

WHITEPAPER

O IMPORTANTE PAPEL DA DETECÇÃO DE VIVACIDADE NA AUTENTICAÇÃO POR BIOMETRIA FACIAL

E COMO ESCOLHER A OPÇÃO CERTA PARA O SEU CASO DE USO





Para que a biometria facial realmente tenha ampla adoção como um método superior de autenticação, é essencial que se faça distinção entre um rosto vivo autêntico e uma representação artificial de um rosto na tentativa de falsificar o sistema. A detecção automatizada de ataques de apresentação, especificamente a detecção de vivacidade, tornou-se um componente obrigatório de qualquer sistema de autenticação baseado na tecnologia de biometria facial que não conta com a supervisão de um ser humano na tentativa de autenticação.

Este artigo discute a necessidade da detecção de vivacidade, como ela funciona e suas abordagens.



INTRODUÇÃO

A biometria facial está rapidamente ganhando aceitação entre consumidores e empresas como um método conveniente e seguro de verificação de identidade. A tecnologia preenche lacunas de segurança que são frequentemente exploradas em soluções que dependem de informações que podem ser perdidas ou roubadas, como uma senha ou a resposta para uma pergunta “secreta”, bem como novos golpes, como fraude de cartões SIM. Simplesmente mostrar o rosto para uma selfie também é muito menos desagradável para os usuários.

A tecnologia de reconhecimento facial progrediu muito nos últimos anos com os avanços da inteligência artificial, a ampla disponibilidade de câmeras de alta qualidade e baixo custo e a subsequente criação de uma grande quantidade de dados publicamente disponíveis para o treinamento de algoritmos de reconhecimento facial. Melhorias contínuas no poder de computação, incluindo unidades de processamento gráfico (GPUs) e sua disponibilidade, possibilitaram a aplicação de algoritmos sofisticados de machine learning — como redes neurais convolucionais e redes neurais profundas — nesses sistemas e sua execução em dispositivos comuns. Além de altamente precisos, os algoritmos de hoje são rápidos o suficiente para serem implementados em grandes sistemas comerciais de autenticação — mesmo aqueles com vários milhões de usuários.

COM A CAPACIDADE DE REFORÇAR A SEGURANÇA E MELHORAR A EXPERIÊNCIA DO USUÁRIO, A BIOMETRIA FACIAL APLICA-SE A VÁRIOS CASOS DE USO, DESDE O DESBLOQUEIO DE DISPOSITIVOS MÓVEIS E A SEGURANÇA DE TRANSAÇÕES FINANCEIRAS E PRONTUÁRIOS MÉDICOS ATÉ A MELHORIA DE PROCESSOS DE INTEGRAÇÃO DIGITAL.

As aplicações na vida real da biometria facial para autenticação levantam a questão da segurança. Se um possível fraudador pode ter acesso fácil à representação do rosto de uma pessoa e apresentá-lo como sendo o seu, é possível confiar nesse método de autenticação?

Para que a biometria facial realmente tenha ampla adoção como o melhor modo de autenticação, é essencial que se faça distinção entre um rosto vivo autêntico (real) e uma representação artificial de um rosto na tentativa de falsificar o sistema. Assim, a detecção automatizada de ataques de apresentação, especificamente a detecção de vivacidade, tornou-se um componente obrigatório de qualquer sistema de autenticação baseado na tecnologia de biometria facial que não conta com a supervisão de um ser humano na tentativa de autenticação.



A detecção de vivacidade também lida com o medo de que nossos dados biométricos possam ser comprometidos — e de que, ao contrário de uma senha, nossa biometria não pode ser “redefinida”. Os modelos biométricos criptografados são, por natureza, de pouca ou nenhuma utilidade em caso de roubo, e a melhor prática é armazenar esses modelos separadamente de qualquer informação de identificação pessoal (PII). Mas a realidade é que nossos dados biométricos já se encontram facilmente disponíveis. Mesmo que você não

tenha um perfil no Facebook nem publique fotos suas, é bem provável que sua imagem possa ser encontrada na internet. Essa é outra razão pela qual a detecção de vivacidade é fundamental. Ao integrar a detecção de vivacidade ao reconhecimento facial, podemos fazer com que nossa biometria seja inútil para os impostores.



NESTE ARTIGO, INVESTIGAMOS A IMPORTÂNCIA DA DETECÇÃO DE VIVACIDADE NA IMPLANTAÇÃO DA BIOMETRIA FACIAL PARA AUTENTICAÇÃO, INCLUINDO AS PRÁTICAS RECOMENDADAS E OS CASOS DE USO ESPECÍFICOS.



COMO A DETECÇÃO DE VIVACIDADE PERMITE CONFIAR NA AUTENTICAÇÃO POR BIOMETRIA FACIAL

No que diz respeito ao uso da biometria facial para autenticação, precisão e desempenho não são mais uma preocupação. No entanto, a ameaça de falsificação evoluiu de artigos teóricos e experimentos de laboratório para ataques reais, que afetam empresas, clientes e seu dinheiro. Detectar falsificações é essencial para que a correspondência biométrica facial seja confiável.

Embora o reconhecimento facial para autenticação possa responder com precisão à pergunta: “Essa é a pessoa certa?”, não responde à pergunta: “É uma pessoa viva?” Esse é o papel da detecção de vivacidade.

UMA AUTENTICAÇÃO BIOMÉTRICA ABRANGENTE DEVE RESPONDER A DUAS PERGUNTAS:



1. ESSA É A PESSOA CERTA?
(CORRESPONDÊNCIA BIOMÉTRICA)



2. É UMA PESSOA VIVA?
(DETECÇÃO DE VIVACIDADE)



EXPLICANDO A DETECÇÃO DE VIVACIDADE

O reconhecimento facial compara as características mapeadas de um usuário inscrito — como a distância entre os olhos ou o comprimento da linha da mandíbula — com um modelo biométrico para verificar a identidade. Examina a imagem que vê e faz medições. O que ele não faz é distinguir a presença física do usuário de uma impressão de qualidade ou uma representação digital. ***Uma fotografia ou imagem em uma tela funciona tão bem como uma pessoa real!***

Ao usar a biometria facial para autenticação, uma pessoa mal-intencionada pode explorar essa limitação para enganar o sistema, fazendo-o acreditar que está vendo o usuário autorizado. Chamamos isso de ataque de apresentação, e esses ataques se tornaram mais fáceis para os fraudadores graças ao acesso online imediato a fotos de alta definição, imagens de tela, máscaras e vídeos que podem ser usados para falsificar um sistema de reconhecimento facial.

A detecção de vivacidade funciona com um sistema biométrico que mede e analisa características e reações físicas para determinar se a amostra biométrica que está sendo capturada é de uma pessoa viva presente no ponto de captura. A tecnologia não executa nenhuma funcionalidade de correspondência, mas detecta ataques de apresentação. São eles:



ATAQUE COM FOTO OU VÍDEO:

O fraudador obtém acesso a uma foto ou vídeo de um usuário autorizado. Isso pode ser feito facilmente por meio de uma pesquisa simples no Google ou uma visita à conta de uma rede social do indivíduo. O fraudador pode usar a imagem impressa para criar uma máscara 2D.



VÍDEO SINTÉTICO OU DEEPFAKE

O fraudador pega uma foto ou vídeo e, através da edição com um software de animação, cria uma versão realista do indivíduo falando e acenando com a cabeça.



MODELO OU MÁSCARA 3D

O fraudador investe em máscaras tridimensionais ou modelos personalizados que imitam a semelhança física do indivíduo.



ABORDAGENS DA DETECÇÃO DE VIVACIDADE – PASSIVA X ATIVA

Existe uma variedade de abordagens para a detecção de vivacidade. Em um nível superior, a detecção de vivacidade pode ser classificada como ativa ou passiva:

A *detecção de vivacidade ativa* exige que o usuário participe da verificação de vivacidade respondendo a um desafio. Alguns exemplos de sistemas implantados atualmente são:

- Acenar ou virar a cabeça de um lado para o outro
- Piscar
- Seguir um ponto na tela
- Sorrir
- Falar uma série de palavras ou números
- Aproximar a câmera do rosto ou inclinar-se para a câmera
- Gravar um vídeo curto

A *detecção de vivacidade passiva* não requer nenhuma ação do usuário. A detecção de vivacidade ocorre quando o usuário tira uma selfie. Várias técnicas são possíveis para a detecção de vivacidade passiva, desde a análise de uma selfie, uma captura de vídeo até a projeção de várias luzes diferentes sobre o indivíduo. Cada abordagem de detecção de vivacidade passiva tem um impacto diferente na experiência do usuário e nos requisitos de processamento.



PASSIVA OU ATIVA: QUAL É MELHOR?

Para saber qual é o tipo certo de detecção de vivacidade para você, a próxima seção examina a detecção de vivacidade ativa em comparação com a passiva, seguida de uma explicação sobre os diferentes tipos de detecção de vivacidade passiva.

	DETECÇÃO DE VIVACIDADE PASSIVA	DETECÇÃO DE VIVACIDADE ATIVA
EXPERIÊNCIA DO USUÁRIO	Não requer nenhuma ação por parte do usuário, resultando em menor abandono e geralmente menos tempo e esforço.	Exige que os usuários respondam a “desafios” que agregam tempo e esforço ao processo e são pouco práticas para casos de uso com correspondência biométrica facial frequente, como login. As empresas relatam taxas de abandono de até 50% para a detecção de vivacidade ativa.
REQUISITOS DE SOFTWARE	Alguns métodos exigem a instalação prévia de um componente de software no dispositivo, outros não.	Geralmente requer a instalação de um software no dispositivo, que é um problema para casos de uso como a integração remota de novos clientes antes de baixar um aplicativo móvel nativo.
ANÁLISE DE IMAGENS	Varia de acordo com a abordagem. Pode se basear em uma única imagem com processamento em tempo quase real.	Requer análise de vários quadros de vídeo para detectar o movimento solicitado.
REQUISITOS DE LARGURA DE BANDA	Baixos, com base no uso de uma única imagem ou análise. Pode usar a mesma imagem tirada para reconhecimento facial, resultando em zero tráfego incremental para o servidor.	Pode exigir que mais dados sejam trocados entre o dispositivo do usuário e a solução baseada em servidor, o que costuma ser um problema em áreas com baixa velocidade de internet.
VELOCIDADE	A velocidade de execução de uma verificação de vivacidade passiva varia conforme o método.	A detecção de vivacidade ativa sempre exige maior esforço do usuário, resultando em um tempo maior de verificação de vivacidade.
ROBUSTEZ CONTRA FALSIFICAÇÃO	Os métodos passivos são geralmente mais imunes à falsificação, oferecendo “segurança através da obscuridade”, quando o fraudador não tem pistas sobre como burlar a verificação de vivacidade.	Os sistemas ativos fornecem aos fraudadores informações sobre como atacar e burlar a verificação de vivacidade. Quase todos têm técnicas conhecidas para quebrá-la, como o uso de uma máscara 2D simples com os olhos cortados e um software de animação que imita movimentos de cabeça, sorrisos e piscadas.
CONFORMIDADE COMPROVADA COM ISO 30107-3 PADRÃO DE ROBUSTEZ	Duas soluções possuem certificação de conformidade	Duas soluções possuem certificação de conformidade

Sob quase todos os pontos de vista, uma solução passiva com robustez comprovada e mensurável é preferível a uma solução ativa. Por que fornecer pistas aos fraudadores, por que tolerar abandonos e por que forçar o usuário a gastar mais tempo e esforço, quando uma solução passiva oferece segurança e uma experiência amigável ao usuário?



PASSIVA X PASSIVA: QUAL É A DIFERENÇA?

Nem todas as soluções passivas são iguais. Existem quatro variações conhecidas:

- Brilho de várias luzes sobre o indivíduo para criar diferentes exposições e garantir que é um rosto vivo
- Captura de um vídeo curto que detecta micromovimentos
- Exame da mesma imagem de selfie usada para a correspondência facial
- Abordagem assistida por hardware (por exemplo, medição de profundidade)

ABORDAGEM PASSIVA	PRÓS	CONTRAS
VARIEDADE DE LUZES BRILHANTES	• Passiva, porque o usuário não precisa se mover	• O usuário deve segurar o dispositivo com firmeza • O processo leva tempo • A abordagem falha em ambientes externos com luz solar intensa • Os usuários podem se incomodar com o brilho das luzes
CAPTURE DE UM VÍDEO CURTO	• Passiva, porque o usuário não precisa se mover	• O vídeo leva tempo para ser capturado • O vídeo pode exigir download prévio de software para o dispositivo ou o envio de uma grande quantidade de dados para um servidor • A observação passiva depende de microsimuladores e pequenos movimentos, que podem ser difíceis de capturar
EXAME DE UMA ÚNICA IMAGEM DE SELFIE	• Não requer absolutamente nenhum esforço extra • Tamanho mínimo de dados, já que é necessária apenas uma imagem, não um fluxo de vídeo • Maior velocidade de processamento	• Requer um componente no lado do servidor
ABORDAGEM ASSISTIDA POR HARDWARE (POR EXEMPLO, MEDIÇÃO DE PROFUNDIDADE)	• Não requer absolutamente nenhum esforço extra • Tamanho de dados aceitável, já que apenas algumas imagens são necessárias • Velocidade rápida de processamento	• Requer hardware específico e caro no lado do cliente (por exemplo, câmera com infravermelho e/ou sensor de profundidade) • Requer um componente no lado do servidor • Usa mais energia da CPU para processamento

QUAL ABORDAGEM É A MELHOR?

A detecção de vivacidade passiva é claramente preferível à ativa. A abordagem preenche lacunas de segurança na biometria facial sem adicionar atrito ao processo de autenticação, além de não exigir que os usuários sejam instruídos sobre o processo.

Das possíveis abordagens passivas, uma única imagem de selfie é preferível às outras opções. No entanto, em qualquer caso, escolha uma abordagem passiva que também esteja em conformidade com a ISO 30107-3.



CASOS DE USO DE DETECÇÃO DE VIVACIDADE

A detecção de vivacidade facial combinada com a biometria facial fornece uma poderosa prova de identidade e autenticação sempre que um aplicativo precisa verificar a identidade de uma pessoa sem a supervisão de um ser humano no processo de correspondência facial. Os casos de uso são:



INTEGRAÇÃO DIGITAL DE NOVOS CLIENTES E CONTAS

A capacidade de novos clientes se inscreverem em uma conta remotamente por um dispositivo móvel ou computador em vez de se deslocarem até um local físico aumenta muito a oportunidade de as empresas adquirirem clientes. Uma etapa importante é a “prova de identidade”. A prova de identidade é o processo de comprovar a identidade de uma pessoa antes que ela crie uma conta. Isso geralmente exige que a pessoa tire uma foto de um documento de identificação válido, como um passaporte, tire uma selfie e depois envie as duas imagens para um sistema que verifica a validade do documento e faz a correspondência da foto do documento com a selfie. A verificação de vivacidade é fundamental para garantir que a pessoa da selfie é real, e não uma identidade fabricada. Atualmente a prova de identidade é regulamentada por entidades governamentais na maior parte do mundo, conforme necessário para o processo “Conheça seu Cliente” (KYC).

PROTEÇÃO DO CLIENTE DIGITAL

Sempre que um canal digital, como um aplicativo móvel, chatbot ou assistente virtual usa biometria facial para autenticar um usuário, a verificação de vivacidade é fundamental. A detecção de vivacidade passiva é especialmente crítica para remover o atrito na experiência do usuário, para que a autenticação seja rápida, fácil e segura.

AUTENTICAÇÃO MULTIFATOR E “INTENSIFICADA” PARA PAGAMENTOS

É comum que os pagamentos ocorram fora dos locais de varejo, e essa tendência aumentará para facilitar as condições de crédito e para que haja menos atrito no processo de compra. Por sua vez, o risco de fraude aumenta. O reconhecimento facial com detecção de vivacidade passiva é o segundo ou terceiro fator perfeito para transações de pagamento de alto risco, fornecendo suporte para vulnerabilidades que podem ocorrer por meio de falsificação de SMS, troca e falsificação de cartões SIM e outros ataques fraudulentos que comprometem a posse do dispositivo móvel como um fator.

ACESSO SEM CARTÃO

Quiosques de autoatendimento, terminais, caixas eletrônicos e sistemas de entrada geralmente dependem de cartões ou tokens, às vezes combinados com códigos PIN, como meio de acesso aos sistemas. Esses sistemas são facilmente comprometidos pelo roubo de um cartão e pelo conhecimento do código PIN. Um fator adicional é o reconhecimento facial, mas como não há a supervisão de um ser humano, a verificação de vivacidade é fundamental. A detecção de vivacidade passiva fornece uma solução superior, já que o fraudador não faz ideia de que a verificação de vivacidade está acontecendo. E os usuários não precisam mais de tokens ou cartões. Um rosto, uma verificação de vivacidade e, opcionalmente, um PIN são todos os elementos necessários para a autenticação.



QUAL SOLUÇÃO DE DETECÇÃO DE VIVACIDADE É CERTA PARA VOCÊ?

JÁ ABORDAMOS AS DIFERENÇAS ENTRE A DETECÇÃO DE VIVACIDADE FACIAL PASSIVA E ATIVA E OS MOTIVOS PELOS QUAIS A EQUIPE DA ID P&D ACREDITA QUE UMA SOLUÇÃO PASSIVA É SUPERIOR, POR RAZÕES COMO A CAPACIDADE DE OFERECER SEGURANÇA E UMA MELHOR EXPERIÊNCIA DO USUÁRIO. A SEGUIR, APRESENTAMOS UM RESUMO DAS CONSIDERAÇÕES AO AVALIAR AS TECNOLOGIAS:



SIMPLICIDADE

Já abordamos as diferenças entre a detecção de vivacidade facial passiva e ativa e os motivos pelos quais a equipe da ID P&D acredita que uma solução passiva é superior no equilíbrio entre o desempenho e a experiência do usuário. Procure uma solução que ofereça alta segurança sem causar incômodo ao usuário, que leva ao abandono e à perda de clientes.



FATORES AMBIENTAIS

Em geral, a detecção de vivacidade opera nas mesmas condições que as de um sistema de reconhecimento facial. Os algoritmos de detecção de vivacidade atuais suportam condições de iluminação variadas — da luz do dia ao crepúsculo e cenários internos e externos. Funções de controle de qualidade devem ser implementadas para restringir a detecção de vivacidade quando não houver iluminação, ou quando uma imagem estiver muito desfocada. Para acesso de alto risco, as empresas podem pensar em intensificar a segurança, usando outra modalidade biométrica ou fator de autenticação quando as condições de reconhecimento facial ou detecção de vivacidade forem insuficientes.



CROSS CHANNEL COMPATIBILITY

A solução é compatível com todos os dispositivos móveis e aplicativos de desktop — seja no dispositivo, na nuvem ou baseada em servidor?

Quando uma solução for usada por clientes em uma variedade de dispositivos, é importante que a verificação de vivacidade funcione universalmente em todos os canais e independa da marca ou modelo do dispositivo, desde que atenda aos critérios mínimos. A tecnologia deve ser compatível com qualquer dispositivo com câmera HD capaz de tirar uma selfie com resolução mínima de 720 pixels. Como exemplo, o iPhone 5, lançado em 2012, atendeu a esse critério e as câmeras de hoje estão na faixa de megapixels.



FACILIDADE DE INTEGRAÇÃO E IMPLANTAÇÃO

Evite travamentos, optando por uma solução de detecção de vivacidade capaz de se integrar a qualquer solução biométrica facial de terceiros. Conheça também as opções de implantação, que podem variar de baseada apenas na nuvem, on-premises ou nuvem privada. Verifique se as opções de fornecedores atendem aos requisitos de acesso e armazenamento de dados da sua empresa.



TESTES DE TERCEIROS

O **iBeta Quality Assurance** é líder do setor em testes biométricos e o único laboratório de testes biométricos credenciado pelo National Institute of Standards and Technology (NIST) através do National Voluntary Laboratory Accreditation Program (NVLAP). O iBeta fornece testes de Detecção de Ataques de Apresentação (PAD) conduzidos em conformidade com a ISO/IEC 30107-3.

Durante os testes, os sistemas passam por milhares de ataques de apresentação. Uma solução em conformidade (anteriormente chamada de “certificada”) deve detectar 100% dos ataques.

O IDLive passou no teste de conformidade de Detecção de Ataque de apresentação (PAD) de nível 1 e nível 2 do iBeta, com uma pontuação perfecta. ID R&D é o único fornecedor a atingir o Nível 2 usando uma abordagem passiva de captura de imagem única.

Os testes de terceiros são uma consideração importante para a validação de reivindicações de fornecedores, mas não devem substituir os testes internos e o devido empenho.





RESUMO

A tecnologia biométrica facial oferece a capacidade de autenticar os clientes de forma amigável ao usuário e, ao mesmo tempo, reforçar a segurança. Mas mesmo as soluções mais robustas são suscetíveis a ataques de falsificação, com o uso de imagens de alta resolução, vídeos, máscaras e deepfakes. Para superar esses desafios, criou-se um nível de atrito que é um incômodo para os clientes e um impedimento para o sucesso da adoção da biometria.

A detecção de vivacidade passiva preenche lacunas de segurança na biometria facial sem adicionar atrito ao processo de autenticação. A tecnologia funciona rapidamente em segundo plano e não exige que os usuários sejam instruídos sobre o processo.

Reduzir o esforço do cliente é uma alta prioridade para a maioria das empresas. Ao implementar a detecção de vivacidade como parte de um sistema biométrico facial, é importante considerar como a solução afeta a experiência do usuário. Isso causará lentidão para os usuários, provocará confusão ou aumentará as taxas de abandono?

Além da experiência do usuário, há outras considerações, como requisitos de software, impacto na velocidade, complexidade de integração, opções de implantação, robustez da solução — e, naturalmente, seu caso de uso específico.

COM A BIOMETRIA FACIAL SE TORNANDO MAIS COMUM NA AUTENTICAÇÃO DE USUÁRIOS ONLINE E REMOTOS, A DETECÇÃO DE VIVACIDADE ESTÁ EMERGINDO COMO PARTE CRÍTICA DE UMA SOLUÇÃO ABRANGENTE.



Sobre o IDLive™ Face da ID R&D

A ID R&D fornece o IDLive Face, o primeiro produto de detecção de vivacidade facial verdadeiramente passivo do mundo. O IDLive Face funciona com qualquer software de reconhecimento facial de terceiros e não requer nenhuma ação adicional do usuário na etapa de detecção de vivacidade. A tecnologia usa a análise de uma única foto e não requer nenhum software especial para a captura. Também funciona em dispositivos móveis, Web e autônomos.

O IDLive passou no teste de conformidade de Detecção de Ataque de Apresentação (PAD) de nível 1 e nível 2 do iBeta, com pontuação PAD perfeita, além de estar em conformidade com a ISO/IEC 30107-3.

Assista nossa demonstração em www.idrnd.ai.

1441 Broadway, Suite 6019
New York, New York 10018 USA
info@idrnd.net