PROJETO DE REDES
www.projetoderedes.com.br

TECNOLOGIA BIOMÉTRICA – ASPECTOS DE SEGURANÇA E PRIVACIDADE

1. ANDRÉIA BRANDÃO DE OLIVEIRA [1]
Rua Primo Zacante, 25 – Jardim Joelma
Osasco, São Paulo
andreiabrandaodeoliveira@yahoo.com.br

2. JOSÉ CARLOS DOS SANTOS [2]
profjcsantos@usp.br

3. ADRIANA PAULA BORGES [3]
adrianapaula25@uol.com.br

4. ANDRÉ EVANDRO LOURENÇO [1]
andreevandro@uol.com.br

5. SILVIA MARIA FARANI COSTA [1]
silviafarani@yahoo.com.br
silviafarani@unifieo.br

[1]Fundação Instituto de Ensino para Osasco - UNIFIEO
Mantenedora do Centro Universitário FIEO - UNIFIEO

[2]Escola Politécnica da Universidade de São Paulo – EPUSP

[3]Faculdade de Educação e Cultura Montessori

Osasco/São Paulo

RESUMO

Com a evolução da tecnologia na era da informação, produtos e serviços que envolvem a identificação de indivíduos aumentaram em grande escala. Com essa proliferação, a identificação e autenticação do indivíduo a partir das suas características biológicas e/ou comportamentais é mais simples e cômoda que a memorização de palavras chave e código de acesso. A biometria, ou seja, o uso de características biológicas e/ou comportamentais para a identificação e autenticação, tem ganhado relevância. Atualmente as tecnologias biométricas podem ser empregadas em sistemas de segurança, transações financeiras, controle de acesso a locais restritos, controle de freqüência, acesso em redes corporativas, validação de documentos, autenticação e comprovação de identidade, dentre muitas outras aplicações.

O foco deste trabalho é a discussão sobre a utilização da biometria e questões associadas à preservação da privacidade dos indivíduos. Pretende-se analisar até que ponto o uso dessa tecnologia pode auxiliar na segurança da sociedade sem que a coleta e o armazenamento de dados biométricos sejam considerados uma invasão de privacidade, pois não se sabe quais dados serão guardados, quais pessoas terão acesso e principalmente como serão manipulados. Como contribuição secundária discutiremos a questão da classificação destas imagens visando otimizar o processamento na fase de verificação.

PALAVRAS CHAVES

Biometria, Segurança de Dados, Reconhecimento de Padrões.

1. INTRODUÇÃO

Este trabalho discute a utilização de uma tecnologia biométrica baseada no reconhecimento de impressões digitais e as questões associadas à preservação da privacidade dos indivíduos. A proposta secundária é contribuir ao gerenciamento dos bancos de dados permitindo otimizar a velocidade de processamento na fase final de comparação através de uma pré-classificação, associando a impressão digital a uma das categorias pré-especificadas de acordo com a topologia geométrica. Na fase de verificação são comparadas duas impressões digitais. Faz-se o confronto entre uma impressão digital cadastrada em um banco de dados e uma impressão digital candidata, verificando se os pontos característicos são correspondentes em tipo e posição. Desta forma, é possível fazer o reconhecimento de uma pessoa.

Desde os atentados de 11 de setembro, várias políticas de segurança vêm sendo discutidas nos Estados Unidos no sentido de garantir inequivocamente a identidade dos indivíduos. Nesse sentido, novas tecnologias estão sendo pesquisadas e a biometria tem papel fundamental nesse cenário. O uso de técnicas de reconhecimento de impressão digital e da íris garantem a autenticação das pessoas em documentos como a carteira de motorista ou passaporte, desde que neles sejam codificados e devidamente criptografados os dados

biométricos que podem ser utilizados na autenticação. Já as técnicas de reconhecimento de face, por exemplo, podem ser utilizadas através de câmeras especiais dispostas em locais estratégicos, como a área de embarque/desembarque dos aeroportos, de forma a reconhecer suspeitos e evitar possíveis ataques terroristas.

De um lado, o uso da biometria auxilia neste processo proporcionando maior segurança. De outro lado, a coleta e o armazenamento de dados biométricos podem ser considerados uma invasão de privacidade, pois não se sabe quais dados serão guardados, e principalmente, quem terá acesso a esses dados. A privacidade é algo regulamentado nos Estados Unidos pelo "*Privacy Act*", ou simplesmente, Ato de Privacidade, editado em 1974. Além do ato de privacidade federal existem algumas outras leis americanas mais recentes, como o ato de 1999 Gramm-Leach-Bliley e o ato HIPAA (*Health Insurance Portability and Accountability Act*).

O ato federal de privacidade foi publicado para proteger cidadãos americanos de forma que informações sensíveis e privadas fossem coletadas por agências do governo, implicando que toda a informação deve ser coletada a partir de uma medida legal. Os dados quando autorizados por uma medida legal por sua vez, só podem ser utilizados por um tempo determinado, além de que o cidadão tem o direito de receber um relatório sobre quais dados foram coletados. Estas leis existem em quase todos os países do mundo. Os princípios de privacidade garantem que a informação deva ser precisa, mantida atualizada, e que não possa ser revelada a um terceiro a não ser que exista uma autorização clara do cidadão. Aos indivíduos cabe ainda o direito de corrigir estas informações pessoais.

A proposta deste trabalho visa pesquisar a viabilidade em implantar um sistema biométrico tanto para controle de acesso a uma Instituição de Ensino Superior como controle de freqüência. Um aspecto relevante associado a esta aplicação é a questão da segurança e privacidade dos indivíduos.

Algumas empresas líderes em softwares de segurança anunciam sua cooperação para ampliar o uso da biometria visando oferecer maior nível de segurança na rede utilizando um método de autorização pessoal confiável, afirmando que a integração da autenticação biométrica permitirá aos usuários acessarem seus computadores e conduzirem transações seguras. Sendo assim, a biometria é ideal para substituir senhas e cartões, pois os dados biométricos não podem ser esquecidos e principalmente compartilhados com terceiros.

As características físicas podem ser usadas como características biométricas, pois são universais (cada pessoa é classificada por um conjunto de características), únicas (indica que duas pessoas não possuem as mesmas características), permanentes (as características não podem ser modificadas) e podem ser medidas quantitativamente.

Este projeto visa analisar e discutir a questão de segurança versus privacidade em sistemas computacionais que utilizam a tecnologia biométrica, onde de um lado o uso da biometria auxilia nos processos de autenticação e identificação de indivíduos proporcionando maior segurança, e de outro lado à coleta, o armazenamento e a manipulação de dados biométricos podem ser considerados uma invasão de privacidade. Secundariamente apresentaremos o software desenvolvido para classificação de impressões digitais visando a otimização na fase de verificação dos indivíduos.

2. MATERIAIS E MÉTODOS

O desenvolvimento deste projeto será conduzido através de revisões bibliográficas a fim de comparar os fatores segurança e privacidade abordando diferentes tecnologias biométricas. Dentre as tecnologias biométricas, maior ênfase será dada ao reconhecimento das impressões digitais visando o controle de acesso e freqüência dos alunos de uma Instituição de Ensino Superior X (por questões de privacidade o nome da Instituição não será citado).

Neste projeto faremos uma abordagem junto aos alunos da Instituição através de questionários e pesquisas realizadas in loco, a fim de apresentar os possíveis resultados (aceitação, resistência, indiferença, insegurança, dentre outros) referentes à implantação de um sistema para controle de acesso (nas diversas dependências da Instituição) e freqüência (controle de faltas). Trata-se de uma proposta inovadora no cotidiano universitário que busca viabilizar o controle de acesso a Instituição e controlar a freqüência dos alunos, minimizando o tempo gasto em sala de aula na realização da chamada, promovendo desta forma um maior aproveitamento. Essa proposta consiste na aquisição de uma tecnologia biométrica que utilize um sistema de autenticação de indivíduos nas catracas de entrada dos campi.

Um aspecto de fundamental importância nesta aplicação diz respeito ao tempo de processamento, pois na fase de identificação, duas impressões digitais são comparadas. Faz-se o confronto entre uma impressão digital cadastrada em um banco de dados e uma impressão digital candidata, verificando se os pontos característicos são correspondentes em tipo e posição. Desta forma, é possível fazer o reconhecimento de uma pessoa. Como objetivo secundário deste estudo foi desenvolvido um software para classificação visando distribuir as imagens em classes propostas pelo FBI (*Federal Bureau Investigation*) a fim de minimizar a busca no banco de dados na fase de verificação dos alunos. A análise manual da impressão digital é uma tarefa tediosa, onde os aspectos para comparação são extremamente pequenos necessitando auxílio de lentes de aumento para obter um melhor exame da marca da impressão digital. Outro ponto a ser considerado é o tamanho do banco de dados, o que pode fazer a análise e comparação manual levar dias em alguns casos. Estes problemas podem ser facilmente superados pela automação do processo de verificação da impressão digital visando otimizar o processamento.

Dispositivos baseados em reconhecimento de impressões digitais são utilizados em numerosos projetos biométricos por todo o mundo. Em paralelo, outras tecnologias biométricas estão sendo desenvolvidas, melhoradas e refinadas até o ponto em que se tornem realidades comerciais. Nestes anos recentes, tem sido considerável o progresso em tecnologias biométricas baseadas no reconhecimento da íris e reconhecimento facial, tecnologias de reconhecimento sem contato.

As aplicações deste segmento biométrico, ou seja, das impressões digitais, destina-se ao aumento de segurança e agilidade em operações empresariais, governamentais ou institucionais. A última década tem sido de maturação da indústria biométrica apresentando um significante crescimento e uma larga escala de aplicações que começam a se desdobrar.

Opiniões controversas geram discussões quando o assunto é segurança, confiabilidade e privacidade o que nos permitirá após este estudo concluir a viabilidade na utilização das tecnologias biométricas.

Primeiramente foram aplicados questionários e entrevistas junto aos alunos da Instituição. Como projeto piloto entrevistamos uma população de 300 alunos inicialmente espalhados nos diversos cursos, conforme Figura 1.

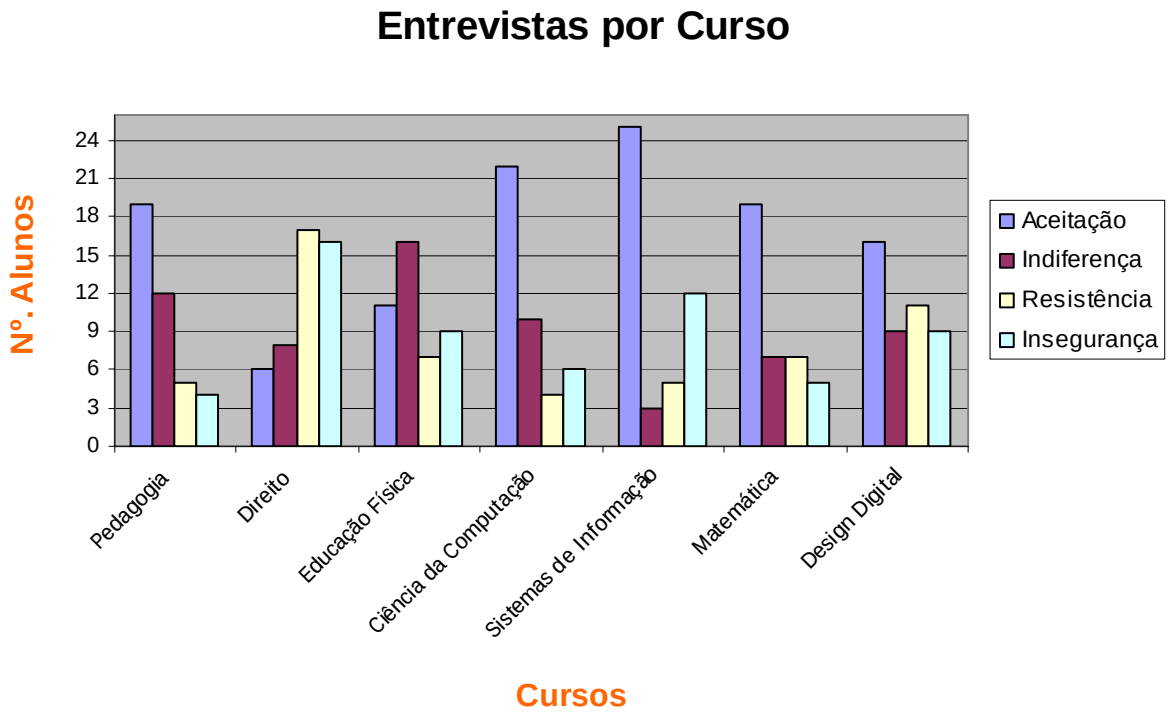

Figura 1: Entrevista com alunos de diversos cursos para averiguar opiniões com relação ao uso de uma tecnologia biométrica para controle de acesso e freqüência.

Após análise dos dados coletados foi possível constatar o alto nível de aceitação da nova tecnologia na maioria dos cursos. Tal fato sofreu resistência somente no curso de Direito onde os atributos mais citados foram a resistência e a insegurança, respectivamente.

Realizamos uma segunda abordagem com os mesmos alunos entrevistados anteriormente para verificar o impacto com relação ao tempo despendido com chamadas, a questão da segurança e a invasão de privacidade. Alguns alunos alegam que o uso de uma tecnologia biométrica poderia gerar um maior aproveitamento em sala de aula uma vez que não seria mais necessário efetuar a chamada. Este fato é muito relevante em cursos cujos 1os anos tem aproximadamente 85 alunos. Outros alunos se mostraram um pouco preocupados com relação à segurança e invasão de privacidade, alegando que muitas vezes a secretaria é bastante desorganizada, por exemplo, e a manipulação destes dados não seria controlada. Ainda assim pudemos constatar que a aceitação da tecnologia proposta é viável. Os resultados podem ser observados na Figura 2.

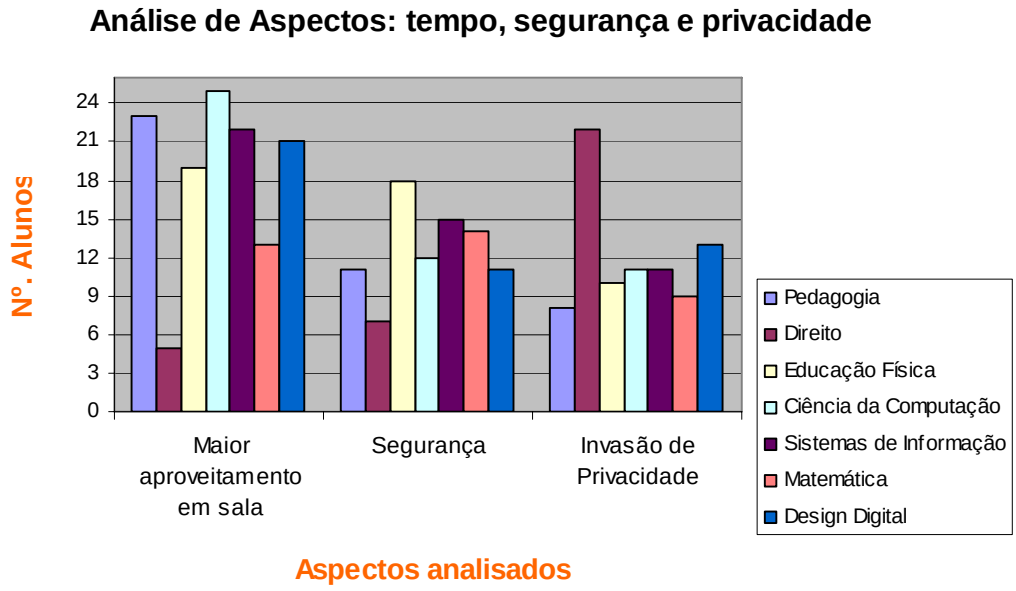

Figura 2: Análise dos aspectos: tempo de aproveitamento em sala, segurança e invasão de privacidade.

Em momento oportuno tais dados serão fornecidos aos responsáveis da Instituição para aprovação do uso da nova tecnologia proposta.

2.1. Desenvolvimento do Software de Classificação de Impressões Digitais

Os sistemas automáticos de identificação de impressões digitais (AFIS – Automated Fingerprint Identification System) consistem em vários estágios de processamento, dentre os quais podemos citar melhoria de imagem, cálculo da imagem direcional, suavização do mapa direcional visando a redução de ruídos. Há um crescente interesse em classificação e verificação de impressões digitais automáticas devido à necessidade de facilitar o manuseio de bancos de dados e agilizar o tempo de processamento.

Os AFIS's atuais usam métodos de classificação exclusiva, onde impressões digitais são divididas em algumas classes distintas predefinidas de acordo com suas características globais.

A maioria dos sistemas de identificação de impressões digitais são baseados em comparações de minúcias que constituem um padrão de impressão digital. A detecção automática de minúcias é um processo extremamente crítico, especialmente em imagens de baixa qualidade, onde ruídos e deficiência no contraste podem gerar configurações de pontos similares ou ignorar minúcias verdadeiras. A proposta principal de um AFIS é minimizar o tempo e o trabalho de um especialista humano.

As impressões digitais de pessoas ou de dedos diferentes de uma mesma pessoa diferenciam-se sob dois critérios principais. O primeiro critério está relacionado ao grupo da impressão e o segundo critério está relacionado à distribuição das minúcias. O critério de grupo representa uma visão global da impressão digital, definida pelo comportamento das linhas dactilares nos dedos. Esta visão macroscópica permite, em um

processo de comparação de duas impressões digitais, afirmar a não identidade no caso de grupos diferentes. Quando os grupos de duas impressões digitais (padrão e candidata) são iguais, o segundo critério, das minúcias, permite afirmar ou não a identidade, em função de um mapeamento posicional entre os diversos tipos de minúcias.

A classificação e verificação (comparação) são duas funções primárias requeridas em um processamento para reconhecimento de impressões digitais. A classificação é feita baseada em macro-aspectos ou características das cristas. Desta forma as impressões digitais são agrupadas de acordo com sua configuração geométrica. A meta da classificação é assegurar que uma dada impressão digital pertença a uma classe específica de acordo com suas propriedades geométricas.

O software desenvolvido pode ser manipulado facilmente pelo usuário. Foi desenvolvida uma biblioteca em C++ onde implementamos os algoritmos propostos para classificação.

O programa de classificação permite a seleção de pontos falsos caso apareçam e gera um relatório descrevendo o número de pontos núcleos e deltas encontrados, bem como uma mensagem de erro na ocorrência de pontos falsos.

Observe a interface gráfica na Figura 3. Inicialmente o programa carrega uma imagem e aplica um filtro de contraste caso seja necessário.

Figura 3: Interface gráfica do software para classificação.

As linhas típicas no padrão da impressão digital são reconhecidas como cristas papilares. O fluxo dessas cristas formam diferentes padrões geométricos classificados como arcos, presilhas, verticilos, e outras estruturas mais detalhadas como cristas finais e cristas bifurcadas, conhecidas como minúcias ou pontos característicos. Observando esses aspectos, a maior parte das técnicas utilizadas para classificação e

verificação automática de impressões digitais dependem da determinação da direção do fluxo das cristas papilares.

A imagem direcional fornece informações contidas nos padrões de impressões digitais e pode ser seguramente calculada em imagens ruidosas, uma vez que para atenuar a influência dos ruídos basta tomar a média das direções. Por esta razão, a maioria dos métodos de classificação existentes fazem uso da imagem direcional.

Enfatizamos neste trabalho a suavização do mapa direcional. O cálculo da imagem direcional permite extrair atributos (direção) em um bloco considerado. Entretanto, para eliminar ruídos é necessário aplicar a suavização. Resultados experimentais mostram que o método que estamos propondo permite fazer a suavização gerando um mapa direcional menos distorcido, conforme mostra a Figura 4.

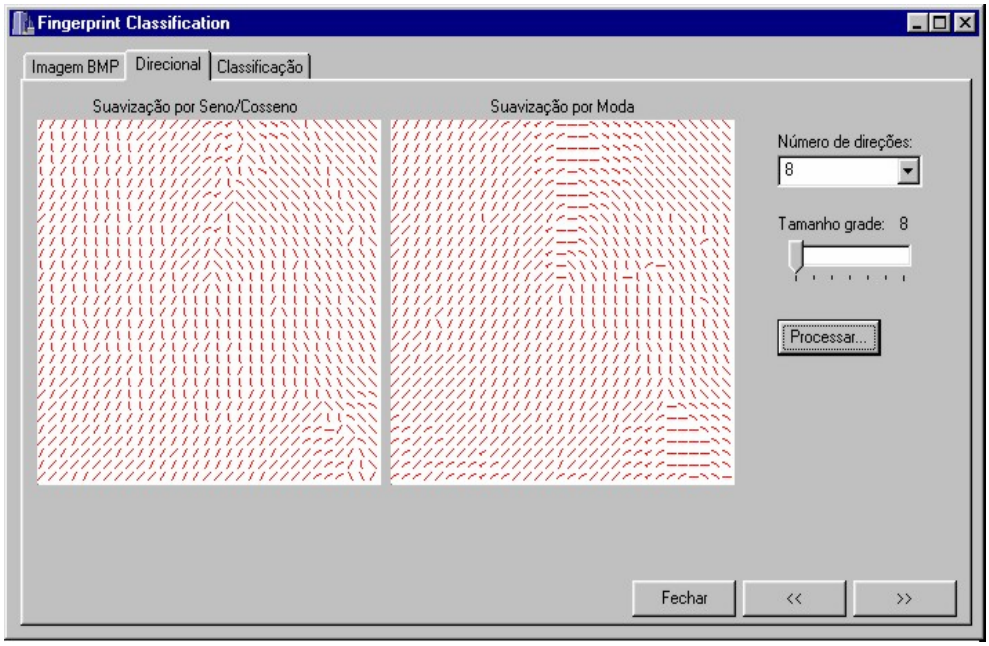

Figura 4: Suavização dos mapas direcionais.

Na etapa final o usuário pode escolher qual mapa direcional será utilizado para classificação da imagem. Observe que os pontos de interesse para classificação são apresentados em diferentes cores: verde para os núcleos, azul para os pontos deltas e vermelho para os pontos ordinários. Os pontos utilizados para classificação são os núcleos e os deltas. Desta forma é possível localizá-los facilmente neste programa. Pode-se ainda selecionar os pontos falsos que porventura apareçam para que sejam desconsiderados na classificação. Observe a interface gráfica após a classificação na Figura 5.

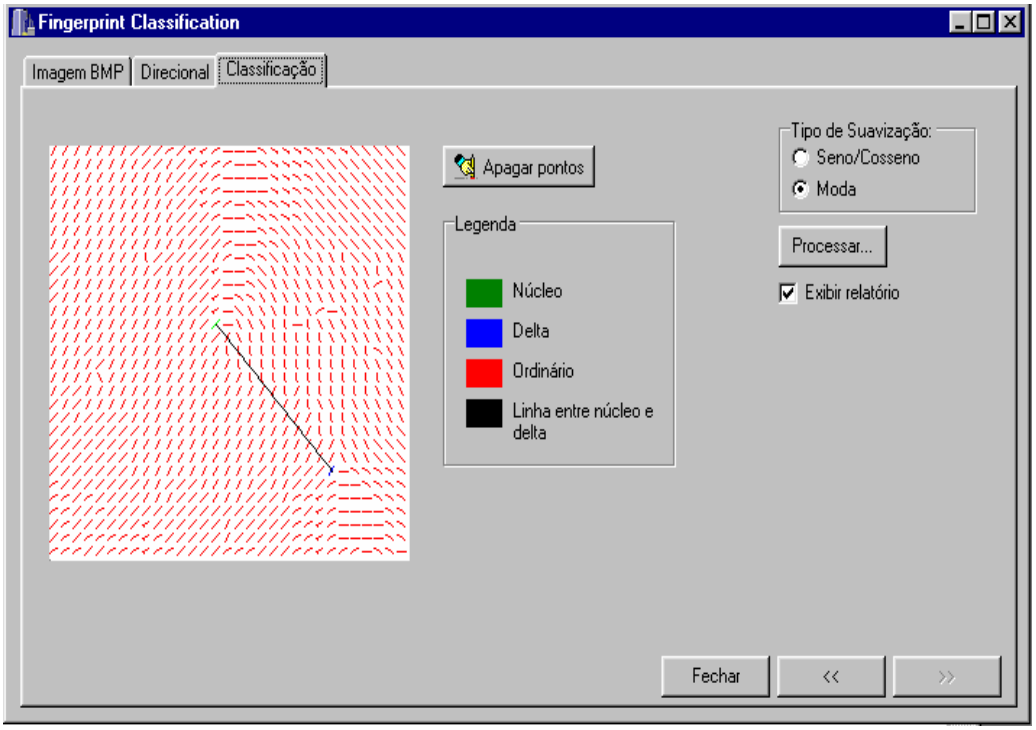

Figura 5: Interface gráfica após a classificação.

Após classificação, o programa gera um relatório com informações sobre a imagem classificada: qual classe pertence, quantos pontos ordinários, núcleos e deltas possui e uma legenda das cores atribuídas, conforme Figura 6.

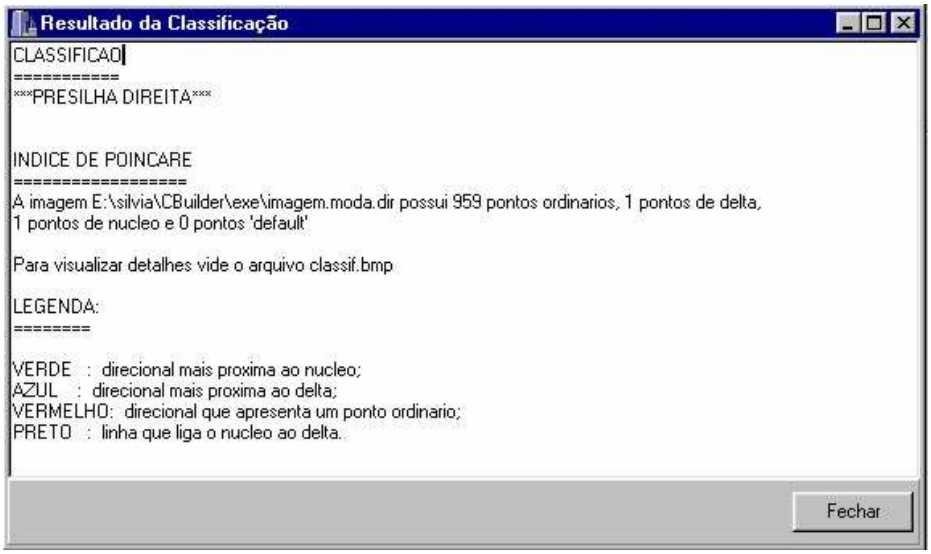

Figura 6: Interface gráfica após a classificação - relatório.

3. RESULTADOS E DISCUSSÃO

O foco principal deste trabalho foi a análise juntamente aos alunos de uma Instituição de Ensino Superior para averiguar o grau de aceitação de uma tecnologia biométrica para controle de acesso e freqüência. Segundo questionários e entrevistas aplicados in loco foi possível constatar que apesar da insegurança com relação a privacidade e manipulação dos dados, grande parte dos alunos são favoráveis ao uso da tecnologia biométrica alegando inclusive o ganho de tempo para maior aproveitamento em sala de aula uma vez que não seriam mais realizadas as chamadas. Observamos também que somente os alunos do curso de Direito apresentaram resistência ao uso de tal tecnologia alegando questões de segurança e invasão de privacidade.

Para aplicação em impressões digitais, o software de classificação desenvolvido foi testado para 330 imagens, provenientes de quatro bancos de dados. O Nist Special Database 4, com 50 imagens disponibilizadas pelo FBI (Federal Bureau of Investigation). O banco de dados DSPAMI com 14 imagens e o FINGDB, com 168 imagens, ambos fornecidos pelo Biometric Systems Lab, e por fim um banco de dados obtido no Departamento de Dactiloscopia do Estado de São Paulo, com 98 imagens. Considerando esse universo foi possível classificar 80% das imagens automaticamente.

Quanto ao software de classificação foram atribuídas cores para diferenciar os pontos de interesse, de forma que o usuário possa visualizar melhor prováveis pontos falsos que podem ser desconsiderados manualmente. Este software foi implementado em linguagem C++ e possui alto grau de flexibilidade, uma vez que o usuário pode optar pelo número de direções, tamanho da grade para suavização e também o mapa direcional que será utilizado para a classificação (seno-cosseno ou estatístico). Finalmente o programa gera um relatório com informações sobre a imagem classificada.

Um dos pontos relevantes apontados pelos usuários é a facilidade, pois senhas e cartões podem ser perdidos, roubados ou esquecidos.

4. CONCLUSÃO

Segurança e confiabilidade são pré-requisitos fundamentais para o uso e também desenvolvimento de sistemas, principalmente quando se trata de autenticação e validação de usuários para acesso a transações financeiras, acesso a locais restritos, validação de documentos e tantas outras aplicações. Desta forma, muitas são as justificativas para a adoção de uma tecnologia biométrica. Algumas empresas líderes em software de segurança anunciam sua cooperação para ampliar o uso da biometria visando oferecer aos usuários o mais alto nível de segurança na rede baseado em um método de autorização pessoal confiável. Desta forma, a biometria é ideal para substituir senhas e cartões, pois os dados biométricos não podem ser esquecidos, perdidos, roubados e principalmente compartilhados com terceiros.

Porém há aqueles que dizem o contrário e afirmam que terão seus dados expostos em um banco de dados, desconhecem as pessoas que terão acesso a estas informações e quem são os responsáveis pela manipulação desses dados.

Opiniões controversas geram discussões quando o assunto é segurança, confiabilidade e privacidade o que nos permite concluir que a biometria por hora deve ser incorporada ao nosso cotidiano, mas associada ao uso de uma chave eletrônica ou qualquer outro artifício que proporcione otimizar a segurança de um sistema.

REFERÊNCIAS

CAPPELLI, Raffaele et al, 1999. *Fingerprint Classification by Directional Image Partitioning*. IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 21, nº 5.

FBI: Federal Bureau of Investigation, 1984. *The Science of Fingerprints: Classification and Uses*. U.S. Government Printing Office, Washington, DC.

HEUSER, Carlos Alberto. Projeto de Banco de Dados. Porto Alegre: Sagra Luzzatto, 2001.

KARU, Kalle; JAIN, Anil J., 1996. *Fingerprint Classification. Pattern Recognition. V*ol. 29, nº 3, pp. 389-404.

MORAES, Alexandre F. de, 2006. *Método para Avaliação da Tecnologia Biométrica na Segurança de Aeroportos*. Dissertação de mestrado apresentada a Escola Politécnica da Universidade de São Paulo.

PRESSMAN, Roger S. Engenharia de Software. Rio de Janeiro: McGraw-Hill, 2002.

SRINIVASAN, V. S.; MURTHY, N. N., 1992. *Detection of Singular Points in Fingerpint Images*. Pattern Recognition, vol. 25, nº 2, pp. 139-153.

URL´s:

ALECRIM, E., 2006. *Introdução a Biometria*. Disponível: http://www.infowester.com/biometria.php. Acesso em: 19 de julho de 2006.

DANTAS, G. F. L., 2006. *Sistemas Biométricos de Identificação pela Imagem Facial*. Disponível: http://www.peritocriminal.com.br/biometria.htm. Acesso em: 26 de outubro de 2006.

FONTES, M.F; DUARTE, O. C. M. B., 2006. *Smart Cards para o Controle de Acesso*. Disponível: http://www.gta.ufrj.br/~fernandes/Smart_Card_Trab.pdf. Acesso em: 20 de outubro de 2006.