

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JOSE BARRETO DOS SANTOS JUNIOR

**DESENVOLVIMENTO DE PROTÓTIPO PARA CONTROLE DE ACESSO
UTILIZANDO RECONHECIMENTO FACIAL COM SBC E OPENCV**

CAMPO MOURÃO

2022

JOSE BARRETO DOS SANTOS JUNIOR

**DESENVOLVIMENTO DE PROTÓTIPO PARA CONTROLE DE ACESSO
UTILIZANDO RECONHECIMENTO FACIAL COM SBC E OPENCV**

**Development of a prototype for access control using facial recognition with
sbc and opencv**

Trabalho de Conclusão de Curso de Graduação
apresentado como requisito para obtenção do título
de Bacharel em Engenharia Eletrônica da Universidade
Tecnológica Federal do Paraná (UTFPR).

Orientador: Eduardo Giometti Bertogna

CAMPO MOURÃO

2022



[4.0 Internacional](https://creativecommons.org/licenses/by/4.0/)

Esta licença permite compartilhamento, remixe, adaptação e criação a partir do trabalho, mesmo para fins comerciais, desde que sejam atribuídos créditos ao(s) autor(es). Conteúdos elaborados por terceiros, citados e referenciados nesta obra não são cobertos pela licença.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Dr. Eduardo Bertonha, pelo apoio e tempo dedicado durante esta trajetória, onde durante a elaboração do trabalho sempre compartilhou conhecimento e experiência.

Aos meus colegas de sala, à minha esposa, e à meus pais, pois sempre confiaram e acreditaram em mim e sem o apoio deles seria mais difícil conseguir superar esse desafio.

RESUMO

O reconhecimento facial é aplicado em diversas tecnologias como desbloqueio de celulares, autenticação de estabelecimentos, meios de pagamento para aplicativos móveis e outros. Para melhorar a confiança em sistemas de segurança, o serviço de reconhecimento facial tem sido cada vez mais utilizado. Diante disso, o presente estudo visa discorrer sobre o desenvolvimento de um protótipo de reconhecimento facial, para controle e autenticação de acesso. Para esse fim, será utilizado um Single Board Computer (SBC), representado por um dispositivo ESP32-CAM, sendo ele responsável por capturar e classificar as imagens em tempo real, por intermédio de algoritmos de detecção facial da biblioteca Open Source Computer Vision Library (OPENCV) e de algoritmos de aprendizado de máquina.

Palavras-chave: reconhecimento facial; controle de acesso; opencv.

ABSTRACT

Facial recognition is applied in various technologies such as cell phone unlocking, establishment authentication, means of payment for mobile applications and others. To improve confidence in security systems, facial recognition service has been increasingly used. Therefore, the present study aims to discuss the development of a facial recognition prototype, for access control and authentication. For this purpose, a Single Board Computer (SBC) will be used, represented by an ESP32-CAM device, which is responsible for capturing and classifying the images in real time, through face detection algorithms from the Open Source Computer Vision Library (OPENVC) and machine learning algorithms.

Keywords: facial recognition; access control; opencv.

LISTA DE FIGURAS

Figura 1 – ESP32-DevKitC.	13
Figura 2 – Fluxograma do Programa	17
Figura 3 – ESP32-CAM	18
Figura 4 – Nextion Intellignet	18
Figura 5 – Fecho Elétrico	18

LISTA DE QUADROS

Quadro 1 – Cronograma de desenvolvimento do trabalho	12
--	----

LISTA DE ABREVIATURAS E SIGLAS

Siglas

SBC	Single Board Computer
OpenCV	Open Source Computer Vision Library
UTFPR	Universidade Tecnológica Federal do Paraná

SUMÁRIO

1	INTRODUÇÃO	10
1.1	Objetivos	10
1.1.1	Objetivo geral	11
1.1.2	Objetivos específicos	11
1.2	Justificativa	11
1.3	Cronograma	12
2	FUNDAMENTAÇÃO TEÓRICA	13
2.1	SBC	13
2.1.1	Arduino IDE	13
2.2	OPENCV	13
2.3	MÉTODO DE RECONHECIMENTO OPENCV	14
2.4	BIOMETRIA FACIAL PARA CONTROLE E ACESSO	14
2.5	TIPOS DE BIOMETRIA	14
2.6	RECONHECIMENTO FACIAL	15
3	METODOLOGIA	17
3.1	Computador de placa única	17
3.2	Interface gráfica	17
3.3	Fechadura eletrônica	18
4	RESULTADOS	19
5	CONCLUSÃO	20
	REFERÊNCIAS	21

1 INTRODUÇÃO

Desde o nascimento o ser humano desenvolve sua capacidade de reconhecer características e essa capacidade atua como um dos principais fatores evolutivos da espécie humana. Sendo as primeiras demonstrações de reconhecimento de características por humanos, dados desde o período pré-histórico.

Biometria (do grego bios vida e metron medida) é a medição de aspectos físicos, biológicos e até comportamentais de seres vivos. Esse reconhecimento visa distinguir o indivíduo de outros no meio em que ele está inserido. A partir daí, é possível permitir ou negar determinada ação ou recurso a essa pessoa.

Dentre as tecnologias atuais de biometria, o reconhecimento facial é uma das mais estudadas atualmente, e, também um dos meios mais seguros de identificação e integridade dos sistemas que a utilizam, em além de oferecer no processo de autenticação, pois é instantâneo, não sendo necessário utilizar equipamentos especiais para identificação uma webcam ou câmera de celular é suficiente para extrair um recurso.

Embora promissora, a biometria enfrenta desafios que devem ser contrabalançados para não levar a interpretações e aplicações equivocadas. Dentre os principais desafios constam: excesso de informação, paradoxo da população, privacidade, intrusividade, ruído, vulnerabilidade e classificação.

Desta forma, observa-se que a biometria deve obstáculos para se tornar um padrão de segurança antifraude. O principal problema da detecção de rosto é determinar se a imagem arbitrária representa um rosto humano ou restaurar as coordenadas do rosto reconhecido.

Como solução, a literatura recente na área propõe técnicas de visão computacional e reconhecimento que, diante do progresso dos sistemas computacionais, permitem corredeiras, levando em consideração a relação de custo entre a velocidade da informação e a limitação de tempo.

Diante disso, o presente estudo visa discorrer sobre o desenvolvimento de um protótipo para o controle de acesso utilizando reconhecimento facial com SBC e OPENVC.

1.1 Objetivos

Neste capítulo serão apresentados os objetivos desse trabalho, estes que são descrever e analisar os métodos utilizados tanto no processamento de imagens, quanto no reconhecimento facial. Utilizando métodos para desenvolver um algoritmo combinando técnicas de processamento de imagens e aprendizado de máquina, buscando o aperfeiçoamento na combinação das técnicas estudadas.

1.1.1 Objetivo geral

Este trabalho tem como objetivo realizar o estudo, implementação e desenvolvimento de um dispositivo para controle de acesso por meio de reconhecimento facial, em um Single Board Computer (SBC), utilizando a biblioteca de visão computacional OpenCV (Open Source Computer Vision Library).

1.1.2 Objetivos específicos

Para que se cumpram os objetivos gerais, são necessárias várias etapas, as quais são apresentadas a seguir:

- Desenvolver o *hardware* para aquisição de imagens, levando em consideração a luminosidade do local e a qualidade da câmera, com o objetivo de obter com uma qualidade razoável para a filtragem e processamento da imagem.
- Implementar um código que seja otimizado e organizado, o suficiente para conseguir filtrar e processar as imagens em tempo real.
- Desenvolver uma interface física, onde os usuários e utilizadores possam interagir e utilizar de forma simples e prática. Permitindo uma boa comunicação, de forma simples e direta.
- Criar um sistema para controle de acesso, onde o usuário administrador irá gerenciar e ser responsável pelo cadastro dos demais utilizadores, seja em um ambiente particular (casas e condomínios) corporativo (empresas) ou publico (Escolas e Universidades) permitindo ou restringindo o acesso, conforme julgar necessário.

1.2 Justificativa

Os sistemas de reconhecimento facial foi uma grande solução para a retomada das atividades presenciais após a pandemia do Coronavírus, ajudando empresas a promoverem uma maior segurança física, como também segurança sanitária, evitando contaminações e agilizando os processos. Pois ao invés de um sistema manual, que normalmente geram atrasos, com a aplicação dessa tecnologia, é possível utilizar mais de um aparelho, aumentando a eficiência e rapidez no controle de acesso.

O grande risco do uso de chaves e tags, é que qualquer pessoa pode entrar sem necessariamente estar credenciado para aquele local. Sendo esta a fragilidade de locais que recebem um grande fluxo de pessoas, porém não possuem sistemas para controlar e acompanhar as entradas e saídas.

Um outro ponto importante, é a economia que este tipo de sistema pode gerar. Com o controle de acesso automatizado, locais como condomínios, hotéis ou recepções comerciais, passam a não ter mais necessidade de porteiros em tempo integral, desta forma, reduzindo custos aos que o utilizam.

Com os leitores faciais, além do acesso mais seguro e exclusivo aos usuários credenciados, por exemplo, moradores, proprietários e funcionários, também é possível credenciar usuários de forma temporária, limitando e liberando os acessos, dentro do tempo que for necessário.

1.3 Cronograma

O cronograma abaixo mostra qual será a sequência de pesquisa de desenvolvimento do trabalho. como no exemplo Quadro 1

Quadro 1 – Cronograma de desenvolvimento do trabalho

Etapa	2022					2023					
	Ag	Se	Ou	No	De	Ja	Fe	Ma	Ab	Ma	Ju
Definição do tema	X										
Definição do escopo do trabalho	X										
Análise de viabilidade e planejamento da execução	X										
Revisão Bibliográfica		X	X	X							
Pesquisa sobre Esp32 e OpenCV		X	X								
Estudo da plataforma Nextion Editor				X	X						
Desenvolvimento do protótipo					X	X	X				
Aplicação do reconhecimento facial						X	X				
Análise dos resultados							X	X			
Correção de erros e aprimoramentos								X	X	X	
Escrita do trabalho	X	X	X	X	X	X	X	X	X	X	X
Apresentação do trabalho											X

Fonte: Autoria própria (2022)

2 FUNDAMENTAÇÃO TEÓRICA

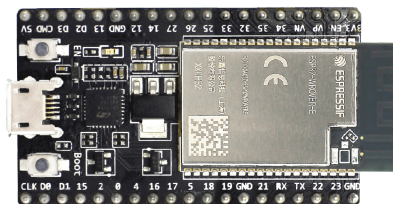
Neste capítulo são apresentados alguns dos conceitos importantes para o entendimento do trabalho. Sendo abordados assuntos como visão computacional, aprendizado de máquinas, biometria e reconhecimento facial.

2.1 SBC

O computador de placa única é um computador onde todos os componentes necessários para sua operação estão localizados em uma única placa de circuito impresso. Esses computadores são geralmente utilizados em sistemas de alarme, sistemas de medição, entre outros.

Quando se trata de computadores de placa única, uma opção com ótimo custo benefício é o ESP32. Não é o modelo mais potente, nem o mais compacto, ainda assim, possui muitos utilizadores devido sua simplicidade, poder de processamento e baixo consumo de corrente.

Figura 1 – ESP32-DevKitC.



Fonte: Adaptado de Espressif Systems (2022a).

A versão para este projeto será o ESP32-CAM, onde além de possuir um chip ESP32 integrado, há também a câmera, entrada para cartão SD e LED de alto brilho.

2.1.1 Arduino IDE

Uma forma para programar o ESP32 é utilizando o Arduino IDE. Um software de código aberto, junto com um utilitário baseado em Python, também de código aberto, chamado Esptool, que se comunica com o bootloader em chips Espressif ESP8266 e ESP32.

2.2 OPENCV

OpenCV é uma biblioteca de programação de código aberto originalmente da Intel com o objetivo de tornar a visão computacional mais acessível a desenvolvedores e amadores. Atualmente possui mais de 500 funções, pode estar em diferentes linguagens de programação e é utilizado para tipos de análise em imagens e vídeos, como detecção, rastreamento e reconhecimento facial, foto e edição de vídeo, detecção e análise de textos. (CEDRO, 2018).

2.3 MÉTODO DE RECONHECIMENTO OPENCV

A primeira etapa do desenvolvimento é determinar qual modelo deve ser utilizado para a detecção. ...

A detecção realmente ocorre usando a função `detectMultiScale`. Porém este método espera como parâmetro a imagem onde deve ser buscada as informações geométricas necessárias para uma boa detecção.

Deve-se tomar cuidado com a iluminação do local, para que não ocorra problemas na detecção. Pois mesmo com algoritmos e métodos sofisticados, ainda assim, perde-se algumas referências de posicionamento, ocasionando resultados com falsos positivos, ou falsos negativos.

2.4 BIOMETRIA FACIAL PARA CONTROLE E ACESSO

A biometria facial é o recurso biométrico mais utilizado por humanos para identificação pessoal. A gama de aplicativos que usam esse recurso varia de aplicativos de reconhecimento facial estático em um ambiente controlado a imagens de fundo complexas de identidade em tempo.

As abordagens mais populares usadas no problema de reconhecimento facial são baseadas na localização e análise de atributos faciais como olhos, nariz e boca, ou em análise global destes, representada como uma combinação de uma série de faces canônicas.

Os sistemas de identificação baseados em biometria são essencialmente sistemas de reconhecimento que, dadas informações biométricas, são capazes de distinguir padrões e classificá-los em diferentes classes ou categorias. (MORAES, 2010).

Ainda de acordo com o autor, algumas das principais características anatômicas, fisiológicas e comportamentais utilizadas em sistemas biométricos incluem impressão digital, impressão da mão, aparência facial, temperatura da face, retina, voz, assinatura, marcha e dental, entre outras.

Atualmente, nenhuma característica biométrica tem todas as propriedades de grau mais alto. Ou seja, não há "melhor característica" para um indivíduo. A escolha depende da aplicação em que será usada.

2.5 TIPOS DE BIOMETRIA

De acordo com Moraes (2010), os principais tipos de biometria são:

Orelhas: Usa a anatomia da orelha para identificar indivíduos, abordagens incomuns. Os pontos fortes são aceitabilidade e permanência; fraquezas, singularidade e desempenho.

Termograma da face e das mãos: O padrão de calor emitido pelo corpo humano é uma

característica de cada pessoa e pode ser captado por infravermelho. Sistemas baseados em imagens termográficas não requerem contato ou cooperação individual. No entanto, a captura de imagem continua sendo um desafio em ambientes não controlados, pois é afetada por fontes de calor que possivelmente podem estar próximas ao indivíduo. Seus pontos fortes são a universalidade, a impostura e a singularidade.

Impressão digital: recurso mais comumente usado em credenciais automatizadas em grande escala. Sua popularidade se deve em parte a dispositivos de coleta de baixo custo e desempenho de processo razoável. Embora a impressão digital não se modifique naturalmente ao longo dos anos, ela é sensível aos fatores ambientais aos quais os indivíduos estão submetidos, o que pode levar à sua alteração e deterioração. Trabalhadores manuais, por exemplo, podem ver suas impressões digitais constantemente alteradas devido a cortes profundos ou outros cortes em seus dedos.

Íris: Formada durante o desenvolvimento fetal, estabiliza-se durante os dois primeiros anos de vida. Sua textura é extremamente complexa e fornece informações a serem utilizadas no reconhecimento facial. Apresenta alta unicidade, sendo distinta mesmo em gêmeos idênticos. Tem um baixo grau de impostura, pois é difícil até cirurgicamente alterar a textura da íris. Seu ponto fraco está em sua capacidade de recuperação, requer equipamentos caros e complexos, bem como cooperação individual.

Voz: Combinação de biometria fisiológica e comportamental. Ele não muda em curtos períodos de tempo, mas é afetado por fatores como um simples frio, estado emocional e ruído de fundo. Possui baixa exclusividade e não é recomendado para identificação em larga escala. O ponto forte é a capacidade de coleta e aceitabilidade, além do baixo custo dos coletores. Geralmente indicado para verificação de identidade em conversas.

2.6 RECONHECIMENTO FACIAL

Desde a infância, o ser humano adquire e desenvolve sua capacidade de reconhecer traços faciais, que é uma particularidade da visão, é o fundamento das relações sociais, atua como um dos principais fatores da evolução da espécie humana. As principais características da face humana foram retratadas relatadas há cerca de 27.000 anos atrás e durante esse período foram retratadas por inúmeros artistas. (ROUHANI, 2019).

Existem estudos sobre automatização do reconhecimento desde os anos 60. Os projetos iniciais nessa área dependiam do administrador encontrar manualmente as características faciais nas imagens, só então o sistema calculava as distâncias entre elas e comparava suas dimensões normalizadas com as referenciadas.

O processo de reconhecimento facial pode ser descrito a partir de uma imagem ou vídeo estático, identificar ou múltiplos indivíduos utilizando um banco de dados de rostos previamente cadastrados. Assim, existem três abordagens conhecidas para reconhecimento:

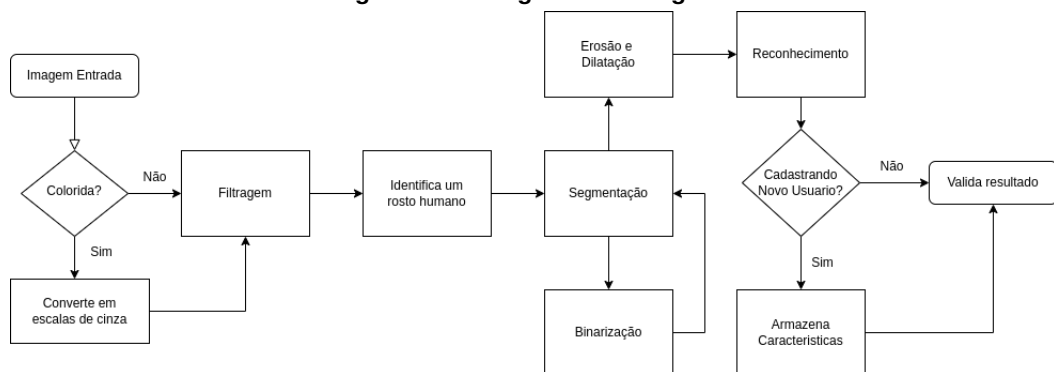
- Imagem a imagem: a amostra e a base de dados composta por imagens estáticas;
- Vídeo para vídeo: a amostra e o banco de dados que consiste em vídeos;
- Imagem para vídeo: o exemplo é um vídeo. O vídeo é comparado a um banco de dados de dados de imagens estáticas. A biblioteca OpenCV possibilita, a partir da versão 2.4, o uso da classe FaceRecognizer para reconhecimento facial. Os algoritmos atualmente disponíveis na biblioteca são: Fisherfaces e Histogramas de Padrões Binários Locais.

3 METODOLOGIA

O trabalho será dividido em três etapas principais: o desenvolvimento do *software*, do *hardware*, e a execução dos testes. Sendo a primeira etapa destinada ao desenvolvimento do algoritmo de reconhecimento facial, utilizando os recursos da biblioteca OpenCV para o processamento de imagens.

O fluxograma da Figura 2 mostra de maneira simplificada e intuitiva como o sistema vai tratar as entradas dos sinais (imagens), até validar os resultados.

Figura 2 – Fluxograma do Programa



Fonte: Autoria própria (2022)

Porém para executar esse algoritmo, será necessário a utilização de um *hardware* capaz de processá-lo, desta forma, a segunda etapa será responsável pela montagem do protótipo. Onde os *hardwares* que serão utilizados, não são muito complexos, sendo compostos por módulos para aquisição dos sinais, processamento e o acionamento referente ao controle de acesso.

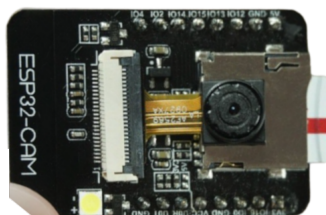
A terceira e última etapa será referente a validação do protótipo, desde testes, ajustes no algoritmo, até melhorias e atualização no hardware. Nessa etapa será analisada a assertividade do código desenvolvido e também a sua viabilidade para utilização no dia-a-dia.

3.1 Computador de placa única

O *hardware* principal do protótipo, será o ESP32-CAM (Figura 3) da Espressif®. Este dispositivo apesar de ser simples e compacto é ideal para este projeto, pois além de possuir uma câmera integrada a sua placa, possui uma capacidade de execução em quase tempo real. Sendo este também, o responsável por processar, analisar e controlar os demais hardwares.

3.2 Interface gráfica

Para uma melhor interação do usuário com o protótipo, será utilizado o *hardware* Nextion Intellignet (Figura 4), display capaz de fornecer uma interface de controle e visualização de

Figura 3 – ESP32-CAM

Fonte: Adaptado de Espressif Systems (2022b).

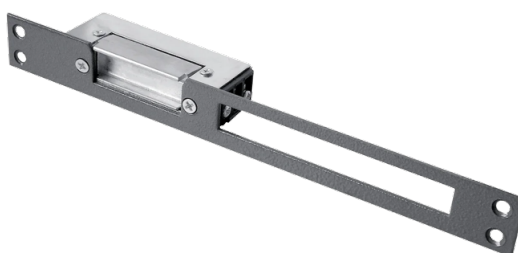
forma simples e rápida. Além desses fatores, essa placa possui um editor visual com inúmeros componentes e recursos, desta forma, facilitando e reduzindo o tempo de programação.

Figura 4 – Nxtion Intellignet

Fonte: Adaptado de Nxtion HMI Solution (2022).

3.3 Fechadura eletrônica

O controle de acesso só será funcional se houver uma fechadura eletrônica integrada ao seu sistema. Desta forma, o protótipo utilizará o Fecho Elétrico (Figura 5) da AGL. Este que é indicado para portas internas, seja de madeira ou metal, sendo acionado por uma tensão em 12v. Desta forma, se o usuário estiver cadastrado e o sistema validar suas credenciais. A trava elétrica será acionada e então seu acesso será liberado.

Figura 5 – Fecho Elétrico

Fonte: Adaptado de AGL Soluções em Segurança Eletrônica (2022).

4 RESULTADOS

Para chegar em um bom resultado será preciso passar por algumas etapas de processamento e considerar alguns fatores naturais. Será preciso utilizar um dispositivo para capturar, processar e armazenar imagens; dessas imagens classificar quais são face, no caso utilizando um algoritmo de detecção de face em tempo real; guardar as informações após a detecção; considerar luminosidade e a umidade no local, pois pode influenciar na qualidade do resultado final; utilizar um algoritmo de aprendizado para classificar e associar determinada face, com um determinada pessoa; E por fim, verificar se a pessoa está cadastrada no banco de dados e se possui acesso ao local desejado.

5 CONCLUSÃO

Diante do exposto, pode-se notar que o avanço da tecnologia em diversos campos tem possibilitado à sociedade moderna oferecer as mais diversas facilidades aos seus indivíduos. Hoje, é possível realizar transações financeiras de casa, realizar reuniões com pessoas que estão a milhares de quilômetros de distância, participar de cursos e conferências ministradas em outro país para viajar de um continente para outro em poucas horas.

No entanto, todas essas conveniências, e um número crescente de quem tira proveito delas, tornou essencial o uso de mecanismos pessoais cada vez mais robustos que podem provar que um indivíduo é quem eles afirmam ser. Esses mecanismos, que são na forma de cartões magnéticos, senhas pessoais, carteiras de identidade, passaportes, entre outros, e, também trazem uma série de problemas associados, como perda, adulteração, empréstimo e dificuldade em ou armazenamento de vários códigos, entre outros.

O processo de identificação pessoal baseado na biometria tenta minimizar esses problemas, pois deixa de ser baseado em algo que o indivíduo possui", ou "algo que o indivíduo passa a considerar o próprio indivíduo como código de identificação.

Assim, o controle de acesso baseado em funcionalidades vem se mostrando uma área extremamente atrativa para explorar e experimentar novas abordagens, visto que possui demanda crescente e extremamente rica em termos de abordagens e técnicas a serem implementadas.

REFERÊNCIAS

AGL SOLUÇÕES EM SEGURANÇA ELETRÔNICA. **fechadura**. 2022. Disponível em: <https://www.aglbrasil.com/fecho>. Acesso em: 05 nov. 2022.

ESPRESSIF SYSTEMS. **devkits**. 2022. Disponível em: <https://www.espressif.com/en/products/devkits>. Acesso em: 04 nov. 2022.

ESPRESSIF SYSTEMS. **esp32cam**. 2022. Disponível em: https://www.espressif.com/en/news/ESP32_CAM. Acesso em: 04 nov. 2022.

NEXTION HMI SOLUTION. **nextion**. 2022. Disponível em: https://wiki.itreadstudio.com/Nextion_HMI_Solution. Acesso em: 02 nov. 2022.