AUTENTICAÇÃO PESSOAL POR IMAGENS DE SINAIS GRÁFICOS

Miguel Gustavo Lizárraga e Lee Luan Ling

Resumo - Neste trabalho é proposto um método automático de autenticação pessoal baseado em imagens compostas por traços manuscritos representando símbolos, palavras, assinaturas ou desenhos. O método apresentado é de simples implementação, eficiente, robusto, exige pouco poder de processamento e utiliza apenas cinco amostras de sinais gráficos para gerar o registro de cadastramento. Tais características permitem sua utilização na autenticação de usuários em tempo real com aplicações diretas no controle de acesso a recursos de redes de computadores e em dispositivos móveis. O método de autenticação foi avaliado em processos de verificação e identificação. Na verificação utilizou-se falsificações aleatórias e habilidosas, e na identificação empregou-se três configurações diferentes de bases de dados. A menor taxa de erros iguais no processo de verificação foi de 0,7 %, enquanto que a maior taxa de classificação correta no processo de identificação foi de 93,7 %.

Palavras-chave: biometria, manuscritos, autenticação pessoal, processamento de imagens.

Abstract - In this work is proposed a personal authentication method based on images composed of handwritten strokes that may represent symbols, words, signatures or any kind of drawings. This method is efficient, robust and can be easily implemented, requiring low CPU processing power and needs only five handwritten signal samples for enrollment. Those issues allow the proposed method to be suitable for real time authentication systems and control access applications. The authentication method has been evaluated under both verification and identification processes. In verification experiments random and skilled forgeries were used, while in identification experiments three different database configurations were setup. Performance of 0.7 % equal error rate and that of 93.7 % correct classification rate were achieved in the verification and identification processes, respectively.

Keywords: biometrics, handwriting, personal authentication, image processing.

1. INTRODUÇÃO

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

A comprovação da identidade pessoal 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 permita a autenticação, como por exemplo, um cartão de identidade ou 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).

Atualmente, a maioria dos casos de autenticação pessoal recaem sobre as duas primeiras maneiras, ou seja, memorizando números de identificação incluindo senha do cartão bancário ou *login* do computador, número de RG, passaporte, CPF e vários outros. Ou ainda, apresentando documentos de identificação, como por exemplo, carteira de identidade, carimbos, selos, cartões e chaves. Porém, esses métodos não são 100% confiáveis, pois 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 fundamentadas na terceira maneira, ou seja, baseadas em medidas biométricas, onde se entende como medida biométrica à mensuração de atributos/características físicas ou de comportamento de uma pessoa com o objetivo de distinguí-la dentre as demais.

A escolha de uma característica biométrica física para implementação de um sistema de autenticação pode gerar amplos debates quanto a sua utilização, eficácia, confiabilidade e praticidade. Entretanto, com relação à escolha de características biométricas de comportamento, existe uma ampla aceitação e consenso quanto à utilização de sinais manuscritos para sua implementação. Dentre as vantagens mais significativas nesse tipo de sistema podemos destacar [4]:

- 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 comparadas com outras técnicas, como por exemplo, 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).

Este trabalho tem como principal objetivo o desenvolvimento de um método de autenticação simples, robusto, com baixa complexidade computacional,

Miguel Gustavo Lizárraga[1] é pesquisador Faculdade de Engenharia Elétrica e de Computação da UNICAMP. Lee Luan Ling[2] é professor da UNICAMP. Endereço: DECOM – FEEC – UNICAMP, Caixa Postal 6101, Campinas, SP, CEP 13081-970. E-mails: [1]lizarrag@bol.com.br e [2]lee@decom.fee.unicamp.br.

necessitando de poucas amostras biométricas para gerar o registro do cadastramento e com taxas de erros próximas a zero. O método de autenticação proposto está baseado na característica biométrica associada à forma como uma pessoa escreve ou desenha, assim sendo, esta característica é considerada de comportamento porque utiliza um processo neuro-motor traduzindo-se na escrita humana, que por sua vez está associada a um conjunto de variáveis relacionadas ao estado emocional de cada pessoa no momento da escrita [3].

2. SENHAS GRÁFICAS

A autenticação pessoal por imagens de sinais manuscritos é uma evolução natural da autenticação pessoal por imagens de assinaturas, onde se entende por sinais manuscritos qualquer imagem que seja composta por traços, como por exemplo, desenhos, emblemas, palavras manuscritas, símbolos, caracteres, dentre outros. 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 [5] diz que as assinaturas ocidentais podem ser divididas em dois grandes grupos. O primeiro é aquele onde a assinatura da pessoa é simplesmente a escrita do seu nome em letra cursiva (ver Figura 1a), sendo por conseguinte geralmente 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, fazendo com que na maioria das vezes o nome escrito fique ilegível (ver Figura 1b).

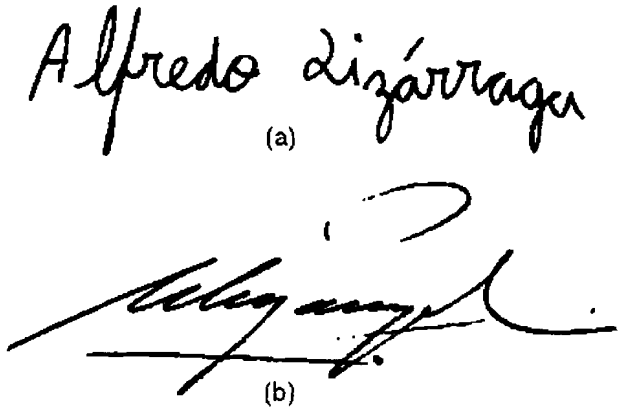


Figura 1. (a) Assinatura legível; (b) Assinatura ilegível.

Entretanto, além das assinaturas ocidentais (legíveis ou não) nas quais se utiliza o alfabeto romano, existem as assinaturas escritas 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, europeus, orientais, árabes ou latinos não é uma boa abordagem, pois 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. O contrário também é verdadeiro, isto é, para alguém que não conhece o alfabeto romano a assinatura representada na Figura 1a será considerada ilegível.

Assim sendo, desenvolvemos um algoritmo que emprega técnicas que levam em consideração características não associadas ao tipo de alfabeto ou à escrita, isto é, características relacionadas exclusivamente com a distribuição e forma dos traços que compõem o sinal manuscrito.

Algumas das observações que nos motivaram a desenvolver um algoritmo de autenticação baseado em símbolos ou sinais manuscritos e não em assinaturas estão relacionados a seguir:

- Ao invés de usarmos nossa assinatura, podemos utilizar simplesmente uma rubrica, a qual pode ser mais simples e rápida de escrever;
- 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.

Fundados nessas observações vemos a utilização de imagens de sinais manuscritos para autenticação pessoal como uma forma de introduzir o conceito de senhas gráficas. Definimos senhas gráficas como imagens compostas por traços manuscritos que podem ser freqüentemente repetidos por uma pessoa mantendo uma pequena variabilidade na sua forma e estilo. As senhas gráficas, da mesma forma que senhas clássicas baseadas na digitação de texto num 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% dos *login*/senhas utilizando dicionários cujas palavras estão disponíveis na Internet [6]. Isto se deve ao fato do ser humano ter uma limitação para o armazenamento de seqüências de letras ou números. Assim, o que fazemos é guardar na nossa memória poucas senhas e as reutilizamos em vários sistemas. Ou ainda, utilizamos senhas fáceis de lembrar, como datas de nascimento, nomes ou mnemônicos que possuam algum contexto dentro da nossa vida. Isto pode ser verificado através do teste que se segue:

Leia o conjunto letras a seguir, feche os olhos e tente lembrar de todas elas na seqüência correta:

O I R A S R E V I N A Z I L E F

Provavelmente não foi possível lembrar de todas elas. Agora leia a mesma seqüência de letras de trás para frente. De repente ficou muito fácil se lembrar da seqüência completa, pois se encontra num contexto familiar [7].

Por outro lado, mesmo com o desenvolvimento de interfaces gráficas muito amigáveis, seja em ambientes Windows, Macintosh ou GUIs do Linux como KDE, Gnome, Window Maker, entre outras, a forma como nos é

permitido o acesso aos recursos do computador são as mesmas de 30 anos atrás:

> Nome do Usuário:
> Senha:

E se por algum motivo cometemos um erro na inserção de nossos dados, ainda aparece:

> Login Incorreto – Tente Novamente:

E existem outras mensagens que em si são muito desagradáveis:

> Sua senha expirou !
> Por favor escolha uma nova senha:
> Digite a senha novamente:

Assim sendo, propomos a utilização de senhas gráficas baseadas em desenhos de sinais manuscritos para realizar o *login* em sistemas de redes de computadores, as quais se sirvam dos recursos e interfaces gráficas que os atuais sistemas operacionais proporcionam.

A amostra de uma possível tela de *login* utilizando senhas gráficas como propõe este trabalho pode ser visualizada na Figura 2. Note ainda que além de modernizar o processo de aquisição de informações dos usuários, a utilização de senhas gráficas elimina a possibilidade do ataque de hackers através do uso de dicionários.

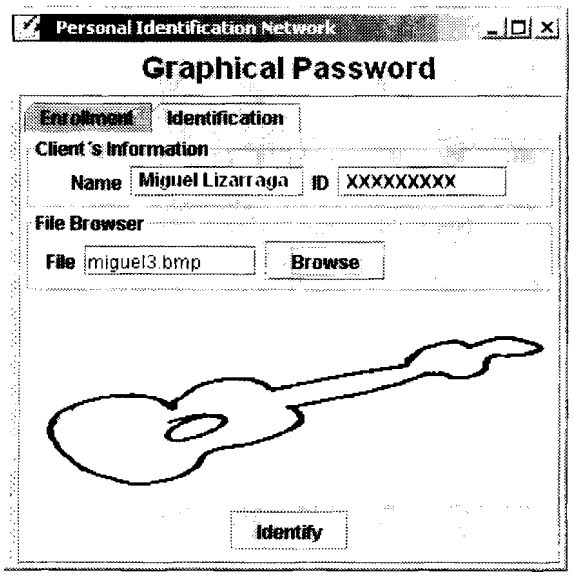


Figura 2. Autenticação por senhas gráficas.

3. BASE DE DADOS

As imagens que fazem parte da base de dados utilizadas neste trabalho são formadas por sinais manuscritos divididos em dois tipos. O primeiro tipo é chamado de *Assinaturas* e é composto por imagens como as mostradas na Figura 1, as quais por sua vez sub-dividimos em dois grupos: *Grupo de Assinaturas Verdadeiras* e *Grupo de Assinaturas Falsas*. O segundo tipo é denominado de *Símbolos* e também foi sub-dividido em dois grupos: *Grupo de Símbolos Verdadeiros* e *Grupo de Símbolos Falsos Habilidosos*. Algumas imagens pertencentes ao grupo dos *Símbolos* podem ser vistas na Figura 3.

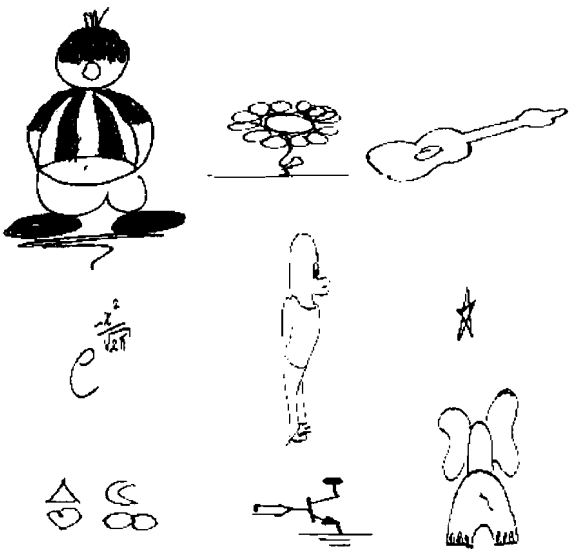


Figura 3. Amostras de símbolos gráficos.

As imagens das *Assinaturas* e *Símbolos* ficam restritas a uma área retangular de 10 cm de comprimento por 8 cm de altura. Na digitalização das imagens foi utilizada uma resolução de 200 pontos por polegada. O instrumento de escrita foi uma caneta com tinta de cor preta e diâmetro de ponta 0,5 mm.

Os grupos em que *Assinaturas* e *Símbolos* foram sub-divididos são apresentados em detalhes, a seguir:

- *Grupo de Assinaturas Verdadeiras* (*AV*): Este grupo é composto por um total de 1200 imagens. As assinaturas foram obtidas junto a 40 pessoas, sendo que cada uma delas contribuiu com 30 assinaturas. A partir de uma inspeção visual dos 40 diferentes estilos de assinaturas foi encontrado que 15 são legíveis e 25 ilegíveis (baseado no alfabeto romano).
- *Grupo das Assinaturas Falsas* (*AF*): Este grupo é composto por um total de 50 assinaturas adquiridas de 50 pessoas diferentes e que não pertencem ao grupo das pessoas que forneceram as assinaturas verdadeiras.
- *Grupo dos Símbolos Verdadeiros* (*SV*): 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.
- *Símbolos Falsificados Habilidosos* (*SH*): Este grupo é composto de 150 imagens adquiridas a partir de 15 pessoas diferentes igualmente separadas em 5 grupos. Cada grupo fica encarregado de falsificar um símbolo verdadeiro, sendo que cada pessoa só pode falsificar 10 vezes um mesmo símbolo. Isto significa que 5 símbolos verdadeiros foram falsificados com um total de 30 amostras de cada um. É importante ressaltar que os falsificadores só podiam reproduzir o símbolo olhando para ele, ou seja, não lhes foi permitido que calcassem a imagem.

4. MÉTODO PROPOSTO

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

4.1 PRÉ-PROCESSAMENTO DAS IMAGENS

Todas as imagens pertencentes à base de dados foram digitalizadas em preto e branco. Assim, as imagens podem ser vistas como uma função $f(x, y) \in \{0,1\}$, onde x = 0, 1, 2 ... M, y = 0, 1, 2 ... N, onde M é a largura e N a sua altura da imagem em pixels. Os traços manuscritos da imagem são definidos como pixels pretos (valor 1) e o fundo da imagem como pixels brancos (valor 0).

Com o objetivo de tratar as imagens e deixá-las num formato que minimize a variabilidade intra-pessoal e maximize a variabilidade inter-pessoal, dividimos o pré-processamento das 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.

4.1.1 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 encontrar o menor quadrilátero que contenha os traços manuscritos.

4.1.2 NORMALIZAÇÃO DE TAMANHO

Com relação à taxa de amostragem com que as imagens foram digitalizadas, Qi e Hunt em [11] afirmam não ser interessante a utilização de resoluções nem muito baixas, nem muito altas. Numa resolução baixa, o método de autenticação tende a errar pela falta de poder de discriminação, principalmente quando se trabalha na distinção entre uma imagem verdadeira e sua correspondente falsificação habilidosa. Em contrapartida, numa resolução alta o método pode rejeitar equivocadamente assinaturas e sinais gráficos genuínos, por causa da inclusão de desvios, nuances e pequenos detalhes nos traços manuscritos que passam a existir devido à elevada amostragem feita sobre a imagem.

O processo de normalização de tamanho tem como finalidade redimensionar a quantidade de pixels no eixo horizontal e vertical de sinal gráfico previamente enquadrado, para assim minimizar a dependência da resolução com a qual a imagem foi originalmente digitalizada. Neste processo, cada sinal gráfico gerará duas imagens de tamanhos diferentes as quais de fato serão utilizadas no processo de extração de características. Esta normalização é feita em duas etapas, a primeira consiste em definir a dimensão no eixo horizontal e na segunda etapa é feita uma média para se calcular o valor da dimensão do eixo vertical. O processo de normalização de tamanho só está completo quando os dois estágios forem executados. A seguir uma explicação mais detalhada sobre os dois estágios será apresentada.

Estágio de Normalização no Eixo Horizontal: Tanto no cadastramento e na verificação/identificação, 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 dos vetores de 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.

Estágio de Normalização no Eixo Vertical: No processo de cadastramento, o valor 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. Exemplificando, para um conjunto de 5 sinais gráficos normalizados em 128 pixels no eixo horizontal, teríamos por exemplo os valores de 60, 80, 116, 90 e 80 nos respectivos eixos verticais (mantendo o *aspect ratio*). O valor inteiro da média desses valores é 85. Assim sendo, a normalização final para todas as imagens seria de 128 por 85 pixels, neste caso o *aspect ratio* não é mais mantido. No processo de verificação/identificação, o tamanho do eixo vertical será definido pelo valor anteriormente obtido no processo de cadastramento.

A Figura 4 mostra uma representação visual do processo de normalização de tamanho, no qual a título de exemplificação utilizamos apenas 3 sinais gráficos como base da normalização.

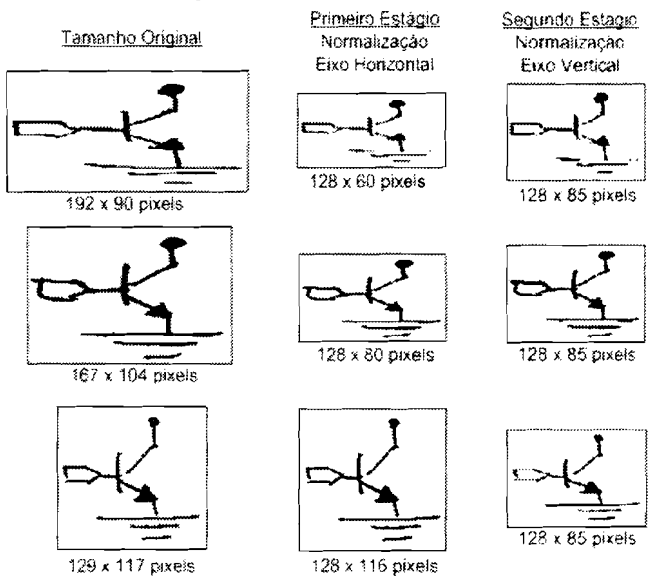


Figura 4. Os dois estágios do processo de normalização de tamanho de um sinal gráfico.

4.1.3 DIVISÃO EM QUADROS

Em um de nossos trabalhos anteriores [8], é introduzido um esquema de divisão de imagens de assinaturas em 5 quadros, como mostrado na Figura 5. Tal esquema somente é uma boa abordagem para imagens que possuem *aspect ratio* maior que 2:1, ou seja, quando a largura da imagem no eixo horizontal é duas vezes maior do que a altura do seu eixo vertical. Para assinaturas ocidentais este fato é na maioria das vezes verdade, porém para qualquer sinal gráfico isto nem sempre se cumpre. A seguir, apresentamos uma nova abordagem para divisão de imagens, onde a imagem é repartida em quatro quadros e cada quadro possui uma sobreposição de 50% entre ele e seu adjacente.

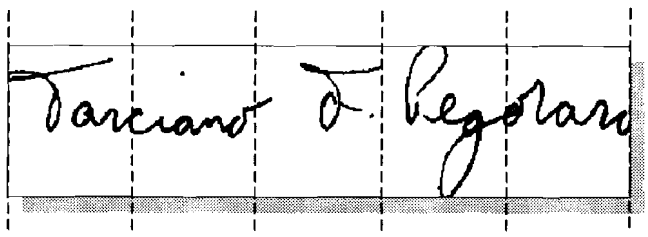
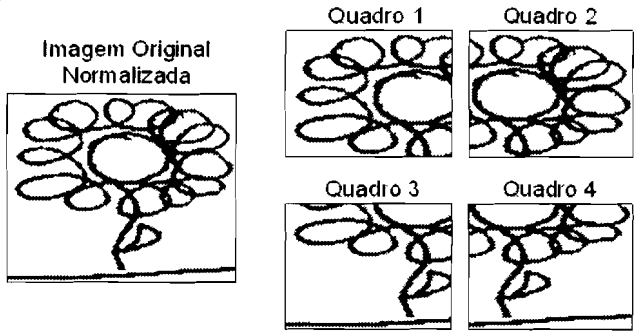
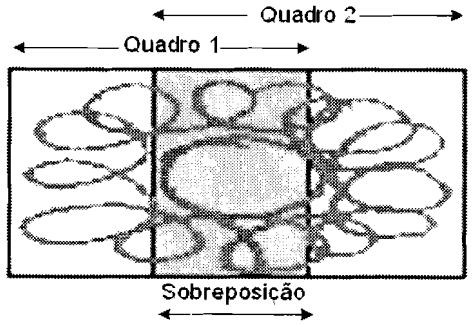


Figura 5. Assinatura dividida em 5 quadros.

Divisão da imagem em quatro 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 os vetores que carreguem consigo informações locais da imagem. A Figura 6a mostra o novo esquema de divisão, no qual os quadros são obtidos repartindo a imagem vertical e horizontalmente. A Figura 6b apresenta um exemplo da sobreposição entre quadros adjacentes, em particular a sobreposição entre o quadro 1 e o quadro 2 de um sinal gráfico.



a) Divisão em Quadros



b) Sobreposição entre dois quatros adjacentes

Figura 6. a) Divisão de um sinal gráfico em 4 quadros. b) Sobreposição entre dois quadros.

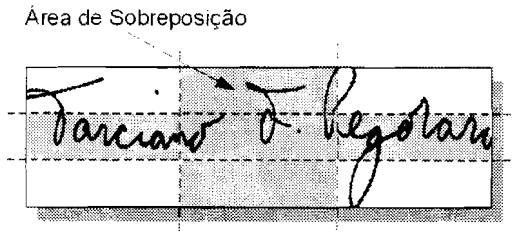


Figura 7. Área de sobreposição onde os traços do sinal gráfico se concentram.

A divisão de uma imagem em quatro quadros melhora o resultado da extração de características em assinaturas (ocidentais ou não) e em sinais gráficos, independentemente do seu *aspect ratio*. Isto ocorre por que a área de sobreposição entre os quatro quadros é a região onde a maioria dos traços dos sinais gráficos se concentram (ver Figura 7).

4.2 CARACTERÍSTICAS

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

1. Inclinação dos traços que compõem o sinal manuscrito
2. Inclinação do contorno do sinal manuscrito
3. Dados de correlação entre uma imagem de referência e a imagem em teste

A Figura 8 mostra graficamente os conceitos de traço e contorno de um sinal manuscrito. Nesta figura observamos que traços são compostos pelos pixels pretos que originalmente formam o sinal manuscrito e que o contorno é representado pelos pixels que fazem parte da borda externa dos traços após um processo de dilatação da imagem.

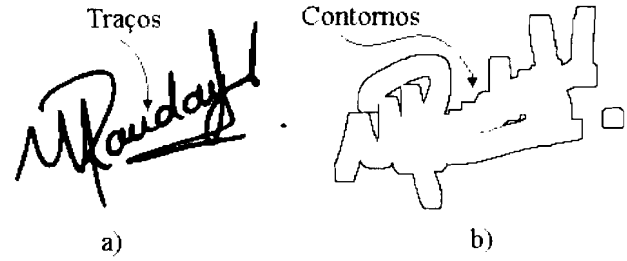


Figura 8. a) Traços de um sinal gráfico b) Contornos de um sinal gráfico.

4.2.1 EROSÃO MORFOLÓGICA COMO DETECTOR DE INCLINAÇÃO

A medida de inclinação dos traços de uma imagem é uma característica muito consistente e por este motivo é comumente utilizada na autenticação de escritor [9]. Em [10], por exemplo, quatro filtros direcionais foram aplicados a imagens de assinaturas para estimar sua forma. Em [11] um algoritmo baseado nas projeções vertical e horizontal foi utilizado para determinar a inclinação geral dos traços das imagens. Outros esquemas mais sofisticados estão descritos na literatura e podem ser utilizados para obter a inclinação dos traços manuscritos em imagens, como por exemplo, filtros de Gabor [12]. Entretanto, não é nosso objetivo desenvolver soluções complexas visto que a abordagem de nosso método visa a simplicidade de sua implementação. Assim sendo, aplicamos conceitos de Morfologia Matemática (MM) sobre imagens binárias que permitem combinar um conjunto simples de operações para resolver problemas complexos em processamento de imagens [13]. As duas operações básicas da MM são dilatação e erosão.

Dilatação Morfológica: Esta operação envolve uma imagem binária f a qual é processada por um elemento estruturante g. A dilatação morfológica pode ser considerada como uma operação onde um elemento estruturante (EE) é transladado sobre cada pixel de um objeto, em nosso caso os traços do sinal gráfico. Se a interseção entre o EE transladado e o objeto (traços) não for vazio, então o pixel corrente recebe o valor 1. Seja $z=(z_1,z_2)$ o pixel corrente e g_z representa o EE transladado, isto é, g tem sua origem centrada em z. Desta forma, a operação de dilatação sobre uma imagem é definida como:

$$\partial_g(f)=\{z \mid g_z \cap f \neq \varnothing\} \quad (1)$$

Erosão Morfológica: De forma semelhante à dilatação morfológica, a operação de erosão envolve o translado de um elemento estruturante g sobre cada pixel da uma imagem binária f, que em nosso caso contém os traços do sinal gráfico. Se o EE transladado está completamente contido nos traços, então o pixel corrente recebe o valor 1. A operação de erosão sobre uma imagem é definida como:

$$\varepsilon_g(f)=\{z \mid g_z \subset f\} \quad (2)$$

A operação da morfologia matemática utilizada para detectar a inclinação dos traços nos sinais gráficos foi a erosão morfológica. A seguir será mostrado que utilizando determinados elementos estruturantes (EEs) numa operação de erosão, é possível detectar a inclinação dos traços e contornos de um sinal gráfico. Para explicar a detecção da inclinação mais intuitivamente nos serviremos da Figura 9.

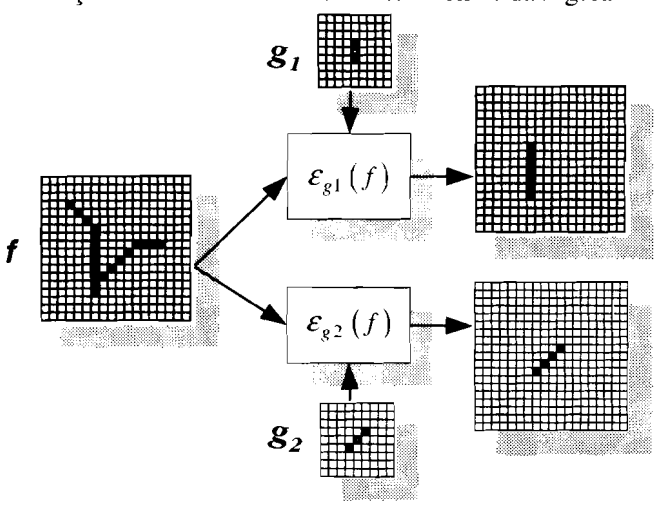


Figura 9. Exemplo de uma imagem erodida.

A Figura 9 mostra a aplicação de uma erosão executada pelos elementos estruturantes g_1 e g_2 sobre uma imagem genérica f. Quando g_1 é aplicado em f, na imagem resultante apenas são mapeados sete pixels pretos. Observa-se que os pixels de f que possuem inclinação diferente da apresentada pelo EE g_1 não foram mapeados. Se um outro EE é utilizado, por exemplo g_2, e uma nova erosão morfológica for executada sobre f, serão mapeados quatro pixels na imagem resultante. Neste caso, o segmento mapeado é mais uma vez composto pelos pixels com a mesma inclinação do EE utilizado. Assim, para detectar qualquer direção de algum traço em particular basta utilizar o EE adequado.

Uma vez que os pixels são mapeados na imagem resultante, esses pixels são contados e o resultado dessa contagem será um dos elementos do vetor de características. Por exemplo, na imagem f da Figura 9 o vetor de inclinações possuirá dois elementos e seus valores serão 7 e 4, respectivamente.

4.2.2 INCLINAÇÃO DO CONTORNO DO SINAL MANUSCRITO

A operação de obtenção do contorno para uma imagem binária f pode ser feita através da diferença entre a imagem resultante da dilatação de f por um elemento estruturante g e a própria imagem f. Ou seja,

$$\beta_g(f)=\partial_g(f)-f, \quad (3)$$

onde g deve ser um EE adequado, sendo que em nosso caso é EE_DIL como apresentado na Figura 10a. Note que o contorno encontrado através desta operação é a fronteira externa da imagem com espessura de um pixel.

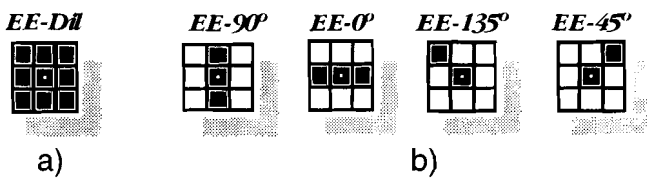


Figura 10. a) EE para dilatação b) EEs para extração da inclinação de contornos.

Para acharmos a inclinação da imagem do contorno, definimos os EEs que representam as inclinações de 90, 0, 135 e 45 graus, como mostrado na Figura 10b. Na notação utilizada, cada um dos EEs foi colocado numa grade 3 x 3 para facilitar sua representação. Os quadrados pretos dentro da grade indicam a presença de pixels pretos, enquanto os espaços em branco representam pixels brancos. Temos ainda que a coordenada (0,0) dessas imagens está representada pelo ponto branco dentro de um dos quadrados pretos.

Para a composição deste vetor de características foram seguidos os seguintes passos::

1. Para uma imagem f, primeiramente fazemos a operação de obtenção de seu contorno utilizando a equação (3), resultando numa imagem h;
2. Sobre h são efetuadas quatro erosões morfológicas independentes utilizando os EEs da Figura 10b. A contagem do número de pixels mapeados através de cada um desses EEs representa um elemento no vetor de características;
3. A imagem f do passo 1 é dilatada por EE_DIL. A imagem dilatada resultante passa a ser chamada de f;
4. Um novo ciclo é iniciado a partir do passo 1. O procedimento termina quando tiverem sido executados 5 ciclos.

A cada ciclo do procedimento quatro novos elementos do vetor de características de contorno são obtidos, gerando no final um conjunto de 20 elementos por quadro.

4.2.3 INCLINAÇÃO DOS TRAÇOS DO SINAL MANUSCRITO

Na extração das inclinações dos traços do sinal manuscrito são utilizados 16 elementos estruturantes. A Figura 11 mostra os 16 EEs, onde cada um deles foi denominado seqüencialmente de EE-1 até EE-16. Os 16 EEs escolhidos representam segmentos de retas compostos por cinco pixels. Cada um desses EEs representa uma inclinação diferente. A diferença entre a inclinação de EEs consecutivos é de aproximadamente 11 graus.

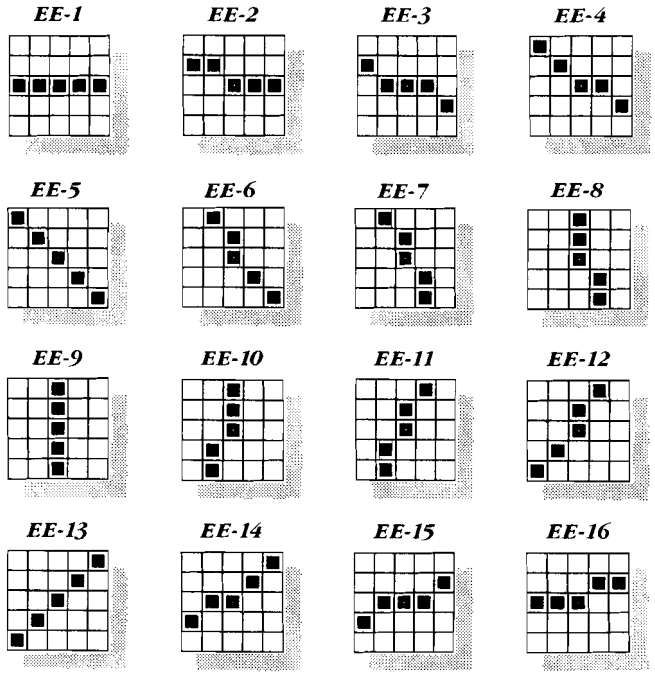


Figura 11. Os 16 elementos estruturantes para extração da inclinação dos traços da imagem.

Seguindo o mesmo princípio descrito seção 4.2.1, operações de erosão através dos EEs de 1 a 16 são utilizadas para detectar a inclinação dos traços presentes na imagem. Logo, para uma imagem *f*, toma-se um EE e se executa a operação de erosão. Sobre a imagem resultante *h* é feita a contagem de todos os seus pixels. O número de pixels de *h* indica quantas vezes aquele EE esteve contido na imagem *f*. Essa operação é repetida para cada um dos 16 EEs, sempre tomando a imagem da assinatura *f* como entrada. Dessa forma, os elementos do vetor desta característica são obtidos pela contagem do número de pixels resultante da operação de erosão feita com os 16 EEs apresentados na Figura 11, o que leva a um total de 16 elementos por quadro.

4.2.4 CARACTERÍSTICA DE CORRELAÇÃO

O vetor de características de correlação é composto de 5 elementos por quadro. O valor dos elementos deste vetor é computado efetuando a sobreposição dos quadros da imagem de teste sobre os quadros de uma imagem de referência que chamaremos de *template*. O *template* por sua vez, foi previamente obtido realizando a operação de união de 5 imagens genuínas do sinal gráfico de uma mesma pessoa. A composição dos elementos deste vetor é descrita a seguir:

1. Número de pixels pretos do quadro em teste;
2. Número de pixels que fazendo a sobreposição entre o quadro em teste e o quadro do *template* são brancos em ambos os quadros;
3. Número de pixels que fazendo a sobreposição entre o quadro em teste e o quadro do *template* são pretos em ambos os quadros;
4. Número de pixels que fazendo a sobreposição entre o quadro em teste e o quadro do *template* são pretos no quadro em teste mas são brancos no quadro do template;
5. Número de pixels que fazendo a sobreposição entre o quadro em teste e o quadro do *template* são brancos no quadro em teste mas são pretos no quadro do *template*.

4.3 CLASSIFICADOR

Seja o vetor médio **m** obtido pela média de 5 vetores de características **x** dado por

$$\mathbf{m} = \frac{1}{5}\sum_{k=1}^{5}\mathbf{x}_k , \tag{4}$$

e **s** o vetor de desvio padrão obtido a partir de **m** e os 5 vetores de características **x** dado por

$$\mathbf{s} = \sqrt{\frac{1}{5}\sum_{k=1}^{5}(\mathbf{x}_k - \mathbf{m})^2} . \tag{5}$$

Seja x_i, m_i e s_i os valores dos elementos *i* dos vetores de características **x**, médio **m** e desvio **s**, respectivamente. Temos que a distância padrão do vetor de teste da características **x** com relação à média e desvio padrão, é definida como

$$p(\mathbf{x},\mathbf{m},\mathbf{s}) = \sqrt{\left[\frac{x_1 - m_1}{s_1}\right]^2 + \left[\frac{x_2 - m_2}{s_2}\right]^2 + \ldots + \left[\frac{x_d - m_d}{s_d}\right]^2} , \tag{6}$$

onde *d* é o número máximo de elementos desses vetores.

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

Para classificar um sinal gráfico em verdadeiro ou falso segundo uma distância padrão encontrada, é necessário escolher um limiar de decisão T_0. No caso em que a distância padrão encontrada for menor que o limiar de decisão escolhido, o sinal gráfico é considerado verdadeiro. No caso em que a distância padrão encontrada for superior ao limiar de decisão, o sinal gráfico é considerado falso (Equação 7).

$$\text{se} \begin{cases} p(\mathbf{x},\mathbf{m},\mathbf{s}) < T_0 \Rightarrow \text{Verdadeira} \\ p(\mathbf{x},\mathbf{m},\mathbf{s}) > T_0 \Rightarrow \text{Falsa} \end{cases} \tag{7}$$

5. IMPLEMENTAÇÃO DO MÉTODO PROPOSTO

Sistemas automáticos de autenticação pessoal através de características biométricas necessitam comparar um registro ou padrão biométrico previamente cadastrado com uma amostra biométrica de teste para decidir se a mesma é genuína ou não. No caso específico do método proposto, as *Informações de Referência* (*IR*) associadas a determinado usuário são previamente adquiridas e armazenadas numa base de dados.

Na Figura 12 observamos o esquema de cadastramento e geração do registro contendo as *IR* de um determinado usuário. As *IR* são compostas de vetores contendo as médias e desvios padrões da inclinação dos contornos, da inclinação dos traços e da correlação, além da imagem *template* e os valores de altura para a normalização de tamanho de 128 e 256 pixels. Estas informações são obtidas utilizando-se 5 amostras genuínas de um mesmo indivíduo.

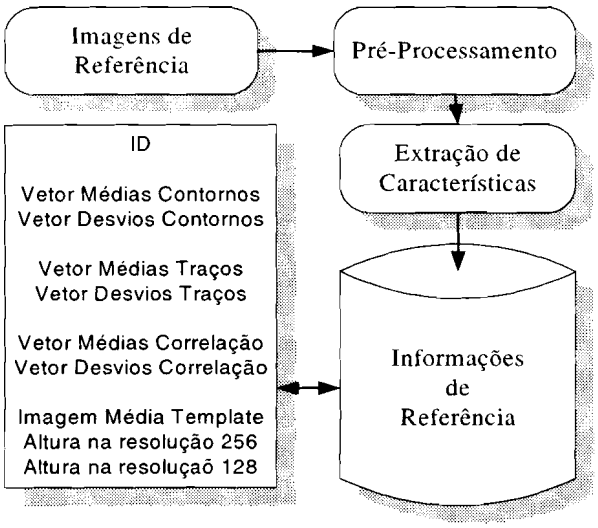


Figura 12. Esquema do cadastramento e conteúdo das informações de referência.

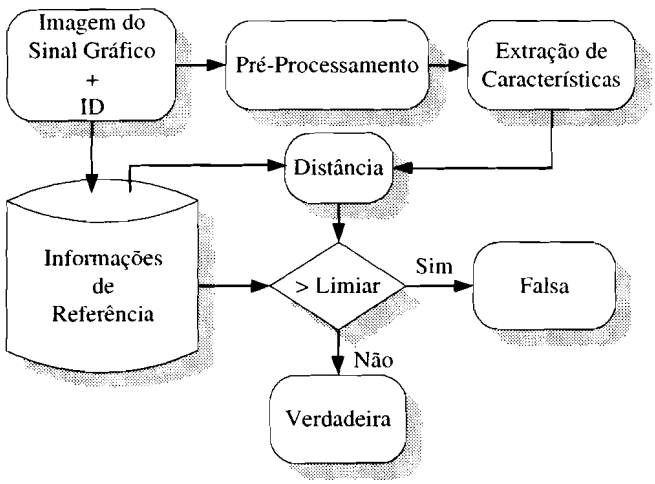


Figura 13. Esquema de autenticação de identidade.

A Figura 13 apresenta o esquema de autenticação pessoal utilizado para realizar os testes de desempenho das características que fazem parte do método de autenticação proposto. Nesse esquema observamos que o início do processo de autenticação ocorre após a entrada da imagem do sinal gráfico. Se a autenticação é um processo de verificação, é necessário apresentar também um identificador (ID). Utilizando-se o ID extrai-se da base de dados as IR 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 IR. Finalmente é feita a classificação da imagem em verdadeira ou falsa segundo o valor do limiar de decisão.

Por outro lado, se a autenticação é um processo de identificação, somente o sinal gráfico de entrada é necessário. O sinal gráfico é pré-processado para realizar-se a extração de seus respectivos vetores de características. A seguir, é calculada a distância padrão entre seus vetores e todas as IR armazenadas na base de dados. A menor distância encontrada entre as IR passará por um limiar de decisão. Se essa distância for menor que o limiar, a pessoa é identificada com sucesso, caso contrário, o sistema rejeitará a autenticação.

5.1 PARÂMETROS PARA ANÁLISE DE DESEMPENHO

O desempenho dos processos de verificação/identificação é medido de acordo com as taxas de erro de falsa rejeição (**EFR**) e falsa aceitação (**EFA**). O EFR é probabilidade do sistema incorretamente indicar que um sinal gráfico é falso, quando de fato é verdadeiro. Enquanto que o EFA é a probabilidade do sistema incorretamente indicar que um sinal gráfico é verdadeiro, quando de fato é falso. O EFR e EFA são expressos em porcentagens e variam de acordo com o limiar de decisão escolhido.

Neste trabalho também foram utilizados as taxas de EFA quando EFR é igual a zero (**EFR_0**), EFR quando EFA é igual a zero (**EFA_0**) e a taxa de erros iguais (**TEI**). O EFR_0 representa a menor taxa de erro quando o sistema incorretamente aceita um sinal gráfico falso como verdadeiro, quando todos os sinais gráficos verdadeiros já foram aceitos. EFA_0 indica a menor taxa de erro quando o sistema incorretamente rejeita sinais gráficos verdadeiros, quando todas as falsificações foram corretamente rejeitadas. A taxa de erros iguais (TEI) é o ponto em que EFR e EFA são iguais e representa a separabilidade entre o grupo de dados falsos e verdadeiros. Convém lembrar que EFR_0 e EFA_0 só podem estar sendo calculados neste trabalho porque foram utilizados dados em quantidade finita.

5.2 LIMIAR DE DECISÃO

O método proposto neste trabalho faz uso de 5 amostras de sinais gráficos cadastrados para determinar o limiar de decisão que é utilizado como ponto de operação do sistema de autenticação [15]. O limiar é obtido da seguinte forma: Primeiro, a distância entre cada amostra e a respectiva IR é calculada. Depois, a maior distância encontrada entre elas é definida como a distância de referência D_{ref}. Note que cada pessoa cadastrada terá uma distância de referência

particular. Entretanto, como o valor D_{ref} foi obtido de um conjunto pequeno de amostras que não representa todas as possíveis nuances e imperfeições que podem ocorrer durante a escrita de um sinal gráfico genuíno, D_{ref} tende a ser bastante inferior ao valor que de fato representa o ponto de separação entre os sinais genuínos e falsos. Por este motivo para uma determinada pessoa k o limiar de operação T_k foi definido como:

$$T_k = \alpha \cdot D_{ref}(k), \quad (8)$$

onde α é uma constante que eleva o limiar de decisão e absorve parte das variações intra-pessoais da escrita. O valor estipulado para α é de $1{,}5 \cdot 10^3$.

6. EXPERIMENTOS

Foram realizados oito experimentos no total. Os primeiros sete experimentos foram dedicados ao processo de verificação pessoal. Nos experimentos de 1 a 6 o processo de verificação é testado contra falsificações aleatórias, ou seja, o falsificador utiliza seu próprio sinal gráfico no lugar do genuíno para ter acesso aos recursos do sistema. No experimento 7 foram utilizadas falsificações habilidosas, ou seja, o falsificador possui uma amostra do sinal gráfico genuíno e, baseado nessa amostra, o impostor tenta reproduzí-lo com a maior fidelidade possível. No experimento 8 estudou-se o desempenho do classificador e das três características propostas no processo de identificação pessoal.

Nos experimentos 1 a 7 foram utilizados limiares de decisão variáveis, com o objetivo de descobrir os EFR_0, EFA_0 e TEI para essas configurações. Além disso, nos experimentos 4, 5, 6 foi também apresentado a média do EFR e EFA baseados no limiar de operação T_k definido na Equação (8).

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 discriminante de cada uma das 3 características isoladamente. Os resultados deste experimento estão apresentados na Tabela 1.

Característica	EFR_0 (%)	EFA_0 (%)	TEI (%)
Contornos	7,4	5,6	3,0
Traços	19,2	11,2	5,9
Correlação	10,3	7,2	6,0

Tabela 1. Taxas de erros médios no experimento 1.

O experimento 2 foi realizado utilizando-se as 40 classes de assinaturas verdadeiras em conjunto com as 50 assinaturas falsas. O objetivo deste experimento foi determinar o poder discriminante conjunto de 2 vetores de características: a inclinação dos contornos e a inclinação dos traços. A distância (p_{final}) deste experimento é definido como o resultado entre o produto da distância dos contornos ($p_{contorno}$) e a distância dos traços ($p_{traços}$), isto é:

$$p_{final} = p_{contorno} * p_{traços} \quad (9)$$

O resultado deste experimento pode ser observado na Tabela 2.

EFR_0 (%)	EFA_0 (%)	TEI (%)
4,8	3,6	1,5

Tabela 2. Taxas de erros médios no experimento 2.

O experimento 3 foi realizado utilizando-se as 40 classes de assinaturas verdadeiras em conjunto com as 50 assinaturas falsas. O objetivo deste experimento foi determinar o poder discriminante conjunto dos 3 vetores de características: inclinação de contornos, inclinação dos traços e de correlação. A distância deste experimento é definida como o resultado dos produtos das distâncias da inclinação de contornos, inclinação dos traços e dos dados de correlação ($p_{correlação}$), isto é:

$$p_{final} = p_{contorno} * p_{traços} * p_{correlação} \quad (10)$$

O resultado deste experimento pode ser observado na Tabela 3.

EFR_0 (%)	EFA_0 (%)	TEI (%)
2,4	1,2	0,7

Tabela 3. Taxas de erros médios no experimento 3.

Da análise do resultado do experimento 3 constatamos que a utilização dos três vetores de características e a Equação (10), reduziu consideravelmente as taxas de erros se comparado com os resultados obtidos quando as características são avaliadas isoladamente. Assim sendo, decidimos continuar utilizando nos experimentos 4, 5, 6 e 7 essa mesma métrica na classificação dos sinais gráficos.

É importante salientar que o emprego da multiplicação das distâncias de cada uma das características tem como objetivo aumentar a separação entre os *clusters* de sinais gráficos genuínos e os falsos. Isto ocorre porque as distâncias $p_{contorno}$, $p_{traço}$, e $p_{correlação}$ para sinais gráficos genuínos tendem a ser pequenas, porém nunca iguais a zero, o que resulta numa distância final também pequena. Por outro lado, nos sinais falsificados ocorre o contrário, resultando numa distância final extremamente grande. Dado este fato, foi possível constatar a eficiência do limiar de operação T_k e o valor estipulado para α definidos pela Equação (8). Verificamos também que utilizando outra configuração de classificador, como por exemplo somando as distância das características, os *clusters* dos sinais gráficos genuínos e falsos ficam muito próximos, elevando as taxas de erros a patamares superiores às encontradas com a métrica da Equação (10).

O experimento 4 foi realizado utilizando-se as 20 classes de símbolos manuscritos em conjunto com os 57 símbolos manuscritos que não pertenciam à classe que estava em teste. O resultado deste experimento pode ser observado na Tabela 4.

EFR_0 (%)	EFA_0 (%)	TEI (%)
1,9	1,5	0,9

Tabela 4. Taxas de erros médios no experimento 4.

Na Tabela 5 são mostradas as médias das taxas EFR e EFA obtidas através do limiar de operação.

EFR (%)	EFA (%)
3,4	0,0

Tabela 5. Média de EFR e EFA no experimento 4.

O experimento 5 foi realizado utilizando-se as 20 classes de símbolos manuscritos em conjunto com as 50 assinaturas falsas. Neste experimento todas as taxas de erros foram iguais a zero, o que significa que foi possível separar totalmente as classes dos sinais gráficos das classes das assinaturas falsas.

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 à classe que está em teste mais as 50 assinaturas falsas. O resultado deste experimento pode ser observado na Tabela 6.

EFR_0 (%)	EFA_0 (%)	TEI (%)
2,5	1,9	0,7

Tabela 6. Taxas de erros médios no experimento 6.

Na Tabela 7 são mostradas as médias das taxas EFR e EFA baseadas no limiar de operação.

EFR (%)	EFA (%)
4,3	0,0

Tabela 7. Médias de EFR e EFA no experimento 6.

O experimento 7 foi executado utilizando-se 5 classes que foram escolhidas aleatoriamente dentro do *Grupo de Símbolos Verdadeiros* (*SV*). Essas 5 classes foram as mesmas utilizadas como referência para a realização das falsificações habilidosas. O resultado desse experimento pode ser visto na Tabela 8.

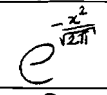
	EFR_0 (%)	EFA_0 (%)	TEI (%)
	3	3	3
	25	43	5
	45	43	5
	22	25	10
	15	35	3
Média da Taxa de Erros	22,0	29,8	5,2

Tabela 8. EFR_0, EFA_0 e TEI frente a falsificações habilidosas.

No experimento 8 foi estudado o desempenho do método proposto quando aplicado num processo de identificação. Foram executados três testes. No primeiro, as assinaturas verdadeiras foram comparadas com as *IR* de todas as pessoas que pertencem ao *Grupo de Assinaturas Verdadeiras* (*AV*). Como resultado das comparações, um conjunto de distâncias foi calculado (baseado na Equação 10), uma distância para cada classe pertencente ao *AV*. Se a menor distância calculada sobre a assinatura genuína for da sua própria classe, considera-se uma identificação correta. No segundo teste a mesma metodologia foi aplicada, porém, somente sinais gráficos que pertencem ao *SV* foram utilizados. No terceiro teste, *AV* e *SV* foram misturados e a metodologia foi aplicada mais uma vez.

A taxa de classificação correta, que mede o número de sinais gráficos corretamente classificados, foi o parâmetro utilizado para avaliar o desempenho no processo de identificação. Os resultados do experimento 8 nos três testes executados são apresentados na Tabela 9.

Espaço das Amostras	Identificação Correta (%)
Assinaturas	83,8
Símbolos	93,7
Assinaturas + Símbolos	87,1

Tabela 9. Desempenho de identificação

7. ANÁLISE DOS RESULTADOS

Os experimentos 1, 2 e 3 serviram para avaliar o poder discriminante das características e do classificador utilizado. Nestes primeiros três experimentos somente imagens de assinaturas foram empregadas, pois nosso objetivo era avaliar se o método de autenticação por sinais gráficos poderia ser satisfatoriamente aplicado como uma generalização da autenticação pessoal por assinaturas. Os resultados obtidos mostraram que nossa abordagem consegue desempenho satisfatório sobre imagens de assinaturas, garantindo taxas de 2,4 % para EFR_0, 1,2 % para EFA_0 e de 0,7 % para TEI.

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

O experimento 7 utiliza falsificações habilidosas para avaliar o processo de verificação do método proposto. A média de 5,2 % para a taxa de erros iguais foi alcançada neste experimento, o que significa que na maioria das vezes os sinais gráficos podem ser unicamente determinados pela inclinação dos traços, pela inclinação dos contornos e pela característica de correlação.

No experimento 8, testes foram realizados para medir o desempenho do método proposto sobre o processo de identificação pessoal. A identificação é um problema mais

difícil do que a verificação, visto que o sistema não conhece *a priori* a classe a qual a amostra em teste pertence [16]. Uma taxa de classificação correta de 87,1 % foi obtida quando todas as amostras dos grupos *AV* e *SV* foram utilizados. Este resultado é considerado satisfatório tendo em vista a simplicidade do método aplicado.

8. CONCLUSÕES

Este trabalho propôs um método de autenticação pessoal através de qualquer sinal gráfico manuscrito, extrapolando a idéia de utilizar exclusivamente imagens de assinaturas na execução dessa tarefa. Foi introduzido o conceito de senha gráfica, a qual pode substituir ou em conjunto com as senhas de texto, aumentar o grau de segurança nas tarefas de *login* em sistemas de computação.

O método de autenticação 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 é eficiente frente a falsificações aleatórias e também sobre falsificações habilidosas nas quais o impostor conhece previamente detalhes da imagem que se dispõe a falsificar.

Foram apresentados também dois algoritmos de extração de características. O primeiro se baseia em operações de morfologia matemática para extrair informações da inclinação dos traços manuscritos e dos seus contornos, e o segundo se baseia na correlação entre os pixels de uma imagem de referência e da imagem de uma amostra de teste.

Em [17] Plamondon e Srihari afirmam que a maioria dos atuais sistemas de autenticação pessoal por imagens de assinaturas possuem taxas de erros dentro da faixa de 2 % e 5 %. Nosso trabalho obteve como resultado taxas de EFR_0 de 2,5 % e a EFA_0 de 1,9 % nos testes apresentados na tabela 6, o que indica um desempenho competitivo com relação esses sistemas.

Um classificador linear simples foi aplicado para separar os sinais gráficos genuínos dos falsos. Assim sendo, o método leva apenas alguns segundos para ser treinado, ao contrário de outros em que a etapa de cadastramento pode ser muito demorada, como aqueles que utilizam Cadeias de Markov, Redes Neurais ou Algoritmos Genéticos [18]. Este é um ponto importante em nossa metodologia visto que num trabalho futuro pretendemos implementar este método de autenticação como uma aplicação em dispositivos móveis tais como PDAs e celulares, os quais possuem pouca memória e baixo poder de processamento.

AGRADECIMENTO

À FAPESP - Fundação de Amparo à Pesquisa do Estado de São Paulo, pelo financiamento desta pesquisa.

REFERÊNCIAS

[1] L. L. Lee e Miguel G. Lizárraga, "Biometrics on internet: Security Applications and Services", Biometrics Solutions for Authentication in an E-World – Kluwer Academic Publisher, 2002

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

[3] O. Hilton, "Signatures – Review and New View", *Journal of Forensic Sciences, JFSCA*, Vol. 37, No 1, pp 125 – 129, 1992

[4] M. C. Fairhurst, "Signature verification revisited: promoting practical exploitation of biometric technology", *Electronics and Communication Engineering Journal*, pp. 273 – 280, December, 1997

[5] H. Cardot; M Revenu, B. Victorri e 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

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

[7] David Bensinger, Human memory and the graphical password. Disponível na Internet: http://www.passlogix.com/media/pdfs/bensinger.pdf, 1998.

[8] Miguel G. Lizárraga. "Um sistema biométrico de identificação pessoal via internet com ênfase em assinaturas estáticas", Tese de doutorado. Universidade Estadual de Campinas, 2000.

[9] Er Brocklehurst, "Computer methods of signature verification", *Journal of the Forensic Science Society*, Vol 35, pp 445-457, 1985

[10]Kai Huang e Hong Yan, "Off-line signature verification based on geometric feature extraction and neural network classification", *Pattern Recognition*, Vol. 30. No 1, pp 9-17, 1997

[11]Yingyong Qi e Bobby R. Hunt, "Signature Verification using global and grid features" *Pattern Recognition*, Vol 27, No 12, pp 1621-1629, 1994

[12]Richard Buse, Zhi-Quiang Liu e Jim Bezdek, "Word Recognition Using Fuzzy Logic", *IEEE Transactions on Fuzzy Systems*, Vol 10, No 1, 2002

[13]J. Serra, "Introduction to Mathematical Morphology", *Computer Vision, Graphics and Image Processing*, Vol 35, pp 283-305, 1986

[14]R. C. Gonzalez, R. Woods, Digital Image Processing, Addison Wesley, 1993

[15]Jaihie Kim, J. R. Yu e S. H. Kim, "Learning of prototypes and decision boundaries for a verification problem having only positive samples", *Pattern Recognition Letters*, Vol. 17, pp 691- 697, 1996

[16]Mario E. Munich e Pietro Perona, "Visual Identification by Signature Tracking", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol. 25. No. 2, pp 200 – 217, 2003

[17]Rejean Plamondon e Sargur Srihari, "On-line and offline Handwriting Recognition: A comprehensive survey", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol 22, No. 1, pp 63 – 84, 2000

[18]Anil Jain, R. Duin e J. Mao, "Statistical Pattern recognition: A review", *IEEE Trans. on Pattern Analysis and Machine Intelligence*, Vol 22, No. 1, pp 4 – 37, 2000

Miguel Gustavo Lizárraga obteve os títulos de engenheiro, mestre e doutor em Engenharia Elétrica pela UNICAMP, nos anos de 1994, 1996 e 2000, respectivamente. Desde 1994 vem realizando trabalhos científicos na área de reconhecimento de padrões e redes de computadores. É especialista em biometria, com ampla experiência em sistemas automáticos de autenticação pessoal por assinaturas manuscritas, faces e dinâmica de digitação.

Lee Luan Ling obteve o título de engenheiro eletricista pela USP em 1980, mestre em Engenharia Elétrica pela UNICAMP em 1984 e PhD em Engenharia Elétrica pela Universidade de Cornell em 1991. Desde 2002 é Professor Titular pela FEEC - UNICAMP.