino, E. J. R., Bortolozzi, F., and Sabourin, R. (2001) "Offline signature verification using hmm for random" In *ICDAR 2001, International Conference on Document Analysis and Recognition*, pp. 1031–1034.