v.13, n.1, p.129-139, jan.-abr. 2006

FCONTROL®: SISTEMA INTELIGENTE INOVADOR PARA DETECÇÃO DE FRAUDES EM OPERAÇÕES DE COMÉRCIO ELETRÔNICO

Leandro dos Santos Coelho

Grupo Produtrônica, Laboratório de Automação e Sistemas,
Programa de Pós-Graduação em Engenharia de Produção e Sistemas,
CCET/PPGEPS, Pontifícia Universidade Católica do Paraná,
Rua Imaculada Conceição, 1155, CEP 80215-901, Curitiba, PR, Brasil,
e-mail: leandro.coelho@pucpr.br

Roberto Tadeu Raittz

Curso Tecnólogo em Informática, Universidade Federal do Paraná,
Rua Dr. Alcides Vieira Arcoverde, 1225, CEP 81520-260, Curitiba, PR, Brasil,
e-mail: raittz@ufpr.br

Maurício Trezub

CIASHOP E-Commerce, http://www.ciashop.com.br,
Rua Alferes Ângelo Sampaio, 301, CEP 80250-120, Curitiba, PR, Brasil,
e-mail: trezub@ciashop.com.br

Recebido em 13/6/2005
Aceito em 14/2/2006

Resumo

A prevenção de fraude em cartão de crédito é uma importante aplicação comercial para aplicação de abordagens de métodos de previsão e inteligência computacional. A inteligência computacional é uma associação de metodologias bio-inspiradas que incluem, como principais membros, as redes neurais, sistemas nebulosos, computação evolutiva, inteligência coletiva e computação probabilística. Recentemente, a aplicação de técnicas da inteligência computacional no suporte de tarefas de serviço, tais como detecção e identificação de anomalia, classificação de padrão, diagnóstico, prognóstico, estimação e controle, tem emergido nos ambientes industrial e comercial. Este artigo apresenta um sistema computacional eficiente baseado em metodologias da inteligência computacional para detecção de fraude em operações reais de dados de cartão de crédito em transações de comércio eletrônico. O novo método proposto é denominado FControl® de detecção de fraude e classificação integra conceitos de sistemas inteligentes híbridos baseado em abordagens de redes neurais, sistemas nebulosos e computação evolutiva. O método proposto gera soluções de qualidade em termos de eficiência e sucesso de previsão. O programa computacional do FControl® está atualmente instalado em um Intel Pentium IV 2.4 MHz (bi-processador e RAM de 4 Gbytes) na companhia Ciashop E-Commerce e está correntemente em uso para detecção de fraude para 250 companhias com serviços de comércio eletrônico.

Palavras-chave: tecnologia da informação, comércio eletrônico, inteligência computacional, detecção de fraude, cartão de crédito, sistemas neuro-nebulosos, computação evolutiva.

1. Introdução

Em sistemas tecnológicos, atividades fraudulentas têm ocorrido em diversas áreas, tais como redes de comunicação, comunicação móvel, *banking on-line* e comércio eletrônico. As fraudes estão crescendo de forma acentuada com a expansão da tecnologia moderna e comunicação global, resultando em perdas substanciais em negócios (Kou et al., 2004). As fraudes virtuais fizeram com que comerciantes perdessem, em 2004, US$ 2,6 bilhões. O montante representa 1,8% do total das vendas e, além de pagamentos fraudulentos, está relacionado ao medo que os internautas têm de realizar transações *on-line*. Em 2000, as perdas foram de US$ 1,5 bilhão, em 2001 chegaram a US$ 1,7 bilhão e, em 2002, US$ 2,1 bilhões. Em 2003, houve uma melhora no cenário, e as perdas caíram para US$ 1,9 bilhão (Folha On line, 2005). Vários trabalhos da literatura têm reportado a preocupação de empresários com o crescimento de fraudes em operações de comércio eletrônico, a citar Donnely (2000) e Network Security (2000).

Neste contexto, a fraude com cartão de crédito é um desafio para lojistas virtuais. As fraudes em negócios realizados na Internet são proporcionalmente mais freqüentes que as fraudes em estabelecimentos físicos e causam um maior prejuízo direto.

As transações com cartão de crédito através da Internet são consideradas pelos bancos e administradoras como CNP (Cartão Não Presente). Como não há a assinatura do comprador para validar a compra neste tipo de transação, a responsabilidade pela transação é do lojista e não do banco emissor ou da administradora do cartão. As fraudes com cartão de crédito podem ocasionar prejuízos para o comerciante bem como podem levar ao cancelamento do convênio do estabelecimento com as administradoras de cartão (FControl, 2005).

Os custos com fraudes para o estabelecimento incluem: i) perda de mercadorias; ii) perda com taxas bancárias, frete e embalagem; iii) risco de cancelamento do contrato com as administradoras dos cartões; iv) taxa de desconto maior no contrato com as administradoras; v) perda de faturamento pela rejeição de pedidos; vi) custo elevado de uma equipe de análise de risco; vii) perda de confiança do cliente; e viii) perda do cliente por insatisfação (demora e incômodo).

Os custos financeiros diretos ocorrem quando há *chargeback*. Os *chargebacks* ocorrem quando um portador de cartão de crédito não reconhece um débito em seu cartão. O indivíduo então entra em contato com o banco emissor do cartão dizendo não ter autorizado o débito. O banco emissor então cancela o crédito do estabelecimento comercial ou ainda efetua um débito na conta do estabelecimento (FControl, 2005).

Paradoxalmente, o risco da compra pela Internet é todo do lojista virtual, e nunca do comprador. Mesmo que venha a ser realizada uma compra fraudulenta com cartão clonado ou roubado, o legítimo dono do cartão sempre pode não reconhecer o débito e simplesmente se recusar a pagar (não há assinatura autorizando o débito).

Em face desse cenário, o lojista virtual tem um desafio. Os estabelecimentos precisam, a cada transação, usar métodos para autenticar o comprador, ou seja, responder com a maior precisão e rapidez possível às perguntas: "Esse comprador é mesmo quem ele diz ser? O cartão que está sendo utilizado nessa compra é legítimo?".

Conseqüentemente, nota-se que o desenvolvimento de tecnologias para a detecção de fraudes é uma importante abordagem a ser explorada pelas empresas vinculadas a operações de comércio eletrônico. A detecção de fraudes envolve a identificação e classificação das fraudes, de preferência o mais rapidamente possível. O desenvolvimento de novos métodos computacionais para a detecção e diagnóstico de fraudes em operações de comércio eletrônico é uma área de estudos recentes. A maioria dos trabalhos publicados nesta área na literatura está relacionada à detecção de fraudes em operações com cartão de crédito, mas sem uso de comércio eletrônico, usando principalmente sistemas especialistas, redes neurais artificiais, raciocínio baseado em casos e mineração de dados (*data mining*) (Ghosh e Reilly, 1994; Hanagandi et al., 1996; Aleskerov et al., 1997; Sorronsoro et al., 1997; Richardson, 1997; Chan et al., 1999; Liu e Yao, 1999; Brause et al., 1999; Chi et al., 2000; Wheeler e Aitken, 2000; Syeda et al., 2002).

Neste artigo, a principal contribuição é o projeto do sistema FControl®, da CIASHOP E-Commerce, para detecção de fraudes em operações de comércio eletrônico. O FControl® utiliza uma abordagem híbrida de inteligência computacional baseada em sistema neuro-nebuloso (Raittz, 2002; Raittz et al., 1998) e otimização (busca local), usando uma estratégia evolutiva com mecanismos de auto-adaptação de parâmetros (Hansen e Ostermeier, 1996; Ostermeier e Hansen, 1999).

O objetivo deste artigo é apresentar um apanhado das metodologias de inteligência artificial (redes neurais artificiais, sistemas nebulosos, computação evolutiva e sistemas especialistas) na concepção do sistema FControl®, para detectar tentativas de fraude nas transações com cartão de crédito de forma rápida e eficiente.

O artigo é organizado da seguinte forma. Na seção 2, são apresentadas características, aspectos operacionais e módulos computacionais inteligentes do FControl®. A descrição da abordagem neuro-nebulosa e a otimização evolutiva são apresentadas na seção 3. Na seção 4, é descrito o problema de classificação vinculado à detecção de fraudes em operações de cartão de crédito para comércio eletrônico e uma análise dos resultados experimentais. A conclusão do trabalho é comentada na seção 5.

2. Descrição de sistemas de detecção de fraudes e a tecnologia do FControl®

A seguir são apresentadas as características dos sistemas convencionais de detecção de fraudes e as características do **FControl®**.

2.1 Sistemas convencionais

No mundo todo, o método mais utilizado para verificar a autenticidade dos pedidos é a revisão manual dos pedidos, com as seguintes etapas mais comuns:

- Análise das informações do pedido, com o objetivo de identificar desvios de padrões e com isso tentar classificar o risco;
- Separação dos pedidos para revisão de forma manual ou por sistema de regras;
- Checagem manual de informações em bancos de dados comerciais externos;

- Verificação de listas negras geradas no próprio estabelecimento; e
- Contato direto com o cliente, com a solicitação de confirmação de informações e cópia de documentos.

Além disso, os bancos e as administradoras de cartão de crédito têm utilizado várias técnicas no intuito de diminuir o índice de fraudes. Tais técnicas e sistemas incluem *Address Verification System* (*AVS*), *Credit Card Security Code* (CVV2) e mais recentemente sistemas de autenticação de transações, tal como o *Verified by VISA*. Embora todos os métodos de prevenção ajudem no combate à fraude, eles possuem vários problemas:

- Ineficientes na detecção de fraudes;
- Causam rejeição de pedidos válidos;
- Invadem a privacidade do consumidor;
- Gastam valioso tempo da equipe de análise de fraudes;
- Podem interferir no fechamento dos pedidos; e
- Causam atraso na entrega dos pedidos.

2.2 Sistema FControl®

A proposta do sistema **FControl®** é possibilitar ao lojista virtual: i) vender mais, aceitando mais pedidos (confiança); ii) automatizar o processo de revisão de pedidos de risco; iv) aumentar a produtividade de seus funcionários; e v) programar regras específicas para seu negócio.

O FControl® é uma abordagem de solução eficiente e rápida para detectar tentativas de fraude nas transações com cartão de crédito. Neste sistema, os dados sobre a compra e o comprador são passados ao sistema FControl® na forma de consulta. Neste caso, cerca de 36 características distintas e outros 124 elementos de informação são analisados com o objetivo de aceitar, rejeitar ou submeter à revisão de eventuais pedidos de risco. O FControl® utiliza-se de inteligência artificial para fornecer ao comerciante uma pontuação de risco de fraude. Dentre os fatores analisados pelo FControl® estão a consistência geográfica, periodicidade (freqüência entre compras), padrões de fraude conhecidos, comportamento típico de compradores e padrões típicos de transações do estabelecimento. Um dos aspectos mais poderosos do modelo FControl® é a capacidade de realizar cruzamento de informações entre todos os seus clientes. As consultas ao sistema FControl® são realizadas automaticamente para todas as transações com cartão de crédito, de forma que o administrador dos pedidos tenha sempre em mãos a informação necessária para sua tomada de decisão. As consultas podem ser feitas ainda manualmente por formulário na Internet (FControl, 2005).

O principal elemento do FControl® é um sistema de análise sofisticado que utiliza inteligência artificial para detecção de características e padrões de fraude. Baseado na pontuação fornecida pela detecção, é possível definir regras para automatizar a aceitação, rejeição ou revisão de cada pedido analisado. Além da rede neural artificial aliada a sistemas nebulosos e otimização por meio de computação evolutiva, o FControl® incorpora outras tecnologias, tais como sistema especialista, lista negra, lista branca, regras de negócio customizáveis e travas de segurança, tudo para garantir sua confiança na venda via Internet.

Neste aspecto, o FControl® possui os seguintes módulos tecnológicos:

i) **rede neuro-nebulosa e pontuação de risco**: As redes neurais permitem ao FControl® se adaptar rapidamente a novos padrões de fraude e permite um retorno imediato. Analisando vários elementos de informação sobre a transação, o sistema retorna um índice de risco de 0 a 1000;

ii) **lista branca / negra**: Quando um pedido é consultado pelo FControl®, o pedido é verificado em uma lista negra, composta por todas as denúncias de todas as lojas virtuais participantes do consórcio FControl®, aumentando exponencialmente o poder de detecção de fraudes e evitando que um mesmo fraudador cause prejuízos a vários estabelecimentos. O sistema conta também com uma lista branca de clientes que já foram checados pelo FControl® e cujos pedidos podem ser prontamente aprovados, pela análise de comportamento histórico;

iii) **regras de negócio**: O FControl® disponibiliza aos administradores um método para definir, testar e aplicar regras para prevenção de fraudes que se enquadram nas políticas de venda dos produtos da empresa, permitindo então o ajuste fino dos níveis de aceitação da empresa. Isso é especialmente útil na definição do número total de pedidos separados para uma análise mais detalhada, considerando fatores como índice de risco aceitável e o custo da equipe de revisão;

iv) **travas de segurança**: As travas de segurança são monitores que automaticamente detectam as atividades suspeitas na utilização de dados, tais como telefone, CEP, endereço, endereço de IP e denunciam as transações fraudulentas;

v) **sistema especialista**: O sistema especialista substitui a necessidade de um humano na análise dos pedidos, liberando seus funcionários para outras atividades. O sistema especialista gerencia as tecnologias acima para orientar as decisões sobre rejeição, aceitação ou revisão dos pedidos; e

vi) **módulo de gerenciamento de pedidos de risco**: O FControl® possui uma interface de administração de fraudes integrada que permite que funcionários gerenciem os pedidos de risco e tomem decisões rapidamente. Utilizando o módulo de gerenciamento de pedidos de risco, os pedidos são aceitos, rejeitados

ou submetidos à revisão de acordo com os índices de risco e as regras definidas para o seu negócio. Este módulo do sistema fornece as seguintes informações no auxílio à tomada de decisão de pedidos de risco:

- Resumo dos dados da compra;
- Escore de risco da transação;
- Justificativas precisas para o escore de risco;
- Padrões de compra do cliente;
- Regras de negócio infringidas;
- Sugestões de procedimentos de segurança;
- Envio automático de e-mail solicitando documentos para pedidos de risco elevado; e
- Acompanhamento do recebimento de documentos.

3. Inteligência computacional

O desenvolvimento da tecnologia de processamento de informação e a inteligência computacional constituem uma solução alternativa para problemas que necessitam aspectos relativos à incorporação de características inspiradas na natureza e na inteligência humana em problemas complexos, a exemplo de previsão do comportamento de sistemas dinâmicos.

Estes sistemas de previsão, ditos "inteligentes", tentam imitar a maneira de tomada de decisão humana e a representação de conhecimento, motivando a atenção crescente de pesquisadores de diversas áreas. Entre as vantagens potenciais oferecidas por estas técnicas, em relação aos esquemas convencionais de previsão linear, pode-se ressaltar: i) menor dependência de modelos quantitativos (vantagem dos sistemas nebulosos); ii) algoritmos estruturados de maneira simples para a tomada de decisões; iii) capacidade de aprendizagem; e iv) maior grau de autonomia.

Os sistemas de previsão, baseados em algoritmos da inteligência computacional, têm a habilidade de aprendizado, raciocínio e tomada de decisão. Todavia, os sistemas convencionais de previsão apresentam certo grau de inteligência. As características que os diferenciam são: o grau de complexidade, incerteza e o tipo de informações apresentadas para o sistema.

Em particular, os sistemas de previsão inteligentes devem possuir a habilidade de tratarem um vasto conjunto de incertezas, os aspectos qualitativos da informação, as estruturas de dados complexas, a vasta quantidade de dados não-estruturados e a informação de especialistas. Entretanto, no atual estágio do desenvolvimento tecnológico, os sistemas de previsão ditos inteligentes apresentam, ainda, características rudimentares quanto aos aspectos de autonomia em termos de aprendizado, raciocínio, planejamento e tomada de decisões.

Zadeh (1994) e Bezdek (1994), de forma independente, propuseram a denominação de inteligência computacional para uma coleção de metodologias que visam explorar: a tolerância a falhas, a imprecisão e a incerteza proporcionando robustez e solução de baixo custo. Os principais membros deste consórcio incluem as áreas de redes neurais, algoritmos evolutivos, sistemas nebulosos, raciocínio probabilístico (gerenciamento da incerteza e aprendizado de máquina) e a combinação destes (sistemas híbridos inteligentes).

O princípio que guia a inteligência computacional é explorar a tolerância à imprecisão e incerteza visando aspectos de tratabilidade e melhor relação com a realidade. Em síntese, o modelo de regra para a inteligência computacional é o pensamento humano (Zadeh, 1994; Ostermeier e Hansen, 1999).

Os pesquisadores da inteligência computacional objetivam atender a estas necessidades com o desenvolvimento de sistemas que combinam as vantagens de algumas metodologias inteligentes por meio da configuração de sistemas híbridos inteligentes. Os sistemas híbridos são relevantes quando se considera a natureza variada das aplicações. As formas dos sistemas híbridos inteligentes usualmente analisados na literatura incluem: i) sistemas evolutivo-nebulosos; ii) sistemas evolutivo-neurais; iii) sistemas neuro-nebulosos; e iv) sistemas neuro-nebuloso-evolutivos (Khosla e Dillon, 1997; Shapiro, 2002).

Na próxima subseção, é apresentada uma recente abordagem de modelo neuro-nebuloso com otimização por estratégia evolutiva para aplicação em detecção de fraudes de comércio eletrônico.

3.1 FAN (Free Associative Neurons): um modelo neuro-nebuloso de reconhecimento de padrões

Na literatura, têm sido propostas diversas variantes de modelos neuro-nebulosos (Jang, 1993; Buckley e Hayashi, 1994; Jang e Sun, 1995; Nauck e Kruse, 1999; Mitra e Hayashi, 2000).

A abordagem da FAN (Raittz, 2002; Raittz et al., 1998) consiste em uma estratégia de reconhecimento de padrões, que garante bom desempenho no aprendizado aliado às vantagens computacionais da clareza na representação dos padrões e portabilidade das unidades de representação que são denominadas *free associative neurons*.

Na abordagem usando FAN, cada padrão de entrada do sistema é expandido em uma vizinhança nebulosa. Cada conjunto suporte dessa vizinhança é a combinação dos valores das características próximos dos originais (Raittz et al., 1998).

O grau de similaridade entre a vizinhança nebulosa e o padrão original de entrada é realizado pelas técnicas usadas em conjuntos nebulosos (Klir e Yuan, 1995). O aprendizado acontece pela projeção da vizinhança nebulosa no espaço FAN. Há uma unidade FAN para cada

classe do domínio do problema. Cada unidade é uma matriz composta por todas as combinações de características observadas em sua classe correspondente (Raittz et al., 1998).

Durante o treinamento, cada combinação é representada por uma célula nebulosa que contém um peso correspondente à sua freqüência de ocorrência e grau de pertinência. O treinamento é baseado no reforço nas células projetadas de FAN – se a classificação foi correta – ou em esquecimento (penalização) – se houve uma classificação incorreta.

Em FAN, dois princípios básicos fundamentam o processo de representação de dados: i) um padrão representa mais que um simples ponto, em termos de informação, assim, na modelagem será considerada uma região na vizinhança do padrão analisado; e ii) cada padrão contém mais informações que vão além dos valores individuais, fazendo a correlação dos valores das características, o desempenho do sistema pode ser aumentado.

Neste contexto, a primeira tarefa está relacionada com a decomposição do padrão, ou seja, a geração de uma vizinhança em torno do padrão de entrada. A vizinhança constitui um conjunto de padrões nebulosos no espaço de entrada, próximos ao padrão original. A tarefa seguinte, no procedimento de modelagem dos dados, é a projeção de cada vizinhança nebulosa em uma região denominada espaço FAN. Esta região consiste em um conjunto de pontos no espaço $\Re^{2H}$ (em que H é o nível de combinação das características) e o algoritmo FAN, neste contexto, mede a similaridade entre essas projeções e as unidades FAN.

Em síntese, o processo de modelagem neuro-nebulosa usando FAN é realizado pelos seguintes procedimentos: i) decomposição do padrão (vizinhança nebulosa); e ii) projeção da vizinhança nebulosa.

Na decomposição, o padrão de entrada é transformado em um conjunto de padrões nebulosos. Dado um padrão de entrada x, a seguinte expressão representa o conjunto de padrões nebulosos:

$$\overline{\mathbf{x}}_z = \mu_{x_i}(v_i(l_i))/v_i(l_i), ..., \mu_{x_p}(v_p(l_p))/v_p(l_p) \quad (1)$$

em que z = 1, $(2D + 1)^p$, D é o raio de decomposição que estabelece o número de inteiros em cada lado da coordenada original x_i (centro) do vetor de entrada x; $v_i(l_i)$ é o valor da i-ésima coordenada inteira, próxima ao valor original x_i, em que o índice l_i = 1,(2D+1), varia para a vizinhança de cada coordenada; e $\mu_{x_i}(v_i(l_i))$ é a função de pertinência que mede a similaridade entre o valor e o original x_i (i = 1, p).

Uma vez gerados os vizinhos nebulosos, o processo de modelagem dos dados dá início à projeção da vizinhança. A idéia é projetar o padrão original x sobre o espaço de combinações das características. Sua dimensão é igual ao produto cartesiano nebuloso da vizinhança das características, em que a similaridade em relação aos valores originais é obtida por meio de técnicas nebulosas. Esta etapa é realizada projetando cada vizinho nebuloso $\overline{x}_z$, sobre o espaço cartesiano nebuloso, gerando a projeção F_z.

O primeiro parâmetro a ser ajustado é o nível de combinação das características, denominado H. Este fator tem impacto direto na dimensão do espaço FAN. O escopo de valores de H é o intervalo [1, p], em que p é dimensão do espaço de entrada.

Desta forma, um fator H = 2, implica que as características serão combinadas em pares. A projeção completa F_z é formada por todas as $C_p^H + p$combinações de características. Esta combinação é composta pelos índices dos vetores $\overline{x}_z$ e pelos valores das coordenadas $v_j(l_j)$ a serem combinados. Cada combinação é avaliada pelo produto dos graus de pertinência correspondentes $\mu(v_j(l_j))$. A projeção de F_z é determinada então por:

$$\mathbf{F}_z \in \Re^{2H}\left(C_p^H + p\right) = \mathrm{Proj}(\overline{\mathbf{x}}_z) = \left(f_m^z, \mathbf{a}, \alpha\right) \quad (2)$$

em que $a = (a_1, ..., a_H)$ é o vetor de índices, com $1 \leq a_j \leq p$, $\alpha = (v_i(i_1), ..., v_H(i_H))$ e

$$f_m^z = \prod_{j=1,H} \mu_{x_i}\left(v_j, (a_j)\right) \quad (3)$$

com m = 1, $(C_p^H + p)$.

As equações 2 e 3 descrevem como um vizinho nebuloso é representado em um subespaço do FAN. Entretanto, na implementação do aprendizado deve-se considerar não apenas um vizinho. Na expressão abaixo, F_z é calculado usando-se todos os vizinhos possíveis para H e D definidos para a aplicação. Em alguns casos práticos não é usada a totalidade, mas sim uma quantidade que seja representativa, evitando problemas de explosão combinatória. O número destas combinações é usado como parâmetro nas aplicações e recebem o nome de número de combinações das características. A projeção da vizinhança nebulosa é a união dos vizinhos nebulosos projetados de F_z:

$$\mathbf{F} = \bigcup_{Z=1,(2D+1)^p} \mathbf{F}_Z \quad (4)$$

O aprendizado envolve a comparação entre a projeção F e todas as unidades FAN^j (j = 1, C, em que C é o número de classes do domínio do problema). A dimensão de F é definida pela expansão do padrão de entrada x (isto é, depende dos valores das coordenadas x_i de x e dos parâmetros D e H). Entretanto, FAN^j possui uma dimensão maior, incluindo as combinações de características que ocorrem para todo x^k FAN^j. A comparação é feita avaliando o grau no qual F é um subconjunto de FAN^j.

O cálculo da similaridade entre F e FAN^j e as expressões usadas para reforço e esquecimento não representam a essência do método proposto, podendo variar de uma

aplicação para outra. Neste caso, a similaridade entre F e FAN^j é calculada por:

$$S\left(\mathbf{F}, \mathbf{FAN}^j\right) = 1 - \prod_g \left(1 - \frac{f_g.fan_g^j}{fan^j}\right) \quad (5)$$

em que fan_g^j é uma célula do conjunto nebuloso FAN^j; f_g é uma célula do conjunto nebuloso F (obtido pela equação 3); g é o índice que cobre todo o domínio de FAN^j que possui um correspondente em F; e fan^j é o número total de ocorrências na unidade FAN^j.

A Equação 5 mede a similaridade da projeção F em cada unidade FAN, FAN^j. A maior similaridade indica a classe associada ao padrão de entrada x. Em outras palavras, a saída da rede é j-ésima classe, em que $j \in [1,C]$ é o índice da unidade FAN que apresenta maior similaridade, FAN^j. Isto é obtido por:

$$S\left(\mathbf{F}, \mathbf{FAN}^{j*}\right) = \max_j S\left(\mathbf{F}, \mathbf{FAN}^j\right) \quad (6)$$

Uma vez que a saída da rede neuro-nebulosa é determinada, acontece o aprendizado (retroprocessamento do erro). Primeiramente ocorre a verificação do acerto na classificação ($j^* = j^t$, em que j^t é a classe do domínio associada ao padrão de entrada x) ou erro de classificação (caso contrário). Em ambos os casos a mudança dos valores de pertinência de FAN^{j*} é determinada pelo grau de pertinência da célula f_g.

Quando a saída da rede neuro-nebulosa for correta, o procedimento consiste no fortalecimento das células FAN^{j*} interceptadas pela projeção **F**.

O fortalecimento consiste em somar ao conteúdo atual da célula fan_g^j o valor de pertinência f_g. A pertinência será determinada pelo somatório das pertinências na célula, dividida pelo total de ocorrências na unidade fan_g^j/fan^j.

No caso de ocorrer uma classificação errada, o algoritmo realiza um procedimento de esquecimento, diminuindo o valor das células FAN^{j*} interceptadas pela projeção F. Neste caso, a pertinência f_g é subtraída do conteúdo da célula, se este conteúdo tornar-se negativo após a subtração, seu valor será definido como sendo zero. Resumindo, o algoritmo FAN pode ser resumido pelas seguintes etapas (detalhes são encontrados em Raittz (2002):

i) iniciar $FAN^j = 0$ para j = 1, C, em que C é o número de classes a serem classificadas do problema em questão;
ii) iniciar o nível de combinações de características H e o raio de decomposição D;
iii) realizar a decomposição do padrão;
iv) realizar a projeção da vizinhança nebulosa;
v) calcular o grau de similaridade;
vi) determinar a saída da rede neuro-nebulosa; e
vii) realizar retroprocessamento do erro.

3.2 Otimização usando estratégia evolutiva

Nos algoritmos evolutivos (AEs), um conjunto de soluções (população) é manipulado a cada iteração, em contraste com outros métodos de otimização, em que apenas uma solução para o problema é utilizada a cada iteração. A chance de que um indivíduo da população seja selecionado na próxima geração depende da função de aptidão (*fitness*) do indivíduo (solução a ser otimizada), que consiste, geralmente, de uma função objetivo ou mesmo uma transformação simples desta para o tratamento do problema em questão. Um compromisso entre convergência (*exploitation*) e diversidade dos membros que constituem a população (*exploration*) é um problema constante em AEs e deve ser considerado na configuração de uma metodologia de otimização eficiente.

Muitas das pesquisas relacionadas aos princípios de auto-adaptação em AEs tratam de parâmetros relacionados com operador de mutação. A técnica de auto-adaptação é geralmente empregada com sucesso nos ajustes de variâncias e de covariâncias em relação a uma distribuição normal n-dimensional.

Segundo Angeline (1995), é possível adaptar dinamicamente os aspectos de processamento de um AE antecipando as regularidades do ambiente, aprimorando o procedimento de otimização e enfatizando a rapidez na busca dos parâmetros. Os AEs que apresentam mecanismos adaptativos (AEMAs) distinguem-se pela configuração dinâmica dos parâmetros selecionados ou mesmo pelos operadores durante o ciclo evolutivo de otimização. Os AEMAs têm uma vantagem sobre os AEs básicos, pois são mais reativos em antecipar as particularidades do problema ou mesmo, em algumas formulações, podem dinamicamente adquirir informação sobre as regularidades no problema e explorá-las. Segundo Angeline (1995), os AEMAs podem ser separados em três níveis nos quais os parâmetros adaptativos estão presentes, que são os seguintes:

i) nível populacional: os métodos adaptativos ajustam dinamicamente os parâmetros, que são globais à população inteira;
ii) nível individual: os métodos adaptativos modificam a maneira que um indivíduo da população é afetado pelos operadores de mutação; e
iii) nível de componente: os métodos adaptativos alteram a forma pela qual os componentes de cada indivíduo são manipulados independentemente dos outros indivíduos da população.

Os mecanismos de auto-adaptação, no âmbito de componente dos parâmetros da estratégia adaptativa, providenciam uma das características principais do sucesso das EEs. As EEs utilizam princípios de busca no espaço de variáveis-objeto e estratégia interna de controle dos parâmetros, simultaneamente (Beyer, 1995). A aborda-

gem de EE com adaptação do sistema independente de coordenadas para o operador de mutação, usada neste trabalho para otimizar (busca local) os valores de raio de decomposição da FAN (após a etapa (vii) de retroprocessamento), foi proposta por Hansen e Ostermeier (1996) e Ostermeier e Hansen (1999).

A mutação é o operador principal de uma EE e sem a mudança na distribuição do operador de mutação durante a seqüência de gerações do ciclo evolutivo, existe uma diminuição na probabilidade da solução evoluir para uma solução adequada.

O caminho de evolução — "caminho" de distribuição da população no espaço de busca ao longo de um número de gerações — revela informações do ciclo evolutivo, principalmente pelas correlações entre os passos de mutação que são sucessivamente selecionados na seqüência de gerações. Se os passos de mutação selecionados são correlacionados paralelamente (produto escalar maior que zero), ou seja, os passos de evolução estão na mesma direção, o caminho de evolução é comparativamente longo. Se, por outro lado, os passos de mutação são correlacionados de forma antiparalela (produto escalar menor que zero), o caminho de evolução é comparativamente mais curto. Conseqüentemente, para a realização de passos de mutação mais eficientes é melhor não possuir uma correlação entre os passos de mutação selecionados no caminho de evolução (Ostermeier e Hansen, 1999).

Ostermeier e Hansen (1999) sugerem o princípio da adaptação fundamental para remover a correlação entre os passos de mutação selecionados sucessivamente, que diz: "uma adaptação aceitável necessita reduzir a diferença entre as distribuições do caminho de evolução atual e um caminho de evolução, por meio de uma seleção aleatória com relação aos parâmetros adaptados".

Uma abordagem baseada no princípio da adaptação fundamental é adotada neste artigo. A abordagem é denominada de adaptação da matriz de covariância e é aplicada a uma (μ, λ) -EE, em que os λ descendentes competem para sobreviver e o(s) μ ancestral(is) é(são) completamente substituído(s) a cada geração. A seguir são apresentadas equações que regem esta abordagem de (μ, λ) - EE para $\mu = 1$.

As equações são apresentadas de forma detalhada em Hansen e Ostermeier (1996). A regra de atualização desta EE é bastante similar à regra de atualização dos métodos do tipo quase-Newton, muito utilizado na concepção de métodos de otimização clássica.

4. Descrição do problema e resultados

A realização de detecção de fraudes em operações de comércio eletrônico é um campo de estudo confidencial e ainda com pouca divulgação pública dos resultados obtidos por empresas comerciais.

Uma abordagem relevante para lidar com este tipo de problema é a adoção de análise de agrupamentos. Neste contexto, análise de agrupamentos é o nome para um grupo de técnicas multivariadas cujo objetivo essencial é agregar objetos com base nas características que eles possuem. A análise de agrupamento classifica os objetivos (por exemplo, clientes, transações) de modo que cada objeto é muito semelhante aos outros no agrupamento em relação a algum critério de seleção pré-determinado. Os agrupamentos resultantes de objetos devem, então, exibir elevada homogeneidade interna (dentro dos agrupamentos). Assim, se a classificação for bem sucedida, os objetos dentro dos agrupamentos estarão próximos, quando representados graficamente, e diferentes agrupamentos estarão distantes (Hair et al., 2005). Os problemas de detecção de fraudes podem ser incluídos na classe de problemas de agrupamento de dados.

Especificamente, o problema real de detecção de fraudes é realizado pelo sistema FControl® (*http://www.ciashop.com.br*) para classificar se uma operação é normal, suspeita ou fraudulenta. Estas características foram selecionadas de acordo com o conhecimento de um especialista e análise de correlação múltipla dos dados vinculados a transações e comportamento histórico de cada cliente do sistema.

A FAN utilizada para esta finalidade é otimizada de 14 em 14 dias para manter o sistema em alerta para o aparecimento de possíveis padrões novos de fraudes. A EE é usada para realizar a otimização dos valores de raio de decomposição da FAN, isto realizado após a etapa de retroprocessamento do erro obtido pela FAN.

Foi testado com banco de dados com 2916 dados de transações (reais) de comércio eletrônico com os mais diversos padrões de transações legais e fraudulentas. Na Figura 1, uma representação das transações legais e fraudulentas do banco de dados é apresentada.

A FAN sem o uso de EE obteve uma taxa de classificação com acerto de 89,5432% para as transações legais e 89,8876% para as transações fraudulentas. Entretanto, com a utilização da otimização pela EE o nível de acerto aumentou para 90,1472% para as transações legais e 92,1348% para as transações fraudulentas. Neste contexto, a EE utilizada na otimização foi projetada para utilizar $\mu = 1$, $\lambda = 20$ e critério de parada quando atingir 500 gerações.

5. Conclusão

No Brasil, as perdas com fraudes em lojas virtuais representam em média 3% do faturamento bruto dos estabelecimentos. Estima-se que outros 3% das transações nas lojas virtuais sejam tentativas de fraude (FControl, 2005), mas há casos em que o índice de fraudes e tentativas ultrapassa 20%, caso de lojas com produtos de alto valor agregado e facilidade de revenda.

Neste artigo, foi apresentado um panorama do projeto do sistema FControl® para detecção de fraudes em operações de comércio eletrônico. O FControl emprega tecnologias da inteligência artificial para detectar tentativas de fraude nas transações com cartão de crédito. Neste contexto, os dados das transações de compra e o comprador são passados ao banco de dados do sistema computacional FControl® na forma de consulta. O FControl® informa ao comerciante uma pontuação de risco de fraude, sendo esta baseada em fatores analisados de consistência geográfica, periodicidade (freqüência entre compras), padrões de fraude conhecidos, comportamento típico de compradores e padrões típicos de transações do estabelecimento. Neste contexto, o FControl® analisa os dados utilizando inteligência artificial para detecção de características e padrões de fraude incorporando também tecnologias de lista negra, lista branca, regras de negócio customizáveis e travas de segurança (detalhados na seção 2 do artigo).

O sistema utiliza uma abordagem FAN híbrida que combina conceitos de redes neurais, sistemas nebulosos e computação evolutiva. A FAN combina simbioticamente os méritos do tratamento do conhecimento quantitativo das redes neurais, as facilidades de representação do conhecimento e tratamento de incertezas dos sistemas nebulosos e as potencialidades de busca e otimização da computação evolutiva.

Os resultados obtidos pela FAN, com otimização evolutiva, no sistema FControl® têm apresentado boa precisão na classificação tanto de operações legais quanto fraudulentas, com taxas de acerto acima de 90%.

Entretanto, alguns estudos quanto aos aspectos de aprimoramento das potencialidades do sistema FControl® têm sido abordados, visando, entre outros aspectos, à obtenção de um melhor compromisso entre interpolação, generalização e aprendizado de sistemas híbridos inteligentes na detecção de fraudes. Atualmente (maio de 2005), o sistema FControl® conta com 250 clientes e um banco de dados atual com 45670 transações realizadas. Exemplos de interface e padrões de transações normais, suspeitas e fraudulentas são apresentados nas Figuras 2, 3 e 4, respectivamente.

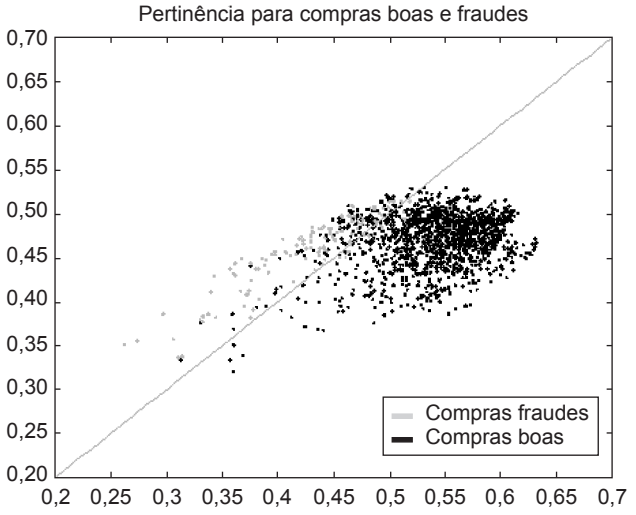

Figura 1. Transações boas e fraudulentas.

Agradecimentos

Os autores agradecem o auxílio financeiro do Convênio FINEP (Financiadora de Estudos e Projetos), projeto número 0.1.02.0184.00, que tornou possível o estudo, implementação e viabilidade comercial do sistema comercial FControl® (*http://www.ciashop.com.br*). Agradecem também os preciosos comentários do editor e dos revisores que visaram melhorar a fundamentação e legibilidade do artigo.

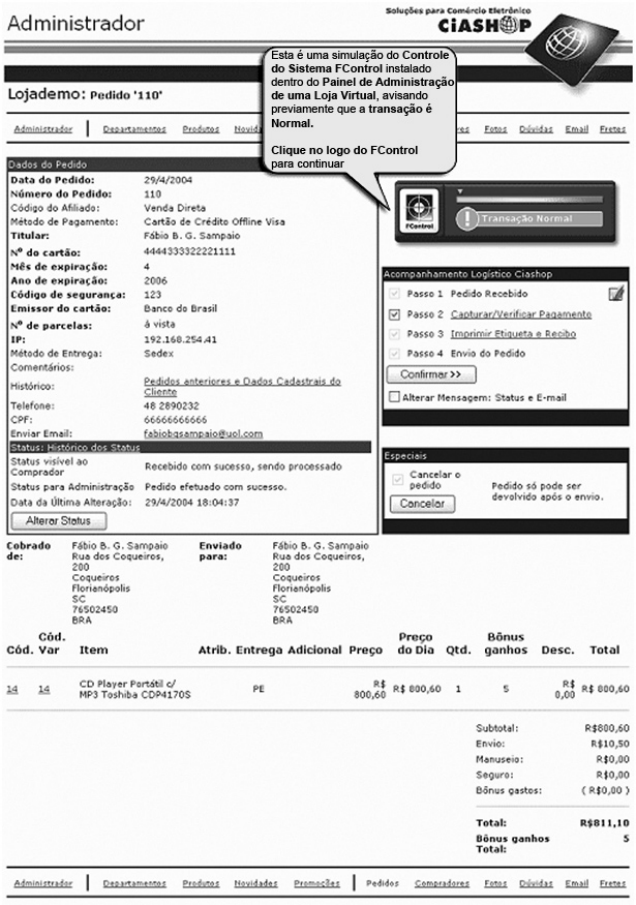

Figura 2. Exemplo de interface do FControl® para uma transação normal.

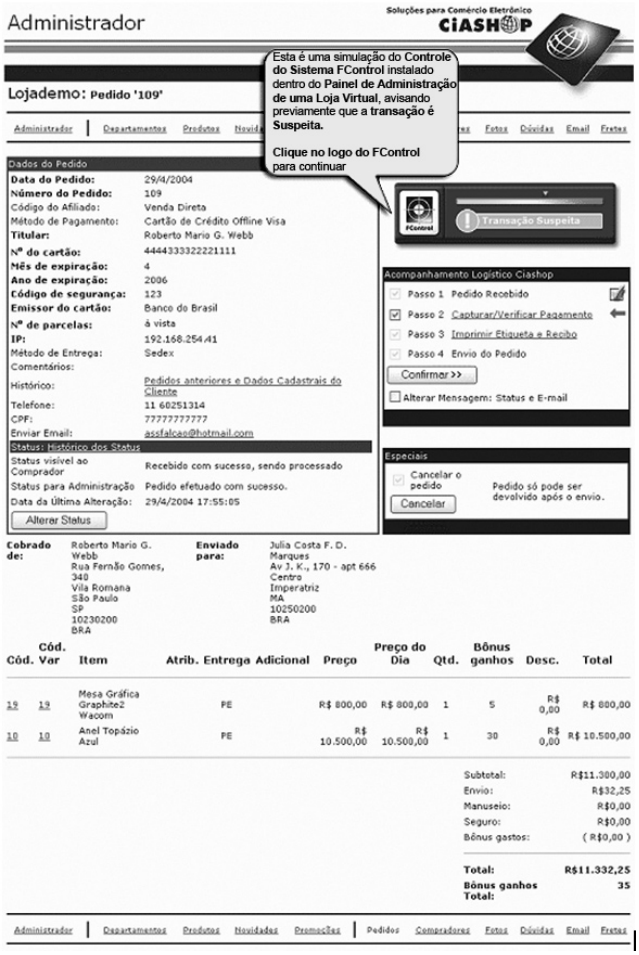

Figura 3. Exemplo de interface do FControl® para uma transação suspeita.

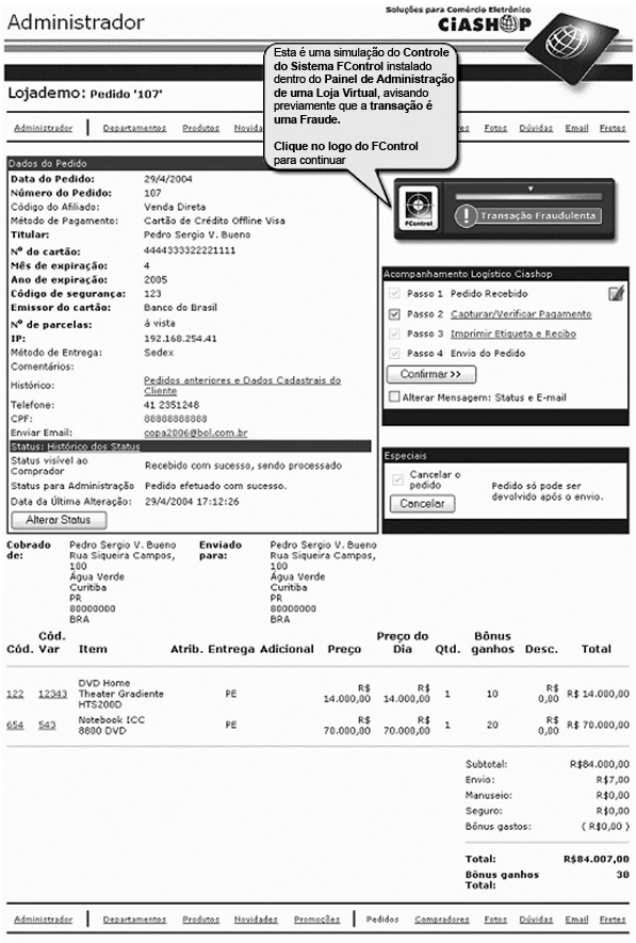

Figura 4. Exemplo de interface do FControl® para uma transação fraudulenta.

Referências Bibliográficas

ALESKEROV, E.; FREISLEBEN, B.; RAO, B. CARDWATCH: a neural network based database mining system for credit card fraud detection. In: IEEE/IAFE of Computational Intelligence for Financial Engineering, New York, NY, USA. **Proceedings…,** New York, p. 220-226, 1999.

ANGELINE, P. J., Adaptive and self-adaptive evolutionary computations. In: **Computational intelligence: a dynamic systems perspective**, Palniswami, M., Attikiouzel, Y., Marks, R., Fogel, D., Fukuda, T. (eds.), Piscataway, NJ, USA, IEEE Press, p. 152-163, 1995.

BEYER, H. G. Toward a theory of evolution strategies: self-adaptation. **Evolutionary Computation**, v. 3, n. 3, p. 311-348, 1995.

BEZDEK, J. C., What is computational intelligence? **Computational intelligence imitating life**, Zurada, J. M., Marks II, R. J., Robinson, C. J. (eds.), IEEE Press, Piscataway, NJ, USA, 1994.

BRAUSE, R.; LANGSDORF, T.; HEPP, M. Neural data mining for credit card fraud detection. In: IEEE International Conference on Tools for Artificial Intelligence, 11., 1999, Chicago, Illinois, USA. **Proceedings…**, Chicago, 1999. p. 103-106.

BUCKLEY, J. J; HAYASHI, Y. Fuzzy neural networks: a survey. **Fuzzy and Systems**, v. 66, n. 1, p. 1-13, 1994.

CHAN, P. K.; FAN, W.; STOLFO, S. J. Distributed data mining in credit card fraud detection. **IEEE Intelligent Systems**, v. 14, n. 6, p. 67-74, 1999.

CHI, S. -C.; KUO, R. -J.; TENG, P. -W. A fuzzy self-organizing map neural network for market segmentation of credit card. In: IEEE International Conference on

Systems, Man, and Cybernetics, 2000, Nashville, TN, USA. **Proceedings…,** Nashville, 2000. p. 3617-3622.

DONNELLY, A., 2000, Online credit card fraud outspaces physical world. **Computer Fraud & Security**, n. 10, p. 9, 2000.

FCONTROL, **FControl – solução definitiva contra fraudes**. White paper. 2005. Disponível em <www.fcontrol.com.br> Acesso em: 15 março 2005.

FOLHA ON-LINE. **Fraudes**. 2005. Disponível em http://jc.uol.com.br/2005/03/15/not_85515.php Acesso em: 15 março 2005.

GHOSH, S.; REILLY, D. L. Credit card fraud detection with a neural network. In: Annual Hawaii International Conference on System Sciences, 27., 1994, Wailea, HI, USA. **Proceedings…,** Wailea, 1994. p. 621-630.

HAIR, J. F.; ANDERSON, R. E.; TATHAM, R. L.; BLACK, W. C. **Análise multivariada de dados**, 5 ed., Porto Alegre: Bookman, 2005.

HANAGANDI, V.; DHAR, A.; BUESCHER, K. Density-based clustering and radial basis function modeling to generate credit card fraud scores. In: IEEE/IAFE Conference on Computational Intelligence for Financial Engineering, 1996. New York, NY, USA. **Proceedings…,** New York, 1996. p. 247-251.

HANSEN, N.; OSTERMEIER, A. Adapting arbitrary normal mutation distributions in evolution strategies. In: IEEE International Conference on Evolutionary Computation, 1996, Nagoya, Japan. **Proceedings…,** Nagoya, p. 312-317.

JANG, J. -S. R. ANFIS: Adaptive-network-based fuzzy inference systems. **IEEE Transactions on Systems, Man, and Cybernetics**, v. 23, n. 5, p. 665-685, 1993.

JANG, J. -S. R.; SUN, C. -T. Neuro-fuzzy modeling and control. **Proceedings of the IEEE**, v. 83, n. 3, p. 378-406, 1995.

KHOSLA, R.; DILLON, T., **Engineering intelligent hybrid multi-agent systems**. Boston: Kluwer Academic Publishers, 1997.

KLIR, G. J.; YUAN, B. **Fuzzy sets and fuzzy logic – theory and applications**. Upper Saddle River: Prentice Hall PTR, 1995.

KOU, Y; LU, C. -T.; SRIWONGWATTANA, S.; HUANG, Y. -P. Survey of fraud detection techniques. In: IEEE INTERNATIONAL CONFERENCE ON NETWORKING, SENSING AND CONTROL, 2004, Taipei, Taiwan. **Proceedings…,** Taipei, 2004. p. 749-753.

LIU, Y.; YAO, X. Simultaneous training of negatively correlated neural networks in an ensemble. **IEEE Transactions on Systems, Man, and Cybernetics — Part B: Cybernetics**, v. 29, n. 6, p. 716-725, 1999.

MITRA, S.; HAYASHI, Y. Neuro-fuzzy rule generation: survey in soft computing framework. **IEEE Transactions on Neural Networks**, v. 11, n. 3, p. 748-768, 2000.

NAUCK, D.; KRUSE, R. Neuro-fuzzy systems for function approximation. **Fuzzy Sets and Systems**, v. 101, n. 2, p. 261-271, 1999.

NETWORK SECURITY, 43% of credit card fraud not reported. **Network Security**, n. 10, p. 4, 2000.

OSTERMEIER, A.; HANSEN, N. An evolution strategy with coordinate system invariant adaptation of arbitrary normal mutation distributions within the concept of mutative strategy parameter control. In: Genetic and Evolutionary Computation Conference, GECCO, 1999, Orlando, FL, USA. **Proceedings…,** p. 902-909.

RAITTZ, R. T. **FAN 2002: um modelo neuro-fuzzy para reconhecimento de padrões**. 2002. Tese (Doutorado em Engenharia de Produção) - Universidade Federal de Santa Catarina, Florianópolis, SC, 2002.

RAITTZ, R. T.; Souza, J. A.; Dandolini, G. A.; Pacheco, R. C. S.; Martins, A.; Gauthier, F. A.; Barcia, M. FAN: learning by means of free associative neurons. In: IEEE World Congress on Computational Intelligence, 1998, Anchorage, AK, USA. **Proceedings…,** Anchorage, 1998. p. 425-430.

RICHARDSON, R. Neural networks compared to statistical techniques. In: IEEE/IAFE Computational Intelligence for Financial Engineering, 1997, New York, NY, USA. **Proceedings…,** p. 89-95.

SHAPIRO, A. F., The merging of neural networks, fuzzy logic, and genetic algorithms. **Insurance: Mathematics and Economics**, v. 31, n. 1, p. 115-131, 2002.

SORRONSORO, J. R.; GINEL, F.; SÁNCHEZ, C.; CRUZ, C. S. Neural fraud detection in credit card operations. **IEEE Transactions on Neural Networks**, v. 8, n. 4, p. 827-834, 1997.

SYEDA, M.; ZHANG, Y. -Q.; PAN, Y. Parallel granular neural networks for fast credit card fraud detection. In: IEEE International Conference on Fuzzy Systems, 2002, Honolulu, HI, USA. **Proceedings…,** v. 1, p. 572-577,

WHEELER, R.; AITKEN, S. Multiple algorithms for fraud detection. **Knowledge-based systems**, v. 13, n. 2-3, p. 93-99, 2000.

ZADEH, L. A. Soft computing and fuzzy logic. **IEEE Software**, v. 11, n. 6, p. 48-56, 1994.

FCONTROL®: AN INNOVATIVE INTELLIGENT SYSTEM FOR FRAUD DETECTION IN E-COMMERCE TRANSACTIONS

Abstract

The prevention of credit card fraud is an important commercial application for prediction methods and computational intelligence of pattern recognition approaches. Computational intelligence is an association of bio-inspired computational methodologies which are founded principally on neural networks, fuzzy systems, evolutionary computation, swarm intelligence, and probabilistic computation. The application of computational intelligence techniques in the support of service tasks such as anomaly detection and identification, pattern classification, diagnostics, prognostics, estimation and control has recently emerged in industrial and commercial environments. This paper presents an efficient system based on computational intelligence methodologies for the detection of fraud in the operation of real credit card data in E-commerce transactions. This new proposed method, called FControl® for fraud detection and classification, integrates concepts of hybrid intelligent systems based on neural networks, fuzzy systems and evolutionary computation approaches. The proposed method generates quality solutions in terms of prediction efficiency and success. The computational program of the FControl® system has been installed on an Intel Pentium IV 2.4 MHz (bi-processor and 4 Gbytes RAM) at the company Ciashop E-Commerce and is currently in use for fraud detection by 250 companies that offer E-commerce services.

Keywords: information technology, E-commerce, artificial intelligence, fraud detection, credit card, neuro-fuzzy systems, evolutionary Computation.