

UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

JOSÉ BARRETO DOS SANTOS JUNIOR

**DESENVOLVIMENTO DE PROTÓTIPO PARA CONTROLE DE ACESSO
UTILIZANDO RECONHECIMENTO FACIAL**

CAMPO MOURÃO

2023

JOSÉ BARRETO DOS SANTOS JUNIOR

**DESENVOLVIMENTO DE PROTÓTIPO PARA CONTROLE DE ACESSO
UTILIZANDO RECONHECIMENTO FACIAL**

Development of a prototype for access control using facial recognition

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

2023



[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.

JOSÉ BARRETO DOS SANTOS JUNIOR

**DESENVOLVIMENTO DE PROTÓTIPO PARA CONTROLE DE ACESSO
UTILIZANDO RECONHECIMENTO FACIAL**

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).

Data de aprovação: 24/novembro/2023

Prof. Dr. Marcio Rodrigues da Cunha
Avaliador(a) 1
UTFPR

Prof. Dr. Osmar Tormena Junior
Avaliador(a) 2
UTFPR

Prof. Dr. Eduardo Giometti Bertogna
Orientador(a)
UTFPR

CAMPO MOURÃO
2023

AGRADECIMENTOS

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

Aos meus colegas de sala, à minha esposa, e à meus pais, por sempre confiarem e acreditarem em mim, sem o apoio de vocês seria mais difícil superar este desafio.

RESUMO

A biometria, em sistemas de segurança, tem sido amplamente utilizada devido sua confiabilidade, sendo 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 dispositivo ESP32-CAM, que será responsável por capturar e classificar as imagens em tempo real, sendo essas imagens processadas por intermédio de algoritmos de detecção e reconhecimento facial.

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

ABSTRACT

Biometrics, in security systems, has been widely used due to its reliability, and can be used to access bank accounts, authentication of establishments, payment on mobile devices, access control, etc. Among the biometrics available, facial recognition stands out for its practicality and because it is 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 develop a prototype of facial recognition for access control and authentication. For this purpose, an ESP32-CAM device will be used, which will be responsible for capturing and classify images in real time. These images are processed through of facial detection and recognition algorithms.

Keywords: facial recognition; access control; biometry.

LISTA DE FIGURAS

Figura 1 – ESP32-DevKitC.	14
Figura 2 – Escala de cinza	15
Figura 3 – Escala de cinza binarizada	15
Figura 4 – Processo de esqueletização	16
Figura 5 – Método de Bertillon	17
Figura 6 – Modelo de impressão digital	18
Figura 7 – Reconhecimento baseado na localização dos olhos e nariz	20
Figura 8 – Rostos em diferentes iluminações	20
Figura 9 – Pontos de referência a partir de características faciais	21
Figura 10 – Fluxograma do <i>firmware</i>	22
Figura 11 – Diagrama de blocos do <i>hardware</i>	23
Figura 12 – ESP32-CAM	23
Figura 13 – GPIO disponíveis do ESP32-CAM	24
Figura 14 – <i>Display</i> LCD TFT 1.8"	25
Figura 15 – Módulo Relé	25
Figura 16 – Fecho Elétrico	26
Figura 17 – Diagrama de trabalho do MTNM	27
Figura 18 – Fluxograma do funcionamento do método <i>recognize face</i>	28
Figura 19 – Telas de inicialização	29
Figura 20 – Fluxo de telas do login	29
Figura 21 – Fluxo de telas do cadastro	30
Figura 22 – Fluxo de telas para deletar usuário	30
Figura 23 – Módulo Adaptador ESP32-CAM MB	31
Figura 24 – Diagrama elétrico do protótipo	31
Figura 25 – Diagrama elétrico do ESP32-CAM	32
Figura 26 – Diagrama elétrico do <i>Display</i> TFT	33
Figura 27 – Diagrama elétrico dos botões	33
Figura 28 – Diagrama elétrico do módulo relé	34
Figura 29 – Projeto da placa de circuito impresso do protótipo	34
Figura 30 – Placa manufaturada	35

Figura 31 – Placa montada	35
Figura 32 – Transformações monótonas em escala de cinza	36

LISTA DE QUADROS

Quadro 1 – Portas de Entrada/Saída ESP32-CAM	24
--	----

SUMÁRIO

1	INTRODUÇÃO	11
1.1	Objetivos	12
1.1.1	Objetivo geral	12
1.1.2	Objetivos específicos	12
1.2	Justificativa	12
2	FUNDAMENTAÇÃO TEÓRICA	14
2.1	Microcontrolador	14
2.2	Processamento de imagem	14
2.3	Biometria	16
2.4	História da biometria	17
2.5	Tipos de biometria	18
2.6	Reconhecimento facial	19
2.7	Biometria facial para controle de acesso	20
3	METODOLOGIA	22
3.1	Microcontrolador ESP32-CAM	23
3.1.1	Pinos de Entrada/Saída (E/S)	24
3.2	Interface gráfica	25
3.3	Módulo de acionamento	25
3.4	Desenvolvimento do <i>software</i>	26
3.4.1	PlatformIO	26
3.4.2	Biblioteca ESP-DL	27
3.4.3	Fluxo de telas	29
3.4.4	Gravação do código	30
3.5	Desenvolvimento do protótipo	31
4	RESULTADOS E DISCUSSÃO	36
5	CONCLUSÃO	38
	REFERÊNCIAS	39

1 INTRODUÇÃO

Desde o nascimento, os seres humanos desenvolvem habilidades de reconhecimento e identificação de objetos. Logo na primeira semana de vida, os bebês estabelecem rapidamente reconhecimentos individuais, discriminando e demonstrando preferência pela face, voz e odor de sua própria mãe (VIEIRA; OLIVA, 2017).

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 (ZHAO; CHELLAPPA; PHILLIPS, 2003).

Embora a identificação facial seja uma tarefa simples para os seres humanos, representa um desafio considerável para os computadores. Isso se deve em parte às restrições impostas pelo sistema biométrico facial, que abrangem o controle da iluminação e dos ângulos das imagens utilizadas. Além disso, várias variáveis estéticas, como barba, cabelo, uso de óculos e bonés, problemas na lente da câmera e até mesmo a possibilidade de inserção de dados incorretos, podem ocasionar falhas no processo de reconhecimento (CAVALCANTI, 2005).

Assim, aprimorar a precisão de um sistema biométrico requer atenção durante o desenvolvimento, com foco na minimização de falsos positivos e falsos negativos no reconhecimento facial. Para superar esse desafio, é essencial encontrar uma abordagem que seja mais adequada ao sistema de autenticação por imagem. Entre as várias abordagens disponíveis, é fundamental avaliar a taxa de identificações incorretas e a taxa de casos não detectados (VIOLA; JONES, 2004).

Diante disso, o objetivo deste estudo é abordar o desenvolvimento de um protótipo que visa simplificar o controle de acesso através de um sistema de reconhecimento facial compacto e acessível, tornando-o de fácil utilização para qualquer pessoa. E também permitindo a integração com sistemas já existentes.

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 utilizados algoritmos de processamento de imagens e aprendizagem profunda no microcontrolador ESP32-CAM.

1.1.2 Objetivos específicos

Para que o objetivo geral seja atingido, algumas etapas essenciais deverão ser realizadas:

- 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 processar as imagens em tempo real;
- Criar uma interface gráfica e física que permita aos usuários interagir e utilizar de maneira intuitiva e simples;
- Por último, desenvolver o módulo de controle de acesso, que permitirá ao administrador gerenciar e cadastrar novos usuários, concedendo ou limitando o acesso de acordo com as necessidades.

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 contato físico (TERRA, 2020).

Atualmente, os controles de acesso mais comuns 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, qualquer pessoa pode ter acesso, sem necessariamente estar credenciada.

Um aspecto relevante a ser considerado é que a implementação de sistemas automatizados tem o potencial de reduzir custos. Isso é notável, por exemplo, em condomínios e hotéis, onde tais sistemas podem desempenhar funções que, anteriormente, eram realizadas por porteiros e recepcionistas no cotidiano. Isso não só permite uma diminuição nas horas de trabalho desses profissionais, mas também resulta em economia de despesas para essas 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, essa abordagem reduz significativamente a probabilidade de golpes e fraudes, uma vez que torna inviável o compartilhamento de acessos.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo são apresentados alguns conceitos importantes para o entendimento do trabalho, sendo abordados assuntos como biometria, processamento de imagens, aprendizado profundo e reconhecimento facial.

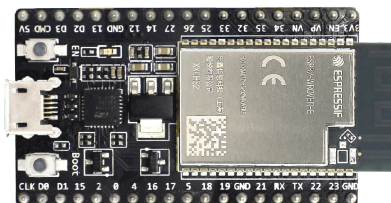
2.1 Microcontrolador

Microcontrolador é um computador em um único *chip* que incorpora: processador, memória, periféricos de entrada e saída, temporizadores e dispositivos de comunicação serial. Eles surgiram como uma evolução natural dos circuitos digitais devido à crescente complexidade. Chegou um ponto em que foi mais prático e econômico substituir a lógica das portas digitais por um conjunto de processador e *software* (PENIDO; TRINDADE, 2013).

O primeiro microcontrolador, o "8048", foi lançado pela Intel em 1977 e evoluiu para a família "8051". Esses *chips* são programados em linguagem *Assembly* e possuem um conjunto de instruções poderoso (PENIDO; TRINDADE, 2013).

Atualmente, quando se trata de microcontrolador, uma boa opção é o ESP32 (Figura 1). Mesmo não sendo o modelo mais potente, nem o mais compacto, ainda assim, possui um ótimo custo-benefício, considerando sua simplicidade, poder de processamento e baixo consumo de corrente (ESPRESSIF SYSTEMS, 2022a).

Figura 1 – ESP32-DevKitC.



Fonte: Adaptado de Espressif Systems (2022c).

2.2 Processamento de imagem

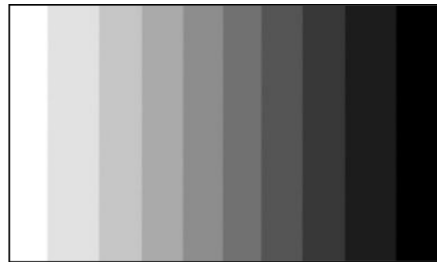
As técnicas de processamento de imagens começaram a surgir no final da década de 1960, para serem utilizadas no realce e restauração de imagens capturadas do espaço, como por exemplo, as imagens da missão Apollo. Logo em seguida, essa tecnologia começou a ser empregada para processar imagens em diagnósticos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

separar ambas as classes.

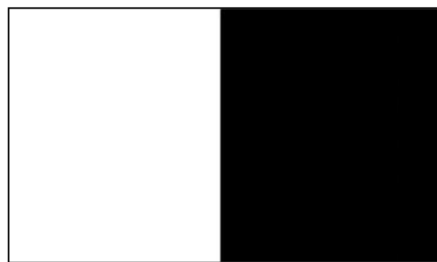
Sendo assim, a forma mais simples de processamento consiste na bipartição do histograma, dando valores iguais a 0 (branco) aos *pixels* que estiverem abaixo do valor de *threshold* (T) e iguais a 255 (preto) aos *pixels* que estiverem acima desse valor. Na Figura 2 é possível observar uma escala de tons de cinza e na Figura 3 verifica-se essa mesma escala pós-processamento, exemplificando o processo de binarização.

Figura 2 – Escala de cinza



Fonte: Autoria própria (2023).

Figura 3 – Escala de cinza binarizada



Fonte: Autoria própria (2023).

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

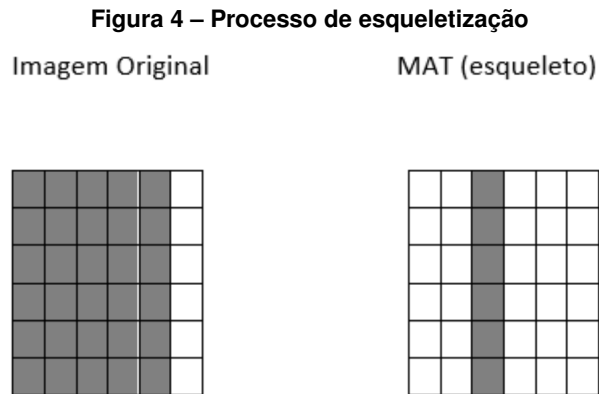
A segmentação de uma imagem é um procedimento importante no que tange essas análises, uma vez que ela subdivide uma imagem em regiões que posteriormente serão ou não tidas como de interesse, o que pode variar muito de acordo com a aplicação (GONZALEZ; WOODS, 2010).

Os principais algoritmos de segmentação de imagem têm suas bases em duas abordagens: descontinuidade e similaridade. A abordagem da descontinuidade envolve a divisão de uma imagem com base em mudanças abruptas de intensidade, como as que ocorrem nas bordas. Por outro lado, a técnica de similaridade segmenta a imagem com base na identificação de regiões que compartilham semelhanças de acordo com critérios predefinidos (GONZALEZ; WOODS, 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; WOODS, 2010).

O que pode ser visualizado com mais facilidade na Figura 4:



Fonte: Autoria própria (2023).

2.3 Biometria

Com o avanço da tecnologia, hoje é possível realizar transações e pagamentos 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 e tem por intuito distinguir os indivíduos por meio 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).

Os sistemas biométricos podem ser divididos em dois grupos distintos: 1) os métodos invasivos, que requerem a colaboração ativa do sujeito para a identificação; e 2) os métodos não invasivos, que podem ser aplicados sem que o indivíduo identificado tenha conhecimento disso. Entre os métodos, incluem-se técnicas amplamente conhecidas, como a biometria da impressão digital, do rosto, da íris, da assinatura, entre outras (TEIXEIRA, 2011)

O foco deste estudo será um método de biometria não invasivo, mais precisamente no processo de identificação e reconhecimento de características faciais, um tema que tem atraído crescente interesse de pesquisadores e cientistas na área de visão computacional.

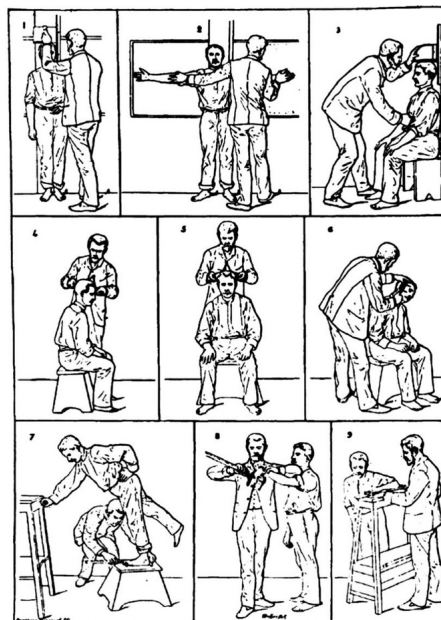
2.4 História da biometria

Contrariando o senso comum, é importante notar que o conceito de biometria não é algo recente, o que realmente se tornou inédito foi a sua aplicação em sistemas computacionais. Na verdade, práticas de identificação com base em características físicas datam de muito tempo atrás. Um exemplo notório é o uso que os faraós do Egito faziam de características como cicatrizes, cor dos olhos, arcada dentária e outros detalhes para distinguir indivíduos (BOECHAT, 2008).

Na Europa, por volta de 1890, o antropologista e delegado policial parisiense Alphonse Bertillon viu na biometria uma maneira de identificar criminosos e a transformou em uma nova área de estudo (MORAES, 2006). Bertillon, com um profundo interesse em pesquisas criminais, começou a medir diversas partes do corpo humano, incluindo o diâmetro transversal da cabeça, comprimento dos pés, dedos, antebraços, estatura, entre outros e, registrou essas medidas em cartões. Embora os resultados obtidos por Bertillon não tenham sido conclusivos, a ideia de relacionar medidas do corpo humano para a identificação continuou a ser usada por autoridades policiais em todo o mundo, sendo conhecida como "Bertillonage" (BOECHAT, 2008).

Na Figura 5, podem ser observadas várias técnicas de medição desenvolvidas por meio do método de Bertillon, abrangendo aferições dos braços, pernas, cabeça e até mesmo das orelhas.

Figura 5 – Método de Bertillon



Fonte: Adaptado de (MORAES, 2006).

Na Suíça, com a introdução da fotografia, essa técnica começou a ser usada de maneira exclusiva nos procedimentos de identificação criminal. Na Índia, um indivíduo chamado William James Hersche, insatisfeito com a falta de cumprimento de contratos por parte dos comerciantes

locais, passou a exigir que as assinaturas fossem acompanhadas pela impressão digital nos documentos (BOECHAT, 2008).

Por fim, nas últimas décadas, novos sistemas biométricos começaram a surgir à medida que novas aplicações biométricas eram desenvolvidas e se tornavam uma realidade comercial.

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, abordagem incomum.
- 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: como pode ser observado na Figura 6, 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.

Figura 6 – Modelo de impressão digital



Fonte: Adaptado de (BOECHAT, 2008).

- 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 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: 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 estáticos.

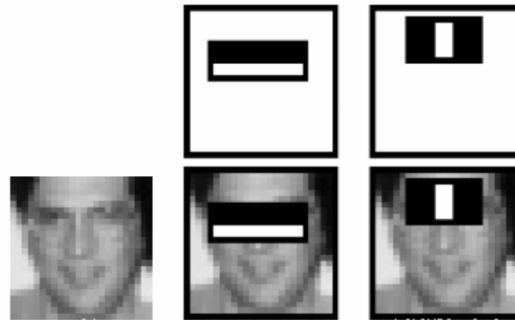
Após a imagem ter sido lida e transformada, a mesma é duplicada e redimensionada proporcionalmente para uma altura fixa. A imagem original é mantida para ser utilizada posteriormente. Em seguida, a imagem é convertida para escalas de cinza e então equalizada para realçar o contraste e facilitar a detecção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

A seguir, é feita a detecção das faces utilizando o classificador de objetos treinados. 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 7), ou em análise global destes.

Ao comparar as informações extraídas com aquelas já conhecidas, complementadas por uma breve análise estatística, é possível categorizar o objeto e determinar com grande precisão sua natureza ou identidade (GONZALEZ; WOODS, 2010).

Figura 7 – Reconhecimento baseado na localização dos olhos e nariz



Fonte: Adaptado de Viola e Jones (2004).

2.7 Biometria facial para controle de acesso

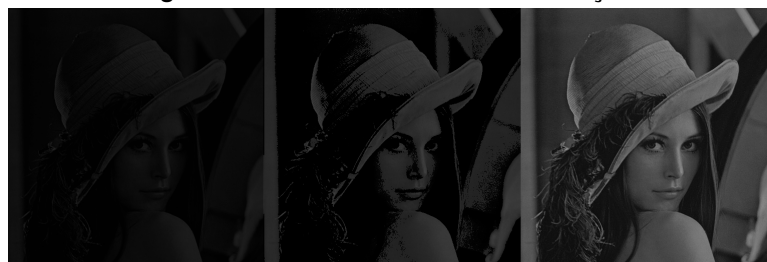
Os sistemas de identificação baseados em biometria são essencialmente sistemas de reconhecimento que, dadas informações biométricas, são capazes de distinguir padrões e classificá-los em diferentes classes ou categorias (MORAES, 2010).

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 representa a técnica biométrica mais adotada atualmente. Embora o reconhecimento de rostos seja uma tarefa simples para as pessoas, ela se revela notavelmente complexa para os computadores. Mesmo em condições desafiadoras, o cérebro humano é capaz de identificar com precisão uma pessoa com base em sua imagem facial, apesar das variações na iluminação, distorções ou deformações.

Embora os sistemas biométricos faciais apresentem um desempenho aceitável em ambientes comerciais, ainda estão sujeitos a restrições relacionadas ao ambiente, como variações na iluminação (Figura 8) e ângulos das imagens. 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.

Figura 8 – Rostos em diferentes iluminações



Fonte: Adaptado de OpenCV (2023c).

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.

Essas etapas desempenham um papel fundamental na avaliação da imagem, eliminando informações redundantes e irrelevantes. Por exemplo, se o algoritmo identifica uma ou mais faces na imagem, essas são extraídas da imagem original para análise individual. É importante notar que, quando a entrada do sistema é uma sequência de vídeo, a dimensão temporal também é considerada, tornando essencial que o algoritmo opere em tempo real, com desempenho crítico, para permitir a detecção em tempo real (BOECHAT, 2008).

Muitos algoritmos de detecção facial requerem treinamento para produzir resultados satisfatórios. Esse treinamento envolve o uso de diversas imagens de faces e objetos diferentes.

Os algoritmos de reconhecimento facial têm a capacidade de identificar indivíduos com base em características específicas, como o tamanho dos olhos, nariz e boca. Essas características são usadas para localizar imagens correspondentes que se assemelham à imagem da face capturada. Além disso, os algoritmos desse tipo normalmente armazenam informações relevantes apenas da região da imagem que contém as características de interesse, conforme pode ser observado na Figura 9. De acordo com (VIOLA; JONES, 1993), um dos primeiros sistemas de reconhecimento facial baseava-se em um modelo de técnicas aplicadas a um conjunto de características faciais, resultando em uma representação facial compacta e correspondente.

Figura 9 – Pontos de referência a partir de características faciais



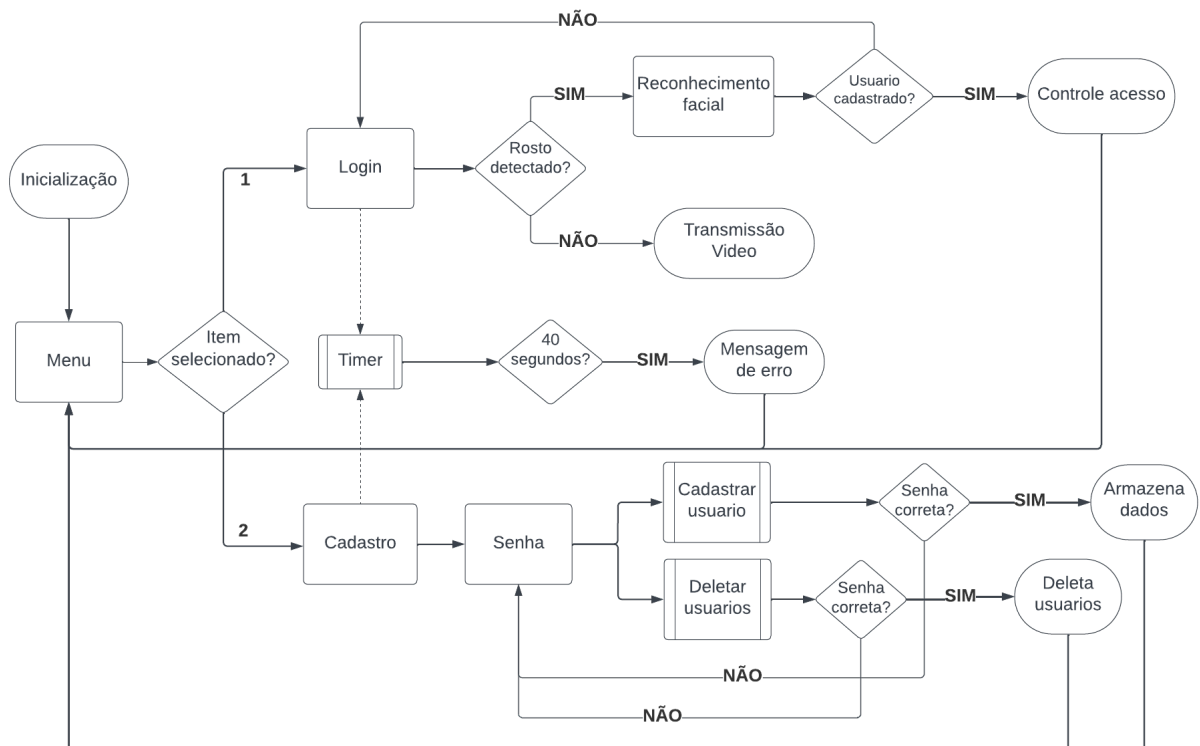
Fonte: Adaptado de OpenCV (2023a).

3 METODOLOGIA

O projeto foi estruturado em duas etapas principais: o desenvolvimento da infraestrutura de *hardware* e a criação do *software*. Desta forma, além da construção do protótipo físico, será desenvolvido o programa de controle de acesso por biometria, atendendo todos os requisitos do projeto, ou seja, desde o processamento de imagens até o acionamento de um relé.

O fluxograma apresentado na Figura 10 oferece uma visão simplificada do funcionamento do *software* do projeto. O sistema de controle de acesso por biometria facial opera em dois ciclos principais: o primeiro é dedicado à autenticação do usuário, enquanto o segundo é responsável pelo cadastro de usuários. Além disso, há um ciclo obrigatório com um temporizador em execução em segundo plano. Esse ciclo é ativado automaticamente sempre que um dos ciclos principais é iniciado, com o intuito de encerrar quaisquer atividades pendentes e prevenir possíveis *loops* dentro do sistema.

Figura 10 – Fluxograma do *firmware*

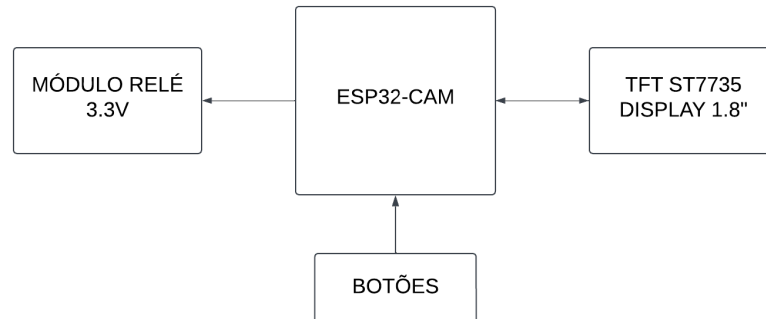


Fonte: Autoria própria (2023).

Para a execução desse programa, é necessário o uso de um *hardware* capaz de processá-lo. Portanto, a primeira etapa do projeto foi dedicada à construção do protótipo físico. E com o intuito de facilitar a compreensão desta parte do projeto, foi criado o diagrama apresentado na Figura 11. Conforme evidenciado, o ESP32-CAM é o módulo central, encarregado do processamento de dados e da coordenação das informações aos demais módulos. Para melhorar a interação com os usuários, é adicionado o módulo com botões e uma interface

gráfica (*display*). Por fim, o módulo relé é responsável pelo controle de acesso, podendo acionar diferentes tipos de fechaduras elétricas.

Figura 11 – Diagrama de blocos do *hardware*



Fonte: Autoria própria (2023).

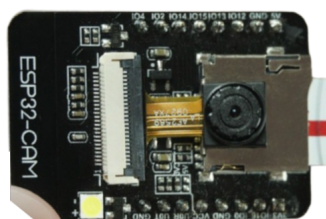
Como um dos objetivos do projeto é o desenvolvimento de um protótipo de baixo custo, a versão selecionada para essa finalidade é o ESP32-CAM, que se destaca por integrar um *chip* ESP32, uma câmera, uma entrada para cartão SD e LED de alto brilho.

3.1 Microcontrolador ESP32-CAM

O ESP32-CAM (conforme ilustrado na Figura 12) é um microcontrolador de alto desempenho, desenvolvido pela empresa *Espressif Systems®* e que se destaca por sua acessibilidade. Embora compacto, é uma escolha ideal para este projeto devido à sua rica variedade de recursos e vantagens. Ele apresenta uma câmera integrada à placa, um processador dual-core de 32 bits capaz de executar tarefas em tempo real e disponibiliza 16 pinos de Entrada/Saída (E/S).

Neste projeto, o ESP32-CAM desempenhou um papel central, sendo responsável pelo processamento de dados, análise das informações e controle dos demais componentes de *hardware*. Isso incluiu o gerenciamento de dispositivos adicionais e a coordenação das funções necessárias para a aplicação proposta.

Figura 12 – ESP32-CAM

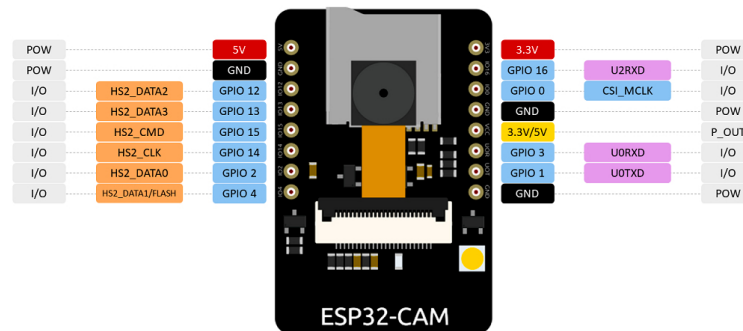


Fonte: Adaptado de Espressif Systems (2022b).

3.1.1 Pinos de Entrada/Saída (E/S)

Os 16 pinos de Entrada/Saída (E/S) do ESP32-CAM (Figura 13) desempenham um papel crucial na versatilidade e funcionalidade deste microcontrolador. Esses pinos oferecem uma interface flexível para conectar o ESP32-CAM a uma ampla variedade de dispositivos e periféricos externos, permitindo que ele interaja com o ambiente e execute tarefas específicas de acordo com as necessidades do projeto.

Figura 13 – GPIO disponíveis do ESP32-CAM



Fonte: Adaptado de Random Nerd Tutorials (2023).

Esses pinos são fundamentais para a comunicação com sensores, atuadores, dispositivos de armazenamento, *displays* e muitos outros componentes eletrônicos, tornando o ESP32-CAM adequado para inúmeras aplicações, desde sistemas de segurança e monitoramento, até projetos de automação residencial.

No quadro a seguir (Quadro 1), são detalhadas as funcionalidades dos 16 pinos de Entrada/Saída (E/S) disponíveis no ESP32-CAM. O entendimento destes pinos, possibilita aos desenvolvedores a flexibilidade de personalizar e expandir suas aplicações de acordo com suas necessidades específicas.

Quadro 1 – Portas de Entrada/Saída ESP32-CAM

Pinos	Descrição
5V	Pino de entrada para alimentação do circuito do ESP32.
3GND	3 pinos de aterramento, usado para referência de potencial zero.
GPIO12	Pino de propósito geral.
GPIO13	Pino de propósito geral.
GPIO15	Pino de propósito geral.
GPIO14	Pino de propósito geral.
GPIO2	Pino de propósito geral.
GPIO4	Pino de propósito geral e pode ser utilizado para acionar o Flash do ESP32.
3.3V	Pino de fornecimento de energia de 3,3V.
GPIO16	Este pino sempre fica em nível lógico alto e é utilizado para alimentar o circuto de PSRAM.
GPIO0	Pino de propósito geral, entretanto este pino é responsável pelo clock da câmera.
3.3V/5V	Pode fornecer energia de 3,3V ou 5V para outros dispositivos.
GPIO3	Pino de entrada de dados UART (RX) para comunicação serial.
GPIO1	Pino de saída de dados UART (TX) para comunicação serial.

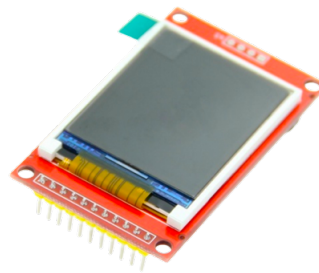
Fonte: Autoria própria (2023).

3.2 Interface gráfica

O *Display* LCD TFT (*Thin-Film Transistor*) de 1.8 polegadas, com resolução de 128x160 *pixels* e *driver* ST7735 (Figura 14) é um componente popular utilizado em uma variedade de aplicações eletrônicas, devido à sua capacidade de fornecer uma interface visual clara e interativa. Esse tipo de *display* é frequentemente empregado em projetos que requerem a exibição de informações, gráficos e interação direta com o usuário.

Neste contexto, o uso deste *display* no projeto tem o propósito de aprimorar a experiência do usuário, fornecendo uma representação visual clara da aplicação. Além disso, sua biblioteca de fácil utilização simplifica o processo de desenvolvimento do projeto, tornando-o mais acessível e eficaz.

Figura 14 – *Display* LCD TFT 1.8"

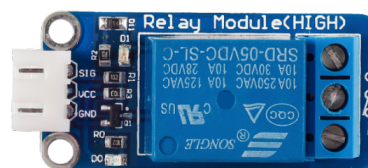


Fonte: Adaptado de LCD wiki (2023).

3.3 Módulo de acionamento

Um módulo relé, como apresentado na Figura 15, é um componente eletrônico amplamente utilizado em projetos que envolvem controle e automação de dispositivos elétricos. Ele desempenha um papel essencial ao permitir o controle de circuitos de alta potência por meio de sinais de baixa potência.

Figura 15 – Módulo Relé

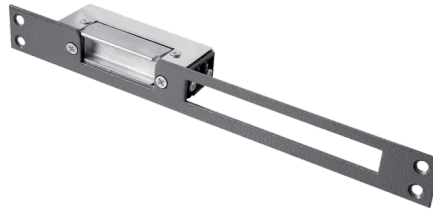


Fonte: Sunfounder (2022)

Quando se trata de fechaduras eletrônicas, como o da Figura 16, os módulos relé desempenham um papel crucial, facilitando o funcionamento e a segurança do sistema de controle

de acesso. Geralmente, essas fechaduras incluem um mecanismo de trinco que pode ser controlado eletronicamente. O módulo relé é utilizado para controlar a ativação e desativação desse mecanismo, quando um usuário autorizado fornece uma credencial válida (como uma senha, cartão RFID ou impressão digital), o sistema eletrônico de controle gera um sinal de baixa potência para acionar o módulo relé. O relé fecha seu contato, permitindo a passagem de energia para o mecanismo de destravamento da fechadura, liberando assim o acesso.

Figura 16 – Fecho Elétrico



Fonte: AGL Soluções em Segurança Eletrônica (2022)

3.4 Desenvolvimento do *software*

Para o desenvolvimento do *software*, foi essencial escolher uma plataforma de desenvolvimento capaz de programar e gravar códigos nos microcontroladores ESP32. Duas opções amplamente conhecidas são o Arduino IDE e o PlatformIO. Além disso, o desenvolvimento exigiu um estudo aprofundado das bibliotecas disponíveis para atender aos requisitos do projeto, tais como o reconhecimento facial, transmissão em tempo real de imagens em um *display* LCD, implementação de um *timer* e a manipulação dos dados de entrada e saída.

3.4.1 PlatformIO

A plataforma escolhida para esse projeto foi o PlatformIO, que é uma ferramenta indispensável para quem trabalha com dispositivos microcontrolados, como o ESP32. Projetado para simplificar o processo de desenvolvimento e programação de microcontroladores, o PlatformIO oferece uma ampla gama de recursos e uma abordagem unificada que facilita o trabalho com diferentes plataformas de *hardware* e ambientes de desenvolvimento.

Quando se trata do ESP32, o PlatformIO desempenha um papel crucial, permitindo que desenvolvedores e entusiastas de eletrônica programem e depurem suas aplicações de maneira eficiente. O PlatformIO é projetado para funcionar com diversos editores de código populares, como *Visual Studio Code* (VSCode), Atom e CLion. Isso permite que os desenvolvedores escolham a IDE que melhor se adapte às suas preferências.

Por fim, outros dois outros pontos fortes da ferramenta PlatformIO podem ser citados: a plataforma possui um gerenciador de bibliotecas embutido que facilita a pesquisa, instalação

e atualização de bibliotecas de código-fonte aberto. Isso é particularmente útil para reutilizar código existente e acelerar o desenvolvimento, como também sua simplificação no processo de compilação e carregamento de código para o *hardware* de destino.

3.4.2 Biblioteca ESP-DL

Para identificação de rostos e reconhecimento facial, foram utilizados os recursos disponíveis da biblioteca ESP-DL.

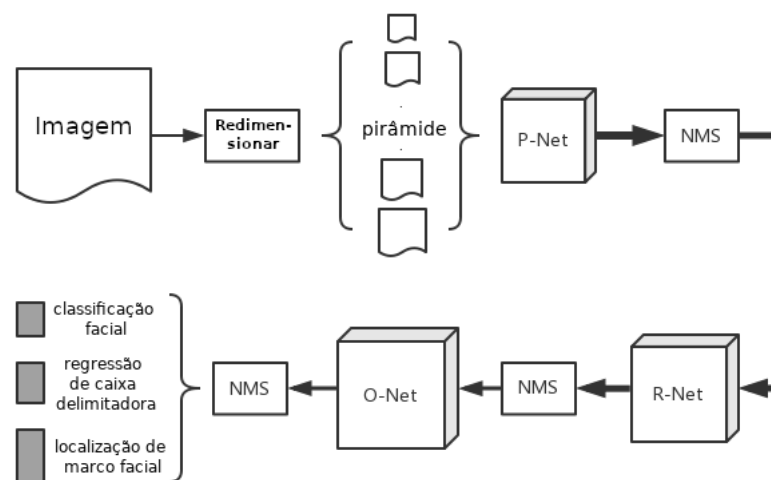
O ESP-DL é uma biblioteca de alto desempenho dedicada ao ESP32, ESP32-S2, ESP32-S3 e ESP32-C3, projetada para recursos de aprendizagem profunda.

O ESP-DL (2023a) disponibiliza APIs para tarefas como inferência de redes neurais (NN), processamento de imagens, operações matemáticas e inclui alguns modelos de aprendizado profundo. Com essa biblioteca, os desenvolvedores podem aproveitar os SoCs (System-on-Chip) da *Espressif* de maneira simples e ágil para a implementação de uma ampla variedade de aplicações.

Dentre os recursos disponíveis do ESP-DL, se encontra o ESP-Face, componente que fornece funções de detecção e reconhecimento facial e também operações de rede neural. O método *face detect* utiliza o modelo MTNM (*Multi-Task Memory Network*) para a detecção de rostos humanos. Esse modelo, especialmente projetado para dispositivos embarcados, apresenta uma operação eficiente que se baseia na arquitetura móvel *MobileNetV2* e utiliza redes convolucionais em cascata multitarefa.

Na Figura 17 é demonstrado o fluxo de trabalho do MTNM.

Figura 17 – Diagrama de trabalho do MTNM



Fonte: Adaptado de ESP-DL (2023c).

O *MobileNetV2* faz parte de uma nova geração de redes neurais convolucionais profundas voltadas para a visão computacional. Essa arquitetura permite a implementação em tempo

real de aplicativos de classificação, detecção e alinhamento de objetos em dispositivos móveis pessoais, destacando-se por sua capacidade de processamento leve.

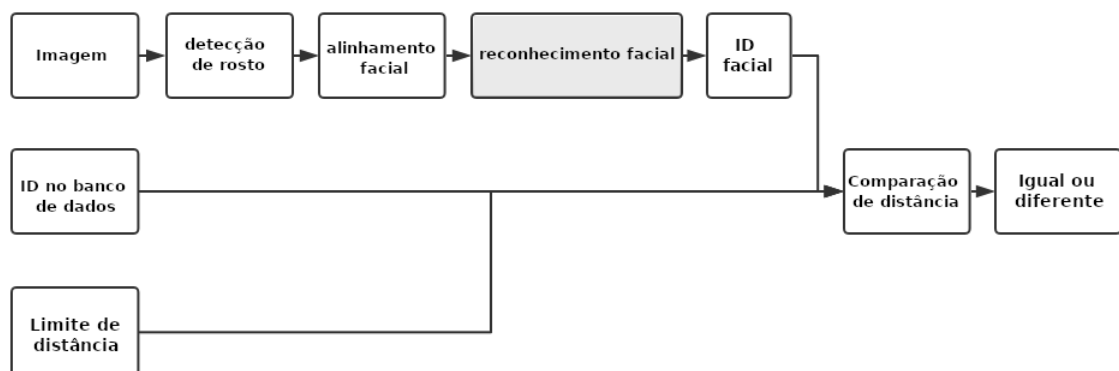
O MTMN se beneficia de redes neurais pré-treinadas, que foram desenvolvidas com base em um vasto banco de dados contendo mais de um milhão de imagens do ImageNet. Essas redes aprenderam representações de recursos de mais de 1.000 categorias de objetos, fornecendo uma base sólida para a detecção de rostos (LUNA *et al.*, 2022).

Uma característica distintiva do MTMN é sua estrutura multitarefa de aprendizagem em cascata. Essa abordagem permite que o modelo resolva desafios encontrados em ambientes diversos, como variações de iluminação, oclusões e poses variadas. O MTMN é composto por três estágios de redes convolucionais profundas que preveem a localização de faces e pontos de referência, proporcionando uma detecção precisa que varia de informações gerais a detalhes específicos (LUNA *et al.*, 2022).

No contexto do reconhecimento facial, uma vez que um rosto humano tenha sido detectado por meio do procedimento mencionado anteriormente, é possível realizar uma verificação comparando-o com os rostos previamente cadastrados. A entrada para esse processo é a imagem original juntamente com os resultados obtidos na etapa de detecção facial.

O método de reconhecimento facial, denominado *recognize face* faz uso do modelo FRMN (*Face Recognition Memory Network*), que também se baseia na arquitetura móvel *MobileNetV2* e emprega o algoritmo *ArcFace*. Para otimizar a complexidade computacional, as imagens foram treinadas em dimensões reduzidas (56x56). Na Figura 18, é possível visualizar todas as etapas do algoritmo no processo de reconhecimento facial.

Figura 18 – Fluxograma do funcionamento do método *recognize face*



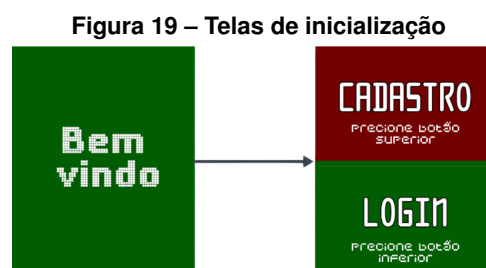
Fonte: Adaptado de ESP-DL (2023b).

Esse procedimento, além de oferecer um processo de reconhecimento facial eficiente, permite a comparação precisa entre o rosto identificado e as informações previamente cadastradas, contribuindo para uma solução de alta qualidade em sistemas de identificação e autenticação.

3.4.3 Fluxo de telas

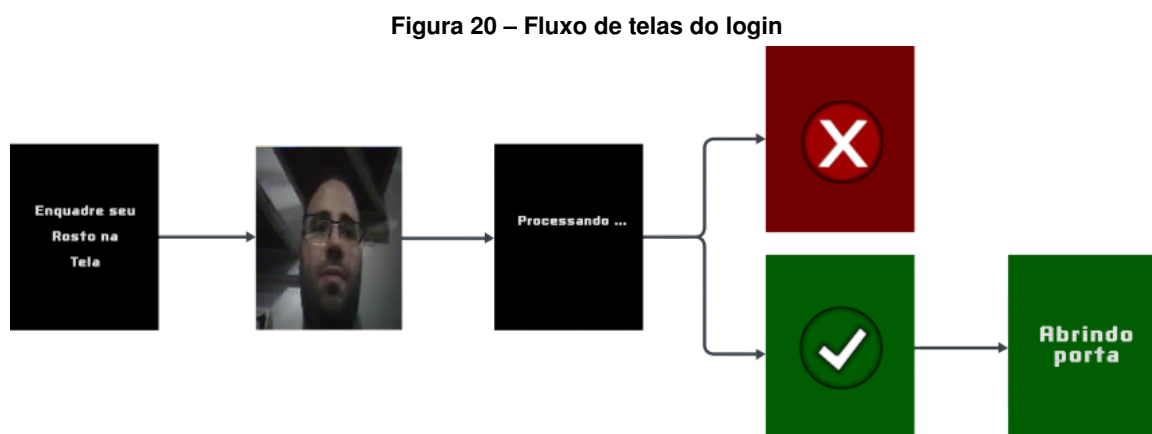
Os recursos gráficos fornecidos pelo *display* LCD desempenham um papel fundamental na usabilidade da aplicação. Nesse contexto, a elaboração do fluxo de telas se torna essencial para proporcionar aos usuários uma experiência eficiente. Todos os fluxos foram planejados e projetados com o objetivo de guiar o usuário por meio de diferentes interações e funcionalidades.

O primeiro conjunto de telas (Figura 19), referente à inicialização dos recursos utilizados no programa do protótipo, abrange o momento em que a câmera, os sensores e o SPIFFS (Sistema de Arquivos Flash de Interface Serial Periférica) são ativados. Além disso, a lista de usuários cadastrados é inicializada antes de exibir a tela de menu.



Fonte: Autoria própria (2023).

Ao chegar no menu e selecionar a opção de login, o usuário inicia o fluxo de telas de login. Inicialmente, é exibida uma mensagem de orientação para enquadrar o rosto dentro do campo de visão da câmera. Se o usuário estiver cadastrado, uma mensagem de sucesso é exibida e em seguida, o módulo do relé é acionado. Caso contrário, o *timer* é executado em segundo plano e quando o tempo se esgota, uma mensagem de erro é exibida, como representado na Figura 20.

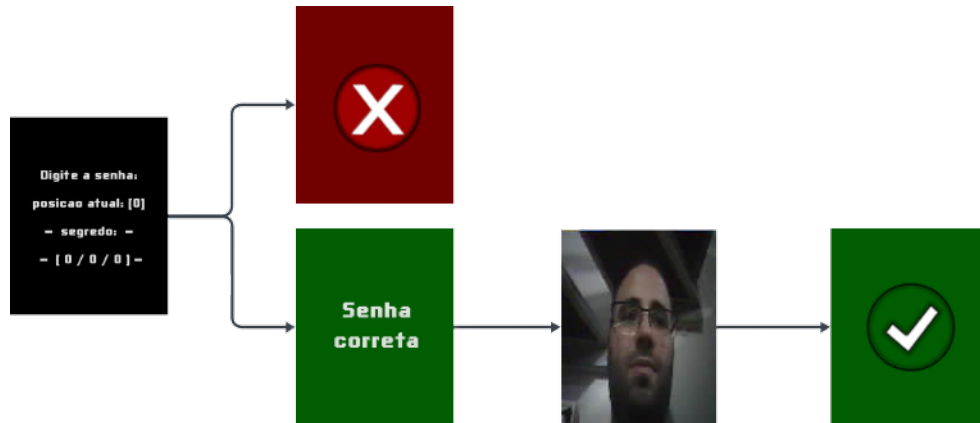


Fonte: Autoria própria (2023).

No entanto, se o usuário escolher a opção de cadastro no menu, ele deverá seguir o fluxo descrito na Figura 21. Na primeira etapa, é solicitado ao usuário para digitar a senha. Se a senha estiver correta, uma mensagem de "senha correta" é exibida e o processo de identificação e reconhecimento facial é iniciado. Se tudo ocorrer conforme o esperado, os dados são

armazenados na memória RAM ou na memória flash. Caso contrário, o usuário visualizará uma mensagem de erro.

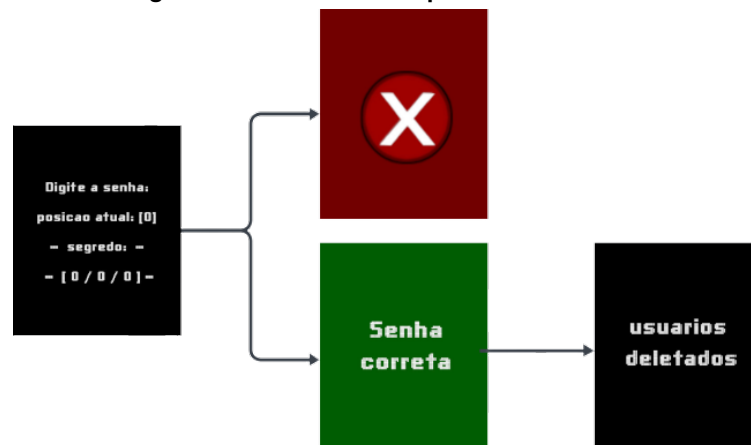
Figura 21 – Fluxo de telas do cadastro



Fonte: Autoria própria (2023).

Por fim, o último fluxo principal é o processo de exclusão de usuários (Figura 22), que se assemelha ao fluxo de cadastro. Como observado, em ambos os casos, a primeira tela solicita a inserção da senha e o usuário tem aproximadamente 40 segundos para descobrir ou digitar a senha correta. Durante esse processo, podem ser exibidas mensagens de erro ou sucesso. Se tudo ocorrer conforme o esperado, a mensagem "usuários deletados" é exibida.

Figura 22 – Fluxo de telas para deletar usuário



Fonte: Autoria própria (2023).

3.4.4 Gravação do código

Para a gravação do código no ESP32-CAM, foi essencial o uso do módulo adaptador ESP32-CAM MB (conforme representado na Figura 23). Este módulo desempenhou um papel importante, estabelecendo uma conexão entre o ESP32-CAM e um computador por meio do cabo USB.

Para desenvolvimento do protótipo, elaborou-se um diagrama elétrico detalhado, conforme ilustrado na Figura 24. Este diagrama foi construído com base em um circuito previamente testado e montado em uma placa de prototipagem ("protoboard"). A escolha dos conectores do tipo borne KRE para as conexões de entrada e saída se justifica pela praticidade e segurança que oferecem, devido ao seu encaixe lateral que simplifica a conexão com os componentes eletrônicos.

Figura 23 – Módulo Adaptador ESP32-CAM MB

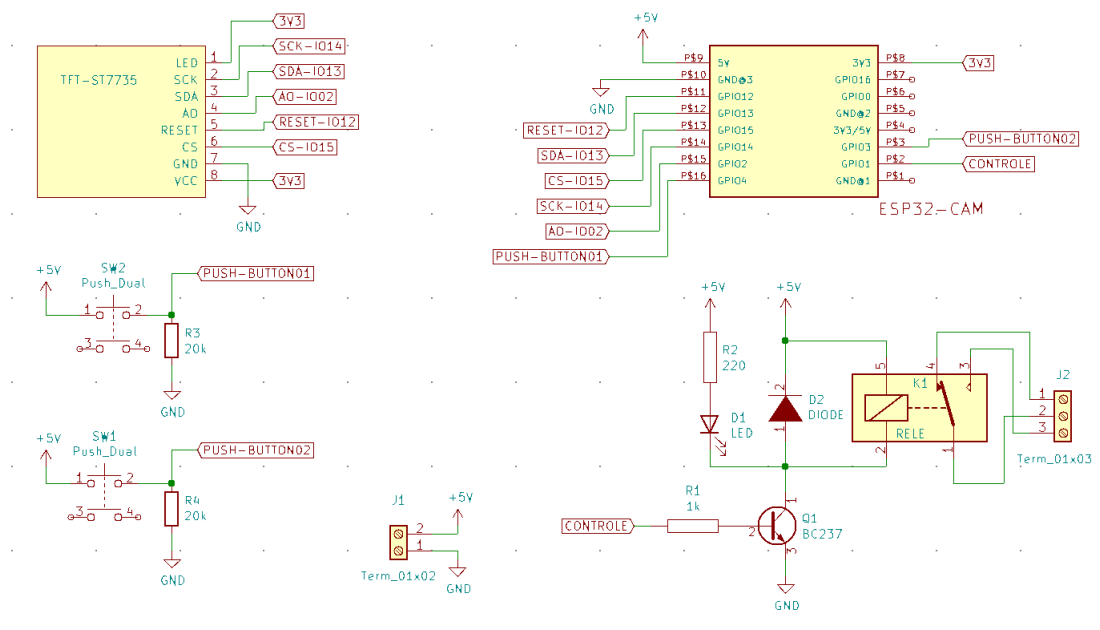


Fonte: Adaptado de Robo Builders (2023).

3.5 Desenvolvimento do protótipo

Para desenvolvimento do protótipo, foi fundamental criar um diagrama elétrico detalhado para guiar a montagem do circuito. O diagrama apresentado na Figura 24, foi elaborado com base no circuito pré-testado e montado em uma placa de prototipagem ("protoboard").

Figura 24 – Diagrama elétrico do protótipo

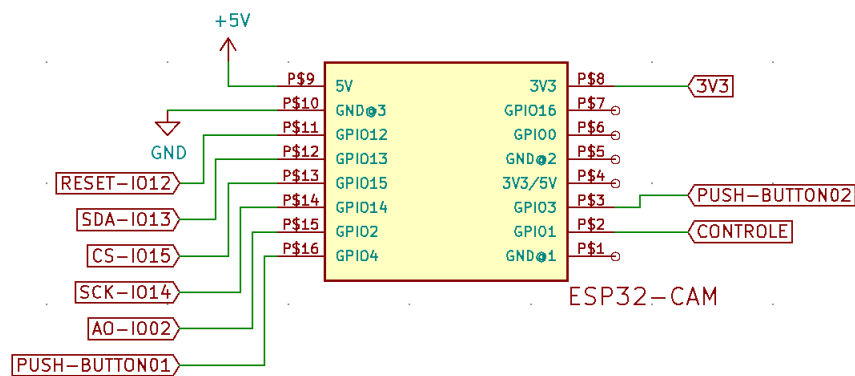


Fonte: Autoria própria (2023).

O diagrama elétrico do protótipo divide o circuito em quatro blocos principais: o ESP32-CAM, o TFT ST7735, o módulo de relé e o módulo de botões (*push button*). O bloco principal, que é o ESP32-CAM, possui 16 pinos de entrada/saída (GPIOs), como representado na Figura 25 e desempenha o papel de controle e coordenação do sistema como um todo. Dos 16 pinos disponíveis, 7 são dedicados ao *display* TFT (GPIOs 2, 12, 13, 14 e 15), 2 são reservados para os botões (GPIOs 4 e 3) e 1 pino é utilizado como saída para controlar o módulo do relé (GPIO 1).

Importante mencionar que algumas GPIOs têm funções específicas. Por exemplo, a GPIO 16 permanece em nível lógico alto e é utilizada para habilitar a memória PSRAM. Além disso, a GPIO 0 é designada como *clock* da câmera e não pode ser realocada para outras finalidades, uma vez que isso afetaria o funcionamento adequado da captura de imagens. Essas atribuições de GPIOs foram cuidadosamente planejadas para garantir o correto funcionamento de cada componente do protótipo.

Figura 25 – Diagrama elétrico do ESP32-CAM



Fonte: Autoria própria (2023).

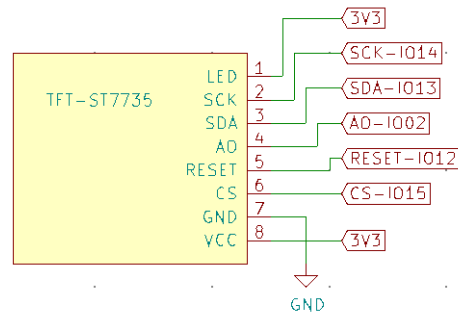
O segundo bloco corresponde ao controlador ST7735 (Figura 26), um componente projetado para o gerenciamento de *displays* TFT de tamanho reduzido e com capacidade de exibir cores. A principal função desse controlador é administrar a apresentação de informações na tela, permitindo a criação de gráficos e a exibição de texto colorido.

A tela em si é composta por uma matriz de *pixels* coloridos, em que cada *pixel* é formado por subpixels nas cores vermelha, verde e azul (RGB), possibilitando a exibição de uma vasta gama de cores. Os pinos SCK (*Serial Clock*), SDA e CS (*Chip Select*) são utilizados para a comunicação serial com o microcontrolador. Por sua vez, o pino de *reset* é designado para reiniciar o *display* em caso de falhas ou erros.

Adicionalmente, o pino A0 desempenha um papel fundamental ao indicar se os dados transmitidos se referem a comandos de controle (estado *LOW*) ou a dados de *pixel* (estado *HIGH*), desempenhando um papel crucial no funcionamento adequado do controlador ST7735.

O bloco que compreende os botões desempenha um papel fundamental na interatividade do projeto, pois permite a seleção de itens no menu e a inserção dos valores da senha.

Figura 26 – Diagrama elétrico do *Display* TFT

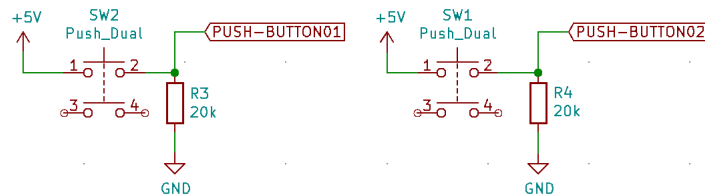


Fonte: Autoria própria (2023).

A estrutura dos botões é ilustrada no circuito apresentado na Figura 27, e cada botão é capaz de enviar um sinal de nível lógico baixo quando não pressionado e de nível lógico alto quando acionado, transmitindo esses sinais ao microcontrolador.

Devido a mudança de estado do botões ao alterar o sinal elétrico conforme são pressionados ou soltos, permite ao microcontrolador reconhecer as ações do usuário, possibilitando a navegação no aplicativo de forma eficiente e prática. Isso torna esses componentes essenciais para a interatividade do protótipo e contribuem significativamente para a experiência do usuário.

Figura 27 – Diagrama elétrico dos botões



Fonte: Autoria própria (2023).

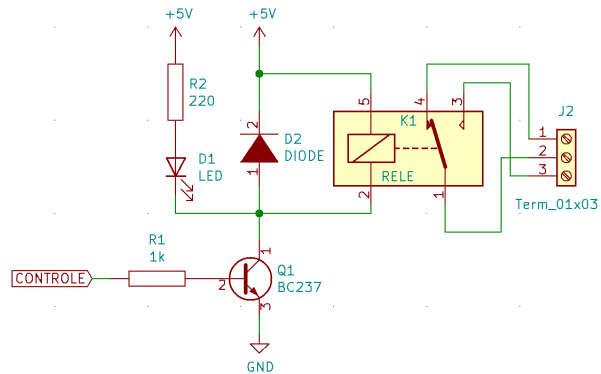
O relé é um dispositivo eletromecânico amplamente utilizado para o controle de circuitos elétricos, permitindo a comutação (abertura ou fechamento) por meio de um sinal elétrico aplicado à sua bobina.

O módulo de relé, conforme apresentado na (Figura 28), consiste em um circuito que viabiliza que um microcontrolador envie um sinal de baixa potência para a base de um transistor. A conexão do coletor do transistor à bobina do relé viabiliza o seu acionamento quando o transistor entra em estado de saturação. Isso, por sua vez, permite que o ESP32 controle dispositivos de alta potência por meio de sinais de baixa potência. Um elemento crucial nesse circuito é o diodo em paralelo ao relé, que também é conhecido como diodo de roda livre.

O diodo de roda livre desempenha um papel essencial na proteção do circuito contra picos de tensão e corrente gerados quando a bobina do relé é desativada. Esse fenômeno ocorre devido à interrupção abrupta da corrente que fluía através da bobina, criando uma sobretensão reversa que poderia potencialmente danificar os componentes do circuito. O diodo age como

um caminho de baixa resistência para a corrente, permitindo um caminho controlado para a dissipação da energia excedente, evitando danos aos componentes sensíveis do circuito. Portanto, o diodo de roda livre é crucial para garantir a integridade e a confiabilidade do sistema elétrico.

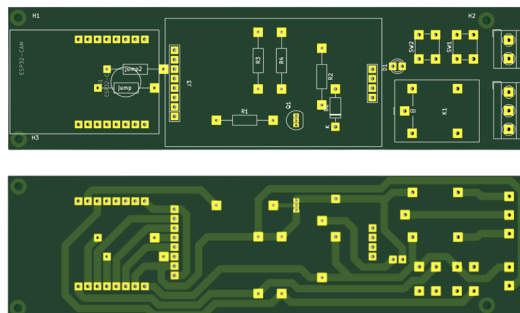
Figura 28 – Diagrama elétrico do módulo relé



Fonte: Autoria própria (2023).

Com base no esquema elétrico e na necessidade de criar um protótipo compacto e eficiente, o projeto da PCB (*Printed Circuit Board* ou Placa de Circuito Impresso) foi concebido com o objetivo de otimizar o aproveitamento de espaço, como pode ser observado na Figura 29. Nessa placa, os componentes estão dispostos de forma organizada, seguindo uma lógica de uso e, ao mesmo tempo, minimizando o espaço ocupado para garantir uma solução compacta e funcional. A disposição estratégica dos componentes na PCB é crucial para a eficiência e o desempenho do protótipo.

Figura 29 – Projeto da placa de circuito impresso do protótipo



Fonte: Autoria própria (2023).

Após a conclusão do projeto da PCB, procedeu-se à fabricação da placa e à integração dos componentes eletrônicos. Como ilustrado na Figura 30, foram adicionados os componentes de acordo com o projeto. Uma escolha estratégica foi a inclusão de barras de pinos fêmea no lugar dos conectores do ESP32-CAM e do *Display* TFT. Essa decisão visou possibilitar a remoção e substituição desses componentes com facilidade. Esse recurso é especialmente útil para o ESP32, permitindo a conexão a um gravador de código externo sempre que necessário, proporcionando maior flexibilidade e versatilidade ao protótipo.

Figura 30 – Placa manufaturada



Fonte: Autoria própria (2023).

Como parte final do processo, uma caixa foi projetada e fabricada para cumprir dois propósitos essenciais: proteger o circuito eletrônico e oferecer um acabamento esteticamente agradável para o usuário. A caixa, como ilustrada na Figura 31, foi dimensionada a partir das dimensões da placa já confeccionada. A modelagem 3D foi realizada para que a caixa pudesse ser impressa em 3D e posteriormente acoplada à placa. Esse invólucro não apenas protege o protótipo, mas também contribui para uma apresentação mais profissional e amigável ao usuário, resultando em uma experiência mais agradável de uso.

Figura 31 – Placa montada



Fonte: Autoria própria (2023).

4 RESULTADOS E DISCUSSÃO

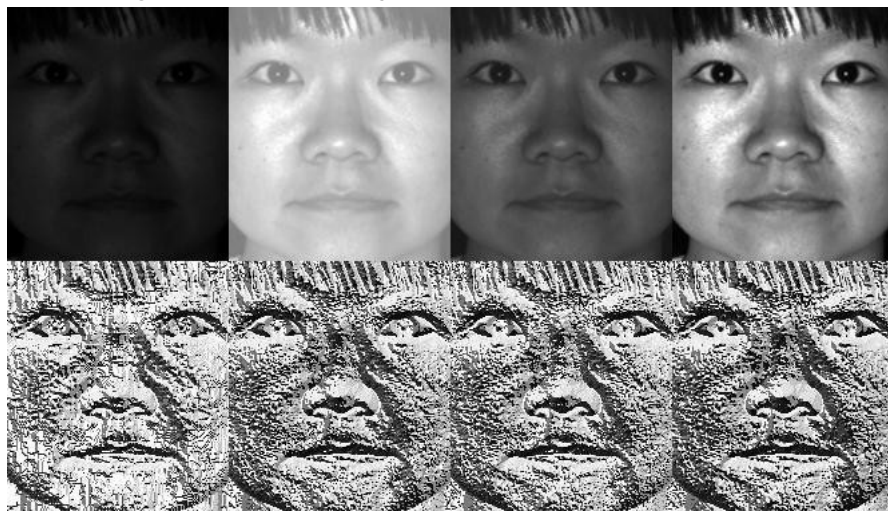
Para alcançar resultados ainda mais satisfatórios, especialmente no que diz respeito ao processo de identificação e reconhecimento facial, seriam necessários recursos de processamento de imagem adicionais para o ESP32. Apesar de o *chip* ESP32 apresentar considerável poder de processamento, ele nem sempre oferece recursos de *hardware* suficientes para tarefas intensivas de processamento de imagem e visão computacional. Como resultado, a maioria das bibliotecas de visão computacional e seus métodos não estão disponíveis para o ESP32.

No entanto, é possível realizar processamento de imagem básico e funções relacionadas à detecção e reconhecimento facial no ESP32, devido a otimizações de código de aprendizado profundo (ESP-DL) e implementações específicas voltadas para dispositivos com menor capacidade de processamento.

Para uma comparação qualitativa dos resultados atuais com outras implementações, a disponibilidade de bibliotecas de visão computacional, como o OpenCV, seria altamente benéfica. Embora as bibliotecas oficiais sejam limitadas, é possível encontrar bibliotecas não oficiais desenvolvidas por colaboradores que possuem métodos de processamento de imagem inspirados nas bibliotecas já existentes. Avaliar a influência da luminosidade nas imagens e a eficácia de parâmetros ou funções específicas é importante para combinar métodos alternativos visando obter melhores resultados.

Na Figura 32, é possível observar as imagens com níveis de luminosidade diferentes. O cenário ideal seria que, independentemente da iluminação estar alta ou baixa, o resultado do processo de reconhecimento fosse igualmente eficaz, assemelhando-se ao desempenho em condições ideais de luminosidade. No entanto, é fundamental considerar que outros tipos de erros ainda podem ocorrer.

Figura 32 – Transformações monótonas em escala de cinza



Fonte: Adaptado de OpenCV (2023b).

O protótipo atual satisfaz praticamente todas as necessidades do projeto, como detec-

ção e reconhecimento facial, cadastro de usuários e implementação do temporizador. Portanto, atende aos requisitos estabelecidos durante o desenvolvimento.

No entanto, há espaço para melhorias a curto e longo prazo. Isso inclui atualizações contínuas, como a possibilidade de configurar o número de usuários cadastrados, a exibição de IDs de usuários e a adição de métodos para excluir usuários por ID. Além disso, a funcionalidade de permitir que um usuário administrador altere senhas de cadastro e a de remover todos os usuários.

Outra melhoria relevante seria a integração do protótipo em aplicativos e servidores da web, ampliando suas possibilidades de aplicação prática, como em sistemas de controle de acesso residencial ou empresarial totalmente baseados na web.

Por último, uma melhoria significativa envolveria a criação de uma placa personalizada, partindo do zero, usando inicialmente apenas o *chip* ESP32. Isso permitiria a liberação do I2C para uso geral, possibilitando a integração de novos recursos devido ao aumento da quantidade de portas (GPIO) disponíveis.

5 CONCLUSÃO

O trabalho, de forma geral, apresentou bons resultados. O desenvolvimento e implementação do protótipo de controle de acesso por reconhecimento facial utilizando o ESP32-CAM mostraram-se promissores, atendendo aos requisitos do projeto. Desta forma, o sistema demonstrou a capacidade de detectar e reconhecer rostos, além de executar com sucesso tarefas como cadastro de usuários e a implementação de um temporizador.

No entanto, algumas limitações foram identificadas durante a elaboração do protótipo. Notavelmente, a falta de recursos de processamento do ESP32 limitou a plena capacidade de processamento de imagem e visão computacional. A ausência de bibliotecas de visão computacional amplamente disponíveis para o ESP32 também representou um desafio. No entanto, soluções alternativas foram aplicadas, permitindo o reconhecimento facial com relativo sucesso.

Para aprimorar ainda mais o sistema, seria essencial a inclusão de bibliotecas de visão computacional mais abrangentes, como o OpenCV, que ofereceriam mais opções e métodos de processamento de imagem. Além disso, a avaliação da influência da luminosidade na precisão do reconhecimento é um tópico importante a ser investigado, bem como a otimização dos parâmetros para melhorar a taxa de assertividade.

Apesar das limitações, o protótipo atendeu a praticamente todos os requisitos do projeto e mostrou-se uma base sólida para desenvolvimentos futuros. A implementação de melhorias, como a possibilidade de configurar o número de usuários cadastrados, exibir o ID do usuário e permitir a exclusão de usuários por ID, tornaria o sistema ainda mais flexível e prático.

Além disso, a perspectiva de integrar o protótipo em aplicativos e servidores web expandiria suas aplicações práticas, tornando-o útil em sistemas de controle de acesso online.

Conforme mencionado anteriormente, uma melhoria substancial poderia ser alcançada ao desenvolver uma placa personalizada, utilizando apenas o chip ESP32. Isso permitiria uma maior flexibilidade na alocação de recursos, liberando GPIOs adicionais para integração de novos recursos e funcionalidades.

Em resumo, o protótipo de controle de acesso por reconhecimento facial demonstrou ser uma solução viável e suas limitações podem ser superadas com melhorias no *hardware*, *software* e integração em sistemas mais amplos. Com uma abordagem contínua de desenvolvimento e aprimoramento, esse sistema tem o potencial de se tornar uma ferramenta poderosa para controle de acesso em diversas aplicações.

REFERÊNCIAS

- AGL SOLUÇÕES EM SEGURANÇA ELETRÔNICA. **Fecho elétrico para aplicação, em portas de madeira ou metal**. 2022. Disponível em: <https://www.aglbrasil.com/fecho>. Acesso em: 05 nov. 2022.
- BOECHAT, G. C. **Proposta de um modelo de arquitetura biométrica para identificação pessoal com estudo da dinâmica da digitação**. 2008. Dissertação (Dissertacao de mestrado) — Universidade Federal do Pernambuco, Ciências da Computação, Campinas, 2008.
- CAVALCANTI, G. D. da C. **Composição de biometria para sistemas multimodais de verificação de identidade pessoal**. 2005. Tese (Tese de doutorado) — Programa de Pós-Graduação em Ciência da Computação - PPGCC, Universidade Federal de Pernambuco, Pernambuco, 2005.
- ESP-DL. **ESP-DL User Guide**. 2023. Disponível em: <https://docs.espressif.com/projects/esp-dl/en/latest/esp32/index.html>. Acesso em: 23 set. 2023.
- ESP-DL. **FRMN**. 2023. Disponível em: https://github.com/espressif/esp-dl/blob/v0.6.0/face_recognition/README.md. Acesso em: 25 out. 2023.
- ESP-DL. **MTMN**. 2023. Disponível em: https://github.com/espressif/esp-dl/blob/v0.6.0/face_detection/README.md. Acesso em: 25 out. 2023.
- 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. C.; WOODS, R. E. **Processamento digital de imagens**. 3. ed. São Paulo: Pearson, 2010.
- LCD WIKI. **1.8inch Arduino SPI Module ST7735S**. 2023. Disponível em: http://www.lcdwiki.com/1.8inch_Arduino_SPI_Module_ST7735S_SKU:MAR1801. Acesso em: 12 out. 2023.
- LUNA, J. I. V. *et al.* System for opening cabinets and equipment containers based on facial recognition. **International Research Journal of Advanced Engineering and Science**, v. 7, p. 7, 7 2022. Disponível em: <https://irjaes.com/wp-content/uploads/2022/07/IRJAES-V7N3P58Y22.pdf>. Acesso em: 22 out. 2023.
- MORAES, A. F. de. **Método para avaliação da tecnologia biométrica na segurança de aeroportos**. 2006. Dissertação (Dissertacao de mestrado) — Programa de Pós-Graduação em Engenharia de Computação e Sistemas Digitais - PPGECS, Universidade de São Paulo, São Paulo, 2006.
- MORAES, J. L. de. **Controle de acesso baseado em biometria facial**. 2010. Dissertação (Dissertacao de mestrado) — Programa de Pós-Graduação em Informática - PPGI, Universidade Federal do Espírito Santo, Vitória, 2010.

- OPENCV. **Face landmark detection in an image**. 2023. Disponível em: https://docs.opencv.org/4.x/d2/d42/tutorial_face_landmark_detection_in_an_image.html. Acesso em: 27 set. 2023.
- OPENCV. **Face Recognition with OpenCV**. 2023. Disponível em: https://docs.opencv.org/3.4/da/d60/tutorial_face_main.html. Acesso em: 25 set. 2023.
- OPENCV. **Introduction to Java Development**. 2023. Disponível em: https://docs.opencv.org/4.x/d9/d52/tutorial_java_dev_intro.html. Acesso em: 26 set. 2023.
- PENIDO Édilus de C. C.; TRINDADE, R. S. **Microcontroladores**. 1. ed. Ouro Preto: Rede e-Tec Brasil, 2013.
- RANDOM NERD TUTORIALS. **ESP32-CAM AI-Thinker Pinout Guide: GPIOs Usage Explained**. 2023. Disponível em: <https://randomnerdtutorials.com/esp32-cam-ai-thinker-pinout/>. Acesso em: 28 set. 2023.
- ROBO BUILDERS. **Módulo Adaptador Esp32 Cam MB Com Conversor Usb Serial**. 2023. Disponível em: <https://www.robobuilders.com.br/produto/modulo-adaptador-esp32-cam-mb-com-conversor-usb-serial-nfe.html>. Acesso em: 29 out. 2023.
- 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 (Dissertacao de 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](http://wiki.sunfounder.cc/index.php?title=Relay(HIGH)_for_Arduino_and_Raspberry_Pi). Acesso em: 22 nov. 2022.
- TEIXEIRA, R. F. da S. **Transformação Multi-escala para Segmentação de Impressões digitais**. 2011. Dissertação (Dissertacao de mestrado) — Universidade Estadual de Campinas, Instituto de Computação, Campinas, 2011.
- TERRA. **Soluções de reconhecimento facial ajudarão na reabertura da economia após a pandemia**. 2020. Disponível em: <https://www.terra.com.br/noticias/dino/solucoes-de-reconhecimento-facial-ajudara-na-reabertura-da-economia-apos-a-pandemia,e5458ffd1885519a92fec6be1b64671ftnn9amkk.html>. Acesso em: 19 set. 2022.
- VIEIRA, M. L.; OLIVA, A. D. **Evolução, Cultura e Comportamento Humano**. 1. ed. Florianópolis: Edições do Bosque/CFH/UFSC, 2017.
- VIOLA, P.; JONES, M. J. Face recognition: Features versus templates. **IEEE Transactions on Pattern Analysis and Machine Intelligence**, v. 15, p. 1, 11 1993. Disponível em: <https://doi.org/10.1023/B:VISI.0000013087.49260.fb>. Acesso em: 27 set. 2023.
- VIOLA, P.; JONES, M. J. Robust real-time face detection. **International Journal of Computer Vision**, v. 57, p. 18, 1 2004. Disponível em: <https://doi.org/10.1023/B:VISI.0000013087.49260.fb>. Acesso em: 04 nov. 2022.
- ZHAO, W.; CHELLAPPA, R.; PHILLIPS, J. Face recognition: a literature survey. **ACM Computing Survey**, v. 35, p. 61, 12 2003. Disponível em: <https://dl.acm.org/doi/10.1145/954339.954342>. Acesso em: 04 nov. 2022.