Um Overview Sobre Reconhecimento de Padrões

Nogueira, A. Azevedo, J. Baptista, V. Siqueira, S.
Sistemas de Informação – Associação Educacional Dom Bosco
Estrada Resende-Riachuelo, 2535 – Resende – RJ
{aislannogueira@yahoo.com.br, jfaelc@yahoo.com.br, vcb_21@hotmail.com,
simarasiqueira@hotmail.com}

RESUMO

Este artigo tem como propósito apresentar os principais tipos de padrões de reconhecimento que podem ser utilizados em aplicações como o processo de autenticação de usuários, oferecendo maior segurança e confiabilidade a outros sistemas. Para tanto, a utilização de mais de um tipo de padrão se faz necessária, haja visto que a utilização tradicional de login e senha, apesar de também serem padrões ainda muito utilizados, já não são tão confiáveis tampouco suficientes.

Palavras-Chave: Padrão, biometria, minúcias, invasivas.

1. INTRODUÇÃO

Desde a invenção dos primeiros computadores eletrônicos digitais, a quantidade e a complexidade das tarefas sob a responsabilidade destas máquinas vêm aumentando consideravelmente. O que antes era restrito à geração de tabelas de cálculo de trajetórias balísticas, como foi o caso do computador ENIAC (Eletronical Numerical Integrator And Computer) durante a 2ª Guerra Mundial, evoluiu para a execução de tarefas bem mais ambiciosas. Métodos computacionais essencialmente exatos e determinísticos passaram a dividir espaço com métodos aproximados e não determinísticos que estão mais próximos da forma como o ser humano se comporta. Tais métodos, que procuram reproduzir determinadas habilidades dos seres humanos, são comumente denominados "inteligentes" e são amplamente utilizados em reconhecimento de padrões. Um padrão é qualquer entidade da qual é possível extrair algum tipo de característica, seja ela simbólica ou numérica, e o que as técnicas computacionais de reconhecimento de padrões buscam, é por uma maneira eficiente de, a partir destas características, organizarem estes padrões em agrupamentos ou classes que compartilhem determinadas semelhanças.

2. RECONHECIMENTO DE PADRÕES

Na natureza os padrões se manifestam de diversas maneiras como, por exemplo, sons, formas, imagens, cheiros e sabores e a todo instante os seres humanos, e também outros animais, percebem e interagem com estes padrões com extrema naturalidade. Exemplos disso são as habilidades que o ser humano tem de diferenciar o som do motor de um automóvel do som de uma música, ou ainda, a habilidade que um animal selvagem tem de distinguir uma presa de um predador. A naturalidade inerente a estas habilidades faz com que o ser humano sequer imagine as complexidades cognitivas que estão por trás

delas. Complexidades que se tornam evidentes quando se tenta reproduzi-las artificialmente em um computador, o que há muito desafia a comunidade científica interessada no assunto.

O reconhecimento de padrões por computador é uma das mais importantes ferramentas usadas no campo da inteligência de máquina. Atualmente está presente em inúmeras áreas do conhecimento e encontra aplicações diretas em visão computacional, análise sísmica, reconhecimento de locutores e de comandos a voz, classificação de sinais de radar, reconhecimento de faces, identificação de íris, identificação de digitais, análise e entendimento de sinais eletrocardiográficos, previsão de comportamentos em mercados financeiros, reconhecimento de caracteres impressos e manuscritos, além de outras.

2.1 RECONHECIMENTO DE CARACTERES

Dentre as modalidades de reconhecimento de padrões, o reconhecimento de caracteres é uma das mais conhecidas e exploradas pela comunidade científica. Prova disso é a grande quantidade de artigos publicados anualmente em periódicos e anais de conferências nacionais e internacionais relacionadas, e até mesmo especializadas no assunto. O reconhecimento de caracteres consiste em a partir de características extraídas de um conjunto de caracteres, separá-los em 10 classes, no caso dos algarismos, ou 26 classes, no caso das letras do alfabeto ocidental.

Os primeiros sistemas comerciais que surgiram foram os chamados sistemas OCR (Optical Character Recognition). Nos OCR's os caracteres a serem reconhecidos se encontram impressos em uma determinada fonte e, por isso, apresentam um formato bem comportado assim como as letras deste texto. Inicialmente os OCR's eram capazes de reconhecer apenas tipos específicos de fontes como, OCR-A, OCR-B, Pica, Elite, Courier, etc. Em seguida, surgiram os OCR's multi-fonte que permitiram que a capacidade de reconhecimento se estendesse para um conjunto maior de opções de fontes. Por fim, surgiram os OCR's omni-fonte, capazes de reconhecer qualquer fonte.

O passo seguinte foi dado em direção aos sistemas ICR (Intelligent Character Recognition). Diferentemente dos OCR's, os ICR's lidam com um problema bem mais complexo, uma vez que os caracteres a serem reconhecidos são manuscritos e não mais impressos. Esta complexidade é devida às variações de estilo existentes na escrita manuscrita, pois de uma pessoa para outra um mesmo caractere pode se apresentar de diferentes formas. Até uma mesma pessoa pode escrever um mesmo caractere de maneiras diferentes. A escrita manuscrita pode ainda se apresentar de duas formas, isolada e cursiva, sendo que no primeiro caso os caracteres estão dispostos de forma não conectada, enquanto que no segundo estão dispostos de forma completamente irrestrita, ou seja, conectados ou eventualmente desconectados.

Os dados de entrada de um sistema de reconhecimento de caracteres podem ser provenientes da digitalização de um documento, por meio de um scanner, ou provenientes de superfícies de cristal líquido, que capturam os caracteres escritos sobre ela com um bastão que imita uma caneta. Estas duas abordagens compreendem os sistemas de reconhecimento denominados off-line e on-line, respectivamente. No caso on-line, à medida que o traço do caractere é delineado pelo escritor, este é prontamente apresentado ao sistema, enquanto no caso off-line, somente a imagem completa do que foi escrito

previamente é apresentada ao sistema. Os OCR's são essencialmente do tipo off-line, enquanto os ICR's podem ser de ambos os tipos.

Hoje, ao contrário de quando começaram a ser comercializados, os reconhecedores de caracteres apresentam desempenhos bem melhores, preços mais acessíveis e são facilmente encontrados no mercado. Os OCR's estão presentes na maioria dos programas de interface dos scanners e os ICR's do tipo on-line são uma das funcionalidades encontradas nos modernos PDA's (Personal digital assistants). Os ICR's do tipo off-line estão disponíveis principalmente para o reconhecimento de documentos, em especial formulários.

2.2 RECONHECIMENTO DA ASSINATURA MANUSCRITA

O ritmo necessário para escrever uma assinatura pode ser usado em um sistema de identificação automático. Esta técnica já é muito usada e popular, uma vez que todos os cheques são verificados usando-se as assinaturas.

Existem dois métodos de identificação: um método examina a assinatura já escrita, comparando-a, como uma imagem, com um modelo armazenado. A maior desvantagem deste método é que ele não pode detectar fotocópias das assinaturas. O outro método estuda a dinâmica da assinatura. Este esquema analisa o processo dinâmico da realização de uma assinatura – ritmo de escrita, contato com a superfície, tempo total, pontos de curva, laços, velocidade e aceleração. Os dispositivos utilizados para análise dinâmica são canetas óticas e superfícies sensíveis.

Como todas as características comportamentais, as assinaturas estão sujeitas ao humor do usuário, ao ambiente, à caneta, ao papel, e assim por diante. As assinaturas de algumas pessoas são muito consistentes, enquanto as de outras variam muito.

O modelo de assinatura tem tipicamente 1Kbyte. Isto facilita seu uso on-line e com cartões inteligentes. Outras características são: possui baixa FAR (Falsa aceitação real), FRR (Falsa rejeição real) em torno de 10%, é fácil de usar e tem um tempo de verificação entre 5 a 10 segundos.

2.3 RECONHECIMENTO PELO RITMO DA DIGITAÇÃO

Como a assinatura, o ritmo de digitação exibe o mesmo fator neurofísico que pode ser utilizado na identificação única de um indivíduo. Esquemas de ritmo de digitação analisam o modo como um usuário digita em um terminal, monitorando o teclado 1000 vezes por segundo.

O método normal é a utilização das latências de digitação – o tempo entre a digitação de duas teclas, conforme ilustrado na Figura 2.1. Certos dígrafos, ou digitação de duas letras adjacentes, freqüentemente, apresentam padrões de tempo únicos que podem ser usados para caracterizar um indivíduo.

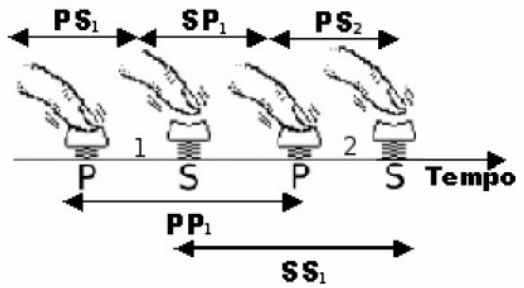

Fig. 2.1 – Representação das características observadas durante a digitação dos caracteres 1 e 2.

PS é o tempo em que a tecla permanece pressionada, SP é o intervalo até a próxima tecla ser pressionada, PP é o intervalo de tempo que o usuário leva para pressionar duas teclas consecutivas e SS é o intervalo de tempo que o usuário leva para soltar duas teclas consecutivas.

O procedimento geral de identificação e verificação requer que o usuário gere um perfil ou modelo. Na operação, a verificação requer a geração de um perfil de digitação, que é comparado com o modelo. Se existir uma grande diferença entre os dois perfis, o usuário terá seu acesso negado. Uma das vantagens deste método é que o usuário não percebe quando está sendo autenticado, ao menos que ele tenha sido informado anteriormente. Outra vantagem é que o cadastro e a verificação não são invasivos.

O ritmo da digitação é identificado pela velocidade, espaço de tempo entre o acionamento de cada tecla bem como duração de pressão sobre a mesma e liberação. Dificilmente poderá ser imitado por usuário ilegítimo, pois, mesmo conhecendo a senha da pessoa pela qual ele tentará passar, dificilmente haverá permissão de acesso.

2.4 RECONHECIMENTO PELA IMPRESSÃO DIGITAL

A impressão digital é composta por vários sulcos, que em sua formação apresentam diferenças chamadas de ponto de minúcias Figura 2.2, ou seja, aquelas partes em que os sulcos se dividem (vales) ou onde terminam abruptamente (terminação). Cada um desses pontos tem características únicas, que podem ser medidas. Ao compararmos duas digitais podemos determinar seguramente se pertencem a pessoas distintas, baseados nos pontos de minúcias. Há muitos anos os institutos oficiais de identificação de diversos países já realizam o reconhecimento de pessoas através do sistema de análise da impressão digital. Na Europa, judicialmente, são necessárias 12 minúcias para saber quem é uma pessoa. Os leitores biométricos são capazes de identificar mais de 40 minúcias de uma impressão digital.

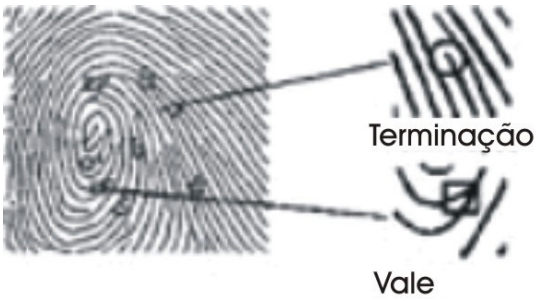

Fig. 2.2 – Ponto de minúcias

A impressão digital é o método de biometria mais utilizado mundo afora. Só para se ter uma idéia, os dispositivos biométricos por impressão digital contabilizam 50% do que foi vendido de produtos do gênero em 2001, segundo o Biometric Group. Além de ser mais barato, sem barreiras culturais, ele também é seguro. Existe uma chance em 100 bilhões de uma pessoa ter a mesma digital que a outra.

Existem três dispositivos que podem coletar a impressão digital: ótico, capacitivo e ultra-sônico. O primeiro trabalha através da reflexão da luz sobre o dedo. Já o segundo mede o calor que sai da digital. Por último, o terceiro envia sinais sonoros e analisa o retorno deles como se fosse um radar milimétrico.

Não é preciso muito que a opção do sensor ótico é a mais utilizada e também a mais segura. Tudo porque o usuário pode estar com o dedo sujo a ainda assim ser reconhecido. Uma vez que a sua digital não será colocada diretamente no sensor, mas em um vidro onde ela é analisada por um laser.

Este é o método que, atualmente, oferece a melhor relação entre o preço, aceitabilidade e precisão. Contudo, os últimos resultados de avaliações mostram que seu desempenho depende muito da qualidade das imagens adquiridas, particularmente durante a fase de cadastro.

A obtenção de uma amostra pode ser feita de forma voluntária/consciente (com o consentimento da pessoa) ou de forma involuntária/inconsciente (sem o consentimento da pessoa).

2.5 RECONHECIMENTO PELA GEOMETRIA DA MÃO

A geometria da mão tem sido usada em aplicações desde o começo de 1970. Ela baseia-se no fato de que virtualmente não existem duas pessoas com mãos idênticas e de que o formato da mão não sofre mudanças significativas após certa idade. Existem diversas vantagens no uso da forma tridimensional da mão da pessoa como um dispositivo de identificação. Primeiramente, é razoavelmente rápida. Leva menos que 2 segundos para capturar a imagem de uma mão e produzir a análise resultante. Secundariamente, requer pouco espaço de armazenamento. É também requerido pouco esforço ou atenção do usuário durante a verificação, e os usuários autorizados são raramente rejeitados.

As dimensões da mão, tal como tamanho do dedo, largura e área são as principais características usadas nas análises. Para a captura, o usuário posiciona sua mão no leitor, alinhando os dedos, e uma câmara posicionada acima da mão captura a imagem. Medidas tridimensionais de pontos selecionados são tomadas e o sistema extrai destas medidas um identificador matemático único na criação do modelo. Um típico modelo requer cerca de nove bytes de armazenamento.

Um dos problemas com os sistemas que utilizam a geometria da mão é causado pela rotação da mão quando colocada no leitor. Isto se resolve usando pinos de posicionamento dos dedos. O sistema também deve levar em conta os diferentes tamanhos das mãos, em diferentes usuários e seu desempenho não deve ser prejudicado por sujeira e cortes na mão da pessoa. A Figura 2.3 apresenta um leitor de geometria da mão.

Fig. 2.3 - Leitor de geometria da mão

2.6 RECONHECIMENTO PELA VOZ

Programas que possibilitam aos computadores reconhecer a voz humana tiveram um avanço notável nos últimos anos. Pode não estar longe o dia em que o computador será capaz de entender sua pergunta - ou pelo menos de pedir que você a repita. Isso não quer dizer que o computador compreende o que falamos. Apenas que ele já é capaz de ouvir e transcrever um texto com um grande índice de acerto. Compreender a fala transcrita envolve uma inteligência que a máquina não tem.

Quando um software de reconhecimento por voz é instalado no computador faz-se necessário uma pré-calibração do software com a voz do usuário.

O programa solicita que o usuário pronuncie um conjunto de palavras de forma pausada e clara. Este conjunto de palavras será armazenado em um banco de dados para que o mesmo possa ter um perfil de comparação vocal.

Quando o usuário fala o software identifica o timbre das palavras pronunciadas e compara com a sua base de dados para identificar com o máximo de precisão a palavra pronunciada.

Pelo fato dos diferentes biótipos vocálicos humanos é necessária a criação de um novo perfil para cada usuário que deseje utilizar o software.

O reconhecimento automático da voz é o processo de extração automática da informação lingüística do sinal de voz. A informação lingüística contida no sinal de voz está codificada de modo que o elevado grau de variabilidade do sinal, causada pelo ambiente e pelo locutor, praticamente não interfere na percepção da informação pelo homem.

O reconhecimento de voz, porém, é restringido por certos problemas que dificultam o processamento. As principais dificuldades relacionadas ao reconhecimento de voz podem ser resumidas nos seguintes aspectos:

- Diferenças fonéticas na mesma palavra pronunciada várias vezes;
- As dificuldades na segmentação da fala;
- As variações nas características da fala;
- Com insuficiente uso do conhecimento lingüístico.

As restrições acima irão influenciar características como precisão, tipo de aplicação, custo, entre outras. Para contornar algumas restrições foram determinados certos fatores para o reconhecimento:

- Dependência do Locutor (dependendo do sistema escolhido);
- Tipo de fala (reconhecimento de palavras isoladas ou fala contínua);
- Tamanho do vocabulário (palavras semelhantes para o algoritmo classificador).

2.7 RECONHECIMENTO PELA FACE

O uso de reconhecimento de face é o método mais natural de identificação biométrica. O uso das características da face para identificação automática é uma tarefa difícil porque a aparência facial tende a mudar a todo tempo. As variações podem ser causadas por diferentes expressões faciais, mudanças no estilo do cabelo, posição da cabeça, ângulo da câmara, condições de luz, etc. Apesar das dificuldades envolvidas, o reconhecimento facial já foi abordado de diversas maneiras, variando de sistemas de reconhecimento de padrões por redes neurais até varreduras infravermelhas de pontos estratégicos (como posição dos olhos e da boca) na face.

Muitos sistemas de reconhecimento de face utilizam um computador com uma câmera para capturar as imagens da face. Estes sistemas utilizam medidas da face como distâncias entre os olhos, nariz, queixo, boca e linha dos cabelos como meio de verificação. Alguns sistemas também podem executar testes "animados" para evitar que o sistema seja fraudado por uma fotografia.

Variáveis como óculos de sol, bigode, barba, expressões faciais entre outras, podem causar falsas rejeições nesses sistemas, não sendo, portanto, sistemas tão confiáveis.

2.8 RECONHECIMENTO PELA ÍRIS

Embora exista um conjunto grande de processos para reconhecimento da íris, existe um conjunto de passos comuns a todos. Na sua grande maioria os processos só diferem no algoritmo escolhido para a detecção e reconhecimento de padrões na íris. As primeiras etapas, designadas por aquisição e pré-processamento do sinal são semelhantes para todos os casos.

Na etapa seguinte é necessário gerar aquilo que se designa habitualmente por "assinatura" ou template (modelo de concepção lógica) da íris, ou seja, converter o padrão numa representação binária que se possa armazenar numa base de dados para posterior comparação. Nesta fase existe um conjunto de algoritmos a considerar baseados em wavelets (pequenas ondas) transformadas e outros filtros diversos.

Os equipamentos comerciais usam habitualmente o algoritmo de Daugman, que está patenteado e cuja utilização não é gratuita. Este algoritmo é, entre todos, o que melhores resultados apresenta. Mas é importante citar que existem ainda uma série de alternativas que devem ser consideradas, como a de Libor Masek que apenas difere do anterior em alguns pontos. Uma outra abordagem, baseia-se numa técnica simples que permite obter resultados bastante satisfatórios, é o algoritmo de "adaptive tresholding". Este algoritmo foi desenvolvido no CBSP (Center for Biometric Signal Processing) e caracteriza-se por ter um overhead computacional menor, funcionando igualmente bem com imagens de menor qualidade.

As etapas para o registro ou autenticação são explicadas na Figura 2.4 abaixo e detalhadas em seguida.

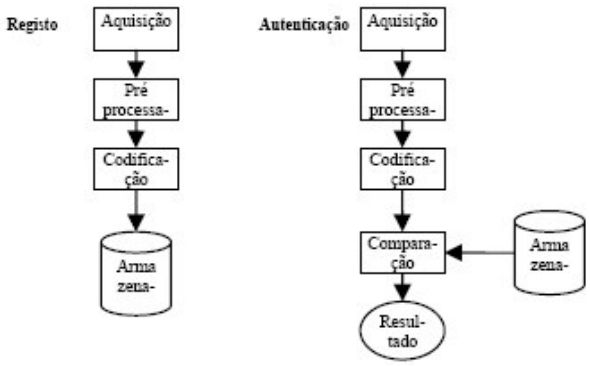

Fig. 2.4 – Registro ou autenticação

O processo de aquisição consiste na captura e digitalização de uma imagem completa do olho de um indivíduo. A captura é feita através de câmeras fotográficas digitais ou leitores próprios e tem características de uma imagem fotográfica normal. Assim

sendo, os cuidados que caracterizam esta fase têm como objetivo garantir que o sinal que vai ser processado é captado com a maior perfeição possível.

Nesta fase é importante dar atenção às dimensões e posições das imagens. A área captada deve ser sempre relativamente semelhante, de forma a facilitar a identificação da zona correspondente à íris. Também é importante dar atenção ao ambiente onde será feita a captura da imagem tomando cuidado com a luminosidade, que devem ser o mais uniforme possível.

Entre a fase de digitalização e a fase de posterior reconhecimento é conveniente que as condições sejam semelhantes, de forma a garantir que os padrões serão o mais semelhante possível.

2.9 RECONHECIMENTO PELA RETINA

Algumas pesquisas têm provado que o padrão de veias da retina é a característica com maior garantia de unidade que uma pessoa pode ter. Os analisadores de retina medem esse padrão de vasos sangüíneos usando um laser de baixa intensidade e uma câmara. Nesta técnica, deve-se colocar o olho perto de uma câmara para obter uma imagem focada.

A análise de retina é considerada um dos métodos biométricos mais seguros. A FAR é nula e as fraudes até hoje são desconhecidas. Olhos falsos, lentes de contato e transplantes não podem quebrar a segurança do sistema.

Recentes pesquisas médicas mostraram, entretanto, que as características da retina não são tão estáveis como pensava-se anteriormente: elas são afetadas por doenças, incluindo doenças das quais o paciente pode não estar ciente. Muitas pessoas ficam temerosas em colocar seu olho próximo a uma fonte de luz e aos problemas que isto possa causar. Como resultado, esta técnica impulsionou o caminho da utilização da análise da íris, que é menos invasiva. A Figura 2.5 apresenta um exemplo de analisador de retina.

Fig. 2.5 - Analisador de retina

Este método não é vulnerável à fraudes: falsos olhos, lentes de contato e transplantes não quebram a segurança do sistema.

3. APLICABILIDADE

Você é quem diz ser? Responder rápido a esta pergunta poderá implicar em algo mais do que dar uma olhada no RG. Talvez você tenha de submeter parte da sua biologia pessoal a um scanner biométrico. Os scanners de voz, impressão digital, rosto e íris foram, durante anos, elementos da ficção científica, mas com o medo do roubo de identidade e o temor ao terrorismo, estão se tornando parte de nossa rotina diária.

Atualmente, utiliza-se o reconhecimento facial, em aeroportos para identificar possíveis terroristas. Alguns colégios empregam leitores de digitais para garantir acesso exclusivo a empregados e estudantes à suas dependências. Já os scanners de íris ajudam a melhorar a segurança em alfândegas. Alguns bancos começam a usar gravações de voz para verificar as transações realizadas por telefone.

Técnicas invasivas, ou seja, técnicas trazem riscos ao ser humano, podem ser uma das maiores desvantagens ao se aplicar um sistema biométrico, mas essa grande desvantagem pode ser suprida pelo nível de segurança oferecido por sistemas biométricos como esses. Outra grande desvantagem é o preço do software, hardware e implantação de um sistema biométrico, já que em alguns sistemas, como o reconhecimento pela íris, por exemplo, a patente do software e o leitor da íris chega a custar US$ 5.000 e US$ 995 respectivamente, mas em compensação o custo do software, hardware e da implantação de um sistema biométrico baseado no reconhecimento pela impressão digital requerem um gasto muito mais baixo, já que a licença do software, na maioria das vezes já vem inclusa no pacote de compra do leitor biométrico, e este chega a custar em média R$ 170,00.

Teoricamente, quaisquer características humanas, físicas ou comportamentais, podem ser utilizadas para a identificação de pessoas, desde que satisfaçam os seguintes requerimentos:

- Universalidade: significa que todas as pessoas devem possuir a característica;
- Singularidade: indica que esta característica não pode ser igual em pessoas diferentes;
- Permanência: significa que a característica não deve variar com o tempo;
- Mensurabilidade: indica que a característica pode ser medida quantitativamente.

Na prática, existem outros requerimentos importantes:

- Desempenho: refere-se à precisão de identificação, os recursos requeridos para conseguir uma precisão de identificação aceitável e ao trabalho ou fatores ambientes que afetam a precisão da identificação;
- Aceitabilidade: indica o quanto as pessoas estão dispostas a aceitar os sistemas biométricos;
- Proteção: refere-se à facilidade/dificuldade de enganar o sistema com técnicas fraudulentas.

4. Conclusão

O Reconhecimento de Padrões tornou-se uma realidade no ramo da segurança de redes e controle de acesso. Assim sendo, a evolução e melhoria dos sistemas biométricos se tornaram uma realidade dentro de um mercado amplo e em constante crescimento, tornando-se o foco das atenções do mercado que busca, constantemente, novas tecnologias de segurança eficientes e com alto nível de qualidade.

Para tanto, podemos afirmar que, a escolha do tipo de tecnologia a ser implantada depende da área de aplicação e, principalmente do nível de segurança exigido e do valor de sua implementação.

Vale salientar que a utilização de sistemas capazes de agregar mais de um tipo de reconhecimento, torna estes mais seguros e confiáveis. Além disso é possível desenvolvê-los de modo a integrá-los a sistemas já em uso.

5. REFERÊNCIAS BIBLIOGRÁFICAS

1. Processamento de imagem para reconhecimento da íris. - Disponível em: http://student.dei.uc.pt/~jmaltez/SII/ acesso em 27/05/2006 às 18:14.
2. Tipos de Biometria. - Disponível em: http://pt.wikipedia.org/wiki/Biometria acesso em 27/05/2006 às 13:17.
3. Reconhecimento de Voz. - Disponível em: http://www.usr.inf.ufsm.br/~santos/ artigos.html acesso em 27/05/2006 às 15:24.
4. Biometria: Você é sua senha. – Disponível em http://www.serpro.gov.br/publi cacao /tematec/2002 acesso em 27/05/2006 às 15:40.
5. Processamento de imagem para reconhecimento da íris. - Disponível em: http://student.dei.uc.pt/~jmaltez/SII/ acesso em 27/05/2006 às 18:14.
6. Tipos de Biometria. - Disponível em: http://pt.wikipedia.org/wiki/Biometria acesso em 27/05/2006 às 13:17.
7. Reconhecimento de Voz. - Disponível em: http://www.usr.inf.ufsm.br/~santos/ artigos.html acesso em 27/05/2006 às 15:24.
8. Biometria: Você é sua senha. – Disponível em http://www.serpro.gov.br/publi cacao /tematec/2002 acesso em 27/05/2006 às 15:40.