WHITE PAPER

O que é biometria?

AWARE

O que é biometria?

"A biometria são nossas características físicas (e comportamentais) mais exclusivas que podem, de forma prática, ser detectadas por dispositivos e interpretadas por computadores, assim, elas podem ser usadas como nossa representação no mundo digital. Dessa maneira, podemos associar dados digitais a nossa identidade com permanência, consistência e unicidade, e recuperar esses dados usando computadores de modo rápido e automatizado.

Identificação e confiança

Existem inúmeras coisas sobre nós que, combinadas, nos torna únicos, como nossos atributos físicos, endereço residencial, data de nascimento, relacionamentos e nosso conhecimento. A unicidade de nossa compleição física e história pessoal é representada pelo o que normalmente consideramos ser nossa "identidade." Em nosso mundo atual, habilitado por computadores interconectado, há uma utilidade cada vez maior em 1) atribuir corretamente informações digitais a um indivíduo e em 2) declarar nossa identidade de forma que possa ser comunicada e confiável. Nossa identidade pode ser usada simplesmente para atribuir corretamente informações pessoais que sejam úteis para propósitos futuros (por ex., um registro médico ou financeiro). Esses registros também nos permitem demonstrar um padrão de comportamento histórico para o estabelecimento de confiança e, consequentemente, compele à responsabilidade pessoal. Usamos essa confiança e responsabilidade para obter privilégios como acesso a um ativo, instalação ou país. Para fins de acesso, a utilidade da identificação é dobrada: primeiro, comunicar nossa confiabilidade e responsabilidade e depois - na tentativa de fazer uma transação com base em nosso "capital confiável" adquirido - para declarar que somos a mesma pessoa com quem a confiança foi anteriormente estabelecida. Por outro lado, nossa identidade pode ser desafiada a contrapor uma representação fraudulenta ou usada por outra pessoa para declarar uma desconfiança sobre nós.

Nossos nomes e números pessoais oferecem meios relativamente eficientes e testados para representar nossa identidade. O mais importante é que eles podem ser interpretados não apenas por pessoas, mas também por computadores para associar informações digitais e atributos de confiança ou desconfiança ao indivíduo, o que é claramente útil para múltiplas aplicações. Um histórico escolar, uma multa por excesso de velocidade e um histórico de crédito, todos servem para esse propósito. Nossos nomes e números são efetivos somente até o grau em que são 1) exclusivos, 2) permanentes, 3) consistentes e 4) únicos associados à nossa pessoa física. Sabemos que eles não são necessariamente exclusivos (p. ex. John Smith) ou permanente (p. ex. Judy Smith née Johnson) e eles não são, de forma clara, inequivocadamente associados a nós fisicamente (p. ex. uma tatuagem na testa). É onde

a biometria moderna é útil. A biometria são nossas características físicas (e comportamentais) mais exclusivas que podem, de forma prática, ser detectadas por dispositivos e interpretadas por computadores, assim elas podem ser usadas como nossa representação no ,mundo digital. Desta maneira podemos vincular dados digitais a nossa identidade com permanência, consistência e inequivocamente, e recuperar esses dados usando computadores de modo rápido e automatizado.

Modalidades Biométricas

Muito é feito sobre a amplitude das modalidades biométricas e a pesquisa de biometrias novas e exóticas (orelha, modo de andar, odor, etc.) são inevitáveis. As modalidades comprovadas em campo e em implantações de larga escala, são impressões digitais, rosto, íris e voz. Essas são as modalidades de biometria que, atualmente, melhor atendem nossos testes quanto à unicidade, permanência e consistência, ao mesmo tempo em que também é condutiva para a captura por meio de sensores de maneira prática em termos de ergonomia e economia. As técnicas proprietárias que também foram implantadas incluem vascular (veias da palma da mão e dos dedos) e geometria da mão.

A biometria, por natureza, é basicamente uma análise estatística, portanto:

a) quanto mais dados temos em uma amostra biométrica (ou conjunto de amostras), maior é a probabilidade de ela ser única,

b) sempre há a probabilidade de que duas pessoas diferentes gerarão amostras biométricas muito similares ou equivalentes, e

c) sempre há a probabilidade de um falso matching ou um falso não matching (erro de Tipo I ou II) resultar de uma comparação biométrica.

Algumas modalidades biométricas são menos permanentes com o decorrer do tempo do que outras, e algumas são mais difíceis de se apresentar e de se obter de forma consistente. Algumas têm uma tendência maior a apresentar problemas na qualidade da amostra.

Não existe uma modalidade biométrica perfeita; cada uma delas tem vantagens e desvantagens para uma determinada aplicação. Por exemplo, talvez a característica mais diferenciadora das impressões digitais como uma modalidade é que evidências são deixadas em uma cena de crime em forma de “latentes” (p. ex., impressões digitais em um vidro). Dentre as modalidades, íris talvez seja a mais consistente, densas em termos de informações e “parecidas com um código de barras”. As imagens faciais se destacam, porque são a modalidade biométrica que os humanos se distinguem em comparação e, portanto, podemos integrar o reconhecimento com base em uma interface homem-máquina. Além disso, as imagens faciais são abundantes no mundo digital e também podem ser coletadas secretamente à distância. A voz é notável por ser comportamental bem como física e, portanto, as amostras disponíveis de uma determinada pessoa são abundantes.

Mesmo quando nossas amostras biométricas são únicas, permanentes e consistentes e fisicamente associadas a nós, os sensores e os algoritmos que disponíveis para adquiri-las e analisá-las são imperfeitos. Os sensores introduzem distorção óptica e elétrica. Informações são perdidas à medida que os dados são convertidos de analógicos para digitais e novamente quando o sinal digital é compactado. As taxas de amostragem (resolução espacial no domínio digital) afetam significativamente a qualidade das amostras biométricas. Os algoritmos projetados para extrair “templates” para matching por um computador a partir de uma amostra, variam significativamente quanto à precisão e ao desempenho, da mesma forma que algoritmos e sistemas usados por computadores para avaliar rapidamente sua similaridade. Máquinas são boas em processamento de sinais automatizados, razoavelmente precisas e muito rápidas e em comparação de templates, mas não têm a capacidade humana de percepção, analisar e caracterizar visualmente a similaridade de duas amostras. Contudo, nosso corpo físico fornece muitos recursos que são adequados para comparação e pequisa biométrica, e os avanços nas tecnologias modernas de detecção e computação continuam aprimorando a capacidade de uma máquina executar a identificação biométrica de forma extremamente rápida e precisa.

Processos biométricos

Os sistemas biométricos contam com vários processos distintos: cadastro, captura ao vivo, extração de template e comparação de templates. A finalidade do cadastro é coletar e arquivar amostras biométricas e gerar templates numéricos para comparações futuras. Ao arquivar amostras brutas, novos modelos de substituição podem ser gerados no caso de um algoritmo de comparação, novo ou atualizado, ser introduzido no sistema. Práticas que facilitem o registro de amostras de alta qualidade são críticas para a consistência da amostra, aumentando o desempenho geral de matching, que é especialmente importante para a identificação biométrica por meio da pesquisa "um contra vários".

Podemos diferenciar a "captura ao vivo" do cadastro como o processo de coletar amostras de "averiguação" biométricas ao vivo durante a tentativa de acesso ou identificação e compará-las contra uma "galeria" de templates registrados previamente.

A extração de templates exige processamento de sinal das amostras biométricas brutas (p. ex., amostras de imagens ou áudio) para gerar um template numérico.

Os templates normalmente são gerados e armazenados no momento do cadastro para economizar tempo de processamento em comparações futuras. A comparação de dois templates biométricos aplica cálculos algoritmos para avaliar sua similaridade. Na comparação, uma pontuação de matching é atribuída. Se ela estiver acima de um determinado limite, os templates são considerados uma como matching positivo.

Normalmente, os algoritmos de extração e comparação de templates biométrico são proprietários (diferentes e secretos) e, portanto, não podem ser usados com aqueles de outros fornecedores no mesmo sistema (p. ex. para comparar templates gerados por produtos diferentes ou usar um algoritmo de matching de uma empresa para comparar templates gerados por algoritmos de outra empresa). As exceções são os geradores de minúcias de impressões digitais certificados pelo MINEX e os algoritmos de comparação. Essa categoria de templates e matchers foi especificamente projetada, testada e certificada de forma independente pelo NIST para ser interoperável para a verificação um a um e, portanto, ideal para armazenamento compacto em cartões inteligentes ou documentos de viagem.

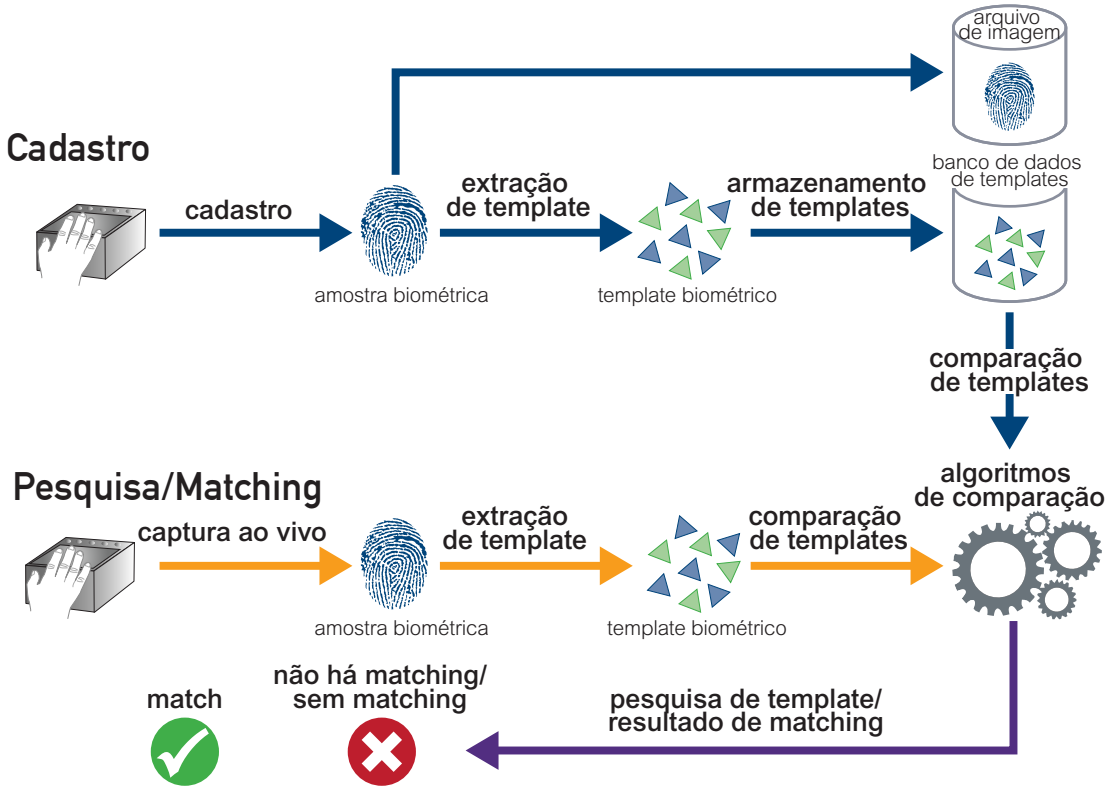

Figura 1 - Um sistema biométrico

Teste de precisão de sistema biométrico

A precisão de um sistema biométrico é quantificada tipicamente por uma "característica operacional do recebedor" ou plotagem de "curva ROC" indicando sua "taxa de identificação falsa, ou false-matching (FMR)" e a "taxa de não identificação falsa, ou false-non-matching (FNMR)" com base em alguma galeria de amostra biométrica. A taxa de matching falsa é a frequência com que as amostras biométricas de diferentes fontes são avaliadas incorretamente como sendo da mesma fonte. A taxa de não correspondência falsa é a frequência com que as amostras da mesma fonte são avaliadas incorretamente como sendo de fontes diferentes. Um sistema biométrico com bom desempenho é caracterizado por resultados imediatos e baixas taxas de matching falsos e não matching falsos. A precisão de um sistema se enquadra em um ponto na curva ROC cujo local é uma função do "limite" de matching aplicado. Um limite de correspondência mais alto reduz a taxa de falsa correspondência, mas aumenta a taxa de não correspondência falsa (maior segurança, menor praticidade). Um limite de matching mais baixo reduz a taxa de não correspondência falsa, mas aumenta a taxa de matching falso (maior praticidade, menor segurança; Veja a Figura 3). Maiores quantidades de dados (p. ex., mais impressões digitais) e amostras de qualidade mais alta (altamente consistentes) são necessárias para os processos de pesquisa "um contra N" em comparação com matching de "um contra um" para verificação.

É importante reconhecer que a precisão do sistema biométrico é altamente dependente da natureza dos dados biométricos contidos no sistema. Cada galeria diferente de dados biométricos em que um conjunto de amostras de averiguação é pesquisado produzirá uma curva ROC de precisão diferente. Existem várias galerias biométricas de domínio público e elas servem para fornecer análises de desempenho comuns para comparação de diferentes algoritmos de matching. Os algoritmos podem ser "treinados" para funcionar melhor em bancos de dados conhecidos, que é similar em ver as perguntas de um teste antes de fazê-lo. Fazer isso aumentará sua precisão comparativa em bancos de dados conhecidos, mas não indica necessariamente o desempenho do sistema em dados desconhecidos, como é o caso em uma aplicação real. Portanto, a melhor maneira de prever como um sistema biométrico se comportará em uma implantação real é testar seu desempenho em dados para os quais ele não foi treinado explicitamente.

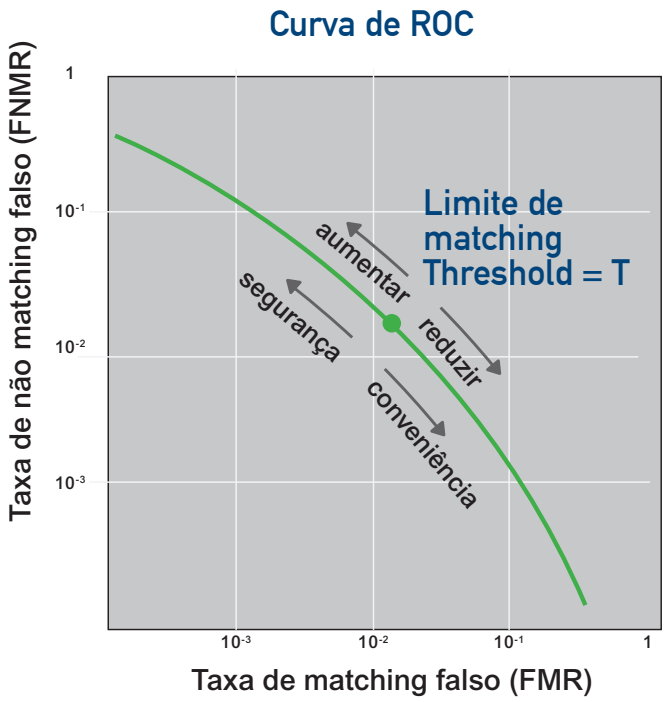

Figura 2 - Uma curva ROC para um determinado sistema de correspondência biométrico e conjunto de dados

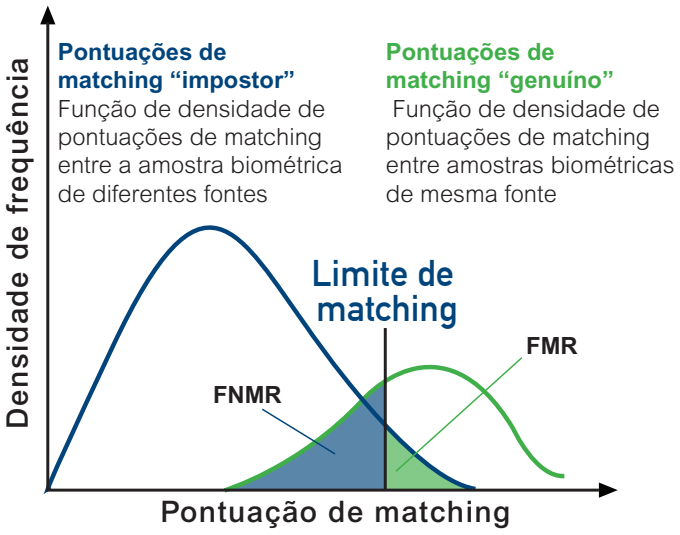

Figura 3 - Funções de densidade de pontuações de comparação entre a) amostras de fontes diferentes e b) amostras das mesmas fontes, ilustrando FMR e FNMR.

Aplicações biométricas

A primeira aplicação para biometria foi o uso de impressões digitais para identificar suspeitos em uma investigação criminal. Com a ajuda de tecnologias modernas de captura de imagem e computação avançada, esse processo que no passado era baseado em papel e trabalhoso, hoje é largamente digital e altamente (mas não completamente) automatizado. A nova tecnologia emprestou a pesquisa biométrica à outras aplicações como "autenticação" para vários aplicativos de controle de acesso lógico e físico, bem como a identificação biométrica em tempo real de proximidade e pesquisa de "lista negra" para controle de fronteira e outras aplicações onde os resultados são requeridos de forma extremamente rápida.

Os aplicativos biométricos podem ser classificados em três objetivos: 1) verificação, 2) identificação e 3) verificação de duplicidade:

A verificação envolve a execução de uma comparação biométrica "um contra um" com relação a acesso seguro a um ativo físico, como uma sala ou edifício, ou a um ativo digital, como um aplicativo de computador ou banco de dados. Para essa aplicação, a biometria é usada como senhas e códigos PIN para otimizar o controle de acesso ao executar uma comparação de uma amostra biométrica capturada ao vivo de um indivíduo com uma amostra armazenada anteriormente confiável única. Essa amostra armazenada pode residir em um banco de dados central, smartphone ou como um token em uma credencial como uma ID de cartão inteligente. Dessa maneira, podemos "autenticar" a declaração de identidade de uma pessoa, respondendo a pergunta "você é a pessoa para quem esse token foi emitido?" e usando o resultado de comparação para conceder ou negar seu acesso. O uso da biometria para controle de acesso é de especial interesse para aplicativos de segurança comerciais ou pessoais. A verificação biométrica pode ser oferecida como uma alternativa mais conveniente ou aprimoramento para PIN ou senha, nesse caso essa opção é oferecida para uso do usuário, mas ele pode optar por ignorá-la e usar a entrada de PIN ou senha a seu critério. Esse é o modelo de uso empregado pelo Apple iPhone 5S, por exemplo.

A identificação é um processo muito diferente e mais exigente (em termos de algoritmo biométrico e desempenho computacional) que serve para avaliar se a biometria de um indivíduo está presente em um banco de dados ou "galeria". Uma galeria pode conter dezenas de milhões de templates ou muito mais. Nesse processo, a biometria capturada de um indivíduo é capturada e enviada para um sistema de pesquisa biométrica para a comparação "um contra vários". O sistema compara matematicamente o modelo da amostra de captura com todos os templates da galeria. Ao fazer isso, a biometria ajuda a identificar um indivíduo, mesmo se ele não apresentar sua identificação verdadeira. A identificação é realizada com mais frequência para aplicações do setor público, onde a identidade confiável é essencial para a segurança pública, incluindo investigação criminal e aplicação da lei, emissão de visto e controle de fronteira, verificações de antecedentes criminais , defesa e inteligência.

A verificação de duplicidade é outro processo biométrico executado para determinar se há indivíduos presentes mais de uma vez em um banco de dados. Essa verificação pode ser executada para detectar fraude como no caso em que um indivíduo tenha se registrado várias vezes em um programa de benefício social. Esse processo envolve a verificação de templates biométricos de cada registro no banco de dados alternado, em um processo chamado "deduplicação biométrica."

Dispositivos e sensores

Dispositivos e sensores são qualquer sistema mecânico ou eletrônico usado para registrar e capturar amostras biométricas brutas de forma que possam ser digitalizadas e convertidas em um template biométrico. Para impressões digitais, rosto, íris e voz, existem sensores de impressões digitais, as câmeras digitais, as câmeras de íris e os microfones, respectivamente. A maioria dos sensores de impressão digital é baseada em tecnologias óticas ou capacitivas, mas os sensores de emissão de luz e as abordagens multiespectrais estão começando a ser adotadas. Os sensores capacitivos podem ser de dedo inteiro ou para passar o dedo. É fundamental para o desempenho dos matchers que as imagens das impressões digitais sejam capturadas com uma resolução (500 ppi) e contraste suficientes, sejam compactadas adequadamente com WSQ e estejam sem distorção. Um sensor óptico usa um prisma, uma fonte de luz e um sensor de luz para capturar as imagens das impressões digitais. Os sensores capacitivos são baseados em um chip de silício que detecta correntes elétricas quando os sulcos do

dedo fazem contato. Os sensores de dedo não geram qualidade de imagem suficiente para identificação de “um contra N”. De modo geral, a quantidade e a consistência das amostras biométricas exigidas é uma função do tamanho do banco de dados que deve ser pesquisado.

A captura de imagens faciais é efetuada por meio de camêras digitais de mercado, câmeras de bolso e webcams. A tecnologia de sensor de baixo custo foi significativamente aprimorada recentemente, também tornando possível a captura facial biométrica por meio de smartphones. Tradicionalmente, as imagens faciais digitais exigem uma resolução entre olhos de cerca de 60 pixels para verificação um contra um e 90 pixels para uma identificação mais precisa um contra vários. O fator mais crítico e desafiador que afeta o desempenho do matcher facial é a consistência; a obtenção de pose consistente, ângulo da cabeça e expressão facial do indivíduo, e brilho, contraste e nitidez e falta de uniformidade de fundo da imagem inteira.

A biometria da íris também se beneficiou das significativas melhorias dos sensores. A identificação da íris difere da de rosto, porque exige uma imagem infravermelha da íris para otimizar o contraste da imagem e, assim, facilitar a análise feita por máquina. Quanto melhor o grau de pureza da imagem infravermelha capturada (com o mínimo de “poluição” a partir da luz visível), melhor será o desempenho de matching obtido. Esse é o motivo pelo qual as câmeras disponíveis no mercado ainda não são usadas para a captura de imagem da íris e é necessária uma câmera especial; um sistema deve iluminar a íris com a luz infravermelha e, em seguida, filtrar outros comprimentos de onda.

Seus recursos de áudio e ubiquidade tornam os smartphones um meio especialmente viável para implantar biometria de voz em larga escala para a verificação um contra um. A biometria de voz é impedida pelos mesmos desafios que os da biometria facial, pois os ambientes de captura podem ser imprevisíveis e inconsistente; como acontecem com os interferências de fundo das imagens faciais podem interferir no processo de captura e correspondência

Modos de uso e arquitetura do sistema

Uma aplicação biométrica “com base no proprietário” é aquela pela qual um único indivíduo usa a verificação biométrica um para um para proteger o acesso a seus próprios ativos, como um smartphone. Um sistema “baseado em permissão” envolve o controlador de um ativo concedendo autoacesso para aquele ativo, (p. ex. uma empresa que usa a biometria para conceder acesso aos funcionários a seus dados). As aplicações “baseadas em operador” exigem que um operador do dispositivo, treinado e autorizado, colete a biometria do indivíduo fornecendo a amostra biométrica, como no caso de aplicação da lei. As aplicações “com base em quiosque” exigem que a captura seja executada pelo indivíduo sem qualquer treinamento ou experiência e o mínimo de instrução, como em controle de fronteira automatizado.

O local do template ou templates biométrico(s) previamente registrado(s) a partir do qual o template de uma amostra capturada ao vivo é comparada pode residir em qualquer um dos vários locais, incluindo em um smartphone, em uma credencial como um chip de cartão de identificação ou código de barras impresso, em um dispositivo móvel de captura biométrica ou em um servidor central. O local dos modelos registrados e o local onde a correspondência é executada são uma função do caso de uso, desempenho e segurança do aplicativo. A comparação biométrica um para um pode ser inteiramente executada até no chip de um cartão inteligente.

Privacidade

Os governos coletam informações pessoais sobre seus cidadãos, normalmente, com interesse em promover melhoria social, médica e de segurança física de algum tipo. Nem todos concordam sobre o quanto dessas informações pessoais é excessiva e a biometria tende a resumir informações pessoais consideradas como sendo excessivas. O uso histórico da biometria por órgãos governamentais de policiamento como uma ferramenta para registro criminal e investigação perpetua, acaba por perpetuar sua associação com a privação de direitos pessoais. Em algumas partes do mundo, existe um histórico de abuso de informações pessoais que gerou uma forte aversão a sua posse pelos governos. Embora, atualmente, as corporações privadas possuam, usem e transfiram quantidades

de dados pessoais significativamente maiores, temos a tendência de considerá-las mais inócuas e que estamos obtendo algo em troca, como o uso de seus produtos.

Mais recentemente, com a proliferação da Internet, das câmeras digitais, smartphones e mídia social foi introduzida a era do "Big Data" e com ela veio um aumento exponencial na disponibilidade de dados pessoais e o potencial para seu abuso. Estamos aprendendo que nessa nova era, a privacidade é uma escolha muito pessoal; alguns indivíduos optam por minimizar a quantidade de informações pessoais que compartilham, enquanto outros, entusiasticamente, "as compartilham em excesso". Nos dois casos, a biometria tem o potencial de fornecer meios mais práticos e seguros para aumentar a privacidade por meio de um melhor controle de acesso a uma crescente e vasta abundância de informações pessoais, especialmente quando usadas em conjunto com outros mecanismos tradicionais de segurança como números PIN e senhas.

A abundância das imagens faciais na Internet oferece a oportunidade que sejam abusadas como biometria. É concebível que por meio de um processo de "resolução de identidade", as imagens faciais e seus dados associados (por ex., nome, escola, associações, etc.) possam ser associados por meio de identificação facial biométrica com informações de diferentes sites e bancos de dados onde as imagens faciais estão armazenadas. A resolução da identidade é um processo, bem diferente, os dados "em silos" são agregados em uma "identidade digital" que compreende uma visão mais abrangente de uma pessoa que existe a partir de qualquer fonte de dados individual. Quando quantidades pequenas e dispersas de informações pessoais foram disponibilizadas — cada uma com um uso específico e um público em mente — a agregação desses dados pessoais a partir de várias fontes disponibilizadas com uma pesquisa facial biométrica pode constituir uma ameaça à privacidade. Deve-se notar que não está claro se isso realmente já foi feito de forma que afetou a privacidade de alguém. Além disso, esse processo é mais tradicionalmente (e talvez mais efetivamente) executado usando os dados em texto e, portanto, existe uma ameaça potencial com ou sem a presença de imagens faciais. Vale a pena notar que outras modalidades biométricas não apresentam o mesmo risco que as imagens faciais para este tipo de processo, porque não existem abundantemente em domínio público. Ao avaliar o impacto da biometria na privacidade, é essencial considerá-la em um contexto mais amplo de todos os dados de identidade baseados em sinal e em texto; isso inclui os dados que são mantidos pelos órgãos governamentais e por entidades privadas, disponíveis na Internet e a partir de outros códigos abertos.

Segurança

Existem pouquissimos relatos de sistemas biométricos fraudados, seja para evitar identificação ou seja obter acesso não autorizado. Ocasionalmente, os jornalistas simulam tentativas de violação e as publicam largamente, portanto, a ameaça de furos de segurança contidos na biometria tende a ser uma percepção aumentada.

O primeiro cenário de ameaça é onde um indivíduo, de alguma forma, obscurece suas amostras biométricas para evitar a identificação, como pela mutilação das impressões digitais ou dilatação da íris. Isso não é eficaz, porque é altamente detectável e, no caso de mutilação, irreversível.

O segundo cenário é aquele em que uma amostra biométrica é obtida ou fabricada secretamente por um impostor e de alguma forma é adulterada ou "falsificada" para obter fraudulentamente entrada ou acesso aos ativos do proprietário legítimo, usando um PIN, uma senha ou uma credencial roubada. Mas embora as senhas possam ser alteradas e reemitidas para o usuário legítimo, a permanência inerente da biometria as impede de ser alteradas e, portanto, o uso seguro daquela modalidade biométrica no futuro ficará possivelmente comprometida, pelo menos, até o impostor ser identificado.

A falsificação ou o obscurecimento de uma biometria requer habilidade e esforço, e é extremamente difícil não ser detectada Ao mesmo tempo em que isso é concebivelmente possível, é particularmente difícil, não confiável e ineficaz em situações onde a captura biométrica tem várias amostras, vários modos, executada por um operador ou usada com outros mecanismos de segurança. Aprimoramentos na "detecção de vida" (por exemplo, detecção de fluxo sanguíneo, piscadela e pulsação da pupila do olho) e outras técnicas antifalsificação torna a maioria dos modos de falha praticamente impossíveis. Outra técnica é emitir a biometria

"revogável", que é codificada e conciliada somente em um domínio criptografado. Ela é segura e pode ser regenerada, caso seja comprometida.

Praticamente todos os mecanismos de segurança podem ser violados com algum grau de habilidade e esforço, e a biometria não é uma exceção. A segurança da biometria deve ser considerada no contexto de sua aplicação em termos relativos com outros mecanismos alternativos de segurança. É importante usar a biometria em conjunto com outras medidas de segurança; nenhum mecanismo de segurança deve parar de funcionar sob um único modo de falha.

About Aware, Inc.

A Aware é uma fornecedora líder de mercado de produtos de software de biometria e serviços de desenvolvimento para departamentos governamentais, integradores de sistemas e fornecedores de solução globalmente. Nossos produtos incluem SDKs, componentes de software, aplicativos de estação de trabalho e uma plataforma modular, centralizada e orientada serviço. Eles atendem uma ampla gama de funções essenciais para a autenticação biométrica e pesquisa usando impressões digitais, face e íris, incluindo captura automática de amostra, controle de qualidade de imagem, abstração de periféricos de hardware de captura, processamento de dados e fluxo de trabalho centralizados, conectividade de subsistema e algoritmos de correspondência biométrica. Os produtos são usados para permitir soluções de segurança centradas na identificação com biometria para aplicações incluindo aplicação de lei, gerenciamento de fronteira, credenciamento e controle de acesso, e defesa e inteligência. A Aware é uma empresa de capital aberto (NASDAQ: AWRE) com sede em Bedford, Massachusetts.

AWARE

Para maiores informações:

sales@aware.com
www.aware.com