A Inviabilidade da Selfie Como Autenticação Biométrica Facial: Uma Análise Crítica

OSVALDO JANERI FILHO

Resumo
Este artigo discute a inviabilidade do uso da selfie como uma forma de autenticação biométrica facial, prática que tem sido adotada por várias instituições financeiras e de tecnologia. A análise aborda as limitações técnicas e de segurança da autenticação baseada em selfie, destacando os riscos de fraudes, a falta de normatização e as implicações legais e de privacidade. São apresentados estudos de caso e comparações com outras formas de autenticação biométrica, como reconhecimento facial 3D, que oferecem maior precisão e segurança.

Palavras-chave: Selfie, autenticação biométrica facial, segurança digital, fraude, privacidade, reconhecimento facial.

---

1. Introdução

Nos últimos anos, a tecnologia de autenticação biométrica evoluiu rapidamente, com muitas instituições adotando métodos inovadores para garantir a segurança dos usuários. Uma dessas inovações é o uso de selfies como forma de autenticação biométrica facial. Embora essa prática tenha se popularizado por sua conveniência, ela levanta sérios questionamentos em relação à sua eficácia e segurança.

O presente artigo tem como objetivo analisar criticamente a viabilidade do uso da selfie como ferramenta de autenticação biométrica facial. Serão discutidos os desafios técnicos, as vulnerabilidades a fraudes e as implicações legais associadas a essa prática, além de propor alternativas mais seguras.

---

2. Autenticação Biométrica Facial e a Selfie

A autenticação biométrica facial é um método de segurança que utiliza características faciais únicas para identificar e autenticar um indivíduo. Tradicionalmente, esse processo é realizado por meio de tecnologias avançadas que capturam imagens tridimensionais do rosto. No entanto, muitas instituições têm optado por uma solução simplificada: a selfie.

A selfie é uma representação bidimensional de um rosto tridimensional. Assim como uma escultura 3D comprimida em uma imagem 2D, a selfie não consegue captar a profundidade e os detalhes necessários para uma autenticação biométrica precisa. Essa simplificação abre espaço para fraudes, como ataques de spoofing, e falhas na identificação de mudanças faciais, como envelhecimento ou maquiagem (NEUPANE et al., 2020).

---

3. Limitações Técnicas e Vulnerabilidades da Autenticação por Selfie

3.1 Falhas na Detecção de Alterações Faciais
Uma das principais limitações da selfie como autenticação biométrica é a incapacidade de detectar pequenas mudanças faciais, como envelhecimento, uso de maquiagem ou acessórios como óculos. Essas variações podem comprometer a precisão da autenticação, tornando o sistema suscetível a erros (KIM; TOH, 2021).

3.2 Vulnerabilidade a Fraudes
As selfies são particularmente vulneráveis a fraudes, como ataques de spoofing, onde um fraudador pode usar uma foto de uma pessoa para se passar por ela. Além disso, existem relatos de reutilização de selfies em contratos anteriores ou até mesmo a compra de selfies para fins fraudulentos, o que agrava o problema (Fantástico, 2023).

3.3 Qualidade da Imagem
Outro fator que compromete a autenticidade da selfie é a qualidade da imagem, que pode ser afetada por iluminação inadequada ou dispositivos de baixa qualidade. Essas variáveis influenciam diretamente a eficácia da autenticação, tornando-a menos confiável (Protectimus Solutions, 2023).

---

4. Comparação com Tecnologias Avançadas de Autenticação Biométrica
Tecnologias emergentes, como o reconhecimento facial 3D, apresentam vantagens significativas em relação ao uso de selfies. Sensores infravermelhos e múltiplos pontos de referência permitem que o reconhecimento facial 3D capture detalhes únicos, como contornos e textura da pele, oferecendo maior precisão e segurança (Security News, 2023).

Esses métodos avançados também são mais robustos contra fraudes, pois levam em consideração aspectos tridimensionais do rosto, tornando muito mais difícil para invasores burlarem o sistema. Além disso, a biometria multimodal, que combina várias formas de autenticação (como reconhecimento facial e impressão digital), se apresenta como uma solução ainda mais segura.

---

5. Implicações Legais e de Privacidade
Além das questões técnicas, o uso de selfies para autenticação biométrica levanta preocupações legais e de privacidade. A coleta, armazenamento e uso de dados biométricos são regulados por legislações cada vez mais rigorosas, como a Lei Geral de Proteção de Dados (LGPD) no Brasil. No entanto, a utilização de selfies como uma forma de biometria facial ainda carece de normas de segurança adequadas (International Security Journal, 2023).

Essa falta de regulamentação cria um ambiente propício para abusos e fraudes, comprometendo não apenas a segurança das instituições que adotam a prática, mas também a privacidade dos usuários.

---

6. O Risco de Fraudes em Instituições Financeiras
Um dos setores mais afetados pelas fraudes relacionadas à autenticação por selfie é o financeiro. Em 2022, foram registradas 57.874 queixas de fraudes em empréstimos consignados envolvendo a utilização dessa tecnologia (Fantástico, 2023). Essas fraudes são frequentemente facilitadas por agentes intermediários, que reutilizam selfies ou adquirem kits fraudulentos contendo selfies e documentos pessoais.

Esses exemplos ilustram os riscos significativos associados à adoção imprudente da selfie como autenticação biométrica, especialmente em transações financeiras que exigem um nível mais alto de segurança.

---

7. Conclusão
Embora o uso de selfies como método de autenticação biométrica facial possa parecer conveniente, sua utilização envolve uma série de desafios técnicos e legais. A simplificação de um processo tridimensional em uma imagem bidimensional compromete a precisão da autenticação e expõe os sistemas a fraudes. Além disso, a falta de regulamentação adequada aumenta os riscos de privacidade e segurança.

Diante dessas questões, é fundamental que as instituições revisem suas práticas de autenticação e considerem o uso de tecnologias mais avançadas, como o reconhecimento facial 3D e a biometria multimodal, que oferecem maior segurança e confiabilidade. As selfies, apesar de populares, não devem ser tratadas como uma forma eficaz de autenticação biométrica.

Referências
FANTÁSTICO. Fraudes em contratos bancários de empréstimos consignados. Exibição em 08 abr. 2023. Rede Globo de Televisão.

INTERNATIONAL SECURITY JOURNAL. ISJ Exclusive: The top three biometric trends to be aware of in 2023. Disponível em: https://internationalsecurityjournal.com/top-three-biometric-trends-2023-fingerprints/. Acesso em: 27 jun. 2023.

KIM, S. H.; TOH, K. A. A New Representation Learning for Anomaly Facial Detection. Journal of Image and Vision Computing, p. 1-10, 2021.

NEUPANE, A.; DOYLE, T.; TOH, K. A.; SAXENA, N. Understanding the Security of Discrete Shoulder Surfing Resistant Pin Entry. Transactions on Computer-Human Interaction (TOCHI), p. 1-34, 2020.

PROTECTIMUS SOLUTIONS. Selfie Based Authentication: reliable or not? Disponível em: https://www.protectimus.com/blog/selfie-based-authentication/. Acesso em: 27 jun. 2023.

SECURITY NEWS. Biometric access control trends to look out for in 2023. Disponível em: https://www.sourcesecurity.com/insights/latest-trends-biometrics-access-control-2023.