

É você mesmo?

A autenticação biométrica já é usada em todo o mundo. Conheça as iniciativas de código aberto para uso dessa técnica.
por **Alessandro de Oliveira Faria (Cabelo)**

Segundo o dicionário, biometria é o ramo da ciência que estuda os seres vivos baseando-se nas medidas e estrutura dos órgãos. “Bios”=“vida” e “metron”=“medida”; sendo assim, define-se biometria como “medida da vida”. A biometria deixou de ser ficção científica há algum tempo e hoje faz parte do nosso dia-a-dia. Ao contrário do que muitos pensam, a biometria era utilizada muito antes da era da informática.

No século II a.C., governantes da China utilizavam impressões digitais para lacrar documentos. Além disso, em todo o mundo a impressão digital e fotos são utilizadas para registrar um ser humano, e com esses registros é possível a identificação sem grandes esforços.

O ineditismo na década de 90 foi apenas a utilização da biometria em sistemas de informática. A biometria ganhou atenção científi-

ca somente no final do século XIX, quando as características físicas das pessoas passaram a ser armazenadas para fins judiciais. Já no início do século XX, a biometria ganhou espaço nos documentos de identidade (RG, no Brasil).

Atualmente, no início do século XXI, esse assunto encontra-se em evidência para garantir a autenticação e gerenciamento de identidade. Para tal tarefa, a biometria é totalmente pertinente à situação. O principal motivo é a estabilidade das características corporais e comportamentais, assim agregando confiabilidade à tecnologia.

A biometria com código aberto evolui a cada dia, cada projeto na sua velocidade de amadurecimento. Essa evolução não acontece na velocidade dos projetos de software convencionais. Os principais motivos, na minha opinião, são a necessidade de profundos conhecimentos matemá-

Para quem deseja fundamentar conceitos de desenvolvimento nesse segmento, são aconselháveis estudos de algoritmos de visão computacional como *OpenCV* e *Mimas* para se familiarizar com processamento de imagens, reconhecimento de padrões e treinamento da rede de algoritmos.

No Brasil, a NETi Tecnologia desenvolve e pesquisa o assunto na plataforma Linux desde 1998. Atualmente, a empresa trabalha comercialmente com foco na tecnologia proprietária de reconhecimento facial da Cognitec System. Entretanto, a divisão de pesquisa sempre tem atenção às soluções de código aberto.

Conceito

O homem sempre teve a necessidade de restringir o acesso de outras pessoas a determinados locais ou bens considerados privilegiados ou particulares. Normalmente utilizamos cartões ou senhas para obter acesso a sistemas ou locais restritos. Entretanto, senhas e cartões podem ser roubados, perdidos, esquecidos ou revelados. Nesse momento começam as preocupações relacionadas a fraude e acesso por usuários não autorizados. Já a biometria converte uma característica ou comportamento em códigos de barras humanos que não apresentam esses pontos negativos.

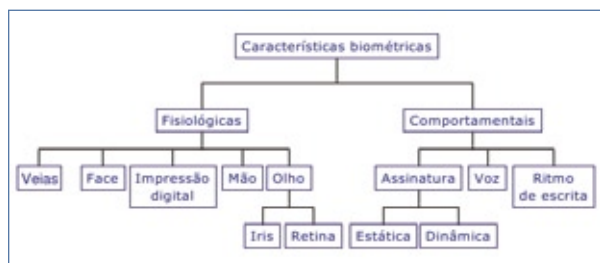


Figura 1 Classificação das técnicas biométricas.

Para efetuar a autenticação biométrica em sistemas computacionais de código aberto ou proprietários, devemos num primeiro momento entender o conceito e a funcionalidade dessa tecnologia, independente do tipo (impressão digital, face, voz, íris e outros).

Em primeiro lugar, a biometria pode resolver duas necessidades distintas, ou seja, podemos utilizá-la para verificar a identidade de um usuário ou para identificá-lo. Em ambos os casos, a biometria é a única maneira de garantir a presença do proprietário durante a operação.

A identificação é apenas uma varredura no banco de características em memória ou em disco. Esse processo decide qual registro de amostragem possui o coeficiente de similaridade mais próximo ao do usuário submetido à identificação. Essa tarefa requer maior poder computacional, sendo que toda a base de dados será analisada no menor tempo possível e aceitável para uma operação. Essa técnica é chamada de 1:N (um para muitos), porque os dados da pessoa são comparados a todos os registros da base de dados.

A verificação de identidade é o processo mais utilizado em sistemas de autenticação de usuários, pois nessa operação o usuário necessita informar a sua identidade ou PIN (número de identificação pessoal). Ao informar o PIN (por meio de um login, código, email ou outros), o usuário estará previamente recuperando na base de dados o seu registro biométrico para uma comparação. Essa técnica é conhecida por 1:1 (um para um), pois os dados do usuário são comparados apenas a um registro do banco de dados.

BioAPI

Com o mercado em constante evolução, diversas APIs e tecnologias biométricas, assim como o grande número de padrões, causam confu-

sões e retrabalhos aos desenvolvedores de aplicativos. Então, algumas empresas sentiram a necessidade da criação de uma API única para garantir o manuseio e evolução das tecnologias biométricas. Vale a pena ressaltar que alguns projetos de código aberto, como o *Libface*, estão prevendo a compatibilidade com o consórcio da BioAPI.

Foi assim que surgiu a BioAPI Consortium, com os seguintes objetivos:

- ▶ propiciar uma API com diversos níveis;
- ▶ disponibilizar uma plataforma suportada por múltiplas tecnologias biométricas;
- ▶ oferecer uma arquitetura de segurança robusta;
- ▶ garantir o desenvolvimento independente do distribuidor.

Sendo assim, a BioAPI proporciona aos programadores o mais alto nível da API, garantindo, dentro do possível, a produtividade, a portabilidade e a preservação do investimento. A criação desse padrão único foi possível tomando como ponto de partida um exame das APIs existentes no mercado e baseando-se nos pontos positivos das chamadas de cada API.

Tipos de biometria

A biometria pode ser utilizada com o comportamento do usuário ou características físicas (veja a [figura 1](#)). Obviamente, cada uma das opções possui seu grau de complexidade matemática. A impressão digital, veias da mão, face, íris, retina e geometria da mão são classificadas como características fisiológicas. Já o reconhecimento de escrita, voz e assinatura encontram-se no grupo de características comportamentais. A aplicabilidade de cada tecnologia deve ser confrontada com a necessidade do cliente para obter a melhor tecnologia empregada.

O **reconhecimento facial** é o método mais usual para reconhecimento entre seres humanos. Além de identificarmos pessoas, podemos perceber seu estado emocional apenas observando sua expressão facial. Aplicações estáticas e assistidas (nas quais a imagem, a iluminação ambiente e a verificação são controladas) favorecem a precisão do sistema. Quando a aplicação é desassistida ou a iluminação ambiente e a imagem não são controladas, devemos aumentar o coeficiente de similaridade, tornando o sistema exigente e obtendo, assim, resultados precisos.

Embora o reconhecimento facial seja uma tarefa simples para o ser humano, é extremamente complexo



Figura 2 Projeto Malic em ação marcando os pontos importantes para a identificação facial.

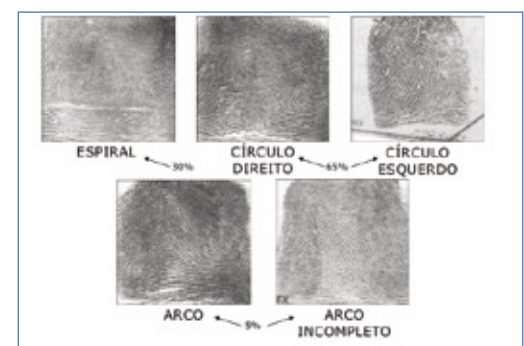


Figura 3 As impressões digitais se enquadram em cinco categorias distintas, mas em todas elas as medições são feitas da mesma forma.



Figura 4 Antes de proceder aos cálculos para identificação da íris, o software precisa definir seus limites.

implementar esse processo em uma máquina, pois não sabemos ao certo como o cérebro humano realiza essa tarefa. O cérebro humano pode identificar corretamente uma pessoa a partir de sua imagem facial mesmo sob as mais diversas condições, como variações de iluminação, observando apenas uma de suas características ou partes, e até mesmo com distorções ou deformações.

Diversos projetos de código aberto, como *Libface* e *Malic* (figura 2), trabalham com a tecnologia de reconhecimento facial. Porém, é aconselhável o uso desses projetos apenas para fundamentar conceitos matemáticos e computacionais, pois eles não sofrem atualizações periódicas. Além disso, esses pacotes trabalham com bibliotecas matemáticas voltadas para o uso de visão computacional e reconhecimento de padrões. Para trabalhar com essa tecnologia na plataforma Linux, é imprescindível ter profundos conhecimentos das APIs de vídeo-captura *V4L* (*video for linux*) nas versões 1 e 2, pois a utilização e conversão dos espaços de cores utilizados (RGB, YUV, YUY2) impacta diretamente no consumo de memória e CPU.

Vale a pena ressaltar que essa tecnologia pode ser aplicada a fluxos de vídeo ao vivo (dispositivo de vídeo-cap-

tura como uma webcam) e também podemos efetuar o reconhecimento com uma foto armazenada em disco. Assim, desvinculamos a tecnologia de um hardware específico.

A **impressão digital** é formada nas superfícies dos nossos dedos nos primeiros meses de vida. Na verdade, sua constituição acontece ainda quando feto. A impressão digital acompanha a pessoa por toda a sua existência sem apresentar grandes mudanças.

As digitais são classificadas em cinco grupos (mostrados na figura 3): círculo esquerdo, círculo direito, arco, espiral e arco incompleto. Ela é composta por linhas formadas pelas elevações da pele. A comparação por impressão digital é um método muito utilizado atualmente como forma de identificação de usuários.

Extraindo os pontos característicos ou “pontos de minúcias” de uma impressão digital, um papiloscopista ou sistemas computadorizados podem identificar pessoas utilizando cálculos bastante confiáveis. Grande parte dos algoritmos trabalham com o princípio de extração dos pontos de minúcias ou pontos característicos. Após a extração, são calculados a relação entre as distâncias desses pontos. Cada algoritmo possui a sua base de cálculo, seja por análise dos pontos entre si ou por agrupamentos de pontos para análise de semelhanças de triângulos com os ângulos internos.

Essa tecnologia está vinculada ao hardware biométrico. Ou seja, os sensores utilizados para obter a imagem da digital impactam na performance do sistema, por causa da resolução da imagem obtida. Existem

diversos projetos de código aberto, em particular o promissor projeto *fprint*, que surgiu da união de outros projetos de código aberto. Além disso, a biblioteca *fprint* se encontra em um estágio de produto e não de prova de conceito.

Embora essa tecnologia apresente um vínculo com o hardware de captura das digitais, o projeto livre *fprint* apresenta uma compatibilidade com uma ampla variedade de sensores disponíveis no mercado (inclusive os da Microsoft).

A **íris** constitui anéis em torno da pupila delimitados pela parte branca do olho. A íris carrega consigo diversas informações de um indivíduo. Gêmeos univitelinos apresentam íris diferentes. A complexidade da íris do olho humano teoricamente a torna única a cada usuário. A imagem da íris pode ser capturada utilizando-se uma câmera convencional, iluminação adequada e luz infravermelha. A captura pode ser automatizada pelo sistema ou capturada manualmente. No caso de captura automática, o software deve se encarregar do ajuste do foco (figura 4), entre outras propriedades da imagem.

O projeto JIRRM, embora não apresente atualizações, reconhece uma íris presente na imagem submetida ao sistema. Na página oficial[1], encontramos informa-

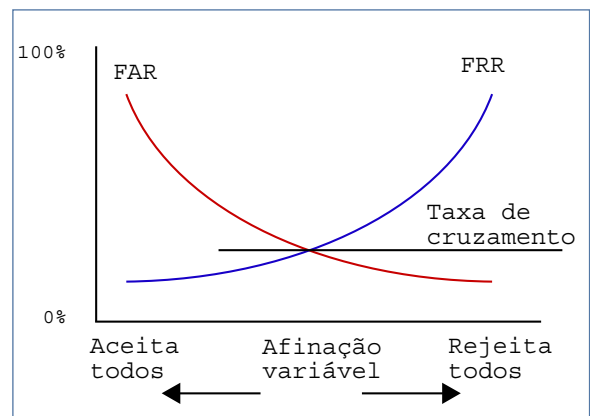


Figura 5 O ponto de cruzamento entre os falsos positivos e falsos negativos é o que se busca no momento de conferir uma medida biométrica.

ções que mencionam planos para processamento e comparação entre amostras. O projeto JIRRM identifica a íris e somente então limita a área para posterior análise. Não se pode deixar de mencionar que essa tecnologia também trata dos problemas de fracasso na leitura (*Failure to Enroll* – FTE).

Precisão e confiabilidade

Na escolha de um sistema de autenticação biométrico, o desempenho deve ser levado em conta, pois também está relacionado à taxa de acertos e erros da biometria. Essas taxas são medidas pelos coeficientes FAR (taxa de falsa aceitação) e FRR (taxa de falsa rejeição). Esses termos são utilizados constantemente em qualquer documentação relacionada a projetos biométricos.

O FAR é o coeficiente que mede e quantifica, em porcentagem, quantas vezes os usuários não cadastrados foram falsamente aceitos no sistema. Já o FRR corresponde à medida de usuários cadastrados que foram rejeitados pelo sistema incorretamente. Como mencionado anteriormente, alguns documentos também trabalham com o FTE (fracasso de leitura), que representa os usuários que não conseguem efetuar o cadastramento. Por exemplo, alguns documentos estatísticos mencionam que, dependendo da região no mun-

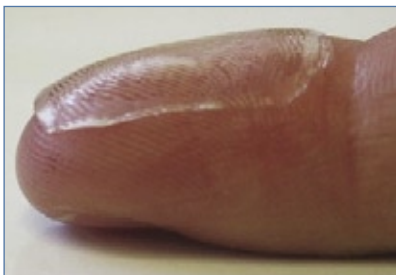


Figura 6 É relativamente fácil burlar um sistema de autenticação por impressão digital com materiais e ferramentas simples.

do, entre cinco e dez por cento da população não possuem impressão digital com amostragem suficiente para cadastramento.

A configuração dessas taxas é fundamental para o desempenho do sistema. A falsa rejeição causa frustração e a falsa aceitação causa fraude.

Muitos sistemas podem ser configurados para fornecer detecção forte (baixo FAR e alto FRR) ou detecção fraca (baixo FRR e alto FAR). A medida crítica é conhecida como taxa de cruzamento (*crossover rate*), e é o ponto onde o FAR e o FRR se cruzam (**figura 5**).

Nada é perfeito

A ciência não é perfeita, e ocasionalmente variações podem causar uma falsa rejeição ou aceitação dependendo do critério na configuração do sistema. Existem maneiras comprovadas para se burlar leitores de impressão digital utilizando uma amostragem digital falsa feita de gelatina ou silicone (**figura 6**). Características físicas da gelatina idênticas à da pele já proporcionaram fraudes ao sistema [2].

Por menor que seja a taxa de erro, ela ainda existe. No ano de 1903, um dos casos mais polêmicos envolvendo identidade enganada foi o de Will West, que foi julgado e condenado por um crime que não havia cometido.

Além da semelhança visual entre Will e o verdadeiro criminoso (confira na **figura 7**), os dois homens também tinham nomes semelhantes. As fórmulas derivadas das medidas de Bertillon também eram quase idênticas, ou seja, encaixavam-se na variação de características aceitável para um mesmo indivíduo.

Com o poder computacional dos dias atuais, a precisão dos algoritmos atingiu um nível de confiabilidade muito alto, principalmente as tecnologias que trabalham diretamente

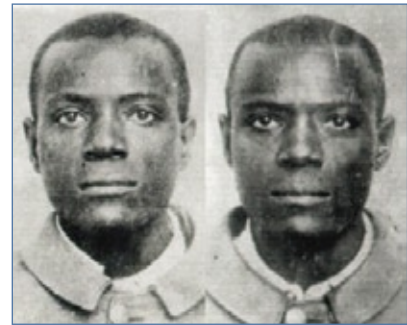


Figura 7 Em 1903, Will West foi condenado erroneamente por um crime que não cometeu – em virtude de um erro do método matemático.

com imagens ao vivo ou estáticas. Porém, para aumentar ainda mais essa margem de acertos, sugere-se a utilização da multi-biometria (utilização de duas ou mais tecnologias biométricas), assim tornando inviável uma fraude em qualquer sistema computacional. Há diversos tutoriais sobre esse assunto no portal Viva o Linux [3]. ■

Mais informações

[1] JIRRM: <http://jirm.sourceforge.net/>

[2] Sandstrom M., “Liveness Detection in Fingerprint Recognition”, 2001: <http://liu.diva-portal.org/smash/record.jsf?pid=diva2:19729>

[3] Portal Viva o Linux: <http://www.vivaolinux.com.br/>

Sobre o autor

Alessandro Faria é sócio-proprietário da NETi Tecnologia (<http://www.neti-tec.com.br>), especializada em desenvolvimento de software e soluções biométricas. Além disso, é consultor biométrico na tecnologia de reconhecimento facial, desenvolve soluções de código aberto desde 1998, é membro colaborador do portal Viva O Linux e mantenedor da biblioteca de código aberto de vídeo captura, entre outros projetos.