XXI Escola Regional de Redes de Computadores / VIII Workshop de Segurança (ERRC). doi : 10.5753/errc.2024.4563

Artigo Curto/Short Paper

Aperfeiçoando Sistemas de Controle de Acesso utilizando Reconhecimento Facial

Improving Access Control Systems using Facial Recognition

Pedro Lucas Martins da Silva • pedro.silva@redes.ufsm.br
Universidade Federal de Santa Maria (UFSM)

Tiago Antonio Rizzetti • tiago.rizzetti@ufsm.br
Universidade Federal de Santa Maria (UFSM)

resumo. Este artigo investiga a otimização de sistemas de controle de acesso através da integração da tecnologia de reconhecimento facial, explorando os benefícios da biometria em relação à segurança e à experiência do usuário. Aborda as vulnerabilidades do RFID e as vantagens do reconhecimento facial, impulsionado por avanços em IA e visão computacional. Propõe um sistema híbrido que integra ambas tecnologias e sua avaliação em ambiente simulado, considerando acurácia, velocidade e usabilidade. Ressalta a importância de garantir a segurança, privacidade e mitigação de vieses na aplicação da tecnologia.

abstract. This paper investigates the optimization of access control systems through the integration of facial recognition technology, exploring the benefits of biometrics in relation to security and user experience. Addresses the vulnerabilities of RFID and the advantages of facial recognition, driven by advances in AI and computer vision. It proposes a hybrid system that integrates both technologies and their evaluation in a simulated environment, considering accuracy, speed and usability. It highlights the importance of ensuring security, privacy and mitigating bias in the application of technology.

palavras-chave: Controle de Acesso • Reconhecimento Facial • RFID • ESP32-CAM • Segurança • Visão Computacional
keywords: Access Control • Facial Recognition • RFID • ESP32-CAM • Security • Computer Vision

1 Introdução

A segurança de ambientes sensíveis, como empresas e residências, depende de sistemas de controle de acesso eficientes. Embora a identificação por radiofrequência (RFID) seja amplamente utilizada devido à sua praticidade e baixo custo, suas vulnerabilidades, como clonagem de cartões e falta de verificação biométrica, comprometem sua eficácia em ambientes que exigem alta proteção. A clonagem de RFID é uma ameaça comum, já que os códigos de identificação podem ser capturados e duplicados facilmente, permitindo acesso não autorizado [1].

Por outro lado, o reconhecimento facial surge como uma solução promissora, sendo mais seguro devido à dificuldade de falsificação de características faciais únicas. Além disso, o reconhecimento facial oferece maior conveniência para o usuário, eliminando a necessidade de portar cartões ou memorizar senhas.

Este artigo explora a combinação dessas duas tecnologias, propondo um sistema híbrido que une reconhecimento facial a um sistema de controle de acesso já existente, que utiliza a tecnologia de RFID como principal forma de acesso. Serão abordados os principais desafios e benefícios da implementação dessa solução, focando em questões como acurácia, velocidade e mitigação de vulnerabilidades. Também discutimos as implicações éticas e de privacidade, essenciais para uma aplicação responsável da biometria.

2 Referencial Teórico

Sistemas de controle de acesso são fundamentais para proteger áreas restritas. O RFID, uma tecnologia madura e de baixo custo, tem sido amplamente utilizado, mas seus riscos de segurança, como clonagem de cartões e uso indevido por terceiros, são preocupantes. Estudos indicam que esses sistemas, por si só,não garantem um nível adequado de proteção em ambientes de alta segurança [2].

O reconhecimento facial, por outro lado, explora características faciais únicas, que são difíceis de replicar ou falsificar. Técnicas de reconhecimento têm evoluído rapidamente, especialmente com o uso de redes neurais profundas, que conseguem analisar rostos de forma precisa mesmo em condições adversas, como variações de iluminação e pose [3]. Algoritmos como o Viola-Jones [4] foram pioneiros na detecção facial, mas abordagens mais recentes, como o MTCNN (*Multi-task Cascaded Convolutional Networks*), oferecem maior precisão ao

combinar várias tarefas, como detecção de rostos e marcação de pontos faciais [5].

Além da detecção facial, a extração de características é crucial para o reconhecimento. Métodos clássicos como PCA (*Principal Component Analysis*) e LDA (*Linear Discriminant Analysis*) foram amplamente utilizados para reduzir a dimensionalidade dos dados faciais [6], enquanto abordagens mais modernas, como *FaceNet* [7], extraem vetores de características altamente discriminativos com precisão aprimorada.

No contexto de sistemas de controle de acesso, a escolha de arquitetura de sistema é crítica. Sistemas baseados em microsserviços [8] são cada vez mais populares, permitindo a integração flexível de componentes independentes, como leitura de RFID e processamento de reconhecimento facial. Essa abordagem facilita a manutenção e escalabilidade do sistema, sendo preferível a sistemas monolíticos, que são menos flexíveis em termos de atualizações e escalabilidade.

3 Metodologia Proposta

Para este estudo, utilizou-se uma metodologia mista, combinando análise qualitativa e quantitativa. O projeto se divide em três fases principais:

1. Análise das limitações do RFID e vantagens do reconhecimento facial.
2. Desenvolvimento de um sistema híbrido de controle de acesso.
3. Avaliação do sistema em ambiente simulado, focando em acurácia, velocidade e usabilidade.

Na fase inicial, foi conduzida uma revisão da literatura utilizando bases acadêmicas para identificar vulnerabilidades em sistemas RFID e explorar tecnologias de reconhecimento facial. Observou-se que, embora o RFID seja uma solução prática, sua principal limitação reside na ausência de mecanismos adicionais de verificação de identidade, o que representa uma vulnerabilidade significativa [1]. Em contrapartida, o reconhecimento facial demonstra maior segurança, especialmente quando associado a técnicas *anti-spoofing*, capazes de prevenir falsificações [9]. Dessa forma, a integração dessas tecnologias em um sistema de controle de acesso pode representar uma melhoria substancial em sua funcionalidade.

Na segunda fase, é desenvolvido um protótipo de sistema híbrido utilizando a linguagem *Python* e bibliotecas como *OpenCV* para processamento de imagens e *Face Recognition* para reconhecimento facial. O sistema é projetado com arquitetura modular, permitindo fácil integração entre os componentes de RFID e reconhecimento facial.

Na terceira fase, o sistema será avaliado em um ambiente simulado, onde serão testadas variáveis como diferentes condições de iluminação, obstrução facial e número de usuários. As métricas analisadas incluírão a taxa de verdadeiros e falsos positivos, tempo de resposta do sistema e *feedback* dos usuários quanto à usabilidade.

A implementação do sistema híbrido busca aliar a robustez do reconhecimento facial à praticidade do RFID, oferecendo uma solução eficiente para controle de acesso. O reconhecimento facial pode atuar como método principal de autenticação, enquanto o RFID pode ser utilizado como uma alternativa de *backup*. Além disso, em ambientes que demandam maior nível de segurança, é possível implementar uma autenticação de dois fatores, exigindo que o usuário se identifique tanto pelo reconhecimento facial quanto pela apresentação de um cartão RFID.

4 Considerações Finais

Este artigo apresentou a proposta de um sistema híbrido que integra reconhecimento facial para otimizar sistemas de controle de acesso beseados em RFID. A revisão da literatura indicou que o RFID, embora popular, apresenta vulnerabilidades que o tornam inadequado para ambientes de alta segurança. O reconhecimento facial, por sua vez, oferece uma solução mais robusta e conveniente, especialmente com o uso de algoritmos avançados de *deep learning*.

A pesquisa mostrou que o sistema híbrido oferece o melhor de ambos os mundos: maior segurança com o reconhecimento facial e redundância com o RFID. Embora em fase embrionária, testes iniciais em ambiente simulado indicaram resultados promissores em termos de acurácia e usabilidade, mas a continuidade da pesquisa será necessária para validar esses resultados em cenários reais, além de investigar maneiras eficazes de ativar o RFID de forma automatizada ou alternativa, em situações em que o reconhecimento facial não seja possível.

Além disso, questões de privacidade e mitigação de vieses são cruciais para garantir uma aplicação ética do reconhecimento facial. Medidas como criptografia de dados e o uso de *datasets* representativos serão investigadas em fases futuras do projeto, garantindo que a tecnologia seja aplicada de forma responsável.

Referências

1 Khattab, A. *et al.* Rfid security. *Springer Berlin Heidelberg*, Springer, v. 11, p. 27–41, 2017.

2 Dardari, D. *et al.* The future of ultra-wideband localization in RFID. *In*: IEEE. 2016 IEEE International Conference on RFID (RFID). 2016. P. 1–7.

3 Ross, A.; Jain, A. Information fusion in biometrics. *Pattern recognition letters*, Elsevier, v. 24, n. 13, p. 2115–2125, 2003.

4 Viola, P.; Jones, M. Rapid object detection using a boosted cascade of simple features. *In*: IEEE. PROCEEDINGS of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001. 2001. v. 1, p. i–i.

5 Zhang, K. *et al.* Joint face detection and alignment using multitask cascaded convolutional networks. *IEEE signal processing letters*, IEEE, v. 23, n. 10, p. 1499–1503, 2016.

6 Belhumeur, P. N.; Hespanha, J. P.; Kriegman, D. J. Eigenfaces vs. fisherfaces: Recognition using class specific linear projection. *IEEE Transactions on pattern analysis and machine intelligence*, IEEE, v. 19, n. 7, p. 711–720, 1997.

7 Schroff, F.; Kalenichenko, D.; Philbin, J. Facenet: A unified embedding for face recognition and clustering. *In*: PROCEEDINGS of the IEEE conference on computer vision and pattern recognition. 2015. P. 815–823.

8 Lewis, J.; Fowler, M. Microservices" martinfowler. com. *Available: martinfowler. com/articles/microservices. html.[Accessed: 7-Apr-2017]*, 2014.

9 Erdogmus, N.; Marcel, S. Spoofing in 2d face recognition with 3d masks and anti-spoofing with kinect. *In*: IEEE. 2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS). 2013. P. 1–6.