

RECONHECIMENTO FACIAL PARA CONTROLE DE ACESSO EM AMBIENTES FECHADOS

Caio César Sabino Soares, Rudimar Luis Scaranto Dazzi
Ciência da Computação - Sistemas de Computação

Apresenta-se uma investigação aplicada sobre reconhecimento facial para controle de acesso em ambientes fechados, motivada pela necessidade de autenticação sem contato que reduza fraudes e falhas operacionais associadas a cartões e senhas, ao mesmo tempo em que automatize o registro de presença. Formula-se como problema de pesquisa a identificação, seleção e validação de técnicas capazes de operar com precisão em condições operacionais típicas (variações de iluminação, ângulo e distância), bem como a comprovação de viabilidade de uma solução integrada em cenário realista. O estudo inicia-se com uma revisão sistemática da literatura que mapeia abordagens de visão computacional e inteligência artificial, sintetizando tendências e lacunas e orientando as escolhas técnicas do protótipo. A metodologia, de natureza aplicada, abordagem quantitativa e método hipotético-dedutivo, compreende:

(i) revisão e síntese de evidências; (ii) projeto e implementação de um sistema funcional; e (iii) experimentação controlada em laboratório. O protótipo integra detectores faciais baseados em redes neurais (MTCNN e RetinaFace) a um extrator de características do tipo FaceNet, implementado em Python e exposto via API e interface web com Flask sob Unicorn, com persistência em nuvem por meio do Firebase e armazenamento de imagens no Google Cloud Storage. O pipeline de pré-processamento opera no espaço YCrCb, aplicando equalização adaptativa de histograma, filtragem bilateral e aguçamento, com parâmetros ajustados dinamicamente conforme o nível de zoom para mitigar perda de detalhes; a classificação baseia-se em embeddings e medida de similaridade cosseno com limiares configuráveis. Para reduzir latência e reprocessamentos, incorporam-se cache local de embeddings, rastreamento de faces e políticas de intervalos mínimos de extração, além de registro detalhado de eventos e tentativas de autenticação para auditoria. A validação ocorre no Laboratório de Inteligência Aplicada (LIA) da Universidade do Vale do Itajaí (UNIVALI), utilizando câmera local e câmera IP, com posicionamento fixo (distância aproximada de 3 m e altura de 1,80 m) e exigência temporal mínima de foco do usuário (cerca de 2 s) para detecção e confirmação; avalia-se o comportamento em fluxo contínuo e em reconhecimento manual pontual, bem como a responsividade da interface e a estabilidade do streaming. Os resultados preliminares indicam que, em condições controladas de iluminação e ângulo, a solução cumpre sua função com tempo de resposta adequado e registro de presença auditável, enquanto degradações são observadas em baixa luminosidade, ângulos pronunciados e passagem acelerada, parcialmente mitigáveis por ajuste de limiares e intensificação do pré-processamento. Identificam-se ainda limitações como ausência de detecção de saída e de mecanismos anti-spoofing, além de oportunidades de refatoração modular do código e reforço das camadas de segurança de dados. Conclui-se que a proposta é viável para ambientes fechados sob condições controladas, contribuindo com a demonstração de um fluxo completo de detecção, extração de características e autenticação facial, e delineando um roteiro de aprimoramentos envolvendo robustez a cenários adversos, incorporação de anti-spoofing, otimizações de inferência e validações ampliadas.

Palavras-chave: Visão Computacional; Reconhecimento Facial; Controle de Acesso.

Apoio: Pró-Reitoria de Pesquisa, Pós-Graduação, Extensão e Inovação da Universidade do Vale do Itajaí - Univali