Autenticação Pessoal por Imagens de Sinais Manuscritos

Miguel Gustavo Lizárraga e Lee Luan Ling

***Resumo*—Neste trabalho é proposto um método de autenticação pessoal automático baseado em imagens que sejam compostas por traços manuscritos que representem símbolos, palavras, assinaturas ou desenhos. O método apresentado é de simples implementação, eficiente e robusto. As taxas médias de erros de falsa rejeição e falsa aceitação deste método são de 2,5% e 1,9% respectivamente.**

***Palavras-Chave*—biometria, manuscritos, sistemas de autenticação pessoal, processamento de imagens.**

***Abstract*—In this work is proposed a personal authentication method based on images that are composed by handwritten strokes which may represent symbols, words, signatures or drawings. This method has a simple implementation, it is efficient and robust. The averages false rejection and false acceptance rates are 2.5 %and 1.9 %, respectively.**

***Index Terms*—biometrics, handwritten signatures, personal authentication, image processing.**

I. Introdução

Na sociedade atual as pessoas passam cada vez mais por situações em que são obrigadas a ter que provar sua identidade e para fazê-lo se utilizam de crachás, cartões, passaportes, números de identidade, senhas, etc. Este tipo de comprovação não somente ocorre quando desejamos nos apresentar perante uma pessoa, mas também quando queremos realizar qualquer tipo transação comercial, seja esta uma simples retirada de dinheiro num caixa automático ou pagamentos de contas via internet [1].

A comprovação da identidade de uma pessoa pode ser realizada basicamente de três maneiras. A primeira é ter acesso a chaves baseadas no seu conhecimento, como por exemplo senhas e contra-senhas. A segunda é possuir fisicamente um dispositivo que em si seja a autenticação, como por exemplo, um cartão válido ou um crachá. A terceira opção é a validação de identidade através da pessoa em si, isto é, através de um padrão ou atividade específica do indivíduo (fala, assinatura), ou ainda através de alguma de suas qualidades físicas (impressões digitais, faces)

Miguel Gustavo Lizárraga e Lee Luan Ling, Departamento de Comunicações, Faculdade de Engenharia Elétrica e de Computação, Universidade Estadual de Campinas, São Paulo, Brasil, E-mails: lizarrag@decom.fee.unicamp.br, lee@decom.fee.unicamp.br. Este trabalho foi financiado pela FAPESP (02/04763-4).

Na maioria das vezes, a forma de autenticar a identidade de um indivíduo recai sobre as duas primeiras maneiras, ou seja, memorizando números de identificação incluindo senha do cartão do banco ou login do computador, número de RG, de passaporte, de CPF e vários outros. Ou ainda, apresentando vários documentos de identificação, como por exemplo, carteira de identidade, carimbos, selos, cartões e chaves. Entretanto, nenhum desses métodos são 100% confiáveis, visto que podem ser esquecidos, roubados, emprestados, perdidos, copiados ou falsificados [2].

Por essas razões, tem aumentado o interesse em desenvolver métodos de autenticação de identidade pessoal que levem em consideração estratégias que se fundamentem na terceira maneira. Essas estratégias se baseiam em medidas biométricas, onde se entende como medida biométrica à mensuração de atributos/características físicas ou de comportamento de uma pessoa com o objetivo distinguí-la dentre as demais.

A escolha de um método de autenticação de identidade através de características biométricas, seja pela abordagem fisiológica ou de comportamento, pode gerar amplos debates com relação a sua utilização, eficácia, confiabilidade e praticidade. Nesse contexto, a implementação de sistemas que utilizam características fisiológicas está bastante aberta a discussões, entretanto, aqueles que se servem de características de comportamento possui um consenso geral, embora outras alternativas possam ser consideradas, a utilização de sinais manuscritos tem a mais ampla aceitação e vantagens significativas [3]:

* O sinal manuscrito é o método mais natural e mais amplamente utilizado para confirmar nossa identidade (assinaturas)
* Medidas das características de sinais manuscritos não são invasivas (quando comparada com outras técnicas, como por exemplo, as medidas feitas sobre a íris)
* A aquisição de sinais manuscritos não tem conotações negativas ou de higiene pessoal (se comparadas com medidas feitas sobre impressões digitais).

II. Senhas Gráficas

A autenticação pessoal por imagens de sinais manuscritos é uma evolução natural da autenticação pessoal por imagens de assinaturas, onde entende-se por imagens de sinais manuscritos qualquer imagem que seja composta por traços,

por exemplo, desenhos, emblemas, palavras manuscritas, símbolos, caracteres etc. Assim sendo, qualquer assinatura pode ser considerada como um sinal manuscrito, entretanto nem todo sinal manuscrito pode ser considerado uma assinatura.

Cardot *et all* em [4] diz que as assinaturas ocidentais podem ser divididas em dois grandes grupos. O primeiro grupo é aquele em que a assinatura da pessoa é simplesmente a escrita do seu nome em letra cursiva (ver figura 1a), sendo por conseguinte legível. O segundo grupo é aquele em que a assinatura é composta não somente pela escrita do nome, mas também por uma série de traços e rabiscos que tentam particularizar a assinatura, o que faz com que na maioria das vezes, o nome escrito fique ilegível (ver figura 1b).

Entretanto, além das assinaturas ocidentais (legíveis ou não) nas quais se utiliza o alfabeto romano, existem as assinaturas que são feitas utilizando-se outros tipos de alfabetos como o grego, cirílico, árabe ou chinês entre outros. Assim, observa-se que separar os estilos das assinaturas em legíveis, não-legíveis, européias, orientais, árabes etc. não é uma boa abordagem, visto que dependendo do conhecimento de determinado alfabeto, será possível ou não ler o que foi escrito. Por exemplo, uma assinatura composta por ideogramas chineses para nós ocidentais é em geral ilegível. Entretanto, para pessoas que conhecem esses ideogramas tal assinatura deve ter um significado claro. E o contrário também é verdadeiro, isto é, para alguém que não conhece o alfabeto romano a assinatura representa na figura 1a seria considerada ilegível.

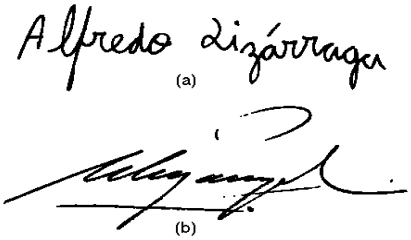

Figura 1: (a) Assinatura legível; (b) Assinatura ilegível

Assim sendo, passou-se a desenvolver um algoritmo que não se servisse de técnicas que levem em consideração características que estão associadas ao tipo de alfabeto ou a sua escrita e que apenas se preocupasse com a forma e os traços que compõe o sinal que foi manuscrito.

Alguns dos motivos que nos incentivam a desenvolver um algoritmo de autenticação de identidade que não se baseie na assinatura em si, mas em símbolos ou sinais manuscritos são:

* Em vez de usarmos nossa assinatura podemos utilizar simplesmente uma rubrica, a qual pode ser mais simples e rápida de ser escrita.

* Não é desejável que as assinaturas mudem muito como tempo, visto que elas devem sempre ser parecidas as existentes no RG ou ainda com aquelas registradas em cartório.

* Se usarmos um símbolo gráfico como login de entrada num sistema, este pode ser facilmente mudado, bastando fazer um re-cadastramento para o novo sinal gráfico.

Baseados nesses motivos vemos a utilização de imagens de sinais manuscritos para autenticação pessoal como uma forma de introduzir o conceito de senhas gráficas. As senhas gráficas, da mesma forma que senhas clássicas baseadas na digitação de um texto no teclado, serviria como a chave que daria acesso aos recursos de um determinado sistema.

A utilização de senhas gráficas torna-se mais atrativo quando é sabido que em sistemas de redes de computadores que possuem um número considerável de usuários, é fácil se quebrar em torno de 20% das senhas dos seus usuários utilizando dicionários contendo um conjunto de palavras seletas disponíveis na internet [5]. As senhas gráficas baseadas em desenhos de sinais manuscritos podem ser utilizadas para se fazer o login em sistemas de redes de computadores, eliminando a possibilidade do ataque de *hackers* através do uso de dicionários.

III. BASE DE DADOS

As imagens que fazem parte da base de dados que foram utilizadas neste trabalho estão formadas de sinais manuscritos que dividimos em duas classes. A primeira é a classe que chamamos de "Assinaturas" e é composta por imagens do tipo mostrado na figura 1, as quais por sua vez as sub-dividimos em assinaturas verdadeiras e falsas. A segunda classe é denominada de "Símbolos" e consta de imagens como as vistas na figura 2.

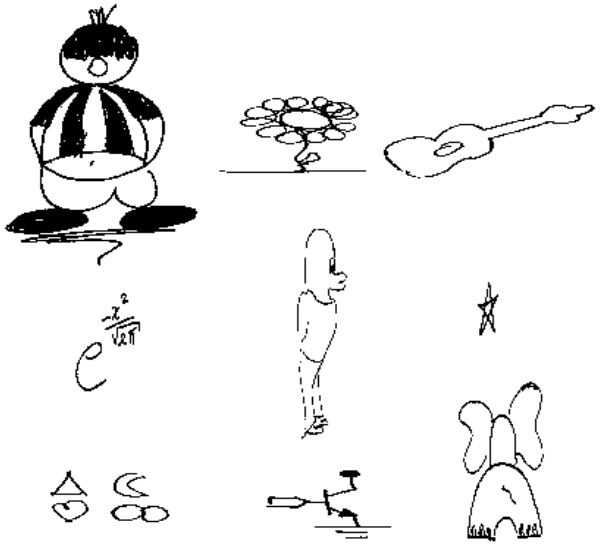

Figura 2: Amostras de símbolos gráficos

Tanto as assinaturas como os símbolos ficaram restritos a uma área retangular de 10 centímetros de comprimento por 8 centímetros de altura. Na digitalização das imagens foi utilizada uma resolução de 200 pontos por polegada. O instrumento de escrita foi uma caneta de tinta de cor preta e diâmetro de ponta 0,5mm.

Para a realização dos testes de avaliação do método proposto dividimos a base de dados em três grupos:

* Assinaturas verdadeiras: Este grupo é composto por um total de 1200 imagens. Essas assinaturas foram obtidas junto a 40 pessoas, sendo que cada uma delas contribuiu com 30 assinaturas. Estas assinaturas são 15 legíveis e 25 ilegíveis

* Assinaturas falsas: Este grupo é composto por um total de 50 assinaturas adquiridas de 50 pessoas diferentes e que não pertencem ao grupo de pessoas que forneceram as assinaturas verdadeiras.

* Símbolos: Este grupo é composto por 600 imagens. Esses símbolos foram obtidos junto a 20 pessoas, sendo que cada uma delas contribuiu com 30 símbolos manuscritos.

IV. MÉTODO PROPOSTO

Nesta seção descreveremos detalhadamente os módulos que compõe o método de autenticação proposto: pré-processamento, extração de características e classificador.

A. *Pré-processamento das Imagens*

Com o objetivo de tratar as imagens e deixá-las num formato que minimize a variabilidade intra-classe e maximize a variabilidade inter-classe, dividimos o pré-processamento de imagens em três etapas. A primeira trata do enquadramento da imagem, a segunda da normalização do tamanho e a terceira da divisão da imagem em quadros.

1) Enquadramento da imagem

O enquadramento da imagem consiste em retirar todo o espaço em branco que fica ao redor das assinaturas ou dos símbolos, de forma a manter apenas o mínimo quadrilátero que contenha os traços que foram manuscritos.

2) Normalização de tamanho

Em nosso algoritmo, a normalização do tamanho está relacionada o número de pixels no eixo horizontal e vertical da imagem. Esta normalização é feita em duas etapas, a primeira consiste em definir a resolução no eixo horizontal e na segunda etapa é feita uma média para se calcular o valor da resolução do eixo vertical.

Os valores escolhidos para normalizar o número de pixels no eixo horizontal são de 256 e 128 pixels. As imagens normalizadas em 256 pixels são utilizadas na extração das características de inclinação dos contornos e dos traços dos sinais manuscritos. As imagens normalizadas em 128 pixels são utilizadas na extração do vetor de características de correlação.

Os valores para normalizar o número de pixels no eixo vertical é dado pela média dos valores do número de pixels no eixo vertical obtidos a partir de 5 sinais gráficos de uma mesma pessoa previamente normalizados no eixo horizontal. Exemplificando, para um conjunto de 5 sinais gráficos normalizados no eixo horizontal em 256 pixels, teríamos por exemplo os seguintes valores nos eixos vertical (mantendo o *aspect ratio*) 201, 210, 199, 200, 205. O valor inteiro da média desses valores é 203. Assim sendo, a normalização final para todas as imagens seria de 256 por 203 pixels, neste caso *aspect ratio* não é mais mantido.

3) Divisão em quadros

A divisão em quadros tem como intuito repartir a imagem em porções menores. Cada uma dessas porções será utilizada no processo de extração de características para gerar vetores que carreguem consigo informações locais da imagem.

A divisão da imagem é feita em 4 quadros. Um atributo importante nesse tipo de divisão é que os quadros possuem uma sobreposição de 50% da sua área com os quadros que estão ao seu redor. A figura 3 exemplifica a divisão de um sinal gráfico nos 4 quadros mostrando a sobreposição entre os mesmos.

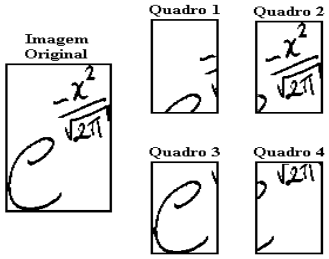

Figura 3: Divisão de um sinal gráfico em 4 quadros

B. *Características*

No método proposto de autenticação pessoal por sinais manuscritos optamos por representar as imagens através de 3 vetores de características:

1. Inclinação dos contornos do sinal manuscrito
2. Inclinação dos traços que compõe o sinal manuscrito
3. Característica de correlação

1) Inclinação dos contornos do sinal manuscrito

O vetor de características que se baseia na inclinação dos contornos do sinal manuscrito, é composto de 20 elementos por quadro. A técnica utilizada para fazer a extração dos elementos que compõe esse vetor foi a morfologia matemática.

Para acharmos a inclinação da imagem do contorno, definimos os elementos estruturantes (EEs) que representam as inclinações de 90, 0, 135 e 45 graus.

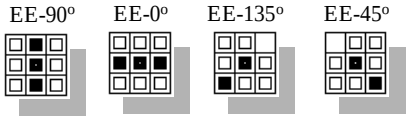

Figura 4: Elementos estruturantes para extração da inclinação do contorno da imagem

Assim, para a composição deste vetor de características foi utilizado o seguinte procedimento: Para uma imagem *A*, primeiramente fazemos a operação de extração de seu contorno e a seguir aplicamos a operação de erosão pelos elementos estruturantes apresentados na figura 4. A contagem do número de pixels mapeados pela erosão através de cada um desses EEs representa um elemento no vetor de características. Em seguida a imagem *A* é dilatada e se repete o procedimento anteriormente descrito por mais 4 vezes.

2) Inclinação dos traço do sinal manuscrito

Na extração da inclinação dos traços da assinatura são utilizados 16 elementos estruturantes. A figura 5 mostra os 16 EEs, onde cada um deles foi denominado seqüencialmente de EE-1 até EE-16.

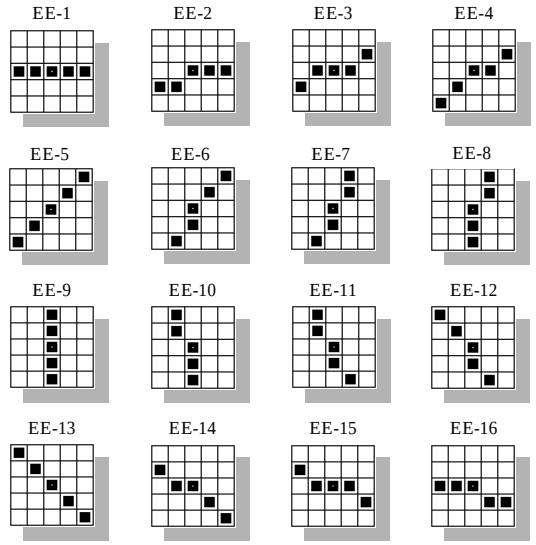

Figura 5: Os 16 elementos estruturantes para extração da inclinação dos traços da imagem

Os 16 EEs escolhidos representam segmentos de retas compostos de cinco pixels. Cada um desses EEs representa uma inclinação diferente.

Seguindo o mesmo princípio descrito na extração da inclinação dos contornos operações de erosão através dos EEs de 1 a 16 são utilizados para detectar a inclinação dos traços da imagem.

Logo, para uma imagem *A*, toma-se um EE e se executa a operação de erosão. Sobre a imagem resultante *B* é feita a contagem de todos os seus pixels. O número de pixels de *B* indica quantas vezes aquele EE esteve contido na imagem *A*. Essa operação é repetida para cada um dos 16 EEs, sempre tomando a imagem da assinatura A como entrada.

Dessa forma, os elementos que compõe o vetor desta característica é o número de pixels resultante da operação de erosão para cada um dos 16 EEs por quadro apresentados na figura 5.

3) Característica de correlação

O vetor de característica de correlação é composto de 5 elementos por quadro. O valor de cada elementos deste vetor é computado fazendo a sobreposição de uma imagem de teste sobre uma imagem de referência que chamaremos de *template*. O *template* por sua vez, foi previamente obtido fazendo a soma pixel a pixel de 5 imagens genuínas de um sinal gráfico de uma mesma pessoa. A composição dos elementos deste vetor são descritos a seguir:

1. Número de pixels pretos da imagem em teste
2. Numero de pixels que fazendo a sobreposição entre a imagem em teste e o *template* são brancos em ambas imagens
3. Número de pixels que fazendo a sobreposição entre a imagem em teste e o *template* são pretos em ambas imagens
4. Número de pixels que fazendo a sobreposição entre a imagem em teste e o *template* são pretos na imagem teste mas são brancos no *template*
5. Número de pixels que fazendo a sobreposição entre a imagem em teste e o *template* são brancos na imagem teste mas são pretos no *template*

C. Classificador

Seja o valor do elemento *i* do vetor de características **x** com *d* elementos, onde *i* = 1 a *d*. Seja o valor médio do elemento *i* de um conjunto de vetores de características **x**, e seja o valor do desvio padrão do elemento *i* do mesmo conjunto de vetores de características **x**. A distância padrão entre o um vetor características **x** e o vetor de características médio **m**, é dada por:

$$p(\mathbf{x},\mathbf{m}) = \sqrt{\left[\frac{x_1 - m_1}{s_1}\right]^2 + \left[\frac{x_2 - m_2}{s_2}\right]^2 + \ldots + \left[\frac{x_d - m_d}{s_d}\right]^2} \qquad (1)$$

Essa distância tem a importante propriedade de ser invariante a escala. Isso significa que ao utilizarmos essa medida, a ordem de grandeza dos elementos que compõem o vetor contribuem de forma equivalente no cálculo da distância.

Para classificar um sinal gráfico em verdadeiro ou falso segundo uma distância padrão encontrada, se faz necessário definir um limiar de decisão T_0. No caso em que a distância padrão encontrada for menor do que o limiar de decisão escolhido, o sinal gráfico é considerado verdadeiro (equação 2). No caso em que a distância padrão encontrada for superior do que o limiar de decisão, o sinal gráfico é considerado falso.

$$\text{se} \begin{cases} p(\mathbf{x},\mathbf{m}) < T_0 \Rightarrow \text{Verdadeira} \\ p(\mathbf{x},\mathbf{m}) > T_0 \Rightarrow \text{Falsa} \end{cases} \qquad (2)$$

V. IMPLEMENTAÇÃO DO MÉTODO PROPOSTO

Sistemas de autenticação automáticos através de características biométricas necessitam comparar um registro ou uma amostra biométrica previamente cadastrada e armazenada numa base de dados, com uma amostra biométrica de teste para decidir se esta última é genuína ou não. No caso específico do método proposto, as informações de referência associadas a determinado usuário (ID) são previamente adquiridas e armazenadas numa base de dados.

Na figura 6 observamos o esquema de cadastramento e geração do registro contendo as informações de referência de um determinado usuário.

Para calcular os vetores de médias, os vetores de desvios padrões, a imagem média *template* e os valores da altura nas resoluções 128 e 256 são utilizados apenas 5 amostras

genuínas de um mesmo indivíduo.

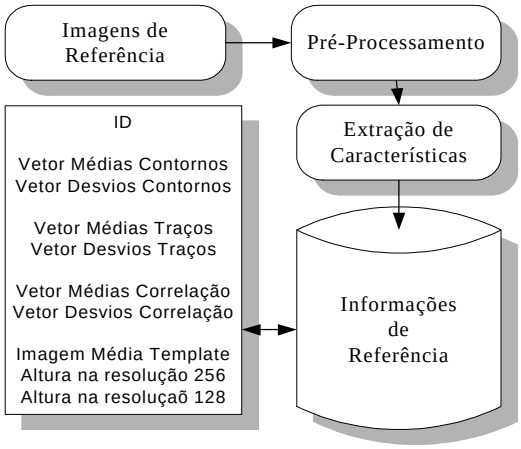

Figura 6: Esquema do cadastramento e conteúdo das informações de referência

A figura 7 apresenta o esquema de autenticação pessoal utilizado para realizar os testes de desempenho das características que fazem parte do algoritmo de autenticação pessoal.

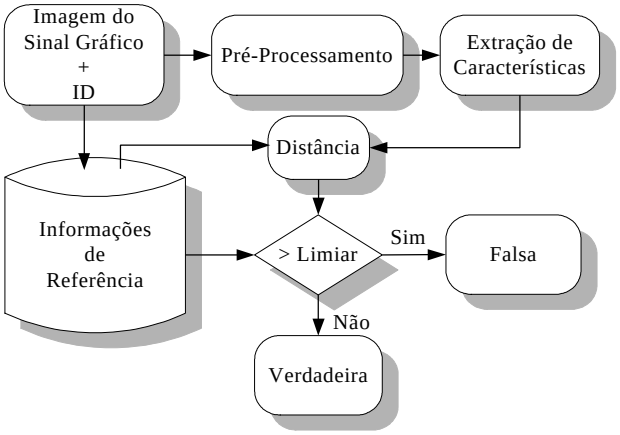

Figura 7: Esquema de autenticação de identidade

No esquema da figura 7 observamos que o inicio do processo de autenticação se dá pela entrada de uma imagem de sinal gráfico e seu respectivo identificador (ID). Com base no ID são extraídos da base de dados as "Informações de Referência" desse identificador. A seguir a imagem do sinal gráfico é pré-processada, isto é, enquadrada, normalizada e dividida em quadros. Para cada um dos quadros são extraídos os vetores de características. Em seguida é calculada a distância padrão entre esses vetores e as informações de referência. Finalmente é feita a classificação da imagem em verdadeira ou falsa segundo um valor do limiar de decisão.

Nos experimentos realizados o limiar de decisão T_0 é variável. Iniciando em 0 e terminando no maior valor possível associado a esse experimento. Desta forma pode-se levantar os valores que apresentam as taxas dos erros de falsa rejeição (EFR), falsa aceitação (EFA) e taxa de erros iguais (TEI).

VI. EXPERIMENTOS

O experimento 1 foi realizado utilizando-se as 40 classes de assinaturas verdadeiras em conjunto com as 50 assinaturas falsas. O objetivo deste experimento era determinar o poder de discriminação de cada uma das 3 características isoladamente. Os resultados deste experimento estão apresentados na Tabela I.

TABELA I
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 1

Característica	EFR(%)	EFA(%)	TEI(%)
Contornos	7,4	5,6	3,0
Traços	19,2	11,2	5,9
Correlação	10,3	7,2	6,0

O experimento 2 foi realizado utilizando-se as 40 classes de assinaturas verdadeira em conjunto com as 50 assinaturas falsas. O objetivo deste experimento era determinar qual seria o desempenho do método ao se utilizar a multiplicação das distâncias obtidas pelas características de contorno e de traços, isto é:

$$p_{final} = p_{contorno} * p_{traços} \quad (3)$$

O resultado deste experimento pode ser observado na tabela II.

TABELA II
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 2

EFR(%)	EFA(%)	TEI(%)
4,8	3,6	1,5

O experimento 3 foi realizado utilizando-se as 40 classes de assinaturas verdadeira em conjunto com as 50 assinaturas falsas. O objetivo deste experimento era determinar qual seria o desempenho do método ao se utilizar a multiplicação das distâncias padrões das características da inclinação dos contornos, da inclinação dos traços e a característica de correlação isto é:

$$p_{final} = p_{contorno} * p_{traços} * p_{correlação} \quad (4)$$

O resultado deste experimento pode ser observado na tabela III.

TABELA III
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 3

EFR(%)	EFA(%)	TEI(%)
2,4	1,2	0,7

Da analise do resultado do experimento 3 constatamos que a classificação de sinais gráficos utilizando a equação 4 baixou consideravelmente as taxas de erros. Assim sendo, decidimos utilizar nos experimentos 4, 5 e 6 esse mesmo classificador.

O experimento 4 foi realizado utilizando-se as 20 classes de símbolos manuscritos em conjunto com os 57 símbolos

manuscritos que não pertenciam a classe que estava em teste. O resultado deste experimento é mostrado na tabela IV.

TABELA IV
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 4

EFR(%)	EFA(%)	TEI(%)
1,9	1,5	0,9

O experimento 5 foi realizado utilizando-se as 20 classes de símbolos manuscritos em conjunto com as 50 assinaturas falsas. O resultado deste experimento pode ser observado na tabela V.

TABELA V
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 5

EFR(%)	EFA(%)	TEI(%)
0	0	0

O experimento 6 foi realizado utilizando-se as 20 classes de símbolos manuscritos mais as 40 classes de assinaturas verdadeiras em conjunto com os 57 símbolos manuscritos que não pertencem a classe que está em teste mais as 50 assinaturas falsas. O resultado deste experimento pode ser observado na tabela VI.

TABELA VI
TAXAS DE ERROS MÉDIOS NO EXPERIMENTO 6

EFR(%)	EFA(%)	TEI(%)
2,5	1,9	0,7

VII. ANÁLISE DOS RESULTADOS

Os experimentos 1, 2 e 3 serviram para avaliar o poder de discriminação das características e do classificador utilizado. Como o método proposto visa extrapolar a utilização de imagens de assinaturas para a autenticação, estes primeiros testes utilizam apenas imagens de assinaturas na sua realização. Os resultados obtidos comprovam que nossa abordagem obtém um bom desempenho junto a essas imagens, onde as menores taxas de erros de falsa rejeição e falsa aceitação foram de 2,4% e 1,9% quando foi utilizado a equação 4 como classificador.

Os experimentos 4, 5 e 6 passam a utilizar símbolos manuscritos em conjunto com assinaturas. Da analise dos resultados observamos que as taxas de erros obtidas pelo método continuam em patamares pequenos. No caso particular do experimento 5, a classe composta exclusivamente por símbolos foi completamente separada da classe composta apenas por assinaturas. O teste 6 foi a experiência mais geral com relação a composição das classes verdadeiras e falsas. Nesse experimento, as taxas de erros obtidas mantiveram-se muito próximas de aquelas previamente alcançadas no experimento 3, o que mais uma vez comprova que a abordagem utilizada é efetiva atingindo um dos nossos objetivos principais que é o de generalizar a autenticação pessoal por imagens de assinaturas.

VIII. CONCLUSÕES

O objetivo deste trabalho foi propor um método automático de autenticação pessoal através de qualquer sinal gráfico manuscrito, extrapolando a idéia de utilizar imagens de assinaturas na execução da tarefa.

Foi apresentado o conceito de senha gráfica, a qual poderia substituir ou em conjunto com as senhas de texto, aumentar o grau de segurança nas tarefas de *login* em sistemas de computação.

O método apresentado é de simples implementação, eficiente, robusto, exige pouco poder de processamento e utiliza apenas 5 amostras biométricas para gerar o registro de cadastramento.

Dos experimentos realizados concluímos que o método apresentado é eficiente frente a falsificações de sinais gráficos onde o impostor não conhece previamente maiores detalhes da imagem que autentica o indivíduo genuíno.

O método proposto utiliza um classificador linear simples, ao contrário de outros sistemas que se servem de classificadores mais complexos. Desta forma, nosso método leva apenas alguns segundos para ser treinado, ao contrário de outros nos quais a etapa de cadastramento pode ser muito demorada, como aqueles que utilizam Cadeias de Markov, Redes Neurais ou Algoritmos Genéticos.

A taxa de erro médio de falsa rejeição igual a 2,5% e a taxa de erro médio de falsa aceitação igual a 1,9% mostrados na tabela VI, se encontram na margem inferior do conjunto de valores entre 2% e 5% que segundo Plamondon e Srihari em [6] afirmam serem as taxas de erro apresentadas pela maioria de sistemas automáticos de autenticação pessoal por imagens de assinaturas.

REFERÊNCIAS

[1] L. L. Lee, Miguel G. Lizárraga, *Biometrics on internet: Security Applications and Services*, Incluído no livro - *Biometrics Solutions for Authentication in an E-World* - Editora Klewer Academic Publisher, 2002

[2] L. L. Lee, Miguel G. Lizárraga, "The Personal Identification Network: Biometric System: Part I", *XIX Simpósio Brasileiro de Telecomunicações* - SBT, Fortaleza - CE, Setembro 2001

[3] M. C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", *Electronics and communication engineering journal*, pp. 273 - 280, December, 1997

[4] H. Cardot, M. Revenu, B. Victorri, M. Revillet, "A static signature verification system based on a cooperative neural network architecture", *Int. Journal of Pattern Recognition and Art. Intelligence*, Vol 8, No 3, pp. 679 - 692, 1994

[5] Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin. "The Design and Analysis of Graphical Passwords" *In Proceedings of the 8th USENIX Security Symposium*, August, Washington DC, pp. 1 – 14, 1999

[6] Rejean Plamondon, Sargur Srihari, "On-line and offline Handwriting Recognition: A comprehensive survey*"; IEEE Trans. on PAMI*, Vol 22, No. 1, pp. 63 – 84, 2000