INTRODUCAO HISTÓRICO

Introdução

A biometria é o ramo da ciência que estuda as medidas físicas dos seres vivos, daí o termo identificação biométrica para indicar as tecnologias que permitem a identificação das pessoas através dos traços físicos característicos e únicos de cada ser humano: os traços faciais, a íris e a impressão digital.

No século II a.C., os governantes chineses já usavam as impressões digitais para lacrar documentos importantes. Foi a primeira vez na história que impressões digitais identificaram positivamente uma pessoa. Desde então, a técnica de reconhecimento de impressões digitais evoluiu e passou a ser empregada em grande escala, tornando-se o principal método para comprovar, de forma inegável, a identidade de uma pessoa.

A tecnologia AFIS - Sistema Automatizado de Identificação de Impressões Digitais, é o modo mais rápido, preciso e fácil de se identificar uma pessoa através da impressão digital. O AFIS é utilizado com sucesso por agências de polícia e institutos de identificação civil em todo o mundo, em razão da sua capacidade única de identificar positivamente uma pessoa dentro de um universo de milhões de registros.

O Diferencial do AFIS 21 da NEC

O algoritmo de comparação do AFIS 21 representa a grande vantagem do software de comparação (matching) da NEC, que foi desenvolvido durante aproximadamente 30 anos de pesquisas no campo da biometria.

O algoritmo relacional do AFIS 21 utiliza o conceito de análise da relação entre as características únicas de cada impressão digital, realizando não só a localização dessas minúcias, mas também a contagem das linhas existentes entre elas, o que aumenta drasticamente a precisão na identificação da impressão digital.

Graças a isso, o AFIS 21 realiza pesquisas e comparações com taxa de precisão de 99,9% e com uma rapidez que possibilita encontrar uma impressão digital em apenas 2 minutos, num universo de até 90 milhões de registros.

O AFIS e a Solução de Crimes

A identificação de fragmentos de impressões digitais encontrados em cenas de crimes, conhecidos como impressões latentes, é o maior desafio à capacidade de precisão de um sistema AFIS. Na verdade, os sistemas da NEC solucionaram mais crimes a partir de impressões latentes do que todos os outros sistemas AFIS do mundo somados.

Em 1984, a NEC instalou o primeiro sistema AFIS nos Estados Unidos, na Polícia de São Francisco (California Department of Justice - DOJ) / Bureau of Criminal Identification and Information. Hoje, os sistemas fornecidos pela NEC possuem registros de impressões digitais de mais de 55 milhões de indivíduos, e são acessados por mais de 300 órgãos judiciais em todo o mundo.
Uma Defesa contra Fraudes.

A segurança das informações contidas nos documentos de identidade é fundamental para assegurar a sua validade e eliminar fraudes e falsificações. O exemplo mais recente de utilização do AFIS 21 com essa finalidade é a sua implantação, no ano

2000, no sistema nacional de identificação civil da África do Sul, onde o banco de dados atingirá brevemente o volume de 35 milhões de indivíduos.

Uso em Penitenciárias

A NEC instalou o primeiro sistema aplicado ao mercado de presídios na cadeia de Pike County, na Pensilvânia. A tecnologia de reconhecimento de impressões digitais é usada no sistema penal para identificar infratores reincidentes, controlar o movimento dos internos de uma penitenciária e verificar a identidade dos internos antes da soltura.

Usos Corporativos

Tendo em vista o sucesso do seu sistema de identificação junto aos órgãos judiciais e de segurança, a NEC apresentou, em 1995, o PID - Identificação Positiva, voltado para o mercado corporativo. Utilizando a mesma base tecnológica do AFIS, o PID atende a requisitos de diferentes mercados, como instituições ligadas à saúde, serviço civil, segurança de redes de computadores e mercado financeiro.

Tecnologia digital para identificação de pessoas
Identificação biométrica é solução para a segurança de informações

por Gabriella Ponte
5º período - Jornalismo

A biometria é o ramo da ciência que estuda as medidas físicas dos seres vivos. A tecnologia biométrica é usada para a identificação de pessoas através das características únicas de cada indivíduo, como a face, a íris e a impressão digital, fixando sua identificação perto da margem zero de erro. Cada ser tem traços físicos únicos difíceis de serem reproduzidos. Esta é uma antiga ambição de cientistas e bastante explorada na ficção científica e no cinema. Nos filmes “Minority Report” e “Gattaca”, esse tema é bastante abordado e mostra como essa tecnologia pode se tornar parte do dia a dia das pessoas. Mas até que ponto isso pode se tornar realidade?
A tecnologia AFIS (Sistema Automatizado de Identificação de Impressões Digitais), é o método mais preciso e rápido para identificação de impressões digitais. O AFIS é utilizado pela polícia e por institutos de identificação civil em todo o mundo. Este método ajuda na identificação de fragmentos de impressões digitais encontrados em cenas de crimes, por exemplo.
A Scotland Yard foi a pioneira em adotar a impressão digital para identificação de criminosos e em pouco tempo, as polícias de quase todo o mundo aderiram a essa maneira de identificação. Já hoje em dia, a identificação pela íris é uma realidade na Holanda. A polícia de estrangeiros de Roterdã começou os testes para identificar imigrantes. O que facilitará é que eles não precisarão mostrar seus passaportes, tendo somente que escanear a íris. A polícia acha que esse sistema vai economizar tempo para a identificação e espera diminuir as chances de fraudes.
Estes métodos de identificação estão ficando cada vez mais comuns e acredita-se que a tecnologia digital estará sendo utilizada brevemente em vários lugares, tais como aeroportos e outros. A segurança das informações contidas nos documentos de identidade assegura a sua validade, eliminando as fraudes e falsificações. O exemplo mais recente de utilização do AFIS com esse objetivo foi a sua implantação no sistema de identificação civil da África do Sul em 2000.
Além da impressão digital, reconhecimento de íris e retina e facial, existem outros métodos como o reconhecimento pela voz, palma da mão, assinatura e digitação. Embora todas sejam ótimos métodos de identificação, a mais segura é a pela íris, com uma margem de erro de 0,05%, porém seu custo ainda é alto.
No Brasil, ainda é uma imagem muito futurista a utilização da impressão digital como senha para o acesso à realização de transações bancárias pela Rede? Nem tanto. O primeiro caso será instalado no Banco Santos a partir de agosto, quando eles prometem lançar esse sistema aos clientes corporativos. E ainda tem mais: o Bradesco testa, em seu call center, a solução de

identificação da pessoa pelo reconhecimento da voz como mais uma medida de segurança.
As informações do governo também estão bem protegidas. Há um ano, no Supremo Tribunal Federal (STF), os ministros acessam seus computadores com a identificação das impressões digitais. “Lidamos com informações sensíveis que não podem ser divulgadas antes da hora”, argumenta Leonardo Alam da Costa, secretário de informática do STF. Hoje, nem todos os funcionários usam essa tecnologia. Mas, daqui a alguns meses, uma nova licitação implantará a identificação biométrica a todos os profissionais do órgão.
O profissional de segurança eletrônica e aluno de engenharia de telecomunicações Anderson Calleia, 30 anos, diz que, apesar da biometria ajudar na segurança de informações, “ela também pode ser usada por alguma organização criminosa que a utilize para esconder informações sigilosas, de forma que os policiais nunca saibam. E ainda, com ajuda de hackers, são capazes de burlar impressões digitais, o reconhecimento facial e até a de retina. Para invadir o banco de dados de uma agência bancária, por exemplo, basta o hacker cadastrar seus dados, colocando uma foto digitalmente. Depois, basta colocar seu rosto para ser escaneado e ele o reconhecerá. O software compara o rosto aos dados que tem no sistema. Sem contar que é posível fazer uma lente com as características do olho da pessoa. Embora esse caso seja bem mais difícil, não é impossível”.
Ele ainda lembra do reconhecimento mais fácil de ser fraudado, a assinatura: “Cada pessoa faz uma certa pressão no papel na hora de escrever e inclina o pulso de forma diferente. A partir daí, você sabe se a assinatura é falsa ou não. Mas, se você escanear uma assinatura e depois imprimir, não tem como comprovar que aquilo não é da pessoa, pois fica idêntico”.
Conhecida há mais de 20 anos, somente agora a tecnologia biométrica está se tornando economicamente viável. Nos próximos anos, deve se transformar em uma alternativa de segurança e de controle de pessoas para um grande contingente de empresas. De acordo com dados da International Biometric Group, o mercado de biometria deve crescer nos próximos quatro anos em 263%, passando de U$ 523 milhões em 2001 para U$ 1,9 bilhão em 2005. Eles irão obter a total segurança das informações. Por isso, o negócio vai ser ficar de olhos bem abertos para garantir uma coisa também única do ser humano, sua privacidade.

IDENTIFICAÇÃO BIOMÉTRICA: SISTEMAS BIOMÉTRICOS DE IDENTIFICAÇÃO PELA IMAGEM FACIAL

George Felipe de Lima Dantas

A biometria, expressão em uso desde o início do Século XX, trata do estudo e análise estatística de fenômenos quantitativos pertinentes a objetos de estudo das ciências biológicas. Mais recentemente, a expressão passou a ser também utilizada para designar as novas tecnologias da moderna ciência da informação, hoje utilizadas para a identificação humana a partir da análise de características individuais. Esse é o caso da identificação pela estrutura da íris ou retina, bem como da análise da imagem facial. Nesse contexto, os sistemas biométricos são processos automatizados de identificação, estando baseados nas características fisiológicas ou comportamentais dos seres humanos.

O sistema biométrico de identificação pela imagem facial baseia-se na característica única de cada face humana. De maneira geral, um sistema biométrico de identificação pela imagem facial funciona da seguinte maneira (três etapas):

Um sensor, ou câmera digital, registra a imagem facial. Para evitar que um rosto falso, ou mesmo um molde seja apresentado diante do sensor, alguns sistemas requerem que o identificado sorria, pisque, ou se mova, de tal maneira que fique patente que a face apresentada realmente pertence a um ser humano. O registro tomado é a "assinatura biométrica" do indivíduo;

Em seguida é gerado um algoritmo que representa a assinatura biométrica normalizada, ou padronizada, de tal forma que ela fique no mesmo padrão, tamanho, resolução e posição de outras assinaturas existentes na base de dados onde ela será arquivada. A normalização da assinatura biométrica individual produz uma "assinatura biométrica individual normalizada";

A assinatura normalizada é então comparada com um conjunto de várias outras assinaturas normalizadas existentes na base de dados do sistema, sendo estabelecido um "escore de similaridade" entre elas. O escore, por exemplo, de zero a cem, determina a probabilidade da identificação ser positiva.

Mais detalhadamente, o reconhecimento facial se inicia com o sensor processando ou, na linguagem usual, "escaneando" uma imagem facial individual. Um dos tipos de processamento consiste em buscar e definir picos e depressões existentes na face, registrando-os como pontos nodais. De acordo com essa técnica, são definidas e registradas as medidas das distâncias entre vários pontos nodais: olhos, nariz, cavidade orbital, ossos laterais da face e do queixo. As medidas são então transformadas em um algoritmo, que passa a ser a "matriz" da assinatura biométrica daquele indivíduo.

Um algoritmo, definido de modo geral, é uma seqüência finita de instruções a serem realizadas, cuja execução conduz à resolução de um problema. O algoritmo fornece a solução genérica de um problema e pode ser utilizado todas as vezes que o mesmo tipo de problema for apresentado. A exemplo, o algoritmo da divisão é genérico, não dependendo dos números que devam ser divididos.

O algoritmo, é representado pela "matriz", arranjo retangular de números semelhante a um formulário de palavras cruzadas que em lugar de letras contém números. A matriz é desenvolvida de acordo com um conjunto de cálculos matemáticos especialmente utilizado pelo sistema computacional. A matriz da imagem processada é então comparada com outras matrizes arquivadas na base de dados, sendo estabelecido o escore para cada comparação. As comparações "verificam" ou "reconhecem" a identidade individual.

A verificação de identidade é um processo simples de comparação, com a matriz da imagem apresentada sendo comparada com uma outra matriz daquele mesmo indivíduo. A matriz interna de comparação terá sido previamente arquivada na base de dados, em nome do mesmo indivíduo cuja identidade está sendo agora verificada. Já o reconhecimento é feito pela comparação da matriz do indivíduo a ser identificado com várias matrizes previamente arquivadas no sistema.

Em situações comuns, a verificação de identidade é feita quando a fotografia de uma cédula de identidade é comparada com a face do portador do documento. Já o reconhecimento é procedido, por exemplo, quando uma vítima identifica o criminoso entre vários indivíduos apresentados.

São muitas as áreas de aplicação da tecnologia biométrica de identificação facial, dentre elas: contra-terrorismo, na busca de reconhecer terroristas que estejam circulando em locais sensíveis como aeroportos; no controle parlamentar, quando da verificação da identidade dos legisladores por ocasião de votações; no controle da circulação, entrada e saída de funcionários e internos de estabelecimentos prisionais; na busca de crianças desaparecidas em meio a multidões; na segurança residencial, com o sistema emitindo alarmes quando se aproxima alguém cuja face não é reconhecida entre as de indivíduos autorizados; no comércio eletrônico (pela Internet), na verificação da identidade de usuários de cartões de crédito; durante pleitos eleitorais, na verificação da identidade de eleitores; bem como na atividade bancária, quando da verificação da identidade de correntistas fazendo transações bancárias.

O Escritório de Desenvolvimento de Tecnologias de Combate a Drogas, órgão do Departamento de Defesa dos Estados Unidos da América, juntamente com o Instituto Nacional de Justiça, pertencente ao Departamento de Justiça (equivalente ao Ministério da Justiça do Brasil), desde 2001 estão avaliando diferentes sistemas biométricos de identificação facial desenvolvidos por empresas e instituições de pesquisa norte-americanas. Os sistemas avaliados devem servir, basicamente, para eficaz e eficientemente verificar e reconhecer a identidade facial individual.

O presídio de El Hongo, localizado no estado mexicano da "Baja California", constitui um exemplo bastante atual da utilização de sistemas de reconhecimento facial no controle de estabelecimentos penais. Em 2002 a empresa comercial norte-americana ImageWar Systems (IW)

firmou um acordo comercial com a administração daquele estabelecimento, no sentido de dotá-lo de um Sistema de Captura de Criminosos ["Crime Capture System" (CCS)] que utiliza um software de Identificação Facial [Face ID software]. O CCS possibilitará que El Hongo cadastre e acesse automaticamente as imagens e registros criminais de seus internos, com o arquivo virtual ficando situado numa base central de dados. O arquivo inclui imagens da face, cicatrizes, tatuagens e outros sinais particulares de identificação de cada prisioneiro.

El Hongo, tido como um dos mais seguros e tecnologicamente avançados estabelecimentos penais da América Latina, irá utilizar o "Face ID" para identificar funcionários, internos e familiares visitantes, simplificando investigações e verificações de identidade. Num acordo bilateral pioneiro, o sistema irá permitir também que as autoridades prisionais mexicanas troquem informações com seus homólogos das organizações policiais norte-americanas da região da fronteira entre os dois países.

A tecnologia de reconhecimento pela imagem facial "aconteceu" em pouco mais de dez anos... Os trabalhos iniciais na área de reconhecimento facial datam do final dos anos 80, com os primeiros sistemas sendo disponibilizados comercialmente já no início da década seguinte. Ainda que muitos possam achar que o interesse no reconhecimento facial surgiu apenas após as tragédias de 11 de setembro de 2001, data dos ataques terroristas aos EUA, meses antes, em Tampa, Flórida, a identificação facial biométrica já era notícia nacional. Durante a partida final de "futebol americano" do campeonato de 2000, e sem que as pessoas que compareceram ao estádio de Tampa soubessem, seus rostos foram comparados com os registros de rostos de criminosos constantes da base de dados da polícia local. Grupos de ativistas de direitos civis contestaram a legalidade do procedimento, alegando sua intrusão na intimidade das pessoas presentes.

Apesar dos eventuais protestos, é muito boa a receptividade aos sistemas biométricos de identificação facial. Ele é bem menos inconveniente que outros existentes, caso do sistema de reconhecimento pela imagem da retina, e que demanda considerável esforço cooperativo da parte do indivíduo que está sendo identificado. Sistemas que identificam através da íris, retina, ou até mesmo de impressões papiloscópicas, via de regra são considerados invasivos à privacidade das pessoas. Os papiloscópicos, mais especificamente, guardam uma séria conotação negativa, na medida em que evocam a relação entre crime e identificação de criminosos. Já o reconhecimento biométrico pela expressão facial, pela analogia com a operação intuitiva e normal de identificação visual entre seres humanos, é muito melhor aceito.

É bastante oportuno o surgimento dos primeiros produtos da moderna tecnologia biométrica de identificação pela expressão facial, mormente no momento em que o governo federal brasileiro considera a constituição de uma base única nacional de identificação civil. No caso da implementação de um sistema tal, dele poderão ser derivadas diferentes aplicações, contemplando áreas de interesse tão diversas como a segurança pública, bancária e das instalações, bem como comércio eletrônico, justiça eleitoral e muitas outras mais. A lista de possíveis aplicações, no controle de acesso físico ou lógico, inclui aspectos tão revolucionários como a assinatura virtual de documentos, acesso a cofres eletrônicos, clubes, escolas e tantas outras possibilidades quantas possam ser imaginadas. Ao que parece, existe um enorme potencial por ser explorado nesse amplo universo tecnológico que é a identificação biométrica e que apenas começa a se descortinar para a humanidade.

HISTÓRICO BIOMETRIA

O QUE É BIOMETRIA ?

A palavra biometria vem do grego, Bios (vida) e Métron (medida) e é definida como a aplicação de teorias matemáticas e estatísticas. Os sistemas de controle de acesso biométricos começaram a ser estudados e desenvolvidos na década de 70, com o objetivo de segregar áreas dentro de departamentos e repartições governamentais secretas dos Estados Unidos, onde autenticavam uma característica corporal única de cada pessoa.

Biometria é mais bem definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um individuo.Elas incluem Impressões Digitais, Voz, Retina, Íris, Reconhecimento de Face, Imagem Térmica, analise de Assinatura, Palma da Mão e outras técnicas. Elas são de grande interesse em áreas onde é realmente importante verificar a real identidade de um individuo.Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entre tanto nós estamos vendo agora sua utilização e proposta de uso em uma grande e crescente área de situações em utilizações publicas no nosso dia a dia.
Elas são de grande interesse em áreas onde é realmente importante verificar a real identidade de um individuo.Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entre tanto nós estamos vendo agora sua utilização e proposta de uso em uma grande e crescente área de situações em utilizações publicas.

HISTÓRIA:

O primeiro método de identificação biométrica aceito oficialmente foi desenvolvido por Alphonse Bertillon no final do século XVIII. Também chamada de antropometria, o sistema se baseava numa combinação de medidas físicas tiradas de acordo com elaborados procedimentos. As métricas junto com cor de cabelo, de olhos e fotos de frente e de costas eram arquivadas. Bertillon criou 243 categorias.

A técnica foi adotada pela polícia de Paris em 1882 e rapidamente copiada por toda a França e Europa. Em 1887 os Estados Unidos aderiram ao sistema. O fracasso do método de Bertillon deveu-se a dificuldade no armazenamento e na consulta dos dados e ao complicado método para coletar as medidas.

Mas havia outra falha no sistema de Bertillon. Ao contrário do que se pensava, as categorias criadas não eram únicas. Aconteceram muitos erros que causaram o descrédito do sistema. Um dos mais conhecidos foi a prisão de um homem que alegou não nunca ter passado pela prisão. No entanto, ao verificar as informações, verificou-se que havia outro homem com as mesmas características do primeiro que estava detido em outro presídio.

O método de Bertillon foi substituído pelo sistema de impressões digitais, criado pelo oficial britânico William Herschel. Em missão na Índia, Herschel estava descontente com os comerciantes locais, que não cumpriam contratos. O oficial passou a pedir que colocassem além das assinaturas, a impressão das digitais nos documentos. A idéia, segundo o próprio, era "assustar os comerciantes, de modo que não pudessem repudiar sua assinatura".

Outros pesquisadores também começaram a estudar as impressões digitais na mesma época. Em 1870, o cirurgião Henry Faulds começou a vislumbrar nas digitais um caminho para comprovar identidades. Mas a classificação final ficou por conta do oficial Edward Richard Henry, que criou e adotou o sistema em 1897, na cidade indiana de Bengal. O sistema funcionou tão bem que foi adotado em toda Índia.

Pouco tempo depois, um comitê da Scotland Yard testou e aprovou o sistema, implantado na Inglaterra em 1901. O sistema antropométrico de Bertillon estava ultrapassado, apesar de algumas agências o terem usado até a década de 30.

Quais são as vantagens da Biometria ?

As vantagens da biometria são várias. Sendo uma tecnologia bastante fácil de utilizar, ela é bastante fiável e segura pois usa uma característica inerente ao ser humano, tal como a íris, ou a sua impressão digital, sendo estas as tecnologias biométricas mais usadas.

Esta tecnologia revela, ainda, uma relação preço/resultados mais eficaz que a maioria dos sistemas tradicionais de identificação e validação, sendo um sistema em que não implica a perda das credenciais (ao contrario dos cartões), ou o esquecimento das mesmas, no caso das *passwords*.
A biometria é a sua prova de identificação mais fiável e cómoda, a sua *password* sem memorização, sem palavras ou imagens, o seu cartão mais pessoal. **Biometria é a sua password eterna.**

Quais são as desvantagens da Biometria ?

Onde a biometria pode falhar?

Como qualquer mecanismo de segurança, os dispositivos biométricos estão sujeitos a falhas. São três os tipos de erros:

- Falsa rejeição do atributo físico de um usuário. O sistema não reconhece o padrão mesmo estando correto. É classificado na taxa de falsa rejeição.
- Falsa aceitação de um atributo físico. Neste caso, o sistema aceita a pessoa errada. O tipo de erro é classificado na taxa de falsa aceitação.
- Erro no registro de um atributo físico. São casos onde a variação de características físicas pode dificultar a operação do sistema. Alguém com

problemas de voz, por exemplo, pode atrapalhar o funcionamento do dispositivo, aumentando a taxa de erro.

Por isso, dependendo do nível de segurança desejado, especialistas recomendam o uso de pelo menos dois tipos de autenticação. Outro ponto fundamental para tirar melhor proveito das ferramentas é o treinamento/conscientização dos funcionários. Se eles estiverem desconfortáveis com a tecnologia, é provável que os erros apareçam numa taxa superior aos índices considerados normais.

Outra recomendação é de que os sistemas que armazenam dados biométricos devem ser protegidos com o uso de criptografia. No tráfego das informações pela rede é fundamental a implementação de PKI (Public Key Infrastructure) para evitar ataques do tipo "man-in-the-middle".

OUTRO PROBLEMAS:

- Alterações como machucados podem atrapalhar o reconhecimento
- Não é dos sistemas mais seguros. De acordo com Scalco, é mais comum acontecerem erros de reconhecimento
- Além de custo, há a questão da barreira cultural – afinal, não é todo mundo que quer ter uma luz entrando no olho
- Ruídos e até mesmo o estado emocional podem alterar a voz

FONTES:

http://www.biobox.com.br/bio.html
http://web01.proglobo.pt:8080/backo/html/biometria.htm

INTRODUCAO BIOMETRIA

Aceita pela primeira vez como método científico de identificação no final do século XVIII, a biometria, ou como era chamada na época, antropometria, usava as medidas de partes do corpo na catalogação de tipos humanos. Hoje, calcada em muitos anos de evolução tecnológica, é considerada uma das formas mais eficazes para comprovar a identidade de um indivíduo.

A biometria é uma das bases do tripé de autenticação do usuário, formado por informações que o indivíduo sabe (senhas), as que possui (cards ou chaves) e as contidas no próprio corpo, encaixando-se a biometria nesta última categoria. O dispositivos biométricos vão desde a verificação de digitais, geometria das mãos e leitura de retina e íris até o reconhecimento facial e de padrões de voz. O registro é feito com o auxílio de scanners, leitores óticos ou mesmo gravadores no caso dos padrões de voz.

De acordo com uma pesquisa do instituto Meridien Research, feita em janeiro, o uso de mecanismos biométricos tende aumentar nos próximos anos, devido ao barateamento da tecnologia, e devem se tornar cada vez mais integrados a diferentes tipos de hardware. Há pelo menos duas razões apontadas para o sucesso do método: é mais seguro e permite o acesso rápido e descomplicado à informação, sem a necessidade de senhas - muito mais vulneráveis à falhas de segurança.

O estudo revela ainda a divisão do mercado americano por tipo de dispositivo. A verificação de digitais fica com 39%; a identificação pelas mãos com 31% e a de rosto com 7,1%. O scaneamento dos olhos responde por 4,3% e de verificação de assinaturas tem 2,7% do mercado. Dados da organização americana International Biometric Industry Association (IBIA) mostram que no ano 2000 foram gastos 100 milhões de dólares em dispositivos biométricos. A expectativa é de que esse valor chegue a 600 milhões em 2003.

Ser mais segura faz parte da própria natureza da biometria, já que o usuário é identificado por características únicas, pessoais e intransferíveis, que não podem ser roubadas, compartilhadas ou esquecidas, como senhas e cards. Apesar de serem facilmente administradas, as senhas estão longe de manter alto grau de segurança.

Onde a biometria pode falhar?

Como qualquer mecanismo de segurança, os dispositivos biométricos estão sujeitos a falhas. São três os tipos de erros:

- Falsa rejeição do atributo físico de um usuário. O sistema não reconhece o padrão mesmo estando correto. É classificado na taxa de falsa rejeição.
- Falsa aceitação de um atributo físico. Neste caso, o sistema aceita a pessoa

errada. O tipo de erro é classificado na taxa de falsa aceitação.
- Erro no registro de um atributo físico. São casos onde a variação de características físicas pode dificultar a operação do sistema. Alguém com problemas de voz, por exemplo, pode atrapalhar o funcionamento do dispositivo, aumentando a taxa de erro.

Por isso, dependendo do nível de segurança desejado, especialistas recomendam o uso de pelo menos dois tipos de autenticação. Outro ponto fundamental para tirar melhor proveito das ferramentas é o treinamento/conscientização dos funcionários. Se eles estiverem desconfortáveis com a tecnologia, é provável que os erros apareçam numa taxa superior aos índices considerados normais.

Outra recomendação é de que os sistemas que armazenam dados biométricos devem ser protegidos com o uso de criptografia. No tráfego das informações pela rede é fundamental a implementação de PKI (Public Key Infrastructure) para evitar ataques do tipo "man-in-the-middle".

TIPOS DE DISPOSITIVOS:

- Verificação de digitais

No final do século XVIII, um policial britânico estabeleceu a primeira classificação de impressões digitais. Atualmente, a comparação de impressões é feita baseando-se em "minutiae" (características únicas da impressão). Em média, a imagem de uma digital tem entre 30 e 40 detalhes únicos. Segundo estudos do FBI, duas pessoas não apresentam mais do que 8 pontos coincidentes.

- Geometria das mãos

Nesse método são usadas medidas das mãos e dos dedos a partir de uma perspectiva tridimensional. Esse tipo de método oferece uma boa performance e é relativamente fácil de ser usado. Já é utilizado no controle de acesso e na verificação de identidades em muitos aeroportos, empresas e usinas nucleares.

- Padrão de voz

Esse tipo de reconhecimento envolve a gravação de um "modelo" para o padrão de voz que será usado na autenticação. O usuário deverá repetir determinada frase para que seu padrão de voz seja gravado.

- Leitura de retinas

Tecnologia em que os padrões dos vasos sangüíneos da retina são "lidos" por uma luz infravermelha com o auxílio de um leitor ótico. Os vasos absorvem mais rápido a luz que o tecido ao redor, formando uma imagem única que será analisada seguindo alguns pontos característicos. A quantidade de dados obtidos por esse processo é semelhante à da análise através de impressões digitais.

Esse método é bastante preciso, entretanto tem algumas desvantagens. A retina é mais suscetível à doenças como catarata, por exemplo, que alteram as características oculares; O método para obter os dados é bastante inconveniente - a luz deve ser direcionada diretamente para a córnea; A obtenção de uma imagem correta da retina vai depender da habilidade do operador e da capacidade da pessoa que está sendo scaneada em seguir os procedimentos.

A identificação exige que o usuário fixe o olhar em determinado ponto, o que não é muito prático, nem confortável. Por isso, esse método tem pouca aceitação entre os usuários, apesar de sua precisão.

- Leitura de íris

Considerado menos intrusivo, esse método baseia-se nas características da íris dos olhos. O usuário deve manter-se à distância de 14 polegadas de uma câmera ccd (usada para criar imagens em bit map). Esse dispositivo não requer contato entre o usuário e a câmera o que o torna mais confortável.

- Padrões de assinatura

Esse processo não se baseia apenas na comparação entre as assinaturas, mas sobretudo na dinâmica da assinatura do usuário, velocidade, direção, pressão e tracejado das letras. A restrição desse método é que se baseia no padrão de comportamento. Ninguém assina do mesmo modo sempre, o que permite maior margem de erros na autenticação.

- Reconhecimento facial

Dois padrões de tecnologia são aplicados. O escaneamento da imagem num padrão bidimensional, baseado na medida de ângulos e distâncias entre traços da fisionomia como olhos, nariz e boca. No entanto, as medidas podem variar de acordo com o movimento do usuário. Num primeiro momento, a aplicação deste método revelou-se pouco eficaz na identificação de nuances do rosto.

O desenvolvimento da captura de imagens do rosto com uso do padrão tridimensional, entretanto, supre essa deficiência significando a percepção de mais detalhes, como a estrutura óssea ao redor dos olhos e do nariz. Uma vez capturada, a representação em três dimensões pode ser construída a partir de um simples frame de gravação de vídeo. Grupos de defesa da privacidade questionam o uso desses dispositivos.

HISTÓRIA:

O primeiro método de identificação biométrica aceito oficialmente foi desenvolvido por Alphonse Bertillon no final do século XVIII. Também chamada de antropometria, o sistema se baseava numa combinação de medidas físicas tiradas de acordo com elaborados procedimentos. As métricas junto com cor de cabelo, de olhos e fotos de frente e de costas eram arquivadas. Bertillon criou 243 categorias.

A técnica foi adotada pela polícia de Paris em 1882 e rapidamente copiada por toda a França e Europa. Em 1887 os Estados Unidos aderiram ao sistema. O fracasso do método de Bertillon deveu-se a dificuldade no armazenamento e na consulta dos dados e ao complicado método para coletar as medidas.

Mas havia outra falha no sistema de Bertillon. Ao contrário do que se pensava, as categorias criadas não eram únicas. Aconteceram muitos erros que causaram o descrédito do sistema. Um dos mais conhecidos foi a prisão de um homem que alegou não nunca ter passado pela prisão. No entanto, ao verificar as informações, verificou-se que havia outro homem com as mesmas características do primeiro que estava detido em outro presídio.

O método de Bertillon foi substituído pelo sistema de impressões digitais, criado pelo oficial britânico William Herschel. Em missão na Índia, Herschel estava descontente com os comerciantes locais, que não cumpriam contratos. O oficial passou a pedir que colocassem além das assinaturas, a impressão das digitais nos documentos. A idéia, segundo o próprio, era "assustar os comerciantes, de modo que não pudessem repudiar sua assinatura".

Outros pesquisadores também começaram a estudar as impressões digitais na mesma época. Em 1870, o cirurgião Henry Faulds começou a vislumbrar nas digitais um caminho para comprovar identidades. Mas a classificação final ficou por conta do oficial Edward Richard Henry, que criou e adotou o sistema em 1897, na cidade indiana de Bengal. O sistema funcionou tão bem que foi adotado em toda Índia.

Pouco tempo depois, um comitê da Scotland Yard testou e aprovou o sistema, implantado na Inglaterra em 1901. O sistema antropométrico de Bertillon estava ultrapassado, apesar de algumas agências o terem usado até a década de 30.

Números da biometria

Tipo de sistema	Falsa rejeição	Falsa aceitação	Tempo*
Impressão digital	9,40%	0,00%	7 seg.
Retina	1,50%	1,50%	7 seg.
Palma da mão	0,00%	0,00025%	3 seg.
Geometria da mão	0,10%	0,10%	3 seg.
Voz	8,20%	0,40%	3 seg.

WWW.BIOMETRIA.COM.BR

Biometria

Biometria é mais bem definida como sendo as mensurações fisiológicas e/ou características de comportamento que podem ser utilizadas para verificação de identidade de um individuo.Elas incluem Impressões Digitais, Voz, Retina, Íris, Reconhecimento de Face, Imagem Térmica, analise de Assinatura, Palma da Mão e outras técnicas. Elas são de grande interesse em áreas onde é realmente importante verificar a real identidade de um individuo.Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entre tanto nós estamos vendo agora sua utilização e proposta de uso em uma grande e crescente área de situações em utilizações publicas no nosso dia a dia.
Elas são de grande interesse em áreas onde é realmente importante verificar a real identidade de um individuo.Inicialmente estas técnicas eram empregadas em aplicações especializadas de alta segurança, entre tanto nós estamos vendo agora sua utilização e proposta de uso em uma grande e crescente área de situações em utilizações publicas.

Origem da biometria

Como isto tudo começou ? Isto nos leva a pensar sobre biometria como uma tecnologia futurista SCI-FI que deveríamos estar utilizando junto com carros com energia solar, pílulas de alimentação e outros equipamentos futuristas em algum lugar do futuro próximo. Esta imagem popular sugere que estes produtos são do final do século 20 na era dos computadores.Na verdade, os princípios básicos da verificação biométrica foram compreendidos e exercitados um pouco antes. Centenas de anos antes para ser preciso, nossos amigos no Vale do Nilo empregavam verificação biometria em um grande numero de situações de negócios diariamente.

Existem diversas referencias sobre indivíduos sendo identificados por características físicas e parâmetros como cicatrizes, critérios de mensuração física ou a combinação de características mais complexas como cor dos olhos, altura e assim por diante. Estes seriam freqüentemente utilizadas no setor de agricultura onde grãos e provisões seriam estocados em uma central de reposições e aguardavam para movimentações futuras após identificação

dos proprietários. Com certeza eles não possuíam leitores biométricos e redes de computadores (até a onde sabemos), e certamente eles não estavam lidando com um numero de indivíduos que temos que lidar hoje, mas os princípios básicos são similares. Mais tarde, no século dezenove houve um pico de interesse em pesquisas criminalísticas na tentativa de relacionar características físicas com tendências criminais. Isto resultou em uma variedade de dispositivos para mensuração sendo produzidos e muitas informações sendo coletadas.

Os resultados não foram conclusivos mas a idéia de mensurar características físicas individuais prosseguiu e os desenvolvimentos paralelos com impressões digitais tornarem-se métodos internacionais utilizados por forças policiais para identificação e verificação. Completa e única; porem, impressões digitais são freqüentemente debatidas, e os critérios que diferentes paises utilizam para verificar uma impressão digital variam ao redor do mundo com maiores ou menores números de pontos de minúcias requeridas para serem identificadas. Adicione a isto a questão de interpretação pessoal a qual pode ser pertinente em casos duvidosos. Nunca menos, esta é a melhor metodologia oferecida e ainda a numero um para as forças policiais, embora o processo de identificação seja muito automatizado em nossos dias.

Com este background, não foi surpresa que por muitos anos a fascinação tenha ocupado a mente de indivíduos e de organizações com a possibilidade de utilização de eletrônicos e a força de microprocessadores para automatizar a verificação de identidades para os setores militares e comerciais.Vários projetos foram iniciados para verificar o potencial da biometria e foi produzido um leitor grande e desajeitado leitor da geometria da mão. Não era bonito , mas trabalhava e motivados seu design e concepção mais a frente foi refinado. Mais tarde , uma pequena empresa especializada criou uma unidade muito menor, e um leitor mais aprimorado da geometria da mão tornou-se o principio da industria biométrica atual.

Equipamentos biométricos que trabalham com Impressões Digitais são um grande aprimoramento e são utilizados em numerosos projetos biométricos por todo o mundo.Em paralelo, outros métodos biométricos estão sendo desenvolvidos, melhorados e refinados até o ponto em que se tornem realidades comerciais. Nestes anos recentes, nos temos visto muito interesse nas técnicas de Scaneamento de Íris e reconhecimento facial., tecnologias potencias de reconhecimento sem contato, entre tanto existe muita polemica a este respeito. A ultima década tem sido da maturação da industria biométrica e industrias especializada brigando de mãos cheias por vendas por um mercado global equilibrado obtendo um respeitável numero de equipamento e um significante crescimento com uma larga escala de aplicações começam a se desdobrar.

AUTENTICAÇÃO BIOMÉTRICA

O mecanismo de autenticação por biometria tem dois modos: registro e verificação. Para o uso inicial da biometria, cada usuário deve ser registrado pelo administrador do sistema. Este, verifica se cada indivíduo registrado é um usuário autorizado. O processo de registro consiste no armazenamento de uma característica biológica do indivíduo (física ou comportamental) para ser usada, posteriormente, na verificação da identidade do usuário.

Uma vez que o usuário está registrado, os dispositivos biométricos são usados na verificação da identidade do usuário. Quando o usuário necessitar ser autenticado, sua característica física é capturada pelo sensor. A informação analógica do sensor é então convertida para sua representação digital. A seguir, esta representação digital é comparada com o modelo biométrico armazenado. A representação digital usada na verificação é chamada de amostra (live scan). A amostra, tipicamente, não confere exatamente com o modelo armazenado. Como geralmente há alguma variação na medida, estes sistemas não podem exigir uma comparação exata entre o modelo original armazenado e a amostra corrente. Ao invés disso, a amostra corrente é considerada válida se estiver dentro de um certo intervalo estatístico de valores.

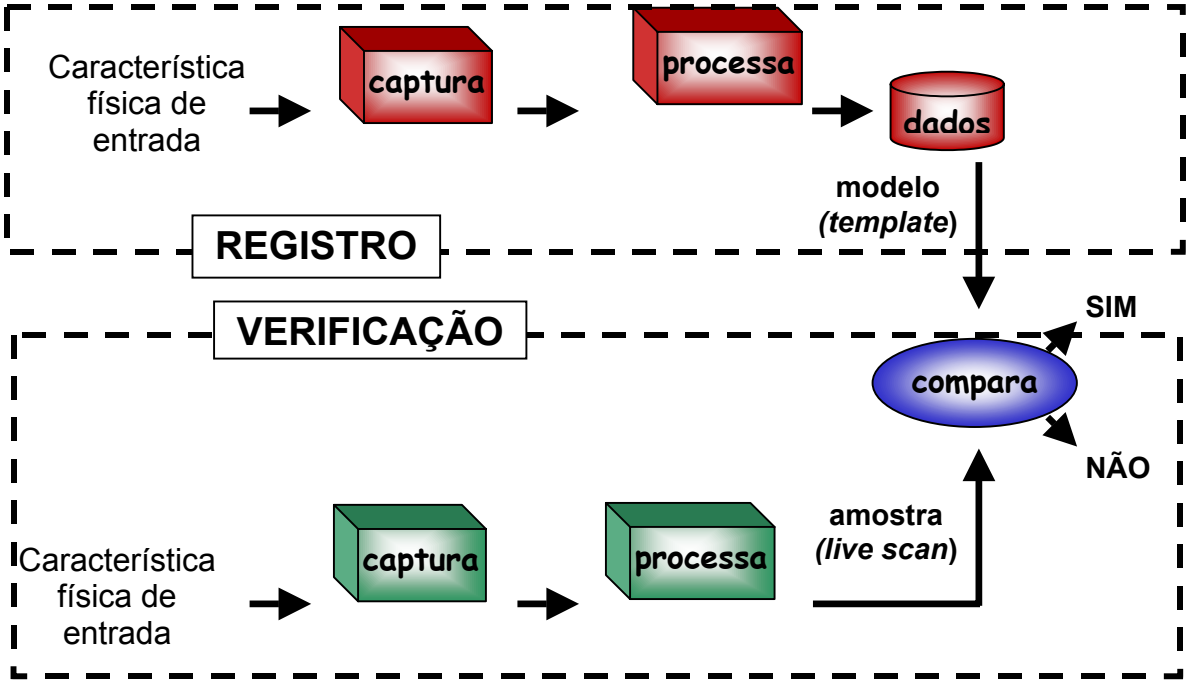
A autenticação por biometria pode ser realiza através da identificação ou da verificação de usuários. Muitos dispositivos usam a verificação, mas alguns usam a identificação.

A identificação biométrica é um processo um-para-muitos, onde uma amostra é submetida ao sistema, que a compara com todos os modelos de base de dados, a fim de verificar se esta coincide com qualquer um dos modelos e, em caso positivo, determina a identidade do usuário a quem aquele modelo pertence.

A verificação biométrica é um processo um-para-um, onde o sistema verifica a identidade de um usuário comparando a amostra com um modelo específico. Através de uma identificação fornecida, o sistema localiza o modelo desejado e o compara com a amostra apresentada. Se houver coincidência entre a amostra e o modelo armazenado, o sistema confirma que o usuário realmente possui a identidade afirmada. Por exemplo, um usuário irá digitar o seu nome e então se adquire uma

amostra para a verificação. O algoritmo de comparação usará apenas o modelo armazenado àquele nome. Verificações biométricas são, tipicamente, mais rápidas do que a identificação porque elas não precisam comparar a amostra com todo o banco de dados de modelos.

Modelo Autenticação Biométrica



MÉTODOS DE AUTENTICAÇÃO BIOMÉTRICOS

Como os sistemas biométricos se baseiam em características intrínsecas do ser humano, podem ser empregados como métodos de autenticação rápida e com alto nível de precisão. Têm, como uma de suas principais vantagens, o fato de ser intransferível, não poder ser perdido e nem roubado.

Na escolha de um sistema de autenticação biométrico, o desempenho deve ser levado em conta. Este pode ser categorizado por duas medidas: a taxa de falsa aceitação (FAR - False Acceptance Rate) e a taxa de falsa rejeição (FRR - False Rejection Rate). A FAR representa a percentagem de usuários não-autorizados que são incorretamente identificados como usuários válidos e a FRR, representa a percentagem de usuários autorizados que são incorretamente rejeitados.

IMPRESSÃO DIGITAL

Na verificação de uma impressão, muitos sistemas analisam a posição de detalhes chamados de minutiae, tais como terminações e bifurcações dos sulcos. Sistemas modernos também verificam outras características para identificação única, tais como arcos e voltas que aparecem no dedo.

Minutiae – posições de detalhes

(crossover, core, bifurcation, ridge ending, island, delta,

Nos dispositivos de impressão digital, o leitor deve minimizar a rotação da imagem. Ele deve compensar uma ligeira variação na imagem armazenada. Existem, também, problemas quando o usuário tem pequenos ferimentos no dedo, sujeira ou ressecamento da pele. Uma freqüente limpeza pode reduzir a percentagem de falsas rejeições.

Existem três tipos de leitores de digitais:
Ópticos: O dedo é colocado sobre uma plataforma de vidro e uma imagem do dedo é capturada. Estes dispositivos tornaram-se pequenos e baratos;

Ultra-som: O dedo é colocado sobre uma plataforma de vidro e uma varredura de ultra-som é efetuada;
Baseados em chip: O usuário coloca seu dedo direto em um chip de silício.

Sistemas de identificação de digitais utilizam somente os leitores ópticos. Sistemas de verificação (executam verificação um-pra-um) utilizam todos os três.

Na Figura mostrada abaixo, veremos alguns dispositivos de leitura usados para a captura das impressões digitais:

Dispositivos de Leitura: (a) Teclado Key Tronic, (b) BioMouse Plus e (c) Identifix TouchSAfe Personal

EXEMPLO (APLICAÇÃO PRÁTICAS)

O Congresso Nacional brasileiro também implantou um sistema desse tipo para registrar a freqüência e a identidade dos deputados nas votações.


Teclado com sensor: segurança no B2B

Chip biométrico: tamanho cada vez mais reduzido


Chip no mouse: em 2001

Impressão Digital é senha para mouse.

Acabar com a necessidade de tantas senhas para acessar o micro. Esse é o Objetivo do mouse com tecnologia SmartThumb, que identifica o usuário com a leitura de sua impressão digital. Um microprocessador converte em fórmula matemática a imagem da impressão digital, captada por um scanner. A fórmula calculada só existe um individuo, o que possibilita a identificação correta do usuário. Caso o mouse venha a ter defeito, o sistema aceita provisoriamente a entrada por senha, pelo método tradicional. O mouse, fabricado para canhoto e destro seu valor é de aproximadamente US$ 150 a US$ 170.

As perspectivas mais promissoras da biometria atualmente estão nas aplicações de e-business. Nesse ramo, os scanners para captura da impressão digital e os softwares

de reconhecimento de voz já saíram na frente. Alguns modelos de chips para captura de imagens são independentes e podem ser anexados ao monitor ou ao gabinete dos PCs. Outros já vêm embutidos no mouse e nos teclados. A Microsoft e a Compaq estão investindo para garantir espaço nesse mercado. Alguns chip-cards também já são fabricados no exterior, conjugando o smart card e a biometria.

Biometria no carro: o dedo é a chave.

Pegar o carro escondido será difícil e perder a chave não será problema.
O motorista deverá colocar o dedo no espaço do sensor computadorizado para que a digital seja lida. Se as características forem reconhecidas, as portas são automaticamente destravadas. Com o reconhecimento um sistema pode memorizar posições do banco, volume do som, altura e profundidade do volante, musicas selecionadas e temperatura do ar-condicionado. O Equipamento é uma criação da empresa alemã Delsy Eletronic Components AG e só será disponibilizado a partir de 2004 para equipar os automóveis de luxo, como Mercedes-Bens Classe S e BMW Série.

RECONHECIMENTO DE VOZ

Para analisar o som produzido pelas cordas vocais, a biometria considera a freqüência e o tamanho das ondas sonoras, que por si só já garantem uma probabilidade de 80% de acerto. O restante é verificado com a análise de timbre e entonação. Nos sistemas mais sofisticados, é pedido ao usuário que grave algumas respostas a perguntas específicas, como por exemplo quantas cores formam o arco-íris, ou mesmo questões de cunho pessoal. Para garantir uma identificação segura, o software faz uma dessas perguntas de forma aleatória e consegue analisar inclusive o tempo que o usuário gasta para respondê-la.
A tecnologia de reconhecimento de voz é fácil de usar e não requer grandes esforços na educação do usuário. Entretanto, deve-se cuidar para garantir que o usuário fale em um tempo apropriado e em voz clara.

Uma vez que as pessoas formam seus padrões de fala através da combinação de fatores físicos e comportamentais, a imitação é impossível. Entretanto, existem problemas com as condições do ambiente onde se encontram os sensores, uma vez que é difícil filtrar o ruído de fundo. Outros problemas incluem a variação da voz devido às condições físicas do usuário, como gripes e resfriados, estados emocionais, como o estresse, e duplicação através de um gravador. A imitação, porém, não é um problema como se poderia pensar, porque os aspectos da voz medida pelos sistemas não são os mesmos que os seres humanos costumam perceber.

EXEMPLO (APLICAÇÃO PRÁTICAS)

As máquinas dizem alô
Na CTBC Telecom, o reconhecimento de fala já substitui o atendimento pessoal

---

"Bom-dia! Eu sou sua assistente CTBC Telecom."

É com essa frase que o computador da mineira CTBC Telecom atende aos usuários que procuram pelo serviço de informações. O sistema de reconhecimento de fala é responsável hoje pelo atendimento de mais de 30% das 900 000 chamadas mensais que o call center recebe de clientes da operadora em quatro Estados do país: Minas Gerais, São Paulo, Goiás e Mato Grosso. "O programa já tem condições de atender a 100% da procura por informações do nosso serviço Auxiliar Lista, mas está automatizando o atendimento gradativamente para que os clientes se acostumem com esse modelo".
A operadora começou a trabalhar no desenvolvimento do reconhecimento de fala em janeiro de 2000. Ela optou pela solução da americana Nuance, que tem em sua carteira de clientes empresas como Bradesco, Telemar, Gradiente, Telefônica e a agenda on-line Elefante.
Programação do despertador, hora certa, horóscopo, interurbanos, reclamações e outros cinco serviços que tinham números próprios foram integrados ao Auxiliar Lista. "Agora, o cliente liga para apenas um número para obter qualquer informação e fornece seus dados apenas uma vez". A praticidade para o usuário significou também economia para a telefônica. Em seis meses de operação unificada com reconhecimento de fala, a empresa conseguiu redirecionar 30% do quadro de atendentes, o que corresponde a 48 pessoas, para a prestação de outros tipos de serviço no call center.
Até o fim do ano devem estrear nesse endereço as operações de v-commerce, o comércio eletrônico via voz.

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.

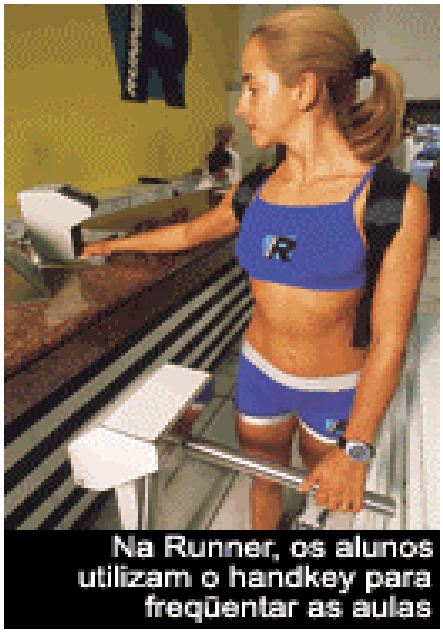
Um dos problemas de sistemas que utilizam a geometria da mão é causado pela rotação da mão quando colocada no leitor. Isto se resolve usando pinos de posicionamento dos dedos. O sistema também deve levar em conta os diferentes tamanhos das mãos em diferentes usuários, e seu desempenho não deve ser prejudicado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

Leitor de geometria da mão

EXEMPLO (APLICAÇÃO PRÁTICAS)

Entre as empresas que já utilizam essa tecnologia em grande escala, estão Academia Runner, Banco do Brasil, Telemig Celular e o Clube Pinheiros, em São Paulo.

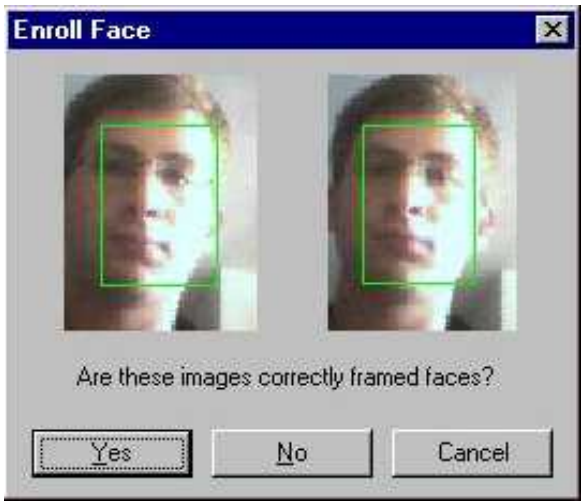
Nas últimas Olimpíadas, em Sydney, a geometria das mãos foi um dos critérios de segurança usado para identificar os atletas que participaram das provas.



Na Runner, os alunos utilizam o handkey para freqüentar as aulas

RECONHECIMENTO DA 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, pois registra vários pontos delimitadores do rosto e define as proporções entre olhos, nariz, queixo, maçãs do rosto e orelhas, que são únicos a cada pessoa. E, ao contrário do que muitos imaginam, os programas de reconhecimento podem identificar corretamente uma pessoa mesmo que ela tenha mudado o corte do cabelo, ou acrescente acessórios como chapéu, óculos, barba ou bigode.

EXEMPLO (APLICAÇÃO PRÁTICAS)

Em algumas cidades pequenas do interior da Inglaterra, como Newham (subúrbio de Londres), a geometria do rosto é utilizada para ajudar a encontrar suspeitos no meio de uma multidão. É possível armazenar as características de um criminoso num banco de dados e deixar que o computador o procure com câmeras instaladas em pontos estratégicos da cidade.

LEITURA DE ÍRIS/RETINA

De todas as tecnologias biométricas, as mais seguras utilizam o olho humano como parâmetro. A mais precisa é a análise da retina. Por ser formada por uma milimétrica rede de vasos sangüíneos, a retina constrói um padrão único para cada ser humano que não pode ser alterado nem por doenças graves, como o glaucoma. A tecnologia de captura dessa imagem, entretanto, é muito cara e difícil de ser realizada, pois é necessário que o usuário olhe fixamente para um ponto infravermelho até que a câmera focalize os padrões. A operação demora menos de 5 segundo, mas não é nada confortável.

Analisador de retina

Íris é o anel colorido que circunda a pupila do olho. Cada íris possui uma estrutura única que forma um padrão complexo e pode ser usada para identificar um indivíduo.
O sistema funciona a partir de um sensor luminoso, que trabalha como um scanner, ou por uma câmera embutida num equipamento médio. Ao colocar o olho próximo desse aparelho, o usuário tem seu globo ocular "dividido" pelo computador, que separa a íris em quadrantes e a converte numa espécie de código de barras. O tamanho da pupila também é medido, pois qualquer dilatação anormal pode distorcer a leitura da íris. A barra de código, então, é comparada à imagem já codificada no banco de dados.
O sistema acomoda usuários de lentes de contato sem dificuldades, embora o sensor deva ser montado ou ajustado de modo a ser satisfatório para usuários de diferentes alturas, incluindo aqueles em cadeiras de roda.


Aparelho de reconhecimento de íris: câmera embutida

EXEMPLO (APLICAÇÕES PRÁTICAS)

A LG possui uma solução que identifica o indivíduo por meio da retina, a IrisAccess. A aplicação é composta basicamente de dois aparelhos. Um terminal de registro fica ligado a um servidor e recebe as informações de uma unidade remota. Para ser identificada, a pessoa se posiciona a uma distância entre 7,5 e 30 centímetros dessa unidade remota, que fotografa sua íris. A imagem fica então armazenada no aparelho e as retículas do olho são decodificadas. Esses dados são enviados ao servidor, que realiza a verificação de identidade. Todo o processo demora cerca de 1 segundo para acontecer.