Uso de Técnicas Adaptativas no Reconhecimento Biométrico por Impressão Digital

F. B. R. do Val,P.R. Marcelino e J. J. Neto

***Abstract*— Recognition of individuals, with practicality and reliability, is an important need of our society, especially when it comes to provide access to restricted places and systems. Based on this, studies about biometric authenticationare increasing, which usually combines easiness for users and security. This article focus on proposing the application of adaptivity concepts on traditional algorithms of fingerprint authentication, the most used biometric technique, in order to improve the performance of these algorithms through the reduction of mistaken decisions.**

***Keywords*— Fingerprint Recognition, Adaptivity, Gabor filter, Image Processing.**

I. INTRODUÇÃO

IMPRESSÕES digitais possuem características únicas capazes de distinguir uma pessoa em uma população. Essas características são denominadas minúcias. As principais minúcias observadas para identificar um indivíduo são: bifurcações e terminações, como é possível observar na imagem a seguir[1].

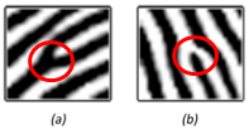

Figura 1. (a) Bifurcação, (b) Terminação.

Cristas são os relevos da pele observados na impressão digital, e sulcos são as depressões localizadas entre as cristas. A bifurcação é quando uma crista da digital se divide em duas e terminação é quando uma crista termina, iniciando-se o sulco.

A qualidade da impressão digital varia de acordo com cada pessoa, muitas vezes estando associada à função laboral da mesma. No geral, indivíduos que trabalham realizando esforços com as mãos - como pedreiros, costureiras, operadores de caixa, entre outros - apresentam digitais em que as minúcias têm qualidade inferior à de um indivíduo que não realiza grandes esforços manuais.

Além disso, a digital de cada ser humano varia com o tempo, seja por envelhecimento ou por feridas e cicatrizes. Por isso, é comum, em sistemas de autenticação biométrica por impressão digital, a pessoa cuja digital alterou-se ter dificuldades para se autenticar no sistema. Desta forma, com o passar do tempo os sistemas passam a rejeitar com maior frequência usuários cadastrados.

Também é comum o sistema detectar falsas minúcias devido a impurezas no leitor de impressão digital, devido a resíduos no dedo do indivíduos ou mesmo distorção elástica da pele ao ser pressionada contra o sensor. A detecção de falsas minúcias dificulta a correta identificação dos usuários.

II. OBJETIVOS

Este projeto objetiva melhorar a qualidade dos sistemas de autenticação por impressão digital através da aplicação de técnicas adaptativas.

As métricas comumente utilizadas para avaliar a qualidade de sistemas biométricos são:

- Taxa de falsa aceitação (*FAR – False Acceptance Rate*): Indicador para avaliar a frequência que o sistema aceita pessoas não cadastradas no mesmo. Idealmente, este indicador deve ser zero ou um valor significativamente baixo.
- Taxa de falsa rejeição (*FRR – False Rejection Rate*): Métrica que indica a frequência que usuários cadastrados no sistemas são rejeitados, isto é, o sistema não reconhece a pessoa como usuária do sistema.
- Taxa de erro equivalente (*EER – Equivalent Error Rate*): Esta métrica representa o equilíbrio entre a taxa de falsa aceitação e a taxa de falsa rejeição.

Tempo médio de processamento de digitais de entrada: Indicador em medida de tempo para avaliar se o sistema leva muito tempo para aceitar ou rejeitar um indivíduo.

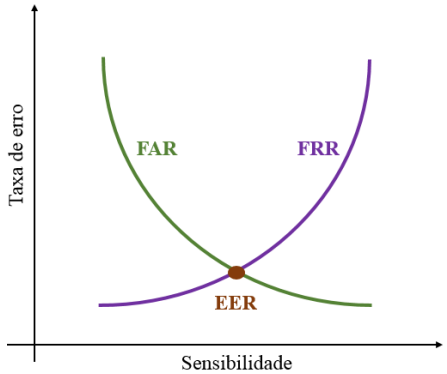

Figura 2. Curvas das principais métricas de sistemas de autenticação por impressão digital.

F. B. R. do Val, Universidade de São Paulo (USP), São Paulo, Brasil, fernanda.brval@gmail.com
P. R. Marcelino, Universidade de São Paulo (USP), São Paulo, Brasil, priscila.ribeiro.marcelino@gmail.com
J. J. Neto, Universidade de São Paulo (USP), São Paulo, Brasil, jjneto@gmail.com

O objetivo do projeto é, por meio de recursos adaptativos, melhorar as métricas de desempenho do sistema, para que o mesmo aceite mais usuários cadastrados e rejeite mais usuários não cadastrados. Busca-se que as melhorias mencionadas não comprometam o tempo de processamento.

Estão em andamento testes para mensurar a melhoria proporcionada pelo sistema desenvolvido com aplicação de técnicas adaptativas. O progresso mencionado já foi observado qualitativamente.

III. VISÃO GERAL DO SISTEMA

O sistema é composto por três etapas:

1. Pré-processamento da imagem da impressão digital;
2. Extração das minúcias;
3. Autenticação (matching).

Na primeira etapa, a imagem de entrada passa por diversos passos que têm a finalidade de melhorar a qualidade da mesma, buscando reduzir a quantidade de falsas minúcias a serem extraídas na etapa seguinte.

Na etapa de extração das minúcias, a imagem tratada anteriormente é avaliada, buscando encontrar terminações e bifurcações. O sistema não faz distinção entre terminações e bifurcações. Para cada minúcia extraída, o sistema indica as coordenadas "x" e "y", o ângulo de orientação da minúcia em relação ao eixo x e a nota de qualidade da minúcia extraída. Ao final da extração de minúcias, gera-se o template da digital, ou seja, um mapa com todas as minúcias referentes à imagem pré-processada. Este template servirá como base para a etapa seguinte.

Figura 3. Imagem original, minúcias extraídas e template gerado.

Na última etapa do sistema, autenticação, faz-se a comparação entre templates cadastrados e o template de entrada. A comparação é feita a partir dos parâmetros extraídos de cada uma das imagens das digitais, isto é, a partir da informação da minúcias, que possuem posição, ângulo de orientação e nota de qualidade.

A comparação retorna uma nota de similaridade entre os *templates* comparados. De acordo com a nota de corte pré-estabelecida, o indivíduo pode ser aceito ou rejeitado no sistema.

Na figura 4, é possível observar as etapas do sistema. Estas etapas estão exibidas de forma simplificada.

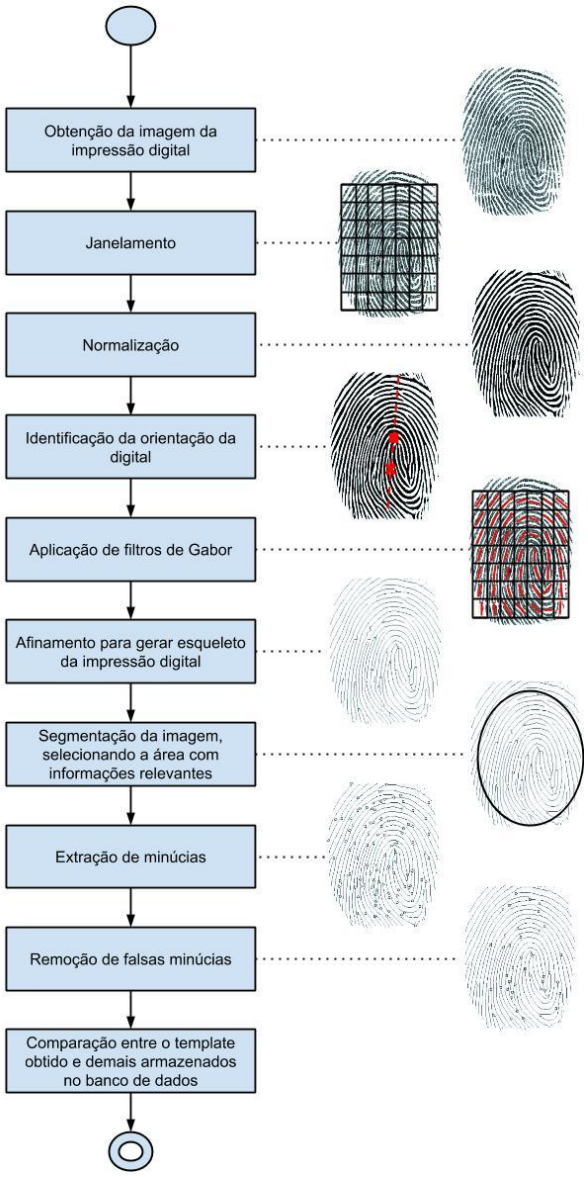

Figura 4. Etapas do sistema de autenticação por impressão digital.

Para uma compreencão global dos algoritmos tradicionais de reconhecimento biométrico, consultar as referências [1], [2] e [3].

IV. APLICAÇÕES DE ADAPTATIVIDADE NO SISTEMA

O projeto aplicou técnicas de adaptatividade em algumas das etapas do sistema, como será explicado a seguir.

IV. I.PRÉ-PROCESSAMENTO DA IMAGEM DA IMPRESSÃO DIGITAL

Na etapa de pré-processsamento da imagem da impressão digital, técnicas adaptativas são aplicadas em dois momentos: na normalização e no filtro de Gabor. Estas etapas podem ser identificadas na figura 4.

IV. I. I.NORMALIZAÇÃO

Normalização é a segunda etapa do sistema, como observa-se na figura 4. Este passo é responsável por

eliminarcomponentes espúrias de intensidade, de baixa frequência espacial, devido a sujeira ou contato irregular entre a superfície do dedo e o sensor, de forma a padronizar a intensidade da mesma.

A figura normalizada é definida por [3]:

$$N(i,j) = M0 + \sqrt{(V0(I(i,j) - M))/V}\text{, se } I(i,j) > M\text{,}$$

ou

$$N(i,j) = M0 - \sqrt{(V0(I(i,j) - M))/V}\text{, se } I(i,j) \leq M\text{.}$$

Em que:

- $I(i,j)$ é o valor do pixel (i,j) em escala de cinza;
- $N(i,j)$ é o valor do pixel (i,j) normalizado em escala de cinza;
- M é a média da intensidade de todos $I(i,j)$ da imagem ou região selecionada;
- V é a variância de todos $I(i,j)$ da imagem ou região selecionada;
- $M0$ é a média desejada;
- $V0$ é a variância desejada;

Neste projeto, a imagem é fragmentada em janelas de tamanhos iguais e, então, aplica-se a normalização para cada uma dessas janelas. Nas imagens a seguir, é possível observar a melhoria na qualidade da imagem ao aplicar a normalização por janelas em vez de na imagem inteira.

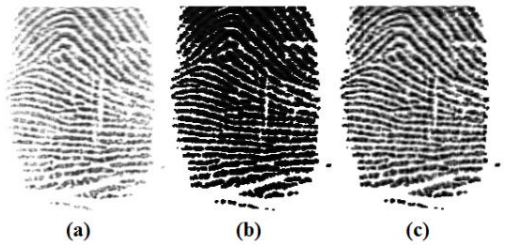

Figura 5. (a) Imagem original, (b)normalização aplicada na imagem não segmentada e (c) normalização aplicada na imagem segmentada em janelas.

Realizando a normalização por janelas, a qualidade da figura melhora significamente se comparada à qualidade da imagem normalizada sem segmentação alguma.

IV. I. II.FILTRO DE GABOR

A etapa do filtro de Gabor é dependente de duas etapas anteriores: mapas de frequência e de orientação, como é possível observar na figura 4.

A frequência de cristas indica o quão próximas ou espaçadas estão as cristas da impressão digital. Para calcular essa frequência, utilizamos transformada de Fourier (DFT: Discret Fourier Transform), passando como entrada a imagem e obtendo como resultado suas componentes senoidais. Na figura 6, é possível observar uma ilustração do funcionamento da transformada.

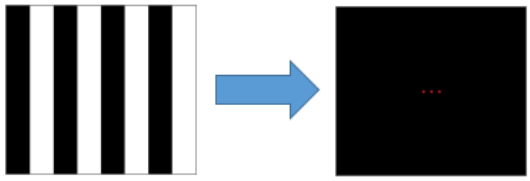

Figura 6. Frequência das cristas de uma janela, após a aplicação da transformada de Fourier.

Na figura 6, a imagem à direita é o resultado da *dft* aplicada na imagem da esquerda. O ponto central representa a componente DC e os outros dois pontos representam a variação no "sinal". Os outros dois pontos estão afastados 4 pixels em relação ao ponto central. Isso significa que na imagem de entrada, há 4 ciclos completos do sinal. Com essa informação e o tamanho da imagem de entrada, é possível calcular a periodicidade espacial.

O cálculo da frequência é realizado para cada janela da imagem de entrada. Denomina-se mapa de frequência, pois é um mapeamento da frequência de cada uma das janelas.

Outra etapa necessária para execução do filtro de Gabor, é a geração do mapa de orientação. Nesta etapa, a direção das cristas de cada janela é avaliada e uma direção que aponta no sentido do gradiente é definida. O gradiente aponta na perpendicular das cristas, que podem ser vistas como análogas a curvas de nível. Nesta etapa, faz-se uso do filtro de Sobel. A figura 7 permite observar a orientação obtida para cada uma das janelas.

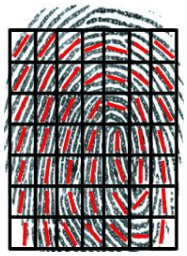

Figura 7. Mapa de orientação da imagem da digital.

Em [4], os modelos matemáticos utilizados como base para as etapas de geração dos mapas de freqüência e orientação estão explicados detalhadamente.

Após obtidos os mapas de frequência e orientação da imagem, aplica-se o filtro de Gabor para cada uma das janelas.

Filtro de Gabor é um filtro passa-banda, que de acordo com a orientação e frequência, apresenta ótimas melhorias na qualidade da imagem. Este filtro é uma combinação de uma função harmônica com uma função gaussiana [1].

Matematicamente, o filtro de Gabor pode ser descrito da seguinte maneira [1]:

$$g(x,y:\theta,f) = exp\left\{-\frac{1}{2}\left(\frac{x_\theta^2}{\sigma_x^2} + \frac{y_\theta^2}{\sigma_y^2}\right)\right\}.cos(2\pi.f.x_\theta)$$

Em que:

- f é a frequência de cada janela;
- σ_x e σ_y são os valores das variâncias do sinal nas direções x e y, respectivamente;
- $[x_\theta, y_\theta]$ são os pontos $[x, y]$ rotacionados por θ.

$$\begin{bmatrix} x_\theta \\ y_\theta \end{bmatrix} = \begin{bmatrix} sen\theta & cos\theta \\ -cos\theta & sin\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Denomina-se filtragem adaptativa, visto que cada janela será filtrada de forma diferente, com base na frequência e orientação daquela janela. O Filtro de Gabor é muito importante para eliminar ruídos da imagem que resultariam em falsas minúcias. Ele analisa o padrão da imagem e corrige regiões que apresentem desvios em relação a esse padrão. Por exemplo, para uma dada frequência média de cristas, se existirem pixels de ruído fazendo com que a frequência seja maior numa pequena parte da imagem, o ruído é eliminado. Na figura 8, há uma ilustração da aplicação do filtro de Gabor, nela nota-se a melhoria obtida com a eliminação de falsas minúcias.

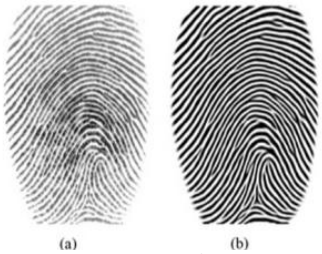

Figura 8. (a) Imagem antes da aplicação do filtro de Gabor e (b) imagem após filtragem.

IV. II.AUTENTICAÇÃO

A etapa de autenticação (*matching*) é realizada a partir da comparação entre dois *templates*.

Cada *template* equivale a um grafo em que os nós são compostos pelas minúcias extraídas de uma imagem de impressão digital. O *template* é uma relação de distância e ângulo entre diferentes minúcias de uma mesma digital. Para verificar a similaridade entre digitais, compara-se os ramos e nós de dois *templates* e quanto mais parecidos, maior é a nota de similaridade.

De acordo com a nota de similaridade resultante da comparação,o sistema decide se a pessoa é aceita ou não na aplicação.

A seguir, estão explicadosos usos de técnicas adaptativas na etapa de autenticação.

IV.II. I.ALTERAÇÃO DA NOTA DE CORTE DE ACORDO COM A FINALIDADE DO SISTEMA

Duas das principais métricas de desempenho de sistemas de autenticação por digitais são as taxas de falsa aceitação e falsa rejeição, que são recíprocas, isto é, uma aumenta enquanto a outra diminui em relação a uma variável comum, que no caso é a nota mínima de similaridade para aceitação.

A proposta de aplicação de métodos adaptativos é modificar a atuação do sistema de acordo com o tipo de aplicação. Por exemplo, aplicação do governo para controlar a entrada e saída de pessoas no país, este tipo de sistema deve ser altamente seguro, com baixíssimos riscos de confundir os indivíduos que saíram ou entraram no país. Outra aplicação seria de controle de acesso de ajudantes de obra que, no geral, têm impressão digital de baixa qualidade.

O que se deseja ilustrar com estes exemplos é: na primeira aplicação, sistema governamental, o ideal é que a taxa de falsa aceitação (*FAR*) – ocorrência de *matching* indevido – seja muito baixa, porém, ao estabelecer isso, compromete-se a taxa de falsa rejeição (*FRR*) – não ocorrência de *matching*, quando deveria ocorrer. Esta aplicação teria maiores dificuldades para identificar as pessoas, muitas vezes solicitando novas digitais de entrada.

Já o segundo exemplo, o sistema de controle de acesso de ajudantes de obra, deveria ser mais tolerante, visto que a qualidade das digitais de entrada não é alta. Para que o sistema não solicite muitas vezes que os usuários insiram a digital novamente, reduz-se a nota de corte; ou seja, a nota de similaridade entre o template da digital de entrada e o *template* de uma das digitais salvas no banco de dados não precisa ser tão alta quanto a da primeira aplicação exemplo. Isso compromete a taxa de falsa aceitação (*FAR*), que tende a apresentar valores maiores, mas reduz a taxa de falsa rejeição (*FRR*).

A solução proposta no projeto é: o administrador do sistema determina qual o tipo de aplicação deseja, se é um sistema rigoroso ou tolerante, e realiza uma etapa de treinamento do sistema antes de colocá-lo em operação. Durante o treinamento, o administrador entra com diversas imagens e informa se cada uma delas deveria ser aceita ou rejeitada. Dessa forma, a nota de corte para a similaridade entre *templates* é alterada automaticamente com base nesse feedback, de forma a reduzir erros futuros.

Essa alteração da nota de corte se dá conforme a seguinte lógica:

a) Caso o administrador opte por limitar a taxa de falsa aceitação, o sistema irá aumentar a nota de corte em uma unidade após cada aceitação errônea que for cometida, se tornando cada vez mais rigoroso, até que essa taxa se mantenha dentro de um limite pré-estabelecido.
b) Caso o administrador opte por limitar a taxa de falsa rejeição, o sistema irá reduzir a nota de corte em uma unidade após cada rejeição errônea que for cometida, se tornando cada vez mais tolerante, até que essa taxa se mantenha dentro de um limite pré-estabelecido.

Caso o administrador do sistema deseje aumentar a confiabilidade, é possível solicitar aos indivíduos que além de inserir a digital, entrem com outras informações, como data de nascimento, RG, CPF, entre outras. Essas informações complementares são campos do banco de dados, e o sistema só analisará as digitais correspondentes a indivíduos que, por exemplo, tenham uma determinada data de nascimento.

IV. II. II.ALTERAÇÃO DA NOTA DE CORTE DE ACORDO COM O USUÁRIO

Outra aplicação de métodos adaptativos é realizar a alteração da nota de corte de similaridade para cada usuário. Caso o administrador não defina o tipo de aplicação – se deve ser rigorosa ou não – o sistema controla a nota de corte de forma individualizada, ou seja, de acordo com a qualidade da digital de cada usuário, o valor da nota de corte muda.

O sistema é constantemente retroalimentado pelo administrador, que indica quando o sistema realiza uma falsa aceitação ou uma falsa rejeição.

No caso de uma falsa aceitação, o sistema aumenta a nota de corte de similaridade do usuário que foi identificado erroneamente. Para que o sistema aprenda, o administrador deve indicar quando foi tomada uma decisão incorreta.

Quando ocorre uma falsa rejeição (um usuário cadastrado no sistema tentou acessar o mesmo, mas não foi aceito), o administrador deve indicar ao sistema qual usuário que tentou entrar. Assim, o sistema aprende que não fez uma identificação correta para determinado usuário. Automaticamente, o sistema altera a nota de corte daquele indivíduo. Obviamente, há um limite para o valor mínimo da nota de corte a fim de garantir que o sistema permaneça confiável.

Alguns dos motivos para que ocorra falsa rejeição são a existência de resíduos no aparelho de detecção de impressão digital, resíduos no dedo ou até mesmo machucados.

Como já mencionado, as principais métricas de desempenho de sistemas de autenticação por digitais são as taxas de falsa aceitação e falsa rejeição, que são recíprocas. Ao adaptar a nota de corte de cada usuário, o sistema reduz ambos os tipos de falsas decisões.

IV. II. III.CADASTRO AUTOMÁTICO DE NOVAS DIGITAIS

Esta terceira aplicação de métodos adaptativos é complementar à segunda – alteração da nota de corte de acordo com o usuário. Considerando que o dedo do indivíduo sofreu alguma modificação, inicialmente o sistema é mais tolerante com aquela pessoa, ou seja, a nota de corte de similaridade sofre redução, como mencionado no item anterior. Porém, se a digital sofreu uma modificação permanente, como é o caso de envelhecimento ou cicatrizes, o sistema, após reduzir a nota de corte de similaridade para aquele indivíduo, identifica que o dedo sofreu alguma modificação permanente, visto que a nota de similaridade está constantementebaixa.

Identificada a alteração permanente na digital do usuário, o sistema – que armazenou anteriormente as digitais de tentativas de acesso sem sucesso, porém sem adicionar como *templates* do usuário para fazer a similaridade com novas digitais de entrada – escolhe as digitais de melhor qualidade que o indivíduo inseriu anteriormente e com as quais o sistema não conseguiu realizar autenticação, e então sim adiciona essas imagens no cadastro do usuário como novos *templates*.

Todos esses procedimentos são transparentes aos usuários. O administrador do sistema é responsável por retroalimentar o programa a fim de indicar quando o mesmo tomou uma decisão errônea.

V. CONSIDERAÇÕES FINAIS

Com a conclusão deste projeto, que segue em andamento, muitos outros trabalhos complementares podem agregar a esta pesquisa.

Podemos agrupar os trabalhos complementares em dois grupos principais: expansão do algoritmo de reconhecimento de padrões para novos tipos de padrões; e expansão do uso de adaptatividade no algoritmo de reconhecimento de impressão digital.

Quanto ao reconhecimento de padrões, a partir de uma imagem são extraídos parâmetros relevantes que tornam determinado objeto ou ser vivo identificável. A aplicação escolhida foi o padrão de impressões digitais, mas também é possível expandir o reconhecimento para: outros padrões biométricos; padrões da natureza; padrões de doenças em exames médicos, dentre outros.

Para citar alguns exemplos, no caso de padrões biométricos, há diversas outras características que nos torna identificáveis, por exemplo o padrão da íris do olho, formato da mão, padrão de voz, formato da face e assinatura. É possível identificar os parâmetros relevantes de cada um desses itens e, a partir da extração deles, identificar os indivíduos.

No caso de padrões da natureza, um exemplo que pode ser citado é a identificação de espécies de abelhas a partir do desenho em suas asas. Outro exemplo são plantas, que podem ser identificadas a partir das ranhuras em suas folhas.

Também é possível identificar padrões para doenças, como câncer de pele, irregularidades no cérebro, dentre outras.

Do ponto de vista de adaptatividade, podemos manter a mesma aplicação escolhida – autenticação por impressão digital – e englobar novos parâmetros ou incluir novas técnicas. Por exemplo, parâmetros internos da etapa de *matching*, relacionados ao cálculo da nota de similaridade, poderiam ser investigados e tornados adaptativos. Ou seja, o sistema definiria o ponto ótimo de operação desses parâmetros com base em treinamento, da mesma forma que faz para o parâmetro de nota de corte. Ainda mais interessante seria tornar o sistema capaz de identificar os próprios parâmetros de interesse, os quais ele deveria variar para melhorar o desempenho da autenticação, de forma que os pesquisadores não precisem pré-definir esses parâmetros.

Vale ressaltar que além de otimizar o desempenho da autenticação de digital, quanto mais amplamente foram aplicados conceitos e técnicas adaptativas, mais apto a reconhecer diversos tipos de padrão de forma automática o sistema pode se tornar. Isso reduziria ou até eliminaria a necessidade de adaptação do código por parte dos pesquisadores a cada nova aplicação. Por exemplo, o sistema poderia, a partir da análise do formato do objeto de entrada, identificar de que tipo ele é (uma impressão digital, um animal, uma planta, um órgão, etc.), para então decidir se ele deve extrair minúcias ou outros parâmetros diferentes, se ele deve aplicar um ou outro filtro de tratamento na imagem, e assim por diante.

Por fim, fica evidente que a área deste projeto pode ser bastante desenvolvida com diversas outras pesquisas e que adaptatividade pode agregar muito valor ao reconhecimento de padrões.

AGRADECIMENTOS

Os autores gostariam de agradecer a contribuição que Albert Nissimoff, diretor de tecnologia da empresa Control ID, fez ao projeto por meio de explicações e esclarecimentos técnicos relacionados aos algoritmos tradicionais de identificação por impressão digital. Sua disponibilidade e interesse no projeto, combinados a sua vasta experiência na área, foram importantes para os resultados alcançados.

Os autores também gostariam de agradecer a Rafael Camargo Leite, estudante da Escola Politécnica, pelo suporte e apoio durante todo o projeto, em especial pela sua contribuição no esclarecimento de diversas dúvidas técnicas relacionadas ao ambiente de desenvolvimento do sofware.

REFERÊNCIAS

[1] T. d. S. Castro, "Identificação de Impressões Digitais Baseada na Extração de Minúcias," Juiz de Fora, Minas Gerais, Brasil, 2008.

[2] X. Jiang, W. Y. Yau e W. Ser, "Fingerprint Image Processing for Automatic Verification," em *IEEE 2nd Intrenational Conference on Information, Communication & Sigal Processing*, Singapore, 1999.

[3] B. N. Lavanya, K. B. Raja e K. R. Venugopal, "Fingerprint Verification based on Gabor Filter Enhancement," *Intrenational Journal of Computer Science and Information Security,* vol. 6, pp. 138-144, 2009.

[4] R. Thai, "Fingerprint Image Enhancement and Minutiae Extraction," University of Western Australia, Perth, Western Australia, Australia, 2003.

[5] W. Chen e Y. Gao, "A Minutiae-based Fingerprint Matching Algorithm Using Phase Correlation," em *9th Biennial Conference of the Australian Pattern Recognition Society on Digital Image Computing Techniques and Applications*, Glenelg, Australia, 2007.

Fernanda Baumgarten Ribeiro do Val é graduanda em Engenharia Elétrica com ênfase em Computação pela Escola Politécnica da Universidade de São Paulo(EPUSP), São Paulo, SP, Brasil. Trabalhou por 2 anos na empresa júnior da EPUSP (Poli Júnior) na aréa de Tecnologia da Informação e Gestão de Projetos. Em 2012, realizou intercâmbio, estudando durante 6 meses na Pontifícia Universidade Católica do Chile, onde aprofundou seus conhecimentos em invoção. Atualmente trabalha na Procter & Gamble na área de análise de categorias. Sua pesquisa se concentra em adaptatividade aplicada ao reconhecimento biométrico.

Priscila Ribeiro Marcelino é graduanda em Engenharia Elétrica com ênfase em Computação pela Escola Politécnica da Universidade de São Paulo (EPUSP), São Paulo, SP, Brasil. Trabalhou por 4 anos na empresa júnior da EPUSP (Poli Júnior), na qual atuou com desenvolvimento de software, gestão de projetos, dentre outras atividades. Atualmente trabalha na Procter & Gamble na área de Tecnologia de Informação. Sua pesquisa se concentra em adaptatividade aplicada ao reconhecimento biométrico.

João José Neto graduado em Engenharia Elétrica (1971), mestre em Engenharia Elétrica (1975) e doutor em Engenharia Elétrica (1980), e livre docente, professor associado (1993) na EPUSP - Escola Politécnica da Universidade de São Paulo. Coordena atualmente o LTA - Laboratório de Linguagens e Técnicas Adaptativas do Departamento de Engenharia de Computação e Sistemas Digitais da EPUSP. Sua especialidade é centrada em Ciência da Computação, com ênfase nos fundamentos da engenharia de computação e em Adaptatividade. Sua atividade principal inclui dispositivos adaptativos e tecnologia adaptativa, autômatos adaptativos e suas aplicações à engenharia de computação e outras áreas, em particular aos sistemas de tomada de decisão, processamento de linguagem natural, construção de compiladores e outros programas de software básico e sistemas operacionais, robótica, educação por computador, modelagem de sistemas inteligentes, aprendizado computacional, reconhecimento de padrões, inferência e outras aplicações baseadas na adaptatividade e em dispositivos adaptativos.