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

RESUMO

A biometria, em sistemas de segurança, tem sido amplamente utilizada devido sua confiabilidade, podendo ser empregada para acessar contas bancárias, autenticação de estabelecimentos, pagamento em dispositivos móveis, controle de acesso, etc. Dentre as biometrias disponíveis, o reconhecimento facial se destaca pela sua praticidade e por ser uma das biometrias mais estudadas e utilizadas. Podendo ser aplicada sem a necessidade de um contato físico. Diante disso, o presente estudo, visa o desenvolvimento de um protótipo de reconhecimento facial para controle e autenticação de acesso. Para essa finalidade, será utilizado um Single Board Computer (SBC), representado pelo dispositivo ESP32-CAM, que será responsável por capturar e classificar as imagens em tempo real. Sendo essas imagens processadas por intermédio de algorítimos de detecção facial da biblioteca Open Source Computer Vision Library (OPENCV) e de algorítimos de aprendizado de máquina.

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

ABSTRACT

Biometrics in security systems has been widely used due to its reliability, and can be used to access bank accounts, authenticate establishments, payment on mobile devices, access control, etc. Among the available biometrics, facial recognition stands out for its practicality and for being one of the most studied and used biometrics. It can be applied without the need for physical contact. That said, The present study aims to present the development of a prototype of facial recognition for access control and authentication. For this purpose, a Single Board Computer (SBC) will be used, represented by the device ESP32-CAM, where he will be responsible for capturing and classifying the images in real time. real. These images being processed through facial detection algorithms Open Source Computer Vision Library (OPENCV) and algorithms of machine learning.

Keywords: facial recognition; access control; opencv.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Desde o nascimento, os seres humanos desenvolvem capacidades de reconhecimento e identificação de objetos, onde essa capacidade foi muito importante durante o processo evolutivo da espécie humana. Sendo as primeiras demonstrações de identificação de seres vivos e objetos, datados no período pré-histórico.

O termo biometria, do grego *bios*-vida e *metron*-medida, pode ser definida como ramo da ciência que estuda a identificação de aspectos físicos, biológicos e até comportamentais dos seres vivos. Na qual, são utilizados para distinguir indivíduos, a partir de suas características únicas (FERREIRA, 2009). Como por exemplo, a face, retina, íris, impressões digitais, geometria da mão, etc.

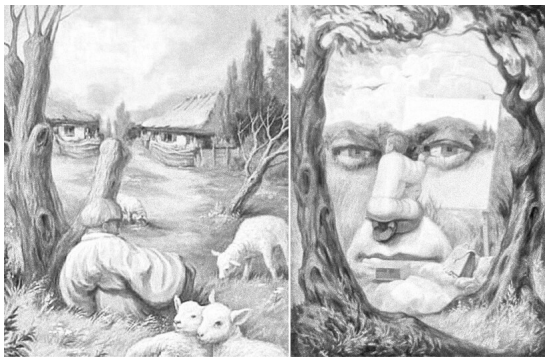
A biometria se tornou uma nova área de estudo a partir do antropologista francês Alphonse Bertillon, em 1890, quando utilizou conceitos de biometria para a identificação de criminosos (MORAES, 2006).

Dentre as tecnologias atuais de segurança, a biometria tem sido amplamente utilizada, seja para acessar contas bancárias, aplicativos e até controlar o acesso a locais públicos e privados. Atualmente o reconhecimento facial é uma das biometrias mais estudadas, pois além da praticidade é considerada uma das formas mais seguras de identificação.

Embora seja promissora, mesmo assim, o sistema de identificação pode falhar durante o processo de reconhecimento, principalmente devido a equívocos e interpretações incorretas do *software*. Esses problemas podem ser causados, desde sujeira na lente da câmera, alta umidade, baixa iluminação, filtros digitais não calibrados, ruídos, excesso de informação, inserção de dados falsos, etc.

Desta forma, para um sistema biométrico obter uma alta assertividade, deve-se validar todos os cenários possíveis e tomar os devidos cuidados durante seu desenvolvimento. Pois, por exemplo, durante o processo de reconhecimento facial, pode-se haver falsos-positivo ou verdadeiros-negativo (Figura 1), ou seja, o *software* pode identificar um rosto humano que não existe, ou não identificar um rosto humano, mesmo existindo.

Figura 1 – Imagens que lembram rostos humanos



Fonte: Adaptado de Pinterest (2022).

Como solução, as literaturas recentes propõem novas técnicas de visão computacional,

reconhecimento e aprendizado de máquina. Em razão disso, a taxa de assertividade vem aumentando, devido ao progresso dos sistemas computacionais e dos novos *hardwares*, sendo possível obter um maior desempenho, com um custo menor.

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

1.1 Objetivos

Nesta seção serão apresentados os objetivos deste trabalho e as etapas necessárias para o desenvolvimento do protótipo. Na qual, além da implementação do *hardware*, também serão necessárias algumas etapas para a elaboração do *software*, tendo como finalidade, obter uma alta assertividade no controle de acesso por reconhecimento facial.

1.1.1 Objetivo geral

Este trabalho tem por objetivo realizar o estudo e desenvolvimento de um protótipo para controle de acesso por meio de reconhecimento facial. Para isso, serão implementados algorítimos de visão computacional e aprendizado de maquina, em um computador de placa única (ESP32-CAM).

1.1.2 Objetivos específicos

Para que se cumpram os objetivos gerais, serão essenciais a realização de algumas etapas, as quais, são apresentadas a seguir:

- Desenvolver o *hardware* para aquisição de imagens, levando em consideração a luminosidade local e a qualidade da câmera. Garantindo assim, bons resultados para a etapa de reconhecimento facial.
- Implementar um código que seja otimizado e organizado, o suficiente para conseguir filtrar e processar as imagens em quase tempo real.
- Desenvolver uma interface física, onde os usuários possam interagir e utilizar de forma simples e prática.
- Por último, criar um sistema para controle de acesso, onde o usuário administrador, poderá gerenciar e cadastrar novos usuários, permitindo ou restringindo o acesso, conforme necessário.

1.2 Justificativa

Os sistemas de reconhecimento facial foram uma grande solução durante 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. Ao contrário dos sistemas manuais, onde normalmente geram atrasos e demandam atenção.

Atualmente o controle de acesso mais comum, são aqueles que utilizam chaves e tags, porém, como possuem inúmeras fragilidades, estes procedimentos não são recomendados em locais que recebem um grande fluxo de pessoas, como por exemplo, hotéis e centros comerciais. Pois, desta forma, qualquer pessoa pode ter acesso, sem necessariamente estar credenciada.

Outro ponto importante é que a implantação de sistemas automatizados, também podem gerar economias. Como por exemplo, em condomínios e hotéis, onde o sistema pode realizar parte do serviço de porteiros e/ou recepcionistas, possibilitando uma redução na carga horária destes trabalhadores e inclusive, resultando na redução de custos para as empresas.

Por fim, a facilidade desses sistemas, fazem com que os usuários não precisem mais memorizar senhas, ou carregar suas chaves, impactando positivamente na experiência de uso. Além disso, esse sistema reduz a probabilidade de golpes ou fraudes, pois impossibilita o compartilhamento do mesmo acesso.

2 FUNDAMENTAÇÃO TEÓRICA

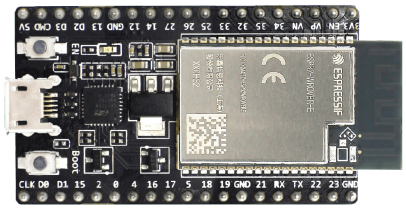
Neste capítulo são apresentados alguns dos conceitos importantes para o entendimento do trabalho. Sendo abordados assuntos como o visão computacional, biometria e reconhecimento facial.

2.1 Computador de Placa Única

Computador de Placa Única ou Single Board Computer (SBC) é um computador onde todos os componentes necessários para sua operação estão localizados em uma única placa de circuito impresso. Esses computadores podem ser utilizados em sistemas simples ou complexos, tendo diversas aplicações, desde sistemas de alarme, sistemas de controle, monitoramento, etc.

Quando se trata de SBC, uma boa opção é o ESP32 (Figura 2). Mesmo não sendo o modelo mais potente, nem o mais compacto, ainda assim, possui um ótimo custo beneficio. Considerando sua simplicidade, poder de processamento e baixo consumo de corrente (ESPRESSIF SYSTEMS, 2022a).

Figura 2 – ESP32-DevKitC.



Fonte: Adaptado de Espressif Systems (2022c).

A versão escolhida para este projeto será o ESP32-CAM, onde além de possuir um chip ESP32 integrado, nele também está incluso uma câmera, uma 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 aplicativo de código aberto, escrito em C e C++, que permite a comunicação e gravação em chips ATmega da família AVR. Entretanto, para gravar em chips ESP32, basta ativar o utilitário Esptool.

Além do ambiente de desenvolvimento, outra vantagem é que o Arduino IDE possui inúmeras bibliotecas e documentação. Facilitando e assegurando o desenvolvimento de novos códigos, pois essas bibliotecas são constantemente testadas e atualizadas pela comunidade da plataforma Arduino.

2.2 OPENCV

OpenCV é uma biblioteca de visão computacional e aprendizado de máquina de código aberto, tendo sido desenvolvida inicialmente pela Intel, com o intuito de fornecer uma infraestrutura comum para aplicativos, acelerar o desenvolvimento dessa tecnologia e tornar a visão computacional mais acessível para desenvolvedores e pesquisadores.

O OpenCV (2022a) é escrito nativamente em C++, mas possui interfaces em Python, Java e MATLAB e suporta plataformas como Windows, Linux, Android e Mac OS. Atualmente a biblioteca possui mais de 2.500 algoritmos otimizados, que inclui algoritmos de visão computacional clássico, de última geração e de aprendizado de máquina. Podendo ser usadas para identificar objetos, detectar e reconhecer rostos, rastrear objetos em movimento, etc.

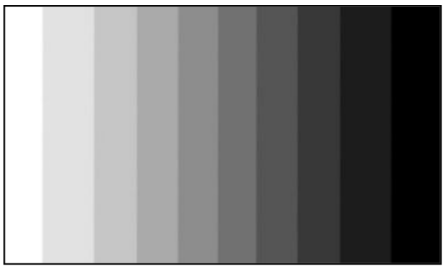
2.3 PROCESSAMENTO DE IMAGENS

As técnicas de processamento de imagens começaram a surgir no final da década de 1960, para serem utilizadas no realce e restauração de imagens capturadas do espaço, como por exemplo, as imagens da missão Apollo. Logo em seguida essa tecnologia começou a ser empregada para processar imagens em diagnósticos médicos, e com o aumento de poder de processamento dos computadores, essas técnicas agora são empregadas nas mais diversas áreas de conhecimento (GONZALEZ, 2010).

Em processamento de imagens um conceito bastante utilizado é a binarização de imagens, que consiste em duas classes distintas, o fundo e o objeto, esse processo serve para de certa forma separar ambas as classes.

Sendo assim, a forma mais simples de processamentos consiste na bipartição do histograma, dando valores iguais a 0 (branco) aos pixels que estiverem abaixo do valor de *threshold* (T), e iguais a 255 (preto) aos pixels que estiverem acima desse valor. A Figura 3 mostra uma escala de tons de cinza, e a Figura 4 mostra essa mesma escala após passar por esse processamento, exemplificando o processo de binarização.

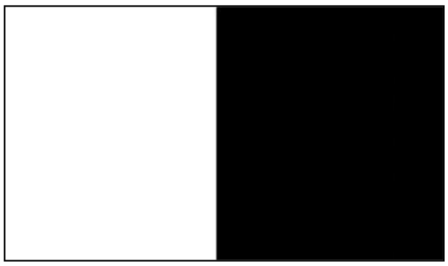
Figura 3 – Escala de cinza



Fonte: Autoria própria (2023)

Especialmente durante o processo de reconhecimento de objetos. A segmentação é uma ferramenta indispensável para fins de análise e interpretação.

Figura 4 – Escala de cinza binarizada



Fonte: Autoria própria (2023)

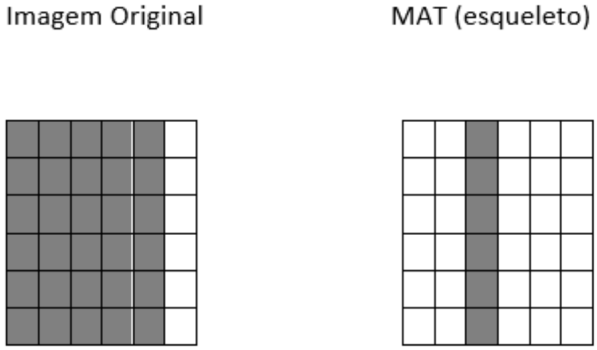
A segmentação de uma imagem é um procedimento importante no que tange essas análises, uma vez que ela subdivide uma imagem em regiões que posteriormente serão ou não tidas como de interesse, o que pode variar muito de acordo com a aplicação (GONZALEZ, 2010).

Os principais algoritmos de segmentação se baseiam nas técnicas de descontinuidade e similaridade, a abordagem de descontinuidade consiste em dividir uma imagem com base nas mudanças bruscas mudanças de intensidade, como ocorre nas bordas. Enquanto na técnica por similaridade a divisão da imagem acontece por regiões que sejam semelhantes de acordo com um conjunto de critérios preestabelecidos (GONZALEZ, 2010).

Por fim, uma outra técnica conhecida como esqueletização, consiste na representação de um conjunto de pontos no interior de um objeto de uma imagem. O esqueleto de uma região pode ser definido pela transformada do eixo médio (MAT) do inglês (*medial axis transformation*). Nessa técnica são selecionados os elementos centrais de um objeto, criando literalmente um esqueleto da imagem. MAT de uma região *R* com uma borda *B* é definida como: para cada ponto *p* contido na região, encontramos seu vizinho mais próximo em *B* (borda), e se houver mais de um vizinho então o ponto pertence ao eixo médio, ou seja ao esqueleto (GONZALEZ, 2010).

O que pode ser visualizado com mais facilidade na Figura 5:

Figura 5 – Processo de esqueletização



Fonte: Autoria própria (2023)

2.4 BIOMETRIA

Com o avanço da tecnologia, hoje é possível realizar transações e pagamentos a partir de qualquer lugar, ou até mesmo, sem sair de casa, apenas com o uso de um dispositivo conectado a internet. Entretanto, também tornaram-se indispensáveis o uso de mecanismos de segurança, principalmente os que são capazes de identificar e comprovar quem realmente está utilizando esses serviços.

Por mais que existam outros processos de identificação, como por exemplo, cartões magnéticos, senhas, tags, etc., atualmente o processo considerado mais seguro é o baseado em biometria.

A biometria pode ser definida como o processo de identificação dos seres vivos. No intuito de distinguir os indivíduos, a partir de suas características únicas. É uma técnica que foi utilizada até mesmo pelos egípcios para o processo de identificação, baseando-se em características da aparência dos indivíduos, como cor dos olhos e cicatrizes (SANTOS, 2007).

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. Tem um baixo grau de impostura, pois é difícil até cirurgi-

camente alterar a textura da íris. Seu ponto fraco está em sua capacidade de recuperação, requer equipamentos caros e complexos, bem como cooperação individual.

- Voz: União de biometria comportamental e fisiológica. 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 e fundamental para relações sociais (ROUHANI, 2019).

Existem estudos sobre automatização do reconhecimento facial 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, identificando um ou múltiplos indivíduos a partir de um banco de dados de rostos previamente cadastrados. Assim, existem três abordagens conhecidas para reconhecimento:

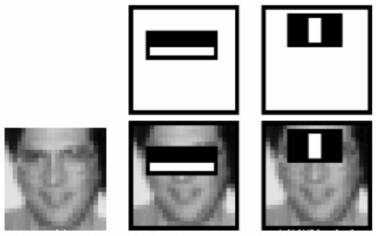
- Imagem a imagem: a amostra e a base de dados composta por imagens estáticas;
- Vídeo para vídeo: a amostra e o banco de dados que consiste em vídeos;
- Imagem para vídeo: o exemplo é um vídeo. O vídeo é comparado a um banco de dados de imagens estáticas. Para esse caso, a biblioteca OpenCV possibilita, 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 (LBP).

Após a imagem ter sido lida e transformada em uma matriz da OpenCV, a mesma é duplicada e redimensionada proporcionalmente para uma altura fixa. A imagem original é mantida para ser utilizada posteriormente. Em seguida a imagem é convertida para escalas de cinza e então equalizada para realçar o contraste e facilitar a detecção de faces.

A seguir, é feita a detecção das faces utilizando o classificador LBP fornecido pela biblioteca OpenCV. Removendo o fundo ao redor da face, pois pode atrapalhar os algoritmos de reconhecimento.

As abordagens mais populares usadas no problema de reconhecimento facial são baseadas na localização e análise de atributos faciais como olhos, nariz e boca (Figura 6), ou em análise global destes.

Figura 6 – Reconhecimento baseado na localização dos olhos e nariz



Fonte: Adaptado de OpenCV (2022b).

E com a comparação das informações extraídas com as informações conhecidas, juntamente com uma pequena análise estatística, pode-se categorizar o objeto e ainda determinar com precisão do que se trata (GONZALEZ, 2010).

2.7 BIOMETRIA FACIAL PARA CONTROLE E ACESSO

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, entre outras.

A biometria facial é o recurso biométrico mais utilizado por humanos para identificação pessoal. Embora usar a face para identificar conhecidos seja uma tarefa trivial para o ser humano, no entanto, é uma tarefa bastante complexa para computadores. Mesmo tendo um desempenho razoável em sistemas comerciais, um sistema biométrico facial impõem algumas restrições no fundo, como iluminação e o ângulo das imagens utilizadas.

Segundo Cavalcanti (2005), alterações estéticas, como cabelo e barba, uso de acessórios, como óculos e bonés, são fatores que aumentam as chances de falha no processo de reconhecimento facial.

Para utilizar a face em sistemas biométricos é preciso seguir três etapas fundamentais. São elas:

- Detecção Facial: Responsável por definir e localizar uma ou mais faces;
- Extração de Características: Esta fase é responsável por remover o excesso de informações que rodeiam as faces detectadas, assim como selecionar as melhores características para serem utilizadas na próxima etapa;

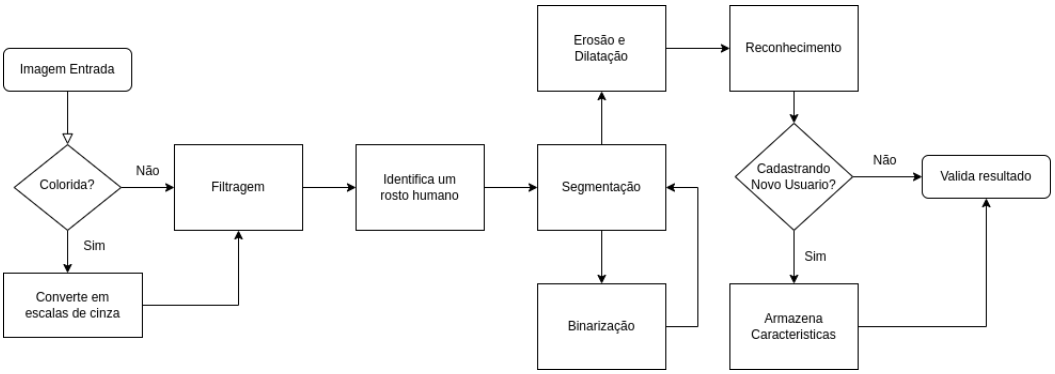
- Reconhecimento Facial: Esta fase compara as características selecionadas pela fase anterior com outras previamente cadastradas em um banco de dados. Sendo responsável por encontrar um registro que se assemelhe ao que precisa ser identificado;

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

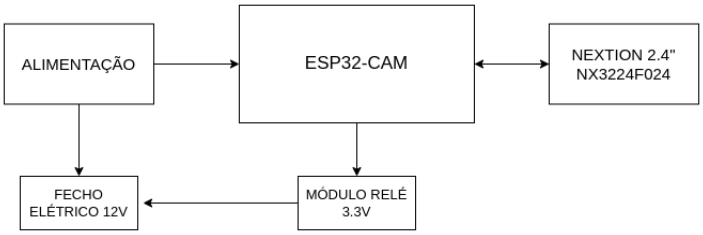
Figura 7 – Fluxograma do *firmware*



Fonte: Autoria própria (2023)

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. No intuito de facilitar a compreensão do seu funcionamento, o diagrama da Figura 8 foi criado. Onde no protótipo serão utilizados módulos para alimentação, aquisição dos sinais e processamento, interface gráfica e por fim, um módulo para acionamento da fechadura.

Figura 8 – Diagrama de blocos do *hardware*



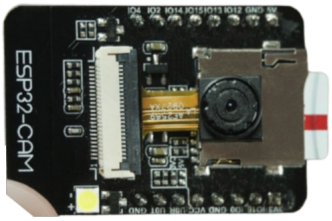
Fonte: Autoria própria (2023)

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 módulo principal do protótipo, será o ESP32-CAM (Figura 9) 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*.

Figura 9 – ESP32-CAM



Fonte: Adaptado de Espressif Systems (2022b).

3.2 Interface gráfica

Para uma melhor interação do usuário com o protótipo, será utilizado o *hardware* Nextion Intellignet (Figura 10), *display* capaz de fornecer uma interface de controle e visualização de 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 10 – Nextion Intellignet

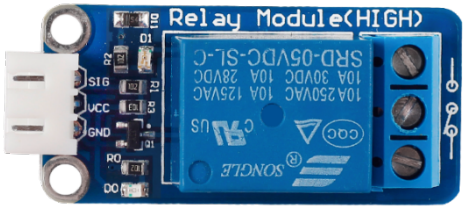
Fonte: Adaptado de Nextion HMI Solution (2022).

3.3 Módulo de acionamento

Os relés são adequados para acionar dispositivos eletrônicos como luzes, ventiladores, ar condicionado, etc. E atualmente são muito utilizados em sistemas de automação residencial e industrial, devido a facilidade em controlar cargas CA de média e alta tensão, a partir de

circuitos CC de baixa tensão. Desta forma, o acionamento do protótipo será feito, por meio de um módulo relé (Figura 11).

Figura 11 – Módulo Relé

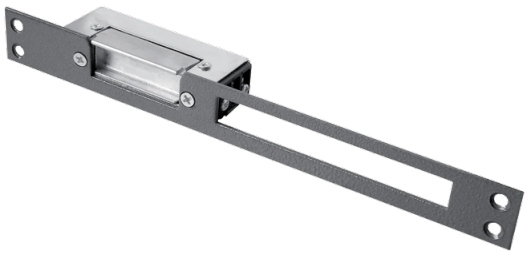


Fonte: Sunfounder (2022)

3.4 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 12) 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 o acesso será liberado.

Figura 12 – Fecho Elétrico



Fonte: AGL Solucoes em Seguranca Eletronica (2022)

4 RESULTADOS ESPERADOS

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 quase 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

Podemos notar que o avanço da tecnologia em diversos campos possibilitou 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 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 e então 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 SOLUCOES EM SEGURANCA ELETRONICA. **Fecho elétrico para aplicação, em portas de madeira ou metal**. 2022. Disponível em: https://www.aglbrasil.com/fecho. Acesso em: 05 nov. 2022.

CAVALCANTI, G. D. da C. **Composição de biometria para sistemas multimodais de verificação de identidade pessoal**. 2005. Dissertação (Mestrado) — Programa de Pós-Graduação em Ciência da Computação - PPGCC, Universidade Federal de Pernambuco, Pernambuco, 2005.

ESPRESSIF SYSTEMS. **ESP32: A feature-rich MCU with integrated Wi-Fi and Bluetooth connectivity for a wide-range of applications**. 2022. Disponível em: https://www.espressif.com/en/products/socs/esp32. Acesso em: 26 nov. 2022.

ESPRESSIF SYSTEMS. **ESP32-CAM and Other Cool Projects on RNT**. 2022. Disponível em: https://www.espressif.com/en/news/ESP32_CAM. Acesso em: 04 nov. 2022.

ESPRESSIF SYSTEMS. **ESP32-S Series**. 2022. Disponível em: https://www.espressif.com/en/products/devkits. Acesso em: 04 nov. 2022.

FERREIRA, A. B. de H. **Dicionário Aurélio Eletrônico**. 5. ed. Curitiba: Positivo, 2009.

GONZALEZ, R. E. W. R. C. **Processamento digital de imagens**. 3. ed. São Paulo: Pearson, 2010.

MORAES, A. F. de. **Método para avaliação da tecnologia biométrica na segurança de aeroportos**. 2006. Dissertação (Mestrado) — Programa de Pós-Graduação em Engenharia de Computação e Sistemas Digitais - PPGECSD, Universidade de São Paulo, São Paulo, 2006.

MORAES, J. L. de. **Controle de acesso baseado em biometria facial**. 2010. Dissertação (Mestrado) — Programa de Pós-Graduação em Informática - PPGI, Universidade Federal do Espírito Santo, Vitória, 2010.

NEXTION HMI SOLUTION. **Nextion HMI Solution**. 2022. Disponível em: https://wiki.iteadstudio.com/Nextion_HMI_Solution. Acesso em: 02 nov. 2022.

OPENCV. **About, Open Source Computer Vision Library**. 2022. Disponível em: https://opencv.org/about. Acesso em: 19 set. 2022.

OPENCV. **Face Detection using Haar Cascades**. 2022. Disponível em: https://docs.opencv.org/3.4/d2/d99/tutorial_js_face_detection.html. Acesso em: 19 set. 2022.

PINTEREST. **Ilusões de ótica do artista ucraniano Shuplyak**. 2022. Disponível em: https://br.pinterest.com/pin/574068283742099558. Acesso em: 14 nov. 2022.

ROUHANI, S. **Reconhecimento de face e de "prova de vida" com Tensorflow para criação de um sistema de segurança voltado a residências e a ambientes de acesso restrito**. 2019. Dissertação (Mestrado) — Programa de Pós-Graduação em Matemática Estatística e Computação Aplicadas à Indústria - PPGMECAI, Universidade de São Paulo, São Paulo, 2019.

SANTOS, A. L. dos. **Gerenciamento de identidades: Segurança da informação**. 1. ed. Rio de Janeiro: Brasport, 2007.

SUNFOUNDER. **Relay(HIGH) for Arduino and Raspberry Pi**. 2022. Disponível em: http://wiki.sunfounder.cc/index.php?title=Relay(HIGH)_for_Arduino_and_Raspberry_Pi. Acesso em: 22 nov. 2022.