BIOMETRIA: A TECNOLOGIA NOS VIGIA OU PROTEGE?

Rosangela Silqueira Hickson[1]

RESUMO

Usado em tramas de Sci-Fi, o uso da Biometria aparece nos filmes há algum tempo. Em 1968, em “2001, uma odisseia no espaço” já encontramos o reconhecimento de voz. E em filme de 007 não pode faltar a Biometria. Entre elas reconhecimento de impressão digital, facial, de íris. Mas o que é mesmo Biometria? Ela nos vigia ou nos protege?

Palavra-chave: Biometria; DNA; reconhecimento facial.

1 INTRODUÇÃO

O alto custo das tecnologias, o baixo êxito dos softwares e o risco de violação da privacidade, reduziram o crescimento da biometria, a tecnologia que utiliza as características biológicas únicas para identificar as pessoas para fins de segurança. Mas as ameaças do mundo atual fizeram com que esta tecnologia tivesse um crescimento de forma que em alguns anos será normal o uso de sistemas de reconhecimento digital, fácil ou da íris.

Imagine que você precise entrar em um local secreto, porém tem que passar por um sistema de segurança, que exige mais do que uma chave ou uma senha: exige a íris, a voz e o formato da mão para conseguir entrar.

Esse tipo de cenário pode ser encontrado durante um dia normal no trabalho. Aeroportos, hospitais, hotéis, mercearias e até os parques temáticos da Disney usam cada vez mais a biometria para ter maior segurança. A

[1] Doutora em Bioinformática, Mestre em Ciência da Computação, Engenheira Mecânica, Coordenadora de Projetos a distância da Faculdade Infórium de Tecnologia, Coordenadora de cursos de pós-graduação, professora e relatora do Comitê de Ética em Pesquisa do Centro Universitário Metodista Izabela Hendrix, Coordenadora de curso de Pós-graduação a distância no SENAC-MG, Avaliadora Institucional e de curso do INEP/MEC.

biometria é a tecnologia que identifica a pessoa baseando-se em suas características físicas ou comportamentais.

FUNCIONAMENTO

As pessoas tomam precauções básicas todos os dias: usam chaves para entrar em casa e fazem login em seu computador com um nome de usuário e uma senha. Provavelmente já tiveram a experiência de perder chaves ou esquecer senhas. Para evitar isso, elas costumam ter cópias das chaves guardadas e as senhas anotadas em algum lugar. A desvantagem é que uma pessoa estranha pode achá-las e usá-las.

Em vez de usar chaves ou senhas, a biometria usa **quem você é** para identificá-lo. A biometria pode usar **características físicas**, como o rosto, impressões digitais, íris ou veias, ou **características comportamentais**, como a voz, caligrafia e ritmo de digitação. Diferentemente das chaves e senhas, as características pessoais não podem ser perdidas ou esquecidas. Elas também são muito mais difíceis de serem copiadas e, por essa razão, são consideras mais seguras do que chaves e senhas.

Sistemas biométricos podem parecer complicados, mas todos usam as mesmas etapas.

- **Registro**: na primeira vez que se usa um sistema biométrico, ele registra informações básicas como o nome ou um número de identificação. Depois, captura uma imagem ou registro de uma característica específica do indivíduo.
- **Armazenamento**: diferentemente do que pode ser visto nos filmes, a maioria dos sistemas não armazena a imagem ou registro completo. Em vez disso, analisam determinada característica e a traduzem num código ou gráfico. Alguns sistemas também registram esses dados em um smart card que o indivíduo carrega com ele.
- **Comparação**: a próxima vez que o sistema for usado, ele irá comparar a característica apresentada com a informação no arquivo, para então aceitar ou rejeitar a pessoa que está se identificando.

Os sistemas também usam os mesmos três componentes:

- um **sensor,** que detecta a característica que está sendo usada para a identificação;
- um **computador,** que lê e armazena as informações;
- um **software,** que analisa as características e as traduz para um gráfico ou código, fazendo as comparações.

Os sistemas biométricos de segurança, como o scanner de impressão digital disponível no IBM ThinkPad T43, estão se tornando mais comuns no uso doméstico.

A seguir, veremos como a biometria pode oferecer segurança usando outras características, começando pela escrita.

SCANNER DE IMPRESSÃO DIGITAL

Escrita

À primeira vista, usar a escrita para identificar pessoas pode não parecer uma boa ideia, pois qualquer um pode aprender a copiar caligrafias em pouco tempo. Seria fácil conseguir uma cópia da assinatura de alguém e falsificá-la.

Mas os sistemas biométricos não prestam atenção somente no formato que se dá a cada letra. Eles analisam o ato de escrever, a pressão, a velocidade e o ritmo com os quais se escreve. Eles também registram a sequência que se usa para formar as letras, como se adicionam pontos e traços ao escrever ou depois de escrever cada palavra.

Sistema de verificação de assinatura

Ao contrário da forma das letras, essas características são mais difíceis de falsificar. Mesmo que alguém consiga uma cópia de sua assinatura e a reproduza, o sistema provavelmente não aceitará a falsificação.

Sensores do sistema de reconhecimento de caligrafia podem incluir uma superfície sensível ao toque ou uma caneta que contenha sensores que detectam ângulo, pressão e direção. O software traduz a caligrafia para um gráfico e reconhece as pequenas mudanças na caligrafia de uma pessoa no dia-a-dia e durante determinado tempo.

Determinando a precisão

Todos os sistemas biométricos usam características humanas que são, de alguma forma, únicas. Determinar qual é o melhor sistema depende do nível de segurança necessário, do público que usará o sistema e de sua precisão. A maioria dos fabricantes usa medidas como estas para descrever a precisão:

- **taxa de falsa aceitação**: quantos impostores o sistema aceita
- **taxa de falsa rejeição**: quantos usuários autorizados o sistema rejeita
- **taxa de falha no registro**: quantos registros de característica são de qualidade insuficiente para serem usados pelo sistema
- **taxa de falha na obtenção**: quantas vezes um usuário precisa apresentar a característica antes de o sistema aceitar ou rejeitá-lo corretamente

Geometria de mãos e dedos

Scanner de dedos

As mãos e os dedos das pessoas são características únicas, mas não tão únicos quanto as impressões digitais ou a íris. É por isso que empresas e escolas, em vez de aparelhos de alta segurança, usam leitores da geometria das mãos e dos dedos para **autenticar** os usuários e não para **identificá-los**. Os parques temáticos da Disney, por exemplo, usam leitores da geometria dos dedos para garantir a entrada de pessoas que tenham o bilhete em todos os lugares do parque. Algumas empresas usam os leitores de geometria das mãos em vez de cartões de ponto.

Os sistemas que medem a geometria das mãos e dos dedos usam uma câmera digital e luz. Para usar um, você simplesmente coloca sua mão em uma superfície plana, alinhando seus dedos com as várias linguetas para ter uma leitura precisa. Uma câmera tira uma ou mais fotos de sua mão e da sombra que ela produz. O sistema usa essas informações para determinar comprimento, largura, grossura e curvatura da mão e dos dedos e traduz essas informações para um padrão numérico.

Os sistemas de geometria das mãos e dos dedos têm prós e contras. Uma vez que as mãos são menos específicas do que as impressões digitais ou a íris, algumas pessoas sentem que esses sistemas invadem menos sua privacidade. De qualquer maneira, as mãos das pessoas mudam com o tempo, em razão de machucados, mudança de peso ou artrite. Alguns sistemas atualizam os dados para refletir as mudanças do dia-a-dia.

MAIS SISTEMAS BIOMÉTRICOS

Timbres de voz

A voz é uma característica única em razão do formato das cavidades vocais e da forma que se movimenta a boca ao falar. Para se registrar em um sistema de timbre de voz, você diz exatamente as palavras ou frases solicitadas ou dá amostras de seu discurso, para que o computador possa identificá-lo, não importando as palavras que foram ditas.

Quando as pessoas pensam no timbre de voz, normalmente pensam na onda que veriam em um osciloscópio. Mas os dados usados no timbre de voz são um **espectrograma** do som e não o formato de uma onda. Um espectrograma é basicamente um gráfico que exibe a frequência do som no eixo vertical e o tempo no eixo horizontal. Diferentes sons de falas criam diferentes formatos dentro do gráfico. Os espectrogramas também usam cores ou tons de cinza para representar as qualidades acústicas do som.

Sistemas de reconhecimento de voz usam espectrogramas para representar vozes humanas

Algumas empresas usam o reconhecimento do timbre de voz para que as pessoas tenham acesso a informações ou possam passar informações sem estar fisicamente presentes. Em vez de aproximar-se de um scanner de íris ou de um leitor de geometria das mãos, alguém pode fazer uma autorização dando um simples telefonema. Infelizmente, as pessoas conseguem enganar alguns sistemas, principalmente os que funcionam por telefone, com uma simples gravação de voz de uma pessoa autorizada. Esse é um dos motivos pelos quais os sistemas usam várias senhas de voz escolhidas aleatoriamente ou usam timbres de voz gerais em vez de timbres de palavras específicas.

Outros usam tecnologia que detecta os artefatos criados em gravações e playbacks.

Outros tipos de sistema são mais difíceis de enganar. Veremos alguns deles a seguir.

Escaneamento da íris

O scanner de íris pode parecer futurístico, mas o centro do sistema é uma simples câmera digital CCD. O escaneamento usa tanto a luz visível quanto a infra-vermelha para ter uma foto clara e de alto contraste da íris. Próximo à luz infravermelha, a pupila de uma pessoa fica bem escura, facilitando a separação, pelo computador, da pupila e da íris.

Anatomia dos olhos

Quando você olha para um scanner de íris, ou a câmera focaliza automaticamente ou você usa um espelho ou um feedback sonoro do sistema para ter certeza de que seu posicionamento está correto. Normalmente, seu olho fica de 7,5 cm a 25 cm da câmera. Quando ela tira uma foto, o computador localiza:

- o centro da pupila
- a beirada da pupila
- a beirada da íris
- as pálpebras e os cílios

Em seguida, o scanner analisa os modelos da íris e os traduz para um código.

Um scanner de íris

Os scanners de íris estão se tornando mais comuns nos aplicativos de alta segurança, porque os olhos da pessoa são únicos (a possibilidade de trocar o código de uma íris pelo de outra é de 1 em 10 elevado à 78ª potência). Os olhos também permitem mais de 200 pontos de referência para comparação, diferente dos 60 ou 70 pontos das impressões digitais.

A íris é uma estrutura visível, mas protegida, e não se modifica com o tempo, tornando-se ideal para a identificação biométrica. Na maioria das vezes, os olhos das pessoas permanecem ilesos após uma cirurgia ocular e mesmo as pessoas cegas podem usar scanner de íris, desde que seus olhos tenham íris. Os óculos e as lentes de contato normalmente não interferem nem causam leituras inexatas.

Escaneamento da retina

Algumas pessoas confundem o escaneamento de íris com o **escaneamento da retina**. O escaneamento da retina é uma tecnologia mais antiga, que precisava de uma luz brilhante iluminando a retina da pessoa para que o sensor pudesse tirar uma foto da estrutura dos vasos sanguíneos da parte escura dos olhos. Algumas pessoas achavam o sistema desconfortável e invasivo. Além disso, as retinas mudam conforme a idade, o que pode levar a leituras inexatas.

Geometria das veias

Assim como a íris e as impressões digitais, as veias de uma pessoa também são características exclusivas. Gêmeos não têm veias idênticas e as veias de uma pessoa são bem diferentes nos lados esquerdo e direito. Muitas não são visíveis através da pele, tornando-se extremamente difíceis de serem falsificadas ou manipuladas. Suas formas também se modificam muito pouco com a idade.

Scanners de veia usam luz infravermelha próxima para mostrar as características das veias

Para usar um sistema de reconhecimento de veias, você simplesmente coloca seu dedo, pulso, palma ou as costas da mão no scanner ou bem próxima a ele. Uma câmera tira uma foto digital usando luz infravermelha. A hemoglobina presente no sangue absorve a luz, de forma que as veias aparecem escuras na foto. Assim como com todos os outros tipos biométricos, o software cria um padrão de referência baseado no formato e na localização da estrutura das veias.

Os scanners que analisam a geometria das veias são totalmente diferentes dos usados nos testes hospitalares. Os scanners com finalidades

médicas normalmente usam partículas radioativas. Já os scanners da segurança biométrica apenas usam uma luz parecida com a luz que vem de um controle remoto.

Como funcionam os leitores de impressões digitais

Por décadas, os leitores de impressões digitais computadorizados apareciam somente nos filmes de espionagem. Nos últimos anos, no entanto, eles começaram a surgir por toda parte: em delegacias, distritos policiais, edifícios com elevado grau de segurança e até mesmo em teclados de computador. Hoje, pode-se encontrar um leitor de impressões digitais USB por menos de US$ 100 nos Estados Unidos. Dessa maneira, o computador fica protegido pela biometria de alta tecnologia. Em vez de, ou em adição a um password, você precisa de sua própria característica para acessar o computador.

Mouse de computador com leitor de impressões digitais embutido

Prós e contras

Há diversas maneiras pelas quais um sistema de segurança pode verificar se uma determinada pessoa é um usuário autorizado. A maioria dos sistemas busca por um ou mais dos itens abaixo:

- o que você tem
- o que você sabe
- quem você é

Para passar pelo primeiro tipo de sistema, é preciso de alguma espécie de símbolo (como algum tipo de identificação magnética, por exemplo). Um sistema baseado no que as pessoas sabem, normalmente requer uma senha ou um código numérico. O terceiro sistema procura por evidências físicas de quem a pessoa diz ser, através de padrões específicos como impressões digitais, voz ou íris.

Os sistemas que buscam evidências físicas, como leitores de impressões digitais, possuem certas vantagens sobre os outros sistemas. Veja algumas:

- atributos físicos são muito mais difíceis de falsificar do que carteiras de identidade;
- não se pode “chutar” um padrão de impressões digitais como pode fazer com uma senha;
- não pode perder as próprias digitais, a voz ou a íris como pode acontecer com um cartão de acesso;
- não pode esquecer das impressões digitais como pode acontecer com uma senha.

Entretanto, por mais eficazes que sejam certamente não são infalíveis e também possuem desvantagens. Leitores óticos nem sempre são capazes de distinguir entre a imagem de um dedo e um dedo verdadeiro. Os leitores capacitivos podem eventualmente ser enganados por um molde do dedo de uma pessoa. Se alguém tivesse acesso às digitais de um usuário autorizado, essa pessoa poderia enganar o leitor e passar pelo sitema de segurança. Alguns leitores possuem sensores adicionais de pulso e calor para verificar se se trata de um molde ou de um dedo desmembrado, mas mesmo esses sistemas podem ser enganados por um molde gelatinoso das digitais tiradas de um dedo real.

Para tornar esses sistemas da segurança mais confiáveis, pode-se combinar uma análise biométrica com meios convencionais de identificação, como uma senha (da mesma maneira que um caixa eletrônico requer o cartão do banco e um código numérico).

O problema com sistemas de segurança biométricos é a extensão dos danos caso alguém consiga roubar informações de identidade. Se você perde seu cartão de crédito ou acidentalmente diz a alguém a sua senha, pode retirar um novo cartão ou alterar sua senha. Mas se alguém roubar suas impressões digitais, você terá um problema para o resto da vida. Você não poderia usar suas digitais como forma de identificação até que tivesse absoluta certeza de que todas as cópias foram destruídas. Não há nenhuma maneira de se obter novas digitais.

Mas, mesmo com esse significativo inconveniente, leitores de digitais e sistemas biométricos são uma excelente forma de identificação. No futuro, eles

provavelmente irão se tornar uma parte integral da vida diária da maioria das pessoas, assim como as chaves, os cartões de banco e as senhas são hoje.

Evidência de DNA

Nos últimos anos, a evidência de DNA passou a desempenhar um papel importante nos sistemas de justiça criminal de muitas nações. É utilizada para provar que os suspeitos estiveram envolvidos em crimes e para libertar pessoas condenadas erroneamente. Nos Estados Unidos, foi integrada a vários casos criminais notórios, incluindo o julgamento de Orenthal James (O. J.) Simpson e a investigação do assassinato de JonBenet Ramsey, em 1996.

Exame comparação de DNA

A maioria das pessoas tem uma idéia do que seja o DNA. É essencialmente um manual de instruções para tudo que existe em seu corpo. Uma molécula de DNA é uma cadeia longa e contorcida conhecida como **hélice dupla**. O DNA parece bastante complexo, mas na realidade é formado por apenas quatro **nucleotídeos**: adenina, citosina, guanina e timina.

Esses nucleotídeos existem como **pares de base** que se ligam como os degraus de uma escada. A adenina e a timina sempre formam pares, assim como a citosina com a guanina. Embora a maior parte da cadeia de DNA não difira de uma pessoa para outra, há alguns **3 milhões de pares de bases** de DNA (aproximadamente 0,10% de todo o genoma) que são diferentes.

Em células humanas, o DNA está agrupado em 23 pares de **cromossomos**. Um membro de cada par de cromossomos vem de sua mãe e outro de seu pai. Em outras palavras, seu DNA é uma combinação dos DNAs de sua mãe e de seu pai. A menos que você possua um irmão gêmeo, seu DNA é único. É isso que torna a evidência de DNA tão valiosa nas investigações - é quase impossível alguém ter o DNA idêntico ao seu.

A hélice dupla de DNA

A chave para a evidência de DNA está na comparação do DNA encontrado na cena do crime com o DNA do suspeito. Para isso, os investigadores devem fazer três coisas:

- coletar o DNA na cena do crime e também do suspeito (ver Como funcionam as investigações da cena do crime para maiores informações);
- analisar o DNA para criar um **perfil de DNA**;
- comparar os perfis entre si.

As autoridades podem extrair o DNA de quase todos os tecidos, incluindo cabelos, unhas, ossos, dentes e fluidos sanguíneos. Às vezes os investigadores possuem a evidência de DNA, mas não têm suspeitos. Nesse caso, os oficiais da lei podem comparar DNAs da cena do crime com perfis armazenados em um banco de dados. O banco de dados mais utilizado nos Estados Unidos chama-se **CODIS**, que significa Sistema de DNA Índice Combinado e é mantido pelo FBI. Pela lei, autoridades de todos os 50 Estados devem coletar amostras de DNA de estupradores para inclusão no CODIS. Alguns Estados americanos também obrigam todos os criminosos condenados a fornecerem uma amostra de DNA.

A maior parte dos testes de Análise de DNA forenses utiliza materiais do **núcleo** da célula. Às vezes, especialmente nas amostras mais antigas de tecido, como cabelos e dentes, não há mais restos do núcleo nelas. Nesses casos, os investigadores frequentemente utilizam a **análise mitocondrial do DNA**, que utiliza DNA de uma mitocôndria da célula.

Os avanços na evidência de DNA

Em 1985, o DNA entrou em um tribunal pela primeira vez como evidência em um julgamento, mas foi somente em 1988 que a evidência de DNA mandou alguém de fato para a cadeia. Trata-se de uma área complexa da ciência forense que se baseia em grande parte em antecipações estatísticas; nos primeiros casos, em que os jurados depararam com muitas evidências fortemente carregadas de fórmulas matemáticas, era fácil para os advogados de defesa criarem dúvidas na mente dos jurados. Desde então, alguns avanços permitiram que os investigadores criminais aperfeiçoassem técnicas envolvidas

e enfrentassem desafios legais para as impressões digitais do DNA. Eis alguns desses aprimoramentos:

- **novos procedimentos de testes** - a análise RFLP necessitava de grandes quantidades de DNA de qualidade relativamente alta. Os procedimentos mais recentes necessitam de bem menos DNA e podem ser concluídos mais rapidamente;
- **fonte de DNA** - a ciência tem maneiras de extrair DNA de fontes que costumavam ser difíceis ou muito contaminadas para serem utilizadas;
- **bancos de dados de DNA expandidos** - vários países, incluindo os Estados Unidos e a Grã-Bretanha, construíram bancos de dados elaborados com centenas de milhares de perfis individuais de DNA. No entanto, esses bancos de dados também levantam questões sobre privacidade. O DNA armazena muito mais informações sobre uma pessoa do que as impressões digitais. Por exemplo, o DNA de uma pessoa inclui informações sobre tudo, desde a cor dos olhos até defeitos genéticos. Algumas pessoas temem que a utilização difundida dos bancos de dados de DNA possa encorajar os governos a discriminar pessoas em razão de informações contidas em seu DNA. No entanto, acredita-se que o DNA utilizado para o banco de dados CODIS do FBI não corresponda aos traços reais de uma pessoa;
- **treinamento** - os laboratórios criminais desenvolveram protocolos formais para manipular e processar a evidência, reduzindo a probabilidade de contaminação das amostras. Na sala de julgamento, os promotores têm sido mais cautelosos ao apresentar evidências genéticas, e muitos Estados estabelecem regras específicas a respeito de sua admissibilidade nos casos criminais.
- **educação científica** - nos últimos anos, muitos debates surgiram em todo o mundo a respeito de questões como a utilização da evidência de DNA, clonagem de animais ou venda de alimentos geneticamente modificados. Desde essa época, os estudos sobre o DNA e suas propriedades têm se tornado mais profundos e divulgados.

Utilizando a evidência de DNA

Em razão do importante papel que a evidência de DNA teve no caso O. J. Simpson, a maioria das pessoas sabe que os perfis de DNA são utilizados por investigadores criminais para:

- **provar a culpa** - perfis de DNA correspondentes podem ligar um suspeito a um crime ou à cena do crime;
- **livrar um inocente** - inocentes foram libertados do corredor da morte nos Estados Unidos com base na evidência de DNA. Até aqui, a evidência de DNA tem sido quase tão útil ao excluir suspeitos quanto ao apontá-los e condená-los; aproximadamente 30% das comparações do perfil de DNA feitas pelo FBI resultam na exclusão de um suspeito;

A evidência de DNA é útil também para outras finalidades.

- **Teste de paternidade** e outros casos em que as autoridades precisam provar se indivíduos são parentes ou não - um dos testes de paternidade dos últimos tempos ocorreu em 1998, quando a revista "Nature" questionou se Thomas Jefferson, o terceiro presidente dos Estados Unidos, teve filhos com alguma de suas escravas.
- **Identificação** de cadáveres - os investigadores da Polícia frequentemente enfrentam a tarefa desagradável de tentar identificar um corpo ou restos mortais. O DNA é uma molécula bastante elástica e as amostras podem ser facilmente extraídas de cabelos ou ossos; uma vez criado o perfil, ele pode ser comparado a amostras de familiares de pessoas desaparecidas para verificar se existe correspondência. Os **militares** utilizam o perfil de DNA até mesmo no lugar do velho cão farejador. Cada novo recruta deve fornecer amostras de sangue e de saliva e essas amostras podem ser utilizadas posteriormente como um identificador positivo para soldados mortos na linha de fogo. Mesmo sem uma correspondência de DNA para identificar conclusivamente o corpo, o perfil é utilizado, pois pode fornecer pistas importantes sobre a vítima, como **sexo** e **raça**.
- Estudar a **evolução das populações humanas** - os cientistas estão tentando utilizar amostras extraídas de esqueletos e de pessoas vivas ao redor do mundo para mostrar como no passado as populações migraram por todo o globo e se diversificaram em tantas raças diferentes.

- Estudar **doenças hereditárias** - os cientistas também estudam as impressões digitais de DNA de famílias com membros que herdaram doenças como o **mal de Alzheimer** para tentar pesquisar diferenças cromossômicas entre aqueles que não têm a doença e aqueles que a têm, na esperança de que essas diferenças cromossômicas possam ser ligadas à aquisição da doença.

O futuro da biometria

A biometria pode fazer muito mais do que apenas determinar se alguém tem autorização para entrar em determinado local. Alguns hospitais usam sistemas biométricos para garantir que as mães levem o recém-nascido certo para casa. Os especialistas também têm aconselhado as pessoas que escaneiem documentos como certidão de nascimento e CPF e os guardem em uma memória com segurança biométrica no caso de uma emergência. Seguem algumas tecnologias biométricas que você poderá ver no futuro:

- novos métodos que usam o DNA, unhas, dentes, formato das orelhas, cheiro do corpo, características da pele e pulsação sanguínea;
- sistemas de uso doméstico mais precisos;
- clubes preferenciais, programas de compradores frequentes e sistemas rápidos de verificação com segurança biométrica;
- mais sistemas biométricos presentes em passaportes para serem usados em fronteiras e aeroportos.

Privacidade e outras preocupações

Algumas pessoas fazem objeções culturais ou religiosas à biometria. Outras imaginam um mundo no qual câmeras as identificam e rastreiam enquanto andam pelas ruas, seguindo suas atividades e padrões de consumo sem sua permissão. Elas se perguntam se as empresas venderão dados biométricos da mesma forma que vendem endereços de e-mail e números de telefone. Pessoas se preocupam também com a possibilidade de existir uma enorme base de dados com informações vitais de cada um e se isso seria seguro.

Os sistemas biométricos não têm a capacidade de armazenar e catalogar informações sobre todas as pessoas do mundo. A maioria deles armazena uma quantidade mínima de informações sobre um número relativamente pequeno de usuários. A maioria dos sistemas também trabalha apenas no lugar em que estão como num prédio comercial ou num hospital. As informações de um sistema não são necessariamente compatíveis com as de outros, embora várias organizações estejam tentando padronizar os dados biométricos.

Além do potencial quanto à invasão de privacidade, surgiram outras preocupações sobre a biometria.

- **Confiança em demasia**: a ideia de que os sistemas biométricos são perfeitos e pode fazer as pessoas esquecerem de procedimentos básicos de proteção aos dados do sistema.
- **Acessibilidade**: alguns sistemas não podem ser adaptados para certas pessoas, como idosos ou deficientes físicos.
- **Interoperabilidade**: em situações emergenciais, agências que usam sistemas diferentes podem precisar compartilhar dados e atrasos podem ocorrer se os sistemas não conseguirem se comunicar entre si.

Como visto na TV

Programas de televisão e filmes sempre mostram pessoas tentando passar por um sistema biométrico de segurança. Veja alguns dos truques mais comuns e saiba se eles funcionam ou não.

Tipo Biométrico	**Tentativa de entrada**	**Resultado**
Caligrafia	Assinatura Falsificada	O sistema mede o ato de escrever em si, não o resultado da escrita.
Geometria das mãos	Modelo exato da mão de uma pessoa	Seria possível burlar o sistema.

Timbre de Voz	Gravação da voz da pessoa	Seria possível burlar o sistema.
Projeção de íris	A imagem da íris de uma pessoa impressa em uma lente de contato.	Seria possível burlar o sistema.
Geometria das mãos	Modelo da mão de outra pessoa	Não seria possível reproduzir com exatidão as veias de uma pessoa.

Conclusão

De uma forma geral, as características biométricas mais utilizadas atualmente têm um período de vida bastante longo, mas algumas são mais persistentes e estáveis do que outras. Por exemplo, as impressões digitais são normalmente bastante estáveis, mas podem ser danificadas ou obscurecidas por danos na pele, devido ao envelhecimento da pessoa ou a desgastes ocupacionais.

Os padrões da íris são formados muito cedo na nossa vida e permanecem estáveis até à morte, a não ser que sejam obscurecidos por cataratas ou por outras doenças oftalmológicas. A geometria da face e da mão é menos estável e persistente, devido ao envelhecimento dos indivíduos, às variações do seu peso, e a outros fatores. No entanto, estes problemas podem ser ultrapassados através de recapturas periódicas das características biométricas.

Podem-se combinar diferentes características biométricas para se conseguirem níveis de segurança mais elevados em aplicações de alta segurança. No entanto, é mais comum combinar características biométricas com outros mecanismos de autenticação - por exemplo, cartão inteligente, ou número de identificação pessoal (PIN). Este conceito de autenticação múltipla permite uma abordagem por níveis que pode aumentar a privacidade e a segurança.

Um sistema de identidade que utilize cartões inteligentes e características biométricas pode reforçar significativamente a relação de confiança entre o portador de um cartão e o emissor desse cartão, bem como reduzir o risco e o custo de fraude e roubo de identidade. Neste tipo de sistemas, a característica biométrica é utilizada como chave segura que desbloqueia a informação sensível armazenada no cartão inteligente e ativa a utilização do cartão. Desta forma, se o cartão for roubado ou perdido, não terá qualquer utilidade sem a chave biométrica única do seu portador original.

Os padrões biométricos já atingiram um nível de maturidade bastante grande. Desde o início da década de 1990 que a indústria biométrica trabalha de forma estreita com organismos internacionais de padronização , de modo a definirem-se padrões para a promoção da interoperabilidade e para a uniformização de abordagens para implementar e testar sistemas biométricos.

Atualmente, os padrões estabelecidos incluem formatos de partilha de dados e APIs, bem como padrões para a utilização da biometria em transações financeiras seguras. Entretanto, os padrões biométricos continuam o seu caminho de maturação.

Para concluir, podemos referir que a tecnologia biométrica fornece a capacidade única de confirmar a identidade pessoal. Cada pessoa recebe características biométricas com o seu nascimento e continua a carregar esses identificadores biométricos consigo para onde quer que vá. Devido a esta capacidade única, a tecnologia biométrica pode ser utilizada para melhorar significativamente a segurança, aumentar a privacidade, e criar confiança nos sistemas de gestão de identidades atuais e do futuro.

Referências bibliográficas

Dr. Manfred Bromba. "Biometrics FAQ."
http://www.bromba.com/faq/biofaqe.htm#Biometrie

Greg Brown. "Ligando os pontos" Latin Trade, abril de 2005.
http://www.findarticles.com/p/articles/mi_m0BEK/is_4_13/ai_n13798070

FindBiometrics
http://www.findbiometrics.com/

Segurança em casa: Biométrica. GlobalSecurity.org
http://www.globalsecurity.org/security/systems/bometrica.htm

Jean-Fran쵠s Mainguet. "Biometrics." 2004.
http://perso.wanadoo.fr/fingerchip/biometrics/bometrica.htm

Prabhakar A., S., Ross e Jain A. Jain., "An Overview of Biometrics."
http://biometrics.cse.msu.edu/info.html

Recursos relacionados a biométrica e pessoas deficientes
http://www.icdri.org/biometrics/bometrica.htm

Thalheim, L., J. Krissler e P. Ziegler. "Body Check." WIBU Systems, novembro de 2002.
http://www.heise.de/ct/english/02/11/114/

John Daugman. "Iris Recognition for Personal Identification." O laboratório de computação: Universidade de Cambridge.
http://www.cl.cam.ac.uk/users/jgd1000/iris_recognition.html

Homepage do reconhecimento da íris
http://www.iris-recognition.org/