RBMC
REVISTA BRASILEIRA MILITAR DE CIÊNCIAS

Revista Brasileira Militar de Ciências, v. 10, n. 24, e175, 2024
ISSN 2447-9071 | DOI: https://doi.org/10.36414/rbmc.v10i24.175

Recebido: 01/07/2024 | Aceito: 05/08/2024 | Publicado: 18/08/2024

Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto

Facial recognition-based access control and remote monitoring system

Rodrigo Pinto Lemos[1]

Carlos Henrique Azevedo[2]

Marcelo Rodrigues dos Passos Júnior[3]

Jonas Augusto Kunzler[4]

Resumo

Este artigo descreve o desenvolvimento de um sistema de controle de acesso por reconhecimento facial com monitoramento remoto, projetado para modernizar e simplificar a segurança em diversas organizações. O sistema utiliza os kits de desenvolvimento ESP32Cam para capturar e processar imagens faciais em tempo real, ESP32 WROOM como atuador do sistema, uma tela TFT de 1.8in e um fecho eletromagnético que permite o acesso com base nos resultados da autenticação ou restringindo usuários. O monitoramento remoto permite que os administradores supervisionem e gerenciem o acesso de forma eficiente à distância. Durante o processo de desenvolvimento, vários desafios foram enfrentados, incluindo questões logísticas na aquisição de materiais, dificuldades técnicas no gerenciamento de versões de software e instabilidades nas conexões de hardware. Cada obstáculo exigiu soluções específicas e uma abordagem detalhada para garantir o funcionamento correto do sistema. Por exemplo, assegurar a compatibilidade entre os componentes exigiu uma pesquisa minuciosa, enquanto a espera por entregas de fornecedores internacionais causou atrasos. O gerenciamento de versões de software envolveu a resolução de conflitos e a garantia de que todas as bibliotecas estivessem atualizadas. Problemas de hardware, como conexões instáveis, foram resolvidos melhorando as técnicas de soldagem e utilizando conectores melhores. Apesar desses desafios, o protótipo resultante é um sistema funcional e confiável que integra tecnologias avançadas com uma interface gráfica intuitiva. A experiência destacou a importância de um planejamento cuidadoso, paciência e atenção aos detalhes no desenvolvimento de sistemas tecnológicos complexos. Além disso, o projeto forneceu insights valiosos sobre processos de desenvolvimento iterativos, ressaltando a necessidade de ajustes e melhorias contínuas. Portanto, o sistema desenvolvido oferece uma solução robusta e econômica para a gestão de acessos. Com aprimoramentos contínuos, ele tem potencial para ampla adoção, contribuindo para a melhoria dos protocolos de segurança em diversos ambientes organizacionais.

Palavras Chave: Controle de Acesso; Inteligência Artificial; Internet das Coisas; Reconhecimento Facial; Segurança da Informação.

[1] Doutor em Engenharia Elétrica, Professor Titular na Universidade Federal de Goiás (UFG).
[2] Graduado em Gestão da Tecnologia da Informação pela Faculdade da Polícia Militar (FPM).
[3] Graduando em Gestão da Tecnologia da Informação pela Faculdade da Polícia Militar (FPM).
[4] Doutor em Engenharia Elétrica e da Computação, Professor da Faculdade da Polícia Militar (FPM) e pesquisador e técnico em telecomunicações na Universidade Federal de Goiás (UFG).

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Abstract

This article describes the development of a facial recognition access control system with remote monitoring capabilities, designed to modernize and simplify security for various organizations. The system employs, among other items, mainly an ESP32Cam module, a TFT display, and an electromagnetic lock which allows capturing and processing facial images in real time, granting or denying access based on authentication results. Remote monitoring allows administrators to oversee and manage access efficiently from a distance. During the development process, several challenges were encountered, including logistical issues in sourcing materials, technical difficulties with software version management, and hardware connection instabilities. Each obstacle required specific solutions and a detailed approach to ensure the system's proper functionality. For instance, ensuring compatibility among components demanded thorough research, while waiting for deliveries from international suppliers caused delays. Managing software versions involved resolving conflicts and ensuring all libraries were up to date, which was critical for system stability. Hardware issues, such as unreliable connections, were addressed by improving soldering techniques and using higher quality connectors. Despite these challenges, the resulting prototype is a functional and reliable system that integrates advanced technologies with an intuitive graphical interface. It demonstrates significant potential for practical applications in enhancing security and efficiency in access management. The experience underscored the importance of careful planning, patience, and attention to detail in developing complex technological systems. Moreover, the project provided valuable insights into iterative development processes, highlighting the need for continuous adjustments and improvements. In conclusion, the developed system offers a robust and cost-effective solution for secure access management. With ongoing enhancements, it holds promise for widespread adoption, contributing to improved security protocols in various organizational settings.

Keywords: Access Control; Artificial Intelligence; Cybersecurity; Facial Recognition; Internet of Things.

INTRODUÇÃO

Nos últimos anos, a tecnologia de reconhecimento facial tem emergido como uma ferramenta poderosa para proporcionar segurança e eficiência em diversas áreas, desde o controle de acesso em edifícios corporativos até a gestão de identidades em ambientes públicos. Com o avanço das técnicas de visão computacional e o aumento da capacidade de processamento, sistemas de controle de acesso baseados em biometria facial têm se tornado cada vez mais viáveis e precisos[1]. Este artigo apresenta um sistema de controle de acesso baseado em reconhecimento facial, complementado por uma funcionalidade de monitoramento remoto, proporcionando uma solução robusta e eficaz para a proteção de espaços físicos.

Neste contexto, destaca-se o conceito de Inteligência Artificial da Internet das Coisas (AIoT - do inglês *Artificial Intelligence of Things*), que combina inteligência artificial (IA) com a internet das coisas (IoT - do inglês *Internet of Things*)[2]. Esta integração visa criar sistemas mais inteligentes e autônomos, que não apenas coletam e transmitem dados, mas também analisam e agem sobre esses dados de forma inteligente, melhorando a eficiência, funcionalidade e confiabilidade dos sistemas[1,2].

A aplicação da IA a dispositivos IoT é ampla e diversificada, abrangendo automação residencial, cidades inteligentes, saúde, agricultura inteligente e a indústria 4.0. Por exemplo, em uma casa inteligente, dispositivos IoT como termostatos, câmeras de segurança e sistemas de

iluminação podem utilizar algoritmos de IA para aprender os hábitos dos moradores e otimizar automaticamente as configurações de conforto e economia de energia. Na manufatura, sistemas equipados com AIoT podem prever falhas em equipamentos antes que elas ocorram, permitindo manutenção preventiva e reduzindo o tempo de inatividade[3,4].

A tecnologia de reconhecimento facial oferece uma camada adicional de segurança em comparação com métodos tradicionais de autenticação. As técnicas de visão computacional permitem o desenvolvimento de sistemas adaptáveis e robustos, capazes de se ajustar às necessidades específicas de cada ambiente. Essa abordagem não apenas fortalece a segurança do controle de acesso, mas também contribui para a conformidade com regulamentações de privacidade de dados e padrões de segurança, garantindo uma gestão de acesso responsável e transparente, conforme requerido pela Lei Geral de Proteção de Dados (LGPD)[5-7].

O restante do artigo está organizado nas seguintes seções: Métodos, Resultados e Discussão. Na seção de Métodos, detalhamos a escolha dos componentes de hardware e software utilizados no sistema, incluindo a configuração da plataforma ESP32Cam, a utilização dos algoritmos de reconhecimento facial utilizando bibliotecas especializadas e a implementação da funcionalidade de monitoramento remoto. Em Resultados e Discussão, apresentamos o protótipo desenvolvido e as funcionalidades do sistema de reconhecimento facial, além disso, a interface de usuário desenvolvida para sistemas de propósito geral é apresentada. Além disso, exploramos possíveis melhorias e futuras direções de pesquisa, visando aprimorar ainda mais a robustez e a aplicabilidade do sistema de controle de acesso com reconhecimento facial e monitoramento remoto.

MÉTODOS

Para o desenvolvimento deste trabalho de pesquisa, adotou-se uma abordagem prática e experimental, combinando simulações computacionais, implementação de hardware e desenvolvimento de software.

A primeira etapa compreendeu a revisão bibliográfica e o levantamento de requisitos, nela foram investigadas as principais tecnologias e técnicas disponíveis para reconhecimento facial[1,5-9], bibliotecas para reaproveitamento de código[10-12] e a fundamentação teórica para o trabalho[1-9]. Na sequência, passou-se para a etapa de Design e Desenvolvimento do produto, além da aplicação de Testes e Implementação final. A gestão do projeto foi realizada através da plataforma Notion seguindo as diretrizes da Engenharia de Software[13,14], a qual pode ser encontrada na página de gerenciamento do projeto[15]. Durante a etapa de design e desenvolvimento pode-se destacar duas subdivisões principais:

- Projeto de Hardware: Seleção e integração dos componentes eletrônicos, incluindo câmeras, microcontroladores, e sensores. Além dos componentes que proporcionam a implementação do processamento digital e alimentação do sistema, foi feito um levantamento dos materiais necessários para constituir a base do protótipo, um mostruário para simulacro de porta, tiras de madeira para fazer o portal, dentre outros.

- Projeto de Software: Reaproveitamento e desenvolvimento de algoritmos de reconhecimento facial e processamento de imagem com uso de inteligência artificial. Nesta fase, utilizou-se ferramentas como Python, OpenCV e bibliotecas de *deep learning* como TensorFlow. Foi também desenvolvido um *layout* para a página de cadastro dos usuários credenciados no sistema.

A etapa de Implementação e Testes compreendeu a integração do sistema e a realização de testes em condições controladas para verificar a precisão do reconhecimento facial e a robustez do sistema. Futuramente, e finalizando o primeiro ciclo de desenvolvimento do produto, propõe-se a manutenção e evolução do sistema, onde se pretende instalá-lo e validá-lo em campo e em um ambiente real, como, por exemplo, em uma sala restrita dentro da Faculdade da Polícia Militar e da Universidade Federal de Goiás.

Arquitetura do sistema

O sistema proposto está baseado em uma arquitetura distribuída, composta por duas plataformas distintas, mas que podem ser integradas: um protótipo com sistema embarcado utilizando ESP32, que será apresentado nesta seção, e um programa de computador em Python para *desktop*/*notebooks*, que será discutido na próxima seção.

O protótipo é constituído pelos módulos de (1) captura e processamento de imagens, (2) atuadores e sensores e (3) armazenamento de dados. Cada módulo desempenha um papel crucial para garantir o funcionamento eficiente e seguro do sistema de controle de acesso por reconhecimento facial.

O módulo de captura será responsável pela aquisição das imagens dos usuários, retorno em tela TFT de 1.8in, criação de servidor e comunicação com cliente HTTP. A câmera presente no sistema é a OV2640 de 2MP e vem com conector embutido na plataforma ESP32Cam que possui conexão direta ao um microcontrolador com CPU Xtensa® Dual-Core 32-bit LX6 (240MHz de clock máximo), memória ROM de 448KBytes, memória RAM de 520Kbytes[10,16].

A memória flash do ESP32Cam atua como um banco de dados embutido, armazenando vetores de características faciais (*face IDs*) e informações associadas a indivíduos cadastrados.

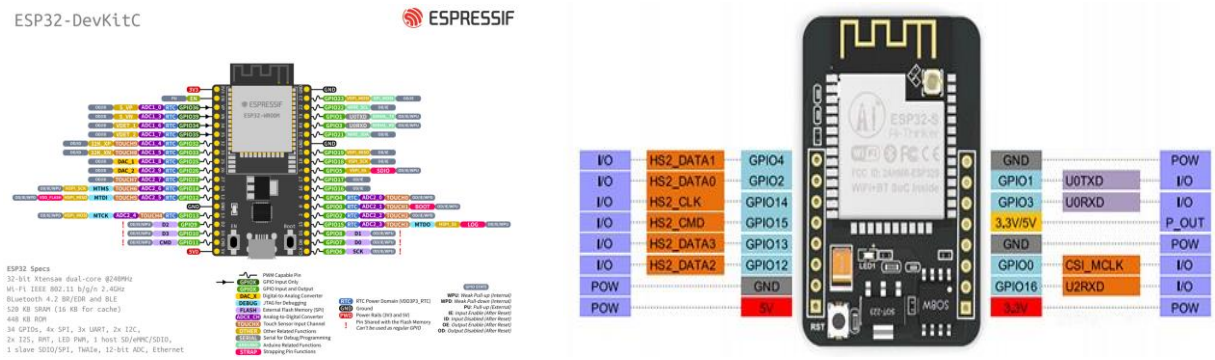
Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Esse armazenamento local permite o acesso rápido e eficiente aos dados durante o processo de reconhecimento, eliminando a necessidade de comunicação constante com um servidor externo. A comunicação com clientes remotos é realizada via *Websockets*, permitindo o controle e monitoramento do sistema em tempo real, enquanto a interface HTTP facilita o acesso e gerenciamento das configurações do sistema[11]. Essa arquitetura integrada e autossuficiente torna o sistema adequado para aplicações de controle de acesso e segurança, oferecendo uma solução prática e de baixo custo.

O módulo de câmera comanda um outro dispositivo microcontrolado, um ESP32 WROOM, com as mesmas especificações de processamento e memória descritos anteriormente, porém, possui 25 GPIOs disponíveis para programação em contraste aos 10 GPIOs do ESP32Cam e não possui câmera. Ele é um microcontrolador versátil e poderoso, ideal para aplicações de IoT e AIoT devido às suas capacidades de processamento, conectividade Wi-Fi e Bluetooth integradas e suporte para bibliotecas de *machine learning*. No âmbito deste sistema, ele controla os sensores e atuadores, como por exemplo, o sensor magnético, o *buzzer*, o fecho eletromagnético e recebe o sinal de abertura da porta.

A figura 1 apresenta os diagramas tanto da plataforma de desenvolvimento (a) ESP32 WROOM quanto a (b) ESP32Cam e seus respectivos pinos de conexão. Além da numeração dos pinos, é possível observar as demais funcionalidades presentes e como cada pino pode se comportar a partir do planejamento do projetista.

Figura 1. Representação gráfica das plataformas de desenvolvimento criadas pela ESPRESSIF.



(a) Pinagem do ESP32 WROOM (b) Pinagem do ESP32Cam

O atuador ESP32 incorpora um sensor magnético para monitorar o estado da porta, proporcionando uma camada adicional de segurança e controle. O sensor magnético é posicionado de forma a detectar quando a porta está aberta ou fechada. Quando o sensor indica que a porta está aberta, um *buzzer* é acionado, emitindo um alerta sonoro para notificar os usuários sobre o estado da porta. Essa funcionalidade é crucial para garantir que a porta não permaneça

inadvertidamente aberta após a autenticação e acesso concedido pelo sistema de reconhecimento facial. A integração do sensor magnético e do *buzzer* não só aumenta a segurança do ambiente, mas também melhora a usabilidade do sistema, fornecendo feedback imediato e claro aos usuários.

Desenvolvimento de software para computador pessoal

Paralelamente ao protótipo com ESP32Cam, foi desenvolvido um programa em Python que executa funções de reconhecimento facial em um ambiente *desktop*. Inicialmente, foi realizada uma análise dos requisitos do sistema, com o objetivo de definir as funcionalidades principais e o fluxo de operação do programa. Foi decidido utilizar a biblioteca face_recognition devido à sua precisão e facilidade de uso, juntamente com OpenCV para captura de imagens em tempo real a partir da *webcam*, e MySQL para armazenamento dos dados de reconhecimento facial.

A configuração do ambiente de desenvolvimento envolveu a instalação das bibliotecas necessárias, como face_recognition, opencv-python e mysql-connector-python. Para isolar as dependências e garantir a reprodutibilidade do projeto, foi utilizado um ambiente virtual Python. Essa etapa foi crucial para preparar a infraestrutura necessária para o desenvolvimento e execução do programa.

A combinação de tecnologias como face_recognition, OpenCV e tkinter, juntamente com o uso de um banco de dados MySQL, proporciona uma base sólida para o desenvolvimento e a expansão futura do sistema

RESULTADOS E DISCUSSÃO

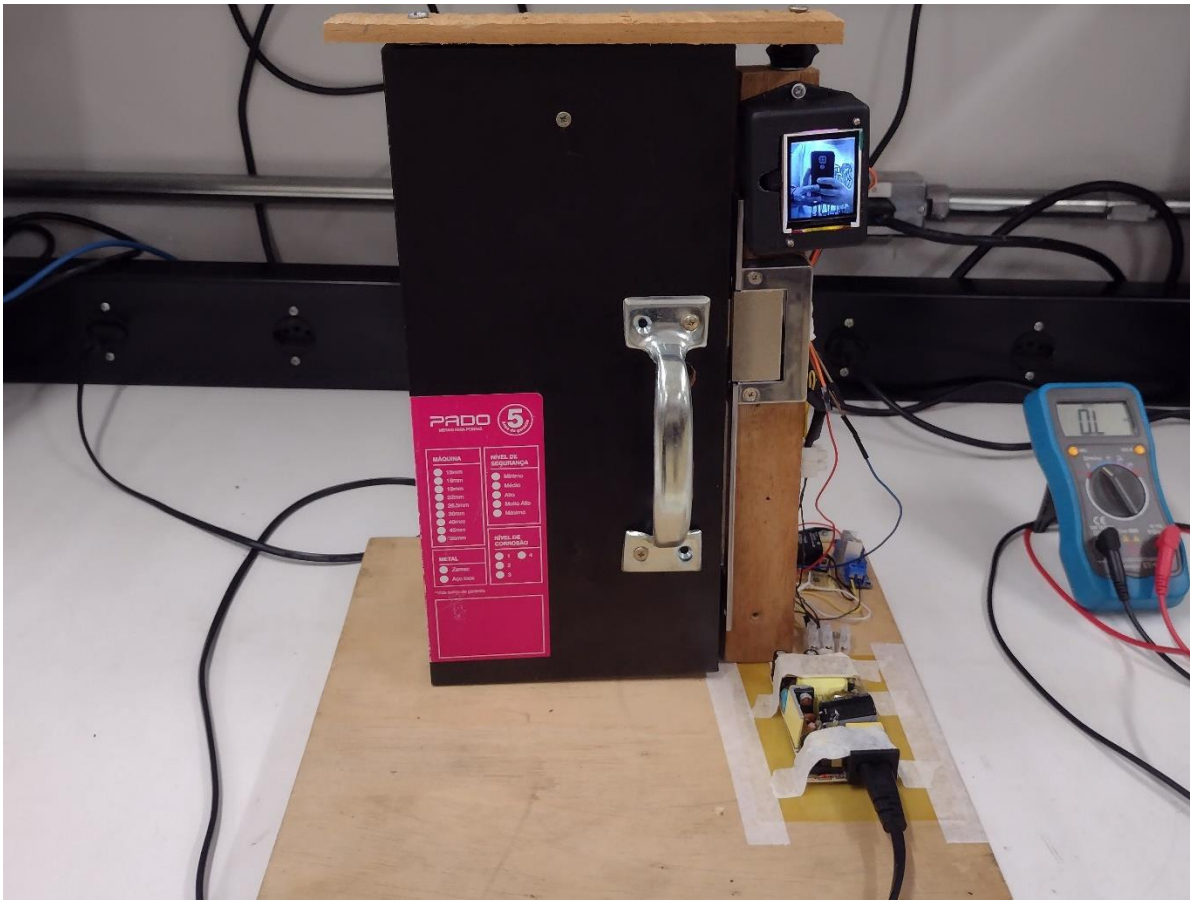
Os resultados obtidos durante o desenvolvimento e implementação do sistema de controle de acesso por biometria facial foram bastante promissores, demonstrando a eficácia da abordagem adotada. A seguir, são apresentados os principais resultados alcançados em cada etapa do projeto.

Dispositivo autônomo com lógica embarcada

Foi desenvolvido um protótipo de dispositivo capaz de reconhecer faces cadastradas previamente que tem potencial de ser instalado em ambientes de uso real. A figura 2 apresenta o protótipo montado e em execução em laboratório.

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Figura 2. Protótipo do sistema de controle de acesso por reconhecimento facial com um simulacro de porta.



Fonte: Elaborada pelos autores.

Alimentação DC e acionamento dos dispositivos

Uma fonte de tensão contínua de 12V, capaz de fornecer 2A e entrada bivolt (110/220 V_{AC}), foi selecionada para o acionamento do fecho eletromagnético e para alimentação dos demais componentes ativos, que é alcançada pela conversão de tensão de 12V para 5V através do dispositivo DC-DC *Step Down* LM317[17].

O fecho eletromagnético é um componente essencial em sistemas de controle de acesso e requer uma fonte de alimentação estável para operar eficientemente. Quando um usuário autorizado é identificado pelo sistema de reconhecimento facial, a fonte de 12V é utilizada para energizar o fecho eletromagnético, liberando a porta e permitindo o acesso. A confiabilidade e estabilidade da fonte de 12V são essenciais para garantir que o fecho eletromagnético funcione corretamente, sem falhas que poderiam comprometer a segurança do sistema.

Além do acionamento do fecho eletromagnético, muitos dos componentes eletrônicos utilizados no sistema de reconhecimento facial, como o ESP32Cam, o ESP32 WROOM, sensores e atuadores, operam a uma tensão mais baixa, tipicamente de 5V ou 3V3. Portanto, é necessário

converter a tensão de 12V fornecida pela fonte principal para 5V e utilizar a conversão de 5V para 3V3 alcançada pelo circuito regulador de tensão presente no próprio kit de desenvolvimento.

Materiais e orçamento

Para a implementação do sistema foi necessário adquirir diversos componentes de hardware. A escolha de apresentar os custos em dólares visa facilitar a comparação global, dado que esta é uma moeda amplamente utilizada e aceita internacionalmente.

Os custos apresentados são estimativas baseadas em preços médios de mercado e podem variar conforme o fornecedor e a localização geográfica. A apresentação dos custos em dólares americanos facilita a comparação e análise por parte de leitores e pesquisadores de diferentes países, proporcionando uma visão clara dos investimentos necessários para a construção de um sistema de controle de acesso por reconhecimento facial com monitoramento remoto.

A tabela 1 apresenta a lista detalhada desses materiais, juntamente com seus respectivos custos em dólares americanos (USD).

Tabela 1. Lista de Materiais e Custos.

Tabela de Especificação e Custos				
Item	Quantidade	Componente	Preço (US$)	
1	1	ESP32 ESP-WROOM-32	14.69	
2	1	ESP32Cam	14.09	
3	1	Sensor Magnético Mc-38	3.79	
4	1	Mini porta com maçaneta	4	
5	1	Relé 12V	0.32	
6	1	Fecho Elétrico 12V	15.13	
7	1	Fonte de Alimentação 12V 2A	11.69	
8	1	DC-DC Step Down LM317	3.76	
9	1	Caixa de Proteção	0.95	
10	1	Tela LCD TFT 1.8in	14.84	
	10	-	82.94	Total

Fonte: Elaborada pelos autores.

O custo total para a implementação do sistema é de US$82.94, o que pode ser considerado baixo para um sistema de controle de acesso com reconhecimento facial. Vários fatores contribuem para essa característica de baixo custo:

1) Componentes de baixo custo, alta funcionalidade: a escolha de componentes como o ESP32Cam, que oferece capacidades avançadas de processamento e conectividade a um preço acessível.

2) Eficiência energética: a utilização de um relé de 12V e um fecho elétrico eficiente garante que o sistema não só é econômico em termos de custo inicial, mas também em termos de operação contínua.

3) Simplicidade na montagem: a utilização de componentes amplamente disponíveis e de fácil integração reduz o tempo e os custos de desenvolvimento e montagem

Esta acessibilidade não compromete a funcionalidade e a eficiência do sistema, tornando-o uma solução viável e prática para ambientes que necessitam de controle de acesso seguro e eficiente. A escolha cuidadosa de componentes de baixo custo e alta funcionalidade reforça a característica de custo acessível para todos os consumidores do sistema, permitindo uma implementação econômica sem sacrificar a qualidade e a segurança.

Desafios de implementação do protótipo

O desenvolvimento do protótipo do sistema de controle de acesso por reconhecimento facial com monitoramento remoto enfrentou uma série de desafios e dificuldades, tanto técnicos quanto logísticos. Um dos primeiros obstáculos foi a busca e aquisição dos materiais necessários. A seleção de componentes específicos, como o ESP32Cam e o fecho elétrico 12V, exigiu uma pesquisa detalhada para garantir que todos os elementos fossem compatíveis entre si e atendessem aos requisitos do projeto. Além disso, a espera pela entrega das encomendas, especialmente de fornecedores internacionais, atrasou o cronograma de desenvolvimento. Os prazos de entrega variaram significativamente, com alguns componentes levando semanas para chegar, o que impactou diretamente a continuidade do projeto.

Outro desafio significativo foi o versionamento de pacotes e bibliotecas utilizadas na IDE do Arduíno durante o desenvolvimento do software para programar os microcontroladores do protótipo. A plataforma ESP32 e suas bibliotecas de suporte são frequentemente atualizadas, e garantir que todas as bibliotecas estivessem na versão correta foi um desafio adicional para evitar incompatibilidades. Durante o desenvolvimento, surgiram conflitos de versão que resultaram em erros de compilação e execução, demandando tempo para diagnosticar e resolver. O gerenciamento dessas dependências exigiu um cuidado meticuloso, frequentemente envolvendo a reconfiguração do ambiente de desenvolvimento e a atualização de firmware.

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Além dos problemas de software, as dificuldades de hardware também foram prevalentes. Conexões físicas instáveis entre os componentes, como fios e conectores, frequentemente causaram mau contato, resultando em falhas intermitentes do sistema. Essas falhas eram particularmente desafiadoras de diagnosticar, pois nem sempre eram evidentes imediatamente e podiam se manifestar como problemas esporádicos. Foi necessário implementar soluções de soldagem e utilizar conectores de melhor qualidade para garantir a integridade das conexões. Além disso, a montagem do protótipo em um espaço compacto, como a caixa de proteção, criou desafios adicionais relacionados à organização e ao gerenciamento de cabos, exigindo um planejamento cuidadoso para evitar interferências e garantir uma operação confiável do sistema.

Programa de computador pessoal

Foi desenvolvido também um programa com interface de usuário para cadastro e reconhecimento facial em sistemas de propósito geral, como *desktops* e *notebooks*. A implementação do código foi organizada em três componentes principais: gerenciamento do banco de dados, lógica de reconhecimento facial e interface gráfica.

O componente de gerenciamento do banco de dados foi responsável por todas as operações relacionadas ao banco de dados MySQL, incluindo conexão, inserção e recuperação de dados. A função de conexão estabelece a comunicação com o banco de dados, enquanto a função de inserção adiciona novos registros de rostos, armazenando o nome e o vetor de características faciais (*encoding*) de cada pessoa. A função de seleção recupera todos os registros armazenados, permitindo a comparação durante o processo de reconhecimento.

A lógica de reconhecimento facial foi implementada utilizando a biblioteca face_recognition para detecção e reconhecimento de rostos, e OpenCV para captura de imagens. A função principal de reconhecimento facial converte as imagens capturadas para o espaço de cores apropriado e extrai as características faciais. Para cadastrar um novo rosto, o programa captura uma imagem da *webcam*, processa para detectar o rosto e armazena as características faciais no banco de dados. Na etapa de identificação, o sistema captura uma imagem em tempo real, processa para extrair as características faciais e compara com os registros armazenados no banco de dados para identificar a pessoa.

A interface gráfica foi desenvolvida utilizando tkinter, proporcionando uma interação amigável e intuitiva para o usuário. A interface permite ao usuário cadastrar novos rostos, digitando o nome e o e-mail, e capturando a imagem através da *webcam*. Além disso, a interface incluem opções para verificar se um rosto está cadastrado no sistema. Os botões e campos de entrada são organizados de maneira clara e acessível, facilitando o uso do sistema mesmo para usuários sem experiência técnica.

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Funções

A função face_recognition recebe um quadro de vídeo como entrada, converte-o para o formato de cor necessário, detecta rostos dentro do quadro, calcula suas codificações de características e retorna essas codificações. Essas codificações são representações numéricas dos rostos detectados, que podem ser usadas para tarefas de reconhecimento facial, como correspondência, verificação e identificação. A função cadastrar realiza as seguintes tarefas:

(a) Verifica se uma imagem foi capturada.
(b) Processa a imagem para obter a codificação facial.
(c) Se um rosto for detectado, salva a codificação facial no banco de dados junto com o nome e e-mail fornecidos pelo usuário.
(d) Exibe mensagens de sucesso ou erro conforme apropriado.
(e) Limpa os campos de entrada após um cadastro bem-sucedido.

Essa função cadastra novos usuários no sistema, associando suas codificações faciais com suas informações pessoais para futuras verificações e identificações. A função capturar realiza as seguintes tarefas:

(a) Inicializa a captura de vídeo usando a câmera padrão.
(b) Captura e exibe continuamente os quadros da câmera até que a tecla "q" seja pressionada.
(c) Atualiza a variável global captured_frame com o quadro capturado atual.
(d) Libera a câmera e fecha todas as janelas do OpenCV quando a captura é interrompida.
(e) Processa a imagem capturada para detectar rostos.
(f) Exibe uma mensagem de erro se nenhum rosto for encontrado, ou uma mensagem de sucesso se um rosto for detectado.

Essa função captura imagens em tempo real da câmera e processa-as para detecção facial, permitindo que o sistema registre novos rostos e forneça *feedback* imediato ao usuário sobre o sucesso ou falha da captura.

Interface gráfica

O planejamento também incluiu a criação de uma interface gráfica intuitiva, desenvolvida com tkinter, permitindo que novos usuários sejam cadastrados e novos rostos sejam associados a identidades únicas permitindo a realização de verificação das identidades de maneira eficaz.

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

A figura 3 mostra o design final da tela de cadastro para novos usuários do sistema a partir de dispositivos de propósito geral como *desktops* e *notebooks*.

Figura 3. Tela da interface de usuário para cadastro de usuários em *desktop*/*notebook*.

Fonte: Elaborada pelos autores.

A interface permite ao usuário cadastrar novos rostos, digitando o nome e o e-mail, e capturando a imagem através da *webcam*. Além disso, a interface incluem opções para verificar se um rosto está cadastrado no sistema. Os botões e campos de entrada são organizados de maneira clara e acessível, facilitando o uso do sistema mesmo para usuários sem experiência técnica

Vantagens do Python

A linguagem de programação Python foi escolhida para a construção do programa de computador pelas características já consagradas de possuir uma sintaxe clara e simples, facilitando a implementação e manutenção do código, a vasta coleção de bibliotecas, como TensorFlow, Keras e PyTorch, proporciona ferramentas avançadas para a construção de modelos de IA, além de uma comunidade ativa e ampla que contribui constantemente com melhorias e novas ferramentas.

Desafios enfrentados

Uma das principais dificuldades encontradas foi a gestão de versões de Python e das bibliotecas utilizadas. Com a constante evolução do ecossistema Python, novas versões do

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

intérprete e das bibliotecas são lançadas frequentemente, introduzindo mudanças que podem quebrar a compatibilidade com o código existente. Isso exige que se mantenha um controle rigoroso sobre as versões utilizadas, optando muitas vezes por fixar o ambiente de desenvolvimento em versões específicas para garantir a estabilidade do sistema.

Outro aspecto problemático foi a compatibilidade entre sistemas operacionais. O código desenvolvido precisava ser funcional em várias plataformas, como Windows, macOS e Linux, cada uma com suas peculiaridades e requisitos específicos. Problemas com a instalação de bibliotecas, diferenças na gestão de dependências e variações na forma como os sistemas operacionais lidam com interfaces gráficas foram obstáculos frequentes.

Por fim, a usabilidade e a experiência do usuário (UX) precisaram ser cuidadosamente planejadas e implementadas. Criar uma interface que fosse ao mesmo tempo funcional e intuitiva, atendendo às necessidades dos usuários finais, exigiu várias iterações de design e testes de usabilidade. Feedback dos usuários é crucial para identificar áreas de melhoria e garantir que o sistema seja fácil de usar e eficaz em seu propósito.

Considerações dos resultados

Os resultados obtidos com a implementação do sistema de controle de acesso por reconhecimento facial foram bastante positivos. A seguir, elencamos os principais pontos:

- **Eficiência e comodidade:** O sistema mostrou-se extremamente eficiente, reduzindo significativamente o tempo de espera para a entrada de usuários. A comodidade proporcionada pela eliminação de chaves físicas é um ponto benéfico para todos os usuários.

- **Precisão e segurança:** Embora o reconhecimento 2D tenha suas limitações, a combinação de algoritmos avançados e constantes atualizações melhorou a precisão do sistema. Entretanto, há necessidade de evoluir para reconhecimento mais eficiente para maior segurança em ambientes de alta criticidade.

- **Aceitação dos usuários:** A interface intuitiva e o design amigável tem o potencial de facilitar a adaptação dos usuários ao novo sistema.

Todos os códigos, documentação e instruções para utilização do projeto estão disponíveis no repositório do GitHub[18].

Lemos RP, Azevedo CH, Passos Júnior MR, Kunzler JA. Sistema de controle de acesso através de reconhecimento facial com monitoramento remoto. Revista Brasileira Militar de Ciências. 2024;10(24):e175.

Trabalhos futuros

A partir dos resultados obtidos e do que foi discutido na seção anterior propõe-se para trabalhos futuros a implementação de algoritmos baseados em reconhecimento 3D, com aquisição de imagens por diferentes ângulos e diferentes intensidades luminosas. Pretende-se ainda estabelecer um banco de dados comum para o sistema embarcado e para o programa de computador, para tanto, deve-se trabalhar na compatibilização dos vetores de características faciais dos usuários. Além disso, o sistema integrado deve ser instalado em sistema de uso real para que seja testado o uso por usuários e sejam apontados pontos de aprimoramentos e evolução.

CONCLUSÃO

Nosso sistema de controle de acesso por reconhecimento facial, desenvolvido com Python e suportado por um design gráfico intuitivo, apresenta um grande potencial para modernizar e simplificar o controle de acesso em diversas organizações. O desenvolvimento do protótipo foi um processo desafiador que envolveu a superação de obstáculos logísticos na aquisição de materiais, dificuldades técnicas no gerenciamento de versões de software e problemas de hardware relacionados a conexões instáveis. Cada um desses desafios exigiu soluções específicas e uma abordagem meticulosa para garantir o funcionamento correto e eficiente do sistema.

A criação deste protótipo não apenas demonstrou a viabilidade técnica e operacional do sistema, mas também proporcionou uma oportunidade valiosa de aprendizado. Enfrentar e resolver esses desafios evidenciou a importância de um planejamento cuidadoso, paciência e atenção aos detalhes na criação de sistemas tecnológicos complexos. Além disso, a experiência reforçou a necessidade de uma abordagem iterativa e adaptativa no desenvolvimento de tecnologia, permitindo ajustes e melhorias contínuas ao longo do processo.

Em suma, o sistema desenvolvido oferece uma solução robusta e eficiente para o controle de acesso, combinando tecnologias avançadas de reconhecimento facial com uma interface de usuário amigável. O protótipo validou a proposta inicial e destacou áreas para futuras melhorias e aprimoramentos. Acreditamos que, com aprimoramentos contínuos, este sistema pode ser amplamente adotado, contribuindo para a segurança e eficiência de diversas organizações

REFERÊNCIAS

1. Parkhi OM, Vedaldi A, Zisserman A. Deep face recognition. BMVC. 2015;1(3):6.

2. Mohammadi M, Al-Fuqaha A, Sorour S, Guizani M. Deep learning for IoT big data and streaming analytics: a survey. IEEE Communications Surveys & Tutorials. 2018;20(4):2923-60.

3. Alam MR, Reaz MBI, Ali MAM. A review of smart homes - past, present, and future. IEEE Transactions on Systems, Man, and Cybernetics: Systems. 2017;42(2):119-33.

4. Lee J, Davari H, Singh J, Pandhare V. Industrial artificial intelligence for industry 4.0-based manufacturing systems. Manufacturing Letters. 2019;18:20-3.

5. Jain AK, Ross A, Nandakumar K. Introduction to biometrics. Boston: Springer, 2011.

6. Campisi P. Security and privacy in biometrics. Boston: Springer Science & Business Media, 2013.

7. Jain AK, Flynn P, Ross A. Handbook of Biometrics. New York: Springer, 2007.

8. Gonzalez RC, Woods RE. Digital image processing. 3. ed. New Jersey: Prentice Hall, 2008.

9. Goodfellow I, Bengio Y, Courville A. Deep learning. Cambridge: MIT Press, 2016.

10. Espressif. Espressif System on Chip ESP32 Series. Disponível em: <https://www.espressif.com/en/products/devkits>. Acesso em: 5 maio 2024.

11. Robot Zero One. Disponível em: <https://robotzero.one/>. Acesso em: 6 jun. 2024.

12. Kristiyana S, Hamzah A, Pasang H, Adhitama V. Smart safe using face detection method ESP32 CAM. Engineering and Technology Journal. 2023;8(12):3212-9.

13. Sommerville I. Software engineering. 9. ed. Boston: Addison-Wesley, 2011.

14. Pressman RS, Maxim BR. Software engineering: a practitioner's approach. 8. ed. Columbus: McGraw-Hill Education, 2014.

15. Notion. Projeto de controle de acesso por biometria facial e técnicas de visão computacional. Disponível em: <https://whimsical-shirt-d6a.notion.site/P-gina-Inicial-TCC-2024-01-4d1727c2a38f46ac89676e31e8778738?pvs=4>. Acesso em: 6 jul. 2024.

16. Espressif, News: ESP32-CAM and other cool projects on RNT. Disponível em: <https://www.espressif.com/en/news/ESP32_CAM> . Acesso em: 6 jul. 2024.

17. Alldatasheet, LM317 Datasheet – STMicroelectronics. Disponível em: <https://www.alldatasheet.com/datasheet-pdf/pdf/22749/STMICROELECTRONICS/LM317.html>. Acesso em: 6 jul. 2024.

18. GitHub. Repositório do projeto de controle de acesso por reconhecimento facial. Disponível em: <https://github.com/jakunzler/access-control-face-recognition>. Acesso em: 6 jul. 2024.

Contato para correspondência:
Jonas Augusto Kunzler

E-mail:
jonas.kunzler@faculdadepm.edu.br

Conflito de interesse: Não

Financiamento: Fundação de Amparo à Pesquisa do estado de Goiás (FAPEG).